Citrix SD-WAN 11.2

Contents

Release Notes

March 12, 2021

This release notes describes what's new, fixed issues, and known issues applicable to Citrix SD-WAN software release 11 version 2 for the SD-WAN Standard Edition, WANOP, Premium Edition appliances, and SD-WAN Center.

For information about the previous release versions, see the Citrix SD-WAN documentation.

What's New

Edge Security - The Citrix SD-WAN Edge Security capability enables advanced security on Citrix SD-WAN branch appliances. It simplifies information security management by providing a single management and reporting pane for **Network Edge Security**. It eliminates the need for multiple branch solutions by consolidating routing, SD-WAN, and security capabilities on a single appliance. This reduces network complexity, operational cost, and provides a more secure network edge. The Edge Security stack includes the following security functionality:

- Web Filtering
- Anti-Malware
- Intrusion Prevention

> **Note**
>
> The Edge Security is only supported for Citrix SD-WAN deployments managed through the Citrix SD-WAN orchestrator.

LTE network and roaming support - You can now select the mobile network on your Citrix SD-WAN appliances that support the internal LTE modem. The supported networks are 3G, 4G, or both. The roaming option is enabled by default on your LTE appliances, you can choose to disable it.

For more information on LTE network and roaming support, see:

- Configure LTE functionality on 210 SE LTE appliance
- Configure LTE functionality on 110-LTE-WiFi appliance
- User interface for SD-WAN 110-SE appliance
- Remote LTE site management

Metered link redesign - In Citrix SD-WAN UI, a new option - **Approximate Data Already Used** is added under **Metered/Standby Link** section. To track proper metered link usage, the user must enter the

approximate usage on the metered link if the link has already been used for some days in the current billing cycle. This approximate usage is used only for the first cycle.

DHCP support on Fail-To-Wire port - The DHCP client capability is now extended on fail-to-wire port for the branch site with serial High Availability (HA) deployments. This enhancement:

- Allows the DHCP client configuration on the untrusted interface group that has fail-to-wire bridge pair and serial HA deployments.
- Allows DHCP interfaces to be selected as part of **Private Intranet WAN links** in addition to Internet WAN links.

Checkpoint firewall - The **Checkpoint Firewall** is integrated with the SD-WAN 1100 platform to provide advanced security for branch appliances. The **Checkpoint Firewall** supplies the next-generation firewall features such as URL Filtering, Antivirus, SSL Inspection, and Intrusion Prevention. This integration offers the ability to deploy the secure SD-WAN at the branch locations using Citrix SD-WAN Center while managing the security policies with the Check Point management platform.

Enable packet duplication for ICA real-time - Packet duplication is now enabled by default for HDX real-time traffic when multi-stream Independent Computing Architecture (ICA) is in use.

Support 256 virtual paths with SD-WAN SE in Azure - Earlier, 128 virtual paths were supported in Azure. From release 11.2 onwards, 256 virtual paths are supported with SD-WAN SE in Azure.

Subnet support - From release 11.2 onwards, Citrix SD-WAN UI allows /31 subnets for configuring the network address.

TLSv1.3 protocol support in HTTPS and new algorithms support in SSH - Citrix SD-WAN now has TLSv1.3 protocol support in HTTPS access and also has new algorithms support in SSH access.

Cloud Direct support - From release 11.2 onwards, the Cloud Direct service is supported on SD-WAN 2100, 4100, and 6100 appliances. Both SD-WAN Center and Orchestrator allow the Cloud Direct service feature to be deployed on SD-WAN 2100, 4100, and 6,100 appliances. SD-WAN Center supports up to 250 Mbps subscription licenses for Cloud Direct.

WAN link bandwidth sharing when Cloud Direct service is inactive - A WAN link bandwidth is no longer needed to be reserved exclusively for the Cloud Direct service. If the Cloud Direct service is not active then the other services such as virtual path, internet, or intranet services configured on that WAN link can use the bandwidth as per the configured shares.

Fixed Issues

SDWANHELP-1098: Citrix SD-WAN Optimization Rules UI crashes after adding or modifying any of its rules name with double quotes. This is applicable for **Application Classifiers, Links, Service Classes, and Traffic Shaping Policies** rules.

SDWANHELP-1159: Citrix SD-WAN does not advertise the routes to the OSPF neighbor. This happens when the routes are changed at SD-WAN appliance or virtual paths flap happens which causes virtual WAN routes to be resynced across the sites. In this case, if the link to the OSPF peer is lossy, SD-WAN appliance might enter a state where it never advertises the SD-WAN routes to the OSPF neighbor.

SDWANHELP-1169: The SD-WAN service gets aborted when a packet is scheduled for transmission for a DVP that is pending removal. The software erroneously tries to remove it from an empty packet list.

SDWANHELP-1189: During the software appliance upgrade, the installation process can fail on the SD-WAN 210 Standard Edition (SE) appliances. To continue with the upgrade process, the appliance must be rebooted.

SDWANHELP-1222: In rare conditions, when connection tracking is enabled on an SD-WAN appliance, a specific combination of IP addresses, packet length, and IP protocol, might cause an error in checksum validation. Hence, the UDP or TCP packets inappropriately get dropped.

SDWANHELP-1241: In few cases, appliance information is not shown on the SD-WAN Center **Inventory** and **Status** page due to the crash of SD-WAN Center service.

SDWANHELP-1248: In few cases, the SD-WAN service might be aborted while processing the Internet Group Management Protocol (IGMP) packets in multi routing domain configurations.

SDWANHELP-1253: The Citrix SD-WAN appliance might drop internet traffic in multi routing domain configurations.

SDWANHELP-1256: During a configuration update in an SD-WAN appliance, when a branch removes all but one Routing Domain, the Network Address Translation (NAT) might fail for Internet traffic.

SDWANHELP-1276: On cloning a site in the Citrix SD-WAN Center, the access interfaces don't get cloned properly. The IP addresses remain the same as the original site even if the modification was done during cloning.

SDWANHELP-1284: If Citrix SD-WAN had BGP enabled, it was not allowed to forward BGP packets originated from and destined for other peers to go over the virtual path to other sites.

SDWANHELP-1385: The SD-WAN device serial number information might be lost and reset to Default string due to an issue in BIOS firmware v1.0b on SD-WAN 210 platform.

NSSDW-21808: The provisioned appliance information on SD-WAN Center gets cleared before the actual de-provision operation gets completed on the appliance. If any error occurred during de-provisioning, then you cannot perform any Palo Alto specific operations on the appliance from SD-WAN Center.

NSSDW-25440: Significant packet loss or network delays might be observed in Azure on instances with network acceleration enabled.

NSSDW-27341: In Citrix SD-WAN Center, you cannot perform the configuration for the Notification Settings that are Email Alerts, SNMP Traps, Syslog, and HTTP.

NSSDW-27530: In Citrix SD-WAN, changing the access interface IP address for a WAN Link can bring down the paths that are associated with the WAN Link.

NSSDW-28146: If Citrix SD-WAN 11.2.0 release is upgraded from 10.2 release or downgraded to 10.2 release once and later it is upgraded to 11.0/11.1 releases, then again downgrading back to 10.2 release fails.

Similarly, after upgrading from Citrix SD-WAN Center from 10.2 release to 11.2.0 release, the downgrading of SD-WAN Center from 11.2.0 to 10.2 release was not supported.

NSSDW-28971: Once you log into the SD-WAN appliances and virtual machines, you might gain root shell access with the 11.x based image using a hardcoded password. The affected SD-WAN platforms are 110 and VPXs provisioned with 11.x images. This is a CLI related issue and not applicable for the GUI.

Known Issues

NSSDW-23558: Citrix SD-WAN Edge Security is not interoperable with the Cloud Direct and Cloud Security features.

NSSDW-25452: The Citrix SD-WAN Orchestrator UI and the Citrix SD-WAN configuration compiler do not catch out of the allowed range of DHCP lease interval, which causes the DHCP daemon to fail.

- **Workaround** - Specify the valid lease time for DHCP is 300–86400 sec.

NSSDW-27105: The Data Plane Development Kit (DPDK) crashed every time when one of the ports is brought down while traffic is going through. At that time DPDK crashes, SD-WAN service gets restarted and the virtual path is dead. After a few minutes the Virtual Path comes **UP** automatically.

NSSDW- 27139: Citrix SD-WAN Edge Security is not interoperable with the WANOP feature.

NSSDW-27587: A disk warning message occurs on the SD-WAN VPX appliance running as MCN with the default 40 GB disk space.

- **Workaround** –It is recommended to use 120/240 GB virtual disks for the SD-WAN MCN VPX with up to 128/256 virtual path support.

NSSDW-27719: Convertible management port cannot be used for VPX deployed on hypervisors using the IXGBEVF driver. This might result in critical software errors and the service being disabled.

NSSDW-27727: Networks with VPX and VPXL instance using the IXGBEVF driver, used for certain Intel 10 GB NICs when SR-IOV is enabled, must not be upgraded to 11.2.0. This might result in a loss of connectivity. This issue is known to impact AWS instances with SR-IOV enabled.

NSSDW-27817: The Web filtering functionality of Citrix SD-WAN Edge Security by default closes the TCP connection when the user tries to access blocked sites when using the HTTPS protocol, instead of redirecting the user to an informative webpage with details about the request being blocked.

NSSDW-27847: Overlapping IP addresses across different Routing Domains are not supported by Citrix SD-WAN Edge Security. The session log messages also do not contain the routing Domain information.

NSSDW-27850: Citrix SD-WAN Anti Malware engine redirects the user to a non-routable IP address when it detects a virus in an HTTP webpage. In a result, the end-user browser becomes unresponsive while trying to retrieve it until it times out.

NSSDW-27928: You cannot enable or disable the modem if no configuration is done on the LTE modem.

- **Workaround**: Perform a configuration change, for example - update Access Point Name (APN).

NSSDW-27934: If Two-Box Solution is enabled, you cannot upgrade from the 11.2.0 release to any upper releases without disabling Two-Box Solution and re-enabling it after the upgrade is complete.

- **Workaround**: It is recommended that customers using Two-Box Solution must upgrade to 11.2.1 (Future release) instead of 11.2.0 release.

NSSDW-27935: HTTP server alerts will not be sent from Citrix SD-WAN appliances.

- **Workaround**: Use Citrix SD-WAN Center to send HTTP server alerts.

NSSDW-27938: STS bundle that is created via the CLI is not downloadable through SD-WAN GUI.

- **Workaround**: Use Citrix SD-WAN GUI to create the STS bundle.

SDWANHELP-1547: After a configuration update, WAN links might not be available for Internet or Intranet traffic.

- **Workaround**: Restart the gateway device, reset the SD-WAN port, or restart the SD-WAN service.

Troubleshooting Citrix SD-WAN 110 SE network issue

June 25, 2021

This section describes the network connectivity issues of the Citrix SD-WAN 110 SE appliance along with troubleshooting instructions.

Symptom

The Citrix SD-WAN 110 SE appliance fails to establish network connectivity under the following conditions.

- Appliance is managed by SD-WAN Orchestrator and/or brought up by zero touch deployment (ZTD).
- Appliance is in factory state and ZTD/SD-WAN Orchestrator agents are not installed.
- Appliance time (CMOS or hardware) is ahead of the actual time.
- Appliance time is set backwards by the NTP daemon before download/installation of the ZTD/SD-WAN Orchestrator agents.

Workaround

After initial installation (or after resetting the unit to its original factory configuration), the end-user installing SD-WAN 110 must verify that the appliance is successfully connected to the organizational network. The end-user must be provided with organization-specific instructions along with the appliance (for example, dial tone on the VoIP phone) to verify network connectivity. If the appliance does not connect to the network, the end-user can follow the instructions provided below:

1. Leave the appliance powered on and wait for 30 minutes or longer.
2. Briefly but firmly press the Power button (1–2 seconds) to shut it down.
3. After the lights on the appliance go dark, press the Power button again to turn the appliance back on. The SD-WAN 110 appliance now restarts and connects to the network.

Release Notes

March 12, 2021

This release note describes What's new, fixed issues, and known issues applicable to Citrix SD-WAN software release 11.2 version 1 for the SD-WAN Standard Edition, WANOP, Premium Edition appliances, and SD-WAN Center.

For information about the previous release versions, see the Citrix SD-WAN documentation.

What's New

New User Interface Enhancements -
The new user interface support is now extended to SD-WAN 210 appliances. All local users with Ad-

min role and remote users have access to the new user interface. Local users can change their account password. Remote user accounts are authenticated through RADIUS or TACACS+ authentication servers. You can configure either the RADIUS or TACACS+ authentication server. Ability to perform SIM PIN operations and manage the LTE firmware are also introduced.

Gateway Service Optimization -
You can now enable the first packet detection, classification, and selective routing (direct internet breakout or over the virtual path) of the traffic destined for Citrix Cloud and Citrix Gateway Service (control and data). This feature is only available via Orchestrator starting from SD-WAN version 11.2.1.

Citrix SD-WAN 6100 Premium Edition Appliance -
The Citrix SD-WAN 6100 PE appliance is a 2U appliance. It has two 14-core processors for a total of 28 physical cores (with hyper-threading enabled), and 256 GB of memory. The Citrix SD-WAN 6100 PE appliance is shipped with the Citrix SD-WAN 10.2.7 image, upgrade the software to Citrix SD-WAN 11.2.1 and above to enable PE functionality.

Advanced Edge Security support for Citrix SD-WAN 210 SE appliances (Tech Preview) -
Citrix SD-WAN 210 SE and 210 SE LTE appliances now support Advanced Edge Security capabilities with Advanced Security add-on licenses. To enable advanced security capabilities on a Citrix SD-WAN 210 appliance, reimage the appliance software to Citrix SD-WAN 10.2.7.17 and install the Advanced Security add-on license. For more details, see USB reimage Utility.

> **Note**
>
> Activating the advanced security add-on license on the Citrix SD-WAN 210 appliance, for the first time, might take up to 20 minutes approximately.

LAG support for Citrix SD-WAN 2100 SE -
Citrix SD-WAN 2100 SE appliance supports simple LAG (ACTIVE-BACKUP). The 802.3ad LACP protocol based negotiations are not supported in the current release. At any time only one port is active and the other ports are in backup mode.

Real-time Reports -
Citrix SD-WAN Orchestrator allows you to view the real-time reports for the following security features:

- **Web Filtering**: Provides the real-time report of the last 1000 web (HTTP, HTTPS) events from the total number of web requests.
- **Anti-Malware**: Provides the real-time report of the last 1000 Anti-Malware events from the total number of the files scanned.
- **Intrusion Prevention**: Provides the real-time report of the last 1000 logged and blocked intrusion prevention system events from the total number of intrusion events.

You can also click the individual slices of the pie chart or the legends beside the pie chart to view the top-10 event details of the Web Filtering, Anti-Malware, and Intrusion Prevention security features.

On-prem Orchestrator -
From Citrix SD-WAN 11.2.1 release onwards, secure appliance connectivity is implemented on the On-prem SD-WAN Orchestrator along with the SD-WAN Appliance and On-prem SD-WAN Orchestrator Certificates, Domain, Authentication Type, and Advanced Configuration options. You can either use the On-prem SD-WAN Orchestrator IP address or Domain or both (IP address and domain) for enabling the On-prem SD-WAN Orchestrator connectivity.

RADIUS and TACACS+ Server - The timeout value for the RADIUS and TACACS+ server is increased from 10 seconds to 60 seconds.

Fixed Issues

SDWANHELP-1193: For an MCN in factory default state, the LCM package downloaded immediately after clicking staging but before activating the staged software, does not contain the necessary content.

SDWANHELP-1210: When both VRRP and HA are configured, the GUI access is interrupted, loss of connectivity and ping failure are observed. Do not initiate the VRRP instance on the HA standby appliance.

SDWANHELP-1299: A branch with dynamic virtual path established with another branch and WAN-to-WAN forwarding enabled, forwards the routes received over the dynamic virtual path to other sites. When the dynamic virtual path goes down, the learned routes are not removed from the other sites.

SDWANHELP-1326: After upgrading SD-WAN to 11.1.0/11.1.1, PPPoE links fail to get connected on the following platforms:

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

SDWANHELP-1330: SD-WAN Center did not deliver email notifications as email settings was set to null in the SD-WAN Center database.

SDWANHELP-1332: If a single data flow is sent on more than three different WAN links, the SD-WAN service might crash during NetFlow statistics collection.

SDWANHELP-1337: For AWS's Elastic Compute Cloud (EC2), the SD-WAN instance having more than 32 GB memory, the virtual instance falls back to the default value of 16 static Virtual Paths. It leads to undefined behavior and possible crash scenarios when more than 16 static Virtual Paths are configured.

SDWANHELP-1365: In a High Availability GEO MCN setup with WAN-to-WAN forwarding enabled, an internet service down event can trigger an erroneous scenario wherein routes learned from the Secondary GEO MCN take higher precedence than the Primary GEO MCN.

SDWANHELP-1370: SNMP service enabled after provisioning the SD-WAN Center with the default community string as public causes a vulnerability issue. SD-WAN Center does not support SNMP service. So, the SNMP service is permanently disabled to resolve the vulnerability issue.

SDWANHELP-1384: Inter-routing domain service routes when created using network objects do not get added. The export route option for all inter-routing domain service routes to export the route to other connected sites does not work.

SDWANHELP-1385: The SD-WAN device serial number information might be lost and reset to Default string due to an issue in BIOS firmware v1.0b on the SD-WAN 210 platform.

SDWANHELP-1386: The user is unable to schedule path bandwidth testing on the SD-WAN appliance.

SDWANHELP-1432: Trace files are not parsed properly when the file name contains a **+** symbol.

SDWANHELP-1464: The SD-WAN service gets aborted while processing packets received over the intranet service configured over the Private MPLS link that has MPLS queues.

NSSDW-27587: A disk warning message occurs on the SD-WAN VPX appliance running as MCN with the default 40 GB disk space.

NSSDW-27727: Networks with VPX and VPXL instance using the IXGBEVF driver, used for certain Intel 10 GB NICs when SR-IOV is enabled, must not be upgraded to 11.0.1. It might result in a loss of connectivity. The issue is known to impact AWS instances with SR-IOV enabled.

NSSDW-27753: If SD-WAN was not registered with MAS before upgrading to SD-WAN 11.2.0 release, then it fails to register with MAS after upgrading to SD-WAN 11.2.0 release.

NSSDW-27928: You cannot enable or disable the modem if no configuration is done on the LTE modem.

NSSDW-27934: If Two-Box mode is enabled, you cannot upgrade from 11.2.0 release to any upper releases without disabling Two-Box mode and re-enabling it after the upgrade is complete.

NSSDW-27935: HTTP server alerts are not sent from Citrix SD-WAN appliances.

NSSDW-27938: STS bundle that is created using the CLI is not downloadable through the SD-WAN GUI.

NSSDW-28146: If Citrix SD-WAN 11.2.0 release is upgraded from 10.2 release or downgraded to 10.2 release once and later it is upgraded to 11.0/11.1 releases, then again downgrading back to 10.2 release fails. Similarly, after upgrading from Citrix SD-WAN Center from 10.2 release to 11.2.0 release, the downgrading of SD-WAN Center from 11.2.0 to 10.2 release was not supported.

NSSDW-28799: Creating a Custom dashboard provides you an option to set it as a primary dashboard. If you check and save the dashboard, you land on that saved dashboard by default with every login or when you navigate to the dashboard page.

NSSDW-29581: Edge security bandwidth rate is not aligned with the Advanced Edition license loaded in the SD-WAN Orchestrator.

NSSDW-29699: When you provision an SD-WAN appliance with 11.2.0 version freshly, single sign-on to MCN from SD-WAN Center does not work as expected. Features like Cloud Direct, Change Management, automated Azure deployment, Azure virtual WAN, Zscaler do not work from SD-WAN Center.

The issue is fixed in SD-WAN 11.2.1 version. When you upgrade from a freshly provisioned 11.2.0 version to 11.2.1 version, regenerate the Appliance certificate.

Known Issues

SDWANHELP-1292: Timezone setting done using the SD-WAN Center is not applied on the SD-WAN appliances.

- **Workaround**: Set the timezone using the SD-WAN appliance GUI or Appliance REST APIs or Appliance CLI.

SDWANHELP-1323: MCN High Availability (HA) device shows not connected if the wire from the first HA interface is not plugged in (when multiple HA interfaces are defined).

- **Workaround**: Remove the HA interface from the configuration if it is not physically connected.

NSSDW-27615: When SD-WAN 210 Standard Edition (SE) is converted to Advanced Edition (AE), the memory parameters (Huge Pages, Max Connections, Flow Limit, and Number of packet buffers) get reduced. The memory parameters remain unchanged even if the SD-WAN 210 AE appliance is converted back to SE.

NSSDW-29146: Once the appliance role is switched from Client to MCN in the legacy UI, the new user interface if open in other browsers, does not get logged out automatically. Having the new UI session open does not affect the legacy UI. Optionally, you can choose to close the new UI session.
Once the appliance role is switched from MCN to Client in the legacy UI, you do not get redirected to the new UI automatically. You can continue to use the legacy UI. If you choose to use the new UI, browse `https://< management-ip>` in a new browser tab.

NSSDW-29513: VPX branch goes into single site mode, if the newly provisioned VM is first downgraded and then upgraded back to the version on which the VM was provisioned.

- **Workaround**: Perform Local Change Management on the affected branch.

NSSDW-29526: When the MCN with HA performs partial site upgrade on the Geo MCN, the Geo MCN becomes the primary MCN. After the partial upgrade, the exiting standby MCN cannot detect the new primary MCN.

NSSDW-29819: At times, the Edge Security subsystem in the Citrix SD-WAN 210 appliance might fail and the appliance might not recover automatically.

- **Workaround**: Reboot the Citrix SD-WAN 210 appliance.

NSSDW-29898: The security reports for the SD-WAN 210 AE appliance are not seen on the SD-WAN Orchestrator UI. The issue happens due to the first-boot timing issue, where the database user gets created but permissions are not granted.

NSSDW-29900: SD-WAN AE activation might fail consistently if the edge security component is stuck to an unresponsive state. Re-booting the failing appliance should resolve the issue and allow activation to proceed.

Release Notes

March 12, 2021

This release notes describes what's new, fixed issues, and known issues applicable to Citrix SD-WAN software release 11.2 version 2 for the SD-WAN Standard Edition, WANOP, Premium Edition appliances, and SD-WAN Center.

For information about the previous release versions, see the Citrix SD-WAN documentation.

What's New

External USB modem MBIM and NCM support -
External USB modems that use MBIM and NCM mode are supported on Citrix SD-WAN 110 and 210 appliances. You can also configure the **APN** settings and **Enable/Disable** modem through the new Citrix SD-WAN GUI and Citrix SD-WAN Center. Mobile broadband operations are not supported on CDC Ethernet USB modems.

Edge Security logs -
Citrix SD-WAN Edge Security logs now follow the CEF (Common Event Format). CEF is a standard that defines the syntax of log messages and therefore allows interoperability of multiple devices generating log messages in a solution.

Citrix SD-WAN Advanced Edition support -
The Citrix SD-WAN Advanced Edition (AE) is now supported on Citrix SD-WAN 210 SE and Citrix SD-WAN 210 SE LTE appliances.

Office 365 Optimization - Microsoft Office 365 Default category traffic is classified based on all the application endpoints marked as required in the Default category. For more information, refer to Office 365 URLs and IP address ranges.

Fixed Issues

SDWANHELP-1161: After upgrading to 10.2.5.6 build, the SD-WAN UI access became very slow.

SDWANHELP-1353: The SD-WAN service might get aborted when WAN links are added for internet load balancing as part of the configuration update.

SDWANHELP-1363: The SD-WAN service might get aborted when ARP entry is updated from host to persistent type.

SDWANHELP-1420: On SD-WAN Premier Edition (PE), the WANOP GUI pages are not accessible over the In-band management Virtual IP address.

SDWANHELP-1423: You must not start the site diagnostics test at the same time for a given site from the peer appliance.

SDWANHELP-1463: Some SD-WAN devices were entering the grace period for a few minutes because the license server was temporarily unreachable.

SDWANHELP-1484: An error in PCKS12 bundle processing prevents bundles where the key precedes the certificate from being processed.

SDWANHELP-1503: Modems can go to unresponsive over time, which leads to qmi-proxy failure in accepting new requests.

SDWANHELP-1504: The SD-WAN service might get aborted when the ARP entries are manually cleared from the GUI.

SDWANHELP-1535: When Geo MCN is used as a active MCN, the standby RCN shows as Not Connected state at the Geo MCN. This issue can occur if there was a switchover done from Active MCN to Geo MCN.

SDWANHELP-1538: The following rare issues are addressed:

- Data path goes to a state where configuration updates of learned source IP/Port, DHCP IP, and PPPoE IP are not applied/missed.
- A configuration update can take more than expected time and cause a data path crash.

SDWANHELP-1553: Back-end validation that the certificate matched the signing authority was broken.

SDWANHELP-1554: Back-end parsing of certificate information was broken.

SDWANHELP-1555: Underscores were not allowed when entering the common name field.

Known Issues

NSSDW-20500: On the Citrix SD-WAN 5100 PE appliance, when you initiate domain join operation, a warning message can display stating that WANOP is initializing.

- **Workaround**: Rejoin the domain after 2 minutes.

NSSDW-28788: The client subnets are not exported when the deployment is in **Bridge** mode.

NSSDW-30660: An error is thrown while trying to push the certificate to collectors, after entering the credentials of the collector from SD-WAN Center Headend during the initial discovery of the RCN based network from SD-WAN Center.

- **Workaround**: Add the NTP server and rediscover the network and enter the SD-WAN Center collector's IP and credentials to push the certificate.

NSSDW-30662: Discovery of RCN fails with Appliance Error when an appliance is in standby mode whose IP is listed in the SD-WAN Center.

- **Workaround**: Make the RCN appliance whose management IP is listed in the collector configuration table as active for discovery to proceed.

SDWANHELP-1400: For an internet service route in a non-default routing domain and a path eligibility configured when the path goes down and the remote site that does not have the given routing domain configured, the internet route is not marked unreachable.

Release Notes for Citrix SD-WAN 11.2.3b Release

July 19, 2021

This release note describes fixed issues and known issues applicable to Citrix SD-WAN software release 11.2 version 3 for the SD-WAN Standard Edition, WANOP, Premium Edition appliances, and SD-WAN Center.

For information about the previous release versions, see the Citrix SD-WAN documentation.

> **Note**
>
> Citrix SD-WAN 11.2.3b release addresses the security vulnerabilities described in https://support.citrix.com/article/CTX319135. It replaces releases 11.2.3 and 11.2.3a.

Fixed Issues

NSSDW-29862: Citrix SD-WAN Center virtual machine running on VMware ESXi hypervisor might hang while taking a snapshot.

NSSDW-31612: To make the Citrix SD-WAN Orchestrator on-premises manage SD-WAN appliances shipped with 11.2.1 or 11.2.2 software, you must upgrade the SD-WAN appliance software to the 11.3.0 version.

NSSDW-32629: Auto-generated summary routes created for the Regional Control Node (RCN) network is assigned a cost of 30,000 instead of 65534.

SDWANHELP-1314: Unable to configure Interface groups for Citrix SD-WAN 210 and 110 appliances using the REST API through the MCN. The fix provides the support to configure the interface groups for Citrix SD-WAN 210 or 110 site model and BASE submodels through REST APIs.

SDWANHELP-1323: MCN high availability device shows **not connected** if the wire from the first high availability interface is not plugged in (when multiple high availability interfaces are defined).

SDWANHELP-1368: SNMP Walk did not show the correct MAC address information for interfaces.

SDWANHELP-1400: For an internet service route in a non-default routing domain and a path eligibility configured, when the path goes down and the remote site that does not have the given routing domain configured, the internet route is not marked unreachable.

SDWANHELP-1437: Disabling the insecure TLS1.0 and TLS1.1 between Citrix SD-WAN and SD-WAN Center connectivity.

SDWANHELP-1485: Packets received on Internet/Intranet service might get associated with the wrong WAN link when multiple WAN link gateways are resolved to the same MAC address.

SDWANHELP-1507: An issue in the configuration module was causing the export route setting to be true while the WAN to WAN forwarding setting was disabled for the site. After the fix, the export route is correctly set to false if the WAN to WAN forwarding is disabled and when the user has not explicitly set the export route setting.

SDWANHELP-1509: Unable to change the default community string (public) for the SNMP trap message in Citrix SD-WAN.

SDWANHELP-1513: DNS settings were not getting updated using DHCP when the Management port is acting as a DHCP client.

SDWANHELP-1520: The issue is with the IP learning on the branch site, where the stale IP details are not cleared for the disconnected WAN link. These stale IP details cause a virtual path between a branch to another branch in a DEAD state. As part of the fix, clean up the old IP details on the branch appliance during the IP learning.

SDWANHELP-1531: In Citrix SD-WAN Center reporting page, the data in the **Top applications** report of a site was inconsistent with the data in the **Top sites** report. It happened due to an unwanted regex match of the site name.

SDWANHELP-1537: Citrix SD-WAN Center authentication for TACACS based users was failing for a few combinations of passwords having **$** and **#** characters in the password. This issue was present in the 11.2.0 release.

SDWANHELP-1547: After a configuration update, WAN links might not be available for Internet or Intranet traffic.

SDWANHELP-1558: Internet service does not use the backup links when the primary link goes down.

SDWANHELP-1580: While public IP address learning is enabled on a branch WAN link, the RCN might not learn the new public IP address and results in a dead path if:

- There is a configuration version mismatch between the branch and the RCN
- The public IP address of the branch WAN link has changed

SDWANHELP-1616: Office365 local internet breakout might not work when multiple routing domains are enabled on a site.

SDWANHELP-1617: When regional subnets are created, the summary routes are auto-created with 65534 costs. When this route is advertised to another site, the cost is rolled over and becomes a non-summary route with the lowest cost.

SDWANHELP-1627: Connections redirected through the hosted firewalls (Palo Alto) and routed over the Virtual Path service experience high latency issues.

SDWANHELP-1641: A crash in the configuration compiler occurs when the auto path group is not set in WAN Link usage for the Dynamic virtual path when it is configured on an LTE-E1 interface.

SDWANHELP-1646: The management port must not be added in the Link Aggregation Group (LAG), hence the management interface is not listed while forming the LAG.

SDWANHELP-1673: Citrix SD-WAN request to download PAC file from the server is being intercepted and served by SD-WAN itself when management IP matches local route.

SDWANHELP-1684: When **Certificate Revocation Lists** were enabled, there was an error causing repeated download attempts of the CRL.

SDWANHELP-1686: Use of the same high availability IPs at different sites was not allowed previously. The high availability IPs are now treated as private allowing them to be used at different sites.

SDWANHELP-1736: Citrix SD-WAN Center's email notification adds an extra < CR > character in the command which causes the SMTP session to terminate.

SDWANHELP-1783: During the dynamic virtual path creation, if the protocol message arrives with an unexpected IP type of service (TOS) value, it might result in core dump.

SDWANHELP-1787: **Import** and **Export** of large network configurations (when the configuration file size exceeded 16 MB) on Citrix SD-WAN Center were failing.

SDWANHELP-1804: After upgrading Citrix SD-WAN device to the 11.2.2 version, more than one VRRP device acts as **Master** because of the wrong VRRP advertisement packet size sent by SD-WAN device.

SDWANHELP-1866: On Citrix SD-WAN 110 and 210 platforms, if the management port is configured as a data port, the **Host ID** might change after upgrading to a newer version. The SD-WAN appliances will use the grace license if this issue occurs.

Known Issues

NSSDW-25387: If local change management is applied on an SD-WAN appliance with no difference in the PPPoE configuration, the existing PPPoE sessions might not be restarted.

- **Workaround**: Re-establish the PPPoE connections (under **Monitoring > PPPoE**).

NSSDW-25452: Citrix SD-WAN Orchestrator UI and Citrix SD-WAN configuration compiler do not catch out of the allowed range of DHCP lease interval, which causes the DHCP daemon to fail.

- **Workaround**: Specify the valid lease time for DHCP is 300–86400.

NSSDW-28788: The client subnets are not exported when the deployment is in Bridge mode.

NSSDW-29146: Once the appliance role is switched from Client to MCN in the legacy UI, the new user interface if open in other browsers, does not get logged out automatically. Having the new UI session open does not affect the legacy UI. Optionally, you can choose to close the new UI session. Once the appliance role is switched from MCN to Client in the legacy UI, you do not get redirected to the new UI automatically. You can continue to use the legacy UI. If you choose to use the new UI, browse **https://< management-ip>** in a new browser tab.

NSSDW-29513: VPX branch goes into single site mode, if the newly provisioned virtual machine is first downgraded and then upgraded back to the version on which the virtual machine was provisioned.

- **Workaround**: Perform Local Change Management (LCM) on the affected branch.

NSSDW-29526: When the MCN with high availability performs partial site upgrade on the Geo MCN, the Geo MCN becomes the primary MCN. After the partial upgrade, the exiting standby MCN cannot detect the new primary MCN.

NSSDW-32879: During staging, the **Change Management** page might occasionally freeze on the preparing packages step.

- **Workaround**: Reattempt staging by clicking the change preparation tab.

SDWANHELP-1292: **Timezone Settings** change on Citrix SD-WAN Center does not take effect on some pages. Time is still shown in UTC.

SDWANHELP-1491: ICMP connections getting WAN to WAN forwarded between Virtual Path and Intranet service over IPsec tunnel experience packet loss.

SDWANHELP-1454: An incorrect WAN Link use setting of Auto was allowed for Internet service which caused a crash. The configuration code has been corrected to block users from selecting the Auto option for WAN Link use for Internet service. An audit has also been added to catch this misconfiguration.

SDWANHELP-1549: **Ignore WAN link status** behavior is restored to SD-WAN 10.2 release behavior. For Internet/Intranet traffic, only the link that has paths in UP state is used. If all paths on the links that are configured to be used for Internet/Intranet service are dead and the **Ignore WAN link** status option is enabled, then the highest bandwidth link is used for Internet/Intranet traffic.

SDWANHELP-1737: When you add a new local user in Citrix SD-WAN Center, a yellow banner appears with a message that the firewall access is changed from **Enabled** to **Disabled**.

SDWANHELP-1739: When two virtual IP addresses (one private and another one non-private) are created in the same subnet, an issue occurs that two routes are created for the same subnet and the subnet is not advertised to a remote site.

SDWANHELP-1755: Snapshot extensions of Azure are not working in the build root environment.

SDWANHELP-1764: You cannot **Stage** and **Activate** a new configuration change. The memory and CPU fields are assigned some default values and that cannot be changed as there is no option available in the SD-WAN Orchestrator UI currently. This issue occurs as the default values vary from customer to customer.

SDWANHELP-1780: The **Public IPv4 Address** field was grayed out under the **Basic** section of the configuration editor.

SDWANHELP-1799: In the case of DHCP server configuration when service restart or upgrade, there is a timing condition due to which one or more interfaces are not able to respond to DHCP client requests.

- **Workaround**: Restart the DHCP server from Citrix SD-WAN UI.

SDWANHELP-1806: An SHA-256 checksum error occurs during downloading when a customer staging an appliance with a new configuration.

SDWANHELP-1808: Incoming VOIP call over T-Mobile Germany carrier fails with Citrix SD-WAN 210 appliance.

SDWANHELP-1835: In rare conditions, Citrix SD-WAN service might crash while processing the packets received over the dynamic virtual path at the time of dynamic virtual path removal.

New user interface for SD-WAN appliances

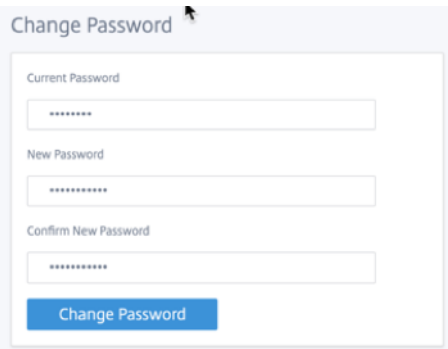
July 16, 2021

A new User Interface (UI) is introduced for SD-WAN appliances. The new UI is built using the latest UI technologies. The new UI design improves the security, has an improved look and feel, it is more performant, secure, and responsive. But the new UI has retained the flow and page layout of each feature from the legacy UI.

The new UI is applicable only for the customers using the following appliances:

Appliance	Release
Citrix SD-WAN 110 SE	11.1.1 onwards
Citrix SD-WAN 210 SE	11.2.1 onwards

> **Note**
>
> - Provisioning the Citrix SD-WAN 210-SE as an MCN redirects you to the legacy UI.
> - All local users with an Admin role and remote admin users can access the new user interface. Remote user accounts are authenticated through RADIUS or TACACS+ authentication servers. It is mandatory to change the default admin user account password while provisioning the SD-WAN appliance. The default password is the serial number of the SD-WAN appliance and is mandated to change on first time after logon to the device.



The legacy UI is maintained for backward compatibility and is deprecated. The legacy UI can be accessed using the URL **https: // < ip-address >/cgi-bin/login.cgi**. The user name and password for the user **admin** remains the same across both (new/legacy) user interfaces, and first time login procedures can be done using either interface. Additional users will be supported in future versions of the new UI.

Citrix SD-WAN new user interface

The new UI can be accessed using Google Chrome (version 81), Mozilla Firefox, Microsoft Edge (version 81+), and Legacy Microsoft Edge (version 44+) browsers.

> **NOTE**
>
> Microsoft Internet Explorer, Apple Safari, and other browsers are not supported.

To access the new UI page, perform the following:

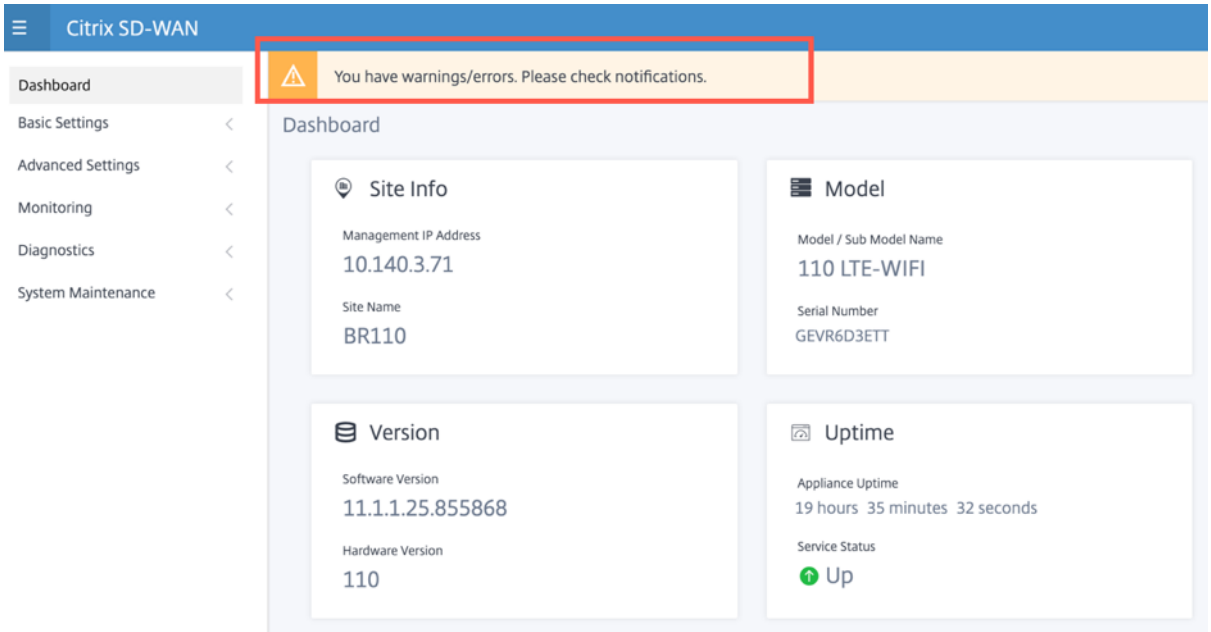
1. Open a new browser tab and navigate to **https: // < management-ip >** to access the new UI on the SD-WAN appliance.

> **Note**
>
> In the scenario where the In-band management is enabled, the interface IP address can be provided in **< management-ip >** to access the new UI. The In-band management can be enabled on multiple trusted interfaces that are enabled to be used for IP services. You can access the UI using the management IP and in-band virtual IPs.

1. Provide the user name and password. Click **Sign In**.

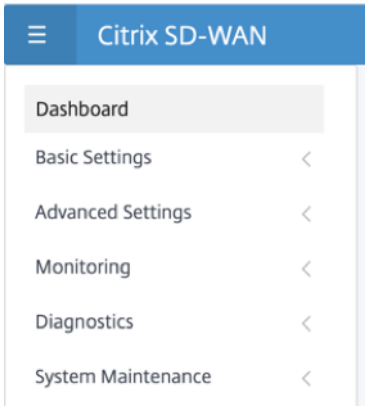
The Citrix SD-WAN user interface page appears.

Once you have successfully logged in, you can see the navigation panel is on the left side. Also, you can see a notifications banner on the dashboard if there are any warnings or errors.



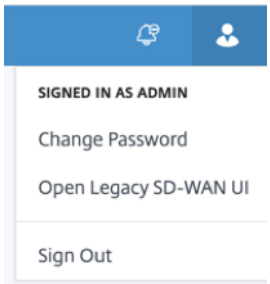
Navigation

The left navigation sidebar can be hidden or made visible on click of the hamburger icon. The hamburger icon on the top left corner provides links to the dashboard, **basic/advanced** settings, monitoring, and management related options.



Menu bar

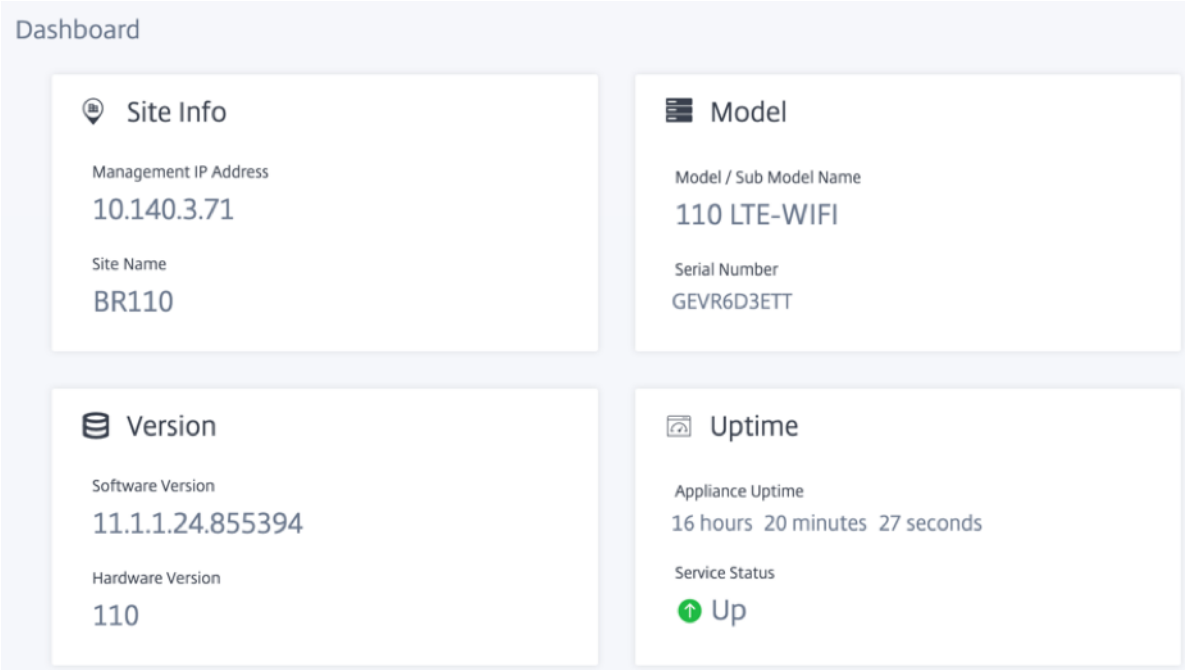
The user menu on the top right corner displays the logged-on user details. You can open the legacy user interface in a new browser tab by clicking the **Open Legacy SD-WAN UI** option. Click the bell icon for any notifications.



Dashboard

The **Dashboard** page displays the following basic information of the SD-WAN appliance as a tile view:

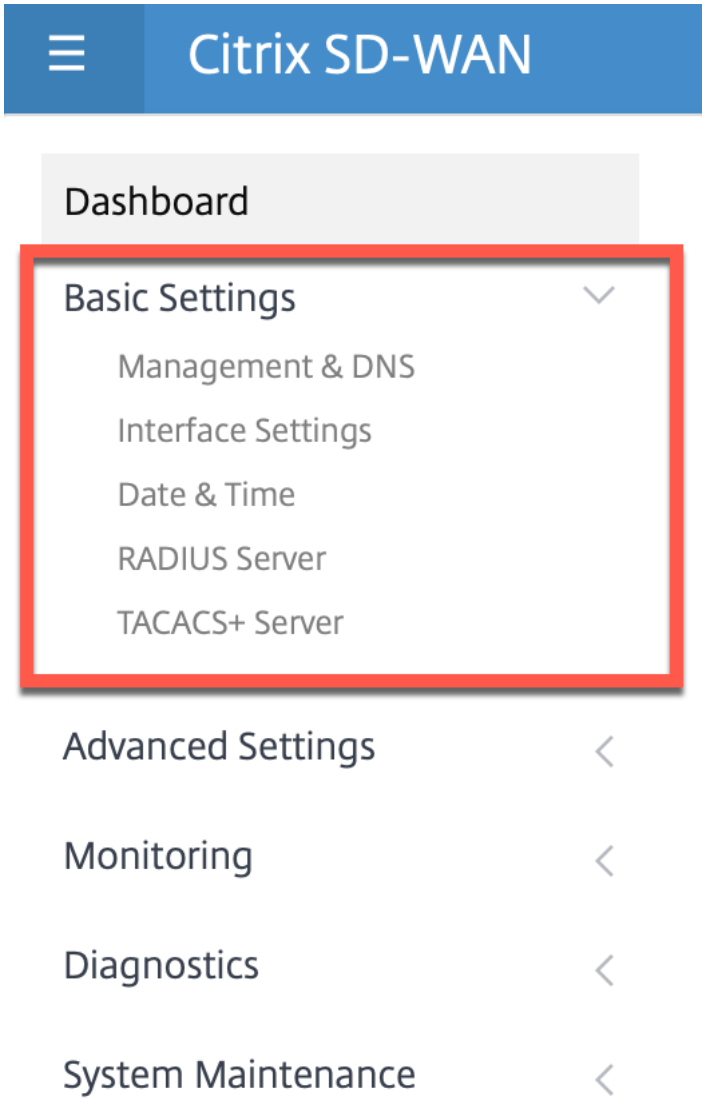
- **Site** –Displays the site information with **Management IP Address** and **Site Name**
- **Model** –Displays the **Model/Sub Model Name** and **Serial Number**
- **Version** –Displays **Software** and **Hardware** version
- **Uptime** - Displays **Appliance Uptime** and **Citrix Virtual WAN Service Status**



Basic settings

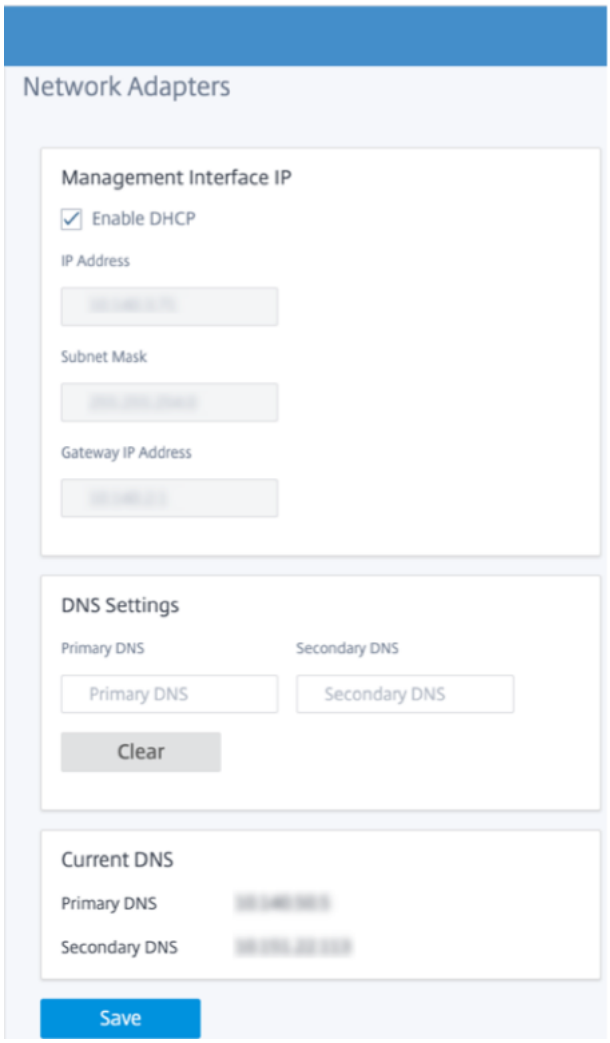
The SD-WAN appliance **Basic Settings** include the following entities configuration. The new UI provides a separate page for configuring each entity individually.

- Management and DNS
- Interface Settings
- Date and Time
- RADIUS Server
- TACACS+ Server



Management and DNS

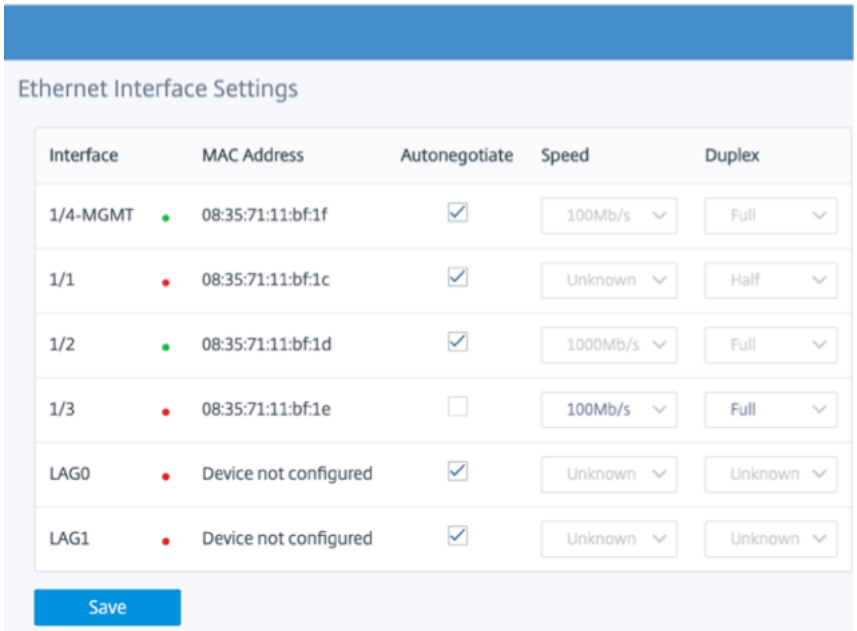
From the **Management and DNS** page, you can configure the management interface IP address and DNS settings. For more information, see Configure Management IP Address.



Enter the **IP address, Subnet mask,** and **Gateway IP address** for the appliance that you want to configure. Under the **DNS Settings** section, provide the primary and secondary DNS server detail and click **Save**.

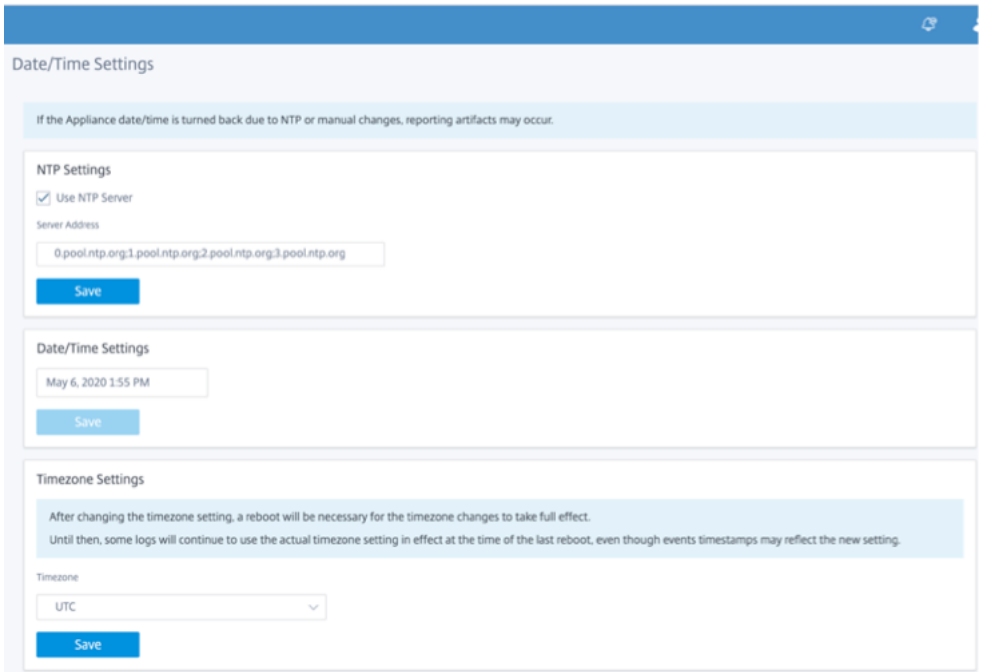
Interface settings

The **Interface Settings** page displays the Ethernet port configuration data. The ports that are down are indicated as a red dot against the MAC address.



Date and Time

From the **Date and Time** settings page, you must set the date and time on the appliance. For more information, see Set date and time.



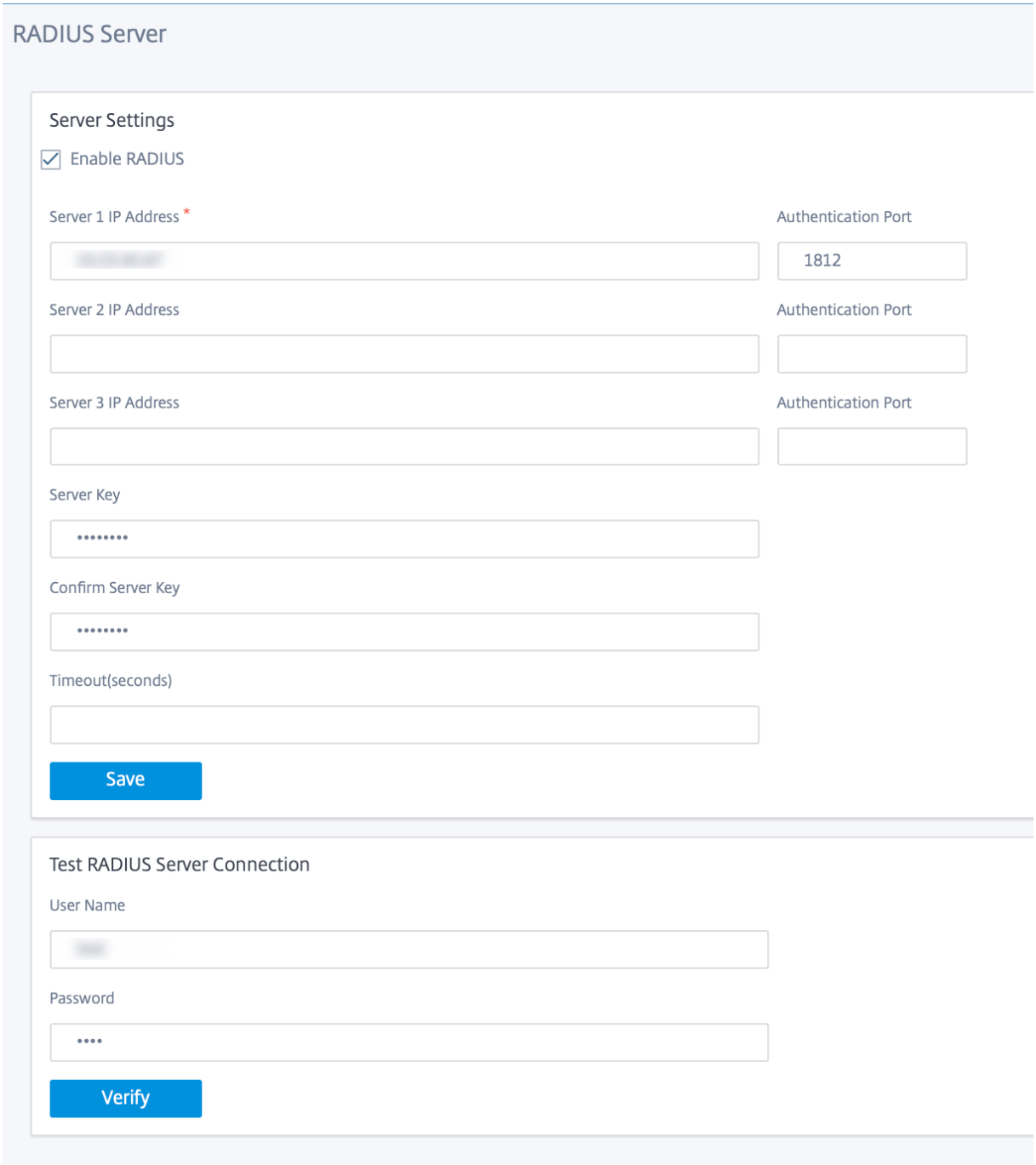
RADIUS Server

You can configure an SD-WAN appliance to authenticate user access with one or more RADIUS servers.

To configure the RADIUS server:

1. Select the **Enable RADIUS** check box.
2. Enter the **Server IP Address** and **Authentication Port**. A maximum of three server IP addresses can be configured.
3. Enter the **Server Key** and confirm.
4. Enter the **Timeout** value in seconds.
5. Click **Save**.

You can also test the RADIUS server connection. Enter the **User Name** and **Password**. Click **Verify**.



TACACS+ Server

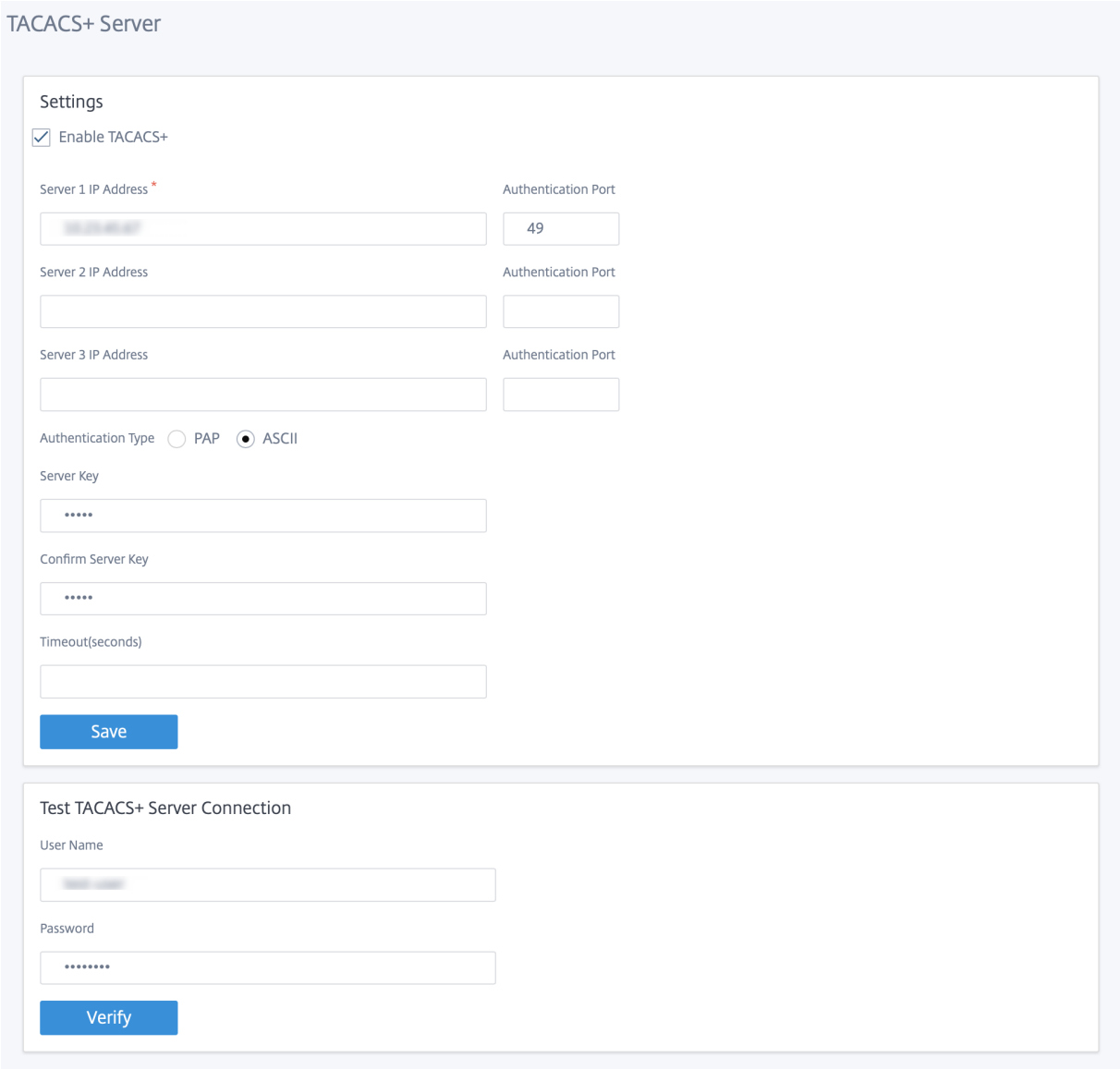
You can configure a TACACS+ server for authentication. Similar to RADIUS authentication, TACACS+ uses a secret key, an IP address, and the port number. The default port number is 49.

To configure the TACACS+ server:

1. Select the **Enable TACACS+** check box.

2. Enter the **Server IP Address** and **Authentication Port**. A maximum of three server IP addresses can be configured.
3. Select **PAP** or **ASCII** as the Authentication Type.
   - PAP: Uses Password Authentication Protocol (PAP) to strengthen user authentication by assigning a strong shared secret to the TACACS+ server.
   - ASCII: Uses ASCII character set to strengthen user authentication by assigning a strong shared secret to the TACACS+ server.
4. Enter the **Server Key** and confirm.
5. Enter the **Timeout** value in seconds.
6. Click **Save**.

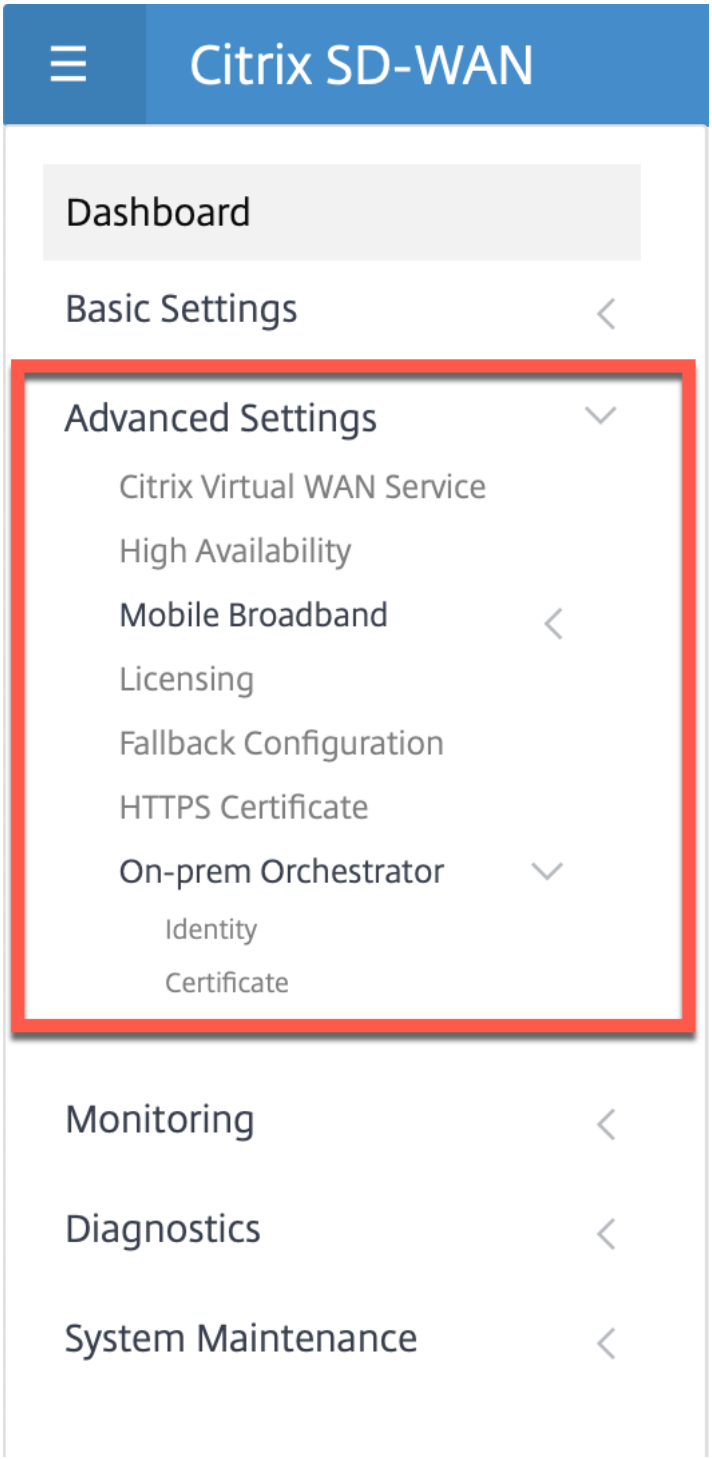
You can also test the TACACS+ server connection. Enter the **User Name** and **Password**. Click **Verify**.



Advanced settings

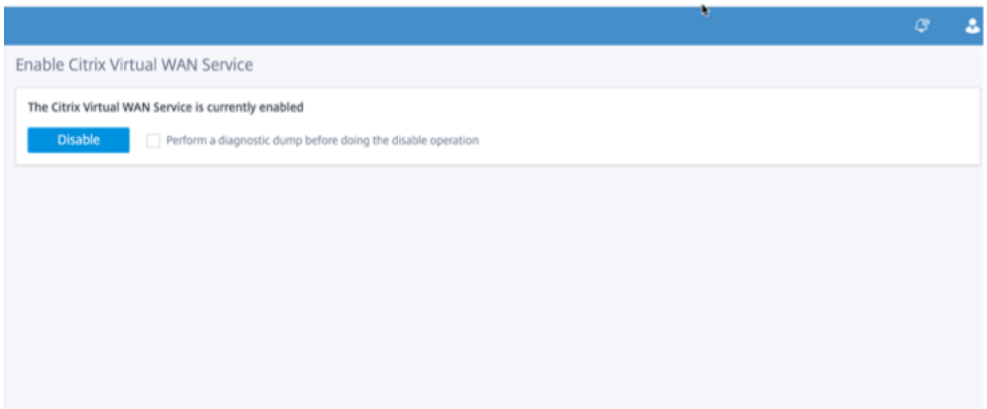
The SD-WAN appliance **Advanced Settings** include the following entities configuration.

- Citrix Virtual WAN Service
- High Availability
- Mobile Broadband
- Licensing
- Fallback Configuration
- HTTPS Certificate
- On-prem Orchestrator



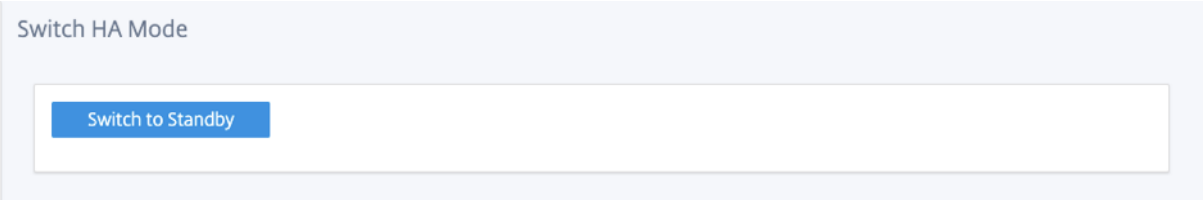
Citrix Virtual WAN service

The **CItrix Virtual WAN Service** page allows you to enable/disable the Citrix Virtual WAN Service. For more information, see Configure Virtual WAN Service.



High Availability

From the **High Availability** page, you can toggle between active and standby state for an SD-WAN high availability (HA) setup. The high availability status is available in the dashboard (if high availability is configured). For more information, see High Availability Mode.



Mobile broadband

The Citrix SD-WAN appliances such as the Citrix SD-WAN 210 SE LTE and 110 LTE Wi-Fi appliances have a built-in internal LTE modem. You can also connect an external 3G/4G USB modem on the following Citrix SD-WAN appliances.

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

CDC Ethernet, MBIM, and NCM are the three types of external USB modems supported.

For more information on configuring LTE using the legacy GUI, see the following topic:

- Configure LTE functionality on 210 SE LTE appliance
- Configure LTE functionality on 110-LTE-WiFi appliance
- Configure external USB LTE modem

For an internal LTE modem, insert the SIM card into the SIM card slot of the Citrix SD-WAN appliance. Fix the antennas to the Citrix SD-WAN appliance. For more information, see Installing the LTE antennas and power on the appliance.

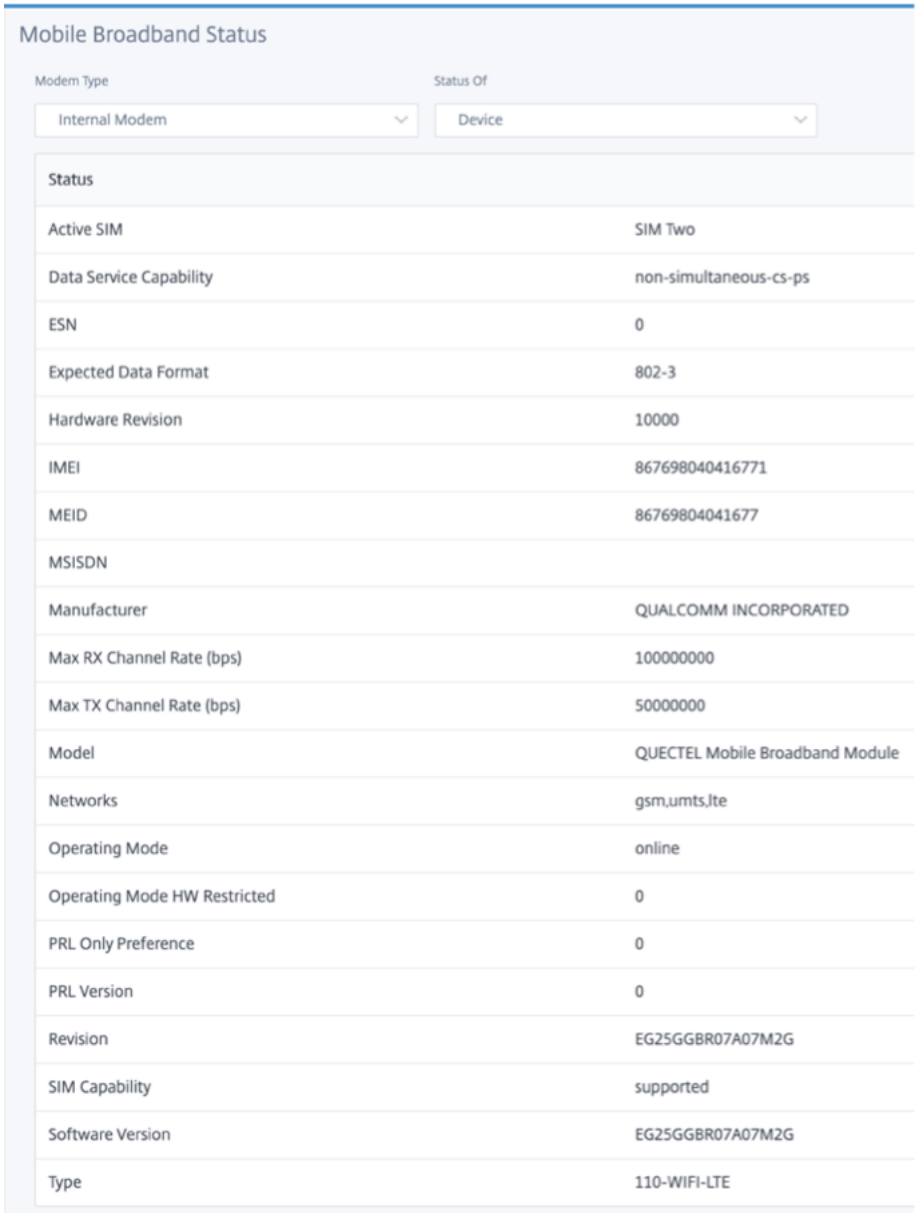
> **Note**
>
> Citrix SD-WAN 110-LTE-WiFi appliance has two standard (2FF) SIM slots. To use Micro (3FF) and Nano (4FF) size SIMs, use a SIM adapter. Snap the smaller SIM into the adapter. You can obtain the adapter from Citrix as a Field Replaceable Unit (FRU) or from the SIM provider. Hot-swapping of SIM for the internal LTE modem is supported only on the Citrix SD-WAN 110-LTE-WiFi appliance.

Perquisites for external LTE modem:

- Use the supported USB LTE dongles. The supported dongle hardware models are Verizon USB730L and AT&T USB800.
- Ensure that a SIM card is inserted into the USB LTE dongle. The CDC Ethernet LTE dongles are pre-configured with a static IP address, this interferes with the configuration and cause connection failure or intermittent connection, if the SIM card is not inserted.
- Before inserting a CDC Ethernet LTE dongle into the SD-WAN appliance, connect the external USB stick to a Windows/Linux machine and ensure that the internet is working properly with proper APN and Mobile Data Roaming configuration. Ensure that the **Connection mode** of the USB dongle is changed from the default value **Manual** to **Auto**.

> **Note**
>
> - The Citrix SD-WAN appliances support only one USB LTE dongle at a time. If more than one USB dongle is plugged in, unplug all the dongles and plug in only one dongle.
> - The Citrix SD-WAN appliances do not support user name and password for USB modems. Ensure that the user name and password feature are disabled on the modem during setup.
> - Unplugging or rebooting an external MBIM dongle impacts the internal LTE modem data session. This is an expected behavior.
> - When an external LTE modem is plugged-in, the SD-WAN appliance takes about 3 minutes to recognize it.

To view the mobile broadband status, select the modem type.

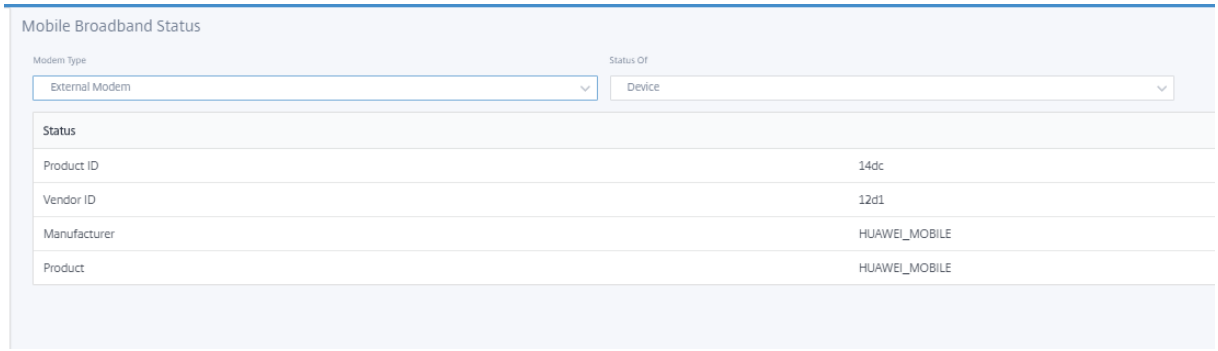


The following are some useful status information:

- **Modem Type**: Select the modem type as External or Internal. Internal modem shows the status under **Mobile Broadband > Status** page. All the other sections such as SIM preference, APN settings, Enable/Disable the modem, Reboot modem, and Refresh SIM are available under **Mobile Broadband > Operations** page.
- **Active SIM**: At any given time, only one SIM can be active. Displays the SIM that is currently active.
- **Operating Mode**: Displays the modem state.
- **SIM Capabilities**: Displays whether the SIM is supported or not.
- **Model**: Displays the mobile broadband module name.

If you select the **External** modem, it shows the status of the external modem. But if the external modem is not configured, it shows a warning message as **Selected Modem is not configured on this device**.

Device details for CDC Ethernet external modem.



Device details for MBIM and NCM external modems. The **Modem Mode** field displays the external dongle type.

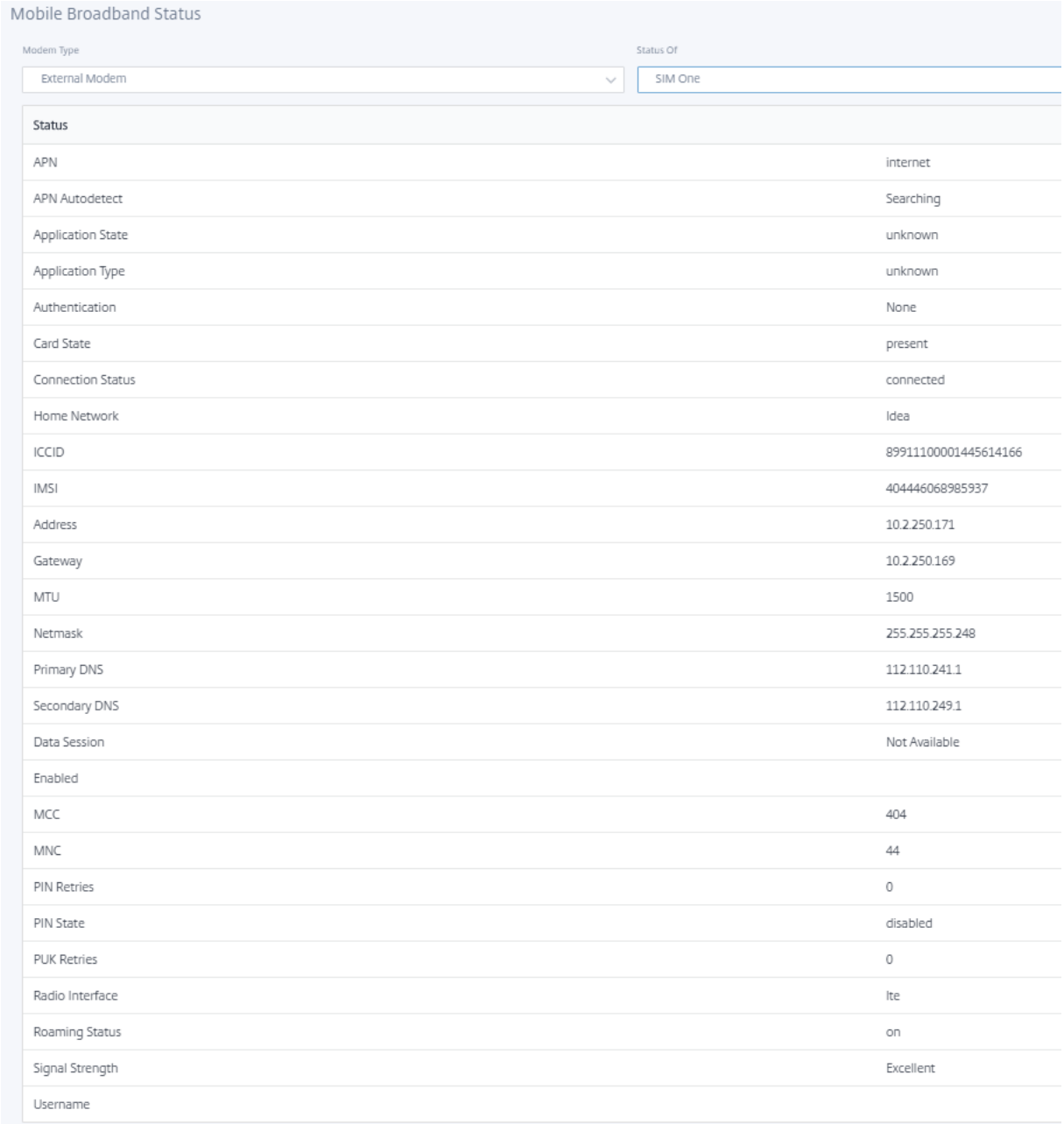
Mobile Broadband Status

Modem Type: External Modem

Status Of: Device

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

SIM details are displayed for MBIM and NCM external modems only.



Mobile broadband operations Operations that are supported on internal and external modems:

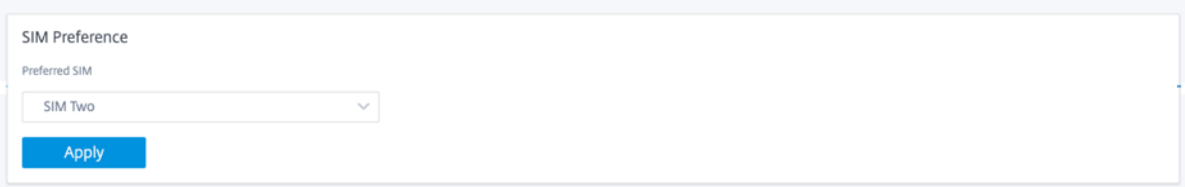
Operations	Internal modem	External modem - CDC Ethernet	External modem - MBIM and NCM
SIM preference	Yes - For appliances that support dual SIM	No	No
SIM PIN	Yes	No	No

Operations	Internal modem	External modem - CDC Ethernet	External modem - MBIM and NCM
APN settings	Yes	No	Yes
Network settings	Yes	No	No
Roaming	Yes	No	No
Manage firmware	Yes	No	No
Enable/Disable modem	Yes	No	Yes
Reboot modem	Yes	No	No
Refresh SIM	Yes	No	No

SIM preference You can insert dual SIMs on a Citrix SD-WAN 110-LTE-WiFi appliance. At any given time, only one SIM is active. Select the **SIM preference**:

- **SIM One preferred**: If two SIMs are inserted, on boot-up the LTE modem uses SIM One, if available. When the LTE modem is up and running it uses whichever SIM (SIM One or SIM Two) is useable at that moment and will continue to use it until the SIM is active.
- **SIM Two preferred**: If two SIMs are inserted, on boot-up the LTE modem uses SIM Two, if available. When the LTE modem is up and running it uses whichever SIM (SIM One or SIM Two) is useable at that moment and will continue to use it until the SIM is active.
- **SIM One**: Only SIM One is used, irrespective of the SIM state on both the SIM slots. SIM One is always active.
- **SIM Two**: Only SIM Two is used, irrespective of the SIM state on both the SIM slots. SIM Two is always active.

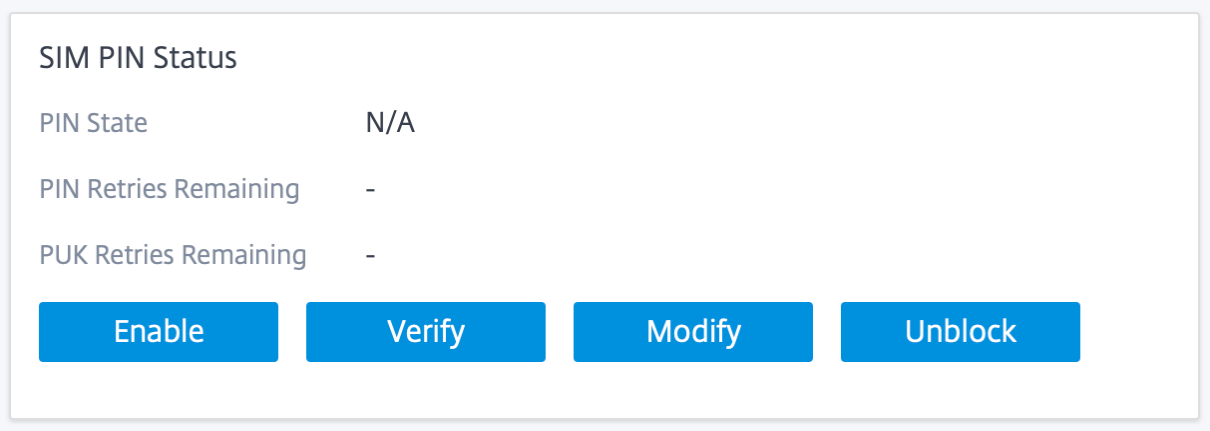
> **Note**
>
> The SIM Preference option is not available for the Citrix SD-WAN 210-SE LTE Wi-Fi appliance as it has only one SIM card slot.



SIM PIN

If you have inserted a SIM card that is locked with a PIN, the SIM status is in **Enabled and Not Verified** state. You cannot use the SIM card until it is verified using the SIM PIN. You can obtain the SIM PIN from the carrier.

To perform SIM PIN operations, navigate to **Advanced Settings > Mobile Broadband > Operations > SIM PIN status**.



You can perform the following operations:

- **Verify SIM PIN**: Click **Verify**. Enter the SIM PIN provided by the carrier and click **Verify**. The status changes to **Enabled and Verified**.
- **Enable SIM PIN**: You can enable SIM PIN for a SIM that has SIM PIN disabled. Click **Enable**. Enter the SIM PIN provided by the carrier and click **Enable**. If the SIM PIN state changes to **Enabled and Not Verified**, it means that the PIN is not verified and you cannot perform any LTE related operations until the PIN is verified. Click **Verify**. Enter the SIM PIN provided by the carrier and click **Verify**.
- **Disable SIM PIN**: You can choose to disable SIM PIN functionality for a SIM for which SIM PIN is enabled and verified. Click **Disable**. Enter the SIM PIN and click **Disable**.
- **Modify SIM PIN**: Once the PIN is in Enabled and Verified state you can choose to change the PIN. Click **Modify**. Enter the SIM PIN provided by the carrier. Enter the new SIM PIN and confirm it. Click **Modify**.
- **Unblock SIM** - If you forget the SIM PIN, you can reset the SIM PIN using the SIM PUK obtained from the carrier. To unblock a SIM, click **Unblock**. Enter the SIM PIN and SIM PUK obtained from the carrier and click **Unblock**.

  > **Note**

> The SIM card gets permanently blocked with 10 unsuccessful attempts of PUK, while unblocking the SIM. Contact the carrier service provider for a new SIM card.

APN settings

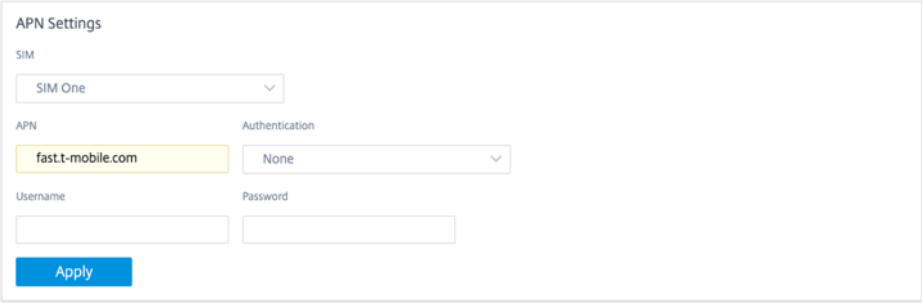
1. To configure the APN settings, navigate to **Advanced Settings > Mobile Broadband > Operations >** and go to the **APN settings** section.

   > **Note**
   >
   > Obtain the APN information from the carrier.

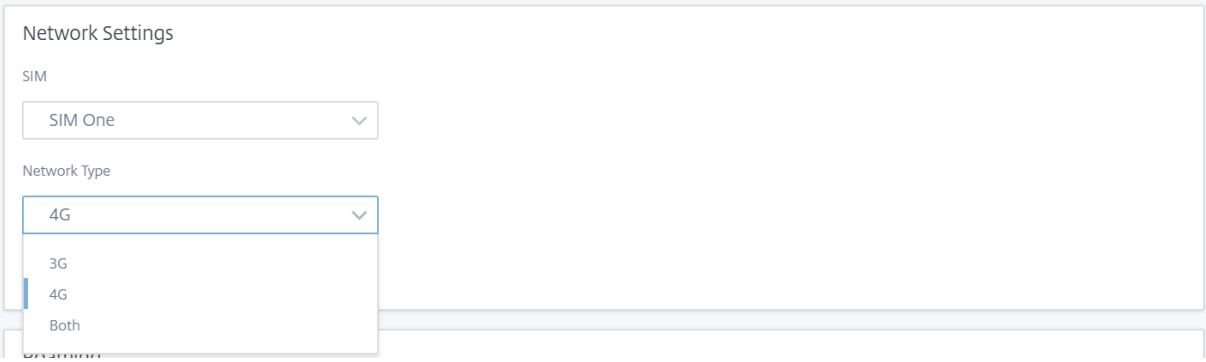
2. Select the SIM card, enter the **APN, Username, Password,** and **Authentication** provided by the carrier. You can choose from PAP, CHAP, PAPCHAP authentication protocols. If the carrier has not provided any authentication type, set it to **None**.

   > **Note**
   >
   > All these fields are optional.

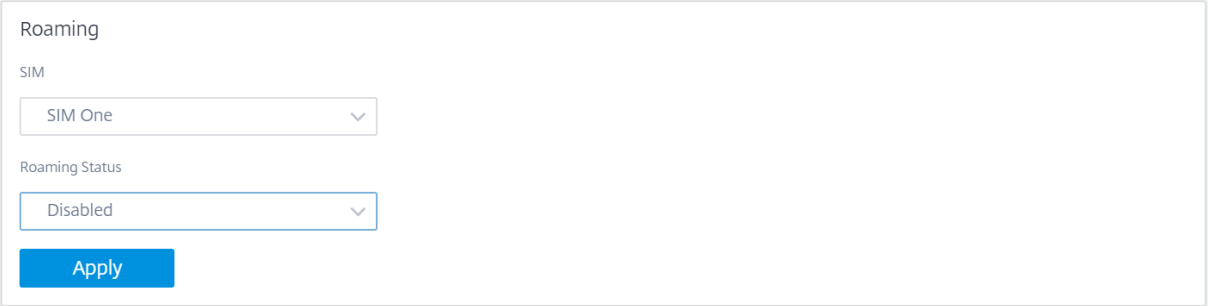
3. Click **Apply**.



Network settings You can select the mobile network on Citrix SD-WAN appliances that support the internal LTE modem. The supported networks are 3G, 4G, or both.

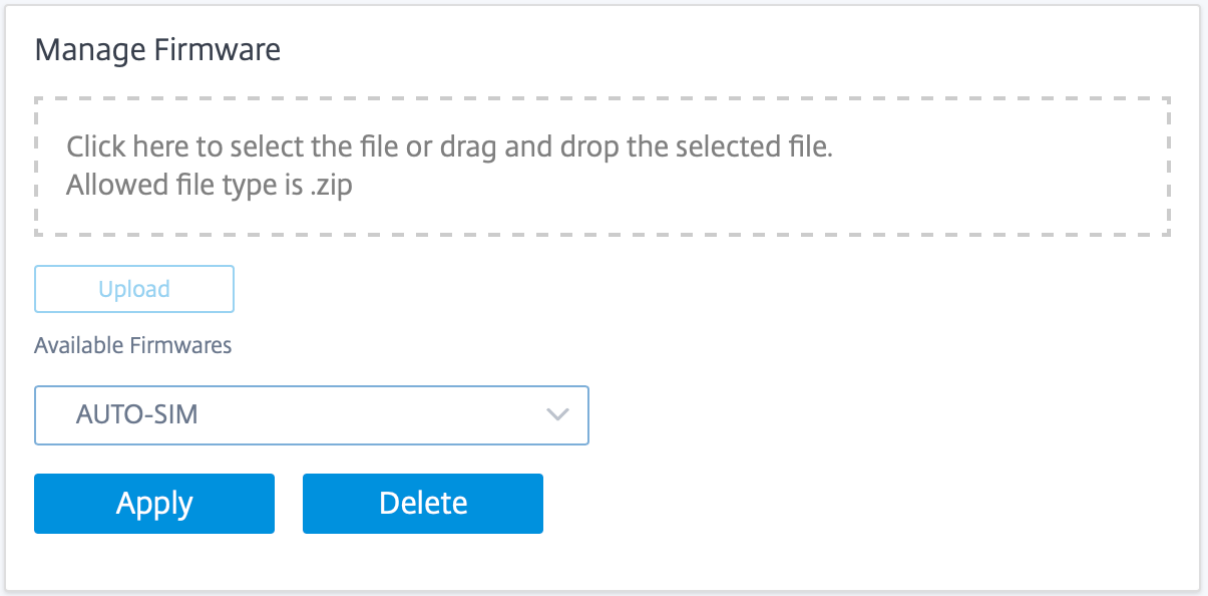


Roaming The roaming option is enabled by default on your LTE appliances, you can choose to disable it.

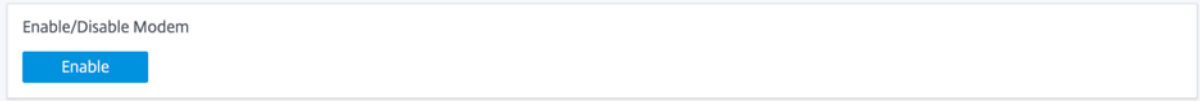


Manage Firmware

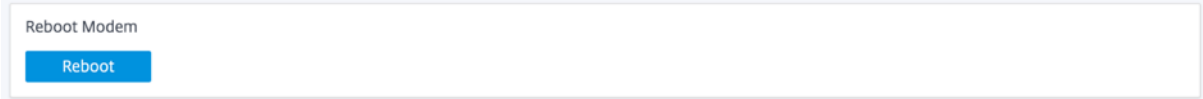
Every LTE enabled appliance has a set of firmware available. You can select from the existing list of firmware or upload a firmware and apply it. If you are unsure of which firmware to use, select the **AUTO-SIM** option. The AUTO-SIM option allows the LTE modem to choose the most matching firmware based on the inserted SIM card.



Enable/Disable modem Enable/disable modem depending on your intent to use the LTE functionality. By default, the LTE modem is enabled.

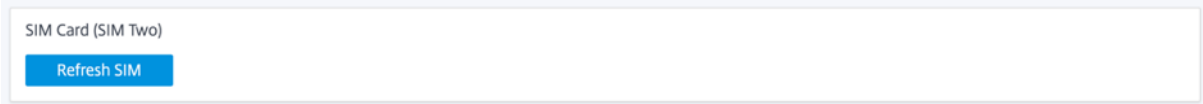


Reboot modem Reboots the modem. It can take up to 7 minutes for the reboot operation to complete.



Refresh SIM Use the **Refresh SIM** option when the SIM card is not detect properly by the LTE-WiFi modem.

> **Note**
>
> The Refresh SIM operation is applicable for the active SIM only.



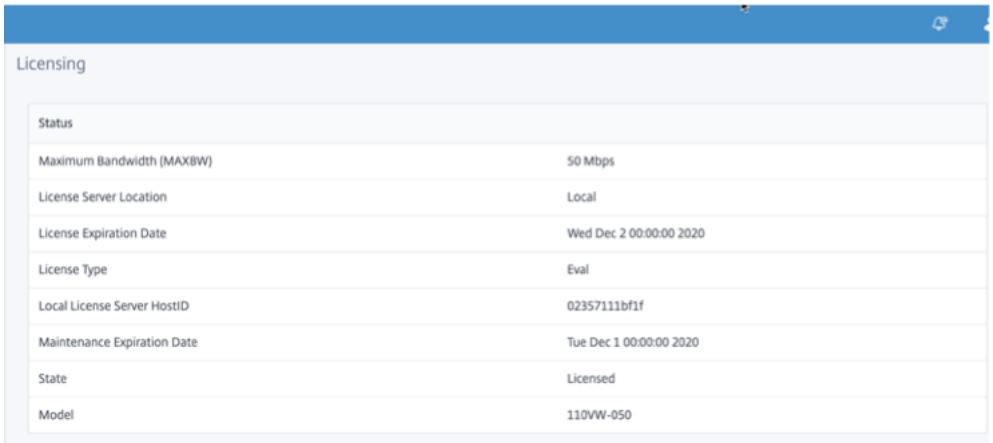
You can remotely view and manage all the LTE sites in your network using the Citrix SD-WAN Center. For more information see, Remote LTE site management.

For more information on LTE configuration, see Configure LTE functionality on 110-LTE-WiFi appliance and Configure LTE functionality on 210 SE LTE appliance.

For information on configuring external LTE modem, see Configure external USB LTE modem.

Licensing

The **Licensing** page displays the license details such as, server location, model, license type and so on.

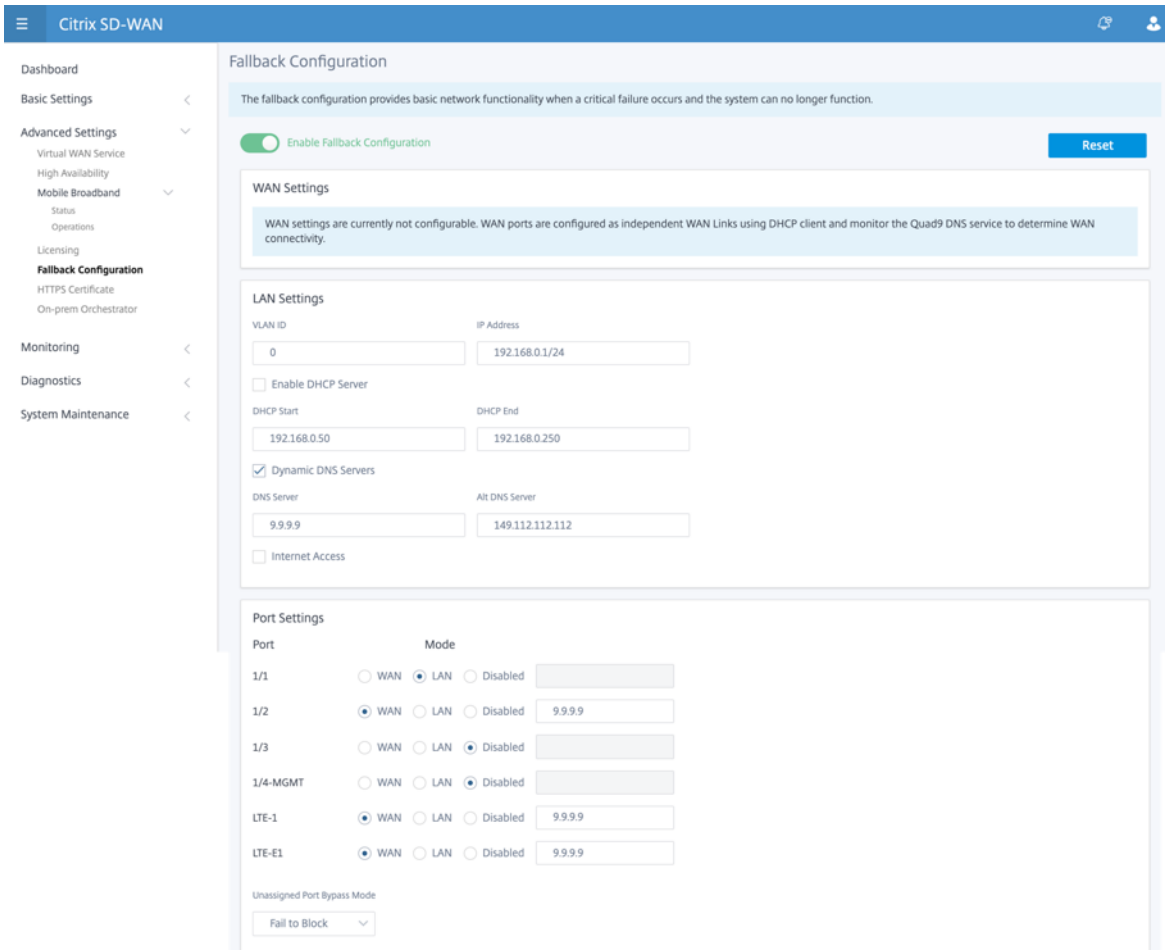


> **Note**
>
> When installing and applying a license from the SD-WAN Center, make sure that your specific

> appliance supports the SD-WAN appliance edition you want to enable, and that you have the correct software version available.

Fallback configuration

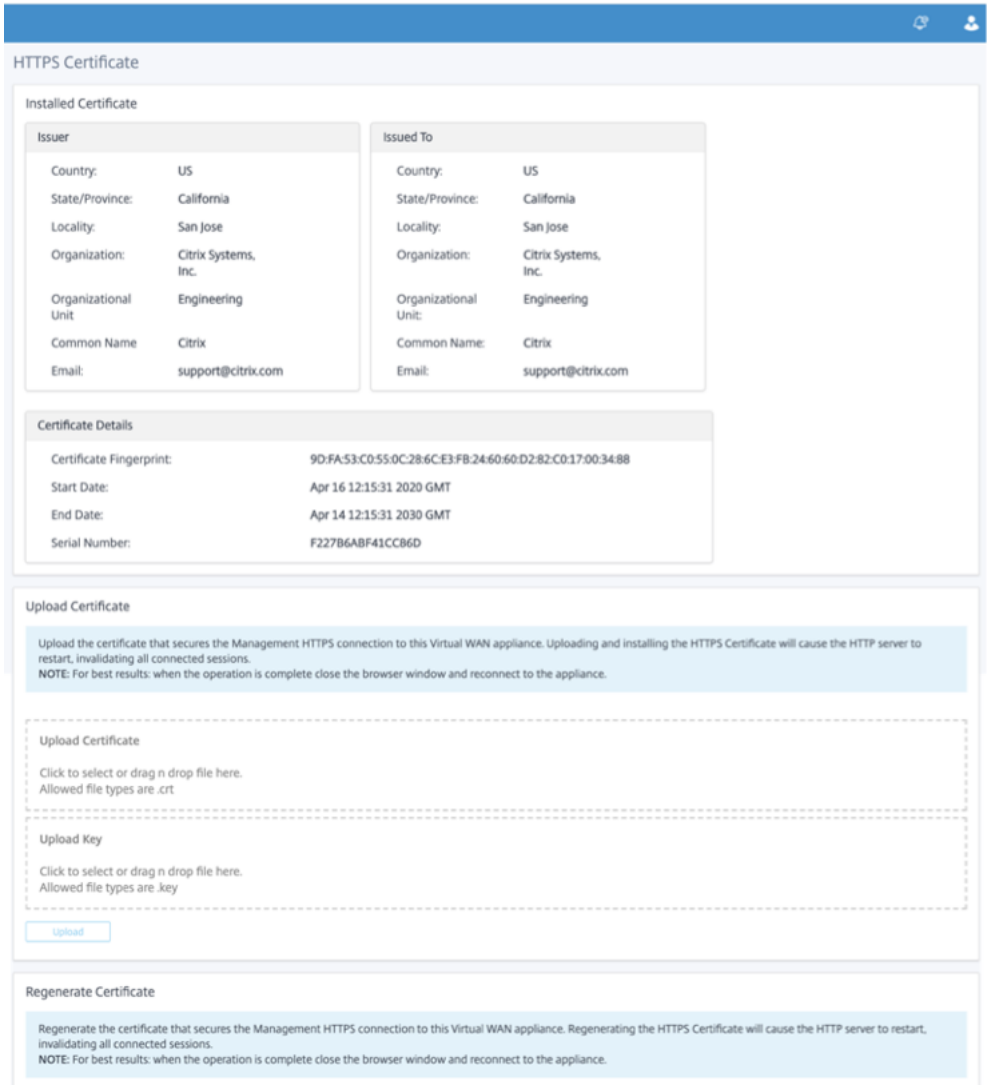
The **Fallback Configuration** page displays the stored fallback configuration data. If the fallback configuration is disabled, you can enable it by switching on the **Enable Fallback Configuration** switch.



For more information see, Fallback configuration.

HTTPS certificate

HTTPS certificate is required for establishing a secured connection. The **HTTPS Certificate** page displays the details of the HTTPS certificate that is already installed. For more information, see HTTPS certificates.



On-prem Orchestrator (Targeted for future)

Citrix On-prem SD-WAN Orchestrator is the on-premises software version of the Citrix SD-WAN Orchestrator service. Citrix On-prem SD-WAN Orchestrator provides a single-pane of glass management platform for Citrix partners to manage multiple customers centrally, with suitable role based access controls.

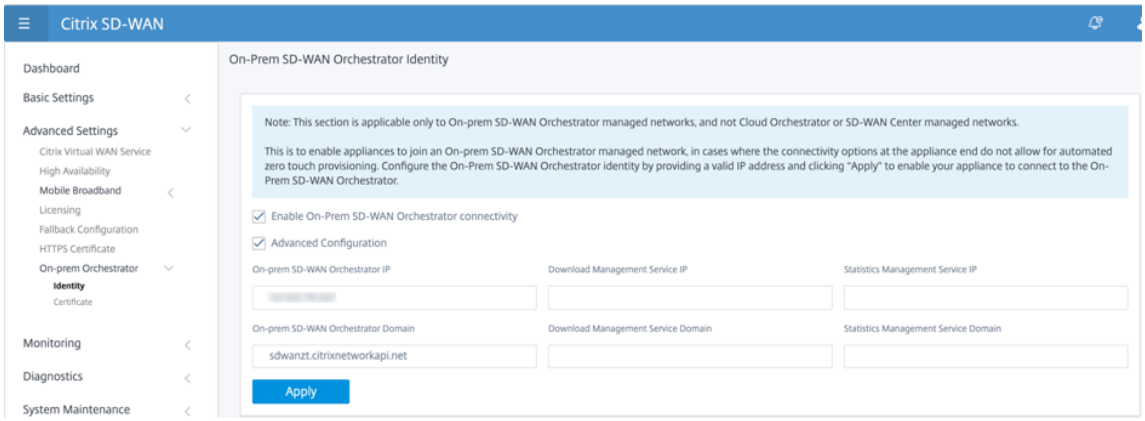
You can establish a connection between your Citrix SD-WAN appliance and the Citrix On-prem SD-WAN Orchestrator by enabling Orchestrator connectivity and specifying the On-prem SD-WAN Orchestrator identity.

> **Note**
>
> - The **On-prem SD-WAN Orchestrator configuration on SD-WAN appliance** feature is an

> enabler for Citrix On-prem SD-WAN Orchestrator. The Citrix On-prem SD-WAN Orchestrator configuration on SD-WAN appliance feature is currently not available, it is targeted for a future release.
> - Zero-touch deployment will not work if **On-prem SD-WAN Orchestrator configuration on SD-WAN appliance** feature is configured on the SD-WAN appliances.

To enable Orchestrator connectivity:

1. In the appliance GUI, navigate to **Advanced Settings > On-prem Orchestrator > Identity**.
2. Select **Enable On-prem SD-WAN Orchestrator Connectivity** check box.



3. Enter either the On-prem SD-WAN Orchestrator IP address or Domain or both (IP address and domain) for configuration.

   If the customer configures only Domain, then they must ensure to add DNS record in their Local DNS server and must configure DNS Server IP Address on SD-WAN Appliances. To configure, navigate to **Configuration > Network Adapters > IP Address**.

   For example, if the On-prem SD-WAN Orchestrator Domain is configured as citrix.com. then you must create a DNS record in DNS Server for the below FQDN and On-prem SD-WAN Orchestrator IP Address:

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

   In case of advanced configuration:

   For Example: If the On-prem Orchestrator domain is configured as **citrix.com**, the Download Management Service Domain is configured as **download.citrix**.com, and the Statistics Management Service Domain is configured as **statistics.citrix.com**. Then you must create a DNS record in DNS Server for the below FQDN and corresponding IP Address:

   - download.citrix.com

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

On-prem Orchestrator might support running services like download, statistics on independent server instance, to enable better scalability for large networks. You can select the **Advanced Configuration** and configure the **Download Management Service and Statistic Management** service.

Select the **Advanced Configuration** check box and provide the following details:

- **Download Management Service IP/Domain**: Provide the IP address /domain that helps offload SD-WAN software and configuration download aspects, to an independent server instance, to enable better scalability for large networks.
- **Statistic Management Service IP/Domain**: Provide the IP address/domain that helps offload collection and management of SD-WAN statistics from devices, to an independent server instance, to enable better scalability for large networks.

4. Click **Apply**.

   To Regenerate, Download, and Upload the SD-WAN appliance or On-prem SD-WAN Orchestrator certificate, navigate to **Advanced Settings > On-prem Orchestrator > Certificate**.

   If the On-prem Orchestrator **Authentication Type** is disabled, then Appliance can connect to the On-prem Orchestrator either via **No Authentication** or **One-way Authentication** or **Two-way Authentication mode**.

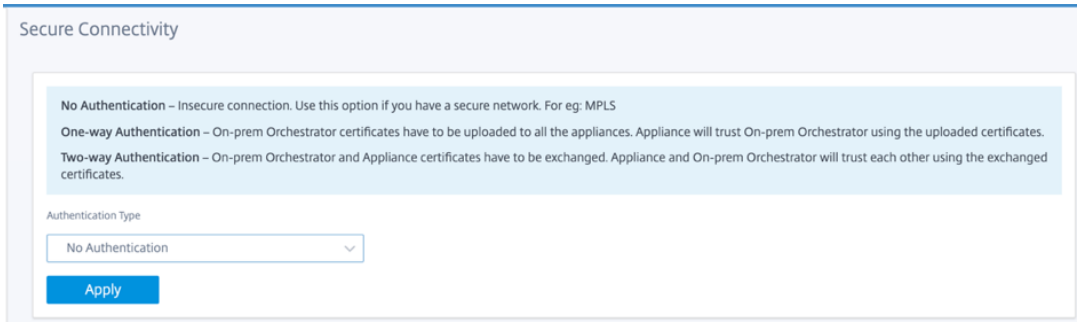
   If the On-prem Orchestrator **Authentication Type** is enabled, then Appliance can only able to connect to the On-prem Orchestrator via **Two-way Authentication**.

   While disabling **Authentication Type** in On-prem Orchestrator from enable state, existing appliances in One-way Authentication mode goes to disconnected state. Customers have to change the appliance Authentication Type to Two-way Authentication and upload the SD-WAN Appliance certificate to the On-prem Orchestrator to get it connected.

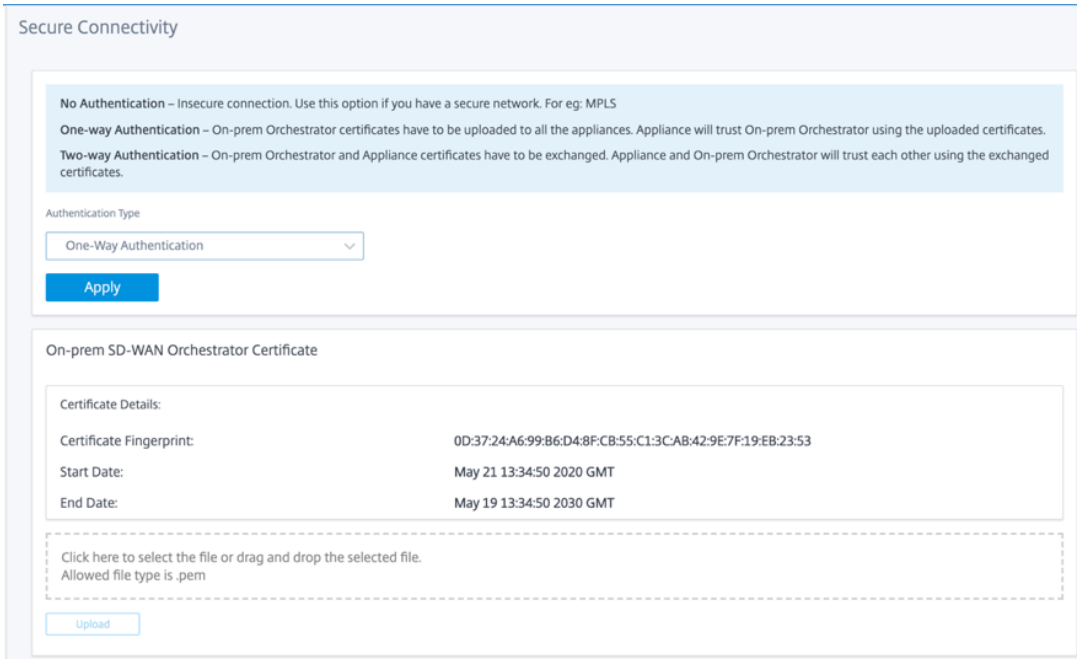
   > **Note**
   >
   > - Generated certificates are X509 self-signed certificates.
   > - Customer must regenerate the certificates if the certificate is expired or compromised.
   > - Validity of the certificate is 10 years.
   > - You can view the certificate details such as, fingerprint, start date, and end date
   > - Customer must ensure that the certificates are regenerated and exchanged between On-prem Orchestrator and SD-WAN appliance to avoid loss of appliance connectivity with On-prem orchestrator.

5. Select the **Authentication Type**. The following are the authentications types that are supported between the SD-WAN appliance and On-prem SD-WAN Orchestrator connectivity:

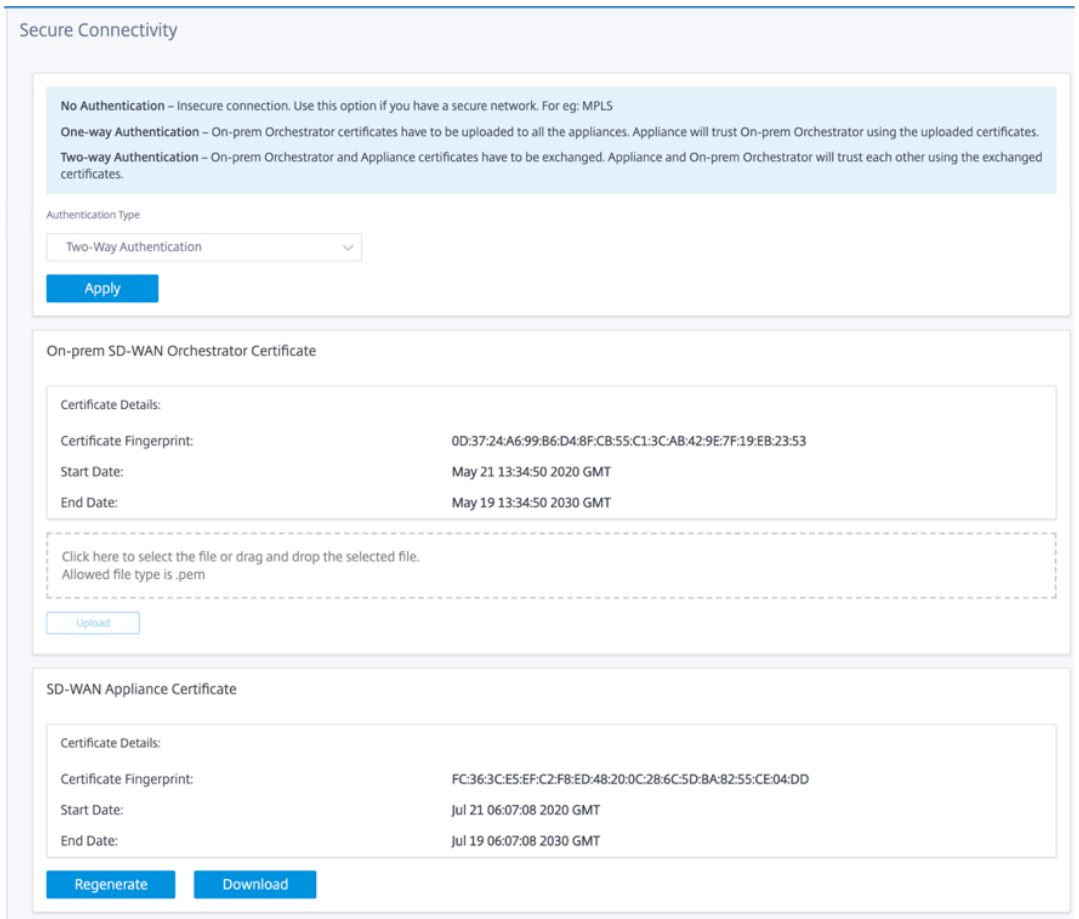
- **No Authentication** –No authentication between the On-prem SD-WAN Orchestrator and SD-WAN appliance, and there is no need to use the SD-WAN Appliance or On-prem SD-WAN Orchestrator Certificate. But you can use this option if you have a secure network such as MPLS.



- **One-way Authentication** –On selecting the One-way Authentication type, you must upload the On-prem Orchestrator certificate. Download the On-prem Orchestrator from the On-prem Orchestrator and click Upload. SD-WAN appliance trusts the On-prem Orchestrator using the uploaded certificates.



- **Two-way Authentication** –On-prem Orchestrator and Appliance certificates have to be exchanged with each other. For **Two-way Authentication**, you must regenerate, download, and upload the SD-WAN appliance certificate on the on-prem Orchestrator. SD-WAN appliance and On-prem Orchestrator trusts each other using the exchanged certificates.



> **Note**
>
> It is recommended to use only One-way Authentication or Two-way Authentication. If there was No Authentication, you have to choose the secure DNS server.

To disable the on-prem SD-WAN Orchestrator connectivity, uncheck **Enable ON-prem SD-WAN Orchestrator Connectivity** and click **Apply**. To convert On-prem orchestrator managed network to either Cloud Orchestrator or MCN Managed network, you need to disable On-prem SD-WAN Orchestrator Connectivity and must perform the configuration reset. To reset configuration, navigate to **Configuration > System Maintenance > Configuration Reset**.

Upgrade and Downgrade

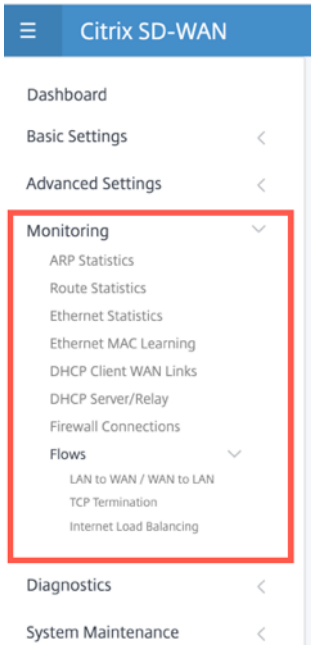
- After upgrading the SD-WAN appliance from 11.1.1/11.2.0/10.2.7 to 11.2.1 software version, you must exchange both appliance and On-prem Orchestrator certificates.
- After Downgrading the SD-WAN appliance from 11.2.1 to 11.1.1/11.2.0/10.2.7 software version, you must apply identity settings again on the Citrix SD-WAN appliance UI. If any issues related to

On-prem SD-WAN Orchestrator configuration or SD-WAN appliance connectivity, disable the On-prem SD-WAN Orchestrator connectivity and then enable the On-prem SD-WAN Orchestrator connectivity again.

The On-prem SD-WAN Orchestrator Authentication Type must be disabled to manage the SD-WAN appliances running 10.2.7/11.1.1/11.2.0 software version.

Monitoring

Under Monitoring section, you can view the **Address Resolution Protocol (ARP), Route, Ethernet, Ethernet MAC** statistics along with **DHCP Client WAN Links, DHCP Server/Relay, Firewall Connections,** and **Flows**.



- **ARP, Route, Ethernet, and Ethernet MAC Statistics**: You can see the statistics information for ARP, Route, Ethernet, and Ethernet MAC. Using the statistics information, you can verify any traffic or interface errors. For more information, see Viewing Statistical Information.
- **DHCP Client WAN Links**: The DHCP Client WAN Links page provides the status of learned IPs. You can request to renew the IP, which refreshes the lease time. You can also choose to **Release Renew**, which issues a new IP address with a new lease. For more details, see Monitoring DHCP client WAN links.
- **DHCP Server/Relay**: You can use the SD-WAN appliance as either DHCP Servers or DHCP Relay agents.
  - The DHCP server feature allows devices on the same network as the SD-WAN appliance's LAN/WAN interface to obtain their IP configuration from the SD-WAN appliance.

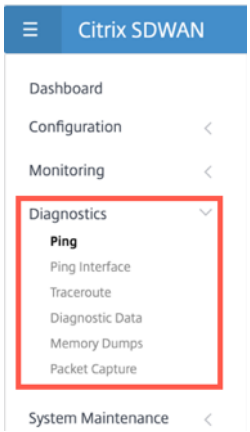
  - The DHCP relay feature allows your SD-WAN appliances to forward DHCP packets between DHCP client and server.

  For more information, see DHCP server and DHCP relay.

- **Firewall Connections**: The **Firewall Connections** page provides the Firewall connection statistics. You can see how the firewall policies are acting on the traffic for each Application. For more information, see Viewing Firewall Statistics.
- **Flows**: The **Flows** section provides basic instructions for viewing Virtual WAN flow information. For more details, see Viewing Flow Information.

Diagnostics

The **Diagnostics** section provides the options to test and investigate connectivity issues. For more information, see Diagnostics.



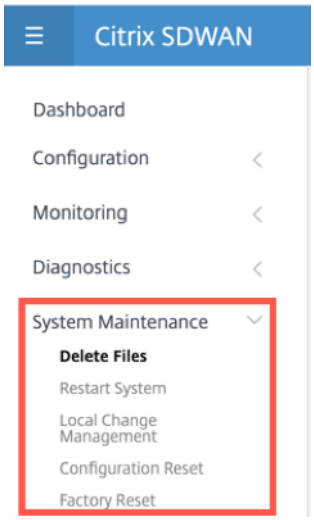
> **Note**
>
> For the Citrix SD-WAN 110 appliance, only one diagnostic package can be present at a time. For the Citrix SD-WAN 210 appliance, a maximum of five diagnostic packages are allowed.

System maintenance

Use the **System Maintenance** section to perform maintenance activities. The **System Maintenance** page contains the following options:

- **Delete Files**: You can delete Log files, Backup files, and Archived Databases. Select the file that you want to delete from the drop-down menu and click the delete button.
- **Restart System**: You can restart the virtual WAN service or reboot the system.
- **Local Change Management**: The **Local Change Management** process allows you to upload a new appliance package to this individual appliance.

- **Configuration Reset**: You can reset the configuration. This option clears out the user data, logs, history, and local configuration data on this appliance.
- **Factory Reset**: Use **Factory Reset** option to reset the SD-WAN appliance to the shipped version.



> **Note**
>
> All of these features are already explained in details in the existing SD-WAN documentation.

System requirements

March 12, 2021

Hardware requirements

Instructions for installing SD-WAN appliances are provided in Setting up the SD-WAN appliances.

Firmware requirements

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

> **Note**
>
> Appliances running earlier software versions cannot establish a Virtual Path connection to the appliance running SD-WAN release 11.2. For additional information, please contact the Citrix support team.

Software requirements

For details regarding license requirements, see Licensing.

Browser Requirements

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

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

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

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

Hypervisor

Citrix SD-WAN SE/PE VPX can be configured on the following hypervisors:

- VMware ESXi server, version 5.5.0 or higher.
- Citrix Hypervisor 6.5 or higher.
- Microsoft Hyper-V 2012 R2 or higher.
- Linux KVM

Cloud Platform

Citrix SD-WAN SE/PE VPX can be configured on the following cloud platforms:

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

SD-WAN platform models and software packages

March 12, 2021

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

> **Note**
>
> Before you download the software, you must obtain and register a Citrix SD-WAN software license. For information, see Licensing.

An 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 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, when the virtual paths to the clients become operational.

Download the software packages

There is a different Citrix SD-WAN software package for each appliance model. You 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; product downloads.
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 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 Premium Edition
- SD-WAN VPX Virtual Appliances (SD-WAN VPX)
  - Standard Edition and WANOP Edition

> **Note**
>
> All SD-WAN appliance models in an 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, refer the SD-WAN product platform edition data sheet on the products download site.

SD-WAN standard edition hardware appliances

Citrix SD-WAN release 11.2 supports the following SD-WAN standard edition hardware appliance models:

SD-WAN SE PLATFORM MODEL	ROLE
110-SE/110-LTE-WiFi	Small branch appliance
210-SE/210-SE LTE	Small branch appliance
410-SE	Small branch appliance
1000-SE	Small branch appliance
1100-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
6100-SE	Data Center - Master Control Node (MCN) appliance

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

Citrix SD-WAN 11.2 supports the following SD-WAN WAN Optimization (WANOP) appliance models:

SD-WAN WANOP PLATFORM MODELS	ROLE
WANOP 800	Small branch appliance
WANOP 1000	Large branch appliance

SD-WAN WANOP PLATFORM MODELS	ROLE
WANOP 2000	Large branch appliance
WANOP 3000	Large branch appliance
WANOP 4100	Data Center appliance
wANOP 5100	Data Center appliance

SD-WAN VPX virtual appliances (SD-WAN VPX-SE)

Citrix SD-WAN 11.2 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

For more information, see the Prerequisites of Citrix SD-WAN Virtual VPX Standard Edition.

SD-WAN WANOP virtual appliances (SD-WAN VPX-WANOP)

Citrix SD-WAN 11.2 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

SD-WAN VPX WANOP PLATFORM MODELS	ROLE
WANOP VPX-200	Large branch appliance

> **Important**
>
> In release version 10.1, the Enterprise platform edition is rebranded to “Premium Edition.”

SD-WAN premium edition hardware appliances (SD-WAN PE)

Citrix SD-WAN 11.2 supports the following SD-WAN Premium (Enterprise) Edition appliance (SD-WAN PE) models:

SD-WAN EE PLATFORM MODELS	ROLE
1000-PE	Large branch, data center appliance
1100-PE	Large branch, data center appliance
2100-PE	Large branch, data center appliance
5100-PE	Large branch, data center appliance
6100-PE	Large branch, data center appliance

Upgrade paths

September 23, 2021

The following table provides details of all the Citrix SD-WAN software version that you can upgrade to, from the previous versions.

SD-WAN	11.4.1	11.3.2	11.2.3	11.1.3	11.0.3	10.2.8
11.3.x	✓	✓				
11.2.x	✓	✓	✓			
11.1.x	✓	✓	✓	✓		
11.0.x	✓	✓	✓	✓	✓	
10.2.8	✓	✓	✓	✓	✓	
10.2.x	—	—	—	—	—	✓

The upgrade paths information is also available in the Citrix Upgrade Guide.

> **Note**
>
> - Customers upgrading from Citrix SD-WAN release 9.3.x are recommended to upgrade to 10.2.8 before upgrading to any major release.
> - While performing software upgrade, ensure that staging to all connected sites is completed before activating. If activation is done before staging completes by enabling Ignore Incomplete, the virtual path might not come up with MCN for the sites to which staging was still in progress. To recover the network, it is required perform local change management for those sites manually.
> - From Citrix SD-WAN release 11.0.0 onwards, the underlying OS/kernel for the SD-WAN software is upgraded to a newer version. It requires an automatic reboot to be performed during the upgrade process. As a result, the expected time for upgrading each appliance is increased by approximately 100 seconds. In addition, by including the new OS, the size of the upgrade package transferred to each branch appliance is increased by approximately 90 MB.

Virtual WAN software upgrade to 9.3.5 with working Virtual WAN deployment

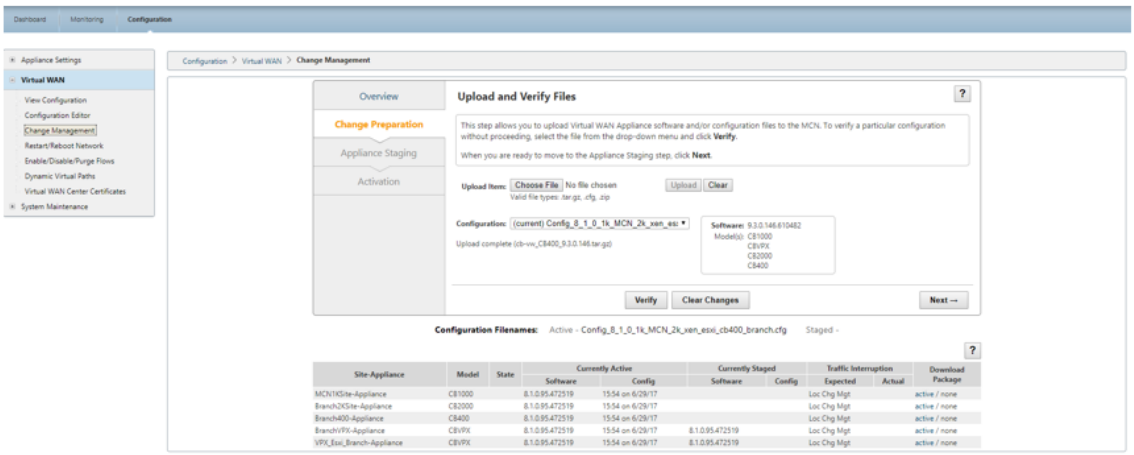
March 12, 2021

> **Note:**
>
> Have a working Virtual WAN configuration running 9.3.4 or below build, with virtual paths established from MCN to the branch sites.

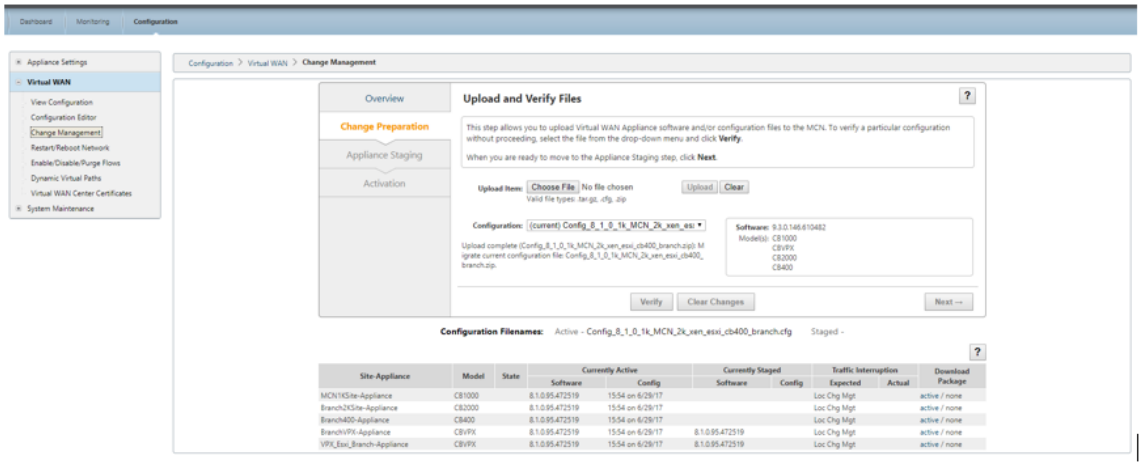
1. On the MCN appliance, navigate to **Configuration** > **Virtual WAN** > **Change Management**.

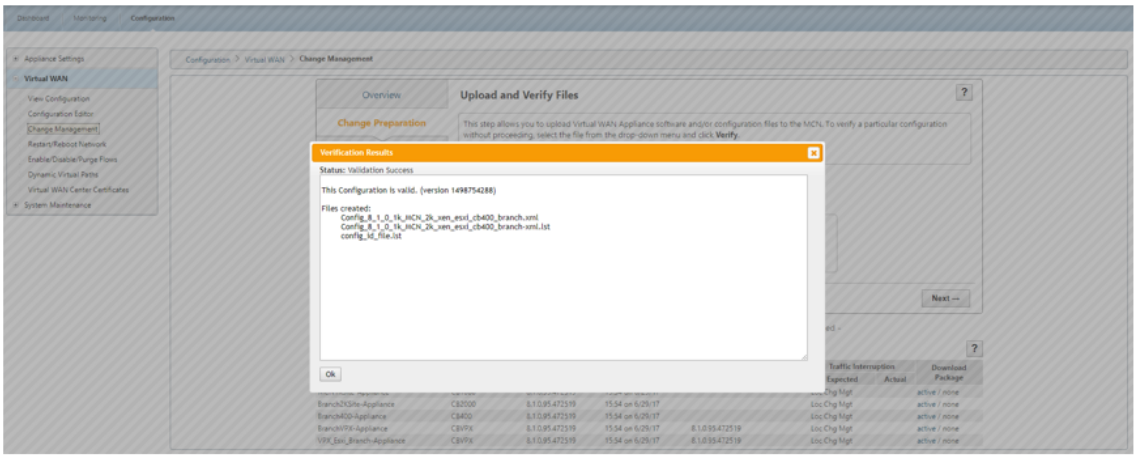
2. Obtain the applicable *cb-vw-<ApplianceModel>-9.3.5.23.tar.gz* file for all sites in the Virtual WAN network from Citrix download page

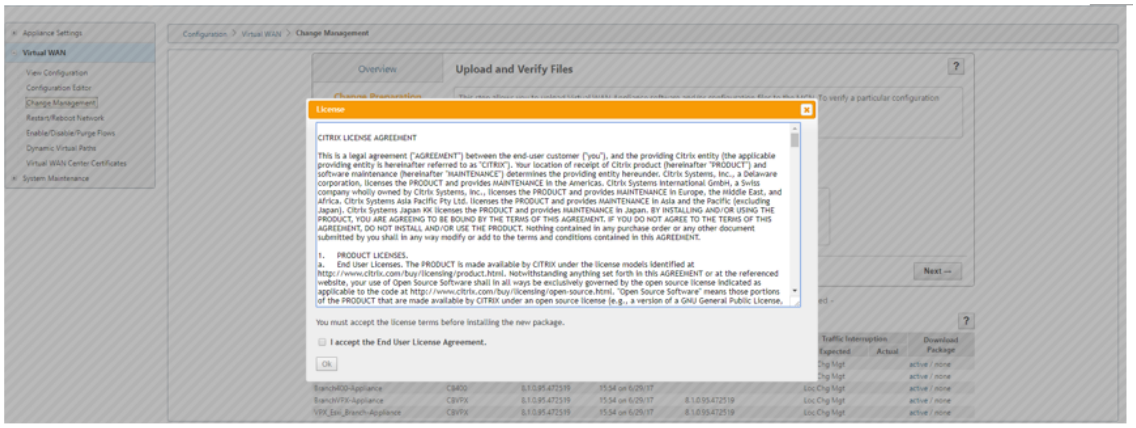
3. Upload the *cb-vw-<ApplianceModel>-9.3.5.23.tar.gz* file for the branches defined in the configuration file for which upgrade has to be performed. Perform Change Management in SD-WAN web interface for the MCN appliance and complete the change management process.



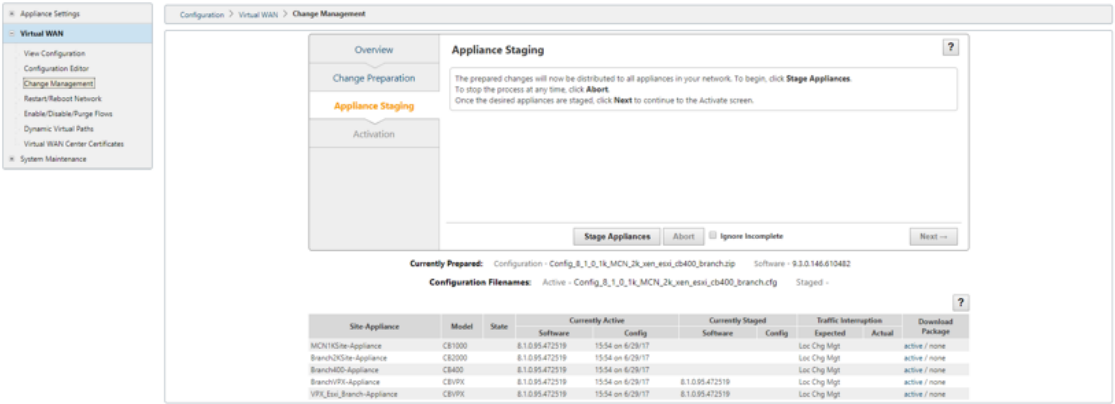
4. Click **Next** to proceed further.



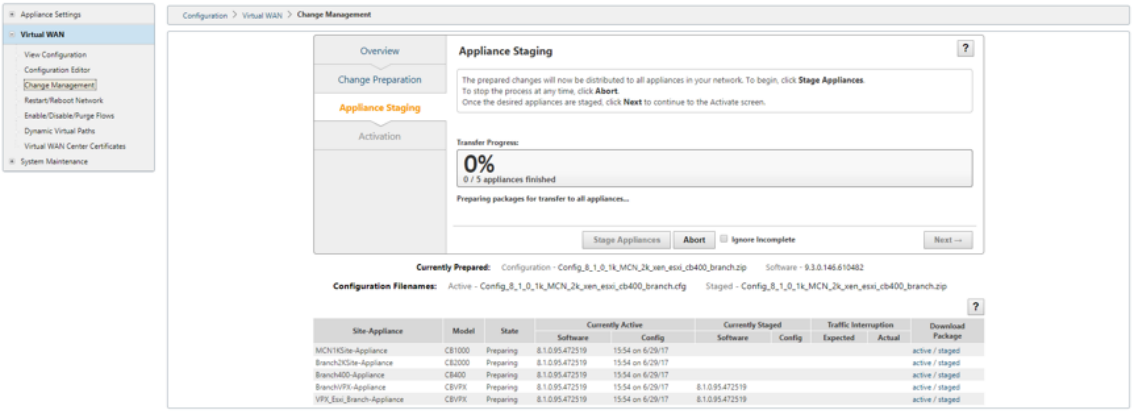


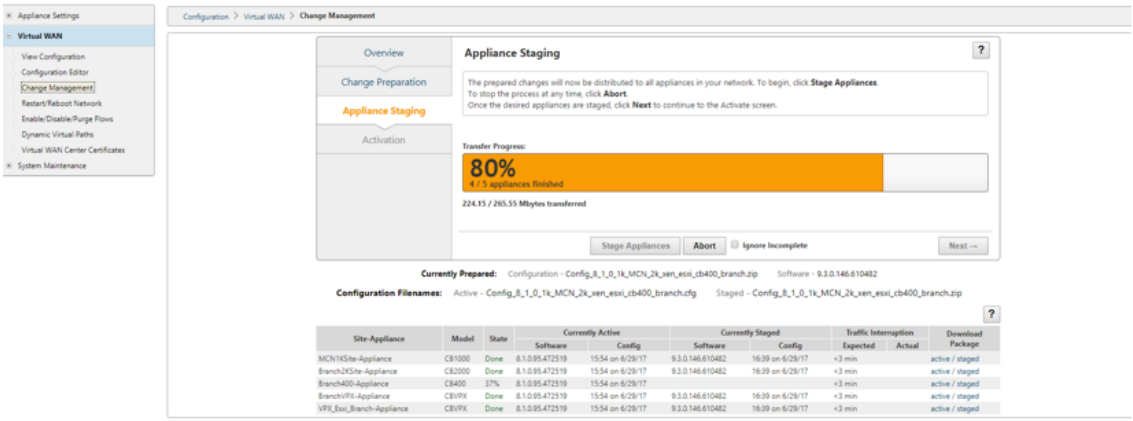


5. After accepting license agreement, you are navigated to **Appliance Staging** where appliances can be staged by clicking on **Stage Appliances**.

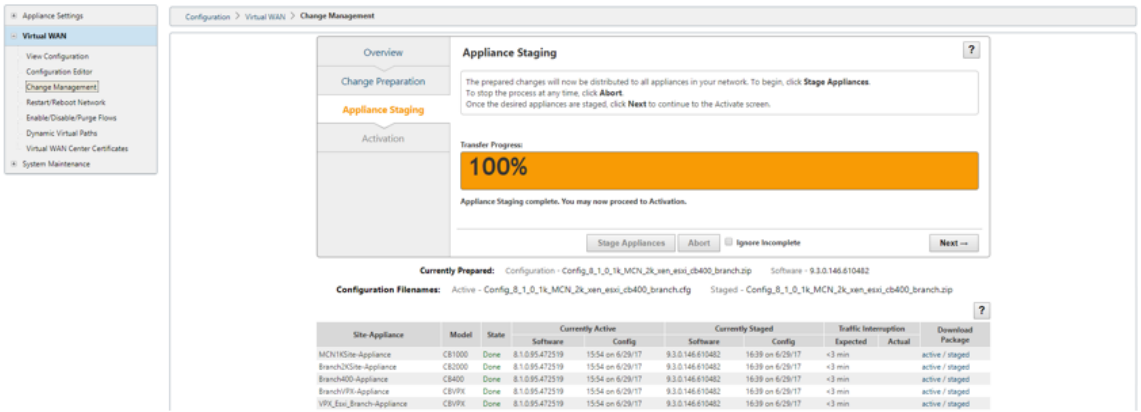


6. Transfer Progress status is displayed as part of preparing and staging the software packages to the appliances.

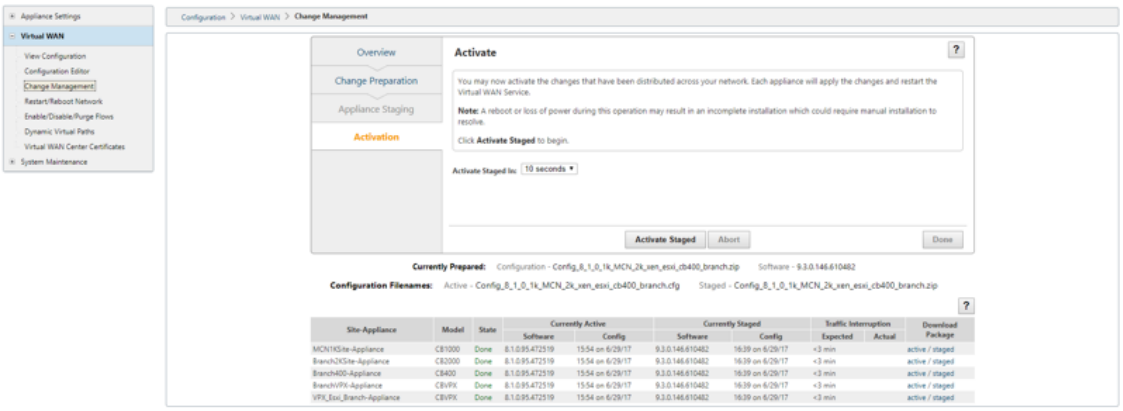


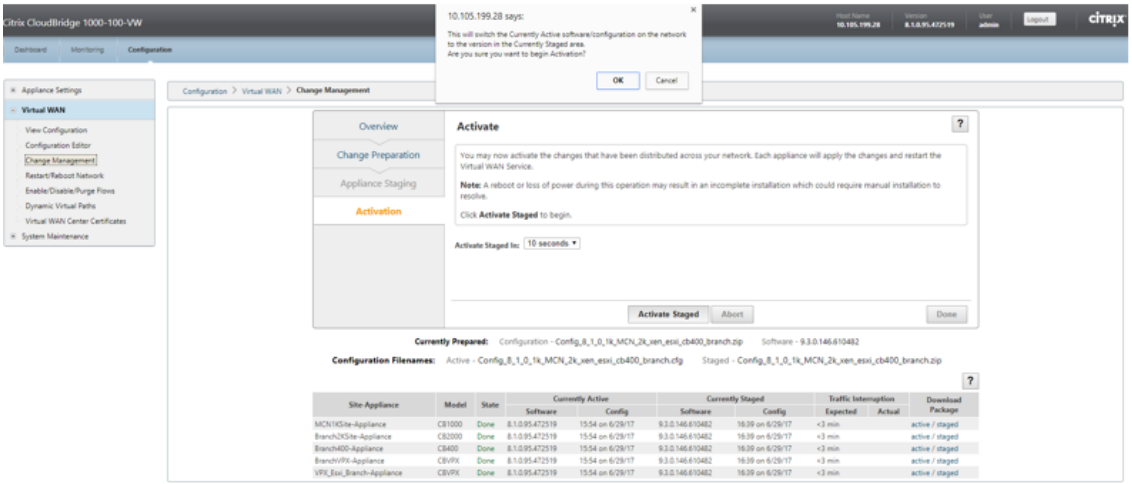


7. Click **Next** when Transfer Progress shows 100%, and button is enabled to proceed.

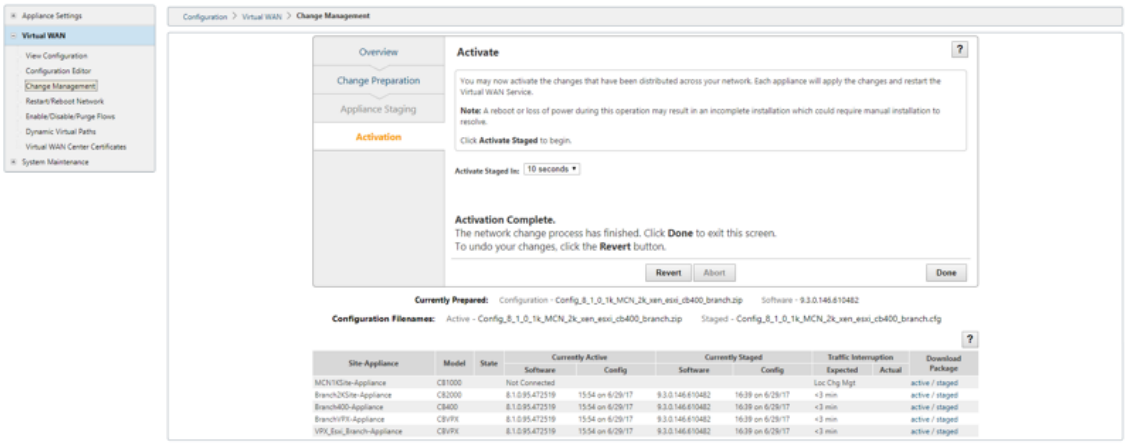


8. In the **Activation** page, click **Activate Staged** to begin activation.





9. After completion of activation countdown of 180 s click **Done**.

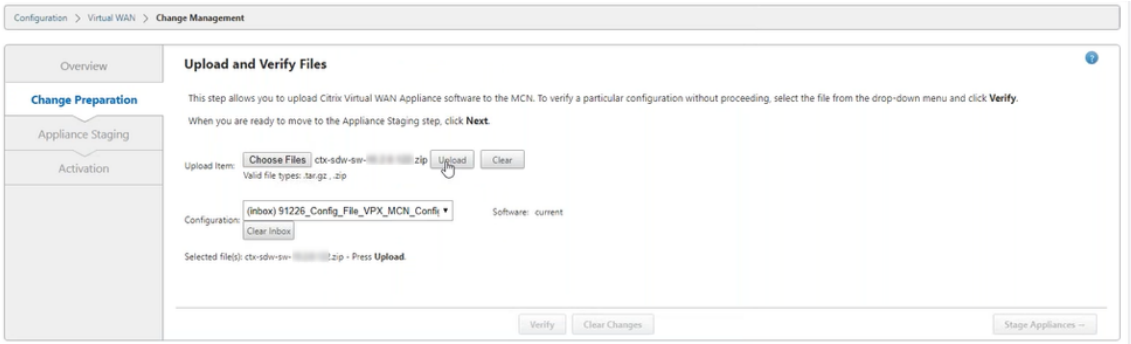


Upgrade to 11.2 with working Virtual WAN deployment

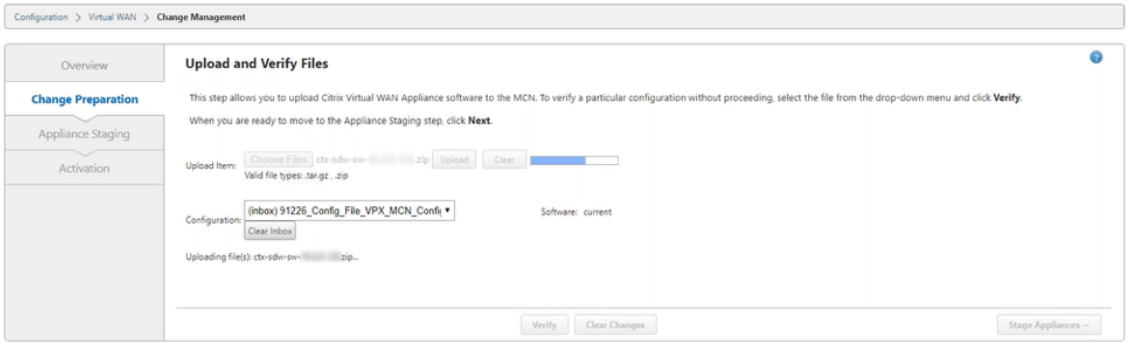
March 12, 2021

1. In the **Change Management > Change Preparation** page, click **Choose Files** and select the *ctx-sdw-sw-11.2.0.x.zip* software package file. Click **Upload**.

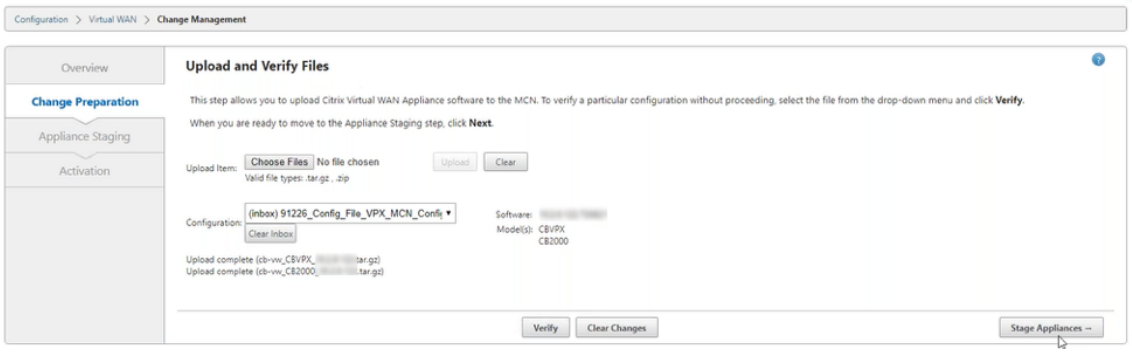
> **Note:**
>
> You can download the Citrix SD-WAN release 11.2 software package from the Downloads page.



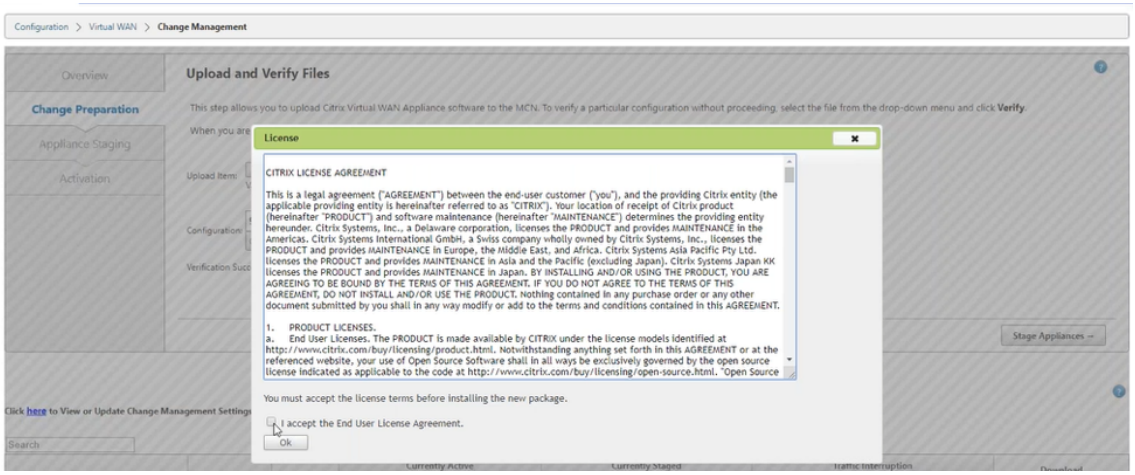
A progress bar appears to show the current upload progress.



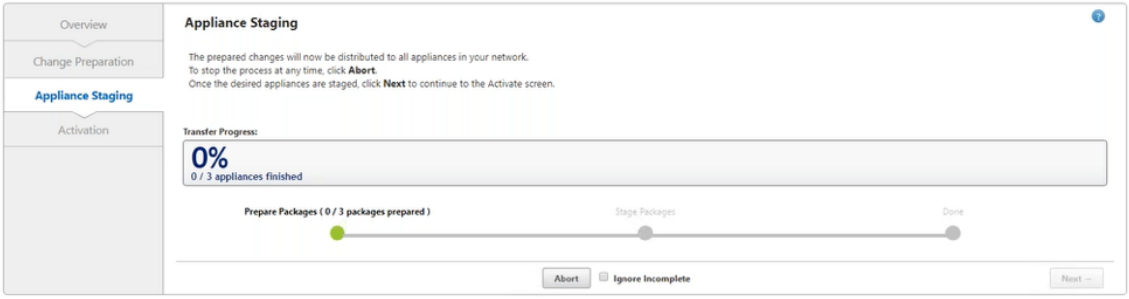
2. After the upload process is successful, relevant appliance models are displayed. The appliances would be upgraded based on the configuration file.



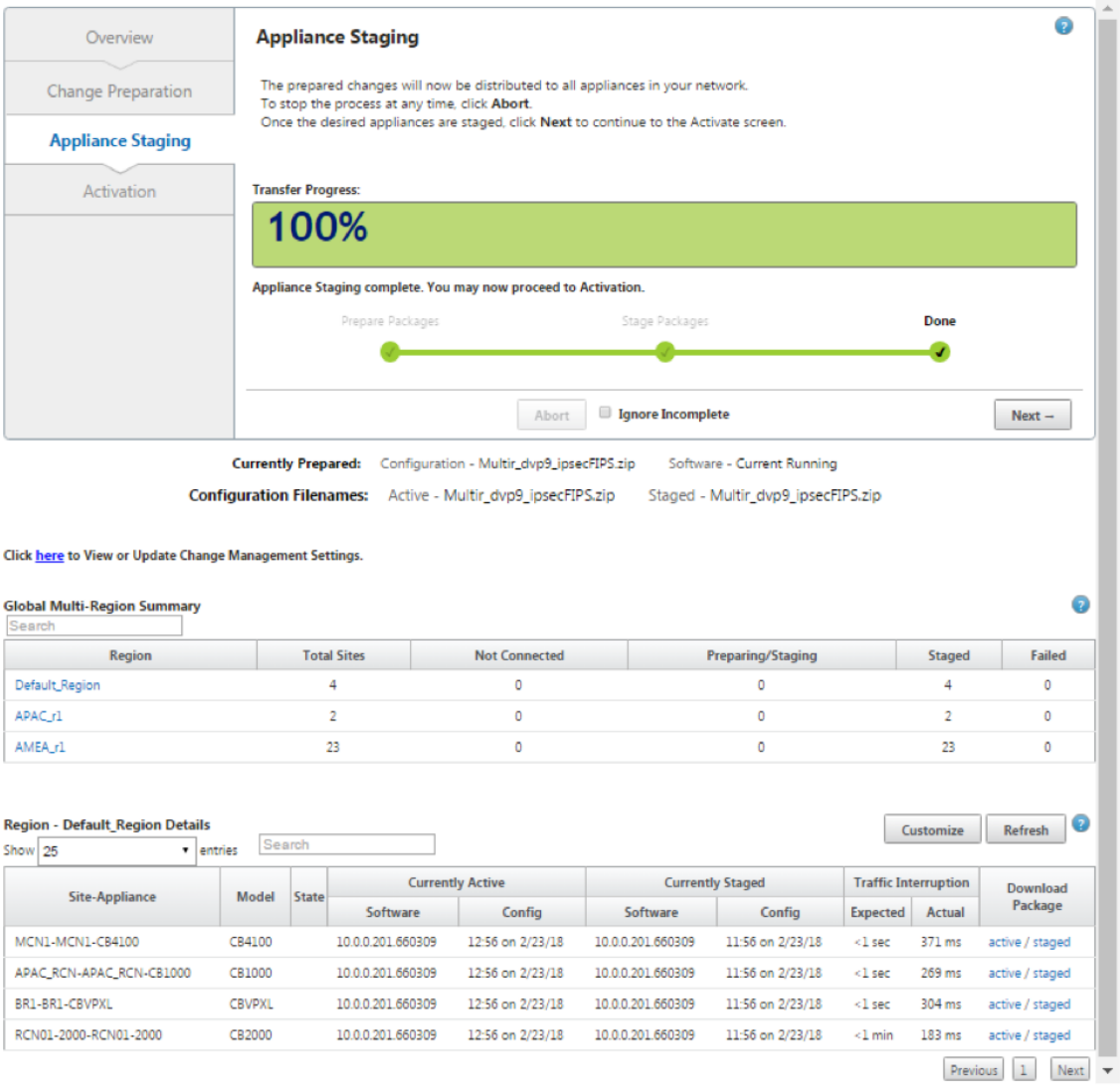
3. Click **Stage Appliance** to proceed with validation of configuration file. The License agreement page for user acceptance appears. Click **I accept the End User License Agreement** and click **OK**.



4. The **Appliance Staging** process is initiated. The changes are distributed to all appliances on the network. The transfer progress bar appears and the site details table is updated.



5. Once the transfer progress is 100% complete, click **Next** to proceed to activation.

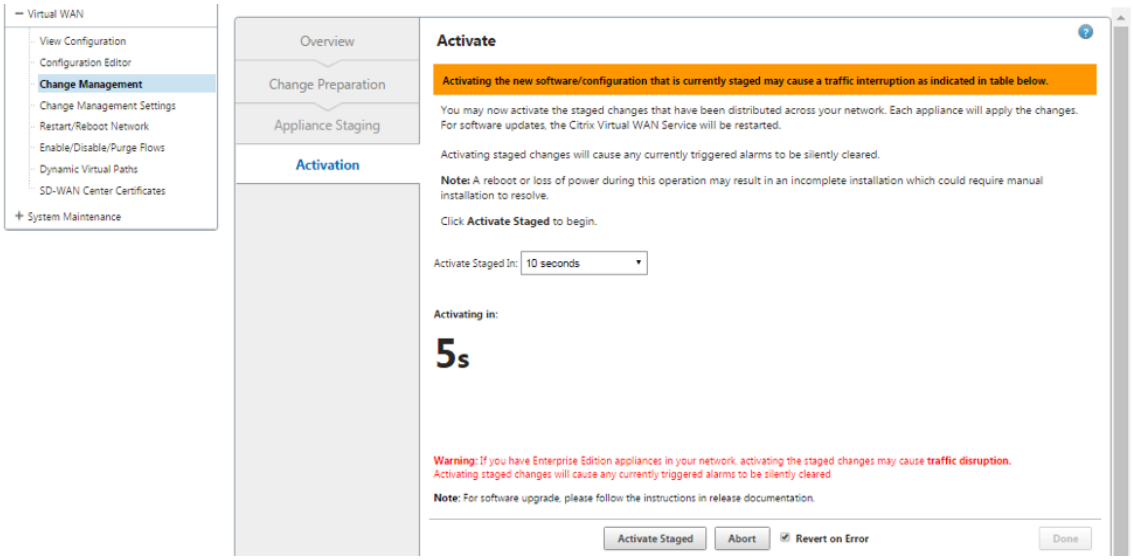


The various states of software package configuration displayed in the summary table indicate the following:

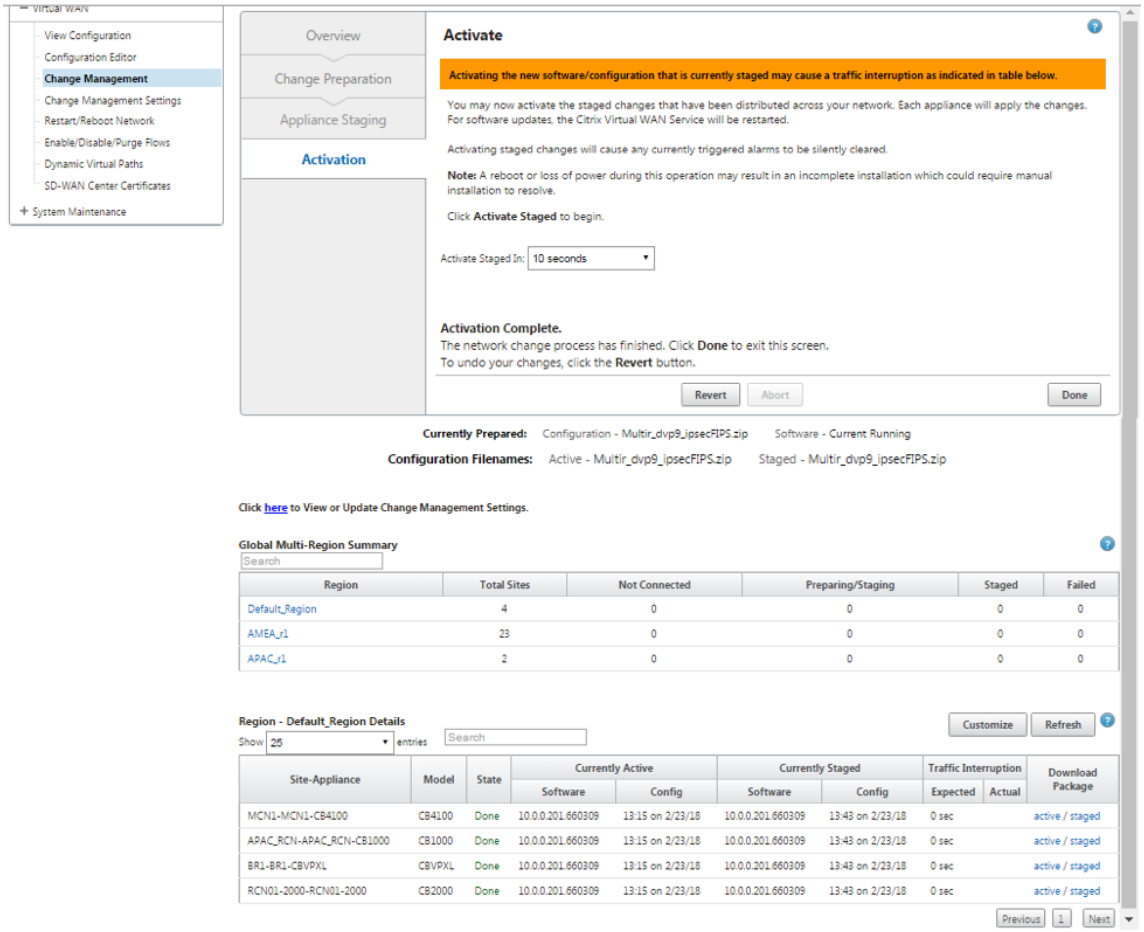
- **Preparing** - Local processing to prepare update package for transfer to the appliance.
- **Preparing Region Packages** - Local processing to prepare update package for transfer to RCN. (Applicable if RCN is part of network).
- **Percentage** - Percent of package transferred to the appliance.
- **Unpacking** - 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.
- **Canceled** - Canceled 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.

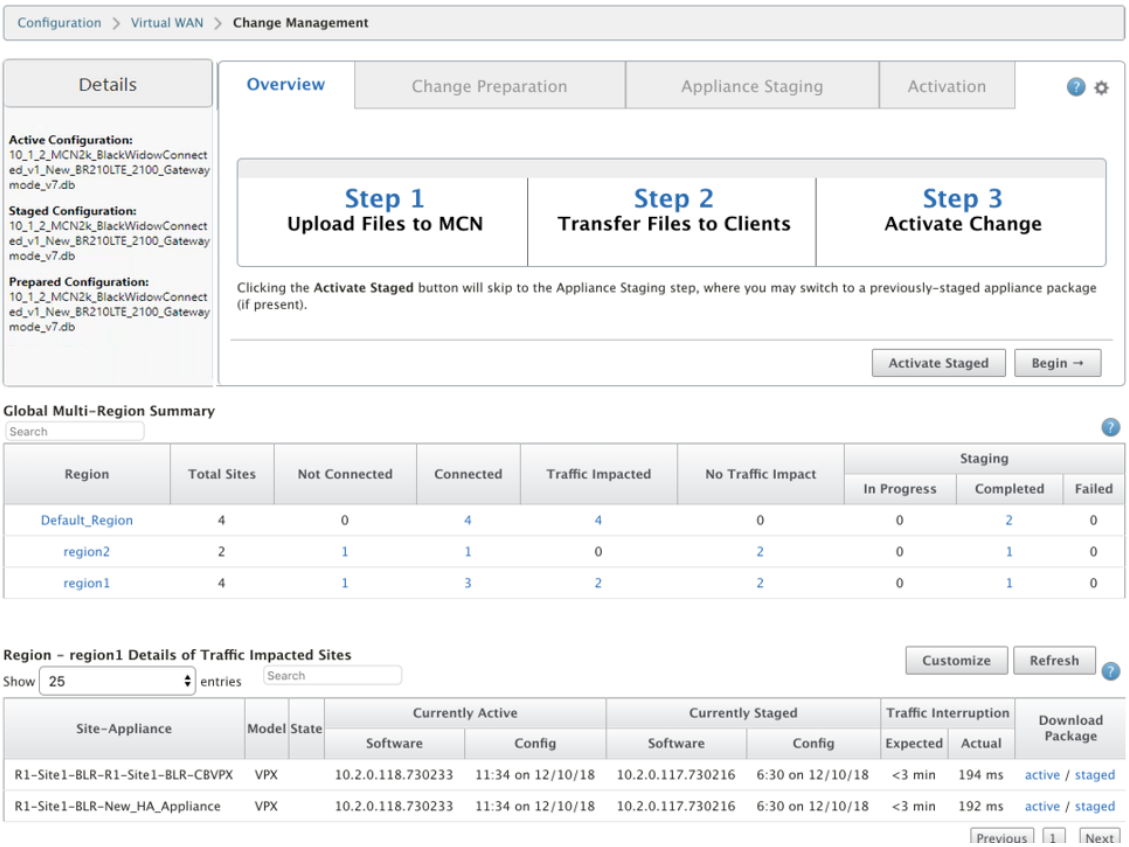
6. Click **Activate Staged** to activate the staged software.



7. After the countdown, a message indicates that activation is completed. Click **Done**.

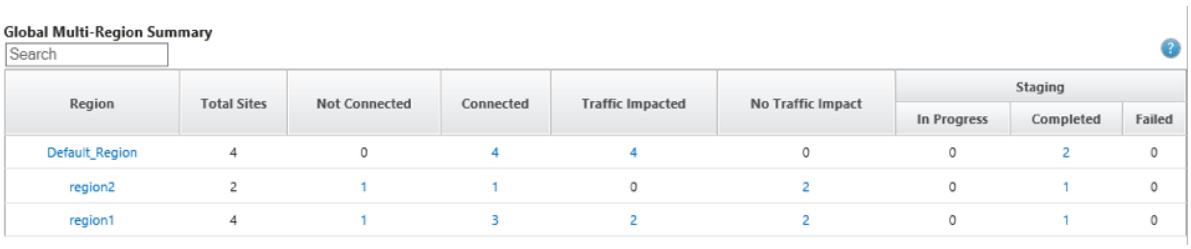


8. Navigate to **Change Management** page to view the transfer status.



The Multi-region summary table provides the following details:

- **Region** –Name of the region
- **Total Site** - Total number of sites in the region.
- **Not Connected** - Total number of sites not connected in the region.
- **Connected** - Total number of sites connected in the region.
- **Traffic Impacted** - Total number of sites where the traffic is impacted in the region.
- **No Traffic Impact** - Total number of sites where the traffic is not impacted in the region.
- **Staging In Progress** - Total number of sites for which local processing is attempting to prepare update package for transfer in the region.
- **Staging Completed**- Total number of sites for which staging has completed in the region.
- **Staging Failed** - Total number of sites for which incomplete transfer was deleted in the region.



Click the **Global Multi-Region Summary** table entry link to filter the region specific configuration reports.

Region - Default_Region Details of Connected Sites

Show 25 entries Search

Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN-NY-MCN-NY-CB2000	2000		10.2.0.118.730233	11:34 on 12/10/18	10.2.0.117.730216	6:30 on 12/10/18	<3 min	82 s	active / staged
Def-Site1-SC-Def-Site1-SC-CBVPX	VPX		10.2.0.118.730233	11:34 on 12/10/18	10.2.0.117.730216	6:30 on 12/10/18	<3 min	209 s	active / staged
R1-RCN-MUM-R1-RCN-MUM-CBVPX	VPX	Done(auto)	10.2.0.118.730233	11:34 on 12/10/18	10.2.0.117.730216	6:30 on 12/10/18	<3 min	195 s	active / staged
R2-RCN-SA-R2-RCN-SA-CBVPX	VPX	Done(auto)	10.2.0.118.730233	11:34 on 12/10/18	10.2.0.117.730216	6:30 on 12/10/18	<3 min	199 s	active / staged

Previous 1 Next

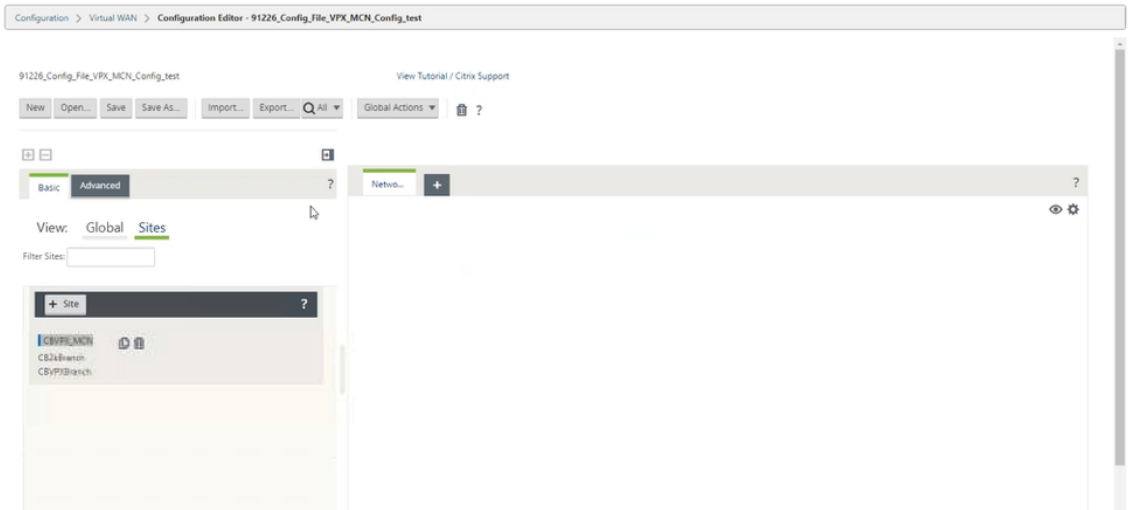
For muliregion deployment, on each RCN navigate to **Change Management Settings** page and schedule the installation of dependent components. By default the MCN/RCN assigns schedules installation to be attempted every day at 21:20:00 based on software availability on the branches.For more information, see Change Management Settings

Upgrading to 11.2 without working virtual WAN deployment

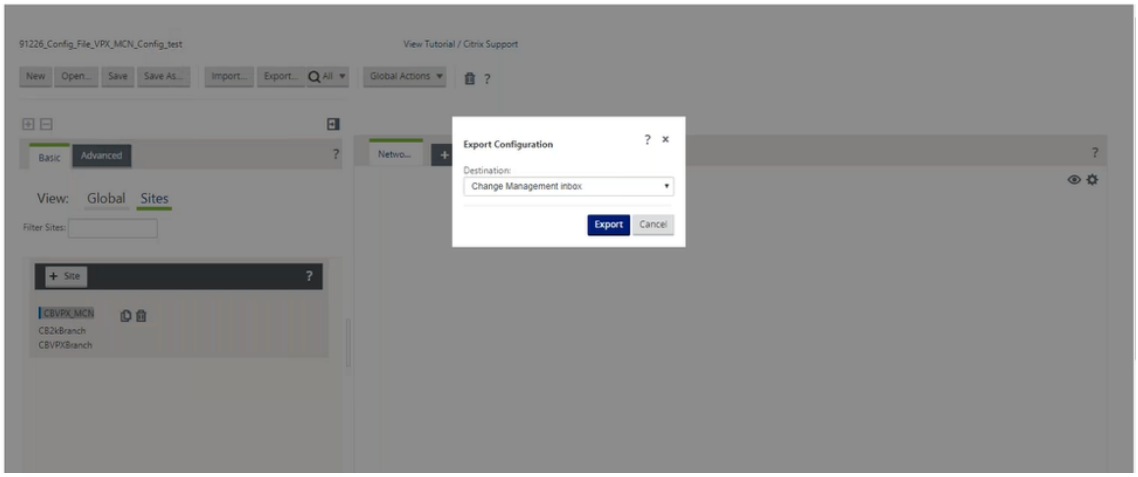
March 12, 2021

> Note: To configure the latest 11.2 features, remiage the MCN appliance to 11.2 software. For more information, see Reimage Citrix SD-WAN appliance software

1. Prepare the configuration using the **Configuration Editor** and save the configuration with a valid name. For more information, see Configuration topic.

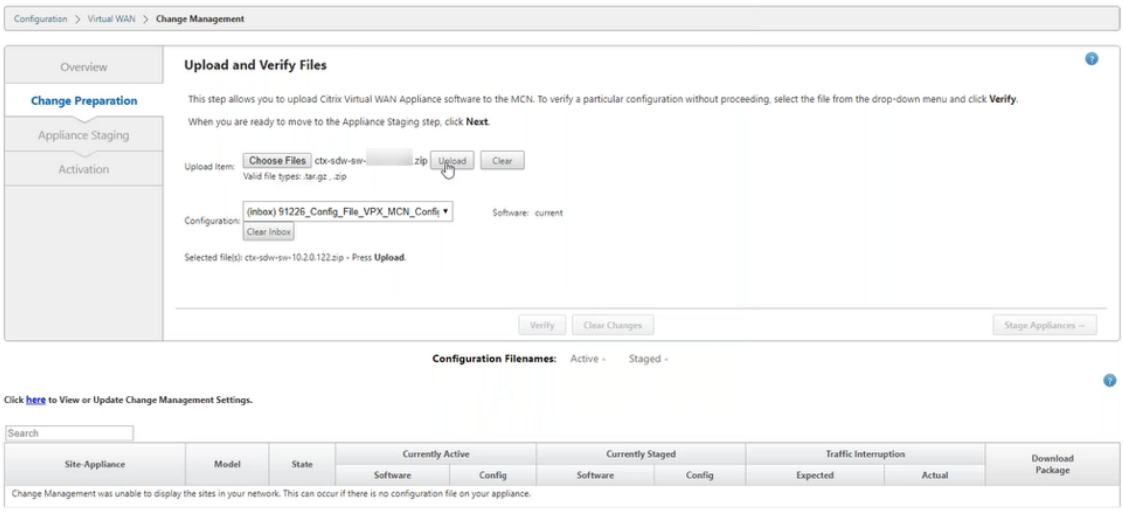


2. Export the saved configuration to Change Management. Click **Export** and select **Change Management Inbox** as the destination. Click **Export**.

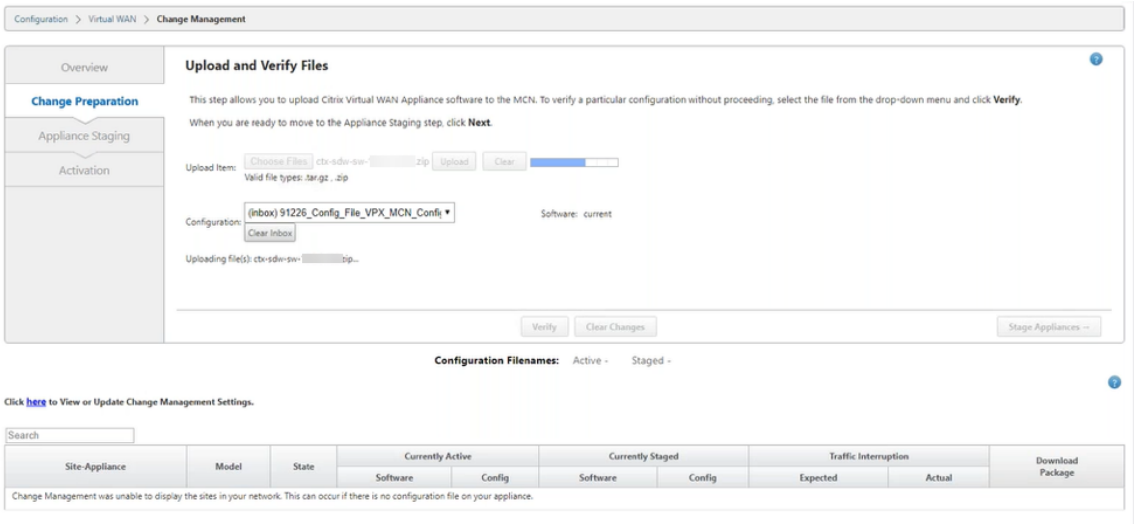


3. In the **Change Management > Change Preparation** page, click **Choose Files** and select the *ctx-sdw-sw-11.2.0.x.zip* software package file. Click **Upload**.

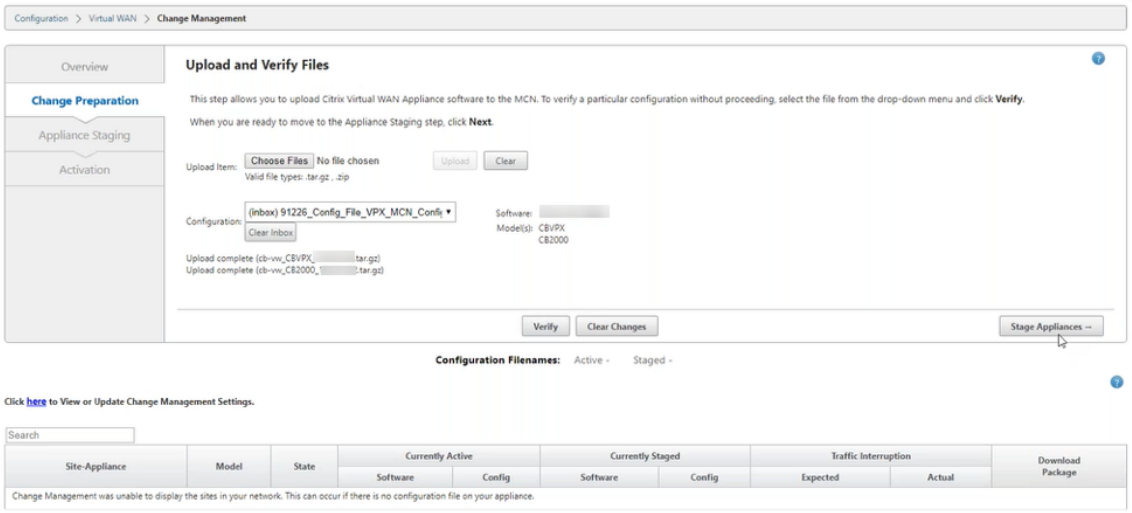
> **Note:**
>
> You can download the Citrix SD-WAN release 11.2 software package from the Downloads page.



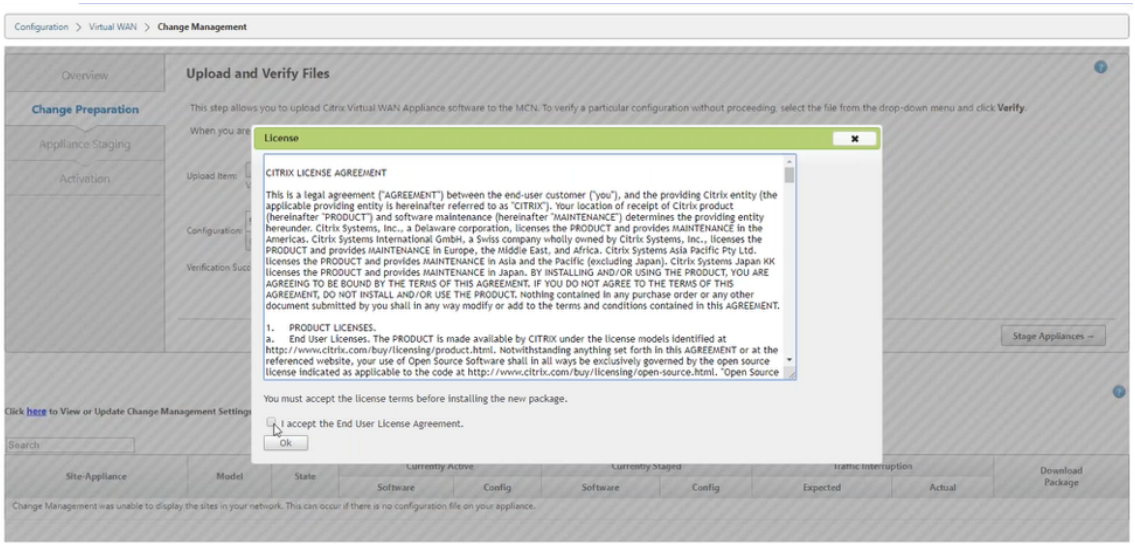
A progress bar appears to show the current upload progress.



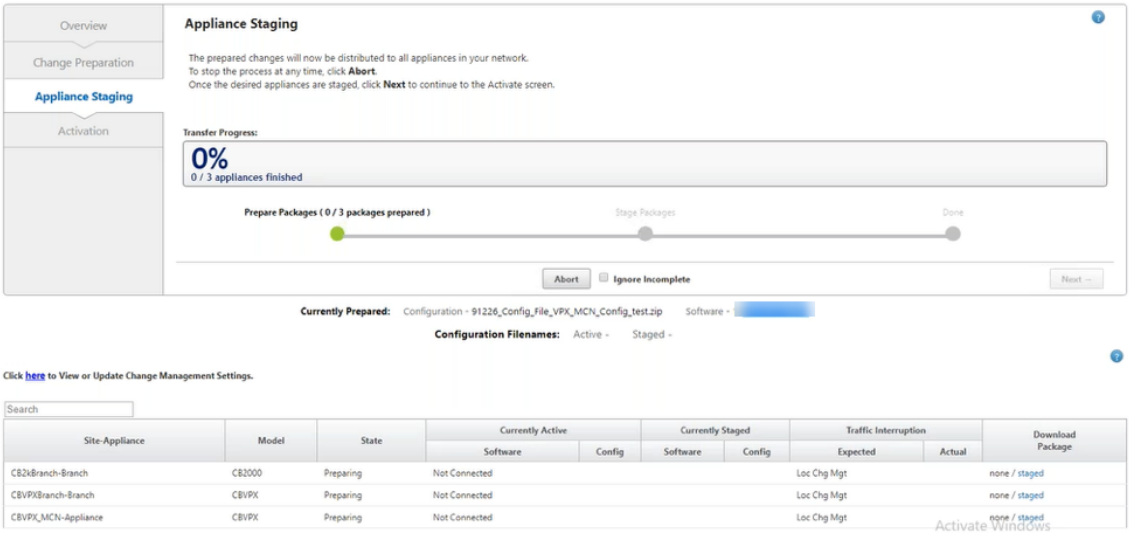
4. After upload process is successful, relevant models are displayed that would be upgraded based on the configuration file that has information about each branch platform model.



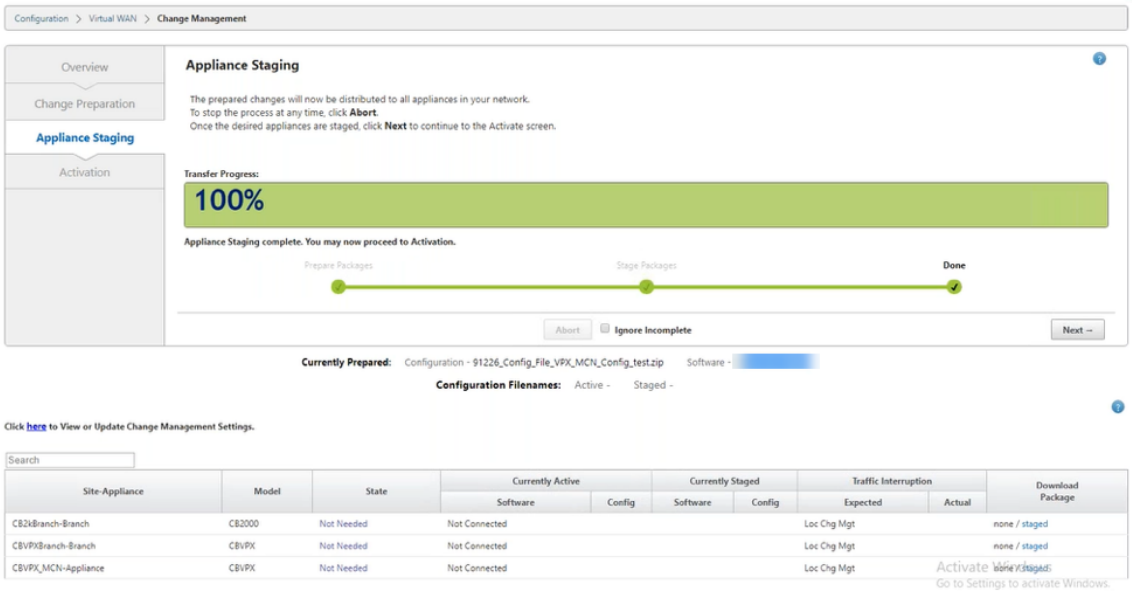
5. Click **Stage Appliance** to proceed with validation of configuration file. The License agreement page for user acceptance appears. Click **I accept the End User License Agreement** and click **OK**.



6. The **Appliance Staging** process is initiated the changes will be distributed to all appliances on the network. The transfer progress bar appears and the site details table is updated.

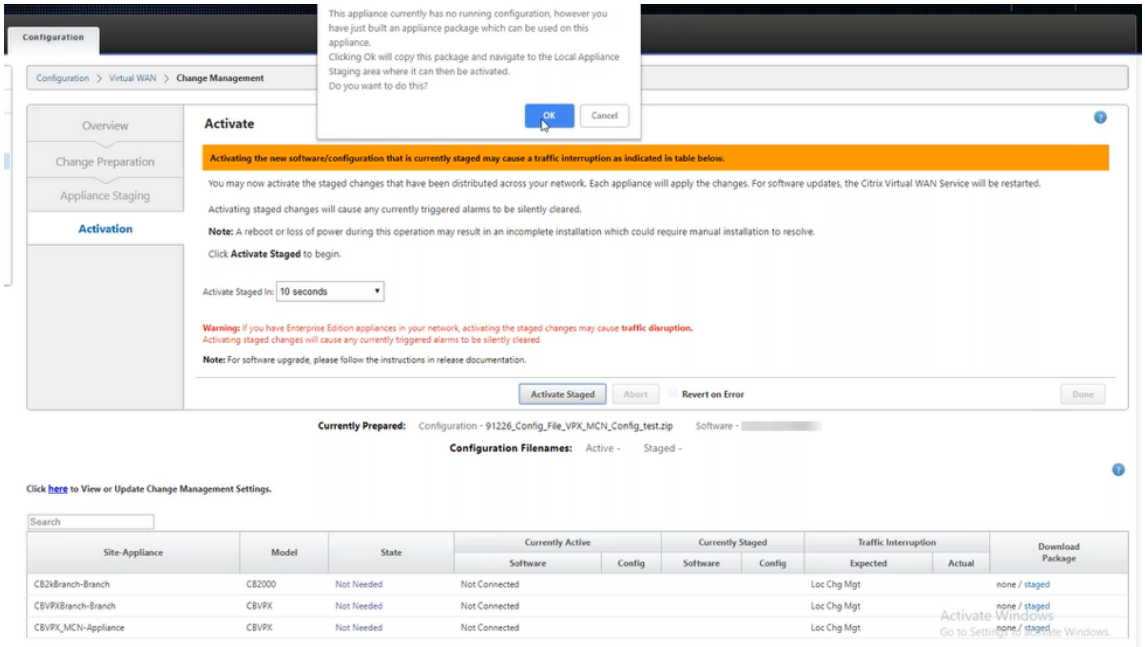


7. Once the transfer progress is 100% complete, click **Next** to proceed to activation.

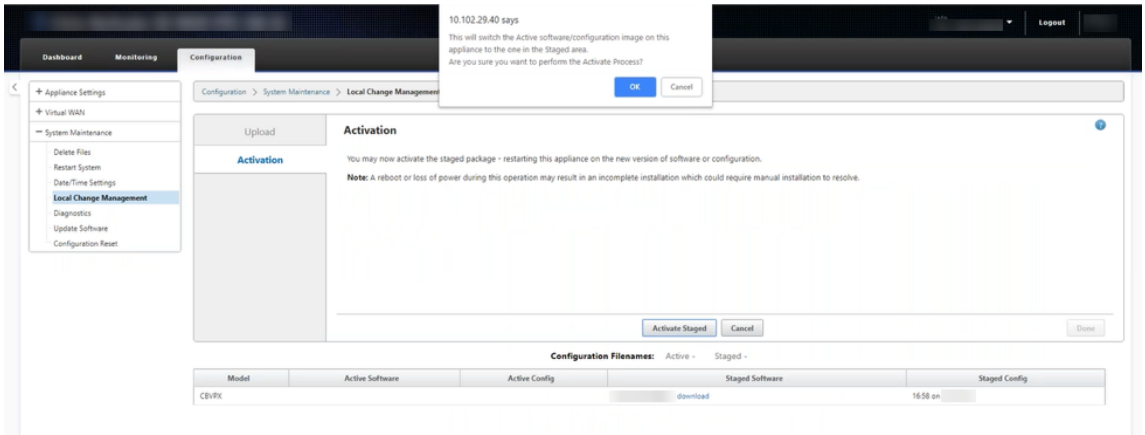


8. Click **Activate Staged**. A user acceptance pop-up message appears as this is the first time the appliance is being staged.

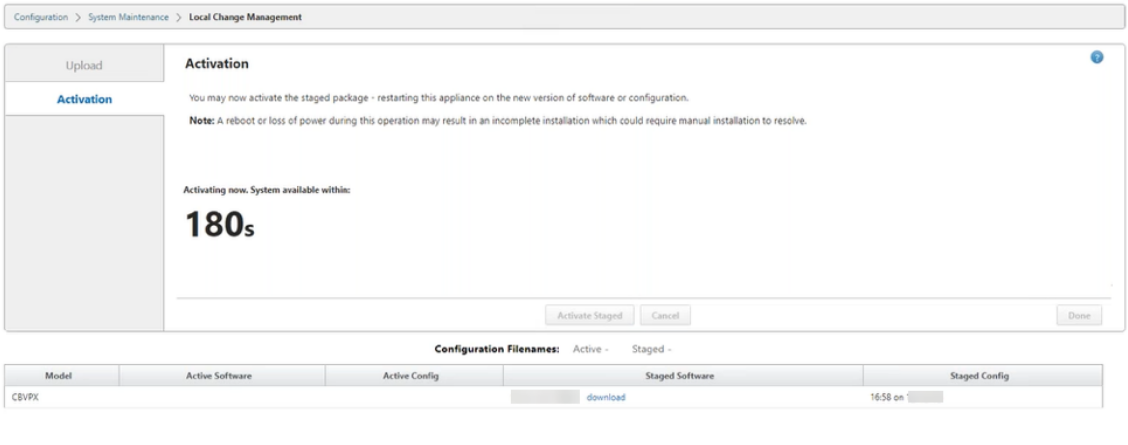
   You are redirected to the **Local Change Management** page for activating the local appliance. Click **OK** to proceed.



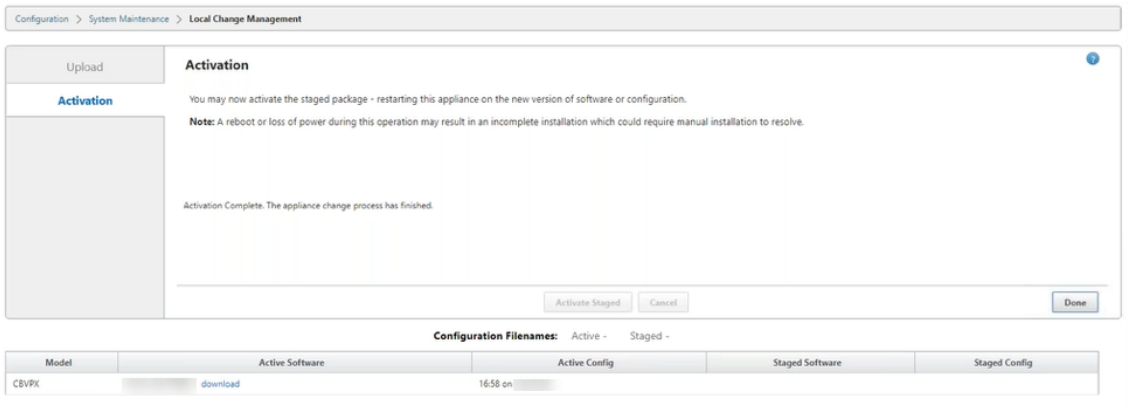
9. Click **Activate Staged** in Local Change Management. An activation confirmation message appears. Click **OK**.



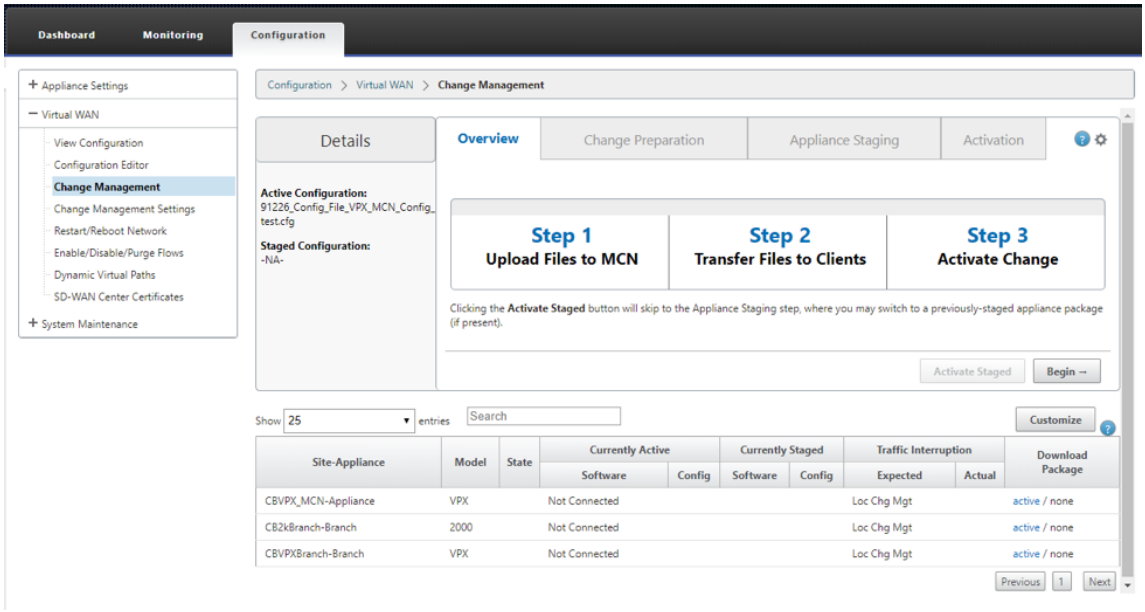
Activation starts with a countdown timer of 180 seconds.



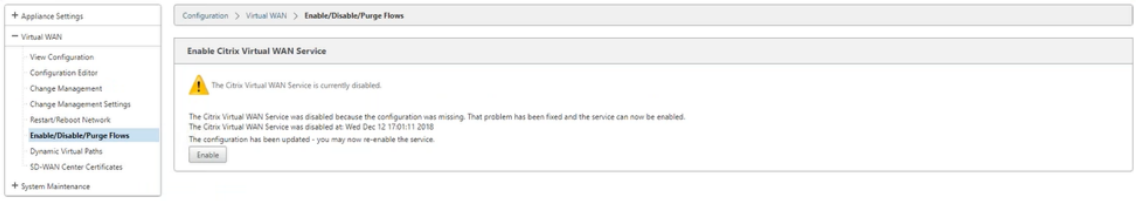
10. After the countdown, a message indicates that activation is completed. Click **Done**, the appliance restarts.



11. After the appliance restarts, navigate to **Change Management** page to download the local change management packages for the respective branches that you need to bootstrap to the network with Virtual WAN software upgrade only.



12. Enable SD-WAN service on the appliance. Navigate to **Virtual WAN > Enable/Disable/Purge Flows** and click **Enable**.



To further configure and add new sites to the network, folow the procedure in Configure branch node topic.

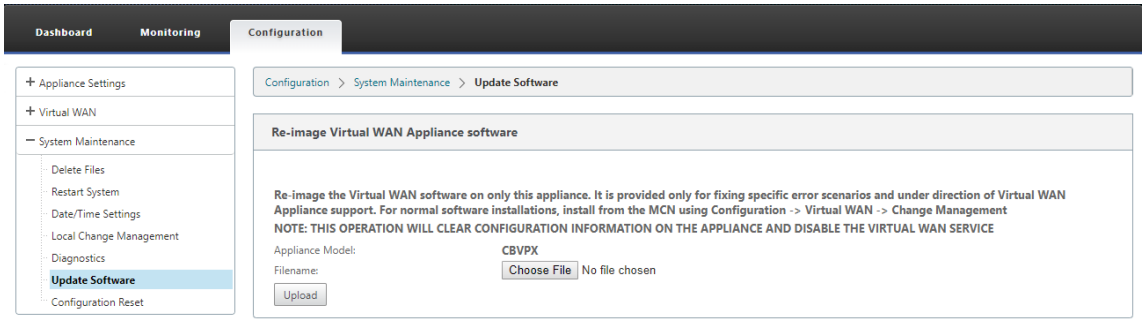
Reimage Citrix SD-WAN appliance software

March 12, 2021

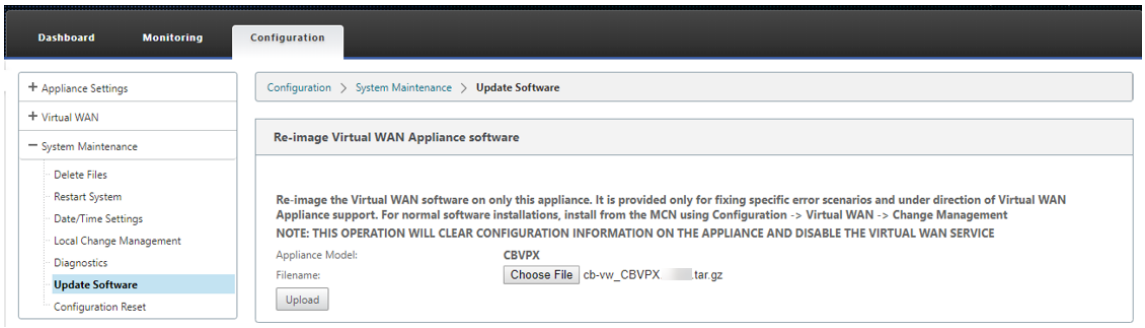
Download the *.tar.gz* file of the required Citrix SD-WAN software version and platform from the Citrix Downloads portal.

To reimage Citrix SD-WAN appliance software:

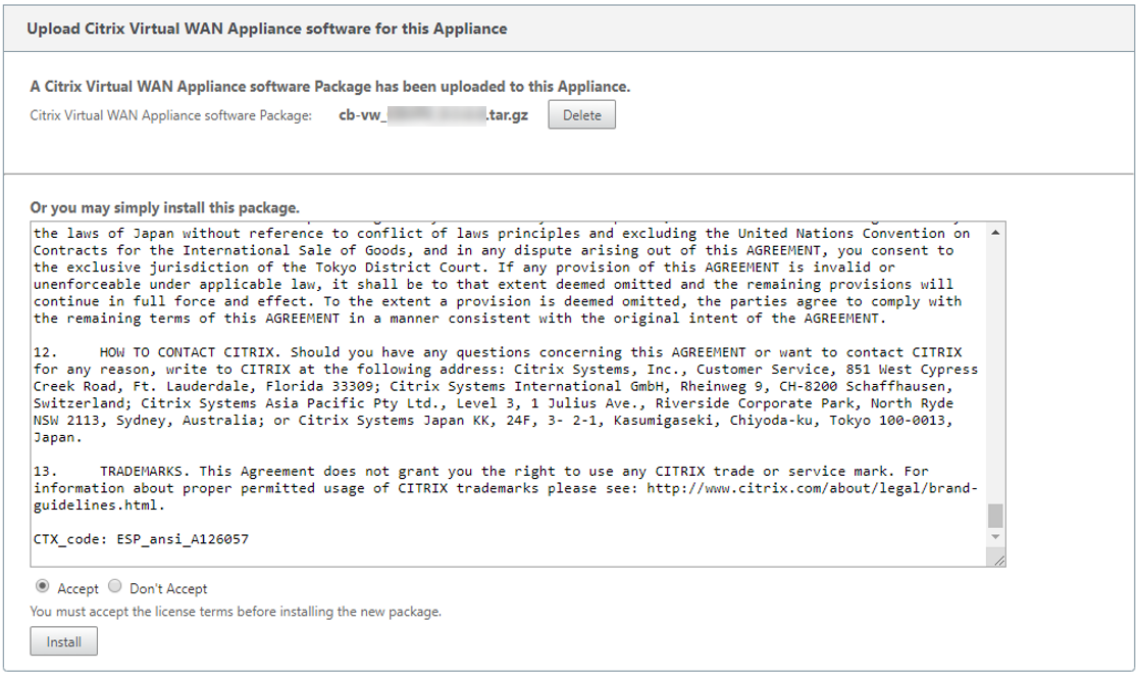
1. In the SD-WAN appliance GUI, navigate to **Configuration** > **System Maintenance** > **Update Software**.



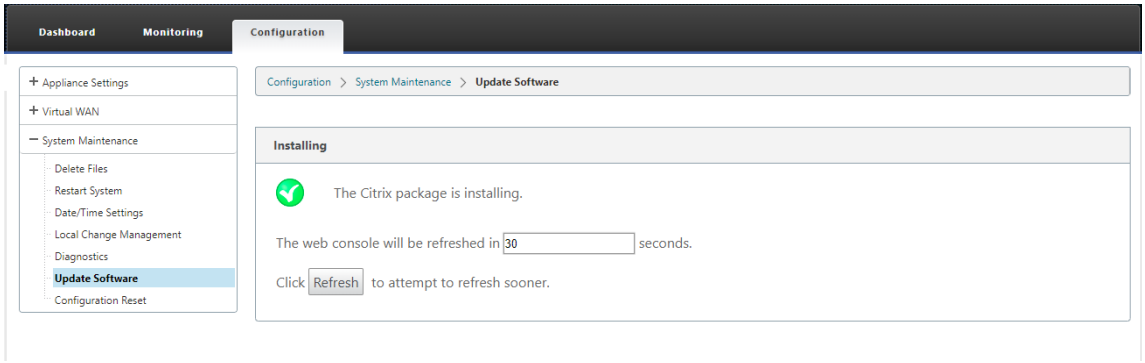
2. Click **Choose File** and select the downloaded Citrix SD-WAN appliance software. Click **Upload**.



3. Read and accept the license terms. Click **Accept** and then click **Install**.



The software update takes around 35 seconds, after which the appliance reboots.



Partial software upgrade using local change management

March 12, 2021

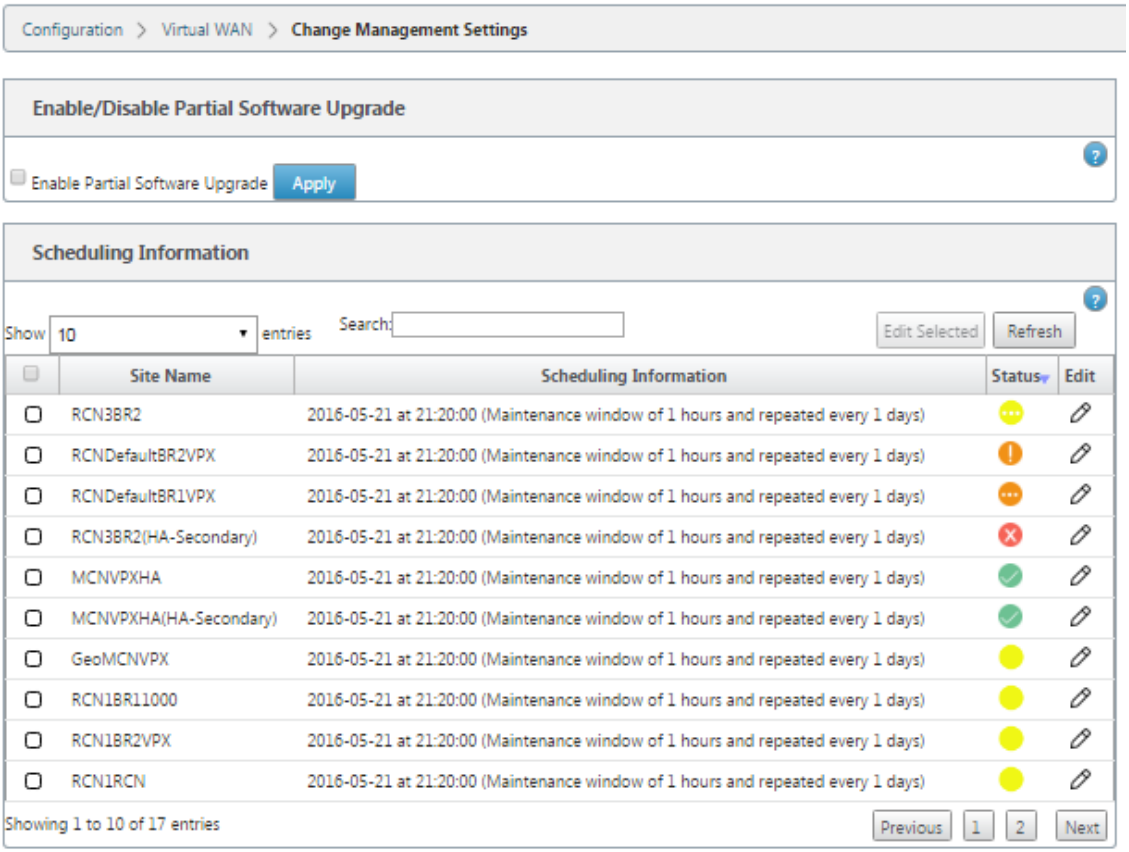
> **Important**
>
> By default, the **Partial Software Upgrade** option is disabled.

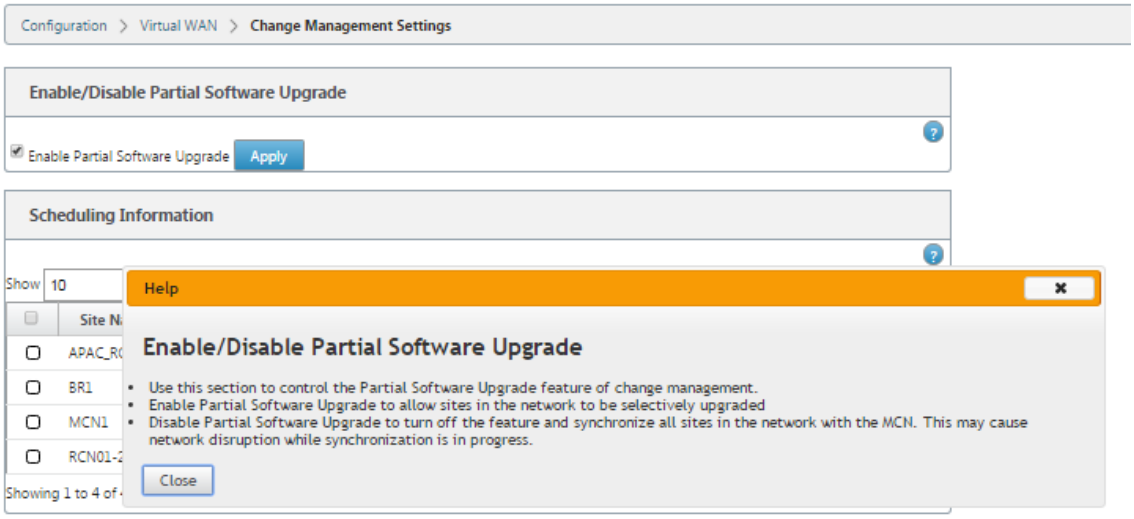
You can install a newer SD-WAN software release version on a subset of client sites using the **Local Change Management** option. This is achieved through the partial software upgrade feature which allows the network administrator to selectively upgrade the software on sites in the network without needing 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.





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.

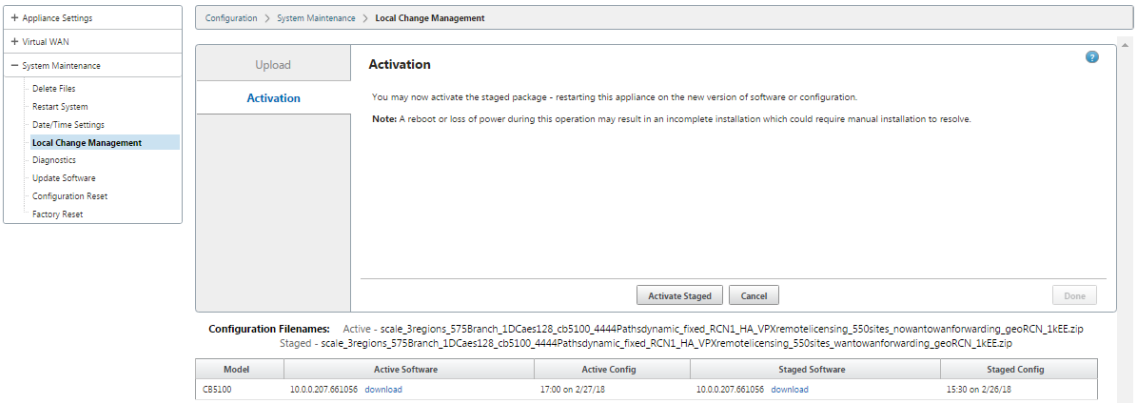
For the configuration of the Active and Partial site, software must be identical on the MCN and Branch sites. It is not possible to have a different feature set enabled on partially upgraded sites. Proceed to individual sites to perform **Local Change Management**. See the instructions below for High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

Upgrade branch node without high availability mode

1. In the Citrix 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.



Upgrade 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.

Upgrade 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 Premium Edition Conversion with USB

March 12, 2021

> **Note**
>
> Only the SD-WAN 1000 and 2000 WANOP appliances can be converted to SD-WAN Premium Edition appliances.

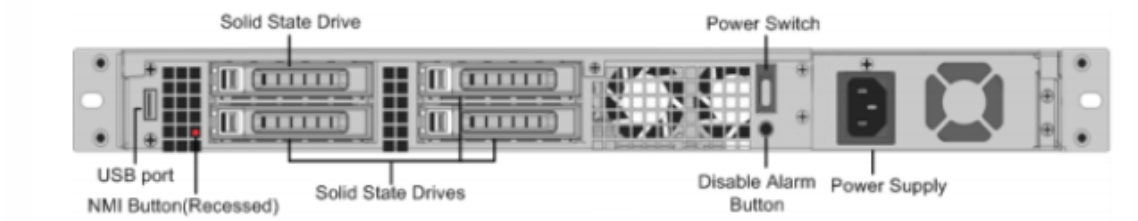
Before you begin

- 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 Premium (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.

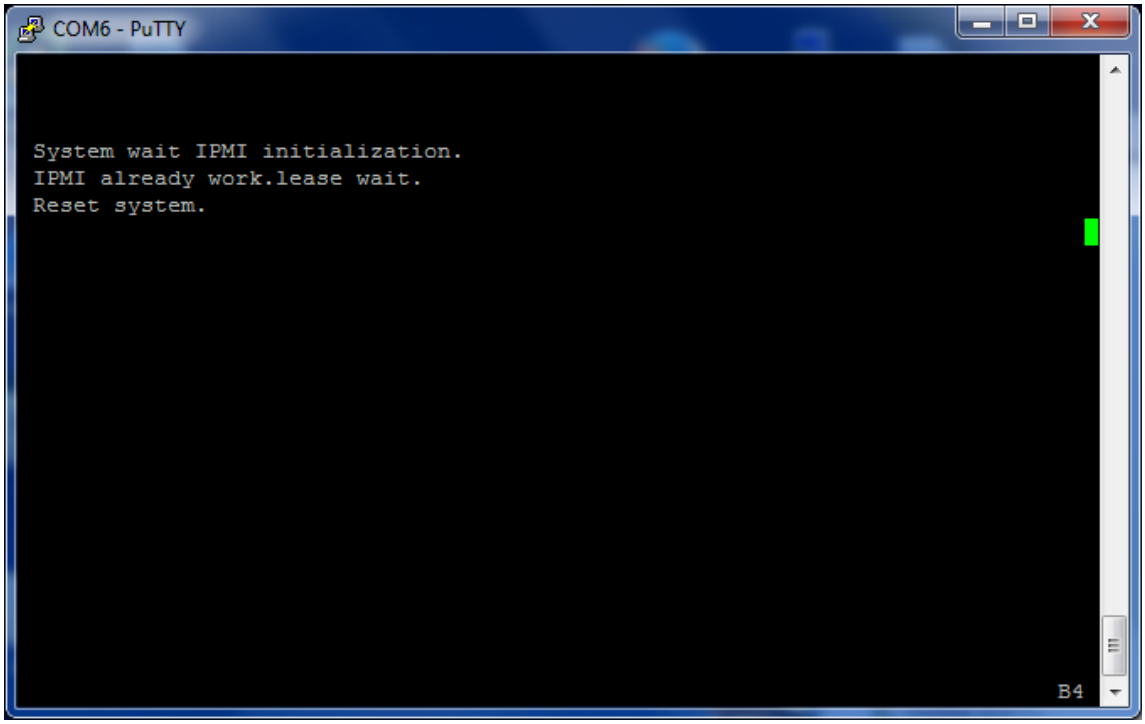


How to convert with USB stick

To upgrade the appliance with USB stick:

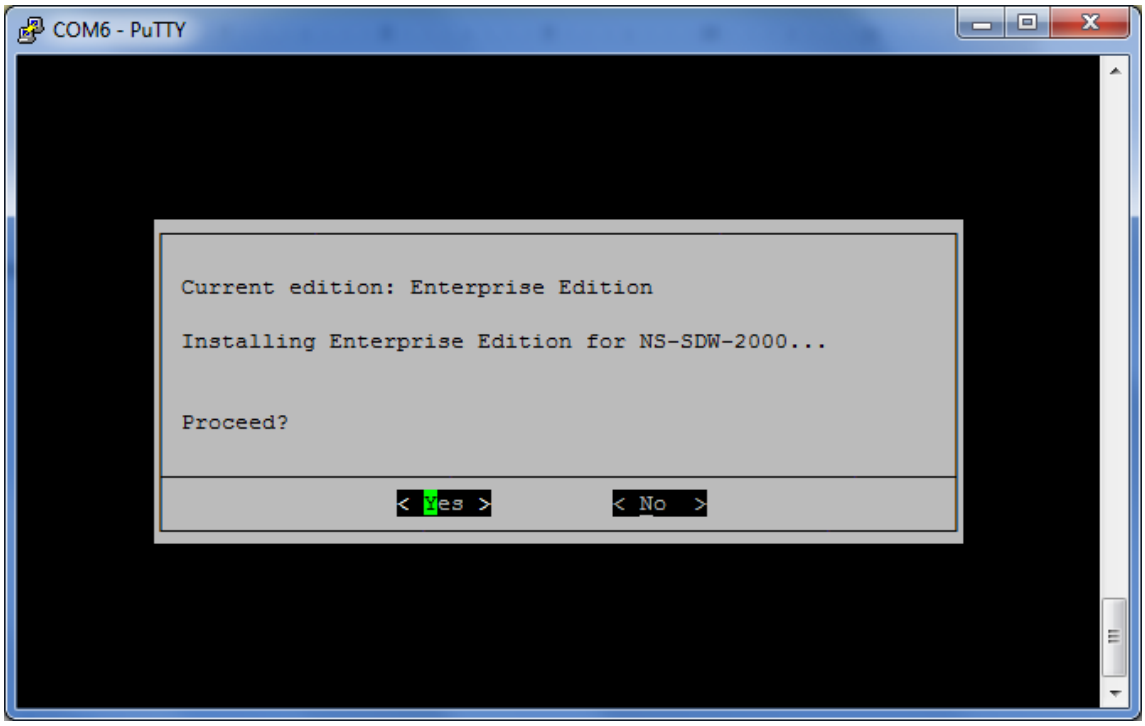
1. Insert the enclosed USB stick into the Citrix SD-WAN appliance.
2. Connect to the serial console of the appliance.
3. Reboot the appliance.
4. During the boot process, when you see the cursor moving across the screen, do the following:
   a) Press and hold the **ESC** key.
   b) Press and hold the **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.

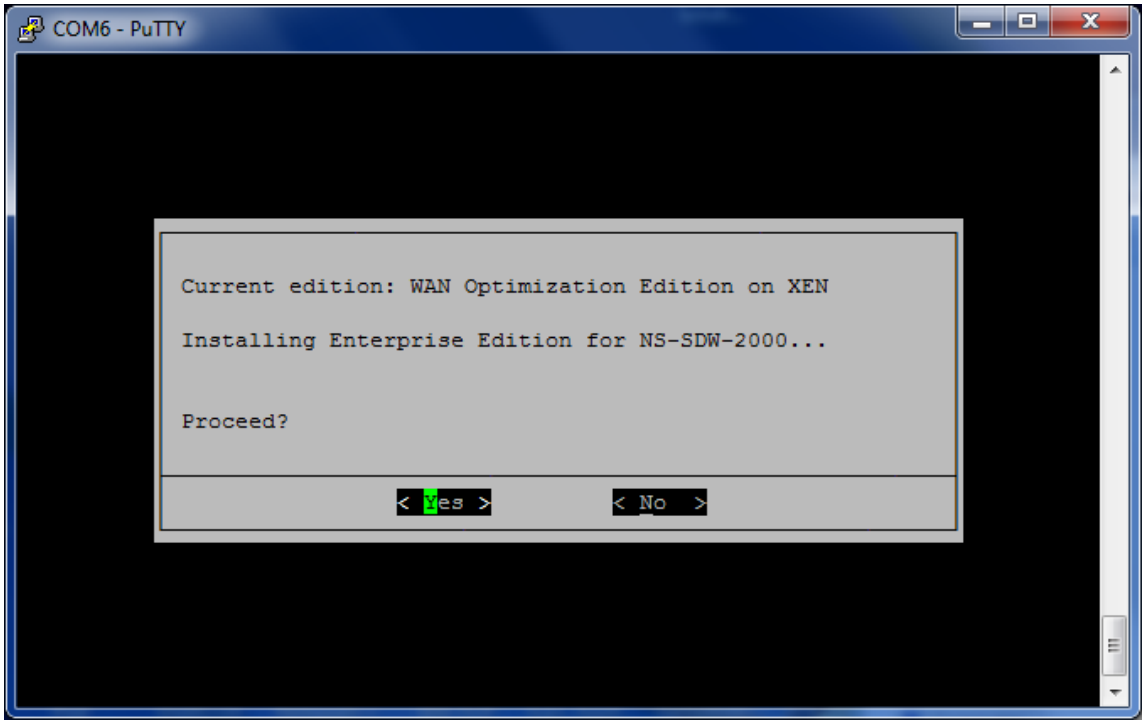
> **Note**
>
> The above steps should be executed during the appliance reboot process. The key strokes should happen during BIOS post stage as described in step 4.



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

Convert Standard Edition to Premium Edition

March 12, 2021

> **Important**
>
> In release version 10.1, the platform edition “Enterprise”is rebranded to the term “Premium.”

To perform platform conversion from Standard Edition to Premium (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** > **Reimage Virtual WAN Appliance software**.
4. Click **Choose File** to provide the *cb-vw_CB1000_x.x.x.x.tar.gz* file. Where x.x.x.x is the SD-WAN software release version.
5. Click **Upload**. Select **Accept** and click **Install** to proceed.
6. Install the Premium (Enterprise) Edition License.
7. Perform **Local Change Management** on the appliance using the downloaded active package in step 2 above.

The following are the conditions for WAN Optimization provisioning:

1. If the site role is MCN, WAN Optimization provisioning happens only:
   - Software Upgrade is done using .zip package (SSUP)
   - License is PE
   - Virtual WAN Service is enabled
2. If the site role is Client, WAN Optimization provisioning happens only:
   - Software Upgrade is done using .zip package (SSUP)
   - Virtual WAN Service is enabled
   - License is PE
   - Virtual Path is formed with MCN
3. For immediate provisioning of WAN Optimization, set the maintenance window value to 0 from the Change management settings page for the corresponding site.

USB reimage utility

March 12, 2021

The SD-WAN USB reimage utility allows repurposing of hardware by installing a clean factory image from a bootable USB stick. Citrix provides a USB stick Field Replaceable Unit (FRU) with a preloaded SD-WAN software image. Use the USB FRU to reimage the appliance to the required supported editions (SE/PE/AE). The appliance license/ configuration used determines the appliance edition.

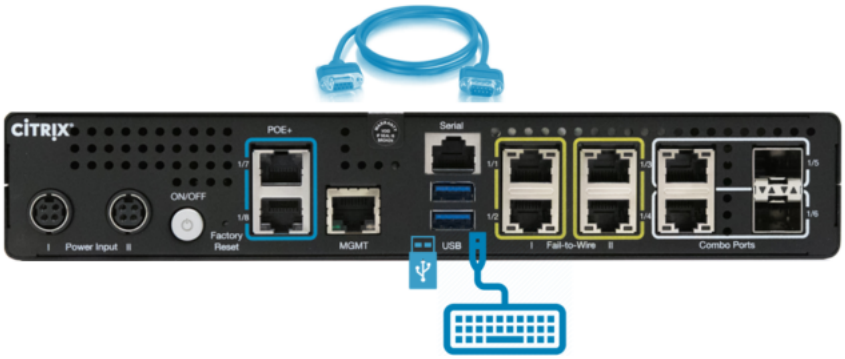
The following table provides details on the available USB FRU images and the editions supported by SD-WAN appliances.

Appliance	USB FRU image	Supported Editions
Citrix SD-WAN 110	11.1.1.39	SE
Citrix SD-WAN 210	10.2.7.17	SE, AE
Citrix SD-WAN 410	10.2.3.32	SE
Citrix SD-WAN 1100	10.2.7.17	SE, PE, AE
Citrix SD-WAN 2100	10.2.7.17	SE, PE
Citrix SD-WAN 4100	10.2.7.17	SE
Citrix SD-WAN 5100	10.2.7.17	SE, PE
Citrix SD-WAN 6100	10.2.7.17	SE, PE

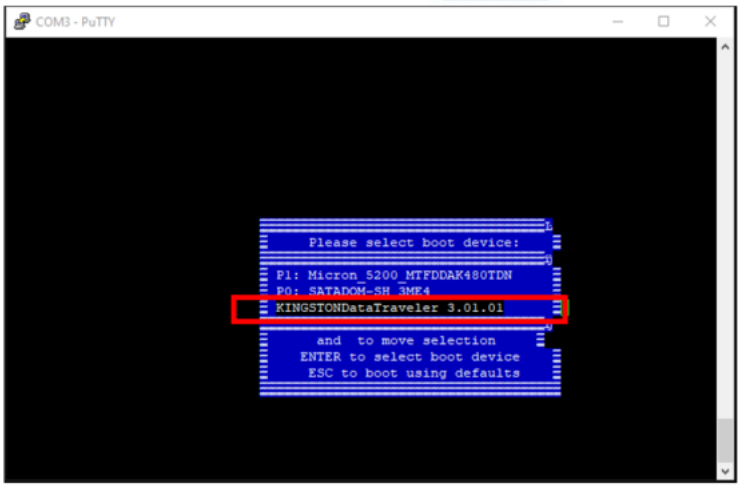
To perform a USB reimage:

1. Insert the USB stick provided by Citrix into one of the USB ports of the appliance.
2. Connect a USB Keyboard to another USB port.

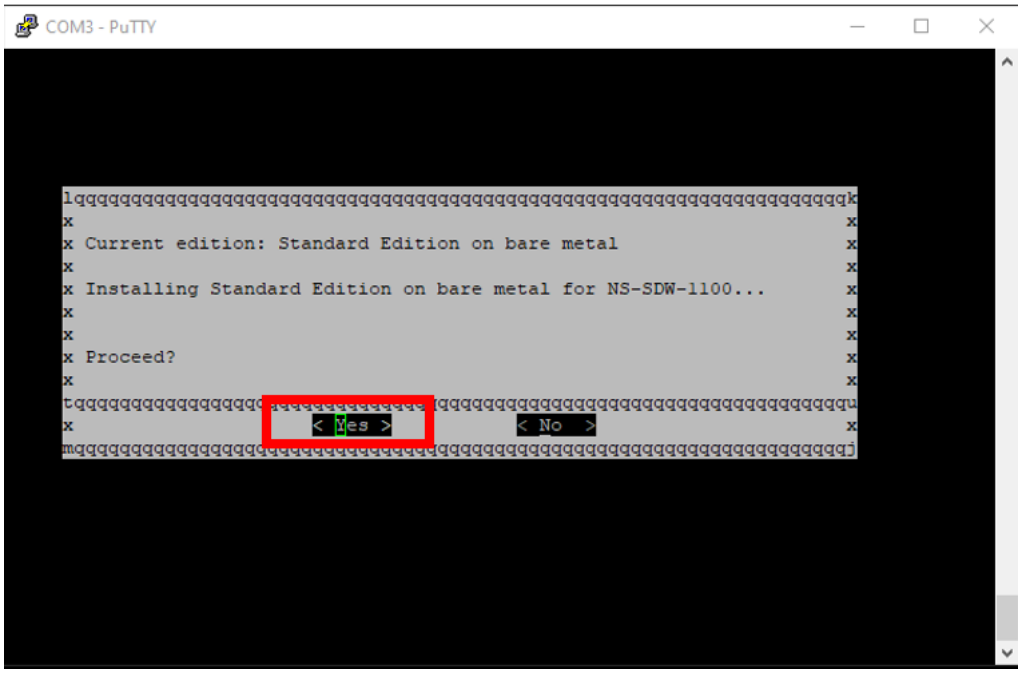
> **Tip**
>
> If there is a single USB port on the appliance, use a USB splitter to connect both the USB stick and the USB keyboard.



3. Log into the serial console as an administrator and issue the reboot appliance command through the CLI.
4. On boot up continuously press the **F11** key on the USB connected keyboard or **SHFT+ESC+1** via serial console connection.
5. Select the USB drive from the boot device menu and press Enter.



6. Depending on the Edition supported for the platform a screen appears requesting permission to proceed with the installation. Select **Yes**.



> **Note**
>
> For PE and AE reimage, the appliance may appear in the GUI as Standard Edition until the appropriate OS and PE/AE license installation is done.

The installation takes 30 minutes to complete. Do not power off the appliance during the reimaging process. It may reboot several times.

7. The factory image has DHCP enabled by default. The default management IP address on all platforms is 192.168.100.1. Use it to access the SD-WAN GUI.

You can also manually configure the management IP from the serial console by issuing the following commands:

Issue command '*management_ip*'

Issue command '*set interface 192.168.100.1 255.255.255.0 192.168.100.254*'

Issue command '*apply*'

8. The software, by default, is upgrade to SE. Install the PE, or AE license as required depending on the editions supported by the appliance.

> **Note**
>
> You can configure and manage AE capabilities through the SD-WAN Orchestrator only. For more information see, Edge security.

Citrix SD-WAN license options

March 12, 2021

There are four Citrix SD-WAN Editions each with a different set or subset of SD-WAN features. The type of license you install determines the platform edition - Standard Edition, WANOP Edition, Premium Edition, and Advanced 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.

Citrix SD-WAN platform software support

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

> **Note**
>
> In release version 10.2, the Enterprise platform edition is rebranded to **Premium** edition.

Version	WAN Optimization Edition	Standard Edition	Premium Edition	Advanced Edition
Release 7.x	Yes	No	No	No
Release 8.x	No	Yes	No	No
Release 9.0, 9.1, 9.2, 9.3	Yes	Yes	Yes	No
Release 10.0, 10.1, 10.2	Yes	Yes	Yes	No
Release 11.0, 11.1	Yes	Yes	Yes	No
Release 11.2	Yes	Yes	Yes	Yes

To view all the appliance models supported in Citrix SD-WAN release 11.2, see Citrix SD-WAN Data Sheet.

Before you can download the software, you must obtain and register a Citrix SD-WAN software license. For instructions on obtaining an SD-WAN software license, contact Citrix 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 set up 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.

> **Note**
>
> As of Nov 4, 2020, there is a change to the "Citrix Licenses Return and Modify"process. With this new process, you cannot return or modify your licenses through the Manage Licenses portal on Citrix.com and the My Licensing Tools on Partner Central.
> For more information and list of use cases, see KB article CTX285157.

Local licensing

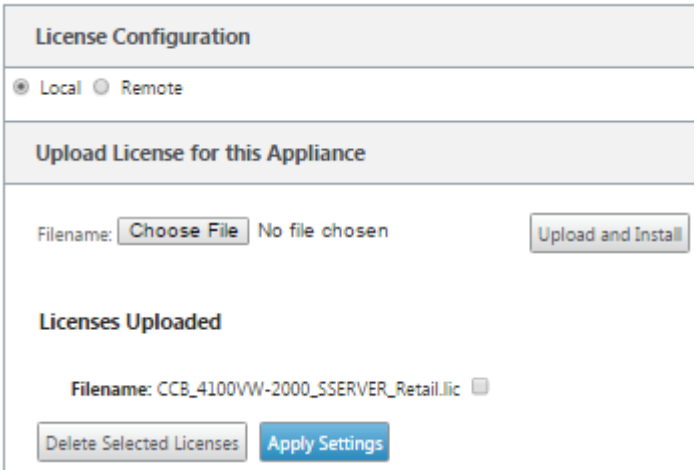
March 12, 2021

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 active network connection. 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**.



Remote licensing

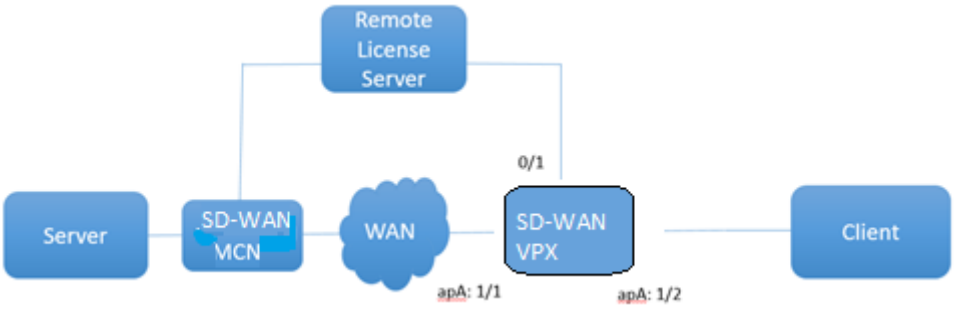
March 12, 2021

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

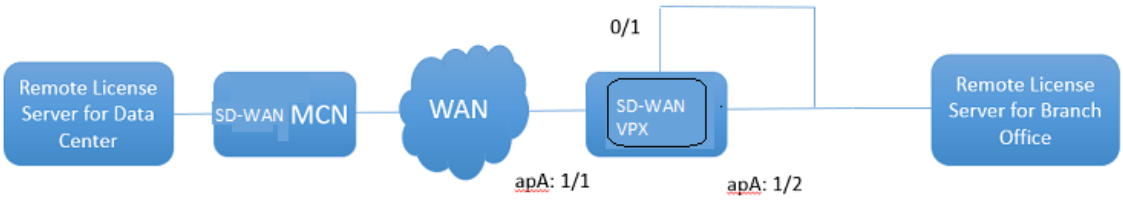
- NTP should be configured for both License server and SD-WAN (date and time should be in-sync)
- It is recommended that you use the latest License Server version:
  - Release 9.1, 9.2: 11.13.1 L.S
  - Release 10.0, 10.1, 10.2, 11.0, 11.0.1, 11.0.2: 11.14.1 L.S
  - Release 11.0.3, 11.1, 11.2: 11.16.3 L.S

Use Cases:

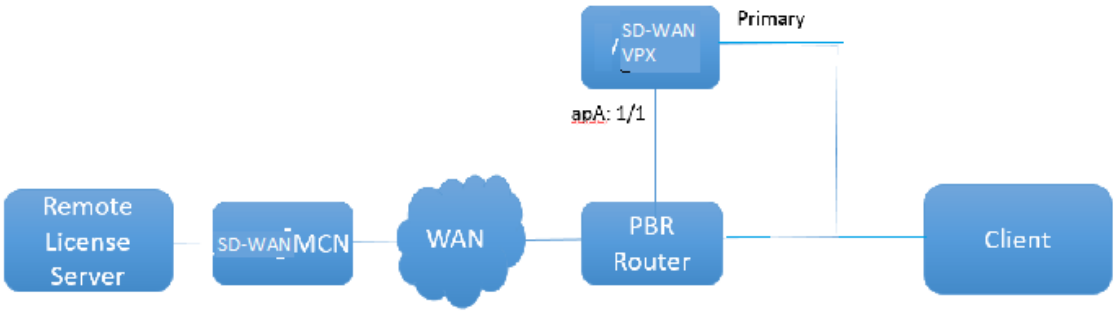
1. Remote license server reachable through the management network without using data/apA Ports.



2. Remote license server in the Branch network.

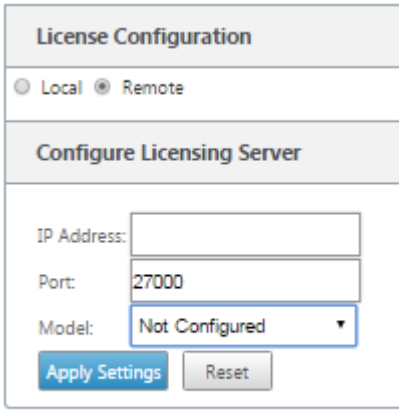


3. SD-WAN VPX-SE - PBR deployment in the Branch office.

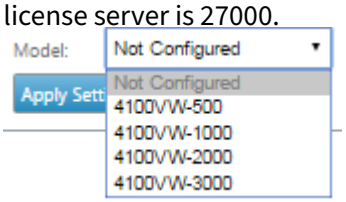


Remote license:

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.



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



> **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

March 12, 2021

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 log in to the appliance.

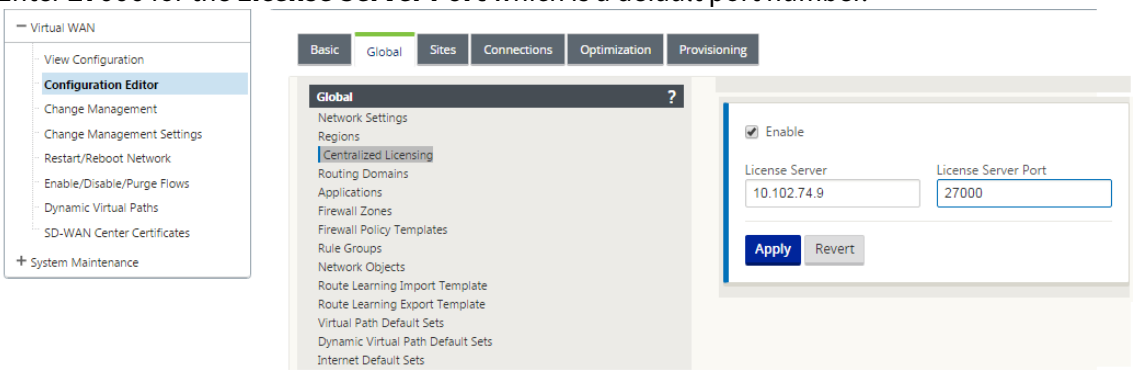
The SD-WAN center IP address is provided in the SD-WAN appliance GUI under **Global > Centralized licensing**. This IP address is propagated to individual appliances through the configuration packages

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.

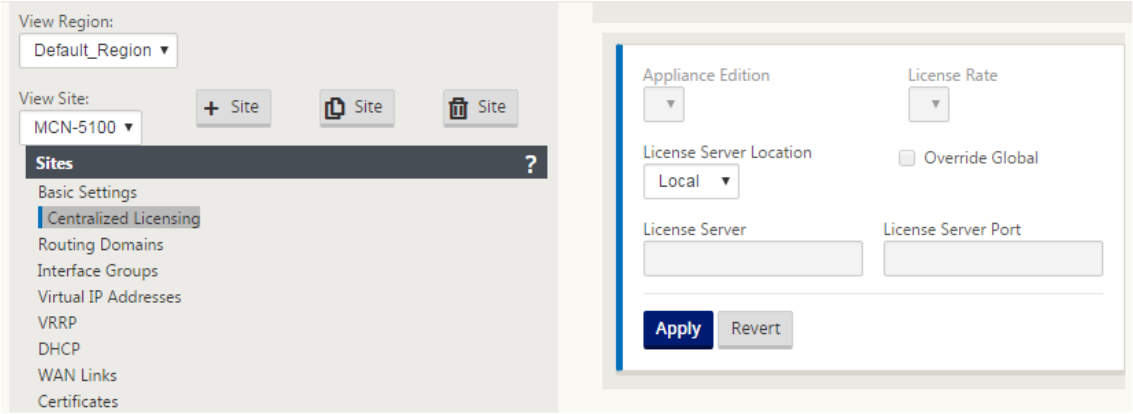
The license bandwidth can be selected with the appliance model for Site settings. The WAN links bandwidth is audited against the license selected.

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

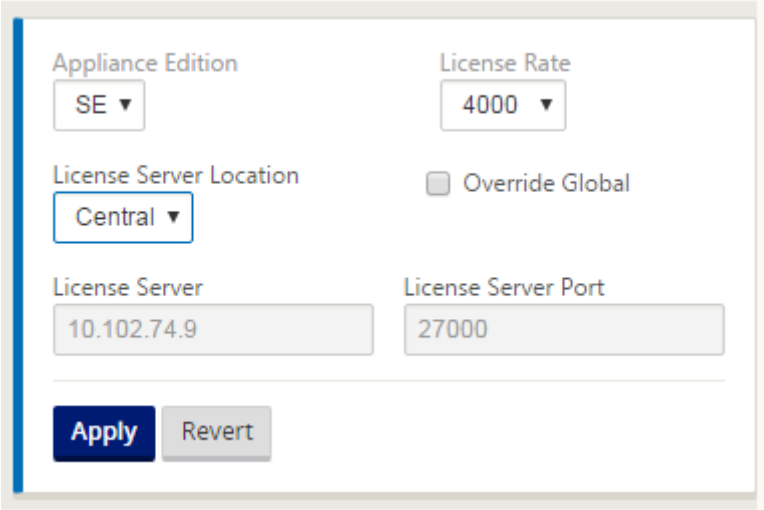
1. Navigate to **Configuration** > **Virtual WAN** > **Configuration Editor**. Open an existing virtual WAN configuration package or create configuration package. The configuration package opens.
2. Navigate to the **Global** tab. Select **Centralized Licensing**. Click **Enable**.
3. Enter the IP address for the License Server from which you can download and manage SD-WAN licenses. Provide the SD-WAN Center management IP address, so 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.



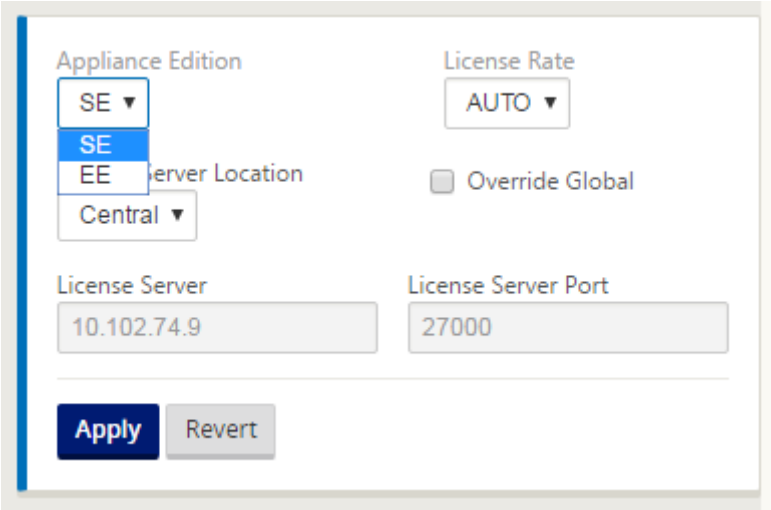
5. Click **Apply**.
6. Navigate to the **Sites** tab. Select MCN or Branch site under **View Site**, depending on the region and site for which you want to manage central licensing.
7. Select **Centralized Licensing**. The central licensing options view is displayed. By default, the **Local** option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

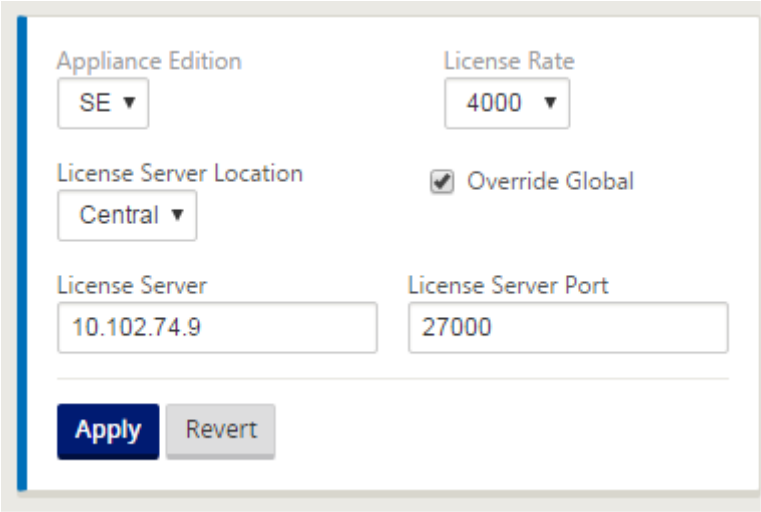


9. Choose the **Appliance Edition** and **License Rate** depending on the appliances to be installed. Click **Apply**.



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**.



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.

The 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.

License based on bandwidth allocation:

Each appliance can choose a license with bandwidth level greater than or equal to the configured bandwidth. If the configured bandwidth license is not available, the capability for an appliance to choose the next higher bandwidth license is added. This capability is valid for both the centralized and remote license server functionality. For example:

- If you have three 410–200 Mbps licenses. You would use the same licenses for all bandwidth allocations associated with 410 appliance. Site A (20 Mbps), Site B (50 Mbps), and Site C (200 Mbps) should all be able to use 410–200 Mbps licenses.
- If you have one each of 410-20 Mbps license and 410–200 Mbps license. Site A is configured to consume 50 Mbps, then Site A can use 410–200 Mbps license.

License grace period:

The grace period allowed is 30 days when the license file or license configuration is removed from the appliance. Grace alerts are supported for Syslog and emails.

> **Note**
>
> When the selected license rate does not match configured WAN link rate, the following message is displayed on the appliance GUI for licensing events.
>
> Message: The total configured permitted rate (LAN to WAN) NNNN (Kbps) must not exceed twice the License Rate which is NNNN (Kbps)

> Severity: WARNING
>
> Events: Syslog, Email

Managing licenses

March 12, 2021

Citrix 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 two 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 two heart beats, the SD-WAN center releases the license allocated to the site into the pool. The grace period is 30 days, so after loss of 2 heartbeats, the appliance goes into the grace period. During these 30 days, the communication has to be restored. Once restored, the appliance reverts to normal operational mode. If the communication is NOT restored, the appliance is 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 comes up with a 30-day grace period with or without ZTD functionality.
- The appliance is enabled 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 functions 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

March 12, 2021

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

March 12, 2021

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

The 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 Premium (Enterprise) Edition WAN Optimization features for your Virtual WAN. To do this, you will use the **Optimization** section forms in the **Configuration Editor** of the Web Management Interface on the MCN.

Initial Setup

March 12, 2021

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.

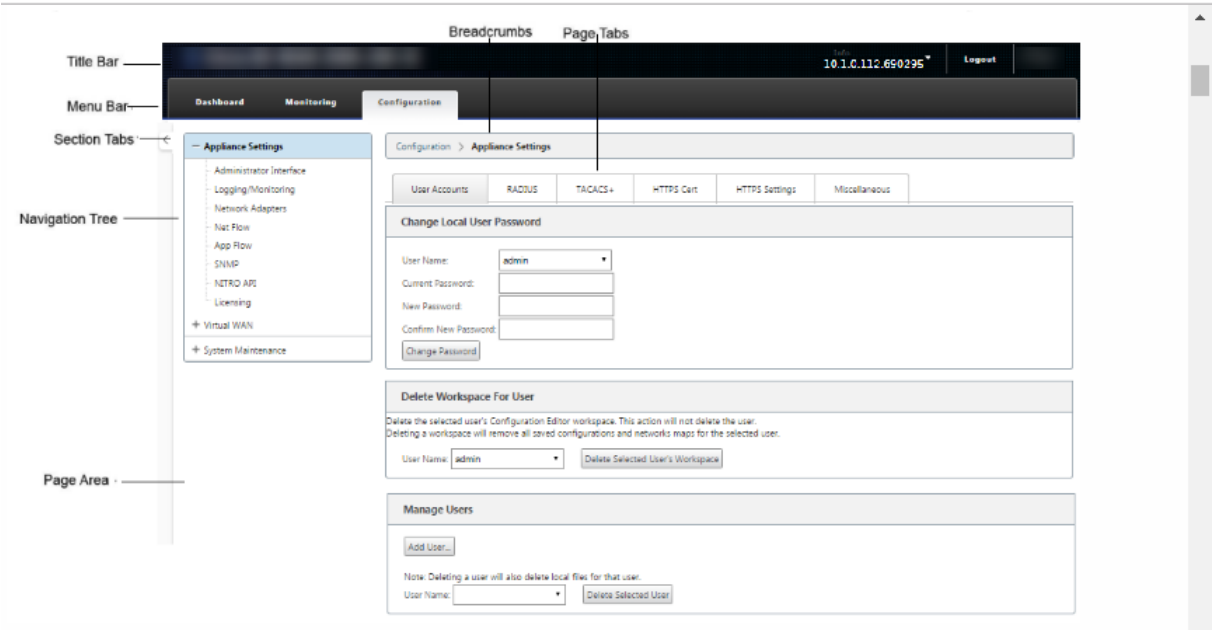
Overview of Web Interface (UI) Layout

March 12, 2021

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 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 more child pages for that topic or configuration form. These are located at the top of the page area, just below the breadcrumbs display. Sometimes (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 more fields in a table or form. Where this is the case, there is a gray, 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.

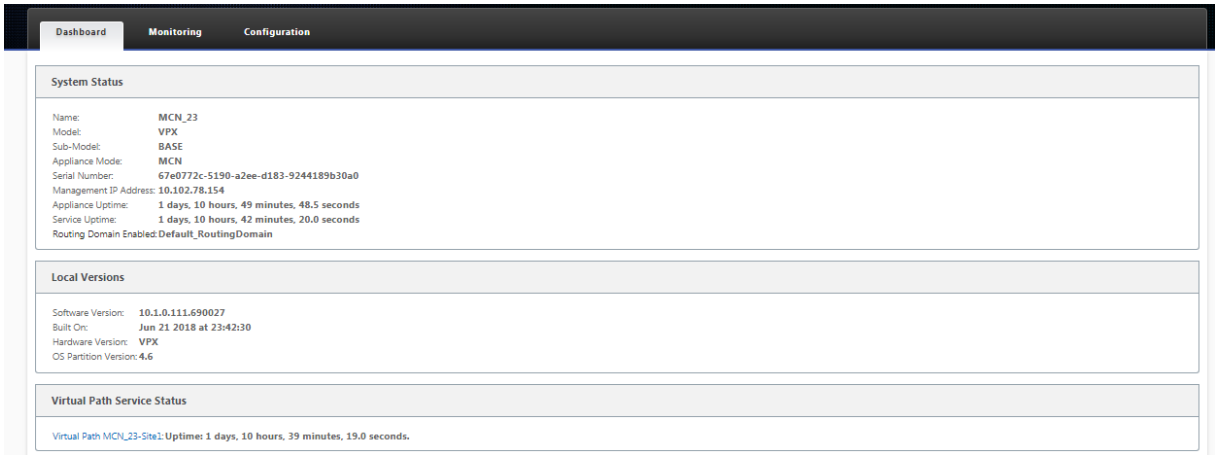
Web management interface dashboard

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

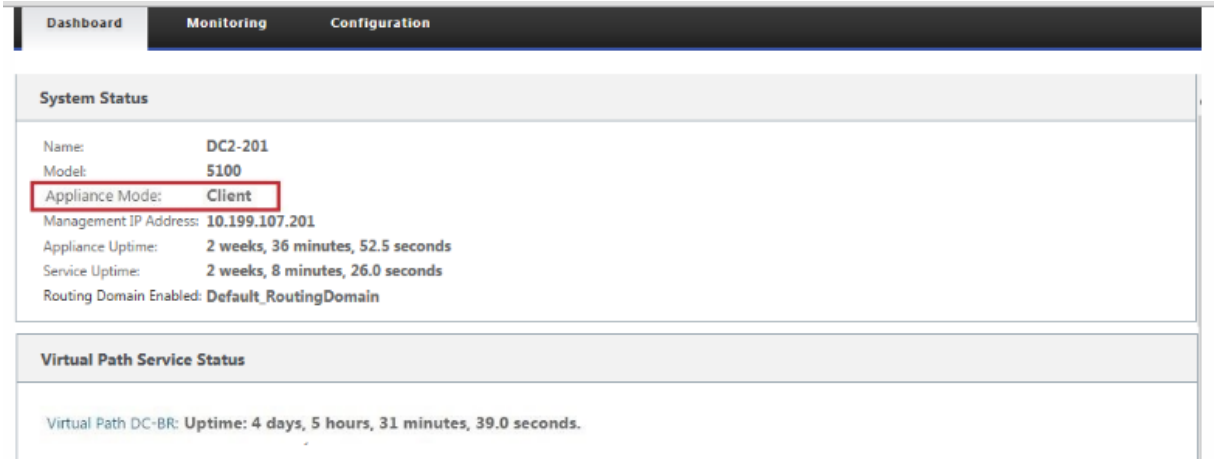
The **Dashboard** page displays the following basic information for the appliance:

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

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



The following figure shows a sample client appliance Dashboard display.



Configuration editor

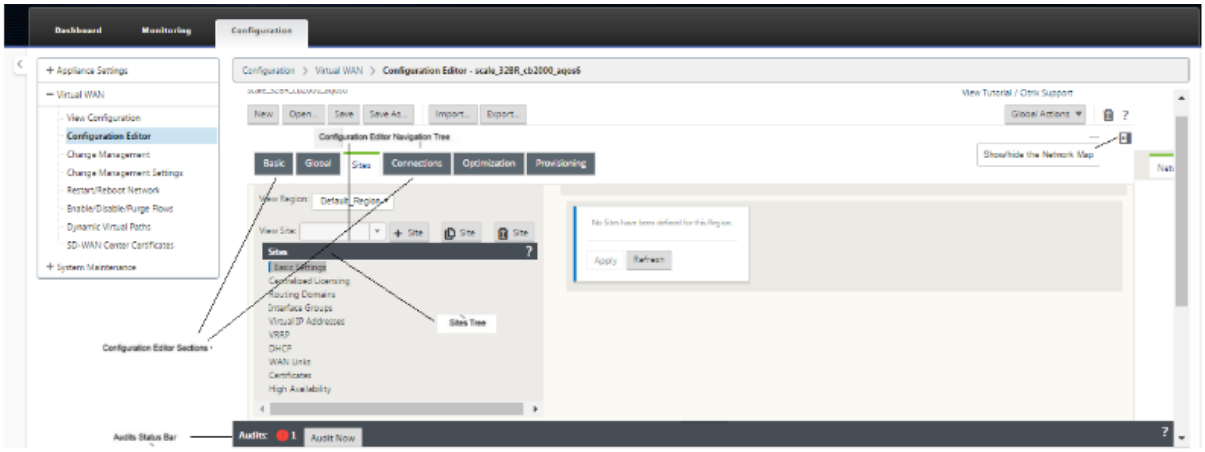
The Configuration editor enables you to add and configure Virtual WAN appliance sites, connections, optimization, and provisioning, and to create and define the Virtual WAN configuration.

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.1. Select the **Configuration** tab.1. In the navigation tree, click **+** next to the **Virtual WAN** branch in the tree. This displays the available pages for the **Virtual WAN** category.1. In the Virtual WAN branch of the tree, select **Configuration Editor**.

   The following 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 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 gray bars located in the left pane of the **Configuration Editor** page area. Each gray bar represents a top-level section. Click a section name to reveal the subbranches 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 subbranches of configuration categories and forms, which in turn can contain more 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 gray 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.

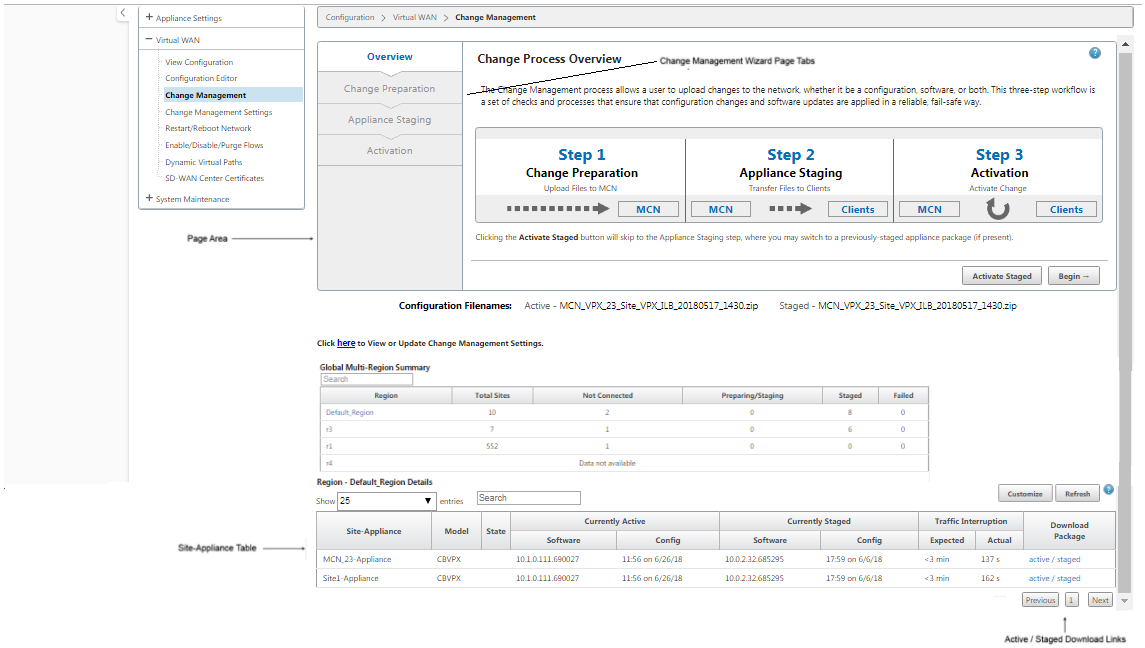
- **Local Change Management wizard** – **The Local Change Management** wizard is available in the Web Management Interface running on both the MCN and on all client node appliances. Use this to upload, stage, and activate the appropriate Virtual WAN appliance package on a local appliance to be added 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 following figure.



4. 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 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 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

March 12, 2021

To set up Citrix SD-WAN appliance hardware (physical appliance), do the following:

1. Set up the chassis.

   Citrix SD-WAN Appliances can be installed in a standard rack. For desktop installation, place the chassis on a flat surface. Ensure that there is a minimum of 2 inches of clearance at the sides and back of the appliance, for proper ventilation.

2. Connect the Power.

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

3. Connect the power.

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

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

   You 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, ensure 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.

SD-WAN VPX-SE Management Port

The 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 need to do so now, as outlined in the section, Configuring the Management IP Address for the SD-WAN VPX-SE.

The 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 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

March 12, 2021

To enable remote access to an 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 PC. 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 (Citrix 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 an 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 are using to set the appliance Management IP Address.

   You must 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 an SD-WAN appliance.
   >
   > Ignore any browser certificate warnings for the Management Web Interface.

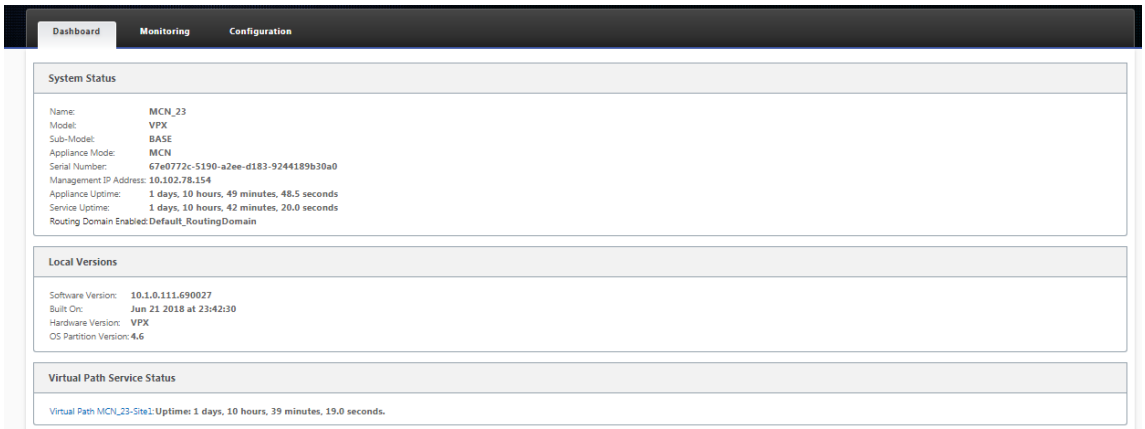
   This opens the SD-WAN management web interface login screen on the connected appliance.

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

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

   > **Note**
   >
   > It is 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.



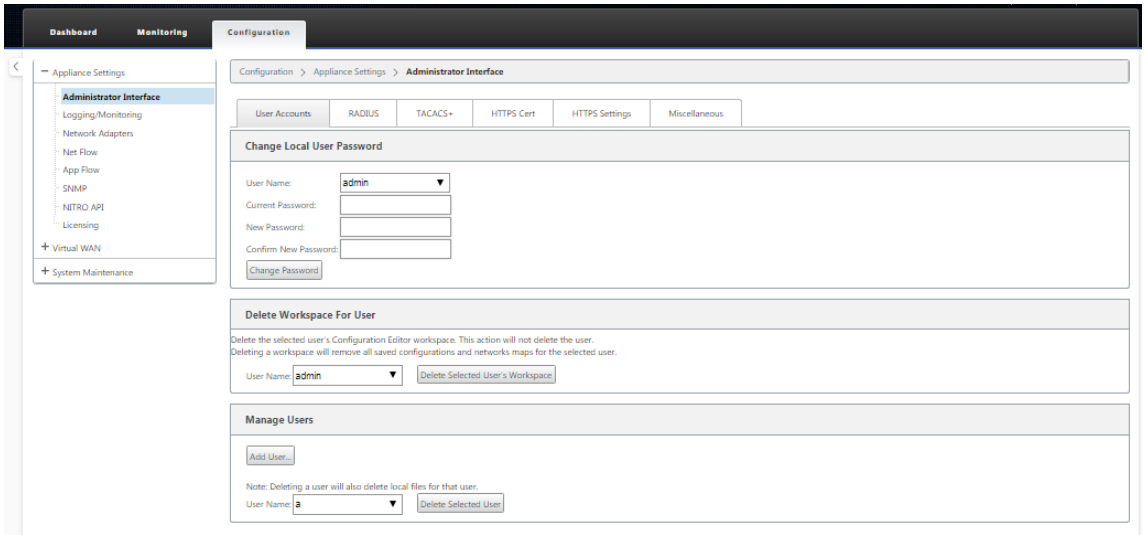
   The first time you log into the management web interface on an appliance, the **Dashboard** displays an Alert icon (goldenrod delta) and alert message indicating that the SD-WAN Service is disabled, and the license has not been installed. For now, you can ignore this alert. The alert will be resolved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

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

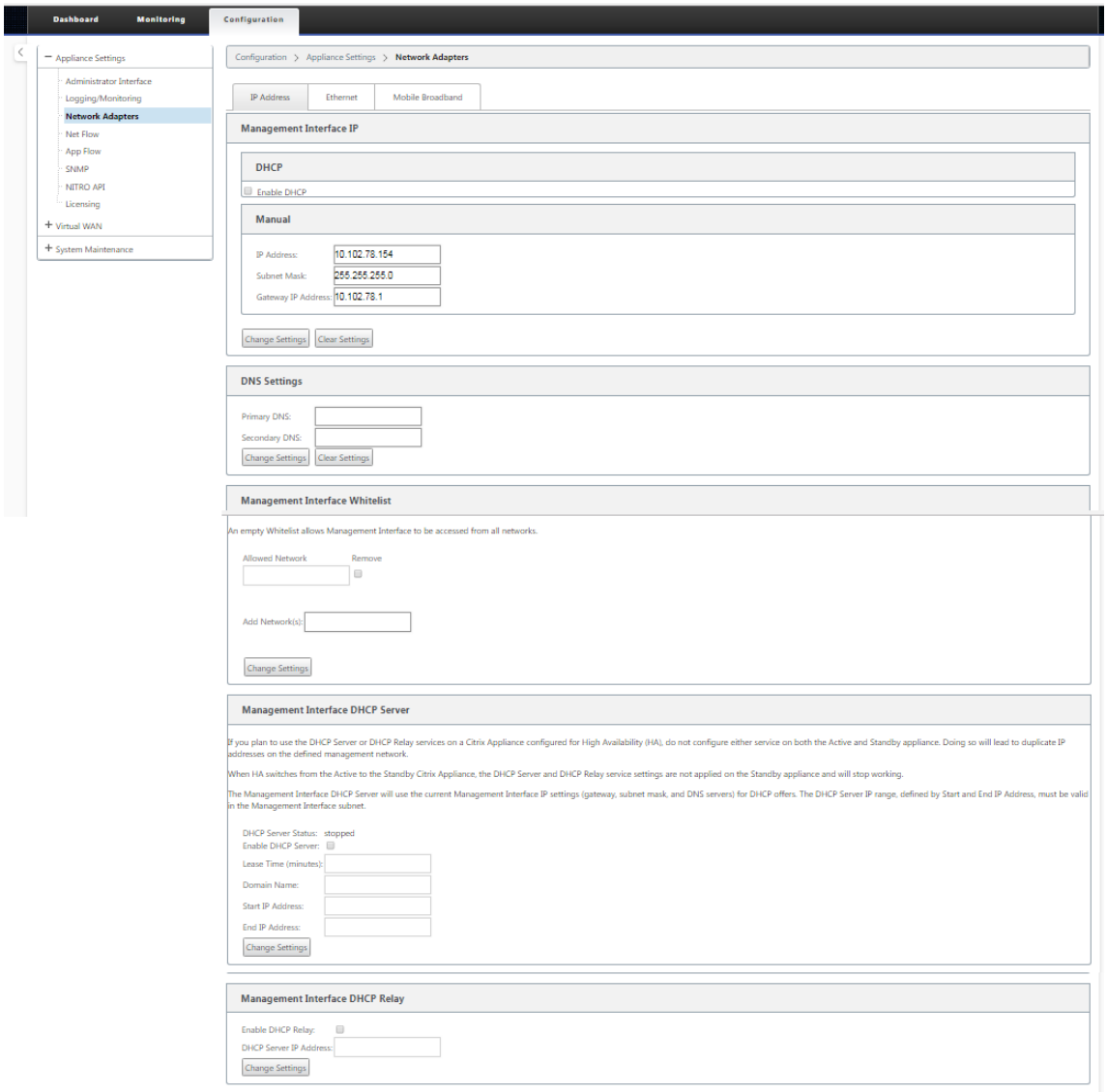
   This displays the **Configuration** navigation tree in the left pane of the screen. The **Configuration** navigation tree contains the following three primary branches:

- 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 Adapters**. This displays the **Network Adapters** 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 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 configured.

    > **Tip**
    >
    > After verifying the connection, do not log out of the management web interface. You are 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

March 12, 2021

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

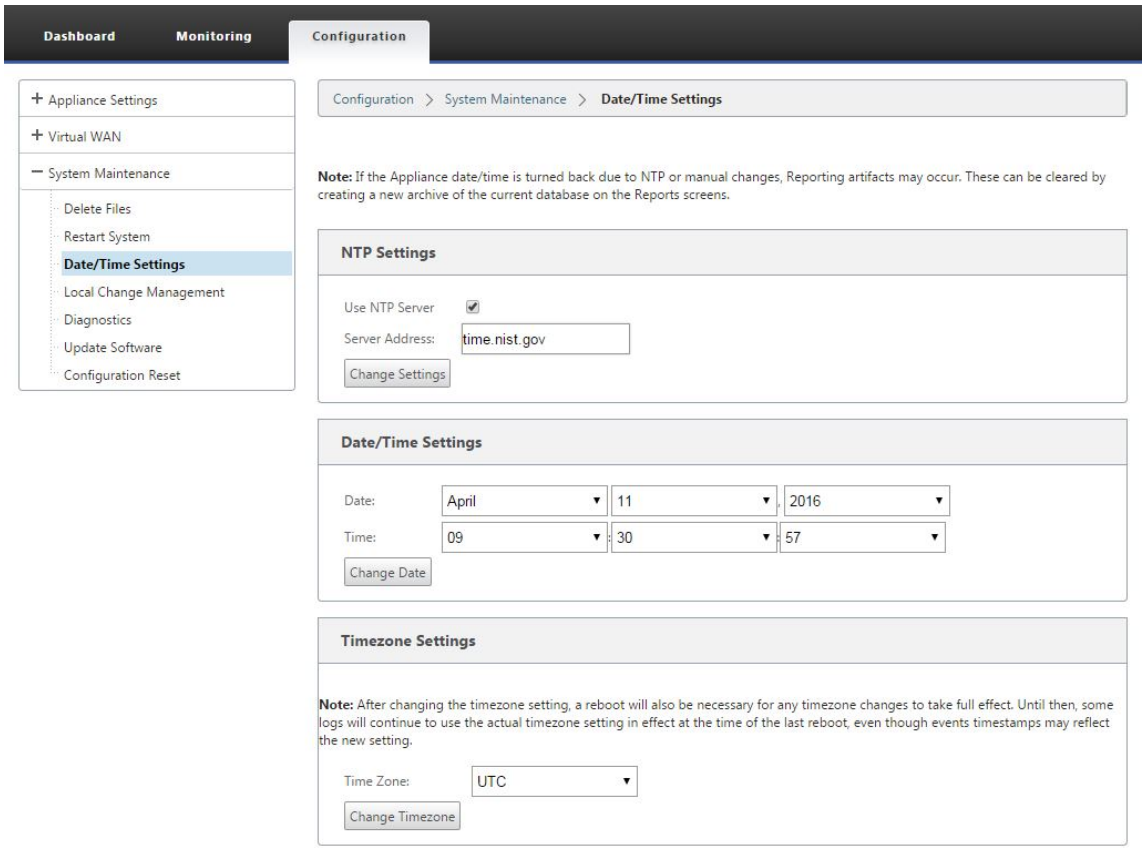
> **Note**
>
> You need to repeat this process for each appliance you want to add to your network.

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 following.



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

> **Note**
>
> If you have to change the time zone setting, you must do this before setting the date and time, or your settings do 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 are no longer 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 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 are lost. Log back into the system, and repeat the configuration procedure from the beginning.

Session timeout

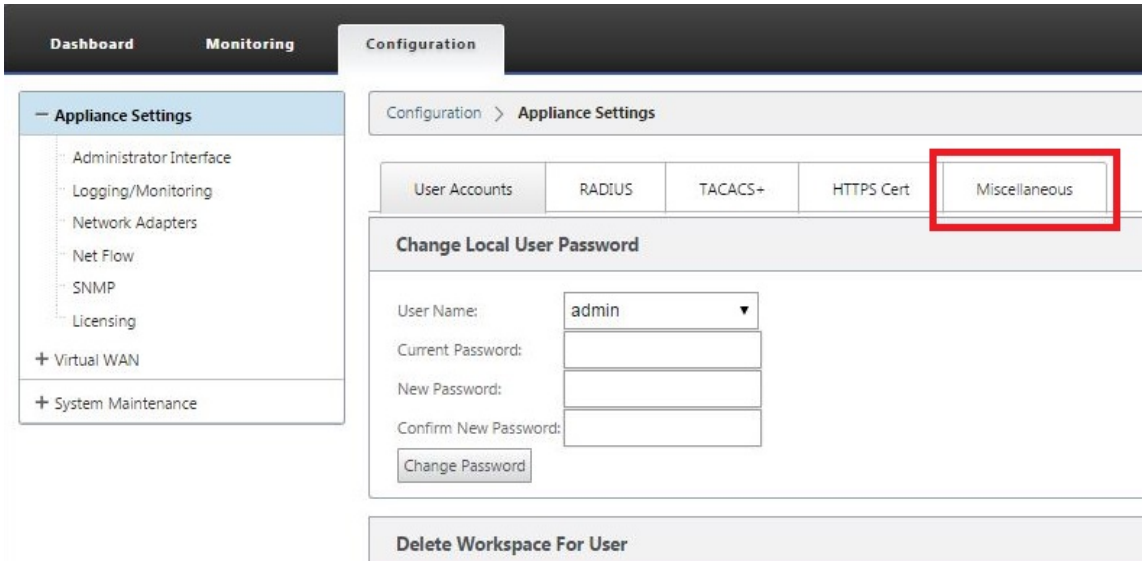
March 12, 2021

If your 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 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 9,999 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:

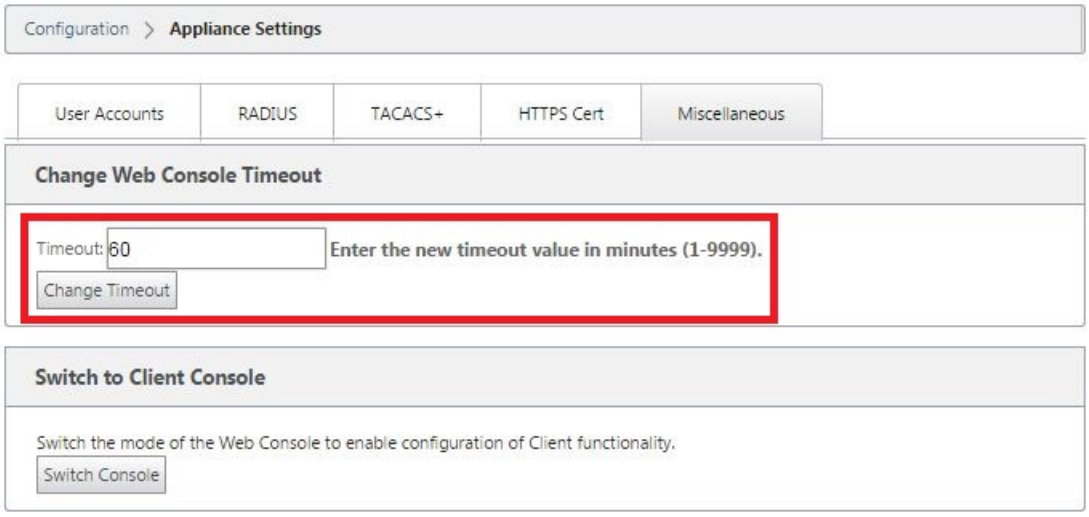
1. Select the **Configuration** tab, and then select the **Appliance Settings** branch in the navigation tree.

   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.



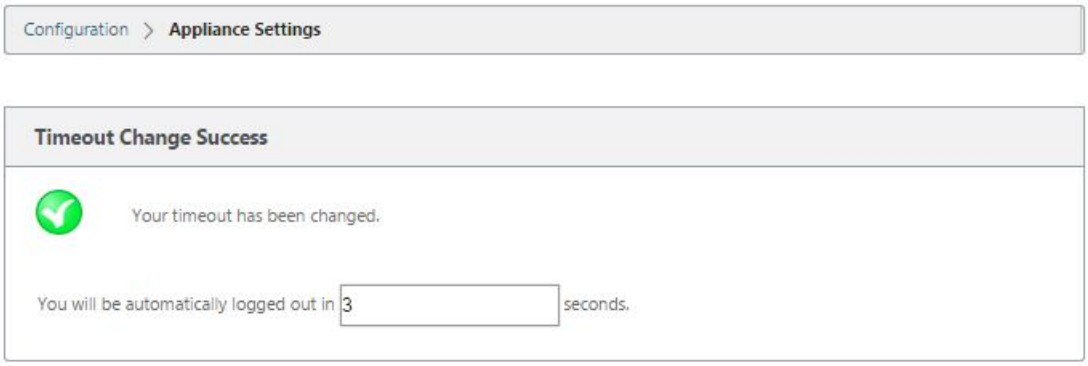
3. Enter the console **Timeout** value.

   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 much too brief for an initial configuration session.

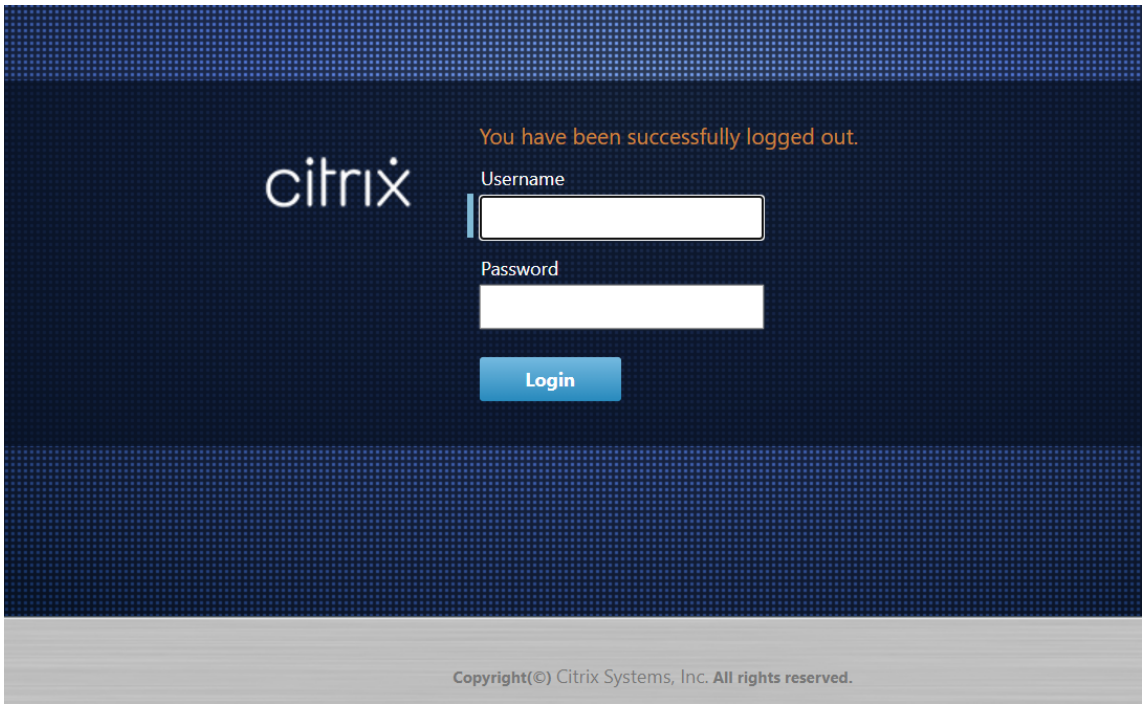
   > **Note**
   >
   > For security reasons, be sure to reset this value to a lower interval after completing the configuration and deployment.

4. Click **Change Timeout**.

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



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 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

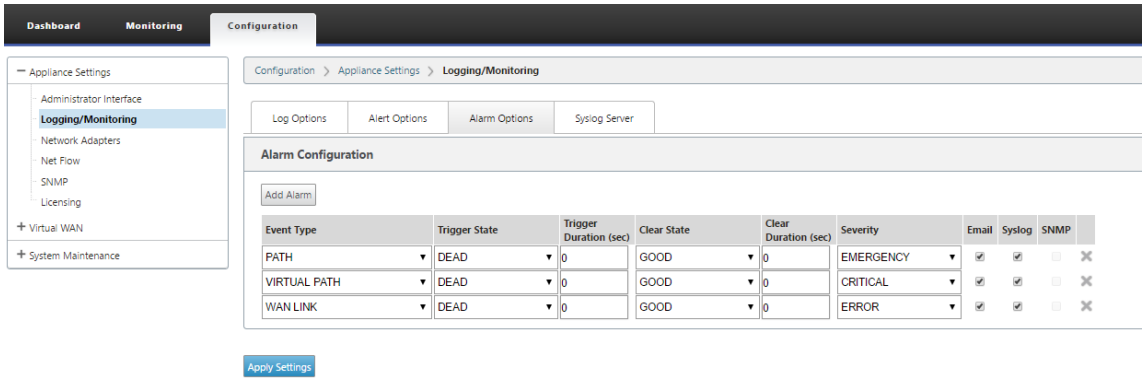
March 12, 2021

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.



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 more events occur on the same object within the Trigger Duration period. More 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.

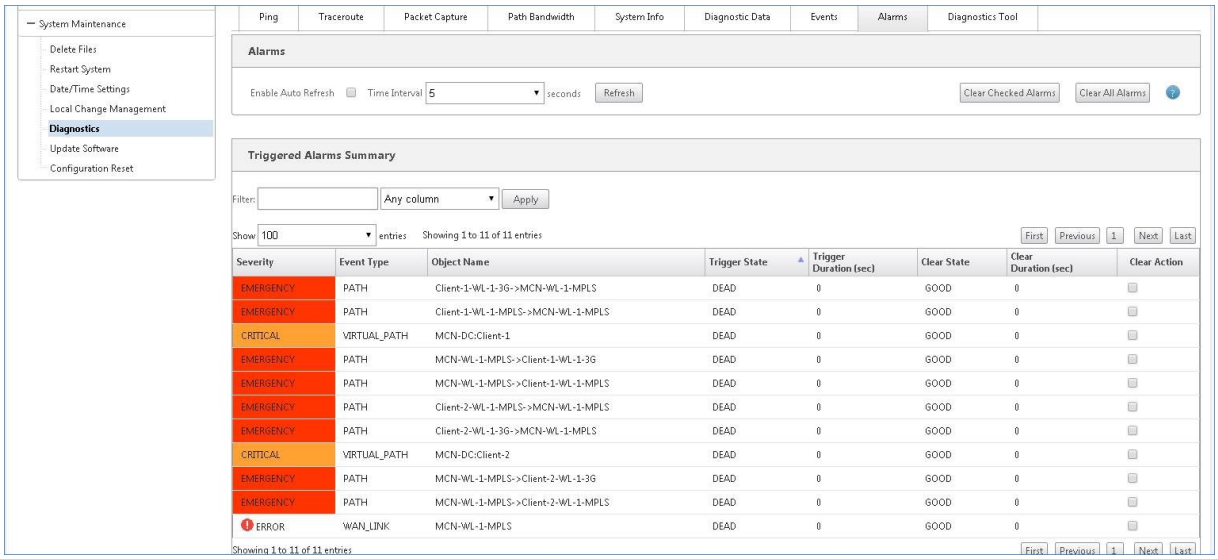
4. Continue adding alarms as required.
5. Click **Apply Settings**.

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.



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.

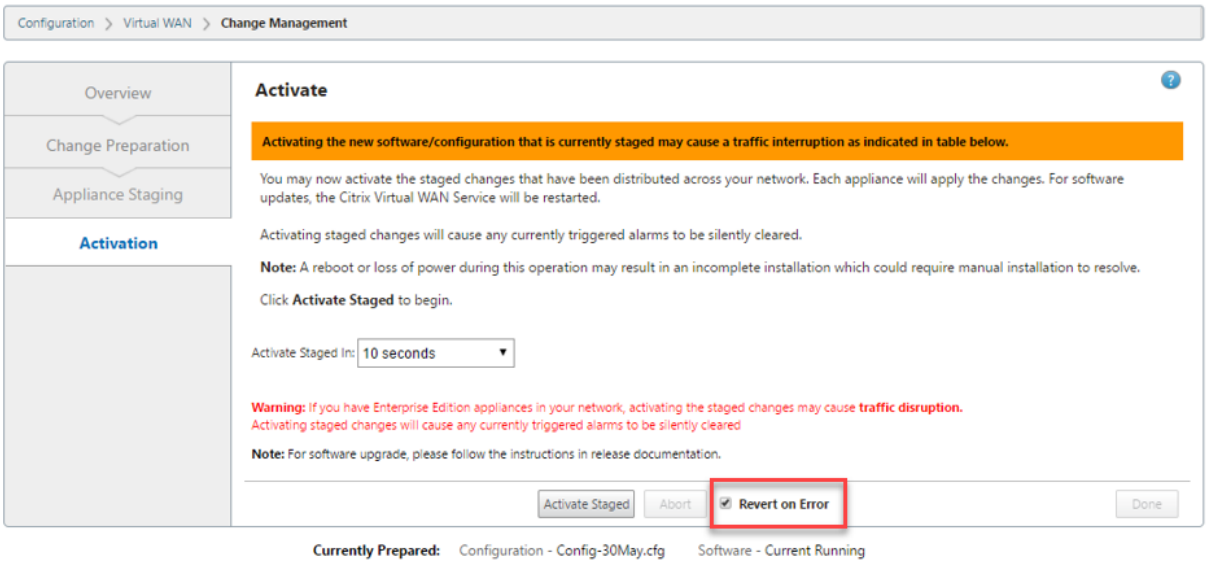
Configure Rollback

April 7, 2021

The Configuration Rollback feature allows the Change Management system to detect and recover from the following software/configuration errors by reverting to the previously active software/configuration:

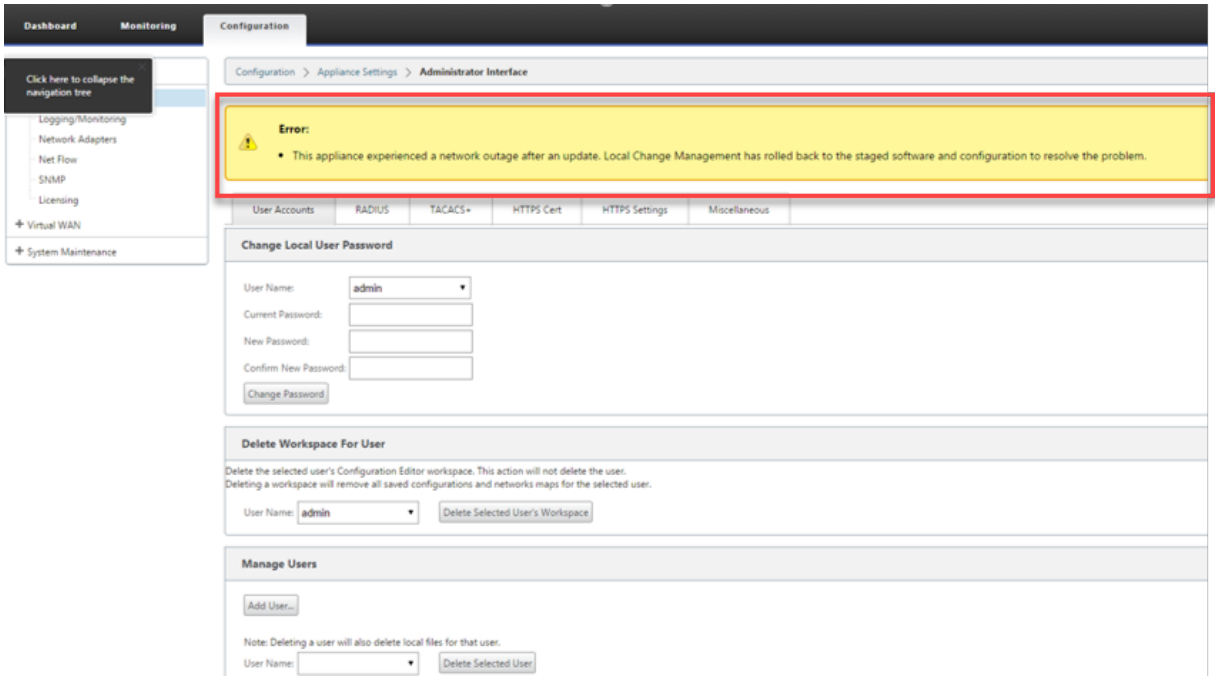
- After a software upgrade, virtual Path is dead and the service gets disabled if the software crash happens.
- After making the configuration changes, virtual Path is dead without any software crash.
- If the configuration for the MCN appliance itself causes a network problem on the MCN site, it does not detect the outage and does not roll itself back. However, all the other clients in the network roll themselves back as they were unable to connect to the MCN.

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



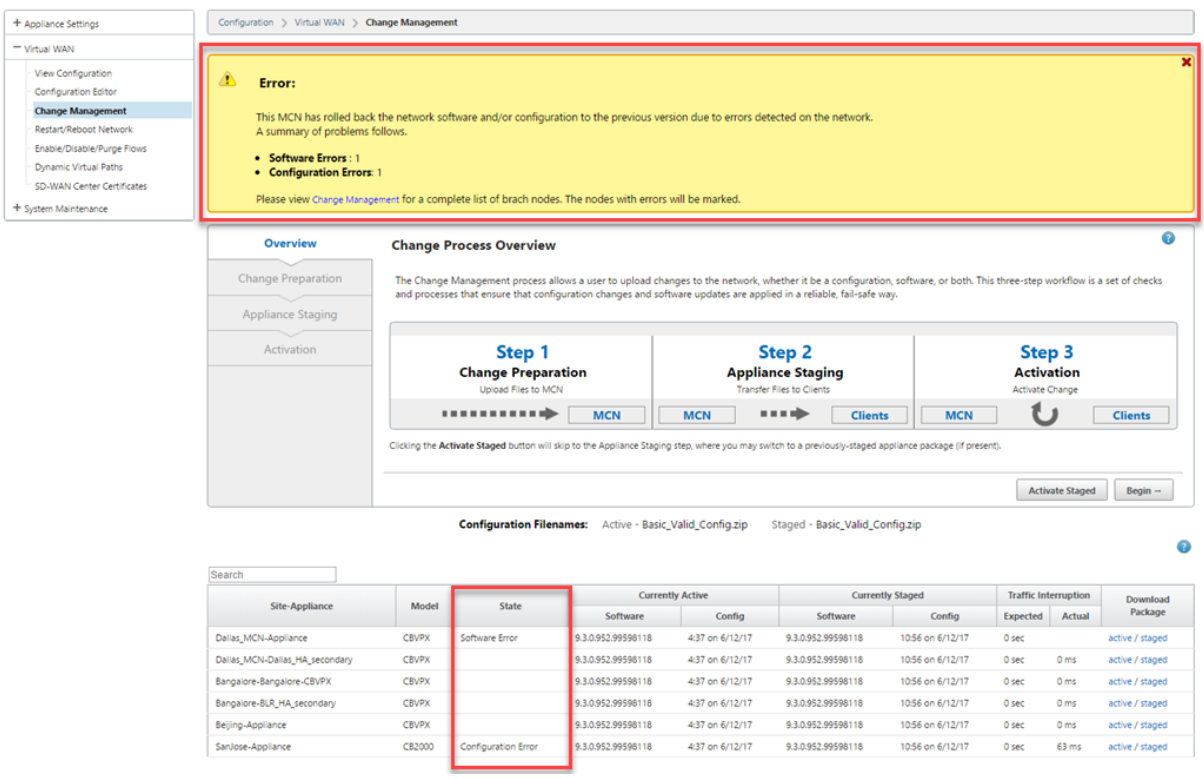
If a system configuration error occurs on a client while activating the staged package from an MCN the client reverts to the previous software configuration and an error message appears as shown in the following screenshot.

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 monitor itself for about 30 minutes. If the software crashes within 30 minutes, or if the network is down (unable to establish a Virtual Path to the MCN) for 30 minutes, then a rollback is triggered.

On the MCN, an error message appears as shown in the following screenshot. 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.



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

March 12, 2021

The **SD-WAN Master Control Node (MCN)** is the head end appliance in the Virtual WAN. Typically, this is a 4000 or 5100 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

- Virtual WAN Gateway Mode Deployment Steps (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.

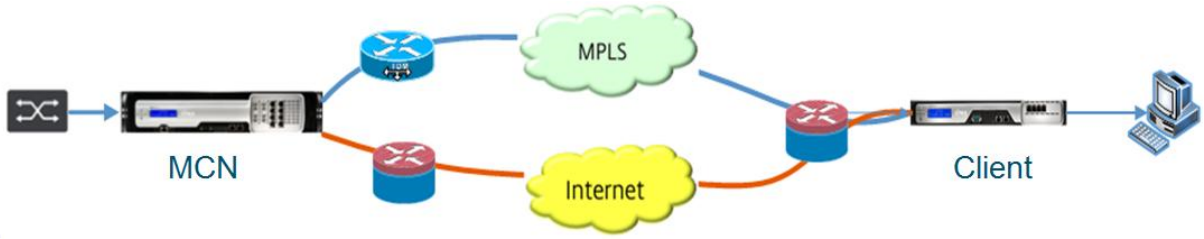
MCN Overview

March 12, 2021

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

March 12, 2021

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.

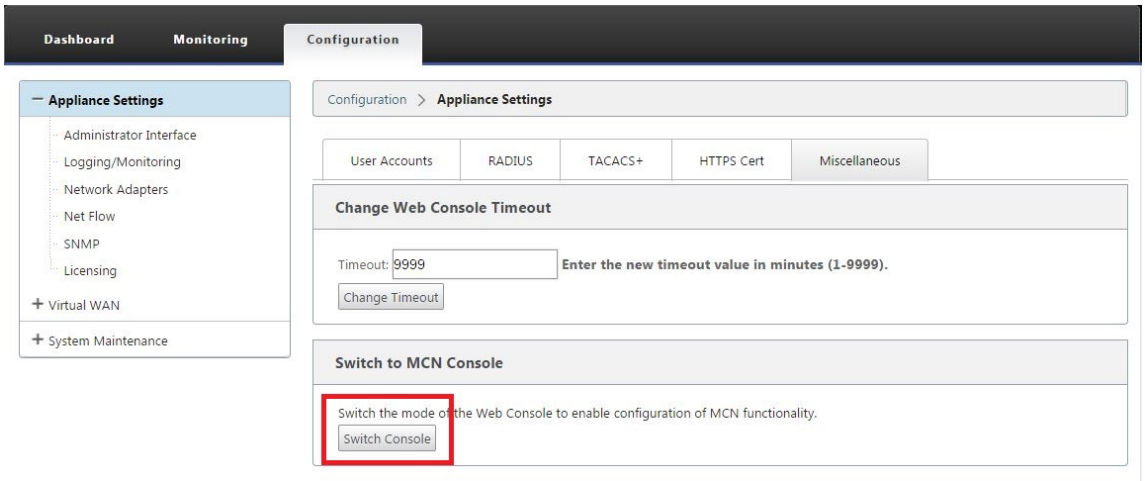
To switch the Management Web Interface to **MCN Console** mode, do the following:

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.



   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.**

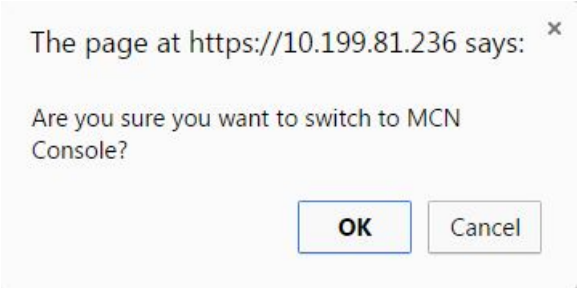
   By default, a new appliance is set to **Client Console** mode.

   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**.

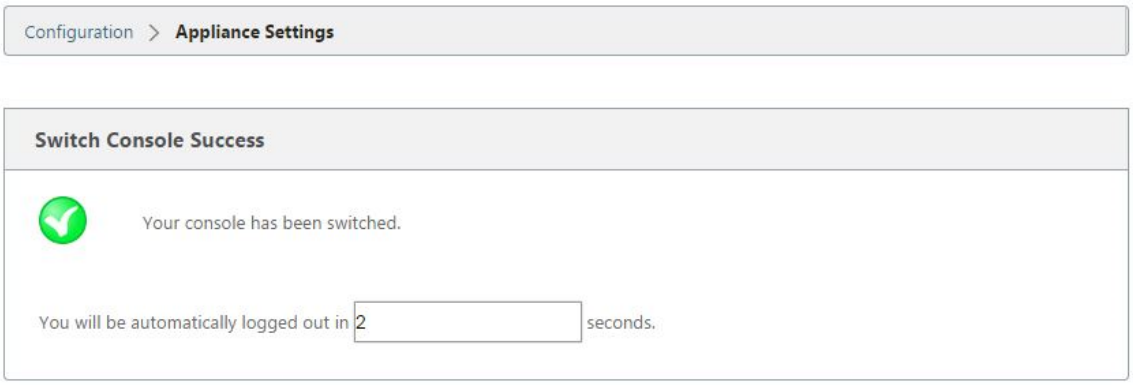
5. Click **Switch Mode** to set the appliance mode to **MCN Console** mode.

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

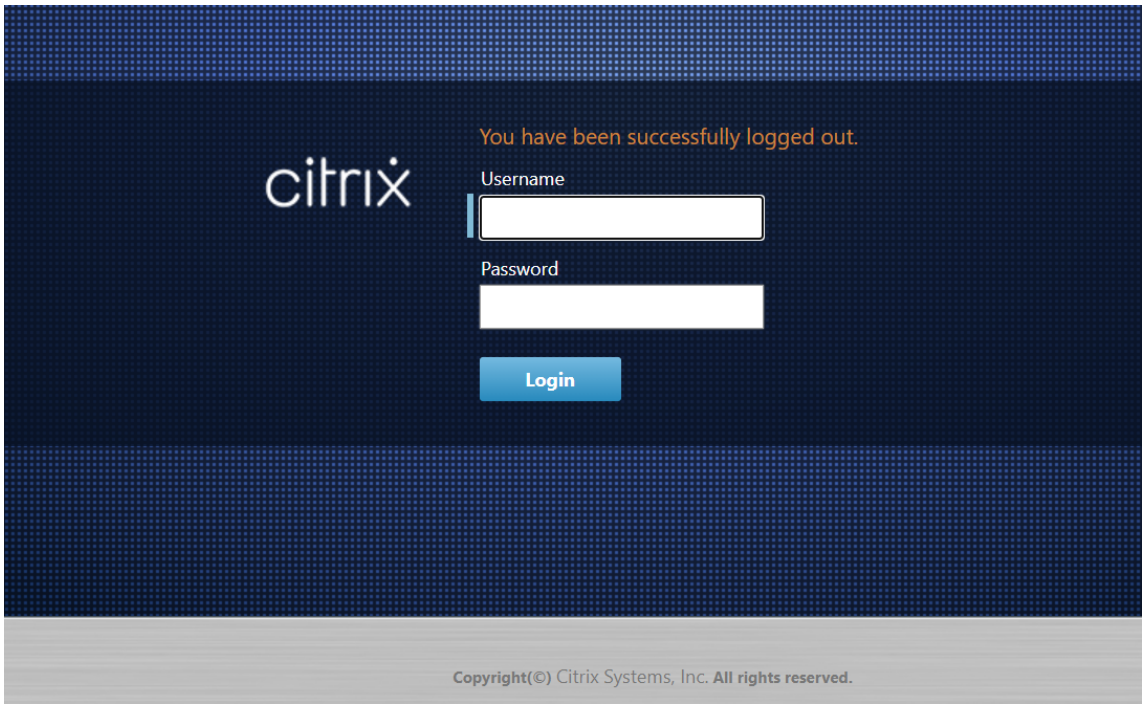


6. Click **OK**.

   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.



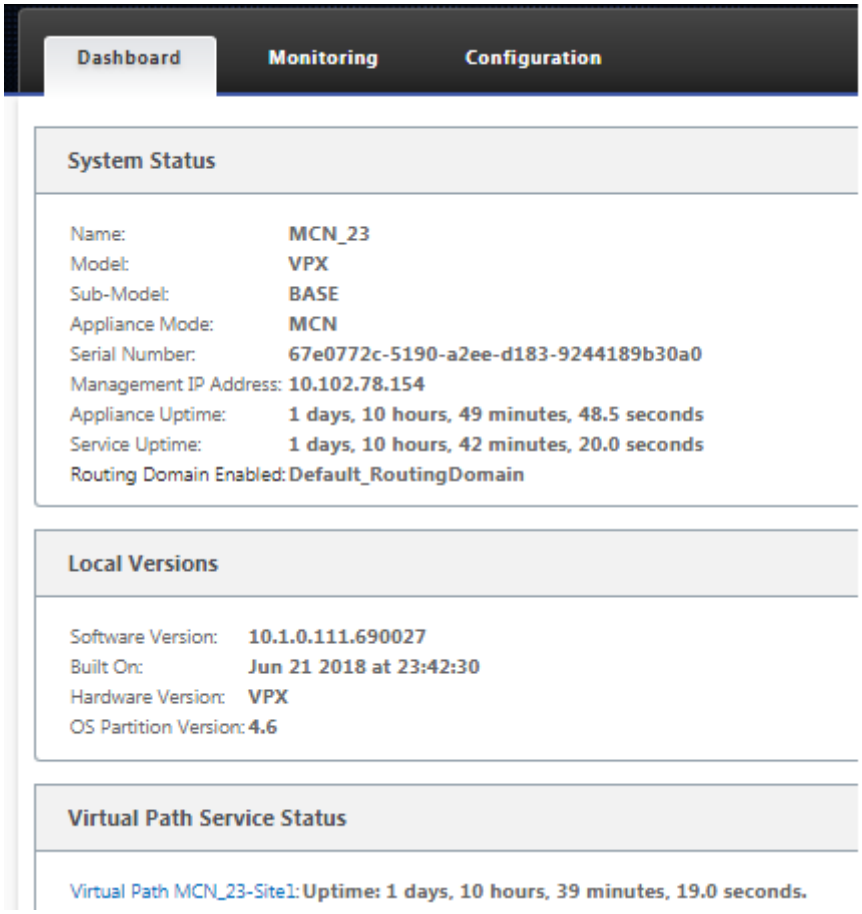
   After the countdown completes, the session is terminated and the login page appears.



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

March 12, 2021

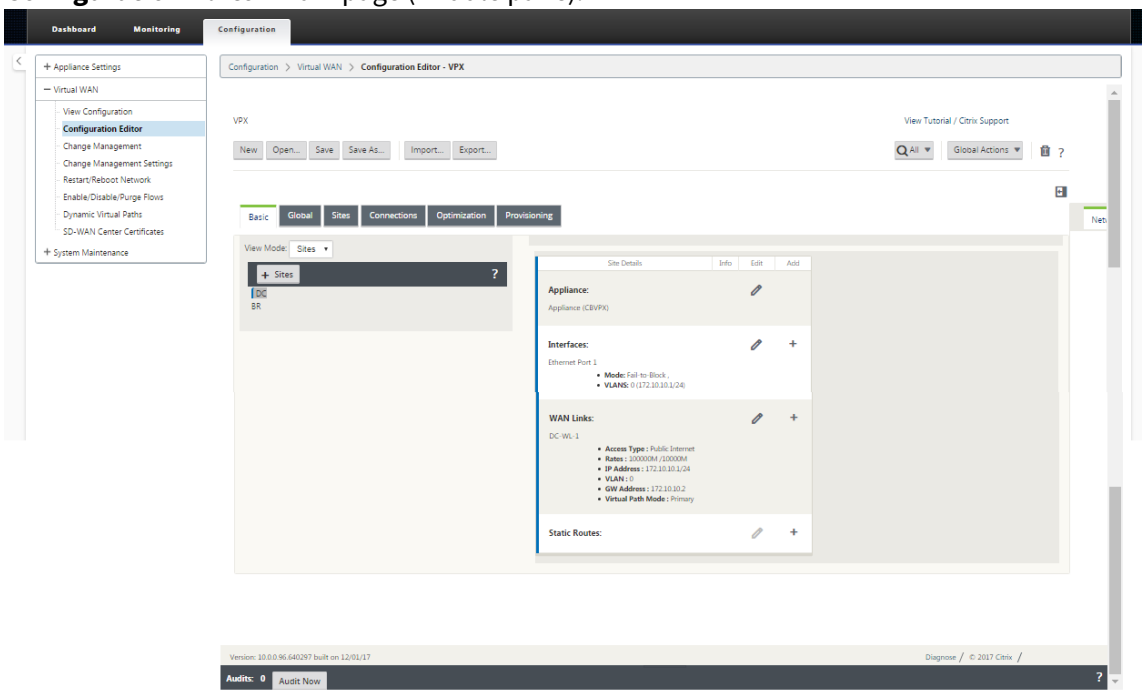
The first step is to open a new configuration package, and add the MCN site to the new configuration.

> **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, see section, Switching the Management Web Interface to MCN Console Mode, for instructions on changing the console mode.
>
> It is 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

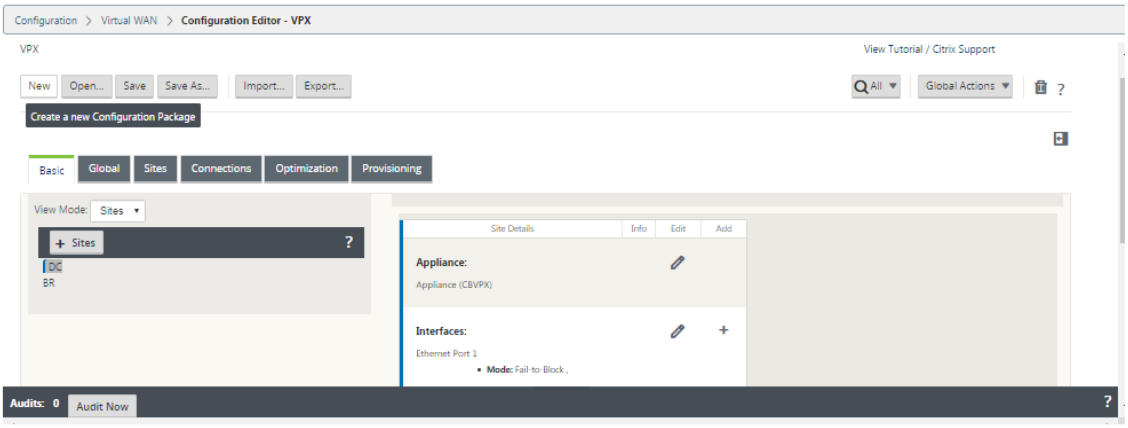
> Configuration.
>
> **Warning**
>
> If the console session times out or you log out of the Management Web Interface before saving your configuration, any unsaved configuration changes are lost. You must then log back into the system, and repeat the configuration procedure from the beginning. For that reason, it is recommended that you 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 9,999 minutes. For security reasons, you must 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:

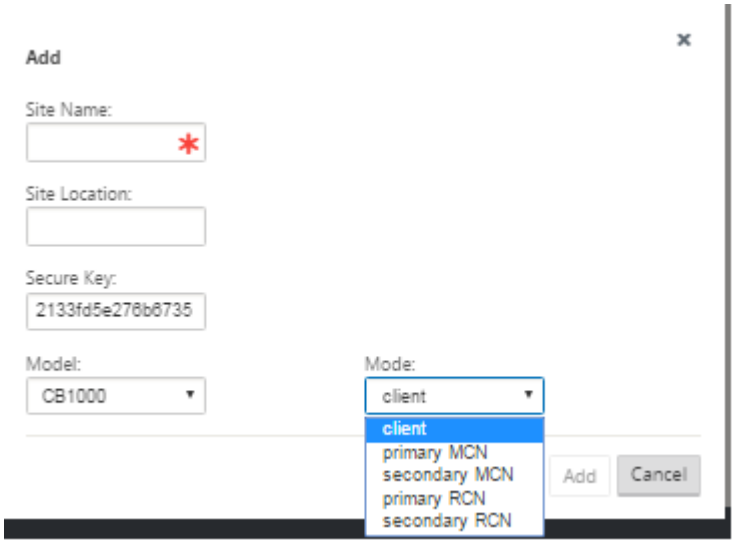
1. In the navigation tree, navigate to **Virtual WAN** > **Configuration Editor**. This displays the **Configuration Editor** main page (middle pane).



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.



4. Enter the site information.

Do the following:

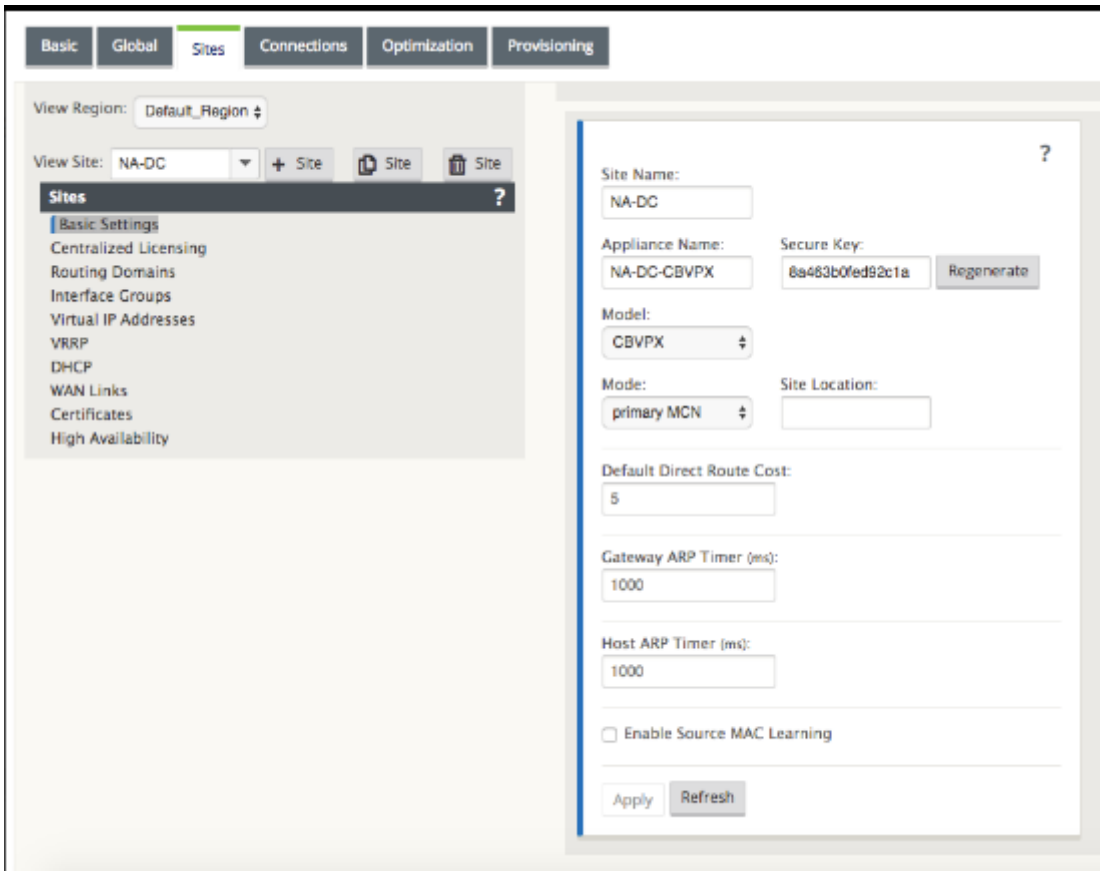
1. Enter the **Site Name** and **Secure Key**.
2. Select the appliance **Model**.
3. Select the **Mode**.
4. Select **primary MCN** as the mode.

> **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 an SD-WAN 4000-SE appliance.)

> Entries cannot contain spaces and must be in Linux format.

To add site:

1. 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.



   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 errors in that section. You can also click the dark gray **Audits** status bar (bottom of page) to display a complete list of all unresolved audit warnings. Configurable Host ARP Timer (ms) is added at a Site level during configuration. The current default value is 1,000 ms. The configurable range is from 1,000 ms through 180,000 ms. The Host ARP timer configuration is not applicable to management port.

2. Enter the basic settings for the new site, or accept the defaults. In Citrix SD-WAN deployments such as Gateway and One-arm, when the ARP requests are received frequently, the access points become overloaded affecting traffic flow. You can now configure ARP timers to send the ARP requests with specific interval times. The time interval is configured in seconds. You can configure ARP time intervals when configuring the data center site under **Basic Settings** tab in

the Citrix SD-WAN appliance GUI.

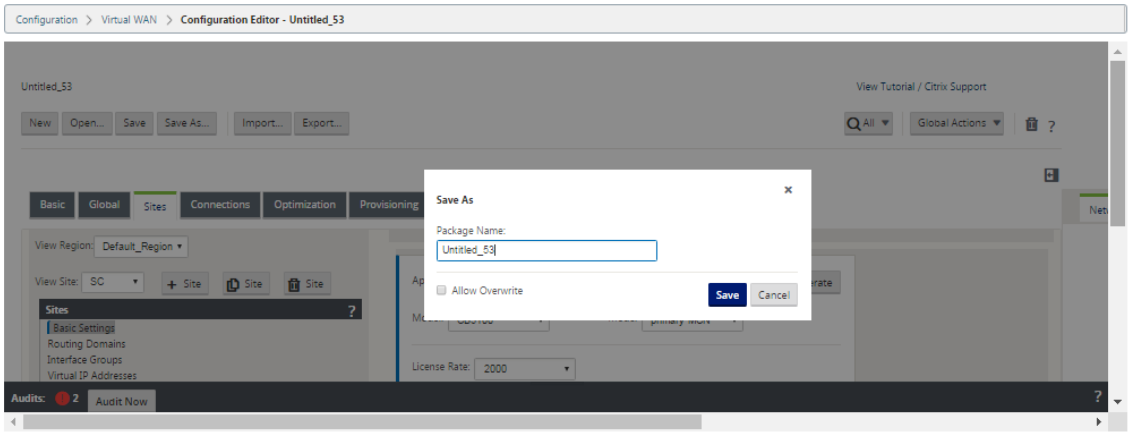
3. (Optional, recommended) Save the configuration-in-progress.

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. 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:

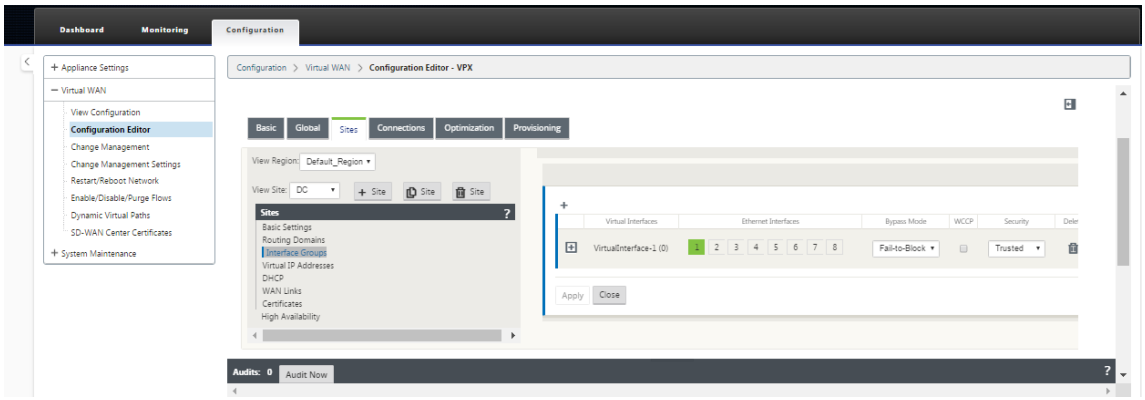
- Use logical names that will best describe the group.
- Trusted networks are networks that are protected behind a Firewall.

- Virtual Interfaces associate interfaces to Fail to Wire (FTW) pairs.
- Single WAN interfaces cannot be in an FTW pair.
- IPv6 address is introduced in 11.1.0 release and it is only supported for untrusted interfaces. Untrusted interfaces are non-routable and used for virtual path traffic.

> **Note**
>
> For more guidelines and information on configuring Virtual Interface Groups, see the Virtual Routing and Forwarding section.

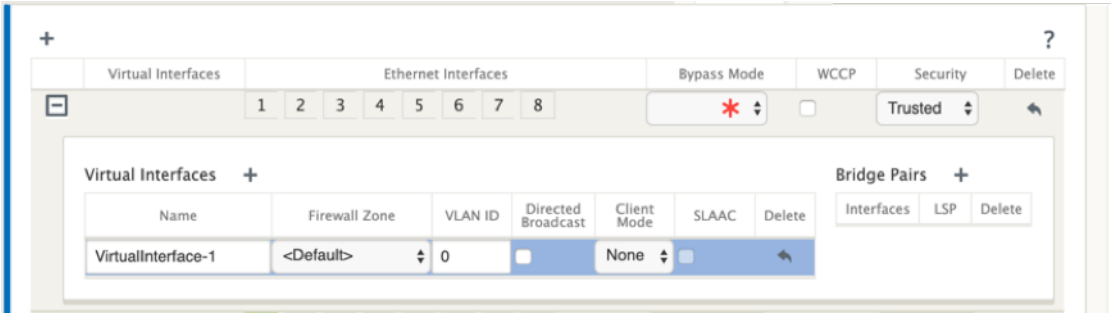
To add a Virtual Interface Group to the new MCN site, do the following:

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.



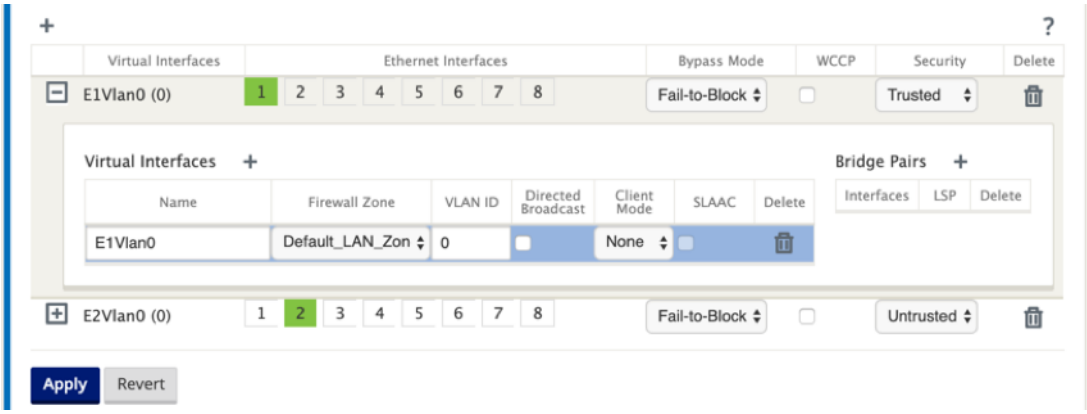
2. Click **+** to add the **Virtual Interface Group**. This adds a new blank Virtual interface group entry to the table and opens it for editing.

3. Click **+** to the right of **Virtual Interfaces**. This adds a new blank group entry to the table and opens it for editing.

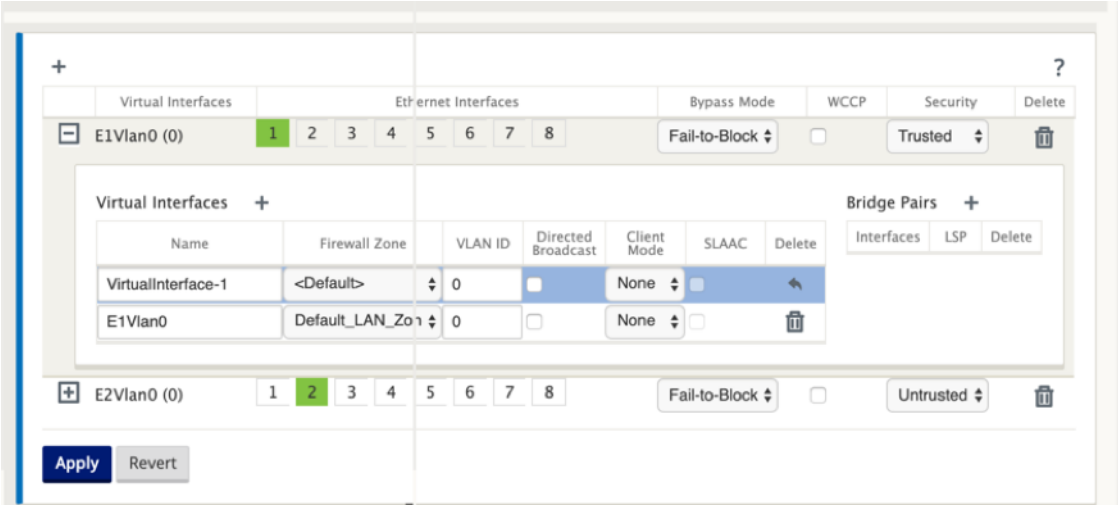


4. Select the **Ethernet Interfaces** to include in the group. Under **Ethernet Interfaces**, click an interface to include/exclude that interface. You can select any number of interfaces to include in the group.

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 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, VLAN ID, Directed Broadcast, Client Mode,** and **Stateless Address Auto-Configuration (SLAAC)**.



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

   - **Name** –This is the name by which this Virtual Interface is 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.
   - **Client Mode** –Select the client mode from the drop-down menu.
   - **Directed Broadcast** - On the virtual interface, Directed Broadcasts packets can be forwarded for Virtual IP subnets by enabling the check box.
   - **SLAAC** –Enabling **Stateless Address Auto-Configuration (SLAAC)** check box on a Virtual Interface allows it to automatically obtain a global IPv6 address from the connected router. Virtual Interfaces with **SLAAC** turned on do not require a configured Virtual IP Address.

     > **NOTE**
     > SLAAC can only be enabled on a branch site on an untrusted interface.

     You have the ability to release or renew the IP addresses for SLAAC.

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. 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 is 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 shown above.

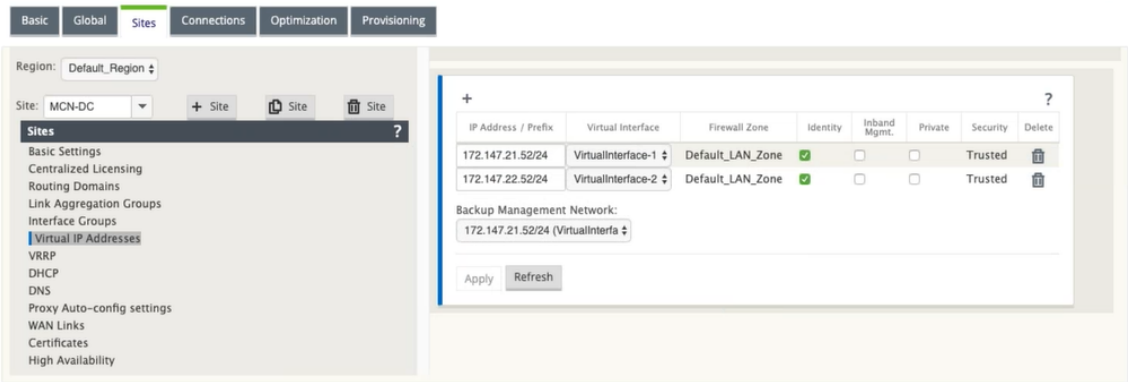
How to configure virtual IP address for the MCN

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. Select **Inband Mgmt** to allow the virtual IP address to connect to management services such as web UI and SSH.

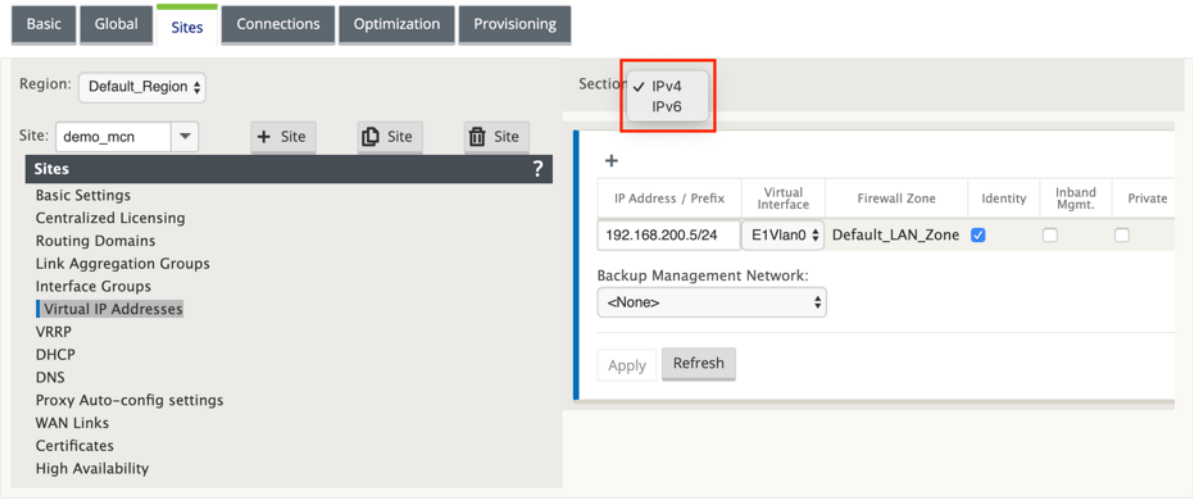
   > **Note:**
   >
   > The interface should be of security type **Trusted** and **Identity** enabled.

6. Select a virtual IP as a **Backup Management Network**. This allows you to use the virtual IP address for management if the management port is not configured with a default gateway.



7. Click **Apply**. This adds the address information to the site and includes it in the site **Virtual IP Addresses** table.
8. To add more Virtual IP Addresses, click **+** to the right of the **Virtual IP Addresses**, and proceed as above.

From 11.1.0 release onwards, there are two subsections available under the **Virtual IP Address** : **IPv4** and **IPv6** addresses.



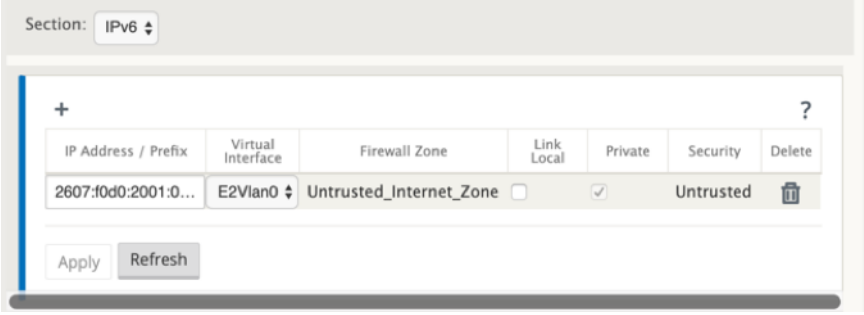
Limitations

- Only one pair of paths is created if both IPv4 and IPv6 Access Interfaces are configured on the same WAN link.
- If IPv6 path goes down, no fall back happens to IPv4 for the same WAN link.
- Tracking IPv6 addresses are not supported for 11.1.0 release.
- IPv6 is only supported for communication between SD-WAN devices over Virtual Path. Internet and Intranet services are not supported. No support for management plane in 11.1.0 release.
- IPv6 will not be supported for LTE links on 210 devices for 11.1.0 release.
- DHCPv6 client and server is not supported for IPv6. You can configure SLAAC for auto-addressing.

You need to add a virtual IP address for the newly created untrusted interface or you can enable SLAAC if it is a branch site. To add virtual IP address:

1. Select IPv6 from the Section drop-don menu.
2. Define the following fields:
3. IP Address / Prefix –Provide the full host address and netmask.
4. Virtual Interface –Select one of the associated virtual interfaces from the drop-down menu.
5. Firewall Zone –The firewall zone for the virtual interface.
6. Link Local (Optional)- If the Link Local check box is enabled, this IPv6 Virtual IP Address can be used as the link local address for the Virtual Interface.

> **NOTE**
> If the Link Local check box is not enabled, the appliance automatically generates and assign a link local address.



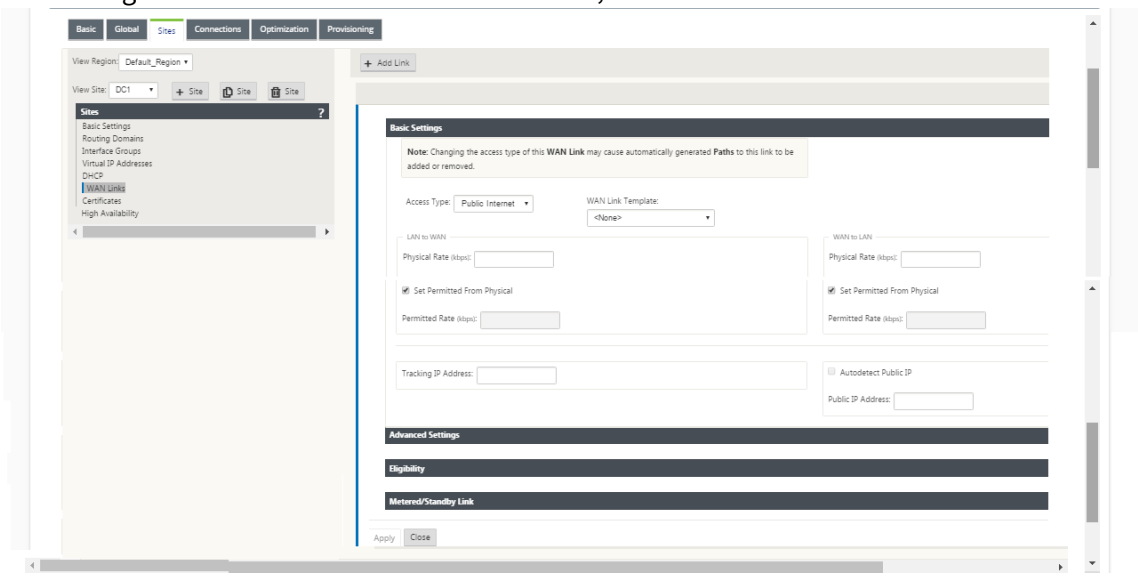
> **NOTE**
> Neighbor Discovery Protocol (NDP) is supported by IPv6.

If both IPv4 and IPv6 Access Interfaces are defined at local and remote site, then the path is formed using only IPv6 address.

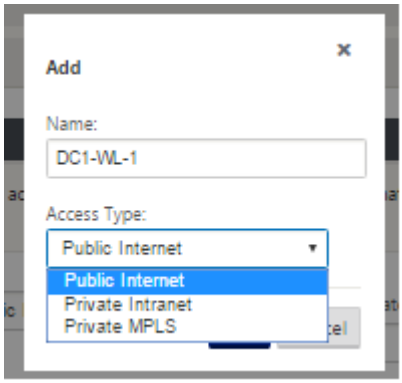
How to configure WAN links for the MCN

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

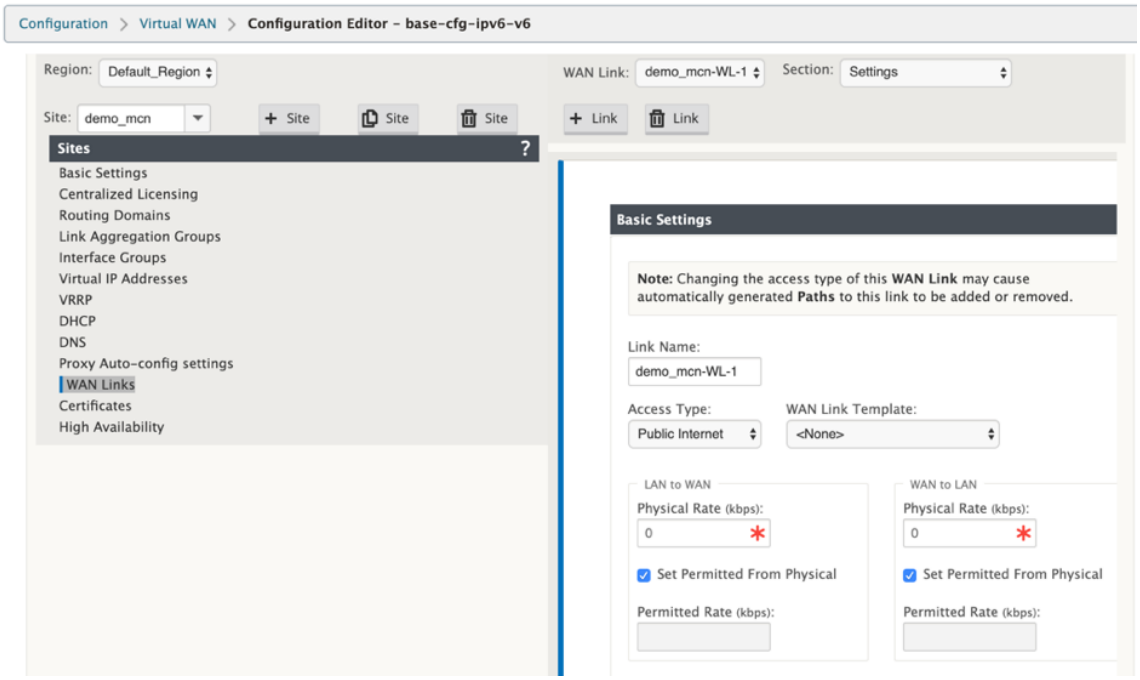
1. Continuing in the **Sites** view for the new MCN site, click the **WAN Links** label.



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

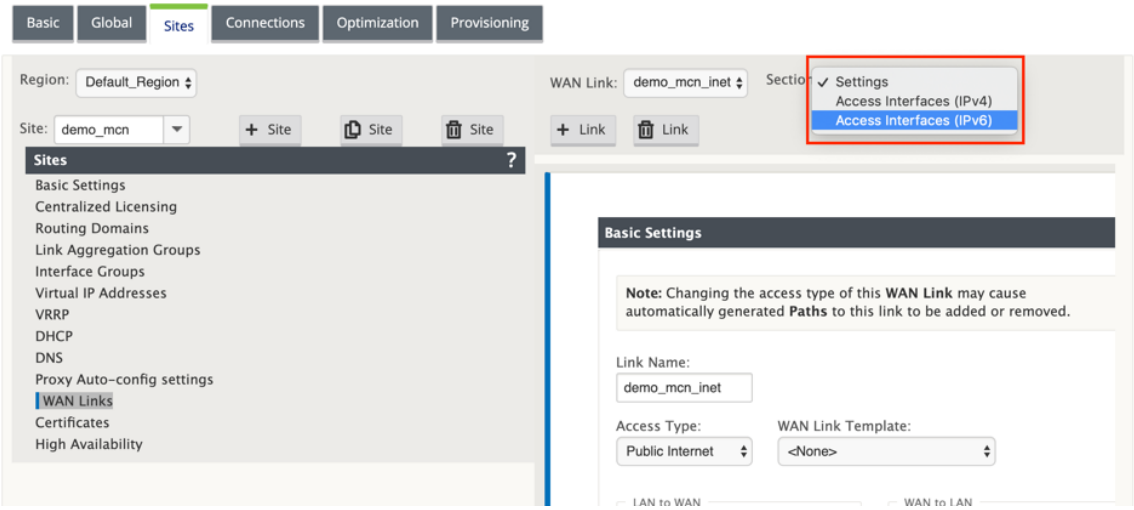


3. (Optional) Enter a name for the WAN Link if you do not want to use the default. The default is the site name, appended with the following suffix: WL-<number>, where <number> is the number of WAN Links for this site, incremented by one.
4. Select the **Access Type** from the drop-down menu. The options 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.



Only IPv6 path between two sites is formed when both IPv4 and IPv6 Access Interfaces are configured for the same WAN Link.

1. Select **Access Interfaces (IPv6)** from the **Setting** drop-down menu.

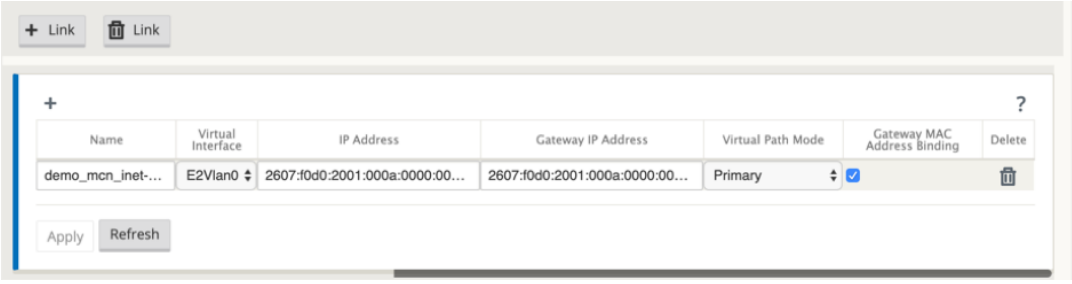


2. Define the following fields:

   - **Name** –Provide the Access Interface name.
   - **Virtual Interface** –Once a routing domain is selected, select one of the associated virtual interfaces from the drop-down menu.
   - **IP Address** –Provide static IP address for the access interface endpoint on the SD-WAN.
   - **Gateway IP Address** –Provide the IP address of the gateway router.

     > **NOTE**
     > You cannot configure the IP address and the gateway IP address when the virtual appliance is configured to use SLAAC mode.

   - **Virtual Path Mode** - Select the virtual path mode from the drop-down menu to determine the priority for virtual path traffic on this WAN link.
   - **Gateway MAC Address Binding** –If the **Gateway MAC Address Binding** check box is enabled, the source MAC address of packets received on internet or intranet services must match the gateway MAC address.



Once the IPv6 interface is created for the WAN link, you can use this interface to communicate with the Internet Service Provider (ISP).

> **NOTE**
> Since the initial IPv6 offering is Virtual Path connectivity only, we cannot send LAN side IPv6 packets.

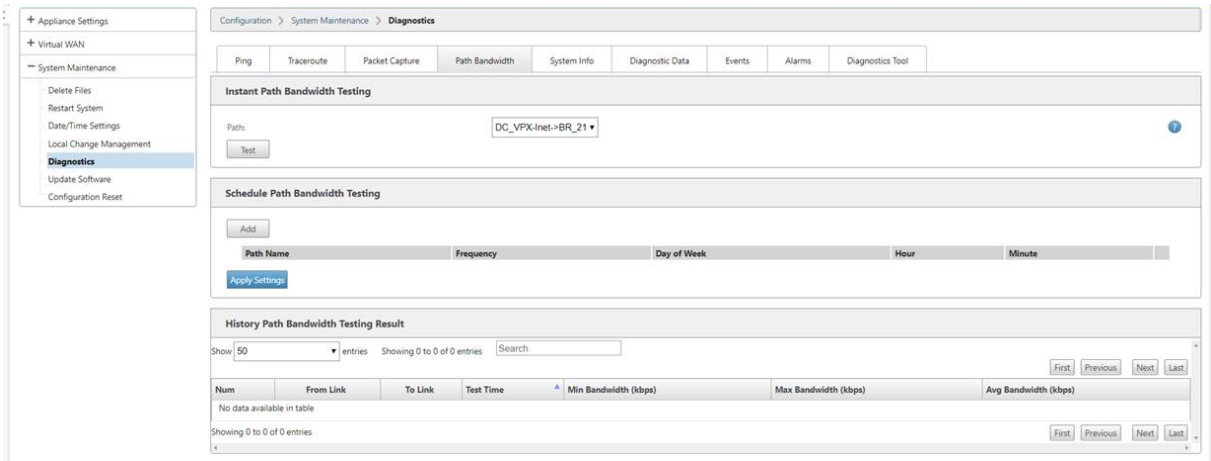
Auto Learn of bandwidth consumption

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

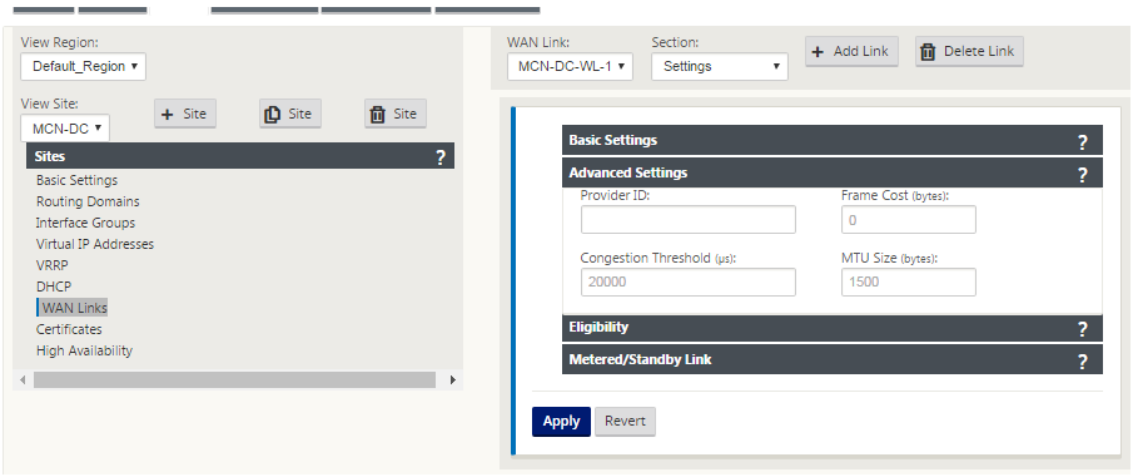
You can execute tests manually or schedule tests in the SD-WAN GUI. Results from these tests should also apply to the permitted rate when the test is successful and auto learn is enabled.

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.

> **Note**
>
> Auto detection of WAN Link bandwidth, is applicable only on branches and not applicable for MCN/RCN.



1. 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.
2. Click the gray **Advanced Settings** section bar. This opens the **Advanced Settings** form for the link.

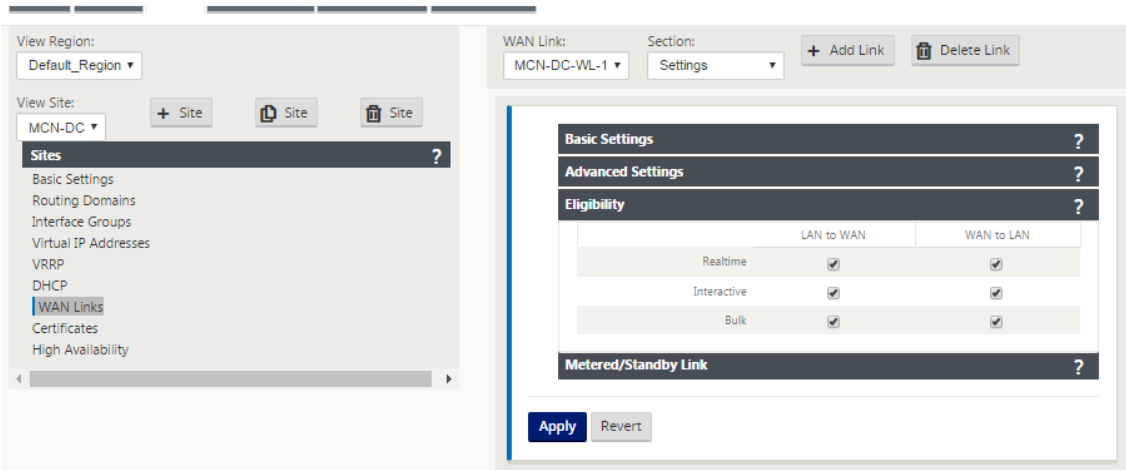


3. Enter the **Advanced Settings** for the link:

   - Provider **ID** –(Optional) Enter 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)** –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 throttles packet transmission to avoid further congestion.
   - MTU **Size (bytes)** –Enter the largest raw packet size (in bytes), not including the Frame Cost.

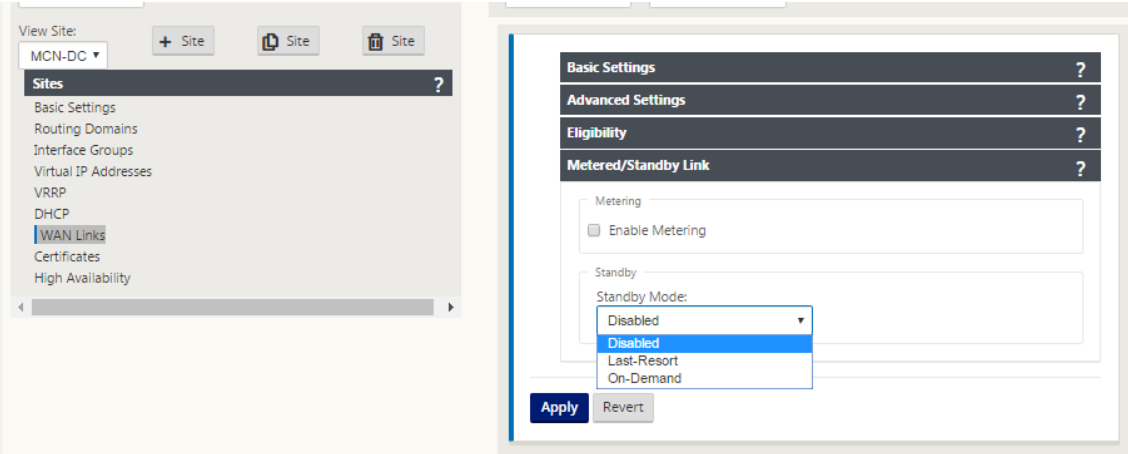
4. Click the gray **Eligibility** section bar. This opens the **Eligibility** settings form for the link.

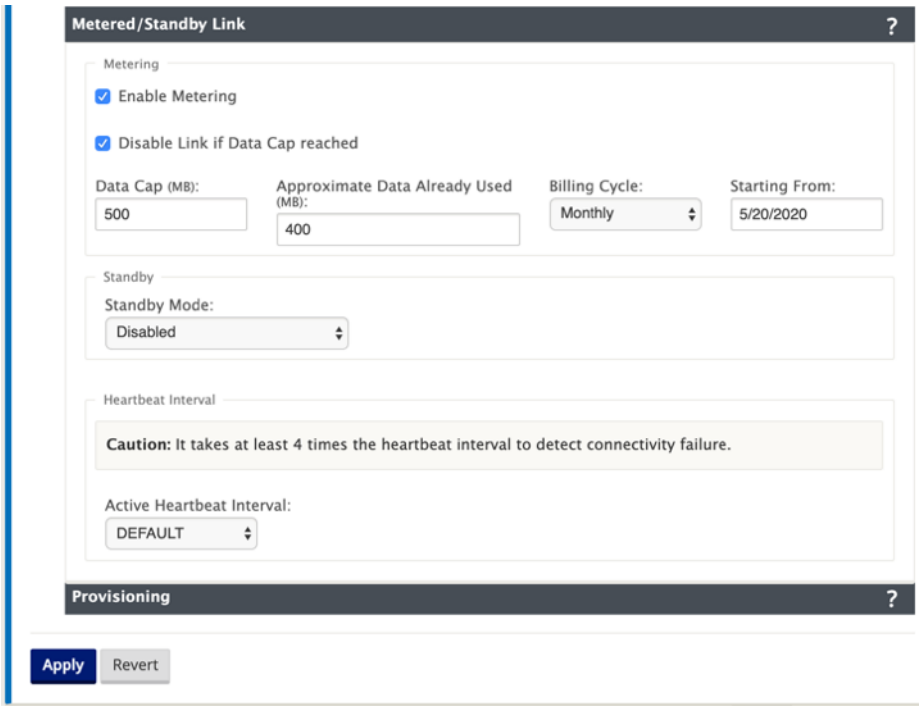
5. Select the **Eligibility** settings for the link.



6. Click the gray **Metered Link** section bar. This opens the **Metered Link** settings form for the link.

7. (Optional) Select **Enable Metering** to enable metering for this link. This displays the **Enable Metering** settings fields.





8. Configure the metering settings for the link. Enter the following:

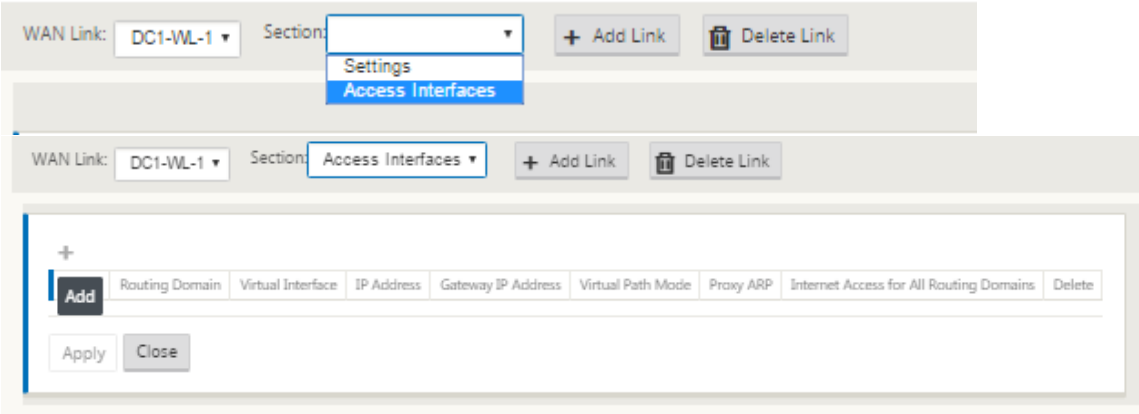
- Data **Cap (MB)** –Enter the data cap allocation for the link, in megabytes.
- Billing **Cycle** –Select either **Monthly or Weekly** from the drop-down menu.
- Starting **From** –Enter the start date of the billing cycle.
- Set **Last Resort** –Select this to enable this link as a link of last resort 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 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.

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

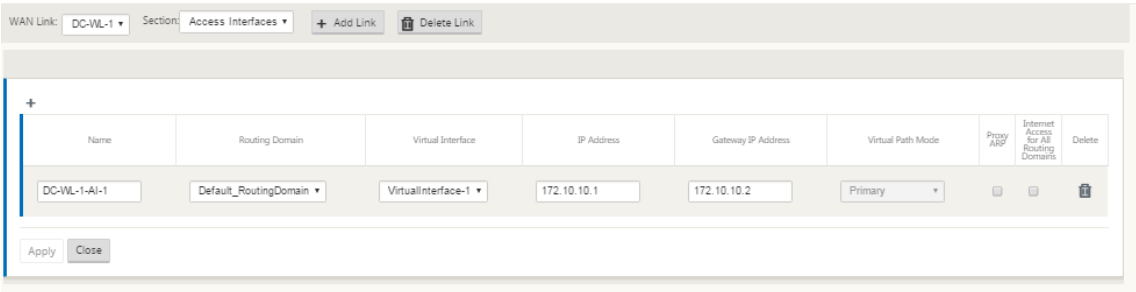
The next step is to configure the Access Interfaces for the new WAN link. An Access Interface consists of a Virtual Interface, WAN endpoint IP Address, Gateway IP Address, and Virtual Path Mode defined collectively as an interface for a specific WAN link. Each WAN link must have at least one Access Interface.

How to configure access interface:

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



2. 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. Each WAN link must have at least one Access Interface.



3. Enter the following:

- Name –This is the name by which this Access Interface is 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 uses. 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 is used for Internet and Intranet traffic, only.
- **Proxy ARP** –Select the check box to enable. If enabled, the Virtual WAN Appliance replies to ARP requests for the Gateway IP Address, when the gateway is unreachable.

1. Click **Apply**.

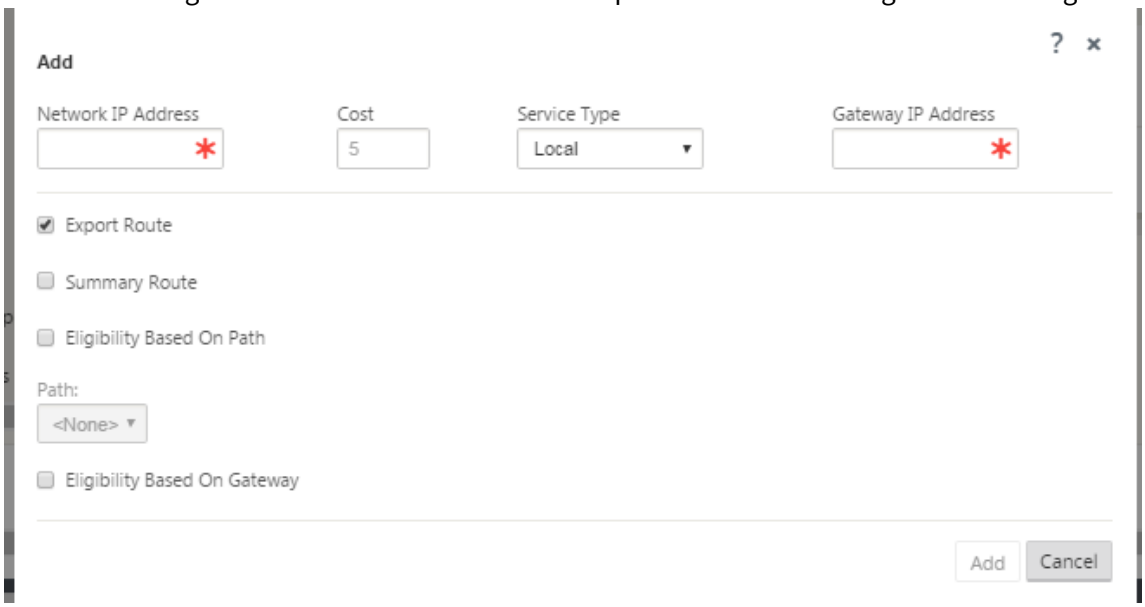
You have now finished configuring the new WAN link. Repeat these steps to add and configure more WAN links for the site.

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.
  - **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. Under certain conditions, and if configured for Intranet Fallback on the Virtual Path, traffic that ordinarily travels by a Virtual Path may 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, as well as traffic on the Virtual WAN Appliance local subnet, configured subnets, or Rules applied by the Network Administrator. This traffic is not delayed, shaped, or modified 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 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.
  - **Inter Routing** - This service enables route leaking between Routing Domains within a site

or between different sites. This eliminates the need for an edge router to handle route leaking.

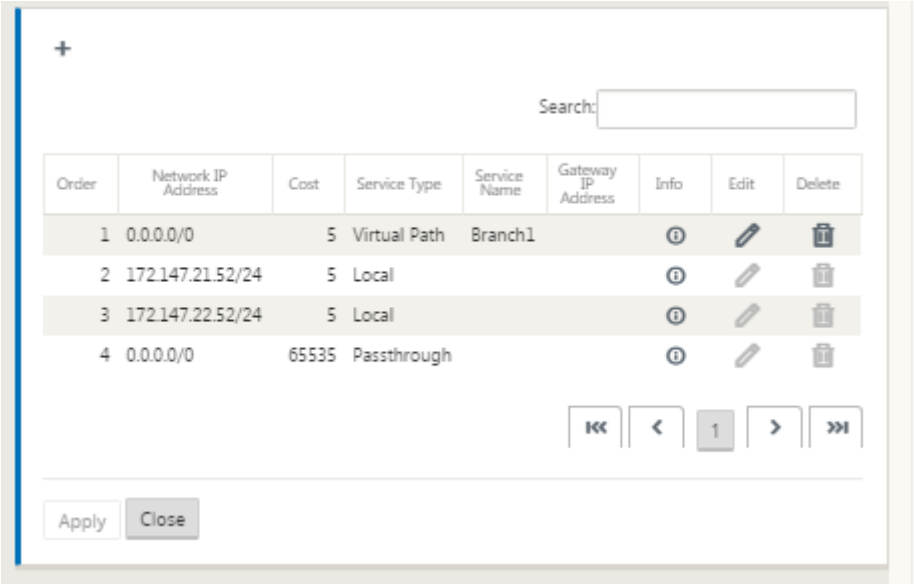
- **Gateway IP Address** –Enter the **Gateway IP Address** for this route.
- **Eligibility** - Based on Path (check box) –(Optional) If enabled, the route does not receive traffic when the selected path is down.
- **Path** –This specifies the path to be used for determining route eligibility.

Depending on the "Service Type,"the following settings are displayed:

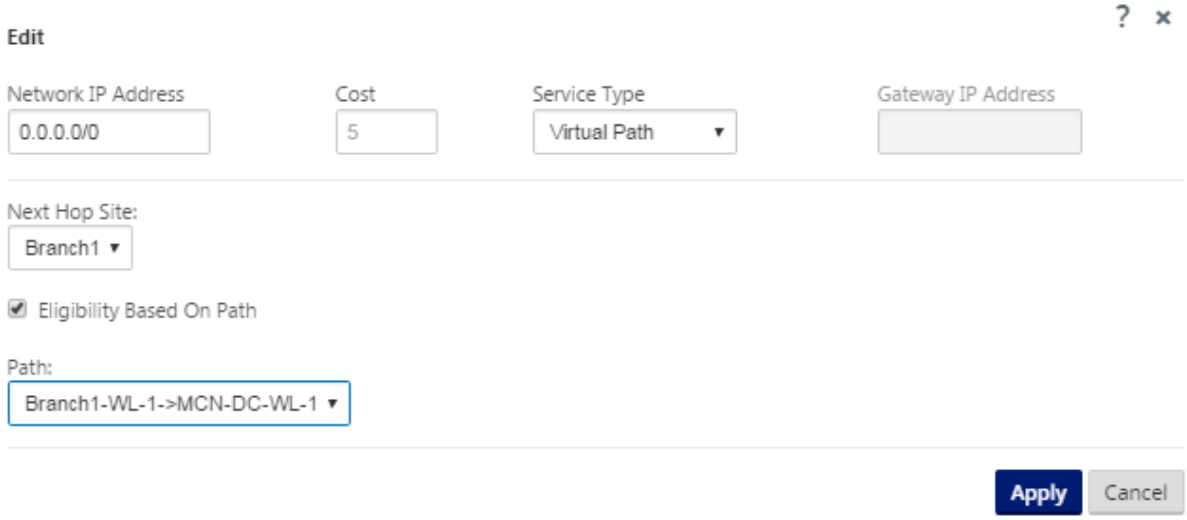
Service Type	Service Type Settings
Virtual Path	Next Hop Site –This indicates the remote site to which Virtual Path packets are directed.
Internet	Export Route: Enable/Disable to export routes to other connected sites, Eligibility based on path
Intranet	Export route, Intranet service, Eligibility based on path, Eligibility based on tunnel
Passthrough	Eligibility based on path
Local	Export route, Summary route, Eligibility based on path
GRE Tunnel	Export route, Eligibility based on path, Eligibility based on Gateway
IPsec Tunnel	Export route, Eligibility based on path, IPsec Tunnel, Eligibility based on tunnel
Discard	Export route, Summary route
Inter Routing	Inter Routing Domain Service

1. 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.



You can also edit configured routes as following.



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 more 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 now, you can proceed directly to the section Naming, Saving, and Backing Up the MCN Site Configuration.

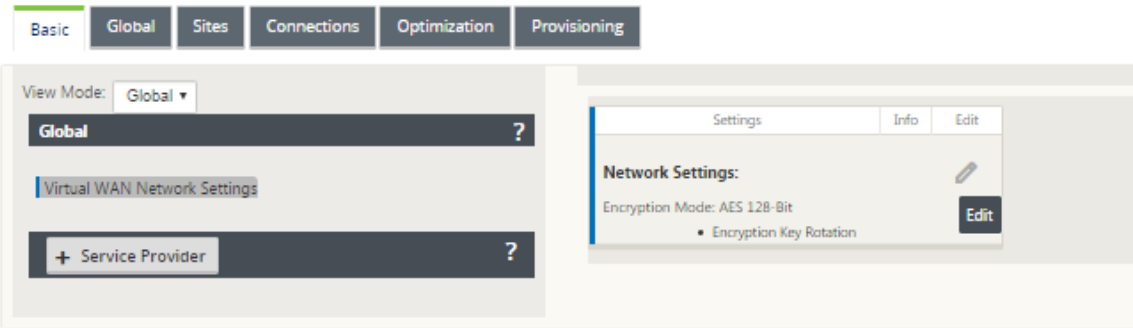
Enable and Configure Virtual WAN Security and Encryption (Optional)

March 12, 2021

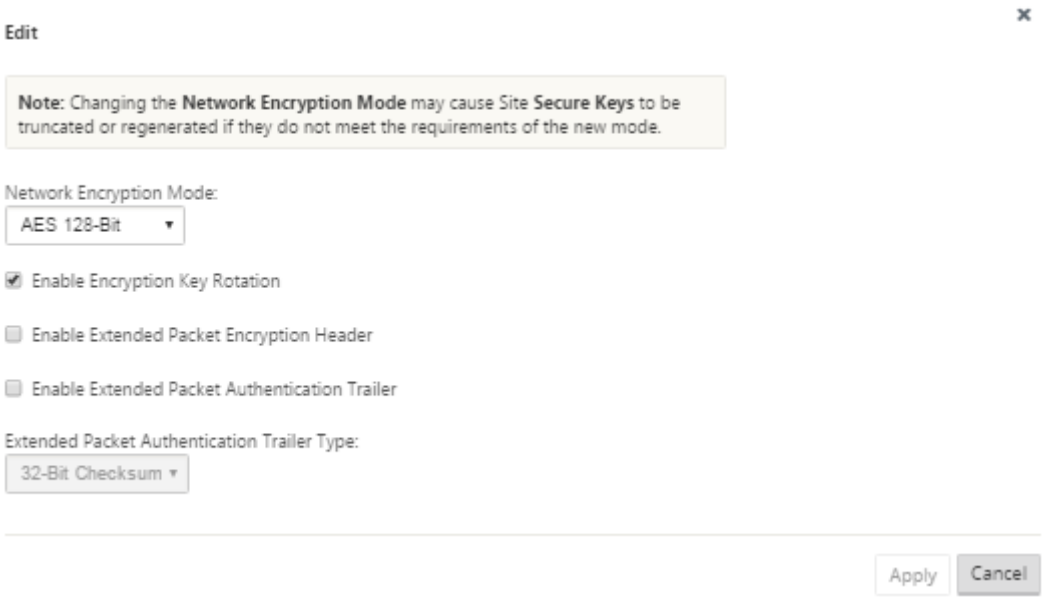
To enable and configure Virtual WAN security and encryption, do the following:

> **Note**
>
> Enabling Virtual WAN security and encryption is optional.

1. Navigate to the **Basic** tab in the **Configuration Editor**, Select **Global** from **View** mode. The Virtual Network Settings configuration form is displayed.



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 Bits** or **AES 256 Bits**.

- **Enable Encryption Key Rotation**: When enabled, encryption keys are rotated at intervals of 10–15 minutes.
- **Enable Extended Packet Encryption Header**: When enabled, a 16 bytes 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 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 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.

Configure Secondary MCN

June 25, 2021

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 can 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.

You can choose an appliance model for secondary MCN based on the usage, bandwidth requirement, and the number of sites to be supported.

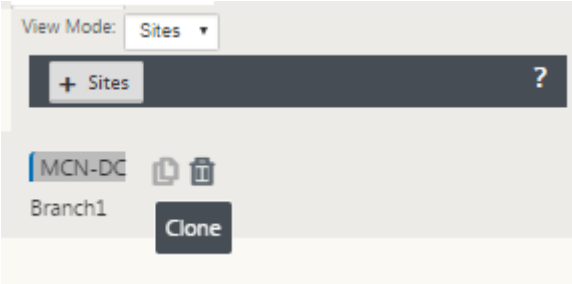
The primary MCN to secondary MCN switch over happens after 15 seconds of the primary MCN being inactive. You cannot configure primary reclaim for secondary MCN, the primary reclaim happens automatically after the primary appliance is back ON and the hold timer expires.

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.

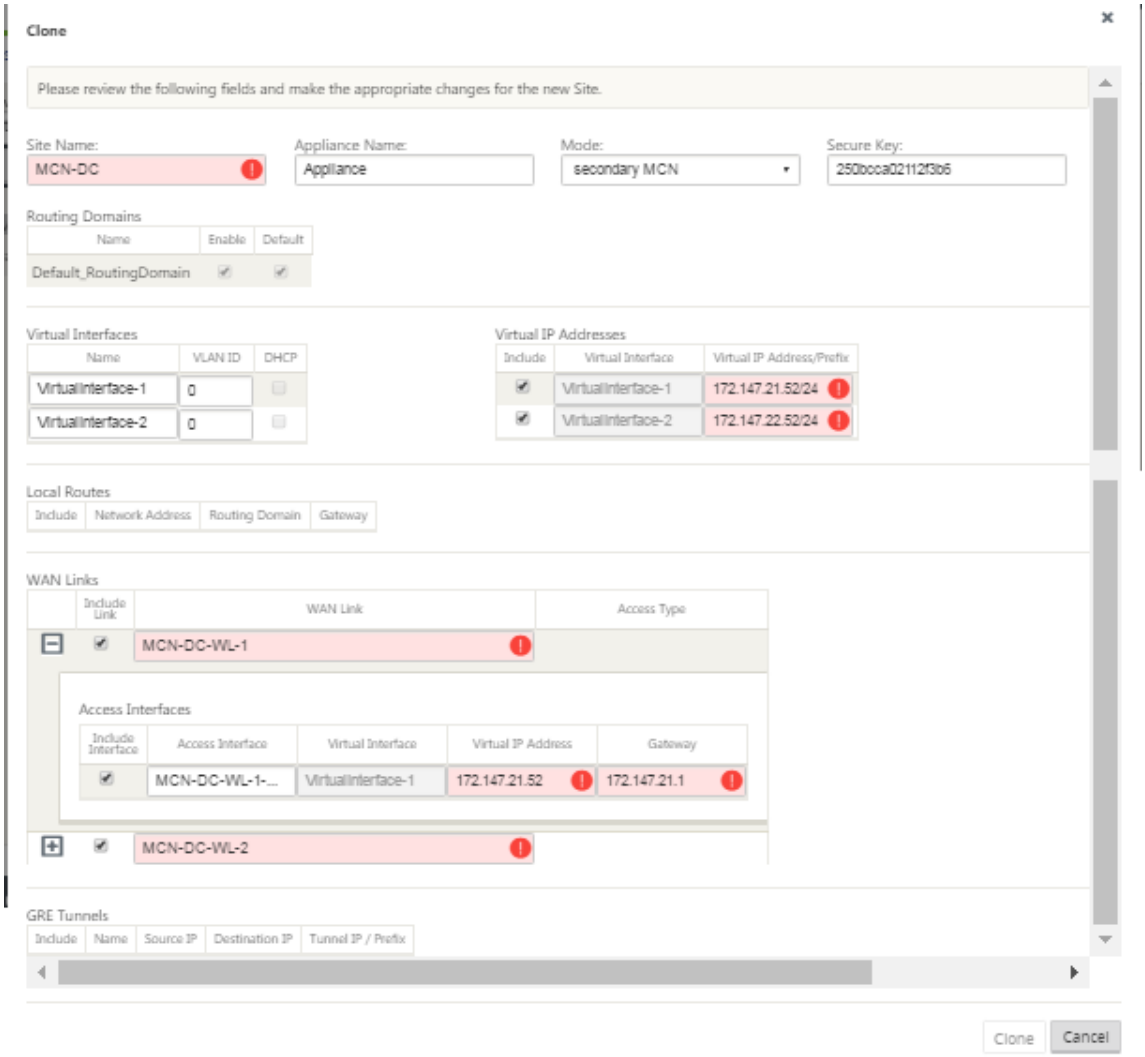
> **Note**
>
> You can clone an MCN to create a secondary MCN or branch sites. You can configure only one secondary MCN.

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.



> **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.

3. In the **Mode** field, select **secondary MCN**. Resolve all Audit Alerts.
4. Click **Clone** to create the secondary MCN site.

Manage MCN Configuration

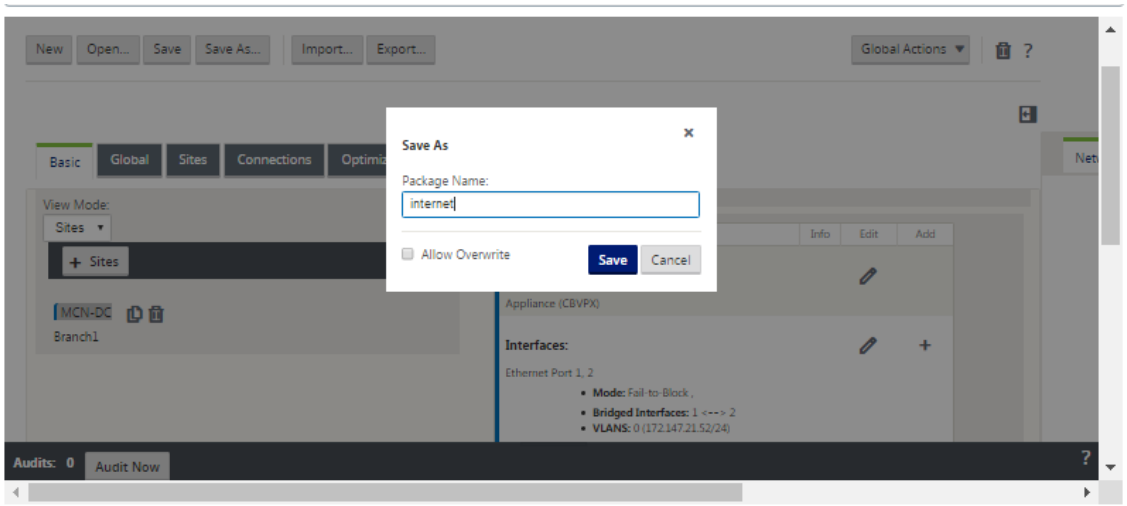
March 12, 2021

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 log out of the Management Web Interface and continue the configuration process later. However, if you log out, you should 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 should 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). The **Save As** dialog box opens.



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 can log out of the Management Web Interface and continue the configuration process later. However, if you log out, you should reopen the

> saved configuration when you resume. Instructions are provided in the section, Loading a Saved Configuration Package into the Configuration Editor.

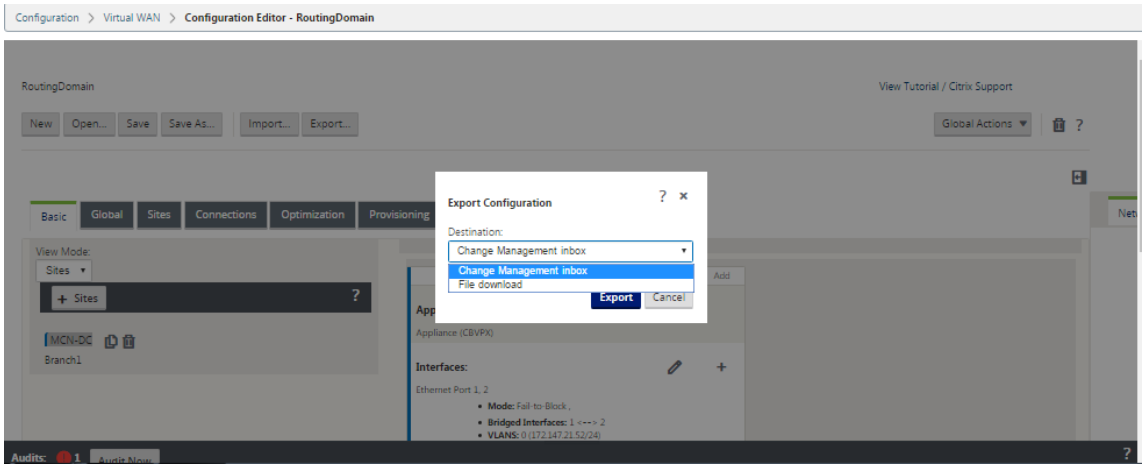
You have now completed the MCN site configuration, and created a new SD-WAN configuration package. You are now ready to add and configure the branch sites. Instructions are provided in setup Branch Sites](/en-us/citrix-sd-wan/11-2/configuration/setup-branch-nodes.html).

Export backup copy of the configuration package

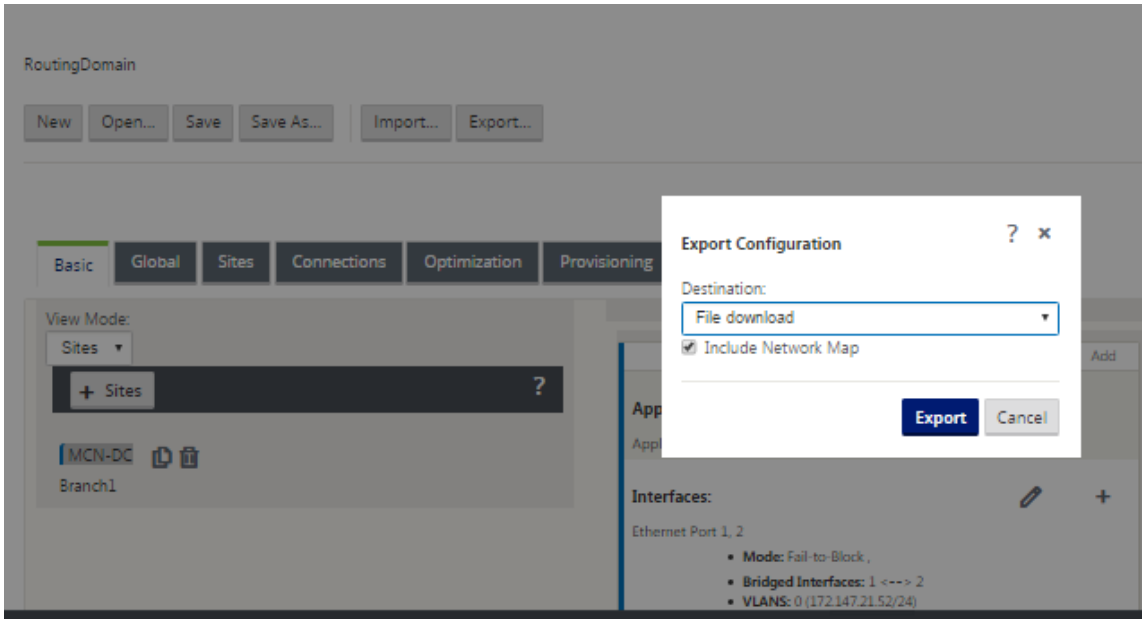
In addition to saving the configuration-in-progress to your appliance workspace, is recommended that you also periodically back up the configuration to your local PC.

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.

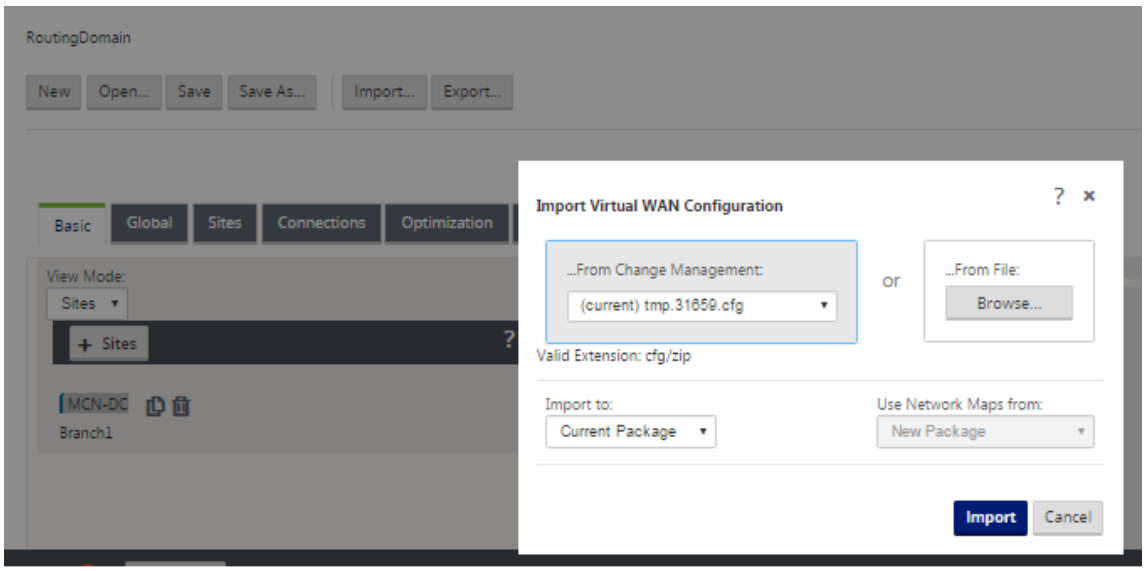
Import backed up configuration package

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**.

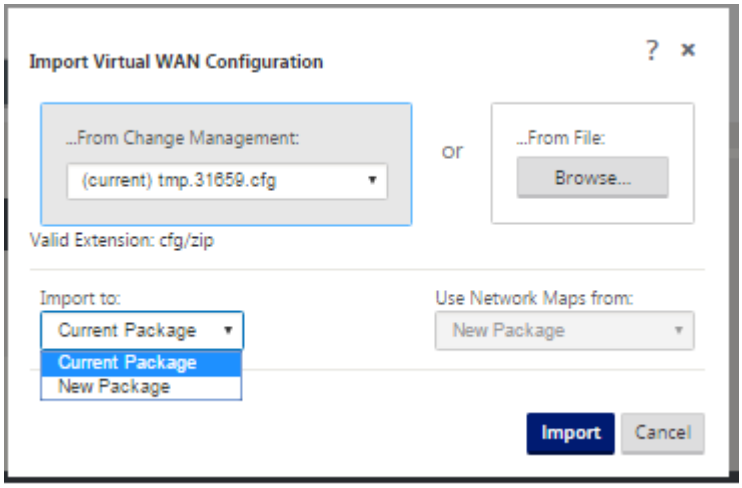
   The **Import Virtual WAN Configuration** dialog box appears.



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.

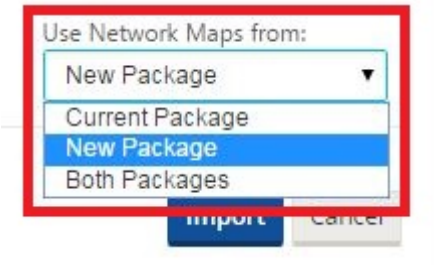


Select one of the following options:

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 is not 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.

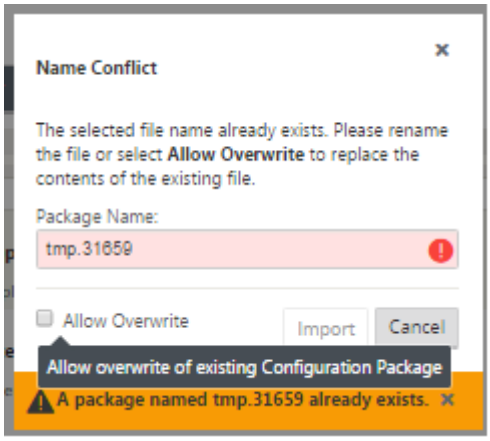


Select one of the following options:

- 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 are 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 are not 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

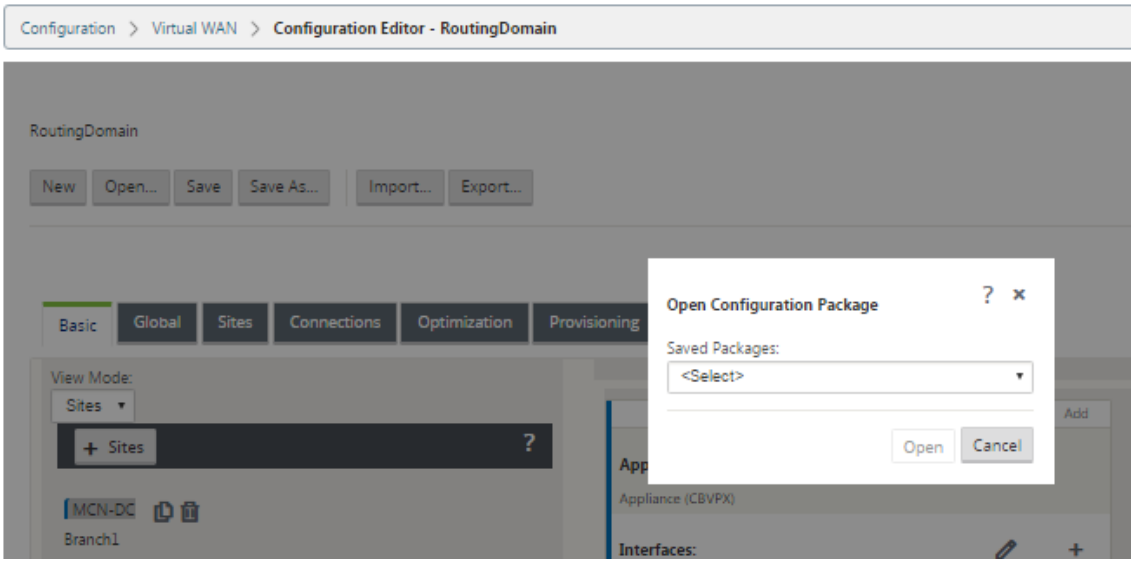
To resume work on a saved configuration package, you must first open the package and load it into the **Configuration Editor.**

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 logged back into the Management Web Interface, the **Configuration Editor** initially opens for a new session, with no configuration package loaded. You can start a new configuration (**New**), open an existing saved configuration (**Open**), or import (**Import)** and then open **(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 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 3 (c) 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.
   b) Click **Next** when processing is complete.
   c) Click **Activate**.
   d) Repeat steps i, ii, iii, iv for the high availability disabled standby MCN appliance.
   e) Enable service on the standby MCN appliance.

> **Note**

> After step 4 (c) 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 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. The RCN's change management process manages the region staging.

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 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 a, band c for the standby appliance.

Setup Branch Nodes

March 12, 2021

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
- Virtual WAN Gateway Mode Deployment Steps (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.

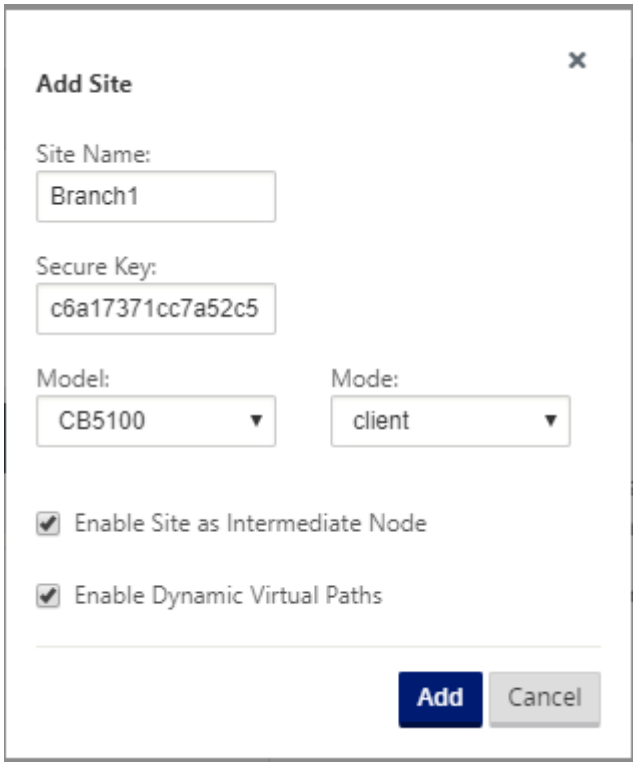
Configure branch node

March 12, 2021

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.



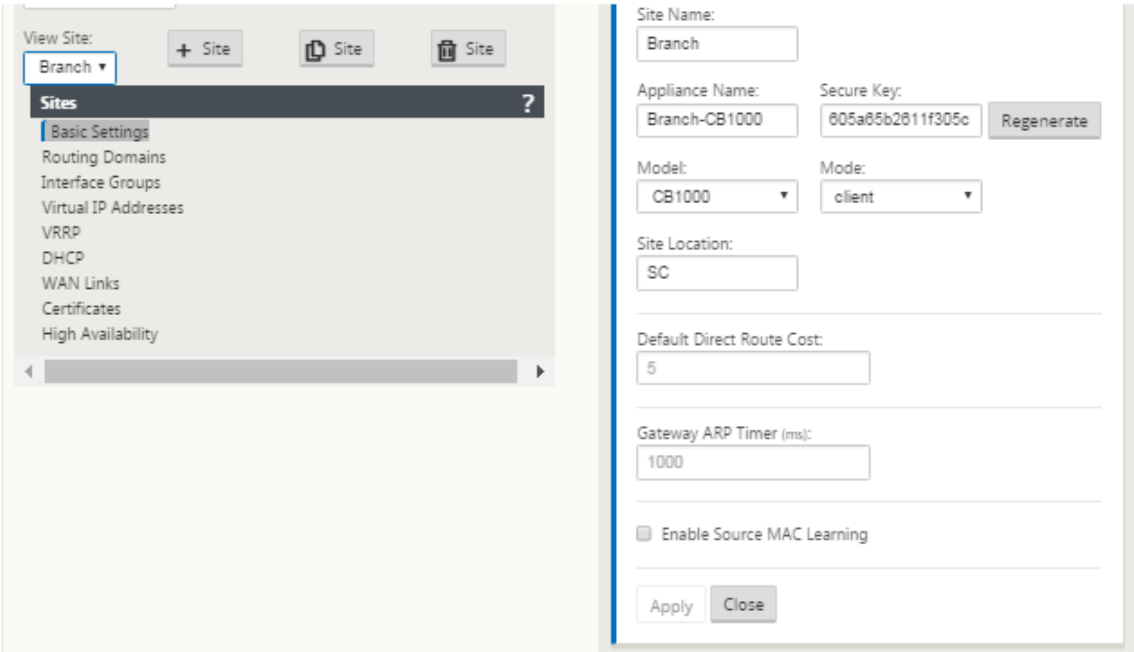
2. Type the following site information.

> **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 prefilled 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.



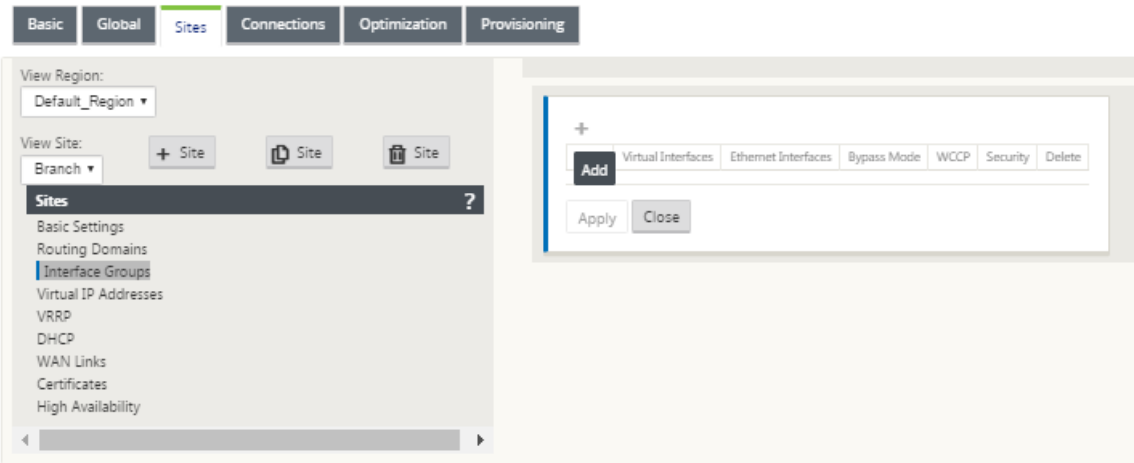
4. Type the basic settings for the site, and click **Apply**.

   The next step is to add and configure the Interface Groups for the new branch site.

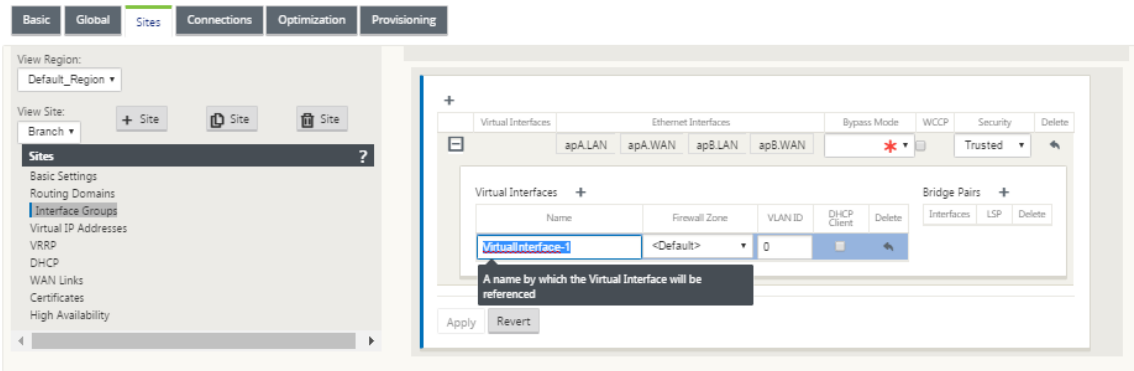
How to configure interface groups for the branch

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).

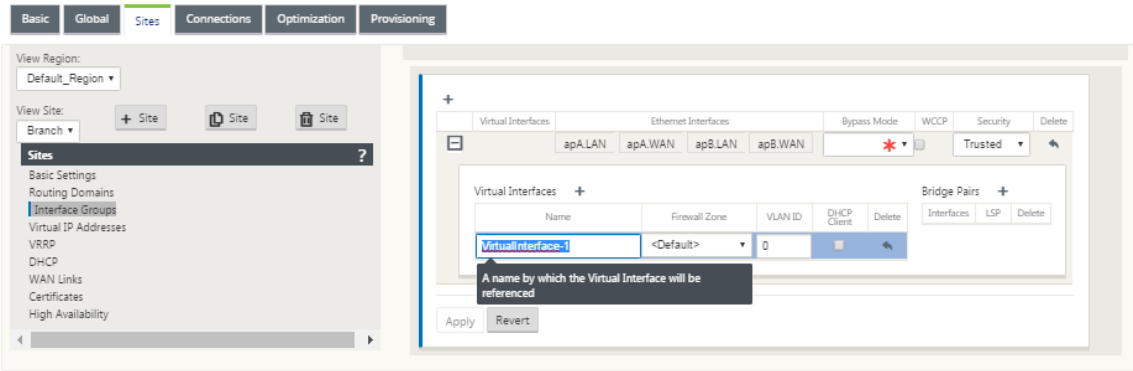
   The **Bypass Mode** specifies the behavior of bridge-paired interfaces in the Virtual Interface Group, in the event of an appliance or service failure or restart. The options are: **Fail-to-Wire**

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 Interfaces are 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 is 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.

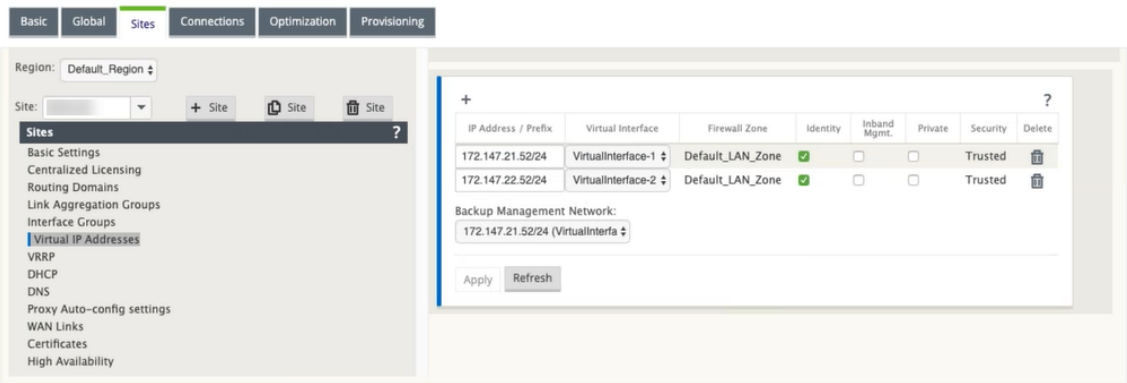
How to configure virtual IP address for the branch site

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. Select **Inband Mgmt** to allow the virtual IP address to connect to management services such as web UI and SSH.

   > **Note:**
   >
   > The interface should be of security type **Trusted** and **Identity** enabled.

6. Select a virtual IP as a **Backup Management Network**. This allows you to use the virtual IP address for management if the management port is not configured with a default gateway.

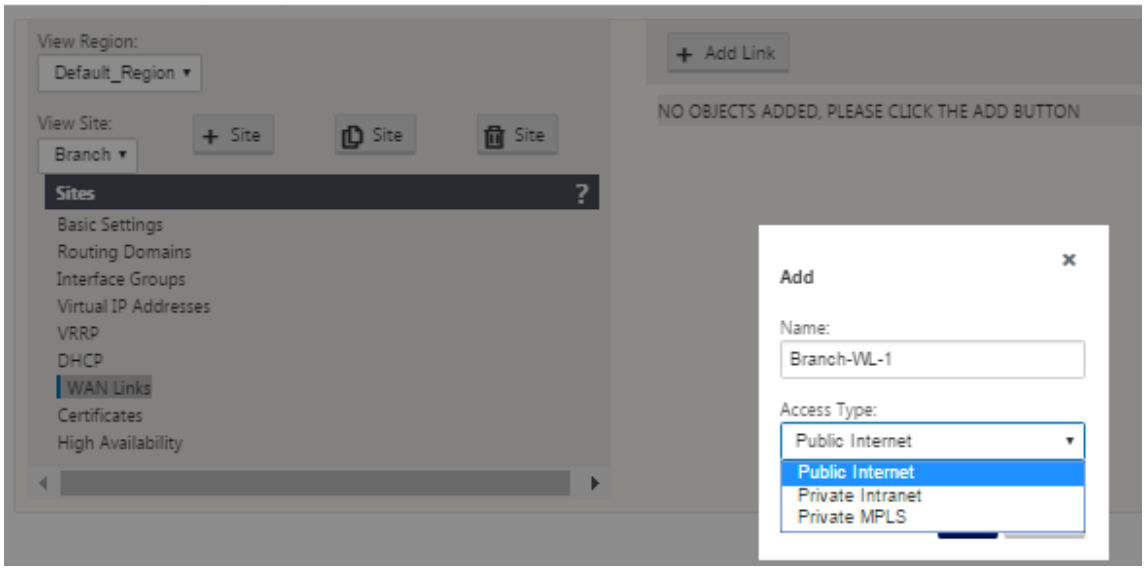


7. Click **Apply**. The address information to the site is added and includes it in the site **Virtual IP Addresses** table.
8. To add more Virtual IP Addresses, click **+** to the right of the **Virtual IP Addresses**, and proceed as above.

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:

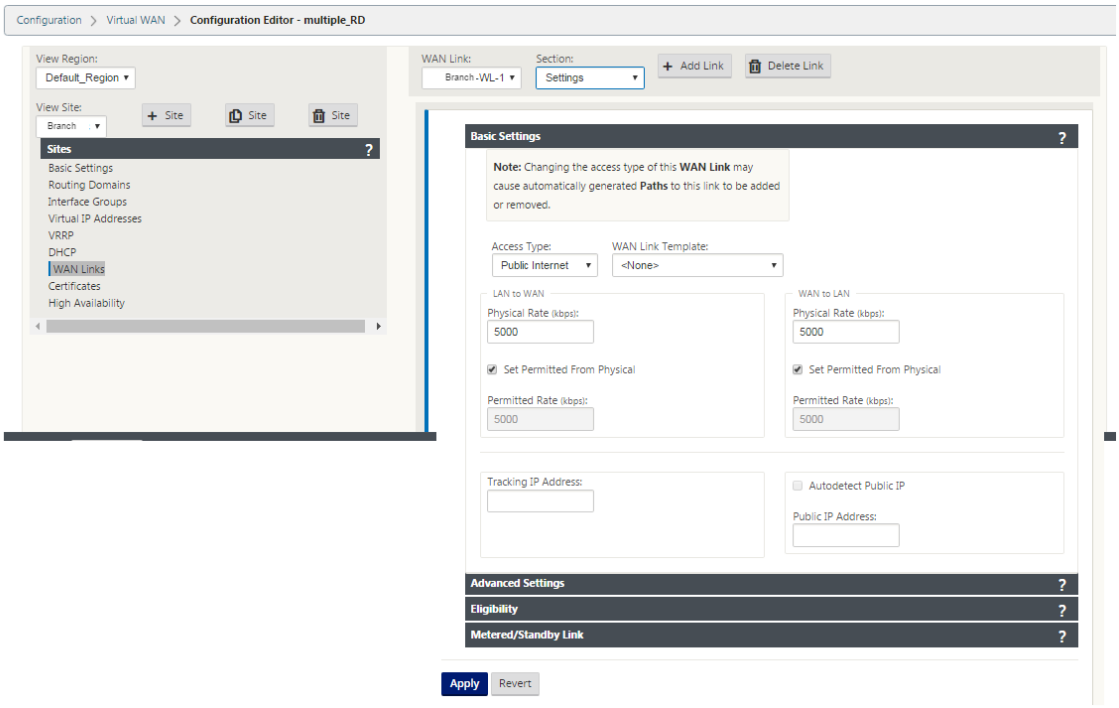
   -WL-<number>

   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.

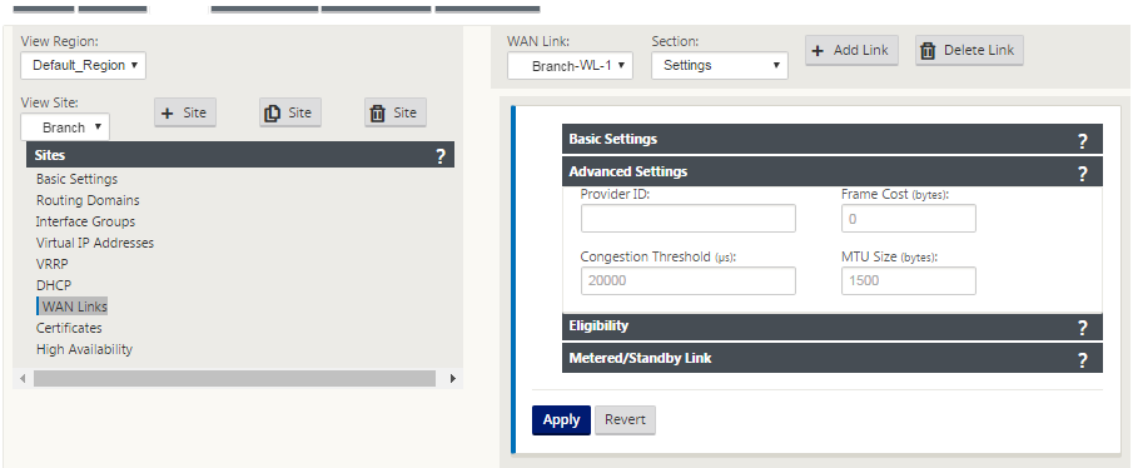


6. Type the link details for the new WAN link. Configure the LAN to WAN, WAN to **LAN** settings.

   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.

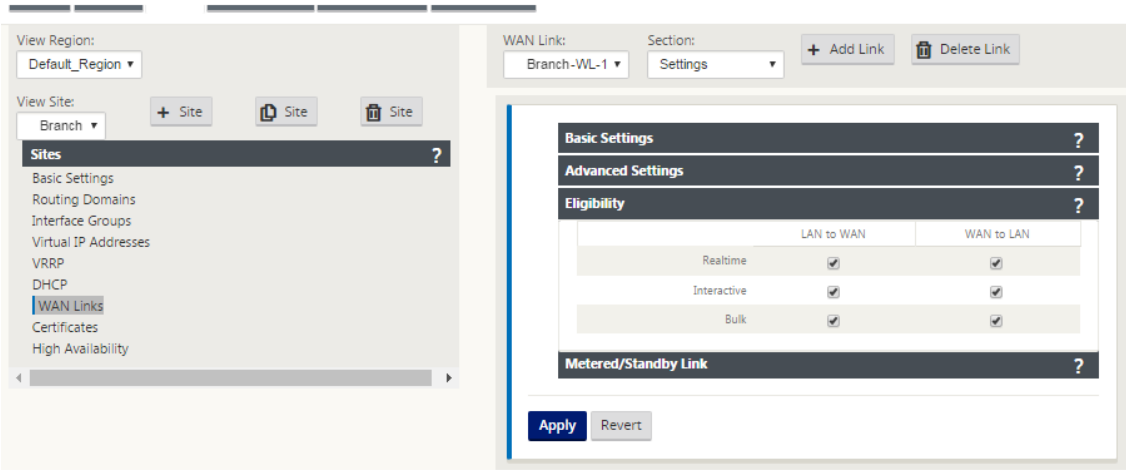
7. Click the gray **Advanced Settings** section bar. This opens the **Advanced Settings** form for the link.



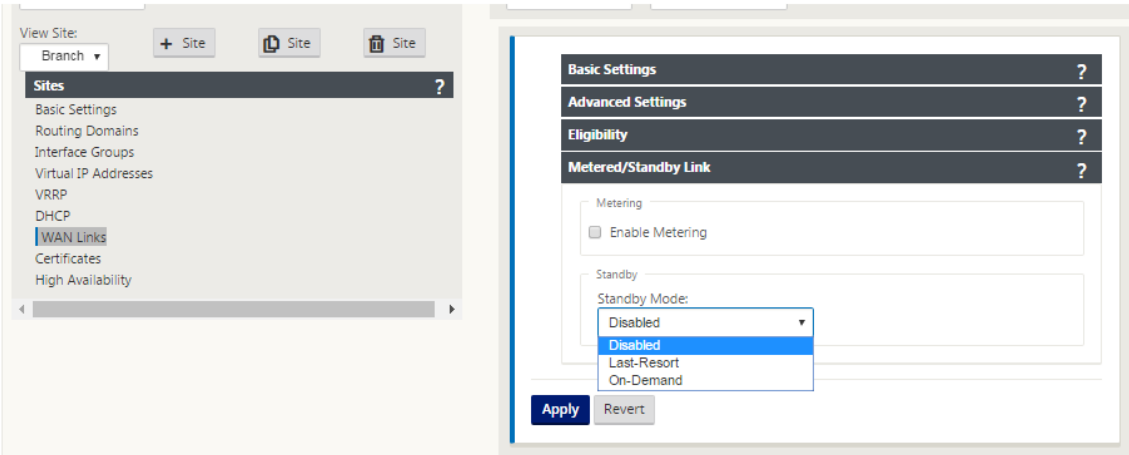
8. Type the **Advanced Settings** for the link.

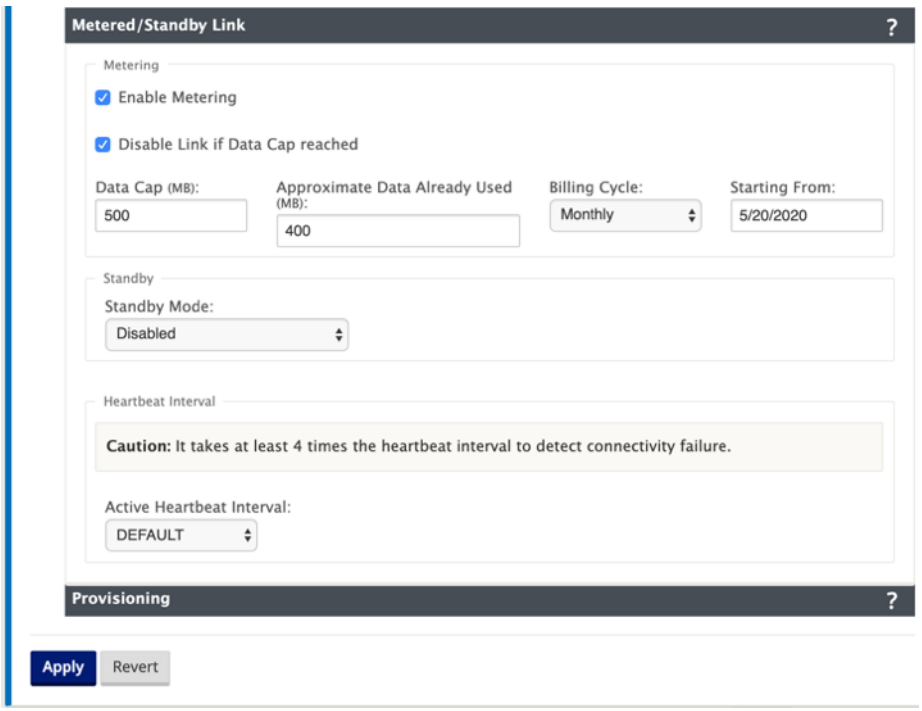
- **Provider ID** –(Optional) type a unique ID number 1–100 to designate WAN Links connected to the same service provider. Virtual WAN uses the Provider ID to differentiate paths when sending duplicate packets.
- **Frame Cost (bytes)** –type the size (in bytes) of the header/trailer added to each packet. 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.





13. Configure the metering settings for the link. Type the following:

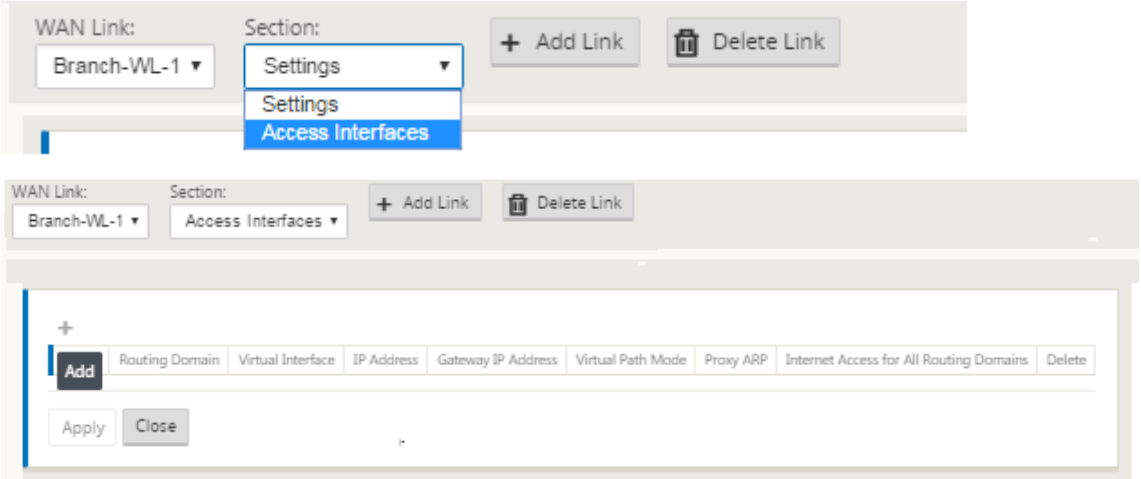
    - **Data Cap (MB)** –type the data cap allocation for the link, in MB.
    - **Billing Cycle** –Select either **Monthly or Weekly** from the drop-down menu.
    - **Starting From** –type the start date of the billing cycle.
    - **Set Last Resort** –Select this to enable this link as a link of last 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.

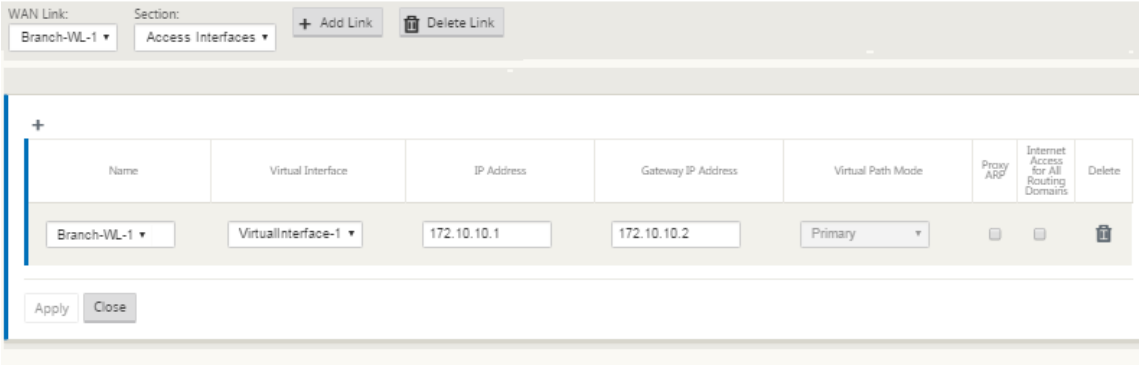
    > **Note**
    >
    > An option to auto-provision shares by considering remote bandwidth is added to configure WAN links. The Set Provisioning using Remote Bandwidth option enables users with large networks and diverse bandwidth configurations to manage bandwidth provisioning for datacenter sites in a dynamic way.

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 is 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.

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

   - **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

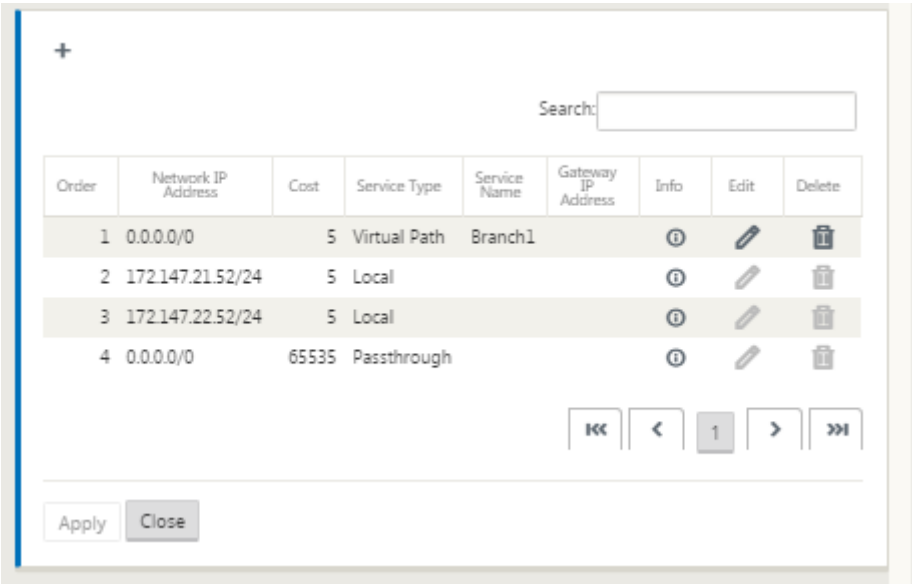
type GRE Tunnel, the gateway must reside in one of the tunnel subnets of the local GRE tunnel.

  - **LAN IPsec Tunnel** –This service manages IP traffic destined for IPsec tunnel.
  - **Inter Routing** - This service enables route leaking between Routing Domains within a site or between different sites. This eliminates the need for an edge router to handle route leaking.

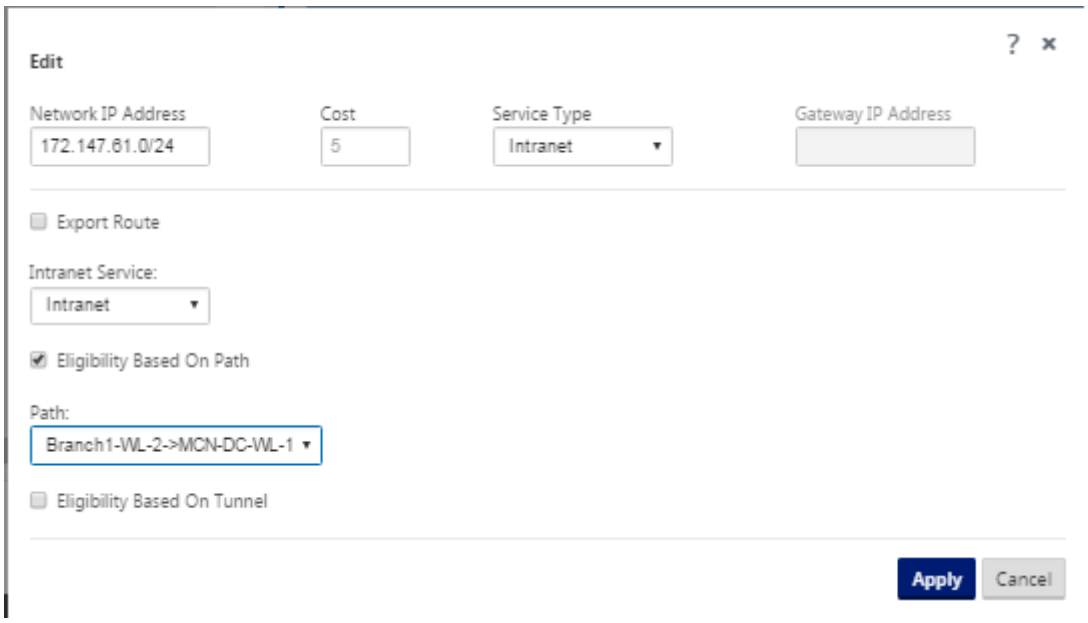
- **Gateway IP Addres**s –type the Gateway IP Address for this route.
- **Eligibility Based on Path** (checkbox) –(Optional) If enabled, the route does not receive traffic when the selected path is down.
- **Path** –This specifies the path to be used for determining route eligibility.

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.



You can also edit configured routes as shown below.



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 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 Citrix 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.

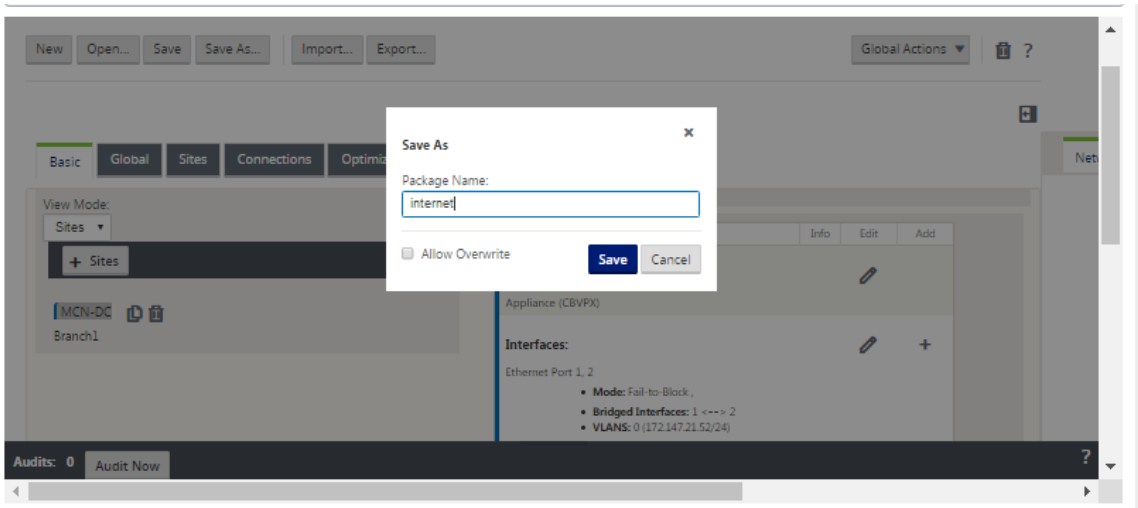
Save configuration

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.
5. Upload the package downloaded earlier. Click **Next** and then click **Activate**.
6. Repeat steps 4 (a) and 4 (b) for the standby appliance.

Clone a branch site (Optional)

March 12, 2021

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 more 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.

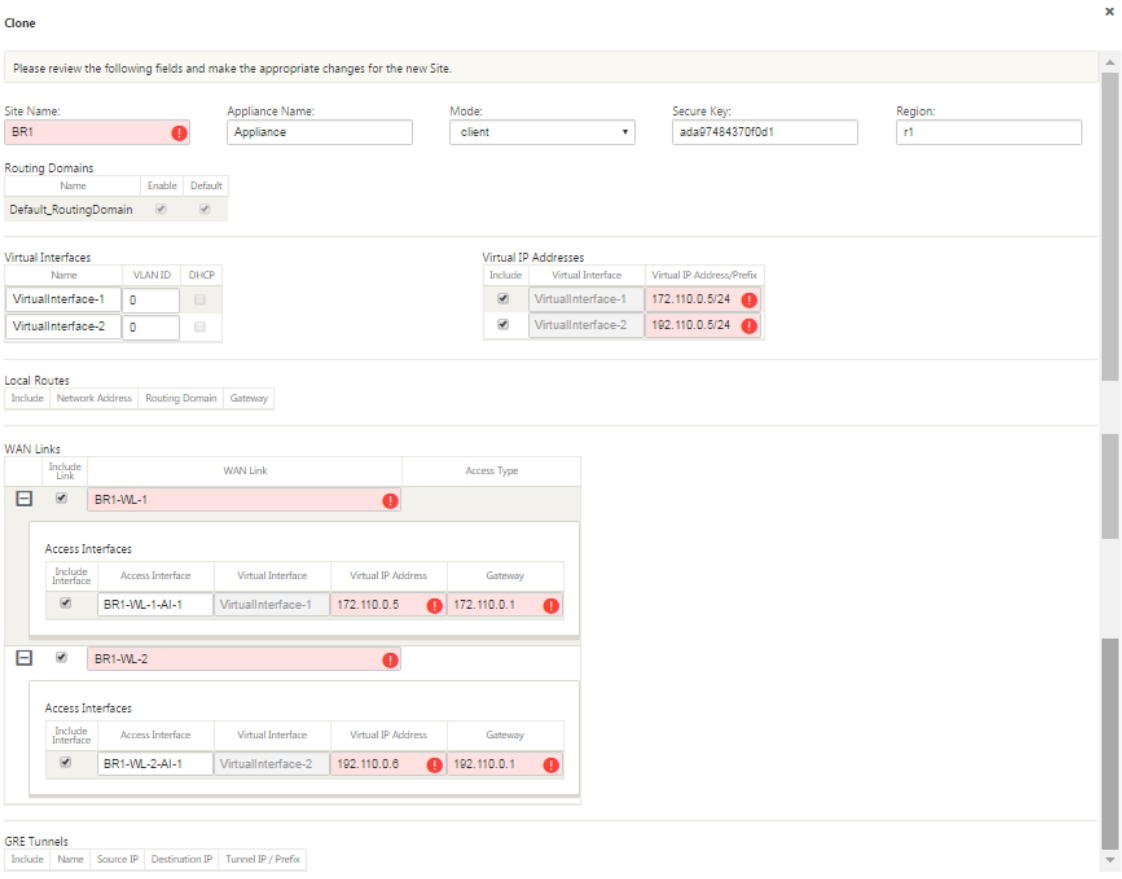
To clone a site, do the following:

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.



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. Usually, 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 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 are not 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

March 12, 2021

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.

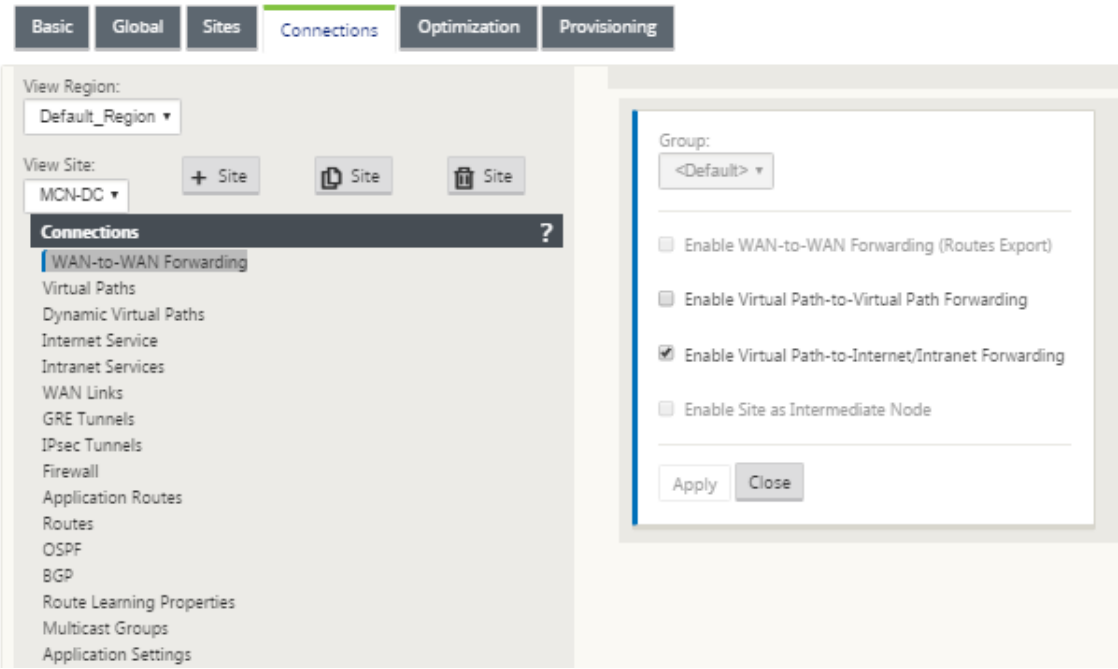
Configuring the virtual path service between the MCN and client sites

March 12, 2021

The next step is to configure the Virtual Path Service between the MCN and each of the client (branch) sites. To do this, you use the configuration forms and settings available in the **Connections** section configuration tree of the **Configuration Editor**.

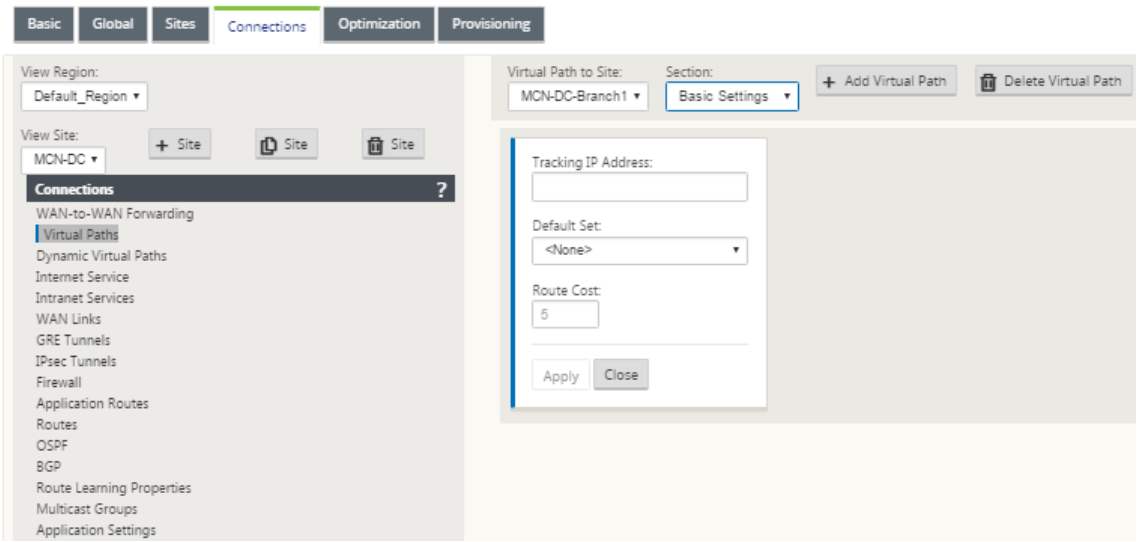
To configure the Virtual Path Service between the MCN and a client site, do the following:

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.

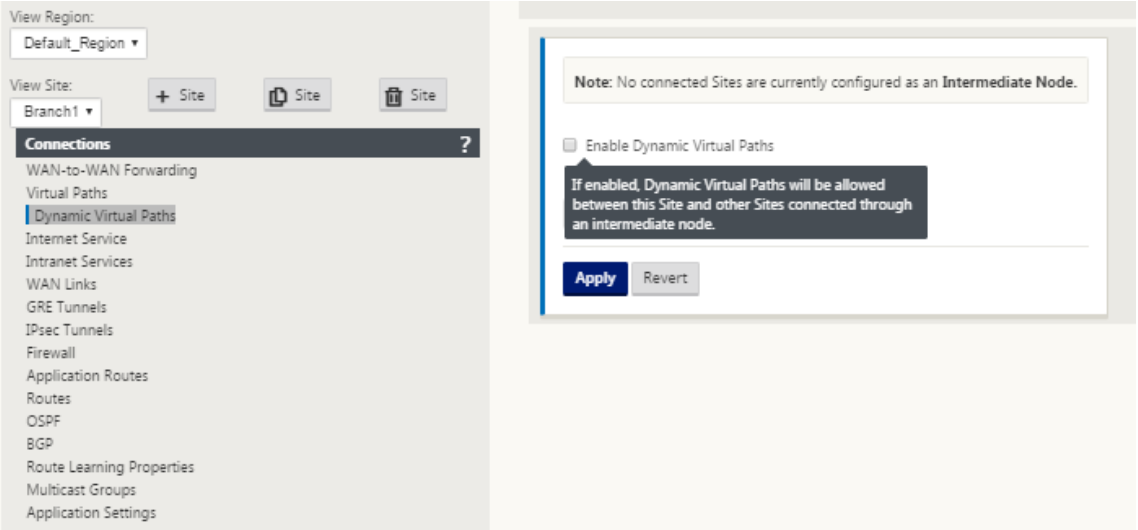


> **Note**
>
> WAN to WAN Forwarding Groups are supported only within a Region and not across Regions. You can use Regions to segregate networks instead of relying on WAN to WAN forwarding groups.

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 following figure shows an example Virtual Paths section for an MCN site.



The following 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>

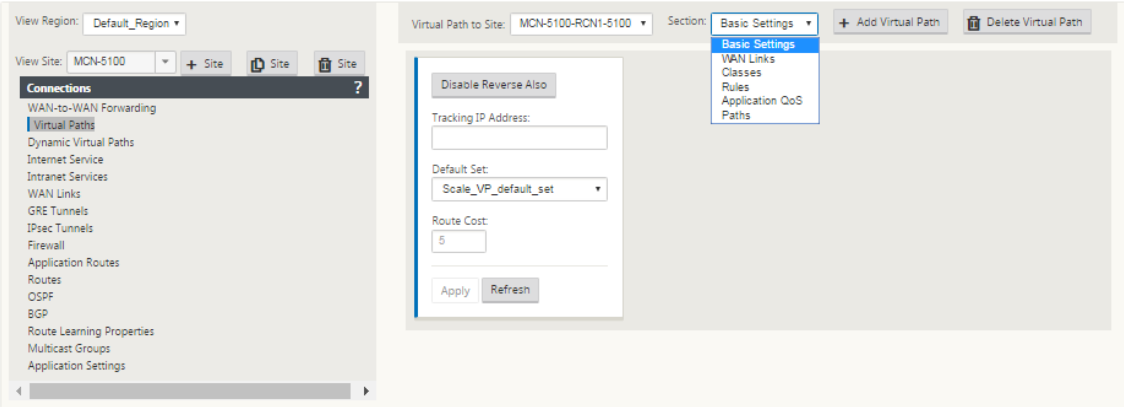
  Where:

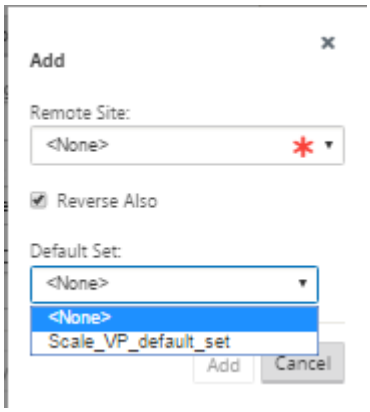
  MCN_Site_Name is the name of the MCN for this Virtual WAN.

  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 as follows.



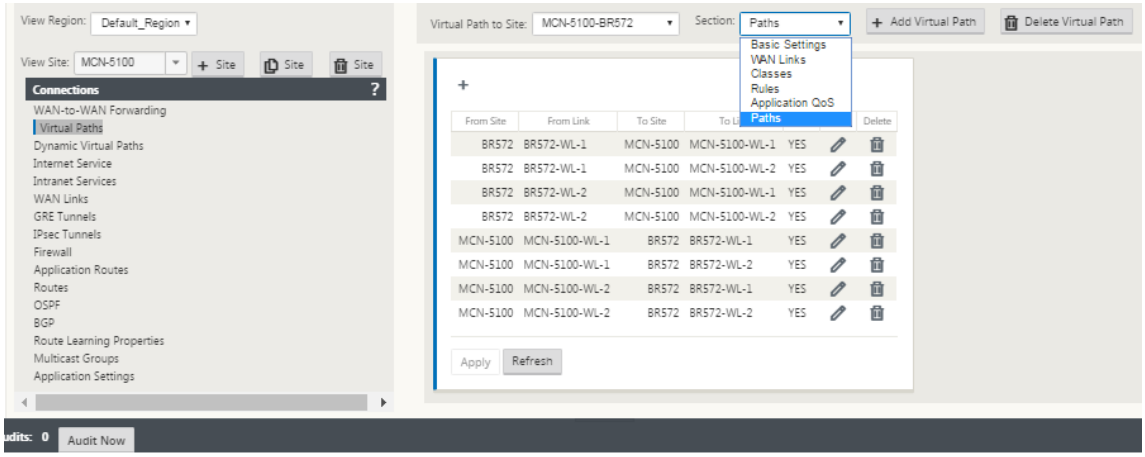


4. Click **+ Add Virtual Path** next to the name of the static Virtual Path in the **Virtual Paths** section. This reveals more configuration for the static Virtual Path:

   a) 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.
   b) **Reverse Also -** When enabled, classes, and rules are mirrored on both sites the virtual path.
   c) **Default Set** - Name of the Virtual Path default set that are used to populate rules and classes for the virtual path on the site.

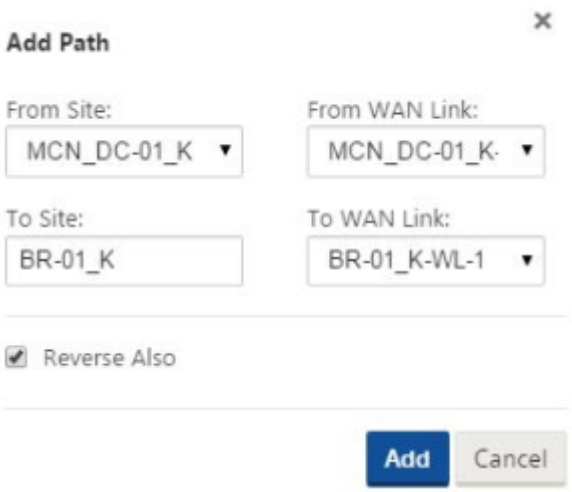
   The following figure shows an example MCN static Virtual Path branch and child branches.

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).



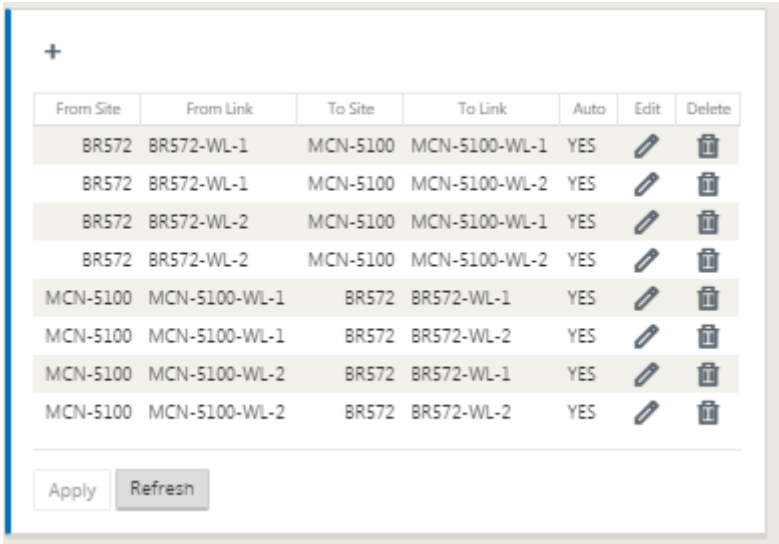
7. Specify the source and destination site information for the new Virtual Path.
8. Specify the following from the available drop-down menus:

> **Note**
>
> Depending on how the WAN links are configured for the sites, some fields are 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.

9. 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		

10. 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.
11. Configure the settings for the Virtual Path, or accept the defaults.

    The **Paths** configuration form contains the following settings:

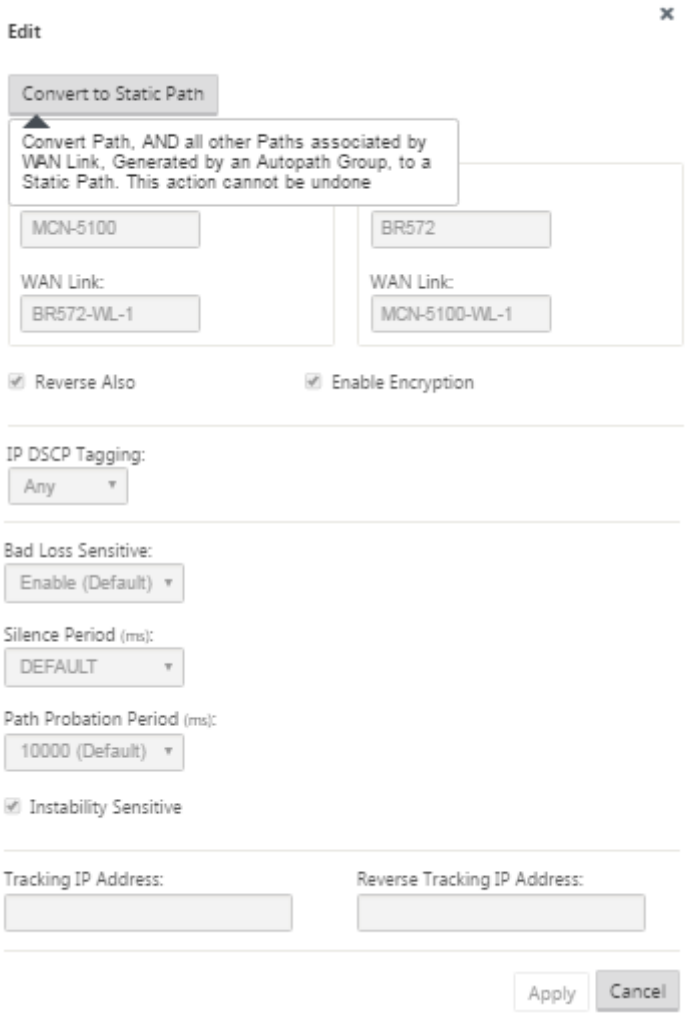
    - **From Site** section:
      - **Site** –This is the source site for the Virtual Path. For the required static Virtual Path, this is configured as the MCN site by default.

  - **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 are 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 more 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 10,000 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.

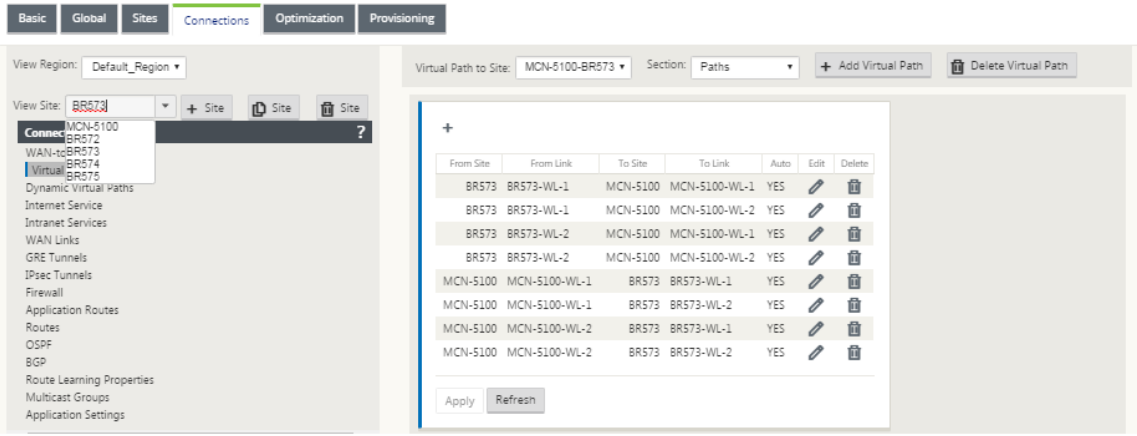
12. Click **Apply**. This reveals that the two new **From Site** and **To Site** Virtual Paths between the MCN and the client site have been added to the Paths table.



13. 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 more paths between clients. Instructions are provided in the remaining steps, below.

14. Select a client site branch from the **View Site** drop-down menu. The configuration for client site branch in the **Connections** tree opens.

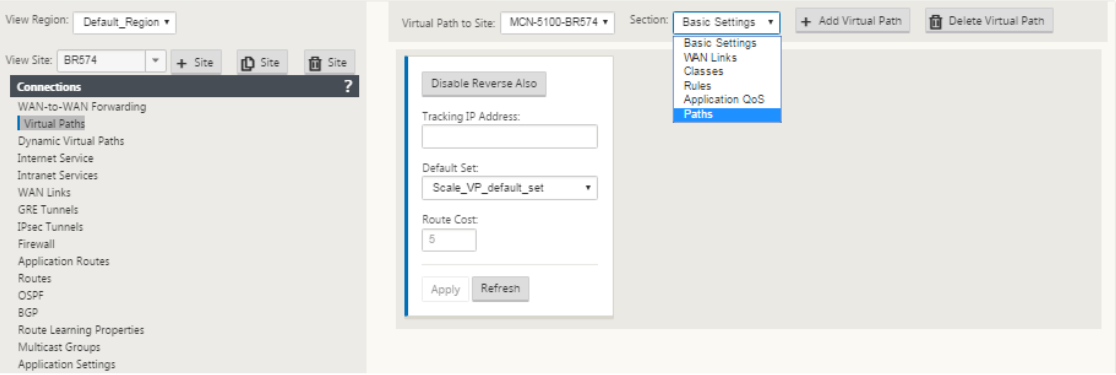


15. Navigate to the **Paths** settings configuration form for any client site Virtual Path you want to configure.

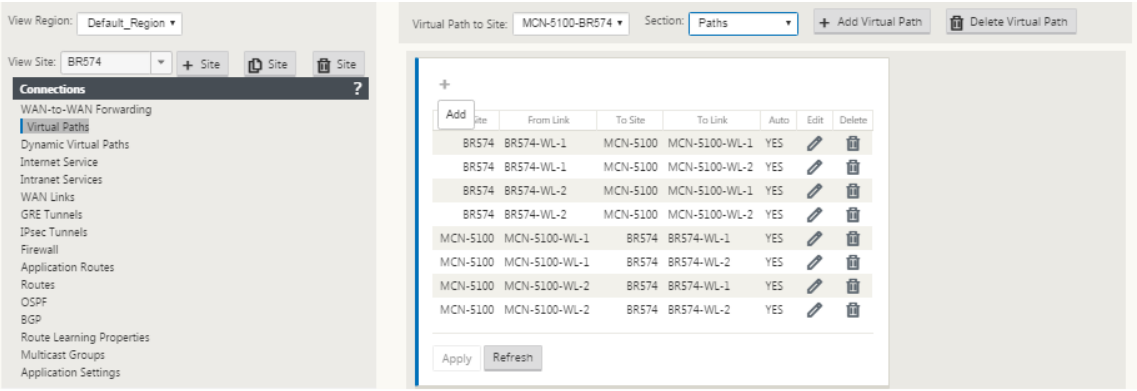
    To navigate to the **Paths** settings form for the client site, do the following:

16. Select **Paths** from the **Section** tab of branch page for the client site.

    The following figure shows an example **Paths** settings form for the new **From Site** path added in the previous steps.



17. 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.



This completes the basic configuration of the Virtual Paths between the client sites and the MCN.

> **Note**
>
> For information on configuring more 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 currently, 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 Premium (Enterprise) Edition** – The Premium (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 Installing the SD-WAN Appliance Packages on the Clients.
- **SD-WAN Edition** – This Edition does not include the WAN Optimization features. You can now proceed directly to Installing the SD-WAN Appliance Packages on the Clients.

Deploy MCN Configuration

March 12, 2021

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.

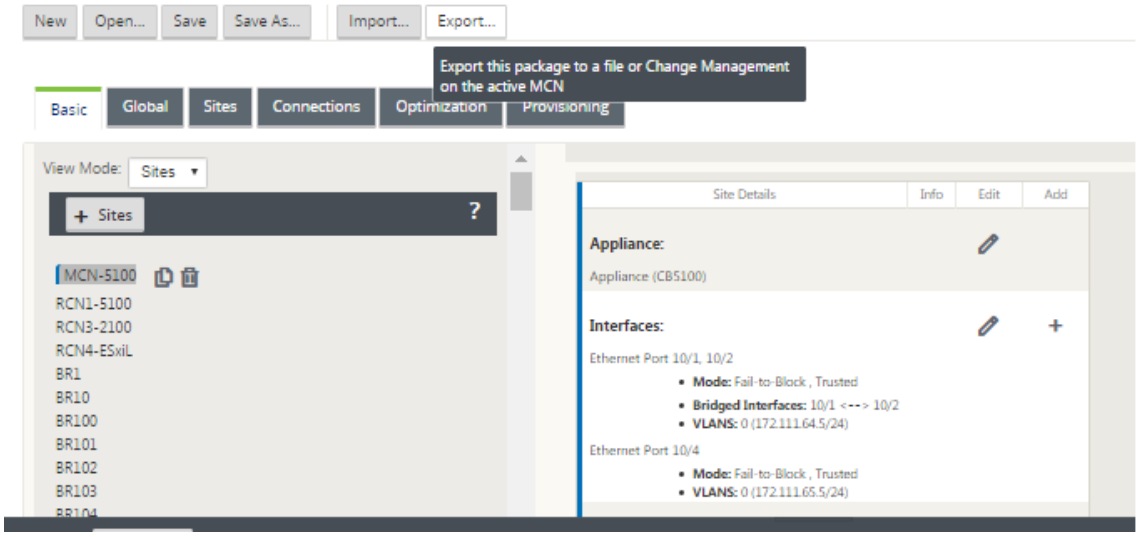
Perform MCN Change Management

March 12, 2021

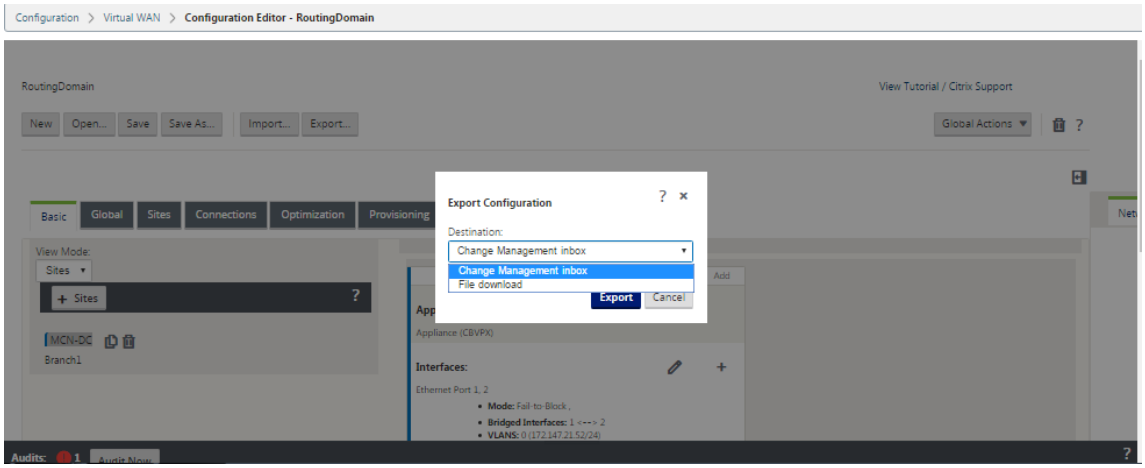
Before you can generate the appliance packages, you must first export the completed configuration package to the Management Web Interface **Change Management** system.

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

March 12, 2021

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. 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. Therefore, 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 can do so now. For information on acquiring and downloading the software, see the section Acquiring the SD-WAN Software Packages

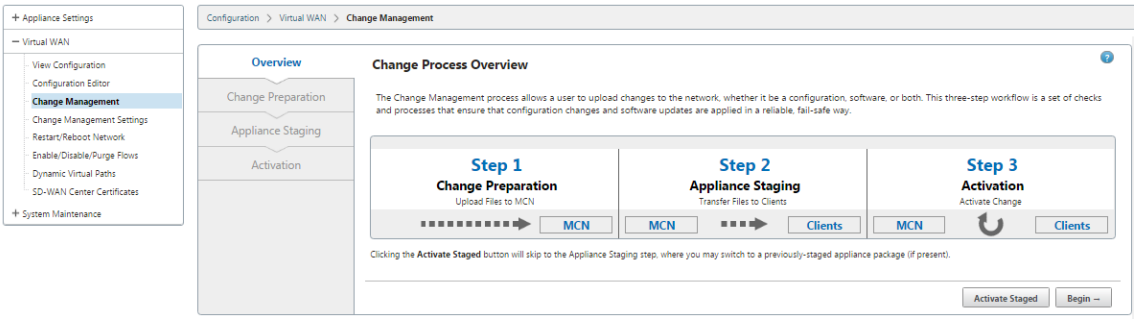
To upload and install the package and configuration to the MCN, do the following:

1. Log into the Management Web Interface on the MCN appliance.

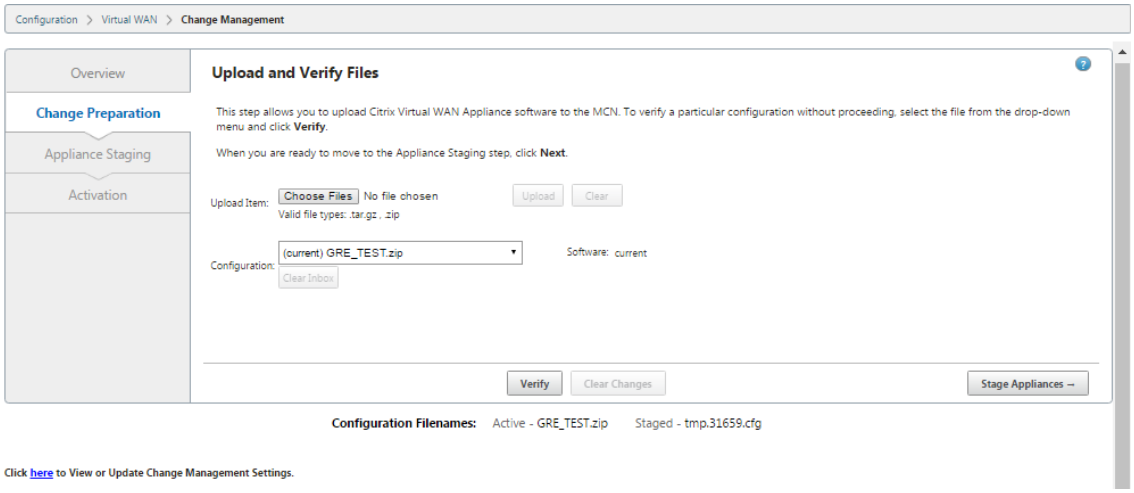
   > **Note**

> You are 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**. The first page of the **Change Management** wizard, the **Change Process Overview** page is displayed.

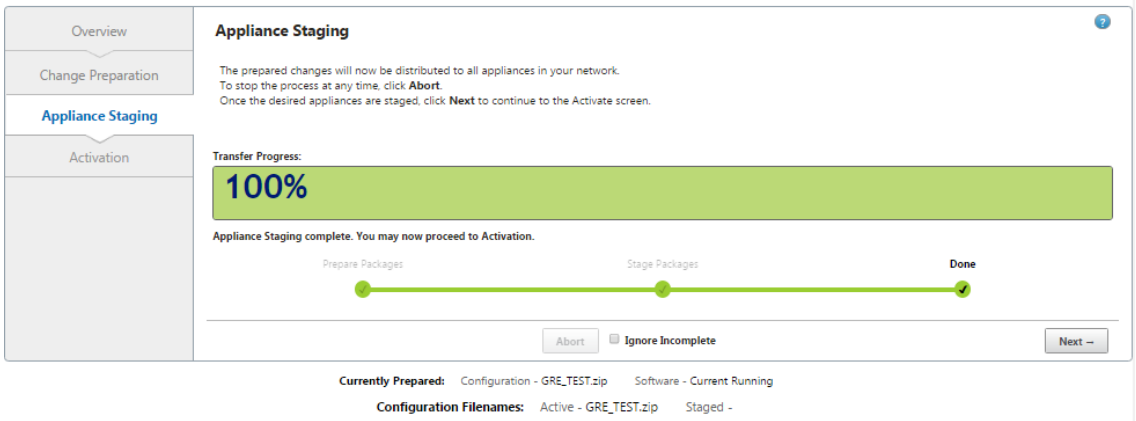


4. Click **Begin**. The **Change Preparation** page for uploading and verifying that the specified configuration and software packages is displayed.



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 an SD-WAN software package to upload.
   b) Select an SD-WAN software package, and click **OK**.
   c) Navigate to the SD-WAN software packages you downloaded earlier to the local PC, and select the package to upload.
   d) Click **Upload**.
   e) Repeat steps (i) through (iii) for each of the SD-WAN software packages required for your network.

6. In the **Configuration** field drop-down menu, select the new configuration package that you just exported to **Change Management**.
7. Click **Stage Appliance**. Appliance staging 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.

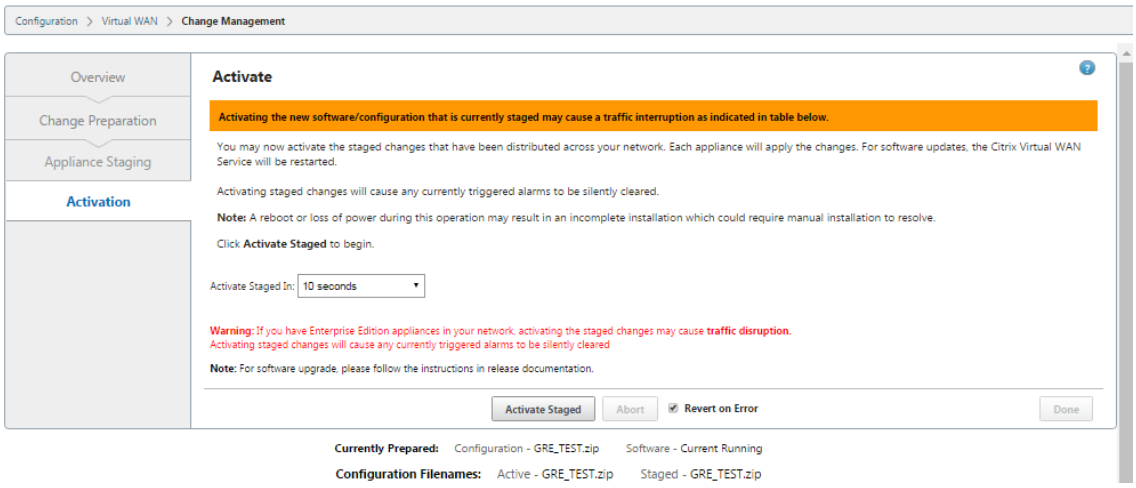


When the staging operation completes, the Site-Appliance** table is populated with the newly staged Appliance Packages information.

> **Note**
>
> If this is an initial deployment, only the MCN is updated and staged now. 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.
>
> From Citrix SD-WAN 11.2.2 release onwards, if the site is shown as **not connected** in the change management page, then it is marked as failed during the staging process and the progress bar completes to 100%. Once the **not connected** site is back online and connected, MCN autocorrects it.

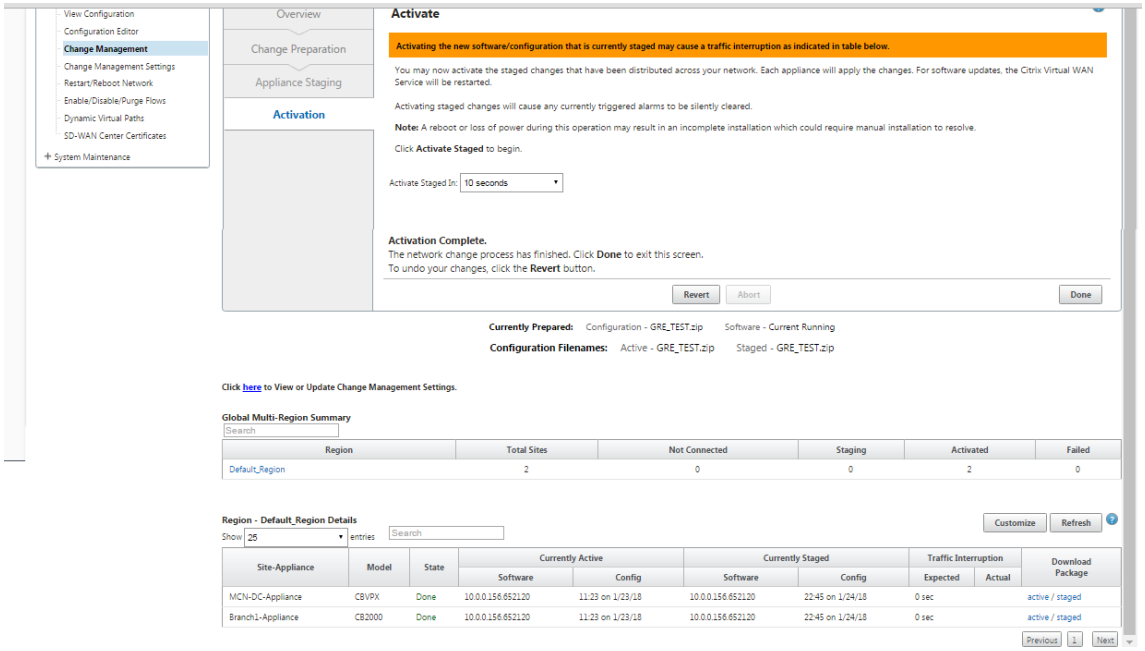
> For releases prior to Citrix SD-WAN 11.2.2, select **Ignore incomplete** when adding more sites to the network or if the site is in **not connected** state. This indicates that only the connected sites and the MCN get updated and staged. Once the site that was in **not connected** state comes back to connected state, it automatically gets staged and updated by MCN as part of auto-correction.

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**.



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, the new configuration and the appropriate Appliance Package on the MCN appliance is activated. 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.



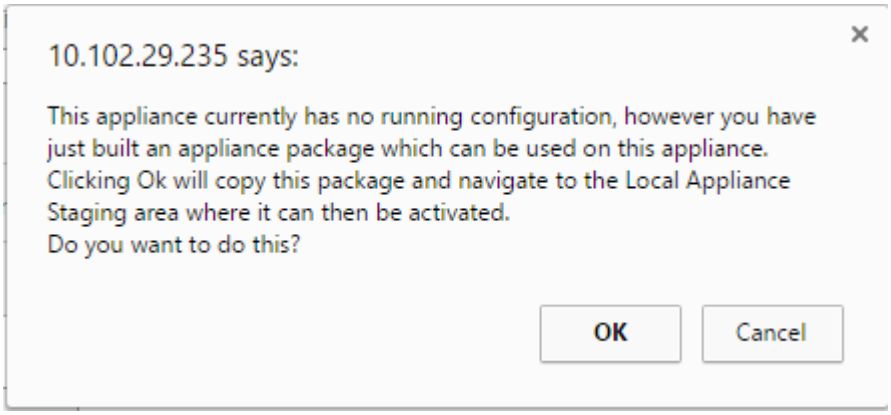
When the activation completes, an **Activation complete** status message appears, and the **Done** button is enabled. In addition, the **Configuration Filenames** status line (above the table) now displays the name of the newly activated package in the **Active** field.

11. 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, proceed to Connecting the Client Appliances to Your Network.
    - If you are activating an initial configuration, the new configuration package is not activated at this point, and there are more steps you must perform. The next step is to copy the configuration package to the Local Appliance Staging area, in preparation for staging and activating the configuration package on the MCN.

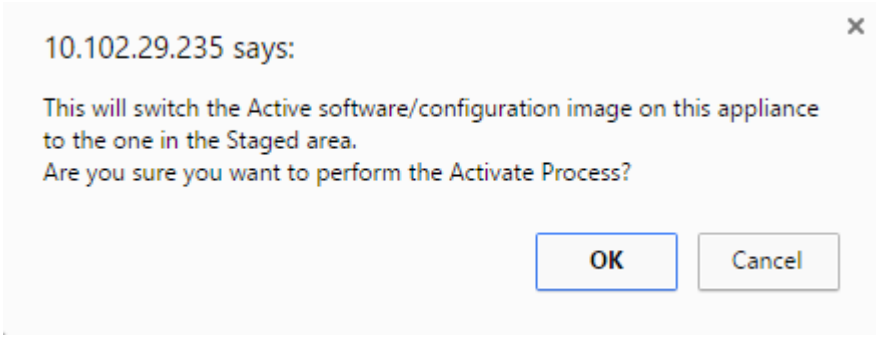
    Do the following:

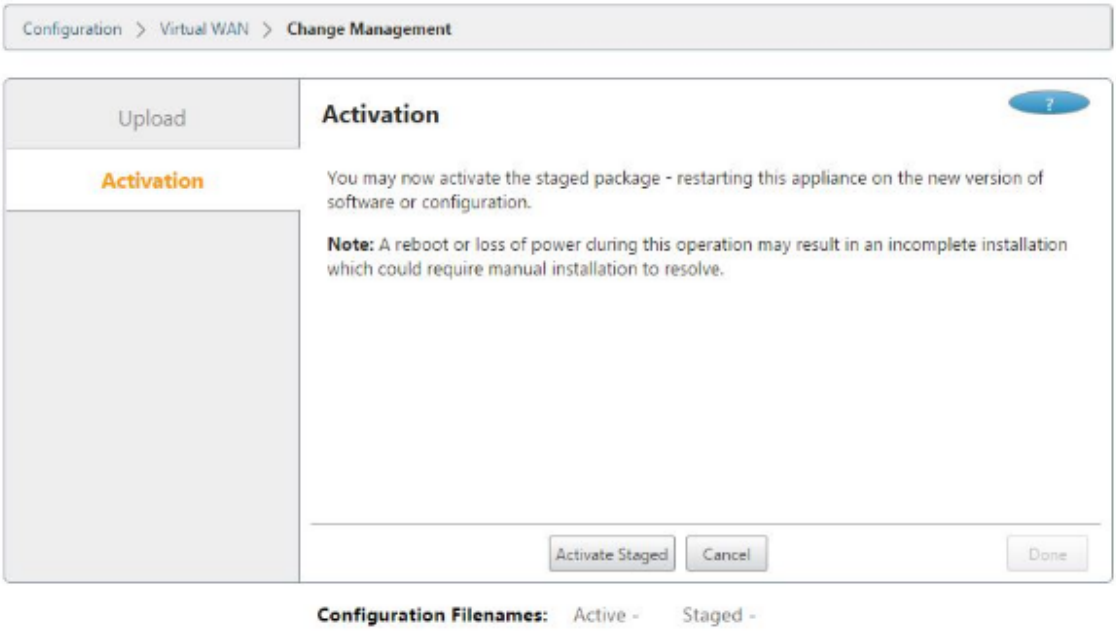
12. Once you click **Activate Staged**, the following message appears.



13. Click **OK**.
14. Click **Activate staged**.

    This displays a dialog box asking you to confirm the activation operation.





15. 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.

16. Click **Done**. This proceeds to the Management Web Interface **Dashboard** page, where you can view the activation results.

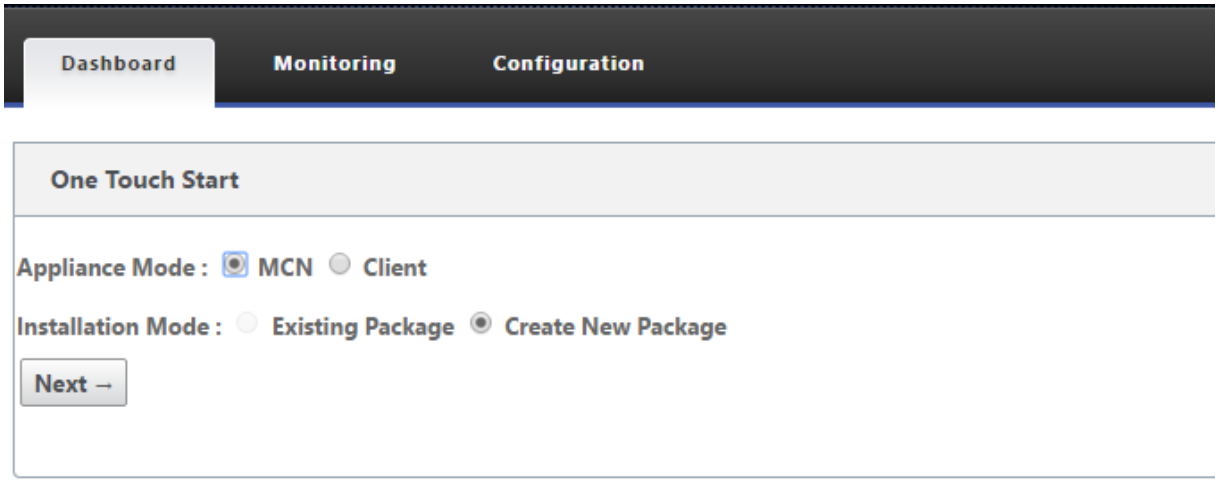
You have now completed the preparation of the SD-WAN Appliance Packages on the MCN. Proceed to (/en-us/citrix-sd-wan/11-2/configuration/connecting-client-appliances-to-network.html) connecting the Client Appliances to Your Network.

> **Tip**
>
> The **Change Management** wizard allows you to search the site-appliance table. This allows you to 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 gives you a list of all the sites in that state.

One Touch Start

March 12, 2021

Once touch start allows you to easily and quickly configure your SD-WAN appliance as a Client on first time startup.
The one touch start option is displayed when your appliance boots up for the first time.



> **Note**
>
> For configuring the SD-WAN appliance as an MCN, create a configuration or import an existing

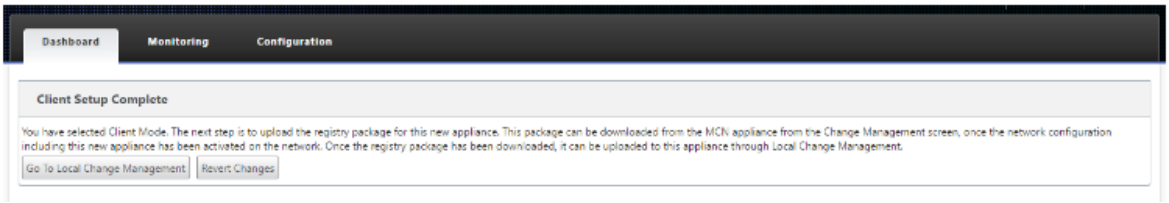
> configuration using the **Configuration Editor**. For more information see, Preparing the SD-WAN Appliance Packages on the MCN

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 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

March 12, 2021

For an initial deployment, or if 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. Connect 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, do the following:

   a) Set up the SD-WAN appliance hardware and any SD-WAN VPX virtual appliances (SD-WAN VPX-SE) you are 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. Then connect 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. Then connect 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

March 12, 2021

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.

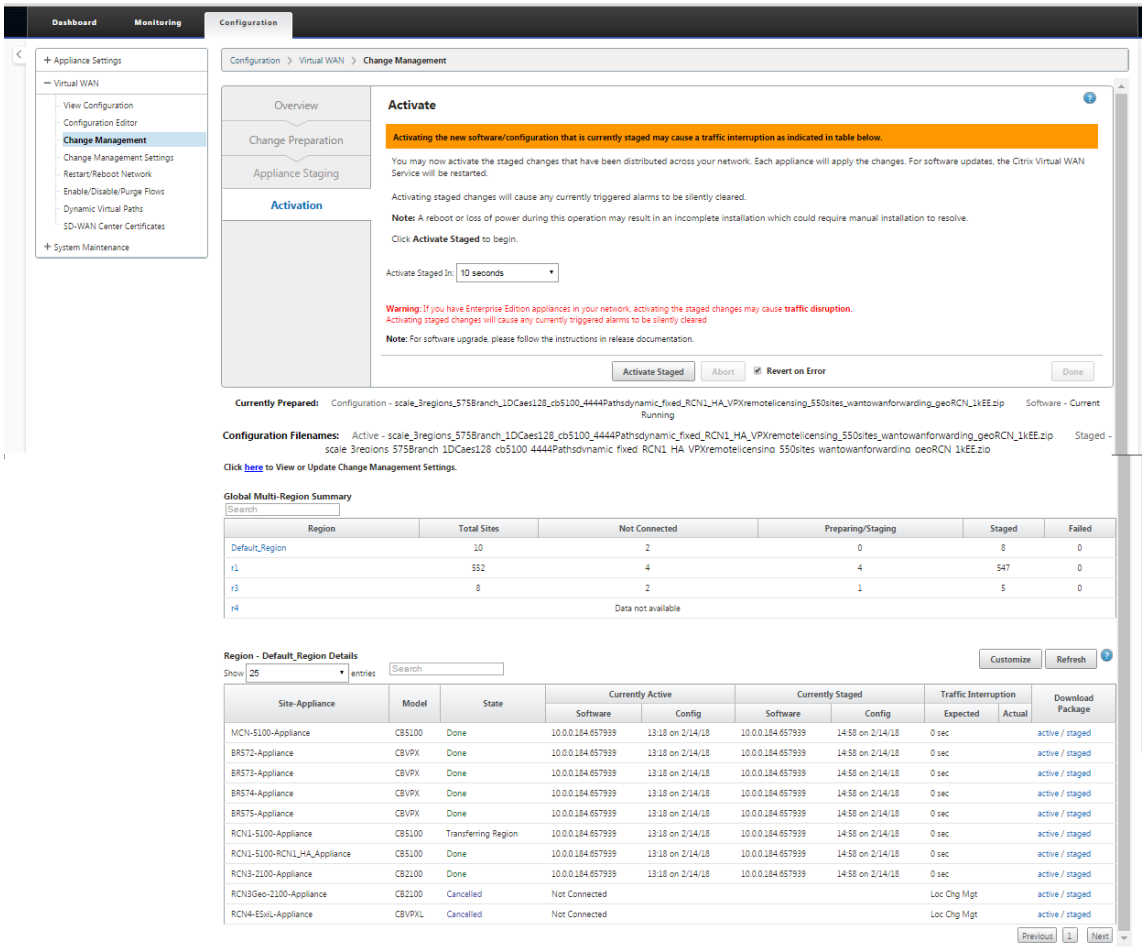
To install and activate the software and configuration on a client appliance, do the following

1. On a connected PC, open a browser and log on to 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. 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).



At the bottom of this page, you can 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 a**ppliance packages.

> **Note**
>
> If this is an initial installation, the **Active** links are not yet available, and are replaced by a plain text marker **none**.

3. 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.

4. Select the download location and click **OK.**

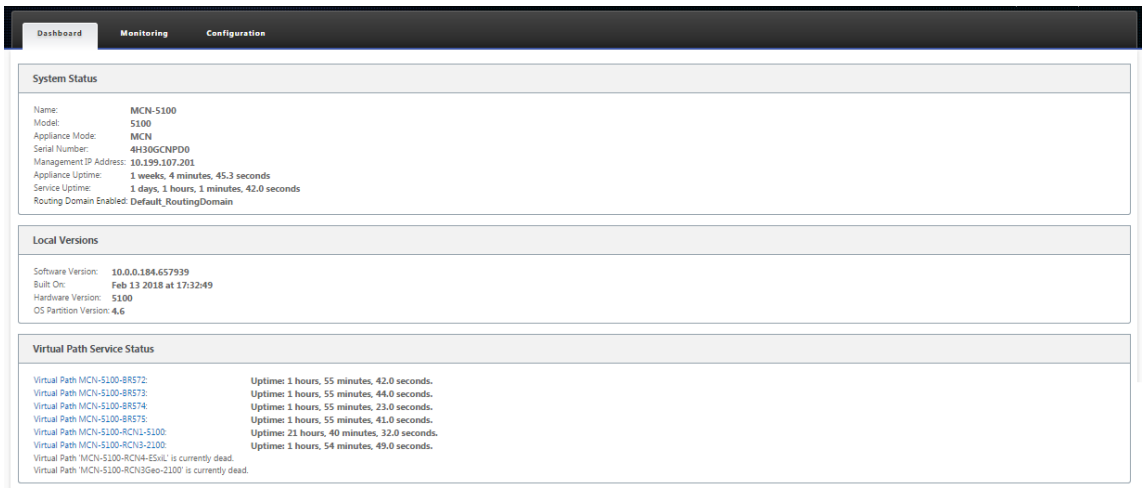
5. (Optional.) After the download completes, log out of the MCN Management Web Interface.
6. Open a browser, and enter the IP Address for the client to which you want to upload the appliance package .zip file.

   > **Note**
   >
   > Please ignore any browser certificate warnings for the Management Web Interface.

   This opens the Citrix SD-WAN Management Web Interface Login screen on the client appliance.

7. Enter the Administrator user name and password and click **Login**. The default Administrator user name is *admin*. The default password is *password*.

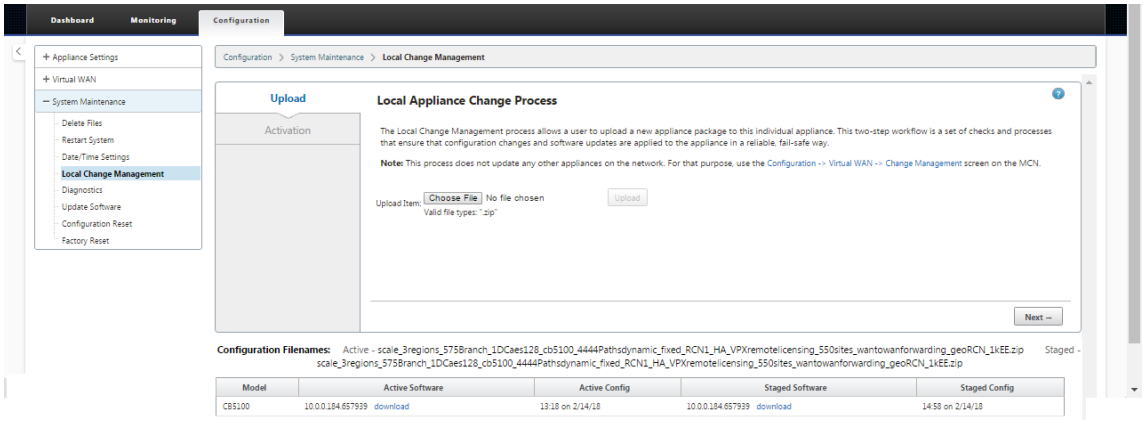
   This displays the Management Web Interface **Dashboard** page for the client appliance.



> **Note**
>
> If this is an initial installation, or if you have temporarily disabled the Virtual WAN Service on this appliance, you can see a goldenrod Audit Alert icon with a status message indicating that the Virtual WAN Service is 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.

8. Select the **Configuration** tab.
9. 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.



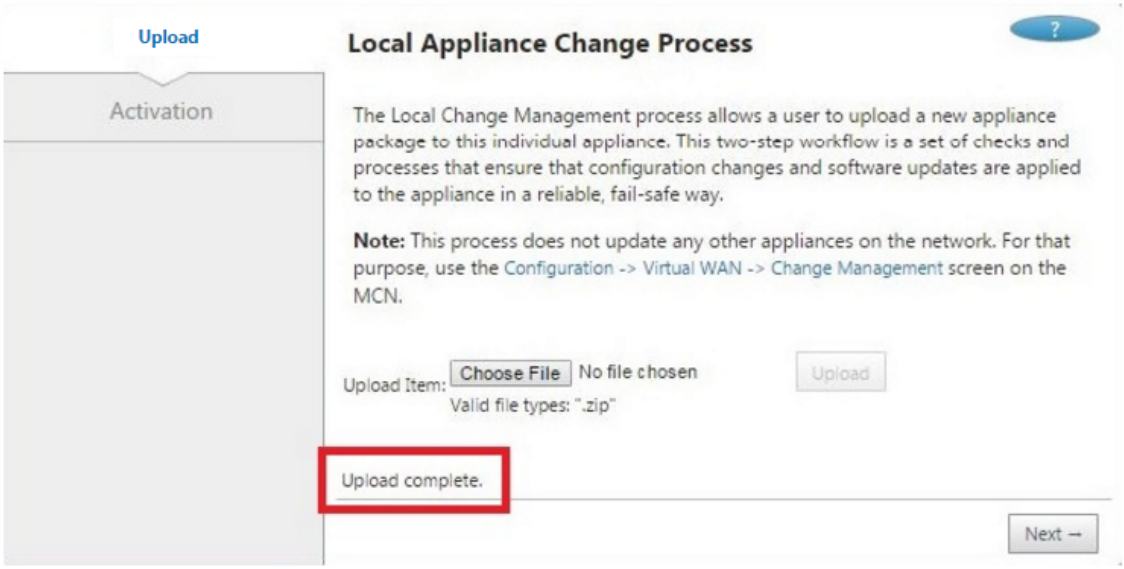
10. Click **Choose File** next to the **Upload Item** label.

    This opens a file browser for selecting the Appliance Package you want to upload to the client.

11. Navigate to the SD-WAN appliance package zip file you just downloaded from the MCN, select it, and click **OK**.

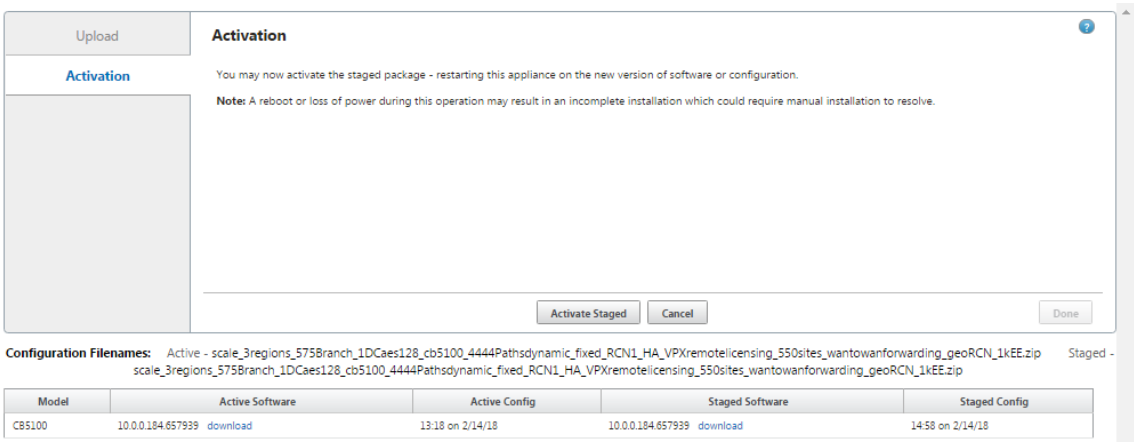
12. Click **Upload**.

    The upload process takes a few seconds to complete. When completed, a status message displays (left middle of page), stating **Upload complete.**



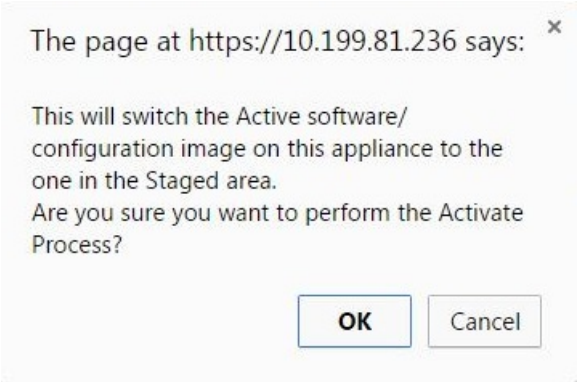
13. Click **Next**.

    This uploads the specified software package, and displays the Local Change Management **Activation** page.



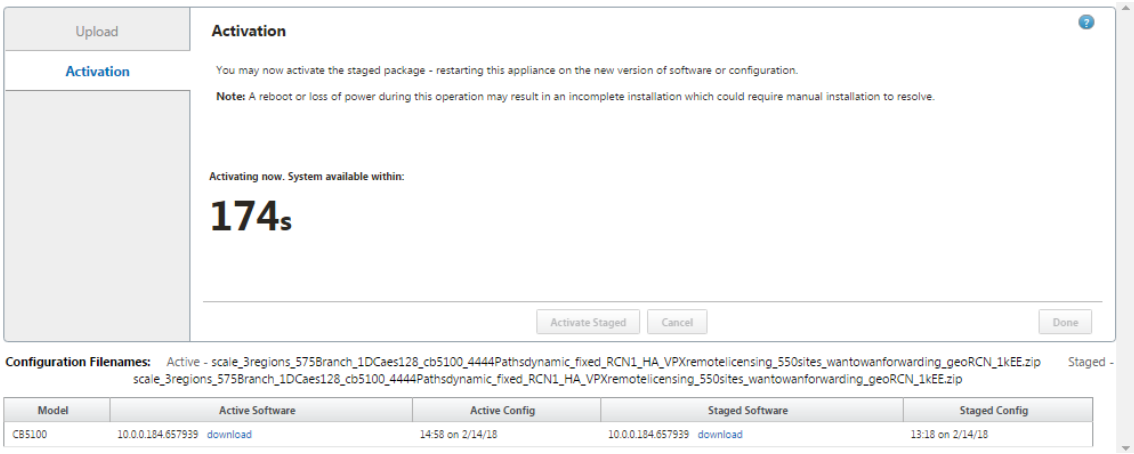
14. Click **Activate Staged**.

    This displays a dialog box prompting you to confirm the activation operation.

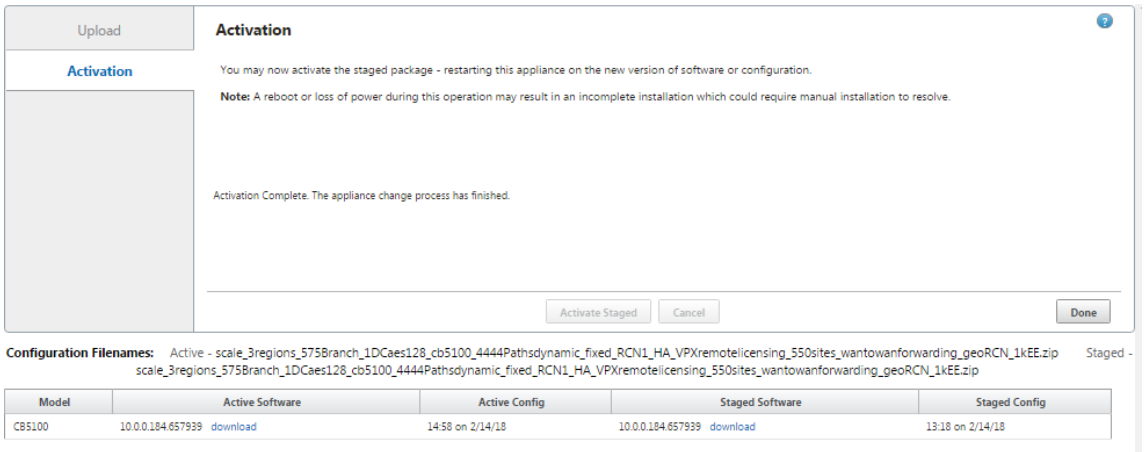


15. Click **OK**.

    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.



    When the activation completes, a status message displays stating **Activation complete**, and the **Done** button becomes available.

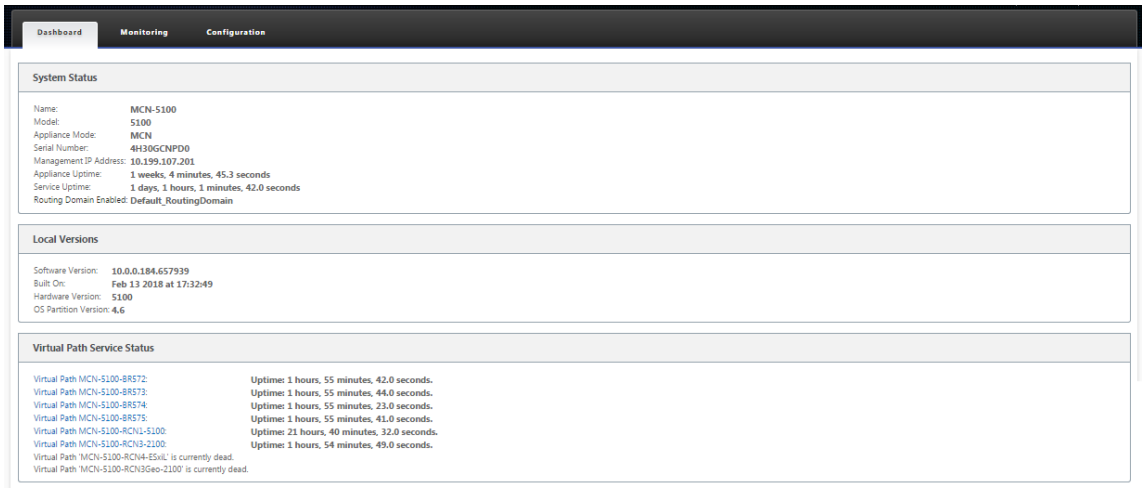


16. Click **Done** to exit the wizard and view the activation results.

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 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 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 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.

Deploy Citrix SD-WAN Standard Edition in OpenStack using CloudInit

March 12, 2021

You can now deploy Citrix SD-WAN Standard Edition (SE) in an OpenStack environment. For this, Citrix SD-WAN image must support config-drive functionality.

> **NOTE**
>
> Create Citrix image to support config-drive functionality.

Config-drive functionality supports the following parameter configuration to establish communication with Citrix Orchestrator via the management network:

- Mgmt. ipv4 address

- Mgmt. gateway
- Name-server1
- Name-server2
- Serial number - Used for authentication and it must be reused for the new instance. Serial number passed in clouding must overwrite the autogenerated trial number in the VPX instance.

> **Note**
>
> - To reuse the serial number, an init script is incorporated in SD-WAN that run on an OpenStack and change the serial number in /etc/default/family.
> - Orchestrator must have a unique serial number with SD-WAN appliances to work.

Cloudinit script supports contextualization for SD-WAN deployment in OpenStack with config-drive.

In the process of contextualization, the infrastructure makes the context available to the virtual machine and the virtual machine interprets the context. On contextualization, the virtual machine can start certain services, create users, or set networking and configuration parameters.

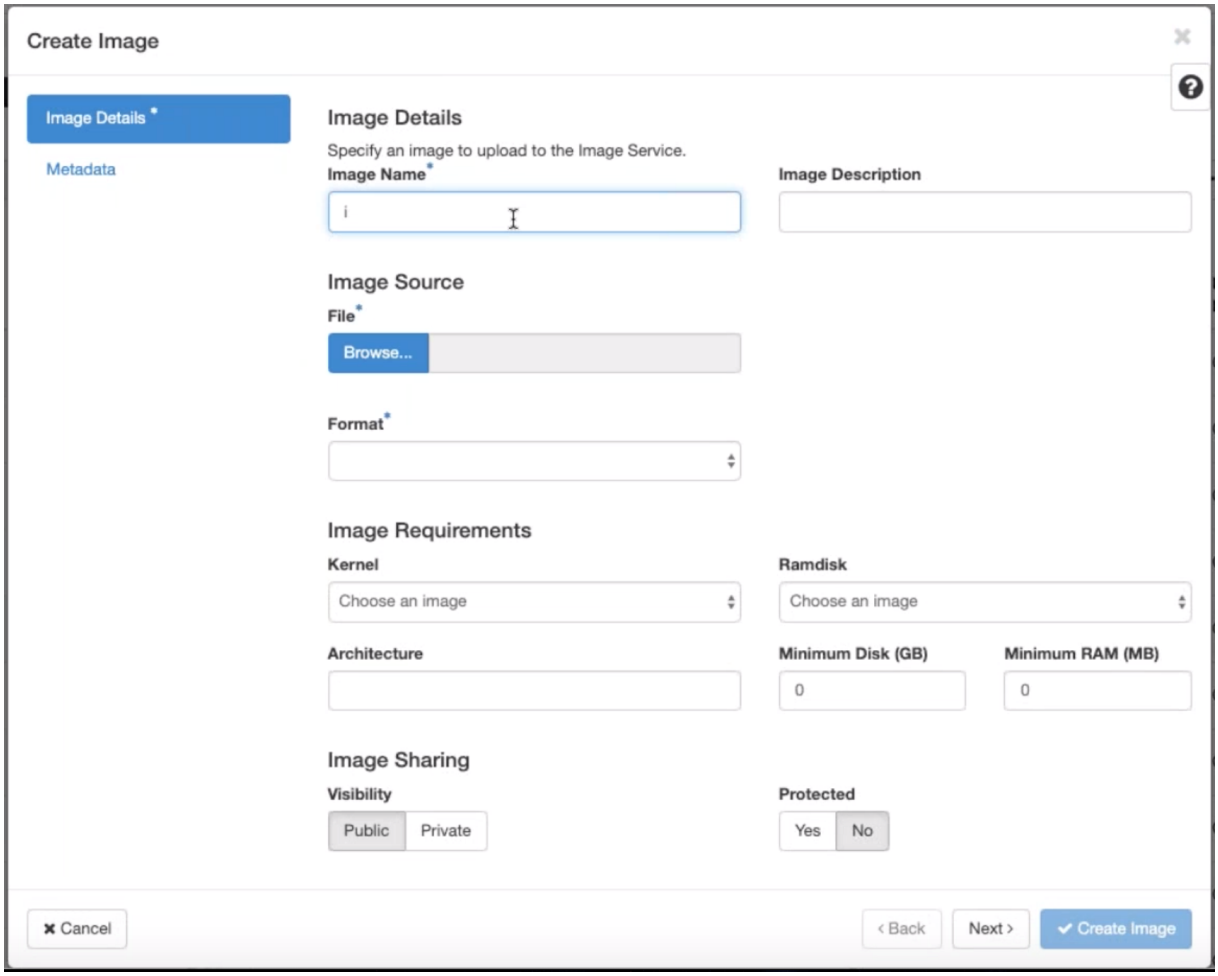
For an SD-WAN instance in OpenStack, the inputs needed for Management IP, DNS, and serial number from the users. The Cloudinit script parses these inputs and provision the instance with the given information.

While launching instances in an OpenStack cloud environment, Citrix SD-WAN appliance need to support two technologies that are User Data and CloudInit to support automated configuration of instances at boot time.

Perform the following steps to provisioning SD-WAN SE in an OpenStack environment:

Pre-requisites

Go to **Images** and click **Create Image**.

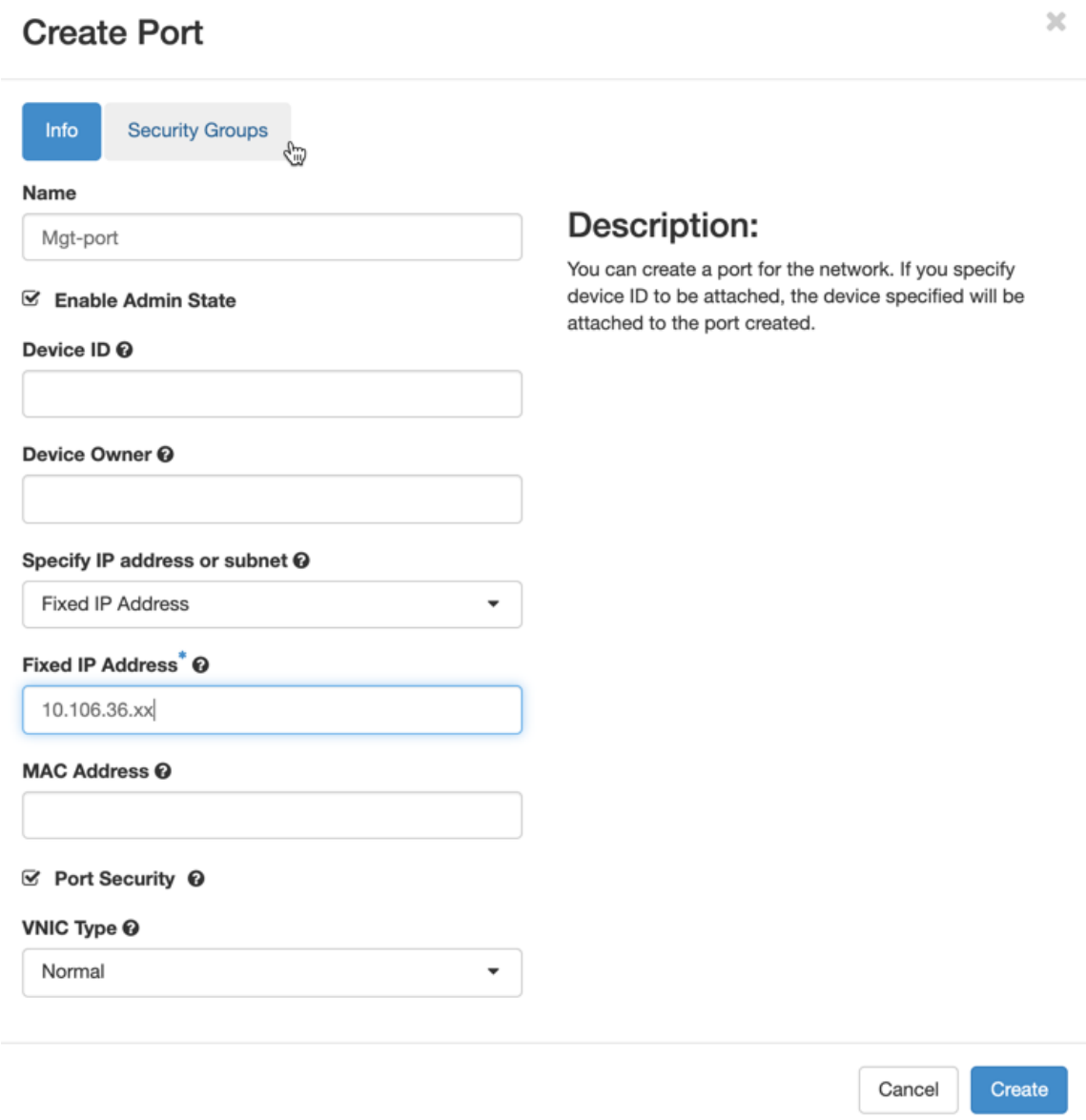


- **Image Name** - Provide the image name.
- **Image Description** –Add an image description.
- **File** - Browse for the kvm.qcow2 image file from your local drive and select it.
- **Format** –Select the QCOW2 –QEMU Emulator disk format from the drop-down list.

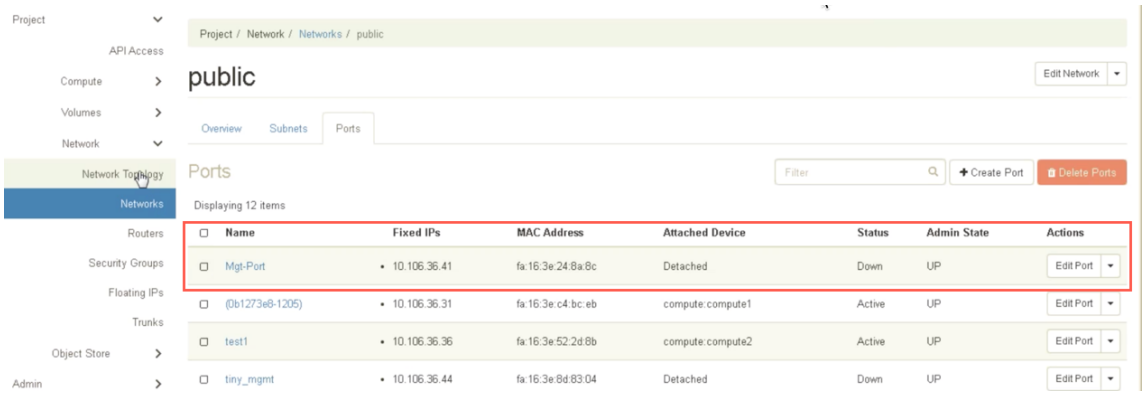
Click **Create Image**.

Both Network and network port must create initially and predefined. To create network port:

1. Select **Networks** under **Network** and go to **Port** tab.
2. Click **Create Port** and provide the necessary detail and click Create.



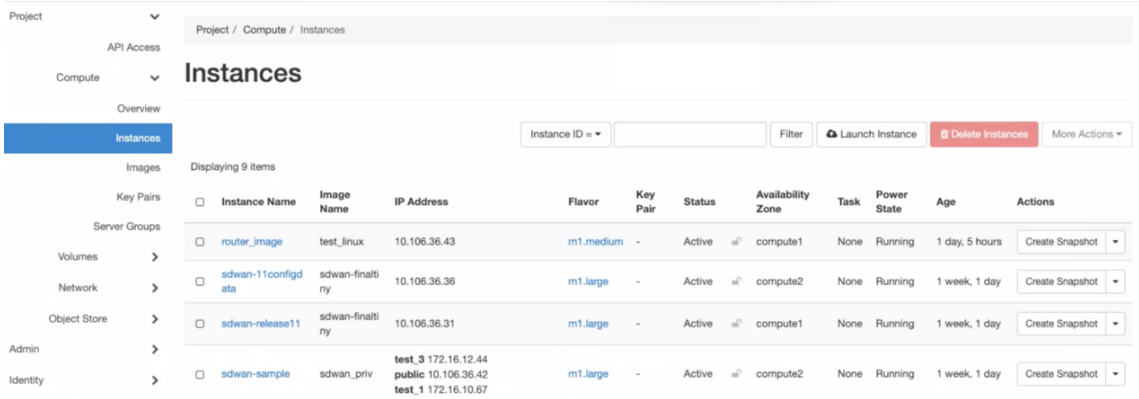
If you select **Fixed IP Address**, then you must provide the subnet IP address for the new port.



The port is created and as it is not attached to any device, the current status shows Detached.

Create OpenStack instance to enable config-drive and pass the user_data.

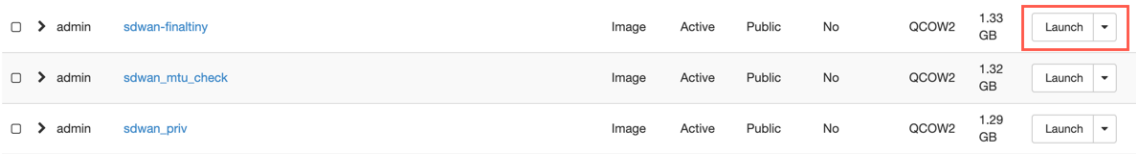
3. Log in to OpenStack and configure Instances.



4. Download the **kvm.qcow2.gz** file and untar it.

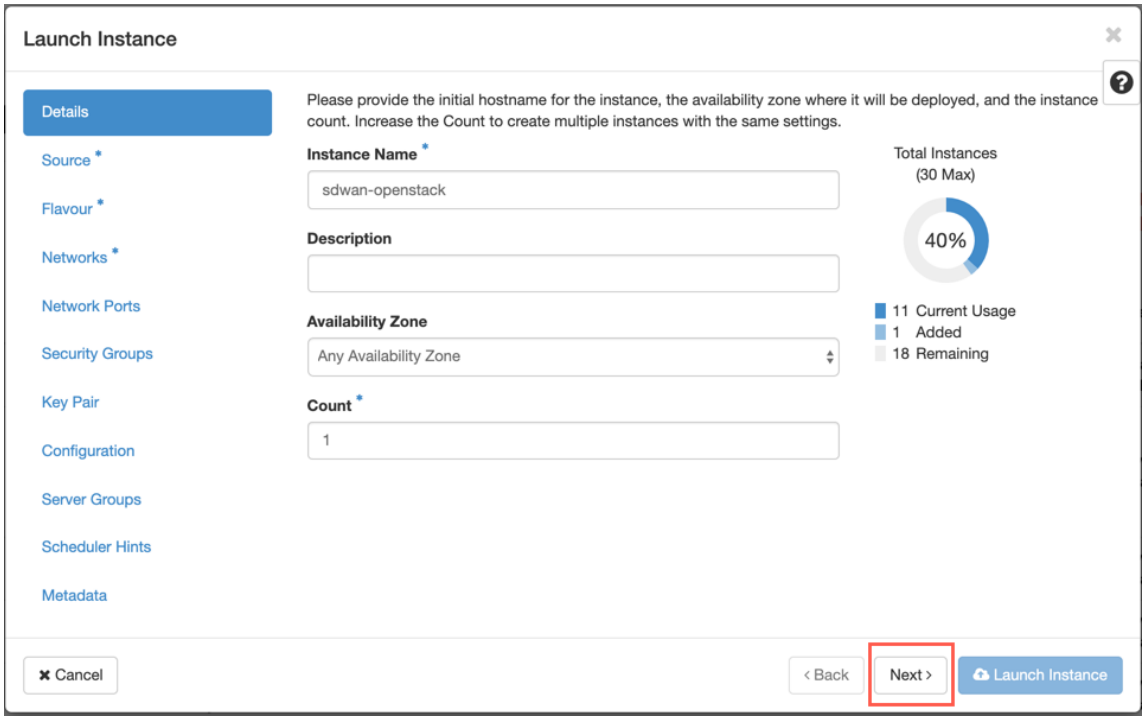
5. Go to **Instances** and click **Launch Instance**.

> **NOTE**
>
> You can go back to **Instances** and click **Launch Instance** or from the Images screen click **Launch** once the image is created.

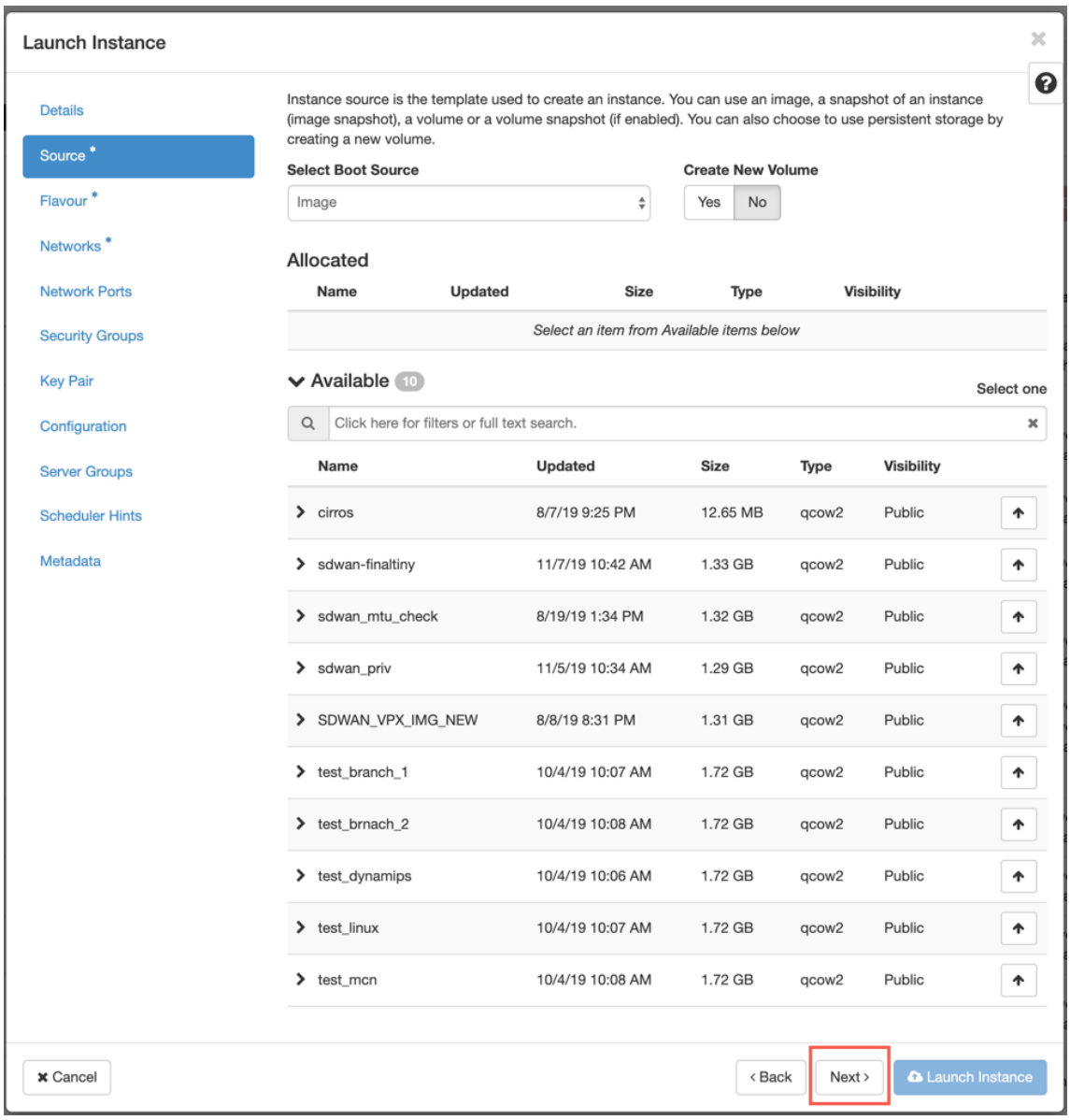


6. Under **Details** tab, provide the following information:

   - **Instance Name** –Provide the host name for the instance.
   - **Description** –Add description for the instance.
   - **Availability Zone** –Select the availability zone from the drop-down list where you want to deploy the instance.
   - **Count** –Enter the instance count. You can increase the count to create multiple instances with the same settings. Click **Next**.



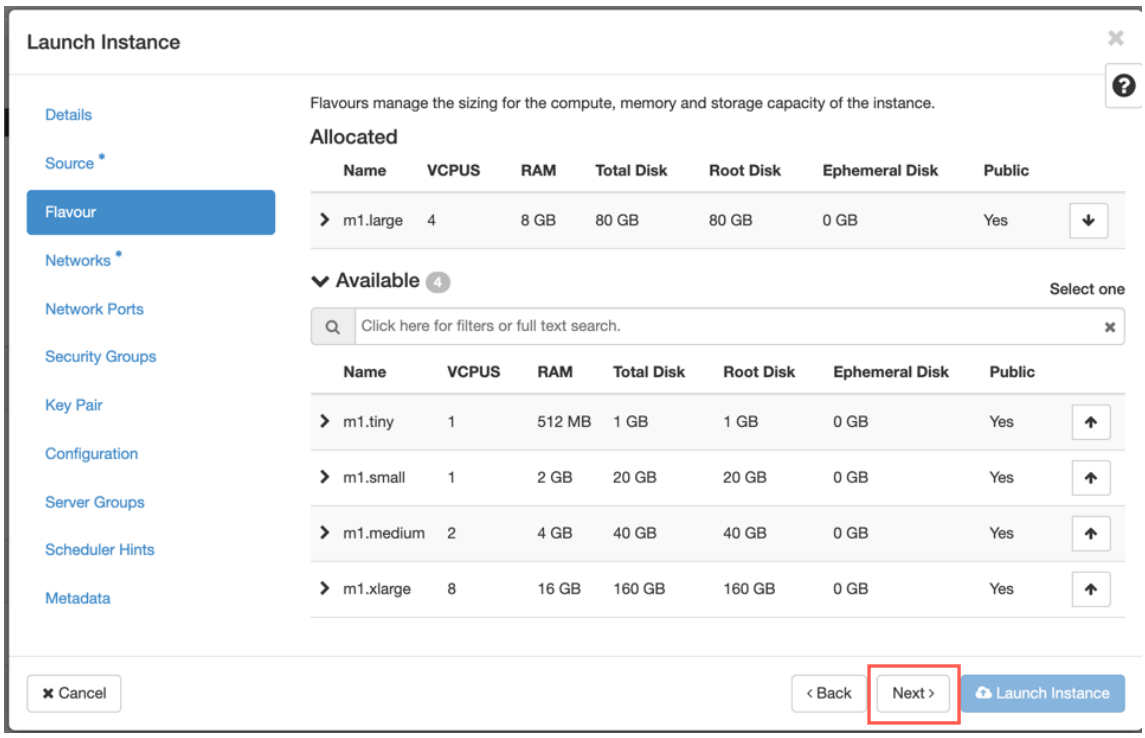
7. In **Source** tab, select **No** under **Create New Volume** and click**Next**. Instance source is the template used to create an instance.



8. Select **Flavour** for the instance and click Next. The flavour you select for an instance manages the amount of compute, storage, and memory capacity of the instance.

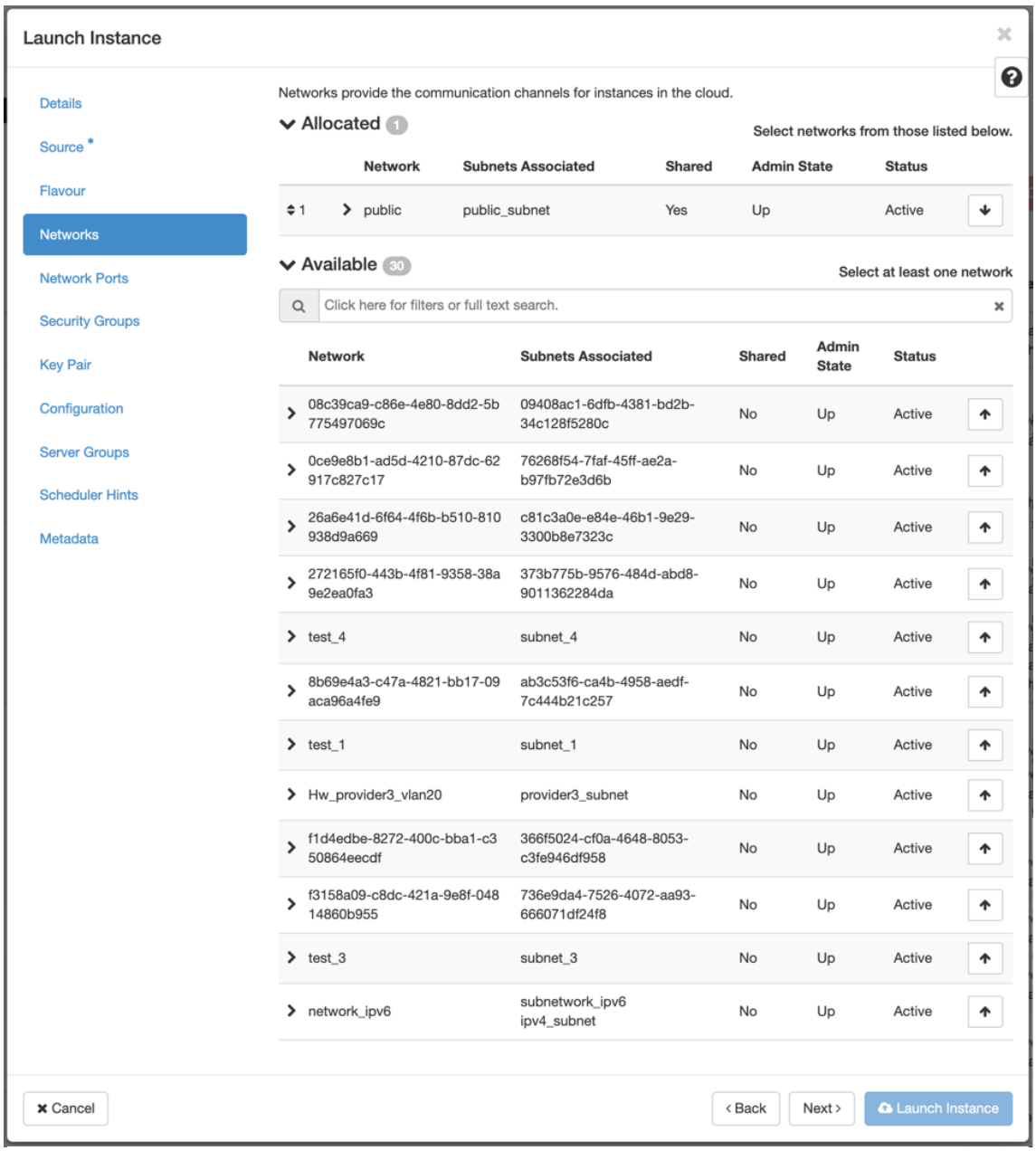
> **NOTE**
>
> The flavour you select must have enough resources allocated to support the type of instance you are trying to create. Flavours that do not provide enough resources for your instance are identified on the available table with a yellow warning icon.

Administrators are responsible for creating and managing flavours. Click the arrow (at the right side) to allocate.



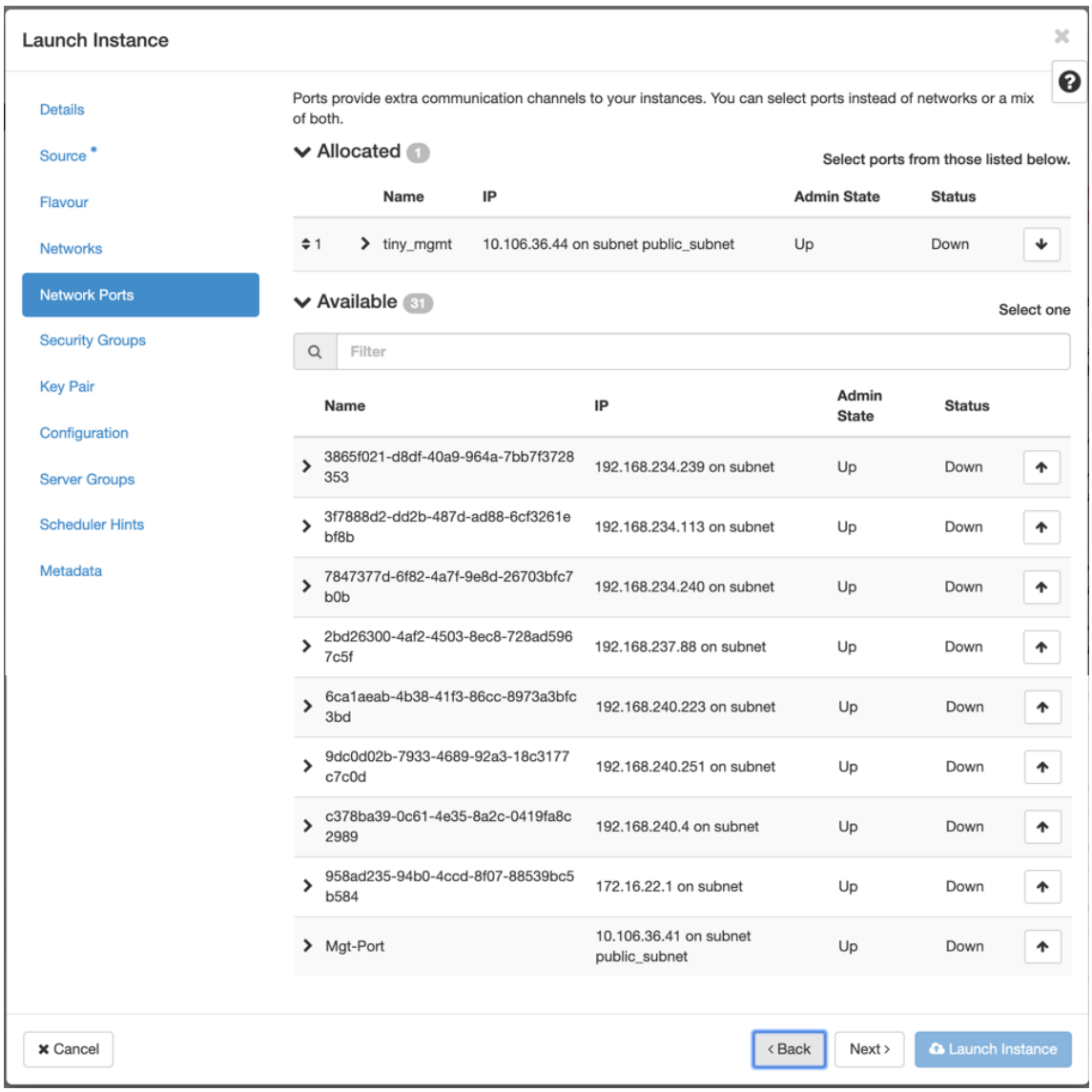
9. Select the network and click **Next**. Networks provide the communication channels for instances.

> **NOTE**
>
> An Administrator is created the Provider networks and these networks are map to an existing physical network in the data center. Similarly Project networks are created by Users and these networks are fully isolated and are project-specific.

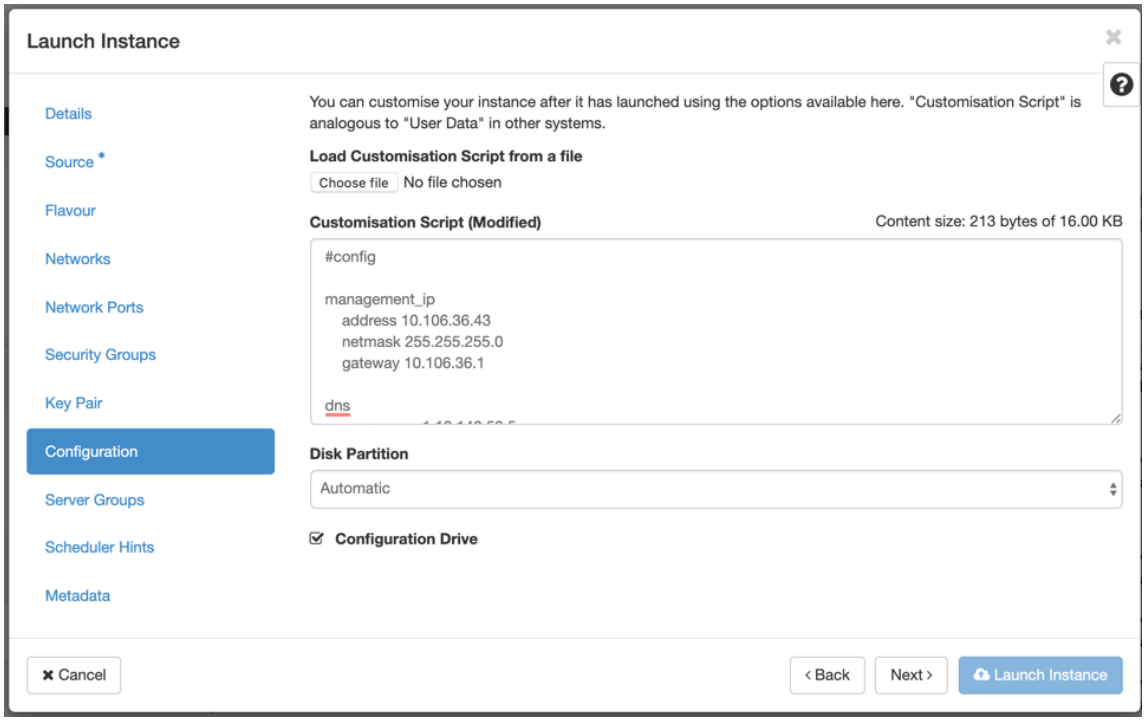


10. Select a network port for the instance and click **Next**. Network ports provide additional communication channels to the instances.

> **NOTE**
>
> You can select ports instead of networks or a mix of both.



11. Go to **Configuration** and click **Choose file**. Select the user_data file. You can view the **Management IP**, **DNS**, and **Serial Number** information in the user_data file.
12. Enable the **Configuration Drive** check box. By enabling the configuration drive you can put the user metadata inside the image.



13. Click **Launch Instance**.

Configure LTE functionality on 210 SE LTE appliance

September 23, 2021

You can connect a Citrix SD-WAN 210-SE LTE appliance to your network using an LTE connection. This topic provides details on configuring mobile broadband settings, configuring the data center and branch appliances for LTE and so on. For more information on Citrix SD-WAN 210-SE LTE hardware platform, see Citrix SD-WAN 210 Standard Edition Appliances.

> **Note**
>
> The LTE connectivity depends on the SIM carrier or service provider network.

Getting started with Citrix SD-WAN 210-SE LTE

1. Insert the SIM card into the SIM card slot of the Citrix SD-WAN 210-SE LTE.

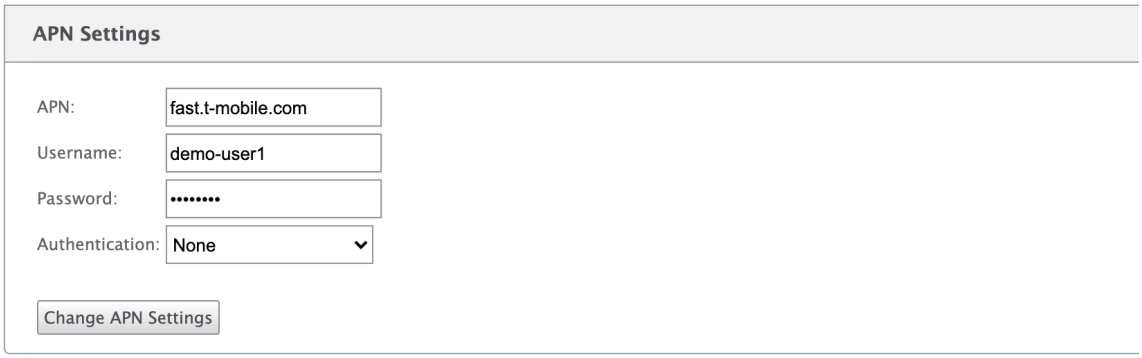
   > **Note:**
   > Only a standard or 2FF SIM card (15x25 mm) is supported.

2. Fix the antennas to the Citrix SD-WAN 210-SE LTE appliance. For more information, see Installing the LTE antennas.
3. Power on the appliance.

> **Note**
>
> If you have inserted the SIM into an appliance that is already powered ON and booted up, navigate to **Configuration > Appliance Settings > Network Adapters > Mobile Broadband > SIM Card** and click **Refresh SIM Card**.

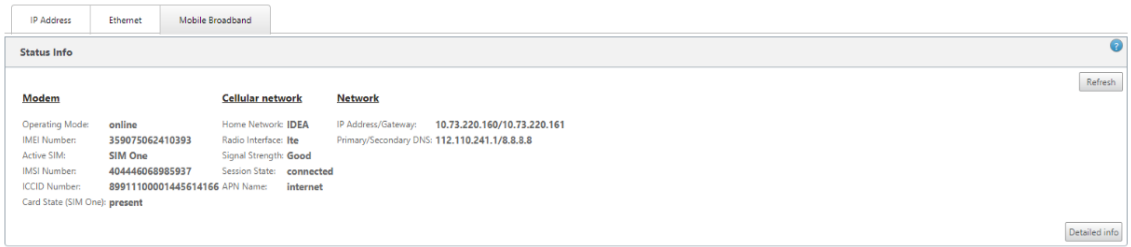
4. Configure the APN settings. In the SD-WAN GUI navigate to **Configuration > Appliance Settings > Network Adapters > Mobile Broadband > APN settings**.

> **Note:**
> Obtain the APN information from the carrier.



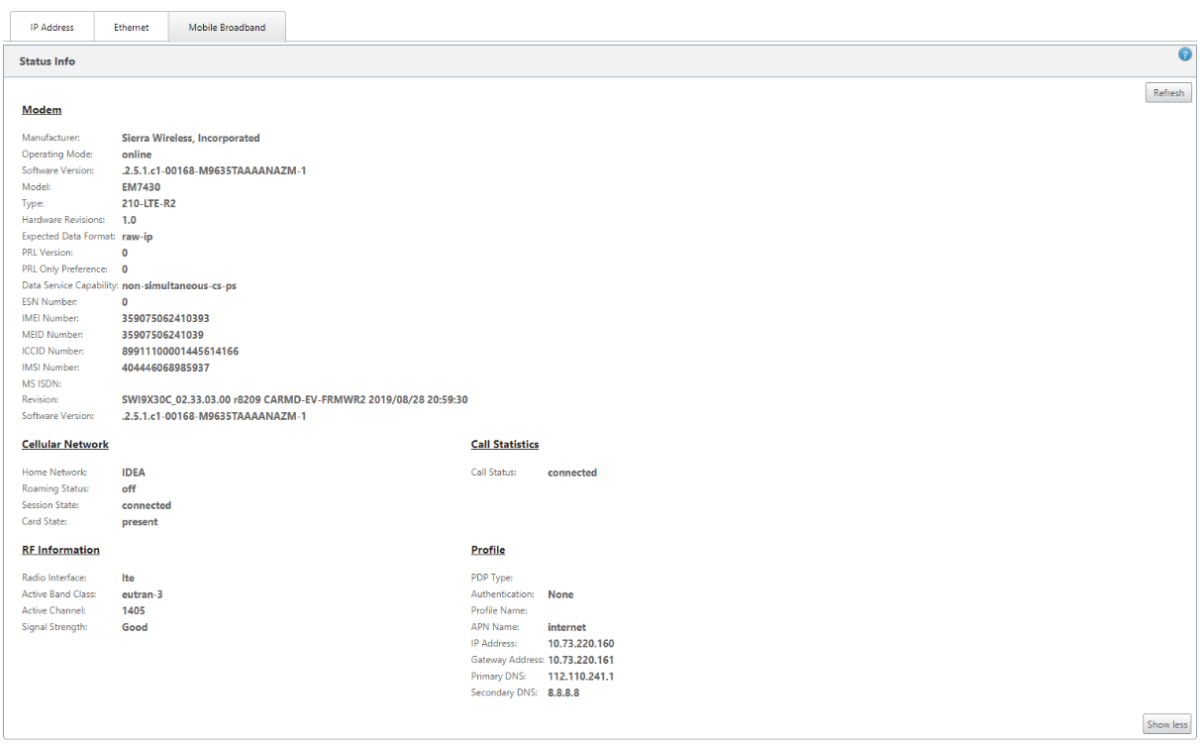
5. Enter the **APN**, **Username**, **Password** and **Authentication** provided by the carrier. You can choose from PAP, CHAP, PAPCHAP authentication protocols. If the carrier has not provided any authentication type, set it to **None**.
6. Click **Change APN Settings**.
7. In the SD-WAN appliance GUI, navigate to **Configuration > Appliance Settings > Network Adapters > Mobile Broadband**.

   You can view the Mobile broadband settings status information.



The following are some useful status information:

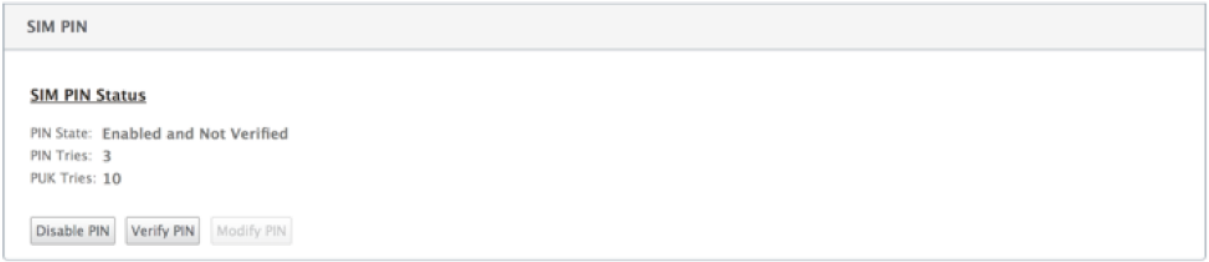
- **Operating Mode**: Displays the modem state.
- **Active SIM**: At any given time, only one SIM can be active. Displayed the SIM that is currently active.
- **Card State**: Present indicates that SIM is properly inserted.
- **Signal strength**: Quality of signal strength - excellent, good, fair, poor, or no signal.
- **Home network**: Carrier of the inserted SIM.
- **APN name**: The access point name used by the LTE modem.
- **Session state**: Connected indicates that the device has joined the network. If the session state is disconnected, check with the carrier whether the account has been activated of if the data plan is enabled.



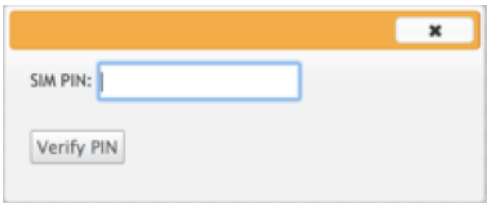
SIM PIN

If you have inserted a SIM card that is locked with a PIN, the SIM status is Enabled and Not Verified** state. You cannot use the SIM card until it is verified using SIM PIN. You can obtain the SIM PIN from the carrier.

To perform SIM PIN operations, navigate to **Configuration > Appliance Settings > Network Adapters > Mobile Broadband > SIM PIN**.



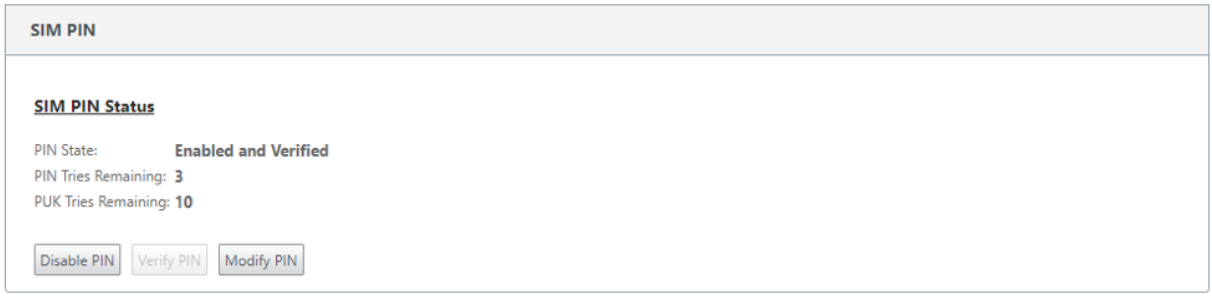
Click **Verify PIN**. Enter the SIM PIN provided by the carrier and click **Verify PIN**.

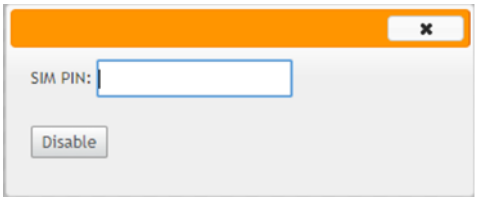


The status changes to **Enabled and Verified**.

Disable SIM PIN

You can choose to disable SIM PIN functionality for a SIM for which SIM PIN is enabled and verified.

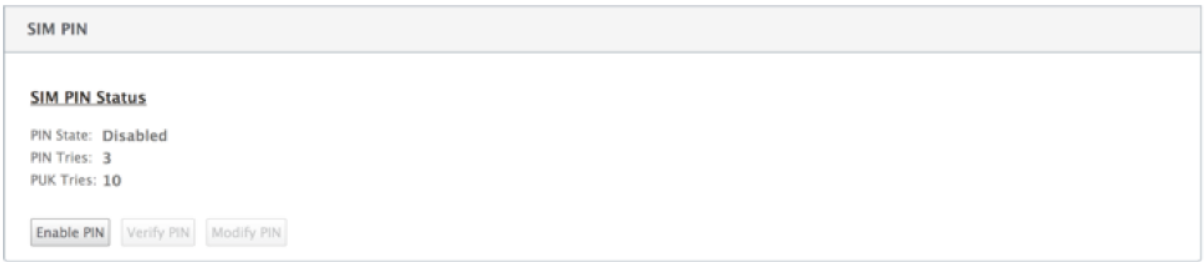




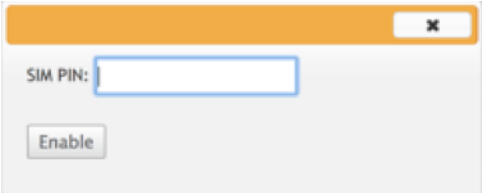
Click **Disable PIN**. Enter the **SIM PIN** and click **Disable**.

Enable SIM PIN

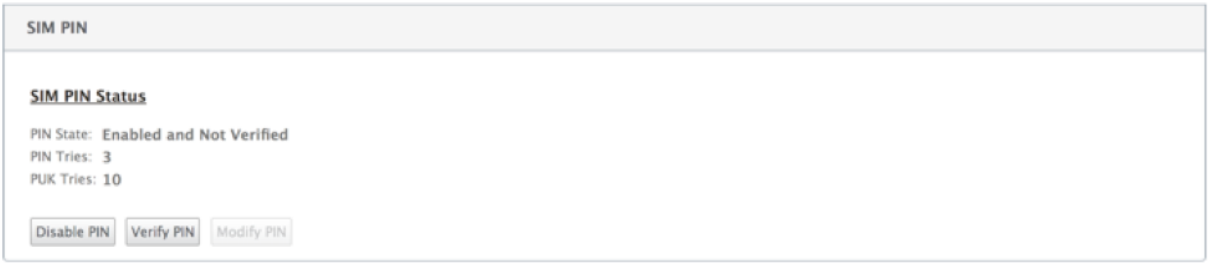
SIM PIN can be enabled for the SIM for which it is disabled.



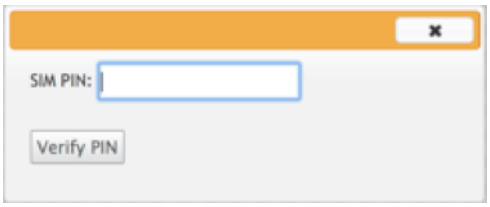
Click **Enable PIN**. Enter the SIM PIN provided by the carrier and click **Enable**.



If the SIM PIN state changes to **Enabled and Not Verified**, it means that the PIN is not verified and you cannot perform any LTE related operations until the PIN is verified.

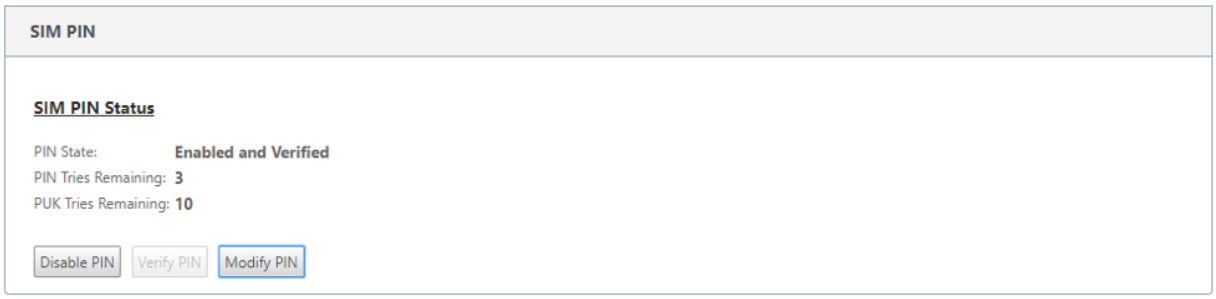


Click **Verify PIN**. Enter the SIM PIN provided by the carrier and click **Verify PIN**.

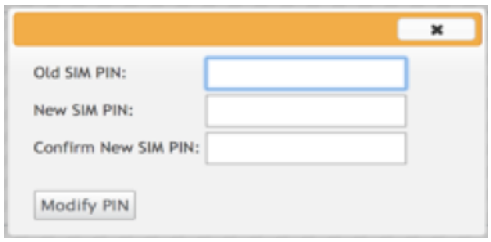


Modify SIM PIN

Once the PIN is in **Enabled and Verified** state you can choose to change the PIN.



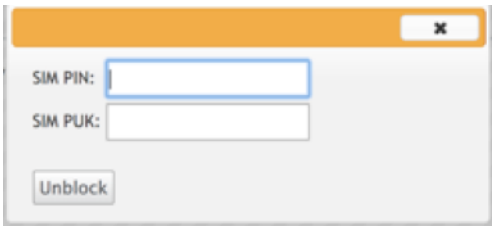
Click **Modify PIN**. Enter the SIM PIN provided by the carrier. Enter the new SIM PIN and confirm it. Click **Modify PIN**.



Unblock SIM

If you forget the SIM PIN, you can reset the SIM PIN using the SIM PUK obtained from the carrier.

To unblock a SIM, click **Unblock**. Enter the **SIM PIN and SIM PUK** obtained from the carrier and click **Unblock**.

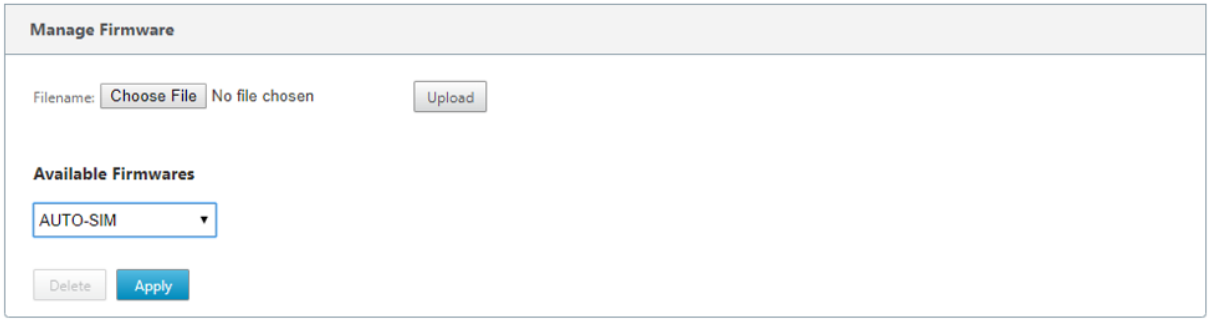


> **Note:**
> The SIM card gets permanently blocked with 10 unsuccessful attempts of PUK, while unblocking the SIM. You need to contact the carrier service provider for a new SIM card.

Manage Firmware

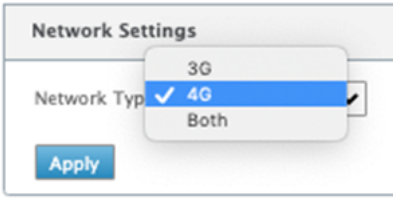
Every appliance that has LTE enabled will have a set of available firmware. You can select from the existing list of firmware or upload a firmware and apply it.

If you are unsure of which firmware to use, select the AUTO-SIM option to allow the LTE modem to choose the most matching firmware based on the inserted SIM card.



Network Settings

You can select the mobile network on Citrix SD-WAN appliances that support internal LTE modem. The supported networks are 3G, 4G, or both.



Roaming

The roaming option is enabled by default on your LTE appliances, you can choose to disable it.

Enable/Disable modem

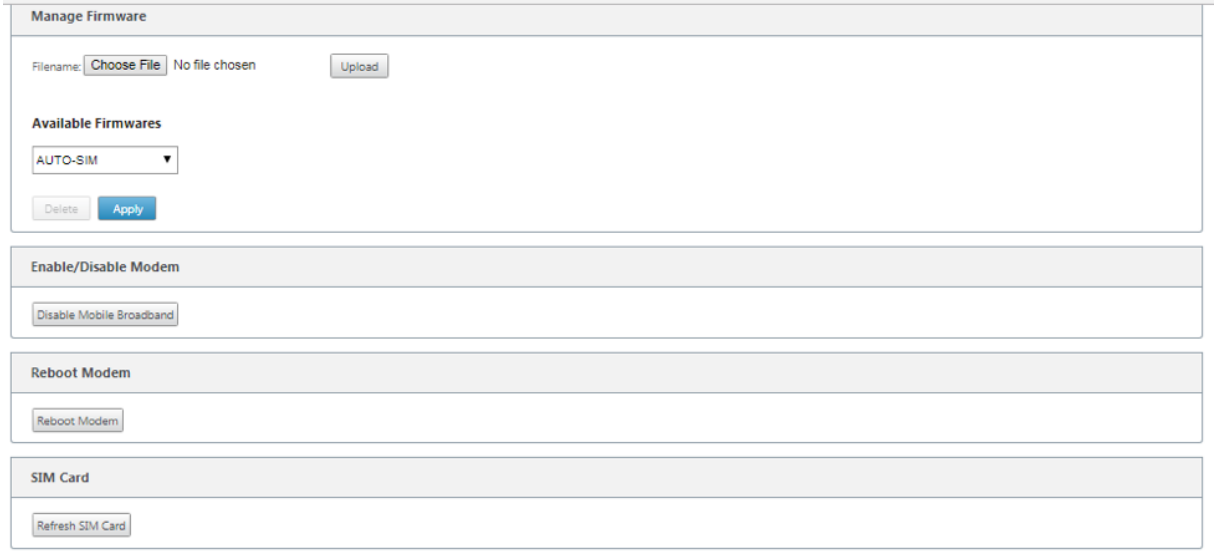
Enable/disable modem depending on your intent to use the LTE functionality. By default, the LTE modem is enabled.

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.



You can remotely view and manage all the LTE sites in your network using Citrix SD-WAN Center. For more information see, Remote LTE site management.

Configure the LTE functionality using CLI

To configure 210-SE LTE modem using the CLI.

1. Log into the Citrix 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.

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

The following table lists the **LTE** command descriptions.

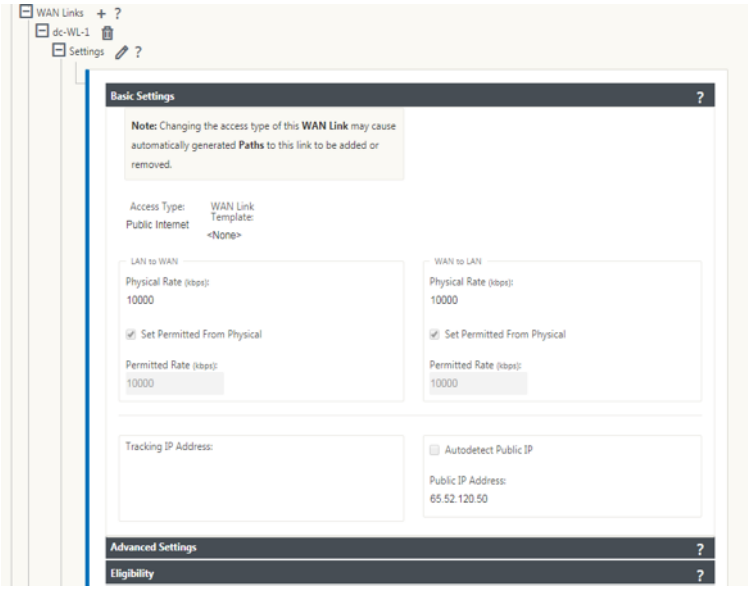
Command	Description
Help {lte>help}	Lists the available LTE commands and parameters
Status {lte>status}	Displays LTE connectivity status
Show {lte>show}	Displays LTE settings
Disable {lte>disable}	Disables LTE modem
Enable {lte>enable}	Enables LTE modem
Apn {lte>apn}	Configures APN settings information
Sim-power off, on, reset>{lte>sim-power off,on,reset}	Powers off sim card, Power on sim card, Refresh sim card
SIM PIN {lte>sim-pin}	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 {lte>apply-fw}	Applies firmware specific to a carrier

Configure MCN for LTE

You cannot configure a 210-LTE appliance as an MCN. However, for an MCN to work with an LTE branch appliance perform the following configurations on the MCN appliance.

To configure an MCN:

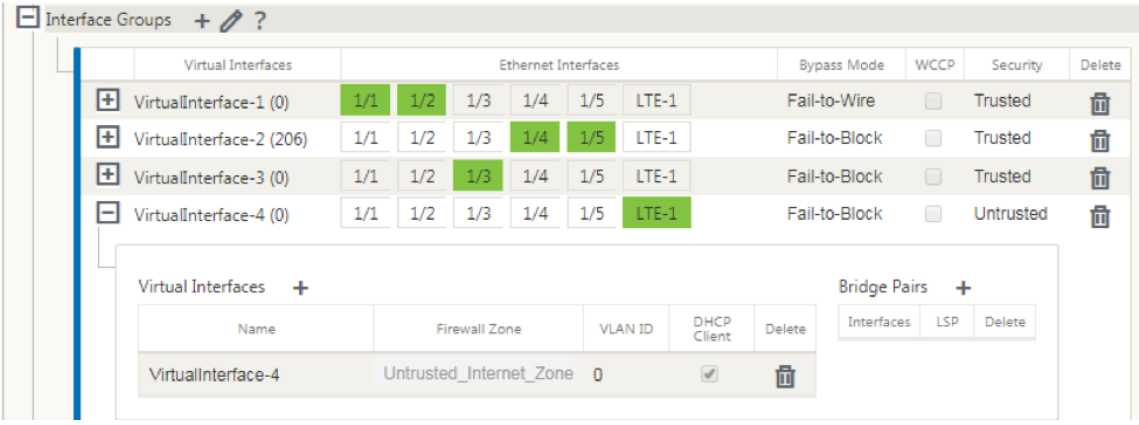
1. Log in to the SD-WAN appliance GUI. Go to Configuration Editor. Complete configuration for the MCN site, see Configure MCN.
2. Ensure that you provide routable public IP address as part of WAN link configuration. You do not have to configure public IP address for client appliances.



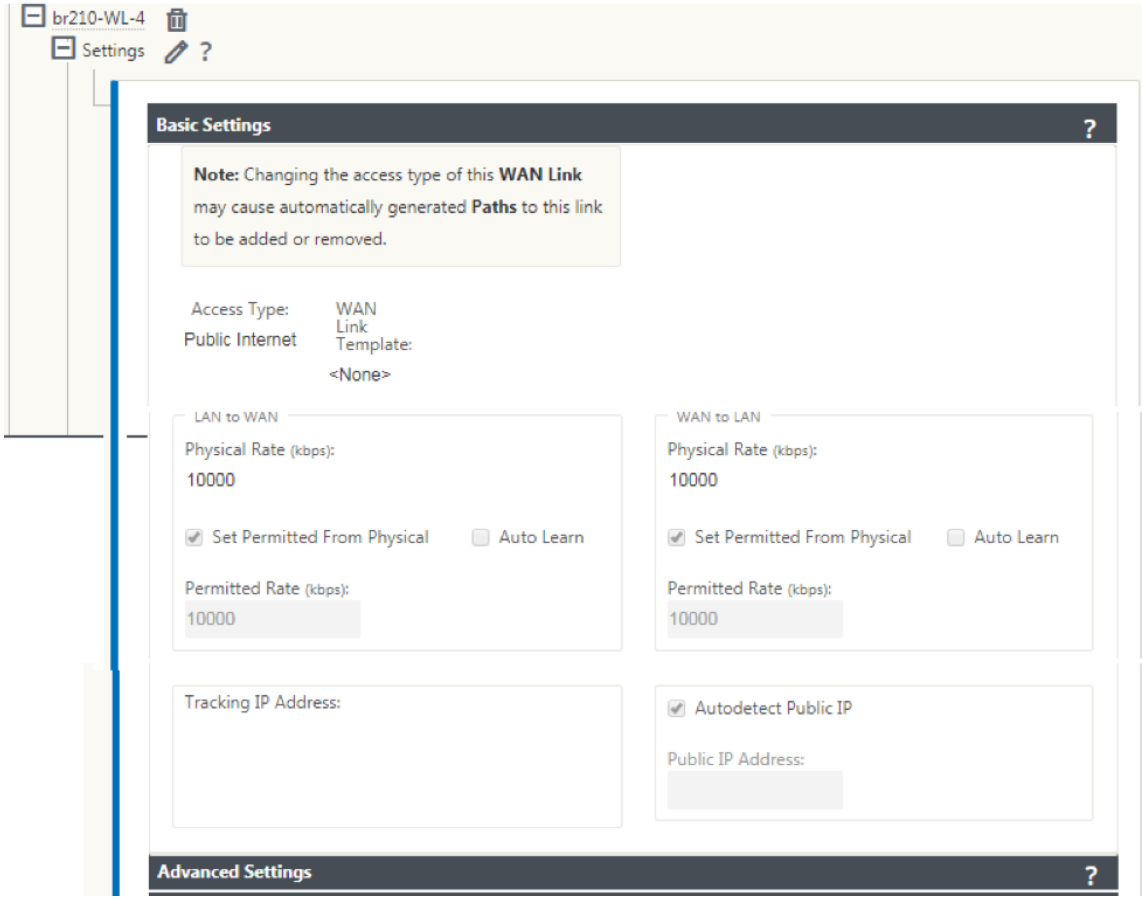
Configure branch for LTE

To configure the 210-SE LTE appliance as a branch site:

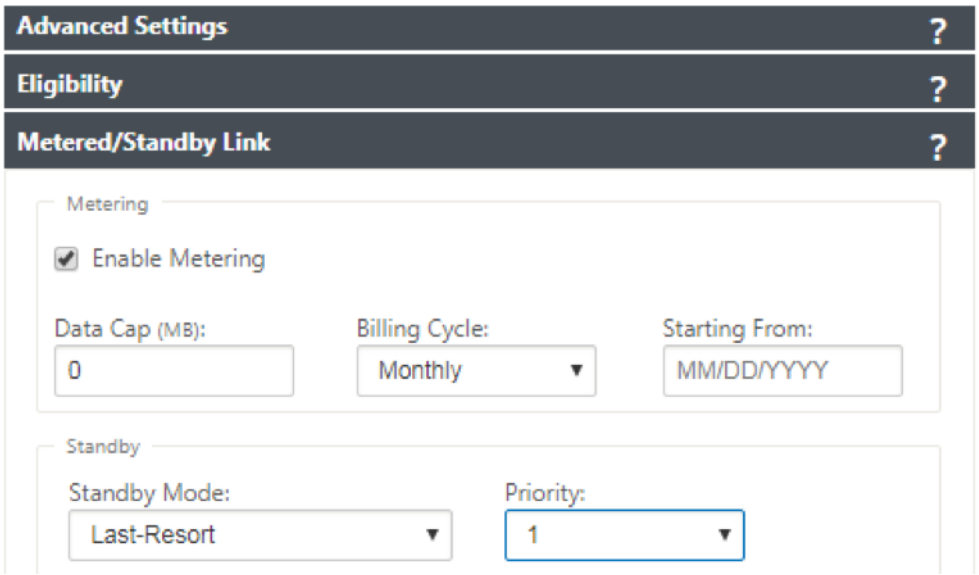
1. In the SD-WAN appliance GUI, go to configuration editor. See Configure Branch.
   - Create Interface Groups.
   - Create up to one Virtual Interface and one Interface Group for the LTE adapter to configure WAN link by selecting the following:
     - Ethernet Interface –LTE 1
     - Security –untrusted (default)
     - DHCP Client –Enabled (default)



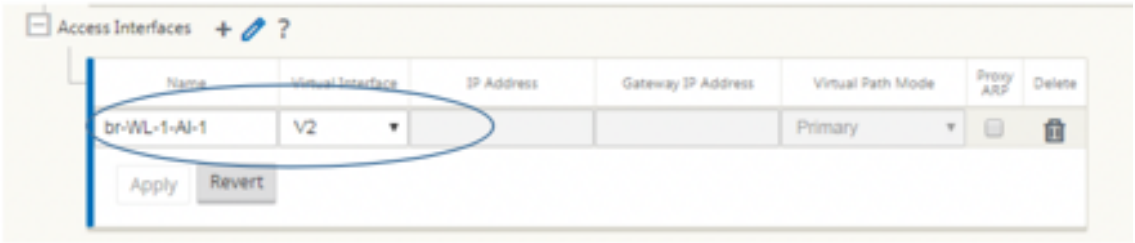
2. Enable **AutoDetect Public IP** for WAN link configuration when configuring WAN link using the virtual interface created for LTE interface.



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.



The IP address and gateway address for the Access Interface of the WAN link need not be configured because it receives that information from the carrier through DHCP.



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.

Zero-touch deployment over LTE

Pre-requisites for enabling zero-touch deployment 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.

- If a static IP address on the Management Interface is configured, you need to configure the Management Interface with DHCP, apply the configuration, and then disconnect the Management port, and restart the appliance.

4. Ensure the 210-SE appliance configuration has internet service defined for LTE interface.

When the appliance is powered on, the zero-touch deployment service uses the LTE port to obtain the latest SD-WAN software and SD-WAN configuration only when the management port has not been connected.

You can use the SD-WAN Center GUI to deploy and configure 210-SE LTE appliance for the zero-touch deployment service.

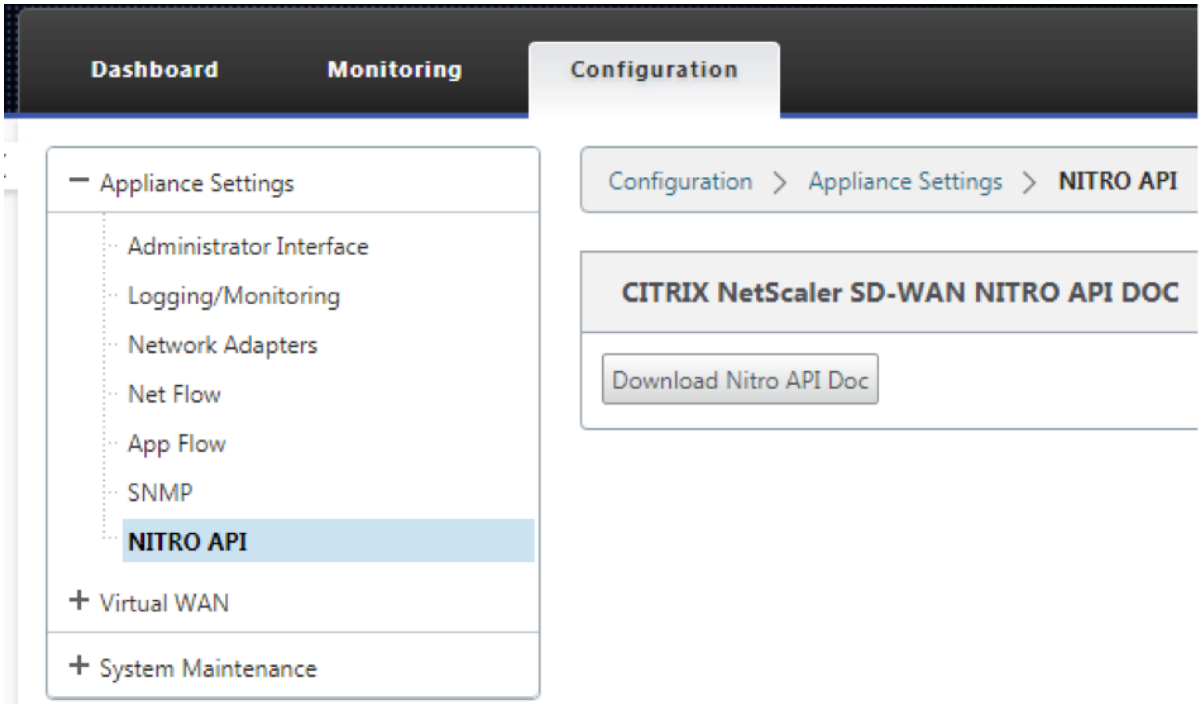
See the zero-touch deployment procedure for more information about deploying and configuring the 210-SE LTE appliance using SD-WAN Center.

Zero-touch deployment Service over management interface for 210-SE LTE appliance

Connect the Management Port and use the standard zero-touch deployment procedure that is supported on all other non-LTE platforms.

LTE REST API

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. The REST API for SIM PIN functionality is introduced in Citrix SD-WAN 11.0.



Configure LTE functionality on 110-LTE-WiFi appliance

May 12, 2021

You can connect a Citrix SD-WAN 110-LTE-WiFi appliance to your network using an LTE connection. This topic provides details on configuring mobile broadband settings, configuring the data center and branch appliances for LTE and so on. For more information on Citrix 110-LTE-WiFi hardware platform, see Citrix SD-WAN 110 Standard Edition Appliances.

> **Note**
>
> The LTE connectivity depends on the SIM carrier or service provider network.

Getting started with Citrix SD-WAN 110-LTE-WiFi

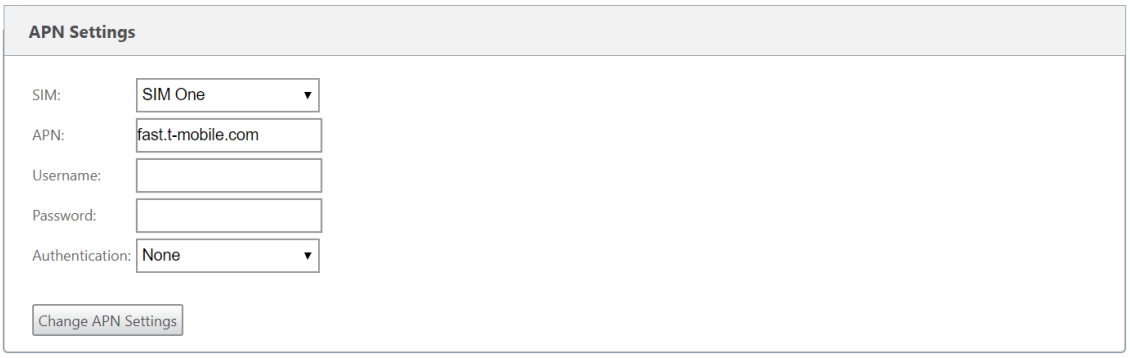
1. Power ON the appliance and insert the SIM card into the SIM card slot of the Citrix SD-WAN 110-LTE-WiFi appliance.

   > **Note**
   >
   > Citrix SD-WAN 110-LTE-WiFi appliance has two standard (2FF) SIM slots. To use Micro (3FF) and Nano (4FF) size SIMs, use a SIM adapter. Snap the smaller SIM into the adapter. You can

> obtain the adapter from Citrix as a Field Replaceable Unit (FRU) or from the SIM provider.

2. Fix the antennas to the Citrix SD-WAN 110-LTE-WiFi appliance. For more information, see Installing the LTE antennas.
3. Power on the appliance.
4. Configure the APN settings. In the SD-WAN GUI navigate to **Configuration > Appliance Settings > Network Adapters > Mobile Broadband > APN settings**.

   > **Note**
   >
   > Obtain the APN information from the carrier.

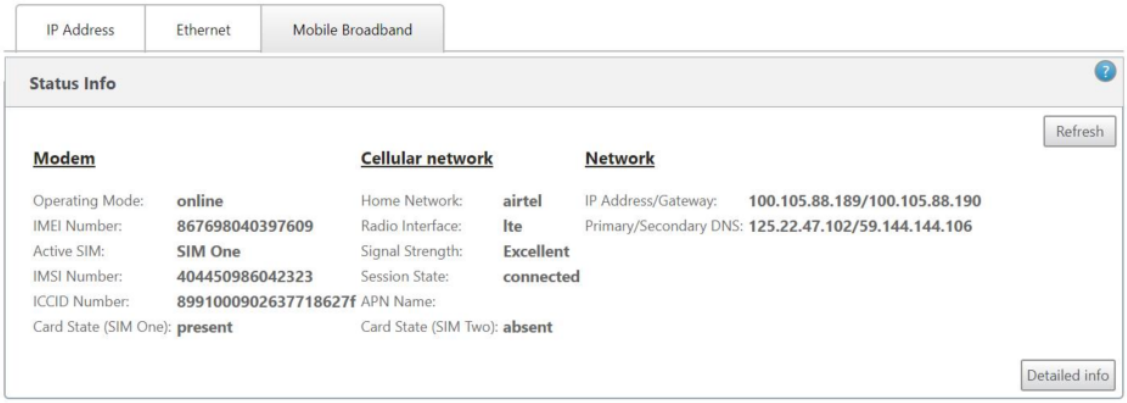


5. Select the SIM card, enter the **APN**, **Username**, **Password**, and **Authentication** provided by the carrier. You can choose from PAP, CHAP, PAPCHAP authentication protocols. If the carrier has not provided any authentication type, set it to **None**.

   > **Note**
   >
   > All these fields are optional.

6. Click **Change APN Settings**.
7. In the SD-WAN appliance GUI, navigate to **Configuration** > **Appliance Settings** > **Network Adapters** > **Mobile Broadband**.

   You can view the Mobile broadband settings status information.



The following are some useful status information:

- **Operating Mode**: Displays the modem state.
- **Active SIM**: At any given time, only one SIM can be active. Displayed the SIM that is currently active.
- **Card State**: Present indicates that SIM is properly inserted.
- **Signal strength**: Quality of signal strength - excellent, good, fair, poor, or no signal.
- **Home network**: Carrier of the inserted SIM.
- **APN name**: The access point name used by the LTE modem.
- **Session state**: Connected indicates that the device has joined the network. If the session state is disconnected, check with the carrier if the account is activated and the data plan is enabled.

SIM Preference

You can insert two SIMs on a Citrix SD-WAN 110-LTE-WiFi appliance. At any given time, only one SIM is active. Select the **SIM preference**:

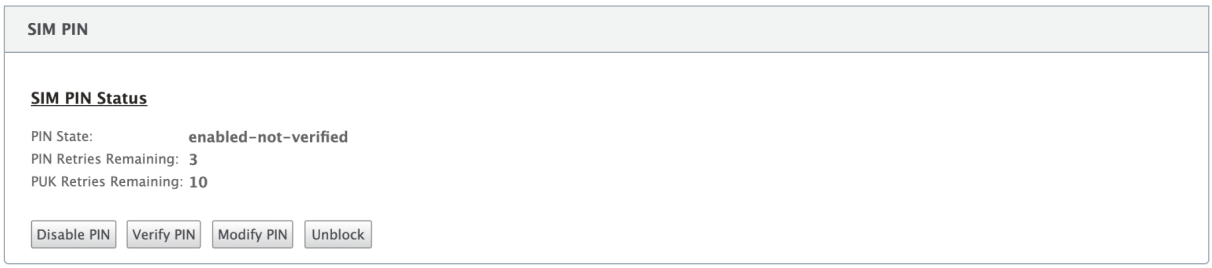
- **SIM One preferred**: If two SIMs are inserted, on boot-up the LTE modem uses SIM One, if available. When the LTE modem is up and running it uses whichever SIM (SIM One or SIM Two) is useable at that moment. It continues to use it until the SIM is active.
- **SIM Two preferred**: If two SIMs are inserted, on boot-up the LTE modem uses SIM Two, if available. When the LTE modem is up and running it uses whichever SIM (SIM One or SIM Two) is useable at that moment. It continues to use it until the SIM is active.
- **SIM One**: Only SIM One is used, irrespective of the SIM state on both the SIM slots. SIM One is always active.
- **SIM Two**: Only SIM Two is used, irrespective of the SIM state on both the SIM slots. SIM Two is always active.

SIM PIN

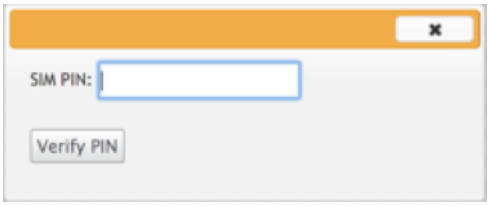
If you have inserted a SIM card that is locked with a PIN, the SIM status is **enabled-not-verified** state. You cannot use the SIM card until it is verified using the SIM PIN. You can obtain the SIM PIN from the carrier.

> **Note**
>
> The SIM PIN operations are applicable for the active SIM only.

To perform SIM PIN operations, navigate to **Configuration > Appliance Settings > Network Adapters > Mobile Broadband > SIM PIN**.



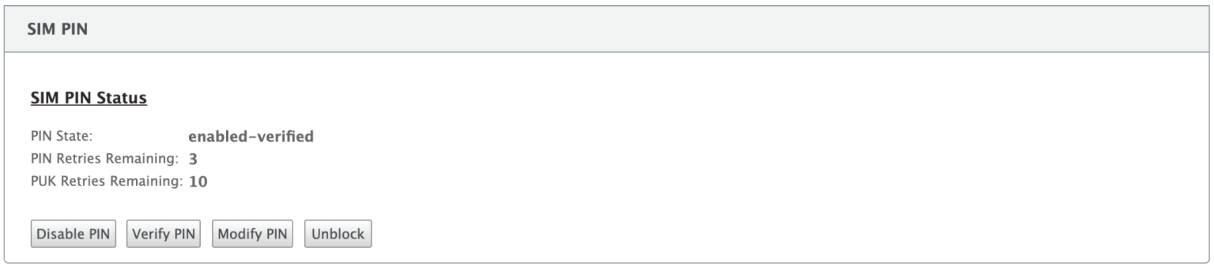
Click **Verify PIN**. Enter the SIM PIN provided by the carrier and click **Verify PIN**.



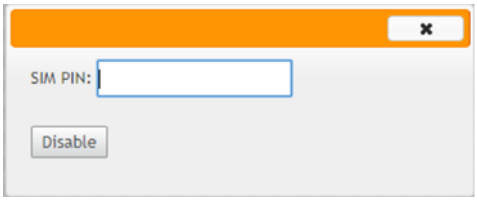
The status changes to **enabled-verified**.

Disable SIM PIN

You can choose to disable SIM PIN functionality for a SIM for which SIM PIN is enabled and verified.

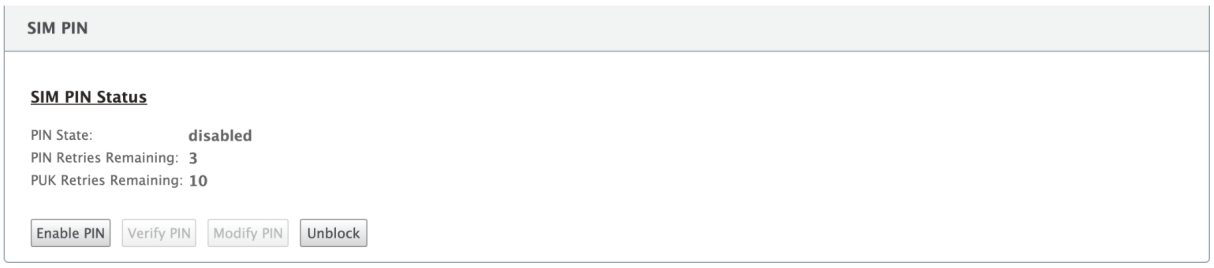


Click **Disable PIN**. Enter the **SIM PIN** and click **Disable**.

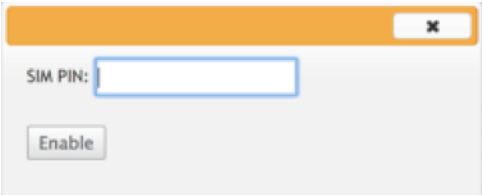


Enable SIM PIN

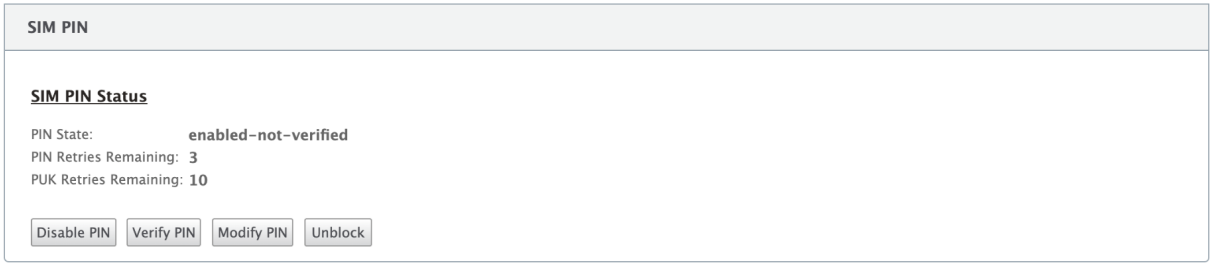
SIM PIN can be enabled for the SIM for which it is disabled.



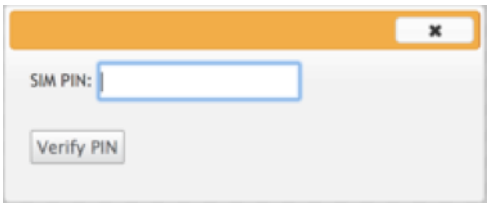
Click **Enable PIN**. Enter the SIM PIN provided by the carrier and click **Enable**.



If the SIM PIN state changes to **enabled-not-verified**, it means that the PIN is not verified and you cannot perform any LTE related operations until the PIN is verified.



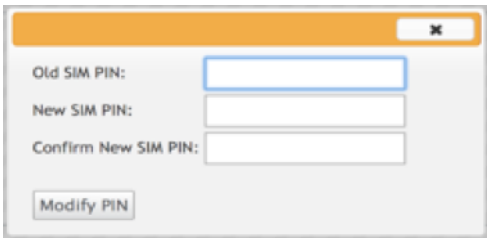
Click **Verify PIN**. Enter the SIM PIN provided by the carrier and click **Verify PIN**.



Modify SIM PIN

Once the PIN is in **enabled-verified** state you can choose to change the PIN.

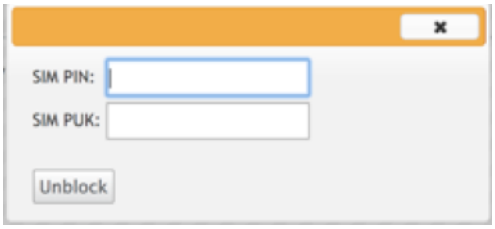
Click **Modify PIN**. Enter the SIM PIN provided by the carrier. Enter the new SIM PIN and confirm it. Click **Modify PIN**.



Unblock SIM

If you forget the SIM PIN, you can reset the SIM PIN using the SIM PUK obtained from the carrier.

To unblock a SIM, click **Unblock**. Enter the **SIM PIN** of your choice. Enter the **SIM PUK** obtained from the carrier and click **Unblock**.



> **Note:**
> The SIM card gets permanently blocked with 10 unsuccessful attempts of PUK, while unblocking the SIM. You need to contact the carrier service provider for a new SIM card.

Network Settings

You can select the mobile network on the Citrix SD-WAN appliances that support internal LTE modem. The supported networks are 3G, 4G, or both.

Roaming

The roaming option is enabled by default on your LTE appliances, you can choose to disable it.

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 7 minutes for the reboot operation to complete.

Refresh SIM

Use this option when the SIM card is not detect properly by the 110-LTE-WiFi modem.

> **Note**
>
> The Refresh SIM operation is applicable for the active SIM only.

You can remotely view and manage all the LTE sites in your network using Citrix SD-WAN Center. For more information see, Remote LTE site management.

Configure the LTE functionality using CLI

To configure the 110-LTE-WiFi modem using CLI.

1. Log into the Citrix 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.

```
lte> help
Usage
    ?|help                                      # Print this message
    status [default|verbose]                    # Show status
    show                                        # Show configuration
    select [1|2] [1|2]                          # Show or choose modem and/or sim to work
    enable                                      # Enable the selected modem
    disable                                     # Disable the selected modem
    apn <apn> [<username> [<password> [<NONE|PAP|CHAP|PAPCHAP>]]]   # Set APN
    sim-prefer <prefer|use> <1|2>               # Prefer to use or use SIM one or two
    sim-power <show|off|on|reset>               # Show, off, on, reset SIM card power
    sim-pin <show>                              # SIM card pin status
    sim-pin <verify|disable|enable> <sim pin> # Verify/Disable/Enable SIM card PIN
    sim-pin <modify> <old pin> <new pin>        # Modify SIM card PIN
    sim-pin <unblock> <sim puk> <sim pin>       # Unblock SIM card PIN
    reboot                                      # Reboot modem
    list-fw                                     # List available firmware
    upload-fw <fw file>                         # Upload firmware file
    apply-fw <fw> [keep-AUTO-SIM]               # Apply firmware
    delete-fw <fw>                              # Delete firmware
    session <show|stop|start>                   # Show/stop/start data session
    exit|quit                                   # Exit LTE CLI
```

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 off,on,reset}	Powers off sim card, Power on sim card, Refresh sim card
Select [1l2] [1l2] {lte>select [1l2] [1l2]}	Select the SIM for LTE modem.
SIM-prefer {lte>sim-prefer}	Select the SIM preferred or to be used.
SIM PIN {lte>sim-pin}	SIM PIN related operations
Reboot {lte>reboot}	Restarts LTE modem

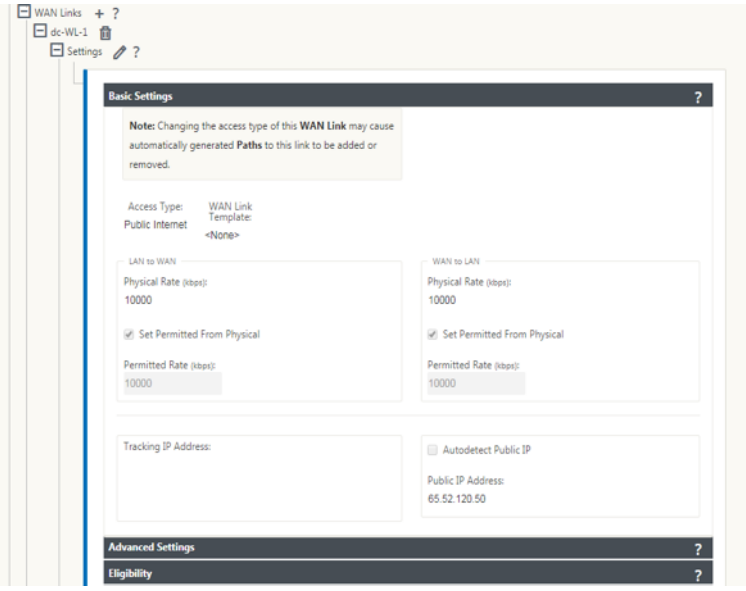
> **Note**
>
> The firmware related operations are not supported on 110-LTE-WiFi appliance.

Configure MCN for LTE

You cannot configure a 110-LTE-WiFi appliance as an MCN. However, for an MCN to work with an LTE branch appliance perform the following configurations on the MCN appliance.

To configure an MCN:

1. Log in to the SD-WAN appliance GUI. Go to Configuration Editor. Complete the configuration for the MCN site, see Configure MCN.
2. 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.

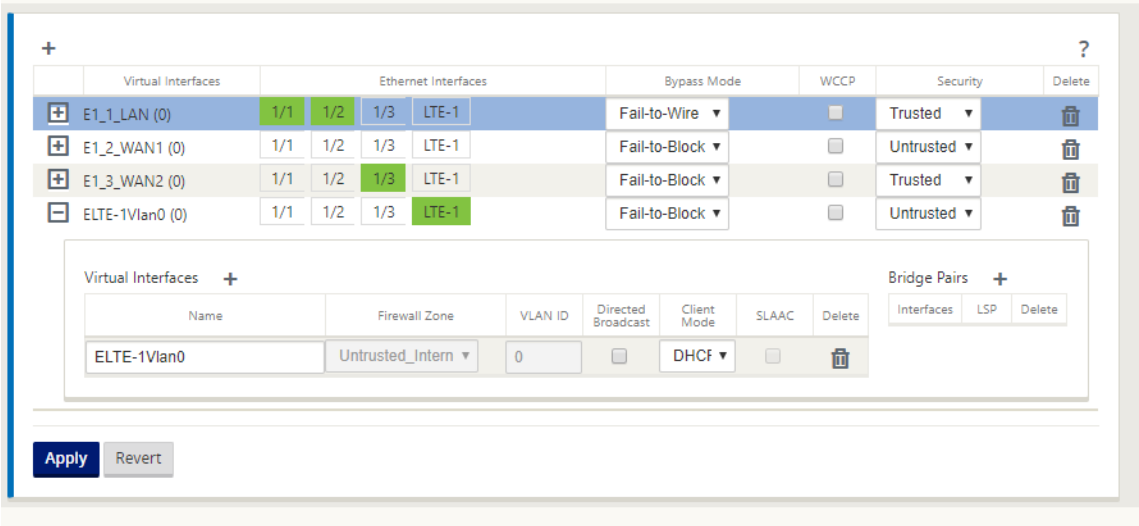


Configure branch for LTE

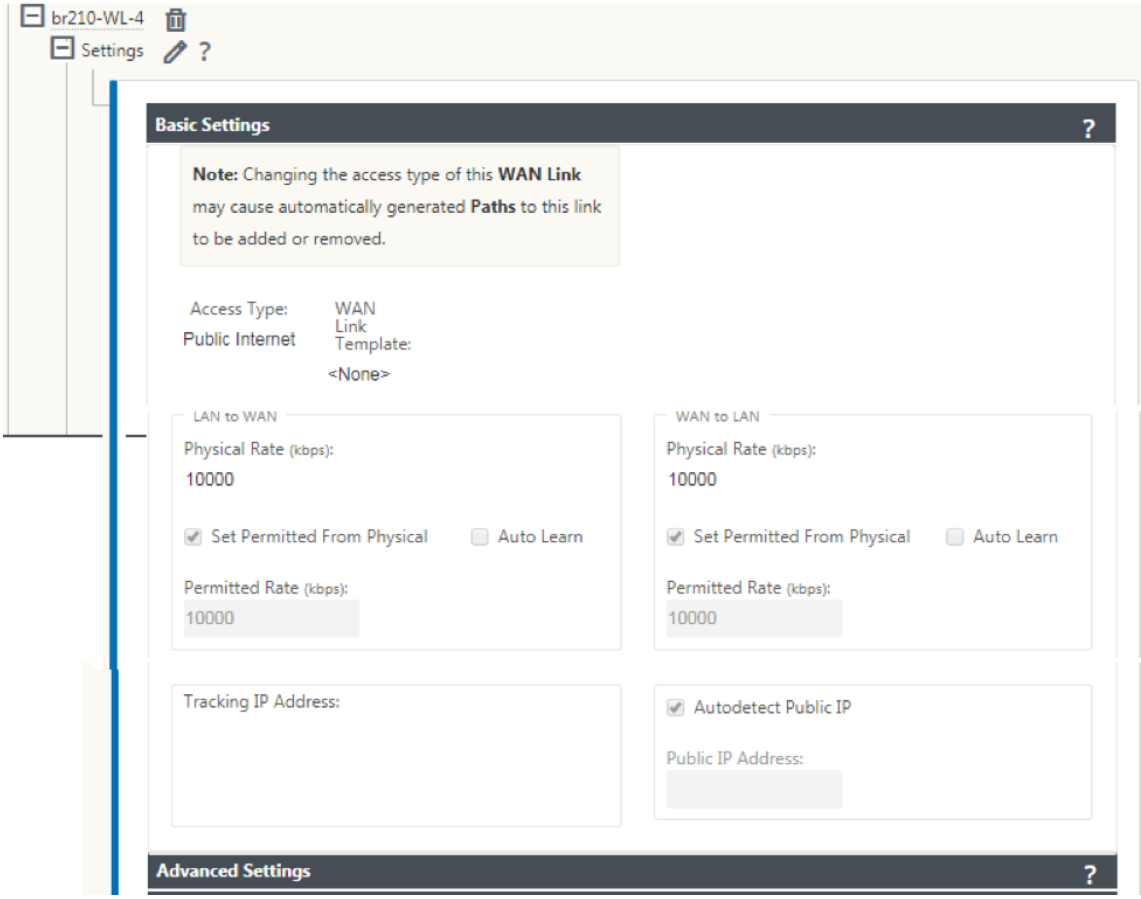
To configure the 110-LTE-WiFi appliance as a branch site:

1. In the SD-WAN appliance GUI, go to configuration editor. See Configure Branch.
   - Create Interface Groups.
   - Create up to one Virtual Interface and one Interface Group for the LTE adapter to configure WAN link by selecting the following:
     - Ethernet Interface –LTE 1
     - Security –untrusted (default)

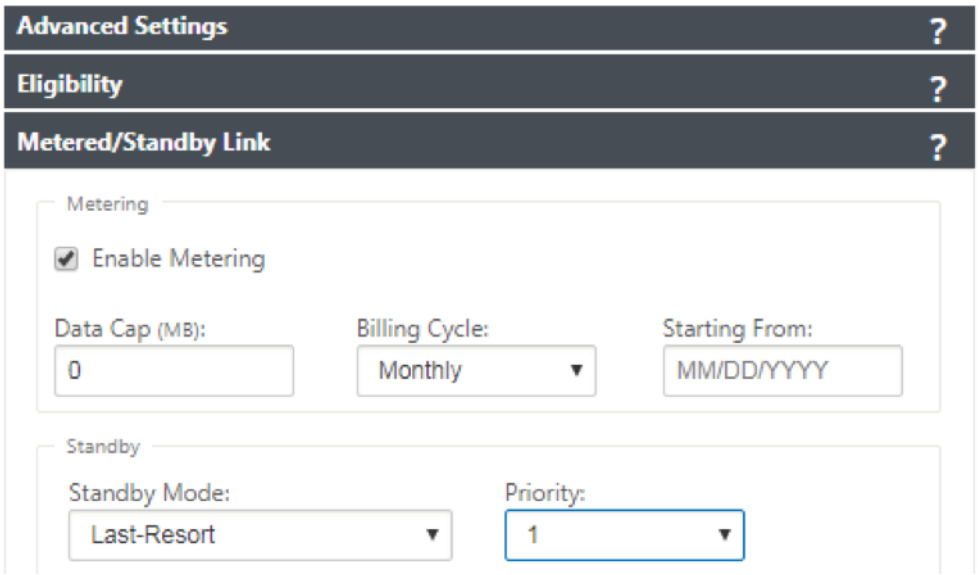
- DHCP Client –Enabled (default)



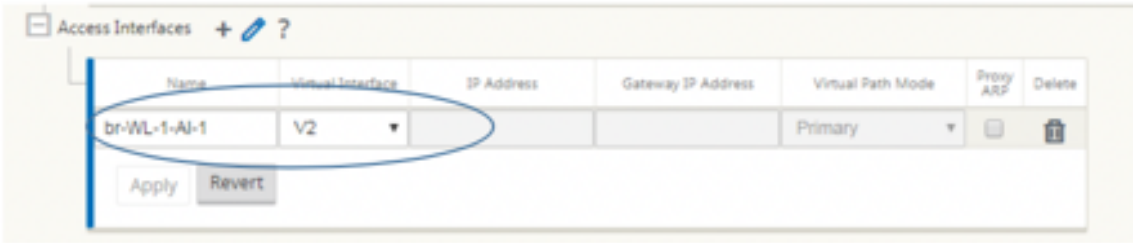
2. Enable **AutoDetect Public IP** for WAN link configuration when configuring WAN link using the virtual interface created for LTE interface.



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.



The IP address and gateway address for the Access Interface of the WAN link need not be configured because it receives that information from the carrier through DHCP.



4. Complete rest of the required Branch configuration for the 110-LTE-WiFi 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.

Zero-touch deployment over LTE

The SD-WAN 110 SE appliance supports both day-0 provisioning and day-n management of SD-WAN appliances via the management and data ports

Pre-requisites for enabling zero-touch deployment service over LTE:

1. Install the antenna, power ON the appliance, and insert the SIM card.
2. Ensure that the SIM card has an activated data plan.
3. Ensure that the management/data port is not connected.

- If the management/data port is connected, disconnect the management/data port.
- If a static IP address on the management/data Interface is configured, you must configure the management/data interface with DHCP, apply the configuration, and then disconnect the management/data port.

4. Ensure the 110-LTE-WiFi appliance configuration has internet service defined for LTE interface.

When the appliance is powered on, the zero-touch deployment service uses the LTE port to obtain the latest SD-WAN software and SD-WAN configuration.

You can use the SD-WAN Center GUI to deploy and configure 110-LTE-WiFi appliance for the zero-touch deployment service.

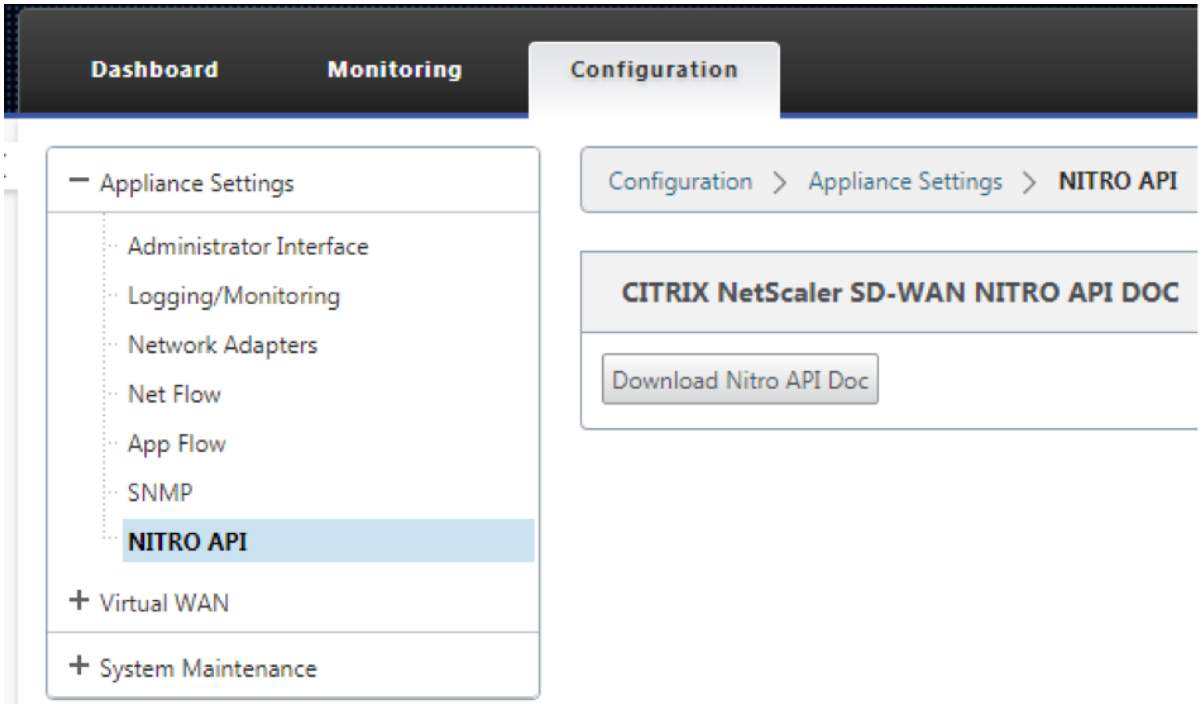
See the zero-touch deployment procedure for more information about deploying and configuring 110-LTE-WiFi appliance using SD-WAN Center.

Zero-touch deployment Service over management/data interface for 110-SE LTE appliance

Connect the management/data port to the internet and use the standard zero-touch deployment procedure that is supported on all other non-LTE platforms.

LTE REST API

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. The REST API for SIM PIN functionality is introduced in Citrix SD-WAN 11.0.



Configure external USB LTE modem

July 16, 2021

You can connect an external 3G/4G USB modem on certain Citrix SD-WAN appliances. The appliances use the 3G/4G network along with other connections to form a virtual network that aggregates bandwidth and provides resiliency. If there is a connectivity failure on the other interfaces, traffic is automatically redirected through the USB LTE modem. The following appliances support an external USB modem:

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

The Citrix SD-WAN 210 SE LTE and Citrix SD-WAN 110 LTE Wi-Fi SE appliances have a built-in LTE modem. Active dual LTE is supported on these appliances.

CDC Ethernet, MBIM, and NCM are the three types of external USB modems supported. You can configure the **APN** settings and Enable/Disable modem through the new Citrix SD-WAN GUI and Citrix SD-WAN Center. Mobile broadband operations are not supported on CDC Ethernet USB modems.

Connecting the USB modem

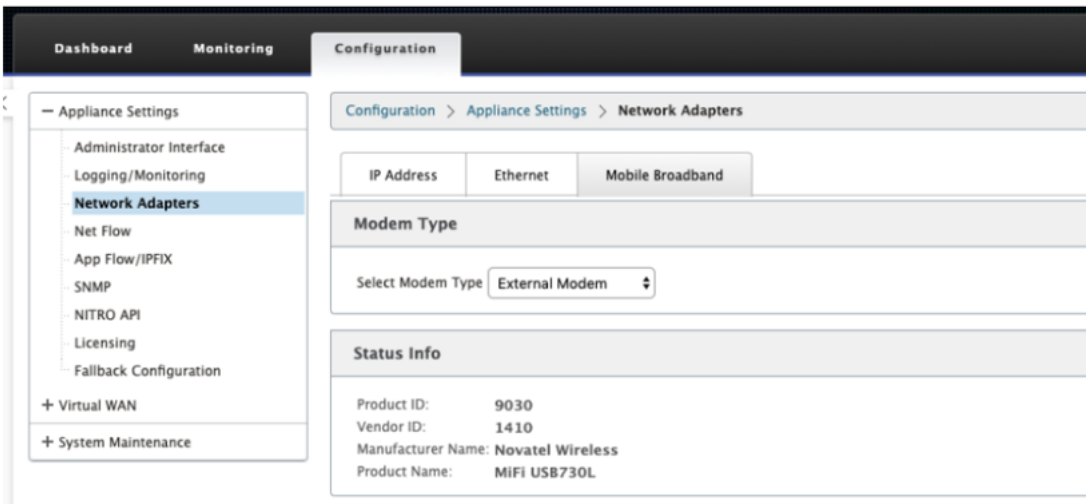
Enable and test the USB modem according to the guidelines provided by your wireless carrier.

Perquisites for external LTE modem:

- Use the supported USB LTE dongles. The supported dongle hardware models are Verizon USB730L and AT&T USB800.
- Ensure that a SIM card is inserted into the USB LTE dongle. The CDC Ethernet LTE dongles are pre-configured with a static IP address, this interferes with the configuration and cause connection failure or intermittent connection, if the SIM card is not inserted.
- Before inserting a CDC Ethernet LTE dongle into the SD-WAN appliance, connect the external USB stick to a Windows/Linux machine and ensure that the internet is working properly with proper APN and Mobile Data Roaming configuration. Ensure that the **Connection mode** of the USB dongle is changed from the default value **Manual** to **Auto**.

> **Note**
>
> - The Citrix SD-WAN appliances support only one USB LTE dongle at a time. If more than one USB dongle is plugged in, unplug all the dongles and plug in only one dongle.
> - The Citrix SD-WAN appliances do not support user name and password for USB modems. Ensure that the user name and password feature are disabled on the modem during setup.
> - Unplugging or rebooting an external MBIM dongle impacts the internal LTE modem data session. This is an expected behavior.
> - When an external LTE modem is plugged-in, the SD-WAN appliance takes about 3 minutes to recognize it.

To view the external modem details, in the appliance UI navigate to **Configuration** > **Appliance Settings** > **Network Adapters** > **Mobile Broadband**. Select **External Modem** as the modem type.



> **Note**
>
> - The SIM PIN and other LTE modem configurations are currently not supported.
> - The LTE USB dongle model number is not displayed in **Status Info** section.

You can remotely view and manage all the LTE sites in your network using the Citrix SD-WAN Center. For more information see, Remote LTE site management.

Configure the external USB modem

To configure an external USB modem, in the Configuration Editor navigate to Sites, select a site, and click **Interface Groups**. The external USB modem interface LTE-E1 is available to be configured. For more information on configuring a branch for LTE, see Configure branch for LTE.

Zero-touch deployment over LTE

Pre-requisites for enabling zero-touch deployment service over USB LTE modem:

- Insert the USB modem in the Citrix SD-WAN appliance. For more information, see Connecting the USB modem.
- Ensure that the SIM card on the USB modem has an activated data plan.
- Ensure that the management/data port is not connected. If the management/data port is connected, disconnect it.
- Ensure the appliance configuration has the internet service defined for the LTE interface.

When the appliance is powered on, the zero-touch deployment service uses the LTE-E1 port to obtain the latest SD-WAN software and SD-WAN configuration.

Use the SD-WAN Center GUI to deploy and configure the appliance for the zero-touch deployment service. For more information, see Zero Touch Deployment.
For information about zero-touch deployment through the SD-WAN Orchestrator see, Zero Touch Deployment.

Supported USB modems

The following modems are compatible with Citrix SD-WAN appliances.

> **Note**
>
> Citrix does not control the wireless carrier firmware updates. Therefore compatibility of new modem firmware to Citrix SD-WAN software is not guaranteed. Modem firmware update is controlled by the customer. Citrix recommends testing a firmware update on a single site before pushing it across the entire network.

Region	Wireless Carrier/ Manufacturer	USB Modem	Modem Type Supported	Interfaces
USA	Verizon	Global Modem USB730L	cdc_ether	4G only
USA	AT&T	AT&T Global Modem USB800	cdc_ether	4G only

Deployments

April 14, 2021

Following are some of the use case scenarios implemented by using Citrix SD-WAN appliances:

- Deploying SD-WAN in Gateway Mode
- Inline Mode
- Deploying SD-WAN in PBR mode (Virtual Inline Mode)
- Dynamic Paths for Branch to Branch Communication
- WAN to WAN forwarding
- Building an SD-WAN Network
- Routing for LAN Segmentation

- Utilizing Premium Edition Appliance to Provide WAN Optimization Services Only
- Two Box Mode
- Zero Touch Deployment
- Single Region Deployment
- Multi Region Deployment
- High Availability

Checklist and how to deploy

March 12, 2021

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.

Prepare for deployment

The following list outlines the steps and procedures involved in deploying the SD-WAN Standard and Premium (Enterprise) Editions.

To view some of the deploement use cases, see Deployments.

1. Gather your Citrix SD-WAN deployment information.
2. Set up the Citrix SD-WAN appliances.
    - For each hardware appliance you want to add to your SD-WAN deployment, you must complete the following tasks:
        - Set up the appliance hardware.
        - Set the Management IP Address for the appliance and verify the connection.
        - Set the date and time on the appliance.
        - (Optional) Set the console session **Timeout** interval to a high or the maximum value.
3. Upload and install the software license file on the appliance.

Installation and configuration checklist

Gather the following information for each 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

Best practices

March 12, 2021

This article outlines deployment best practices for the Citrix SD-WAN solution. It provides general guidance, advantages, use cases for the following Citrix SD-WAN deployment mode.

Edge/Gateway Mode

Recommendations

The following are the recommendations for the **Gateway** mode deployment:

1. The Gateway mode is best used for SD-WAN branches where router consolidation happens and customers are ready to allow SD-WAN to be the edge device terminating connections.

2. A great network architecture can be rendered with a scrupulous design when a project is built from scratch.

> **Note**
>
> The Gateway mode can be used on the data center side for the existing projects with some infrastructure disruption.

Advantages/Use cases

The following are the advantages/use cases for the Gateway mode deployment:

1. Best use case for Router/Firewall/Network element consolidation at the customer branch.
2. Simple and easy LAN host management via DHCP.
    - Allows SD-WAN to become the next-hop and offer DHCP based IP addressing to all LAN hosts for data ports.
3. All connections terminate at the SD-WAN edge/gateway and management becomes easy.
4. SD-WAN is the focal point of edge routing and is steered of all traffic. The decisions are made on the edge to breakout or backhaul or overlay including the bandwidth/capacity accounting.
5. All LAN subnets hosts as the LAN hosts are allowed to have SD-WAN LAN VIP as the next-hop. If SD-WAN LAN connects to a core switch, you can run dynamic routing to get visibility to all LAN subnets.
6. Great flexibility for High Availability (HA) - Strict recommendation for the gateway mode so that the site operates with an Active/Standby mode. Also, it helps to prevent traffic blackhole if the SD-WAN device goes down.
    - Switches available at the branch - Parallel high availability can work in gateway mode.
    - Switches not available at the branch - SD-WAN can also operate on SD-WAN edge high availability mode (fail-to-wire high availability mode) where the two SD-WAN boxes are daisy-chained to make use of fail-to-wire ports to act as a converged high availability pair.
7. Allow the Internet to be defined as **UNTRUSTED** interfaces which automatically create a dynamic NAT for breakout and source NAT the connection so the response comes back to SD-WAN.
8. Security considerations to **UNTRUSTED** interfaces are implied naturally, in that only ICMP/ARP/UDP control packets on 4980 are allowed.

Cautions

The following are the information that you need to be careful about in the Gateway mode:

- **Careful design and Network Architecture** - Gateway mode might need careful design and networking considerations as the entire branch/edge networking is in SD-WAN. What to block, what to route, how to network LAN, how to terminate WANs, and so on.
- **Failure of Device** - Edge mode cannot have the fail-to-wire capability. The entire branch goes down when the device is down.
- **Security Posture** - As the routing is managed at the edge, the security postures such as firewall, breakout/backhaul considerations are crucial and that must be conceived with the customer.
- **High Availability** –Fail-to-wire high availability must have some port availability considerations and depending on deployments might become tricky to design.
  - SD-WAN 110 is NOT an option as it does not have fail-to-wire ports.

For instance, if you need 2 WAN Links to operate, you need 5 ports including a dedicated port for the high availability interface including the LAN interface.

Inline Mode –Fail-to-wire/Fail-to-block

Recommendations

The following are the recommendations for the **Inline** mode deployment:

1. The inline mode is best for the branches where the existing infrastructure is not to be changed and SD-WAN sits transparently inline to the LAN segment.
2. Data center's can also employ inline fail-to-wire or inline parallel high availability as it is immensely important to ensure that the data center workloads are not blackholed due to device down/crash.

Advantages and use-cases

The following are the advantages/use cases for the Inline mode deployment:

1. Keeping the MPLS router therefore fail-to-wire is a lovely feature. Fail-to-wire capable devices enable seamless failover to underlay infrastructure if the box went down.
   - If your devices support fail-to-wire (SD-WAN 210 and above), this allows placing a single SD-WAN inline to hardware bypass the LAN traffic to the customer edge router when the SD-WAN crashes/goes down.
   - If the MPLS Links are present that yield a natural extension to the customer's LAN/Intranet, the fail-to-wire bridge-pair port is the best choice (fail-to-wire capable pairs) such that,

when the device crashes or goes down the LAN traffic is hardware bypassed to the customer edge router (still maintained the next hop).

2. Networking is simple.
3. SD-WAN sees all traffic through the inline mode, so it is the best-case scenario for the proper bandwidth/capacity accounting.
4. Few integration requirements as you need only an IP of the L2 segment. LAN segments are well known as you have an arm to the LAN interface. If you connect to a core switch, you can also run dynamic routing to get visibility to all LAN subnets.
5. Customer's expectations are that SD-WAN must blend into the existing infrastructure as a new network node (nothing else changes).
6. **Proxy ARP** –In inline mode, it is a blessing for SD-WAN to proxy ARP requests to LAN next-hop if the gateway went down or the SD-WAN interface towards next-hop went down.
   - Generally, in inline mode with bridge-pair (fail-to-block or fail-to-wire) with multiple WAN connections (MPLS/Internet), it is recommended to enable Proxy ARP for the bridge pair interface that connects the LAN hosts to their next-hop gateway.
   - For any reason when the next-hop is down or the SD-WAN interface to the next-hop is down rendering the gateway unreachable, SD-WAN acts as a proxy for ARP requests allowing the LAN hosts to still seamlessly send packets and use the remaining WAN connections that keep the virtual path up.
7. **High availability** - If fail-to-wire is not an option, devices can be placed in parallel high availability (common LAN and WAN interfaces for the Active/Standby) devices to achieve redundancy.
   - If your appliances don't support fail-to-wire, like the SD-WAN 110, you have to go with inline parallel high availability that enables to have a standby device kick in if the primary went down.

Cautions

The following are the information that you need to be careful about in the **Inline** mode:

- Plumbing network with two arms to the SD-WAN (LAN and WAN side), needs some downtime as the network must be plumbed in two arms.
- Must ensure if fail-to-wire is used, it is behind a customer edge router/firewall in a **TRUSTED** zone so that security is not compromised.
- MPLS QoS changes a little in this as the previous QoS policies might have depended on the source IP addresses or DSCP based which will now be masked because of an overlay.

- Care must be taken to repurpose the MPLS router with a well-designed SD-WAN specific reserved bandwidth with a specific DSCP tag, such that SD-WAN's QoS takes care of prioritizing traffic and sends out high priority applications immediately followed by other classes (but be able to account for the overall bandwidth reserved for SD-WAN on the MPLS router). MPLS queues are an alternative or MPLS with a single DSCP set on the auto path group that can take care of this.
- If the Internet interfaces are **TRUSTED** as the links terminate on the customer edge router, to use Internet service, you must write an exclusive dynamic NAT rule to enable internet breakout from the appliance.
- If the Internet links are the only WAN connections and still terminate on the customer edge router, it is still fine to bypass the connections if the customer edge router takes precautions to steer the packets via their existing underlay infrastructure.
  - Proper care must be taken to account for the flow of bypassing LAN traffic over bridge-pair with an Internet connection and when the appliance is down. Since this is a sensitive enterprise Intranet traffic, in the eve of failure, the customer must know how to handle it.

Virtual Inline/One-arm mode

Recommendations

The following are the recommendations for the **Virtual Inline** mode deployment:

1. The virtual inline mode is best for data center networking as the SD-WAN network plumbing can be worked on parallel while the data center is serving its existing workloads with existing infrastructure.
2. SD-WAN is in a one-arm interface that is managed with an SLA tracking on VIPs. If the tracking goes down, the traffic resumes routing via existing underlay infrastructure.
3. Branches can also be deployed in virtual inline mode, however are more predominant with In-line/Gateway deployments.

Advantages and Use-cases

The following are the advantages/use cases for the **Virtual Inline** mode deployment:

1. Simplest and recommended way to network SD-WAN in the data center.
   - The virtual inline mode allows parallel network plumbing of SD-WAN with the head-end core router.

    - The virtual inline mode allows us to easily define PBRs to divert LAN traffic must go through SD-WAN and get overlay benefits.

2. Seamless failover to underlying infrastructure if SD-WAN is to fail, and seamless forwarding to SD-WAN for overlay benefits under normal conditions.
3. Simple **Networking** and **Integration** requirements. The single one-arm interface from headend router to SD-WAN in virtual inline.
4. Easy to deploy dynamic routing in **Import only mode** (export nothing) to get visibility of LAN subnets so they can be sent to remote SD-WAN peer appliances.
5. Easy to define PBR on the routers (1 per WAN VIP) to indicate how to choose the physical.

Cautions

The following are the information that you need to be careful about in the **Virtual Inline** mode:

- Proper care must be taken to distinctly MAP the SD-WAN logical VIP of a WAN link defined to the right physical interface (else this might cause undesirable issues in WAN metric assessment and choice of wan paths).
- Proper design considerations are to be made to know if all traffic is diverted via SD-WAN or only specific traffic.
- This means SD-WAN must be dedicated some share of bandwidth exclusively for itself that must be set on the interfaces such that SD-WAN's capacity is not used by other non-SD-WAN traffic causing undesirable outcomes.
    - Bandwidth accounting issues and congestion issues might occur if SD-WAN WAN links capacity is defined incorrectly.
- Dynamic routing can cause some issues if improperly designed where if the SD-WAN routes data center and branch VIPs are exported to the headend and if routing is influenced towards SD-WAN, overlay packets start looping and cause undesirable outcomes.
- Dynamic routing must be properly administered considering all potential factors of what to learn/what to advertise.
- One-arm physical interface might become a bottleneck sometimes. Needs some design considerations in those lines as it caters to both upload/download and also acts as LAN to LAN and LAN to WAN/WAN to LAN traffic from SD-WAN.
- Excessive LAN to LAN traffic might be a point to note during design.
- If the dynamic routing is not used, there must be proper care if administering all LAN subnets, which if not, might cause undesirable routing issues.

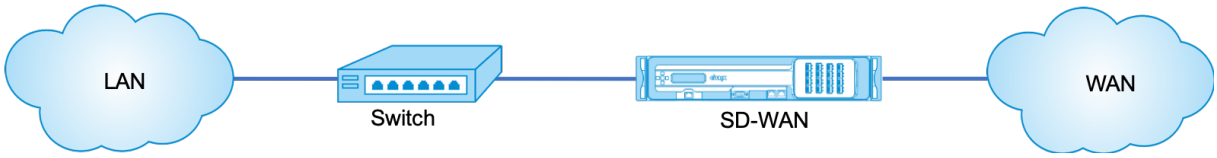
- There are potential routing loop issues if you define some default route (0.0.0.0/0) on the SD-WAN in the virtual inline to point back to the headend router. In such situations, if the virtual path went down, any traffic coming from the data center LAN (like monitoring traffic) is looped back to the headend and back to SD-WAN causing undesirable routing issues (If the virtual path is down, the remote branch subnets become reachable **NO** causing the default route to be HIT, that causes the loop issues).

Gateway mode

March 12, 2021

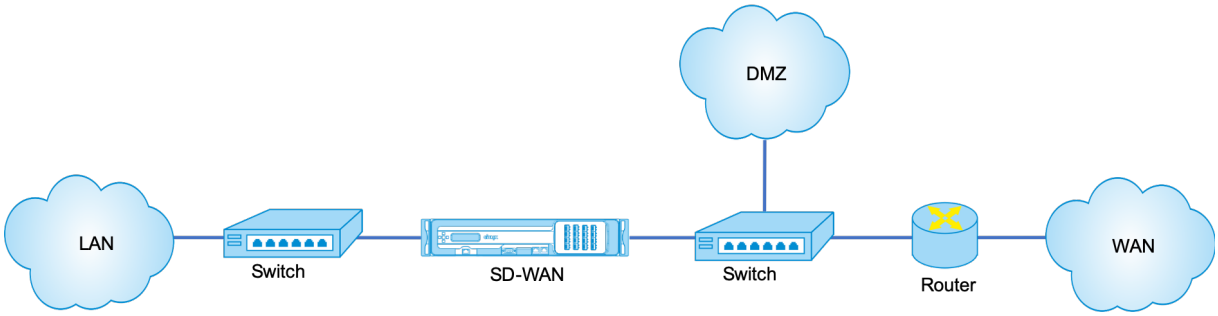
Gateway mode places the SD-WAN appliance physically in the path (two-arm deployment) and requires changes in the existing network infrastructure to make the SD-WAN appliance the default gateway for the entire LAN network for that site. Gateway mode used for new networks and router replacement. Gateway mode allows SD-WAN appliances:

- To view all traffic to and from the WAN
- To perform local routing



> **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.

In the **Inline** mode, the SD-WAN appliance appears to be an Ethernet bridge. Most of the SD-WAN appliance models include a fail-to-wire (Ethernet bypass) feature for inline mode. If power fails, a relay closes and the input and output ports become electrically connected, allowing the Ethernet signal to pass through from one port to another. In the fail-to-wire mode, the SD-WAN appliance looks like a cross-over cable connecting the two ports. Inline mode used to integrate into already well-defined networks.

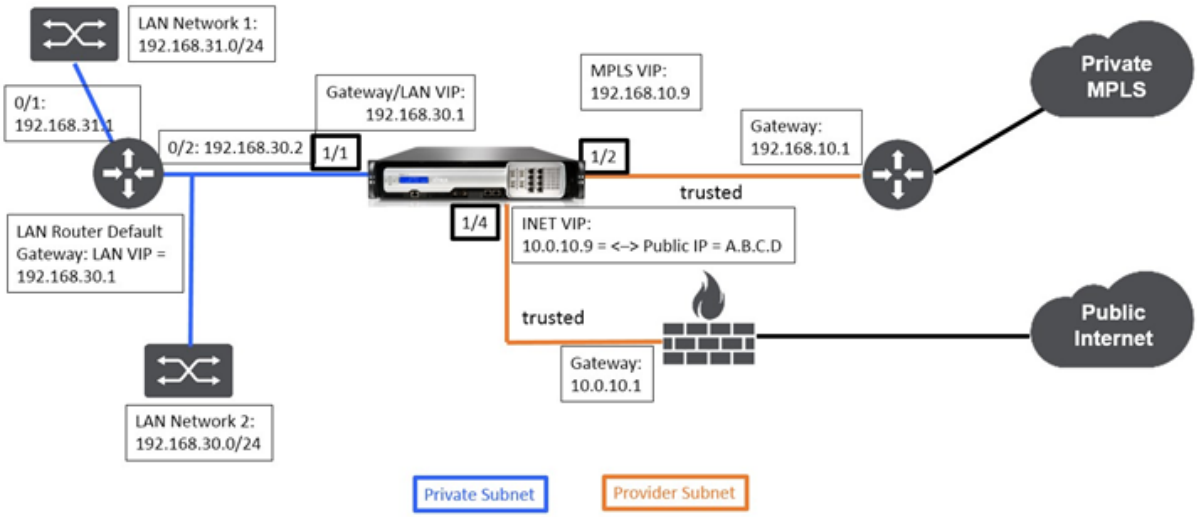


This article provides step-by-step procedure to configure an SD-WAN appliance in Gateway mode in a sample network setup. Inline deployment is also described for the branch side to complete the configuration. A network can continue to function if an Inline device is removed, but loses all access if the Gateway device is removed.

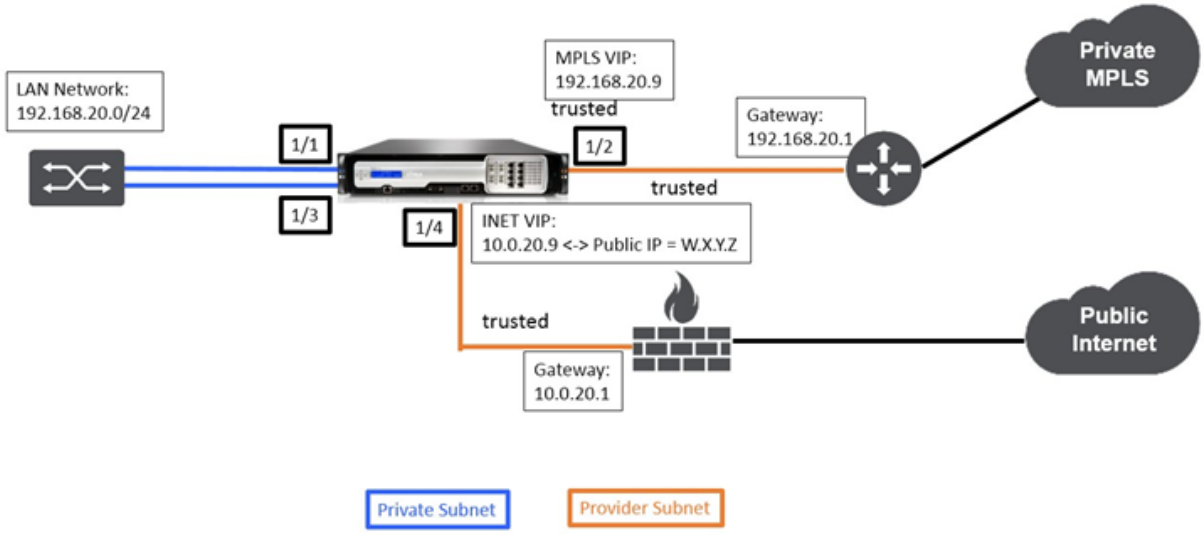
Topology

The following illustrations describe the topologies supported in an SD-WAN network.

Data Center in gateway deployment



Branch in inline deployment



Deployment requirements

Deployment requirements and related information are described below to assist you in building the configuration.

Site Name	Data Center 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

Site Name	Data Center Site	Branch Site
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

Configuration pre-requisites

- 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 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 must only be one active MCN in an SD-WAN network.

2. Start Configuration by navigating to **Configuration** > **Virtual WAN** > **Configuration Editor**. Click the **New** to begin configuration.

Data center site gateway mode configuration

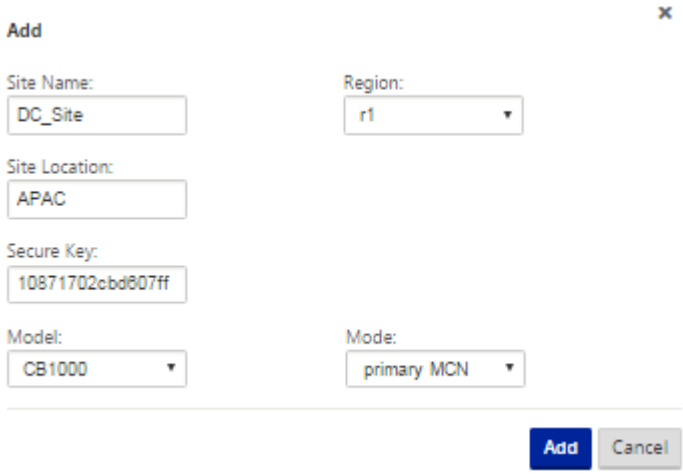
Following are the high-level configuration steps to configure data center site Gateway deployment:

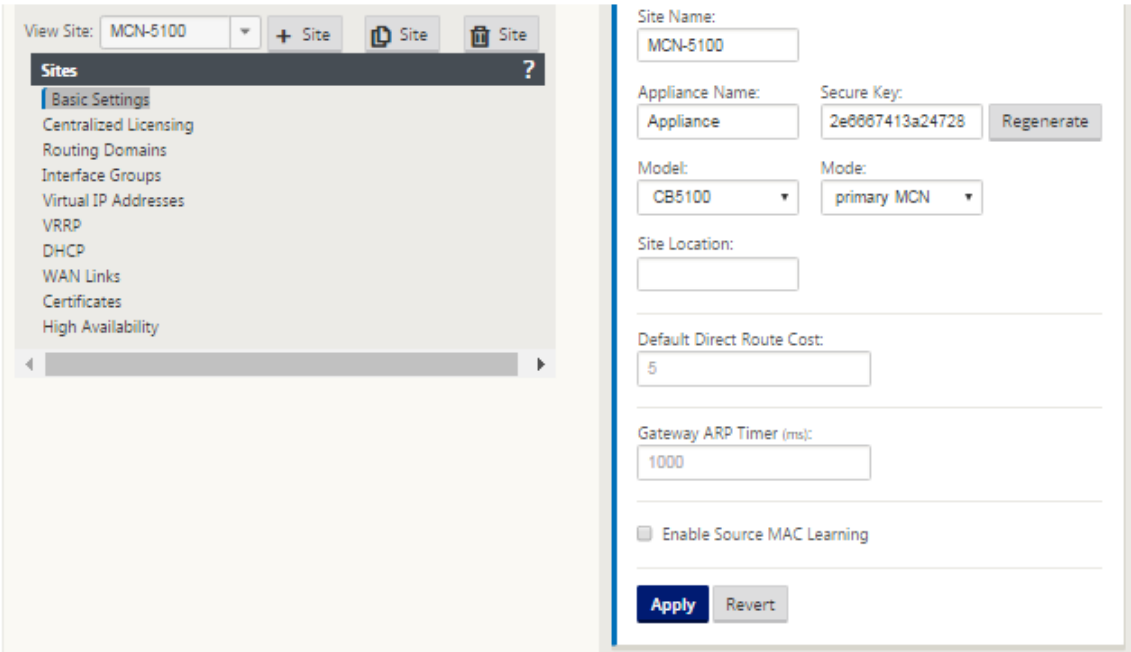
1. Create a DC site.
2. Populate Interface Groups based on connected Ethernet interfaces.
3. Create Virtual IP address for each virtual interface.
4. Populate WAN links based on physical rate and not burst speeds using Internet and MPLS Links.
5. Populate Routes if there are more subnets in the LAN infrastructure.

To create a DC site

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.

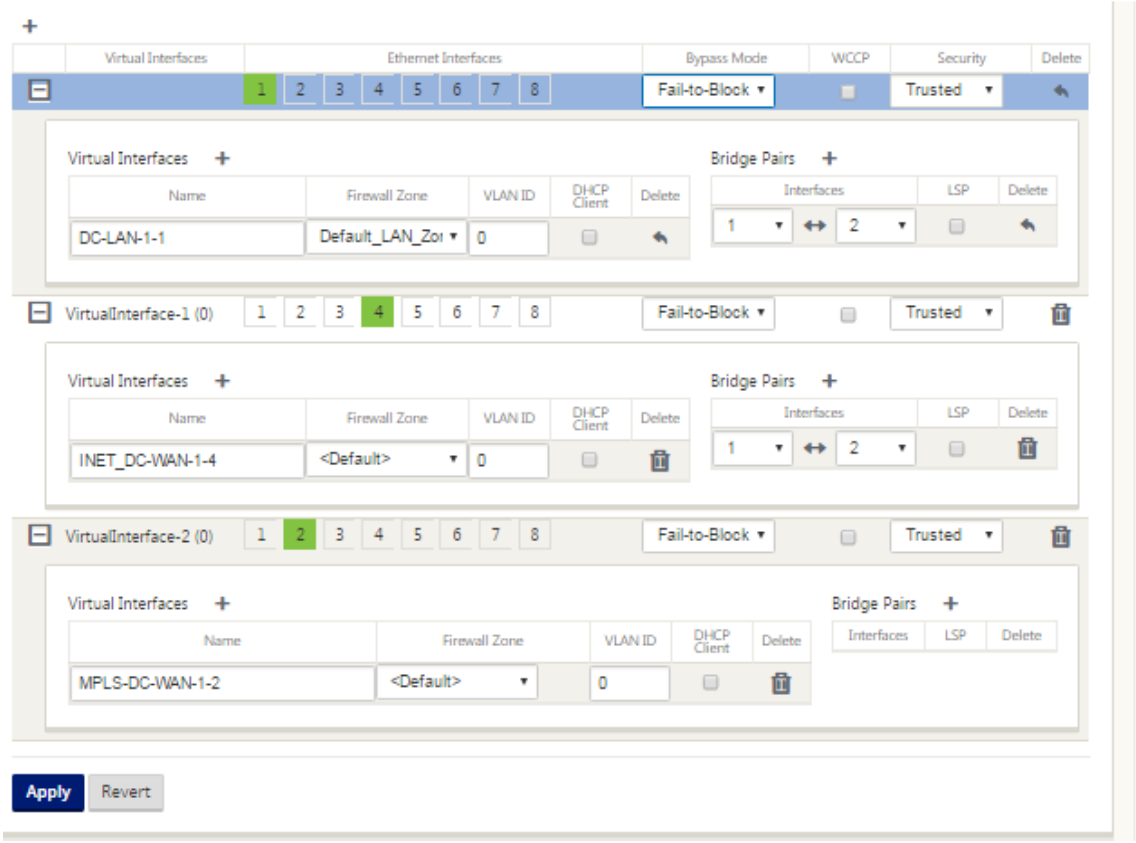




To configure interface groups based on connected Ethernet interfaces

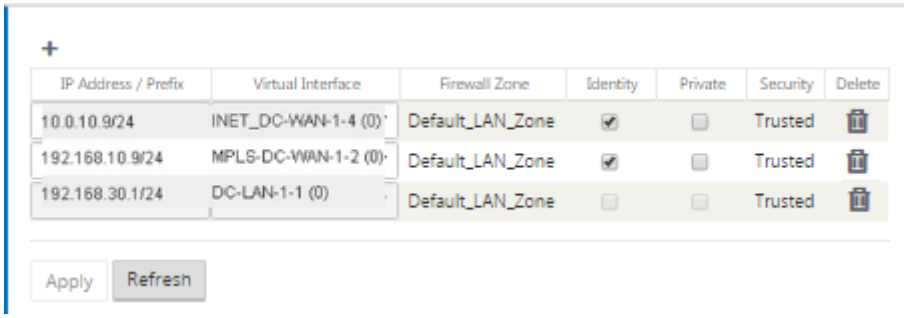
1. In the **Configuration Editor**, navigate to **Sites** > **View Site** > **[Site Name]** > **Interface Groups**. Click **+** to add interfaces intended to be used. For Gateway Mode, each Interface Group is assigned a single Ethernet interface.
2. Bypass mode is set to **fail-to-block** since only 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.



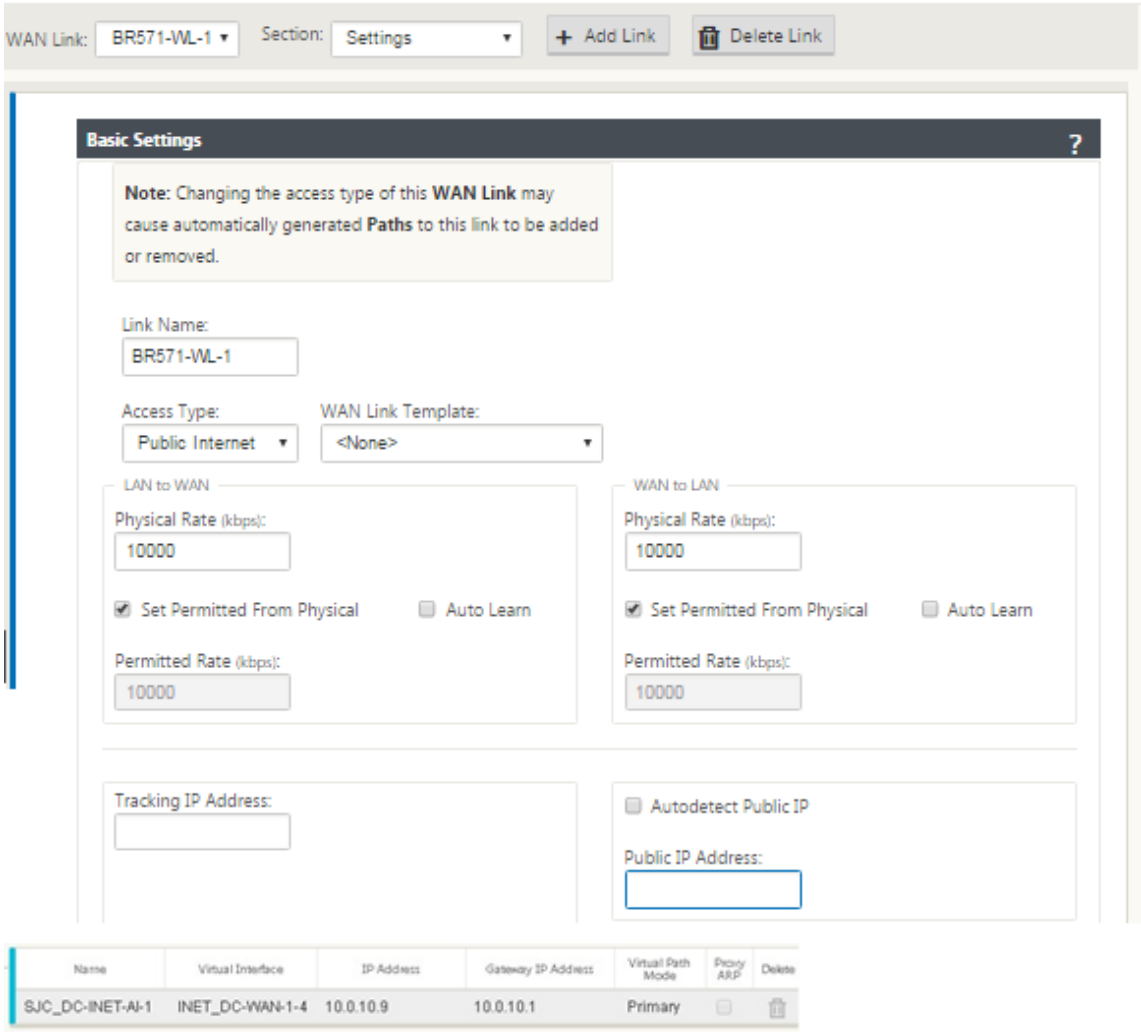
To create Virtual IP (VIP) address for each virtual interface

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.



To populate WAN links based on physical rate and not on burst speeds using Internet link:

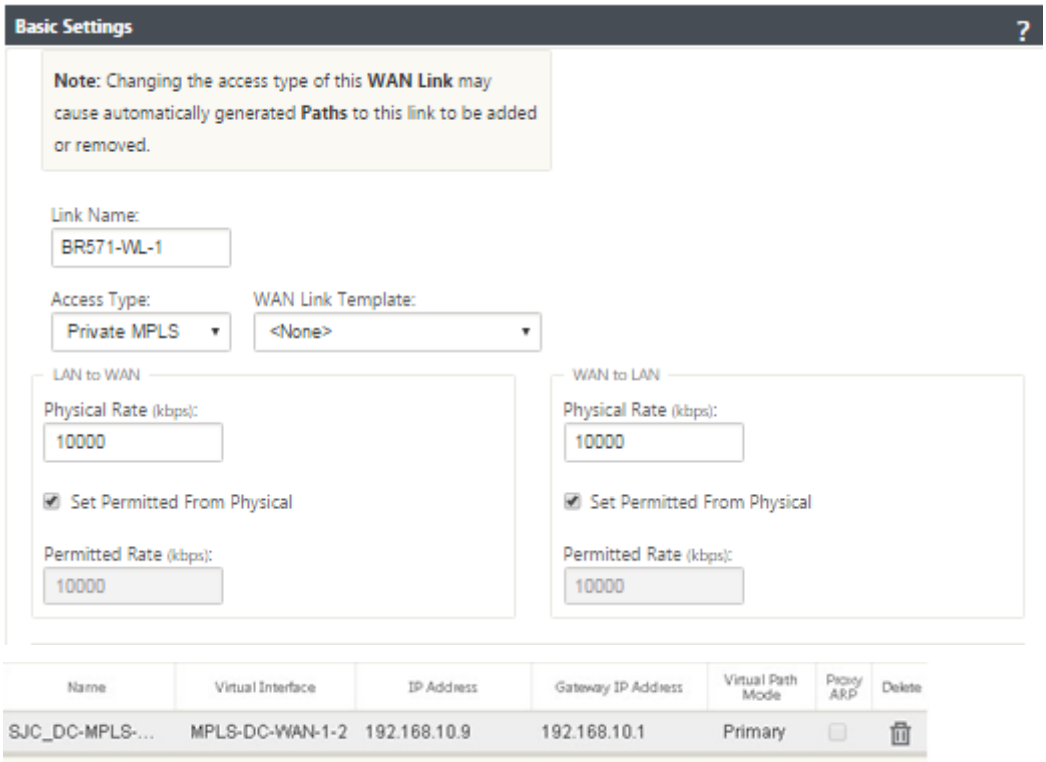
1. Navigate to **WAN Links**, click the **+ Add Link** button to add a WAN Link for the Internet link.
2. Populate Internet link details, including the supplied Public IP address as shown below. AutoDetect **Public IP** cannot be selected for SD-WAN appliance configured as MCN.
3. Navigate to **Access 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.



To create MPLS Link

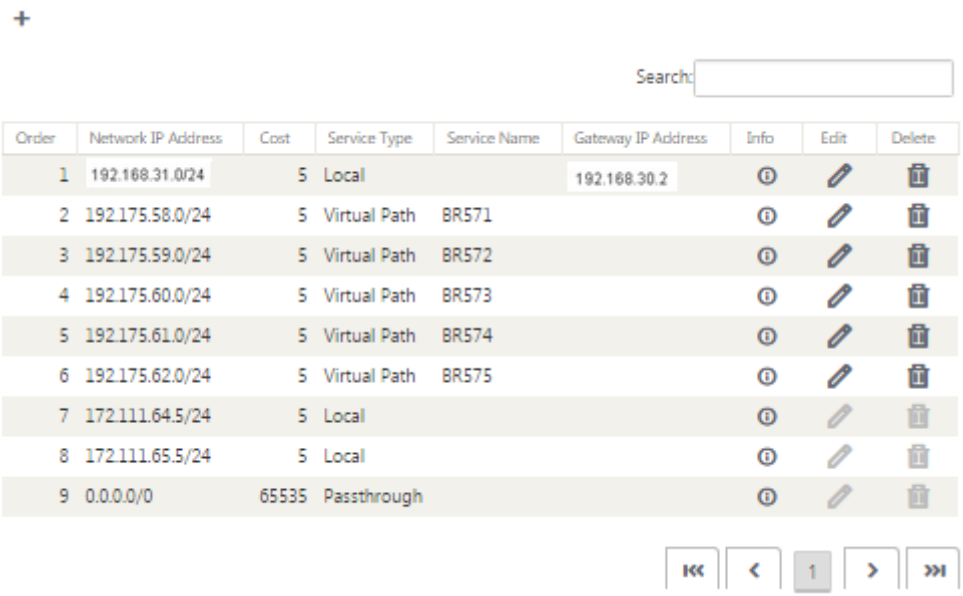
1. Navigate to **WAN Links**, click the **+** button to add a WAN Link for the MPLS link.
2. Populate MPLS link details as shown below.
3. Navigate to **Access Interfaces**, click the **+** button to add interface detail specific for the MPLS link.

4. Populate Access Interface for IP and gateway addresses as shown below.



To populate Routes

Routes are auto-created based on the above configuration. The DC LAN sample topology shown above has an extra 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.



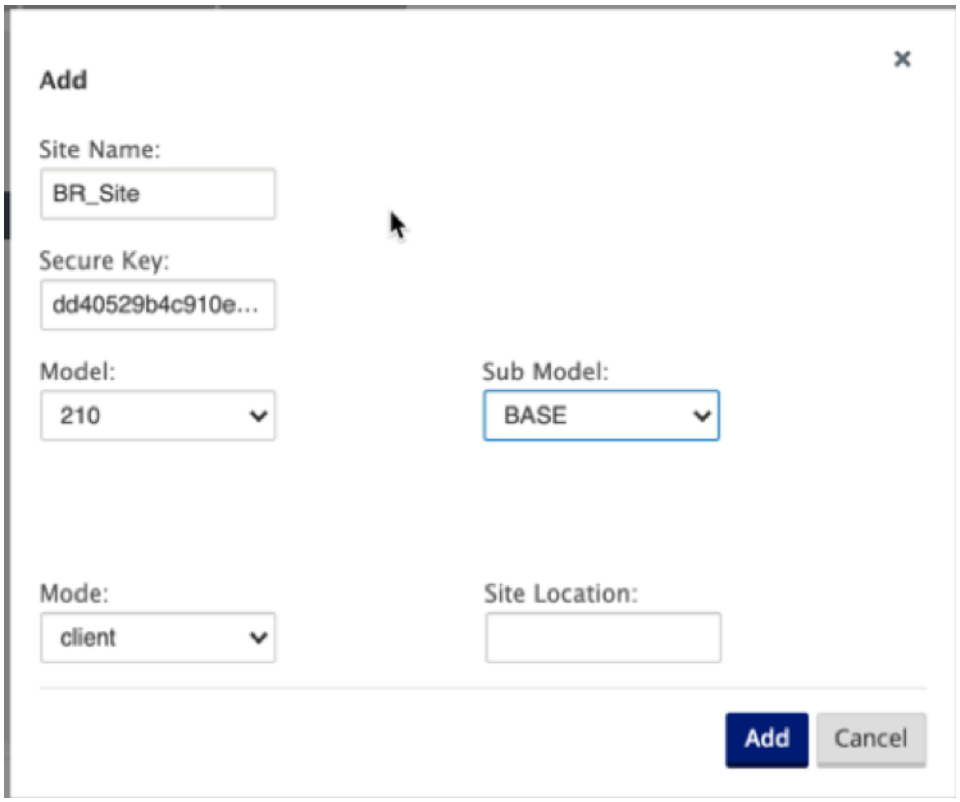
Branch site inline deployment configuration

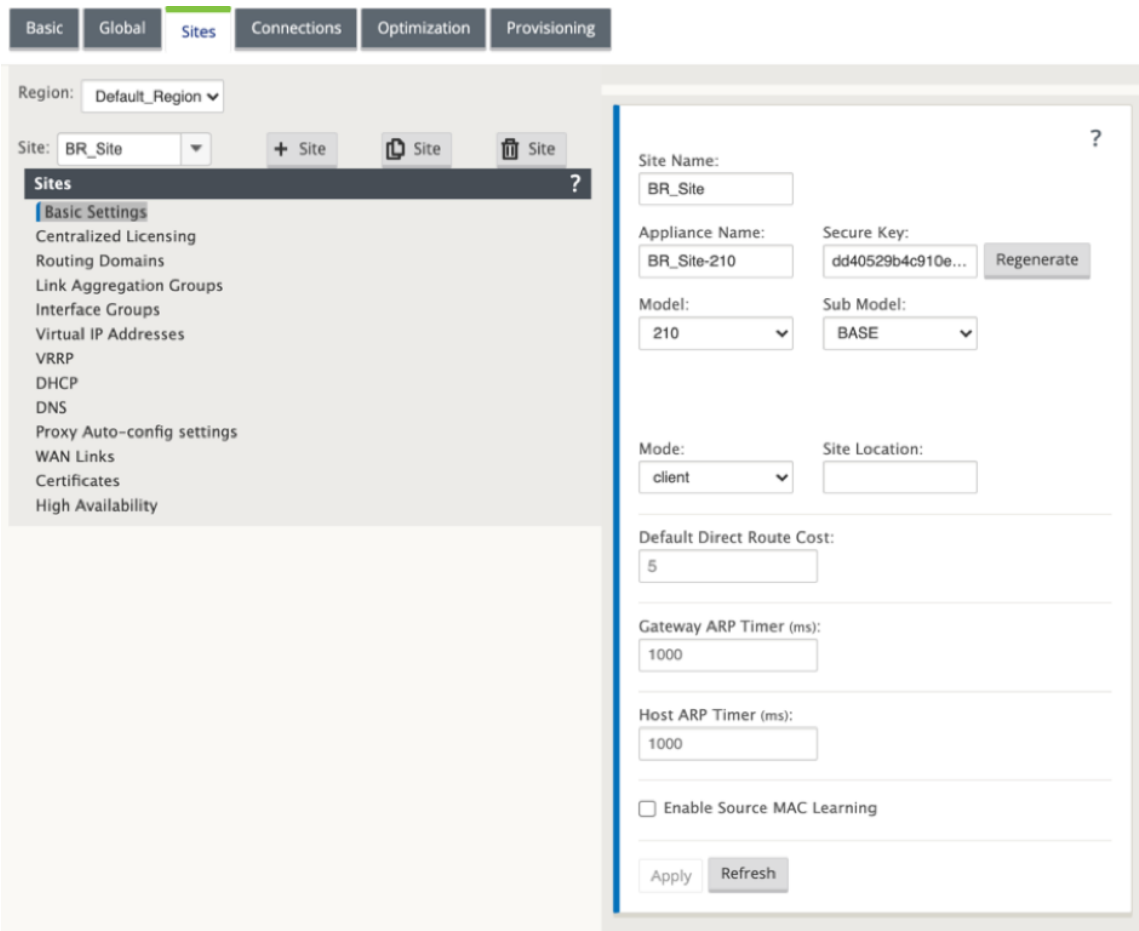
Following are the high-level configuration steps to configure Branch site for Inline deployment:

1. Create a 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 more subnets in the LAN infrastructure.

To create a Branch site

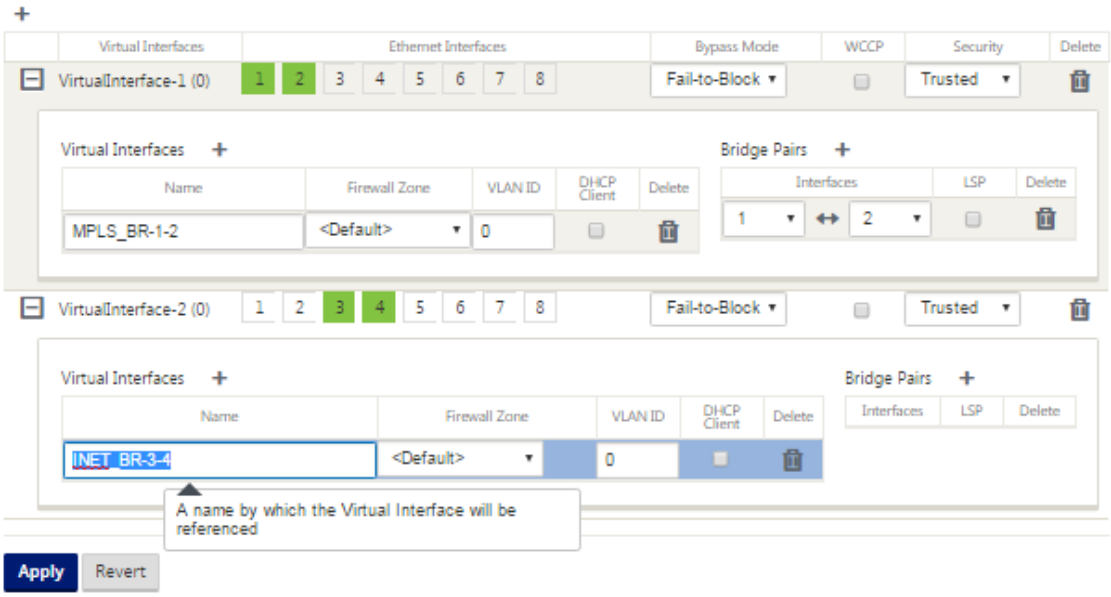
1. Navigate to **Configuration Editor** > **Sites**, and click the "**+**"**Add** button.
2. Populate the fields as shown below.
3. Keep default settings unless instructed to change.





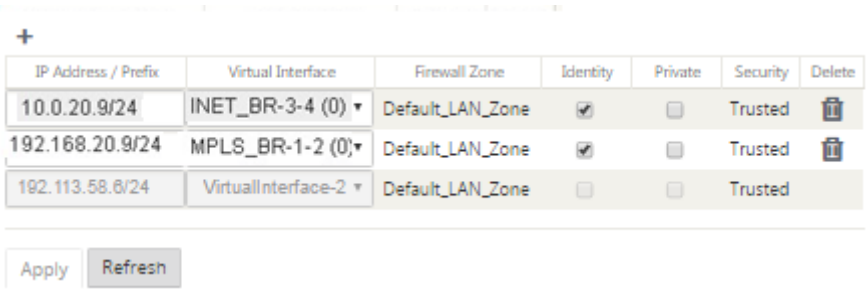
To populate interface groups based on connected Ethernet interfaces

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.



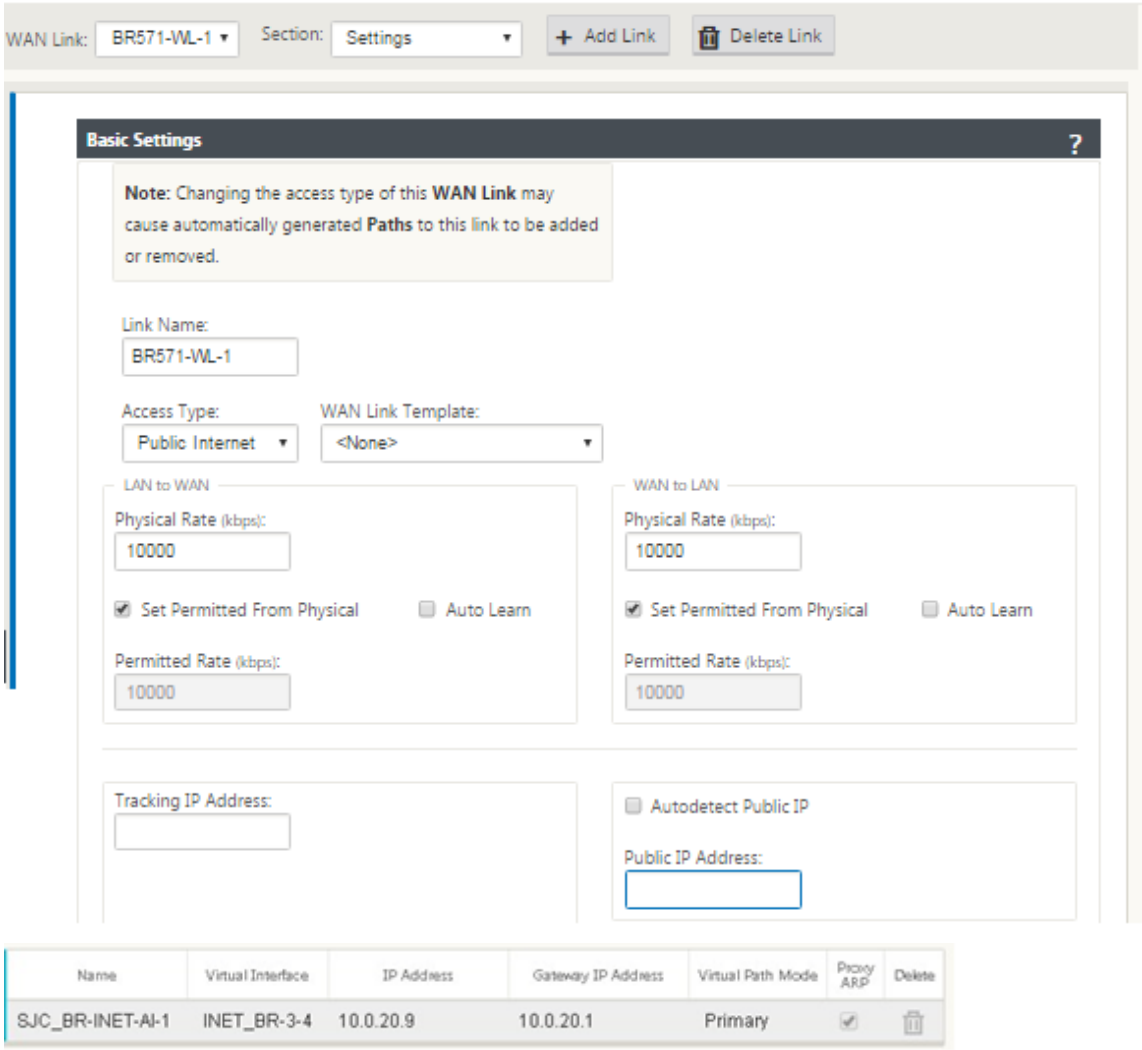
To create Virtual IP (VIP) address for each virtual interface

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.



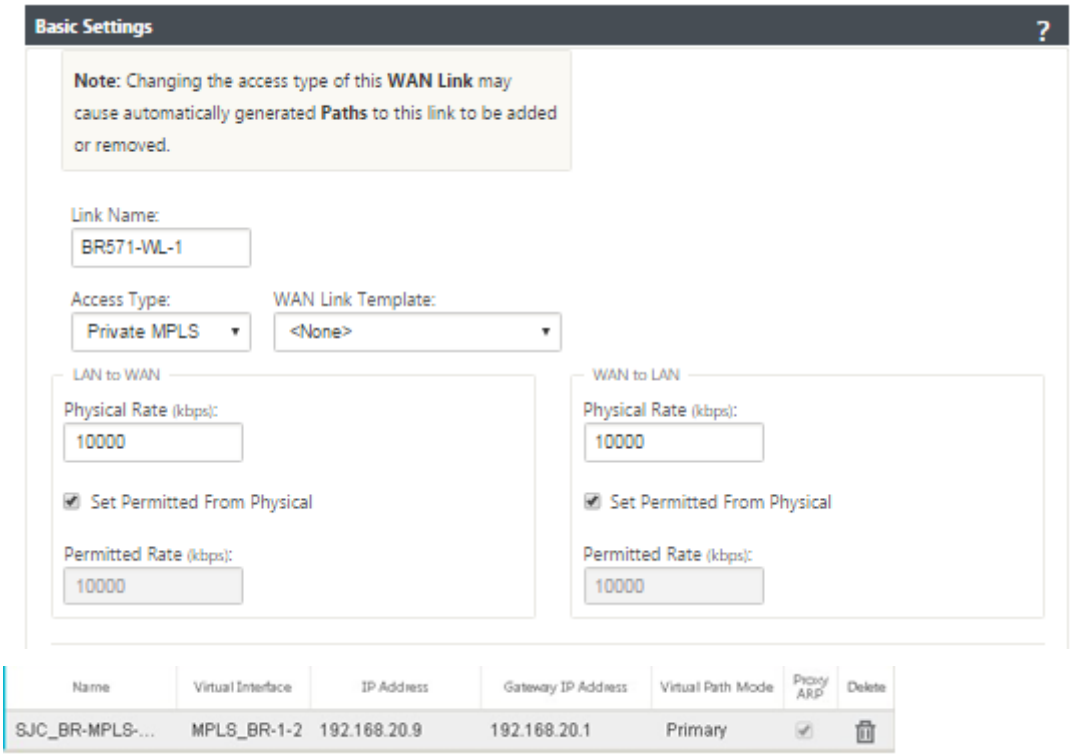
To populate WAN links based on physical rate and not on burst speeds using Internet link:

1. Navigate to **WAN Links**, click the **+** button to add a WAN Link for the Internet link.
2. Populate Internet link details, including the Auto Detect 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.



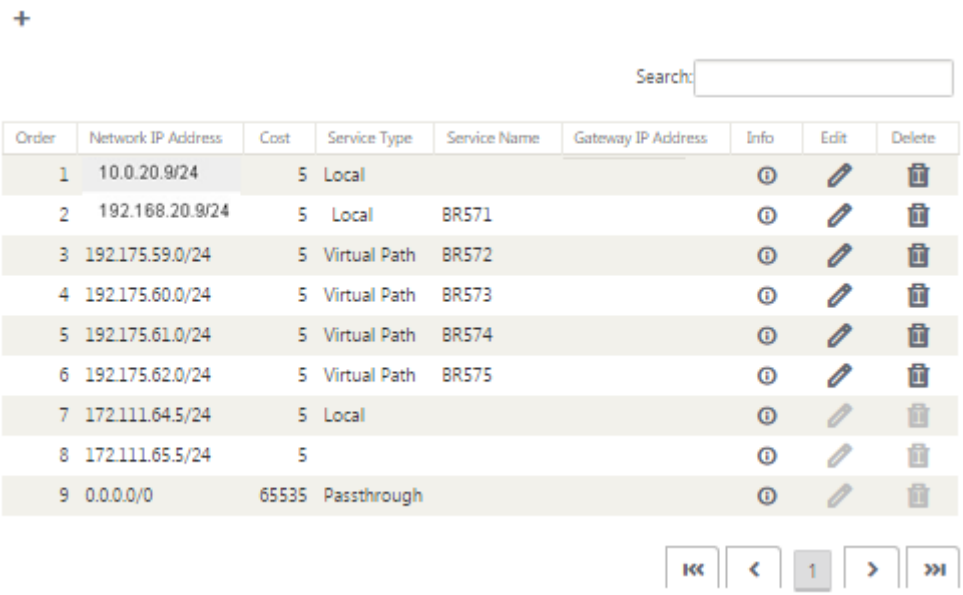
To create MPLS link

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.



To populate routes

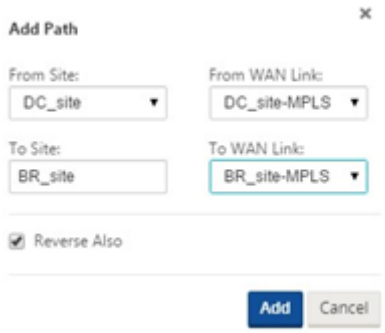
Routes are auto-created based on above configuration. In case there are more subnets specific to this remote branch office, then specific routes need to be added identifying which gateway to direct traffic to reach those back-end subnets.



Resolve audit errors

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 generates 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 Add operator (in the green rectangle).



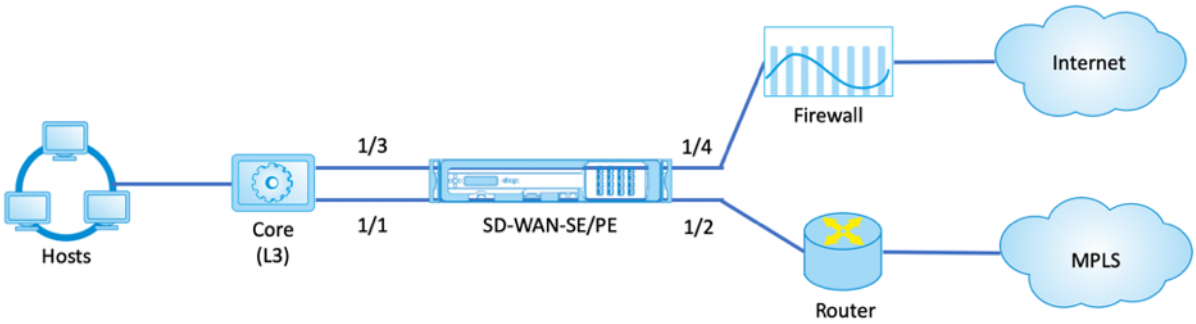
After completing all the above steps, proceed to Preparing the SD-WAN Appliance Packages.

Inline mode

March 12, 2021

This article provides the detail on configuring a branch with **Inline Deployment** mode. In this mode, the SD-WAN appliance appears to be an Ethernet bridge. Most of the SD-WAN appliance models include a **fail-to-wire** (Ethernet bypass) feature for inline mode. If power fails, a relay closes and the input and output ports become electrically connected, allowing the Ethernet signal to pass through from one port to another. In the fail-to-wire mode, the SD-WAN appliance looks like a cross-over cable connecting the two ports.

In the following diagram interfaces 1/1 and 1/2 are hardware bypass pairs and will fail-to-wire connecting the Core to the edge MPLS Router. Interfaces 1/3 and 1/4 are also hardware bypass pairs and will fail-to-wire connecting the Core to the edge Firewall.



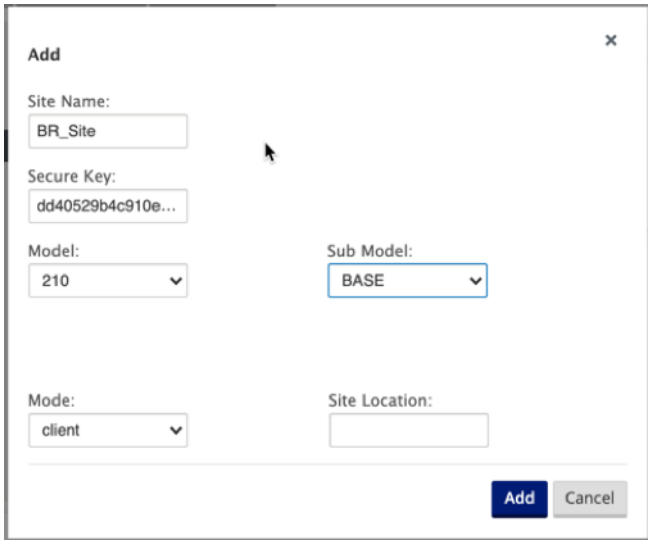
Branch site inline deployment configuration

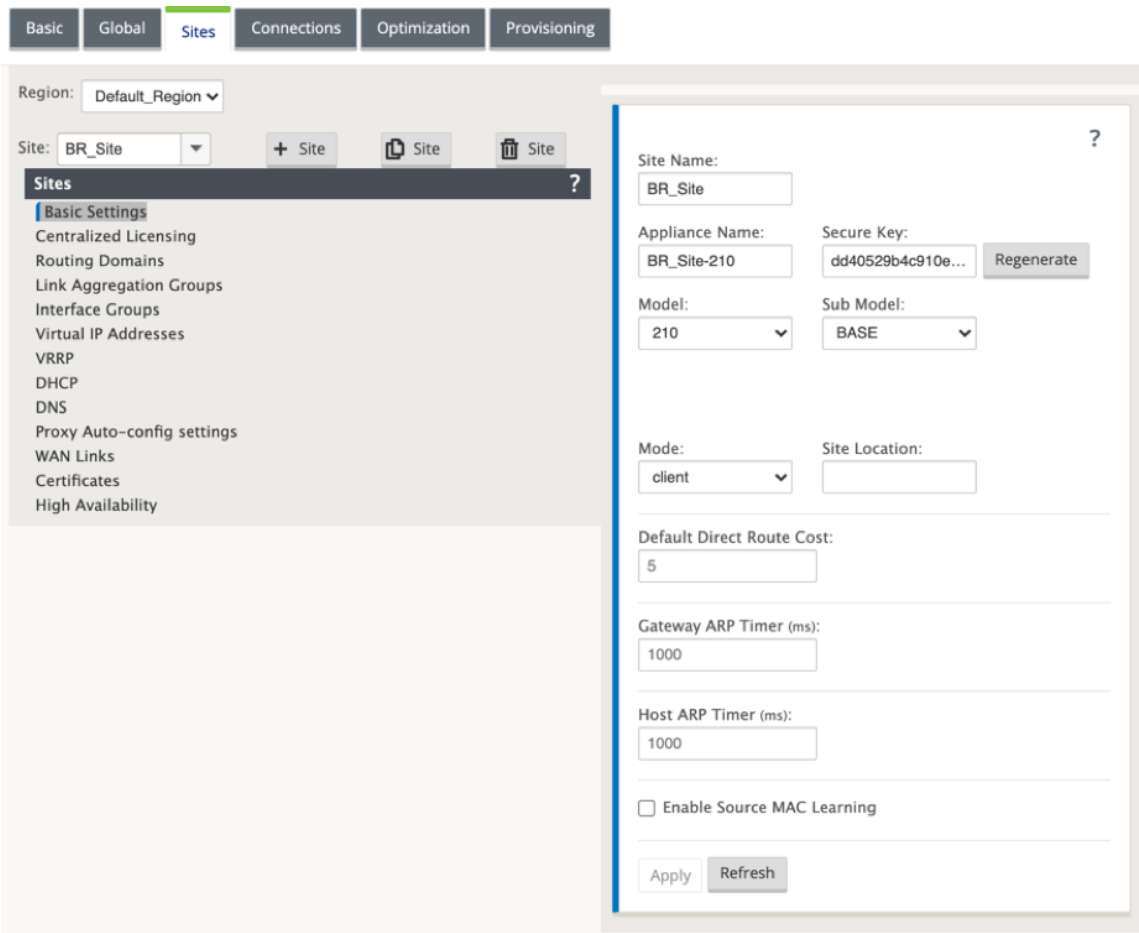
Following are the high-level configuration steps to configure Branch site for Inline deployment:

1. Create a 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 more subnets in the LAN infrastructure.

To create a Branch site

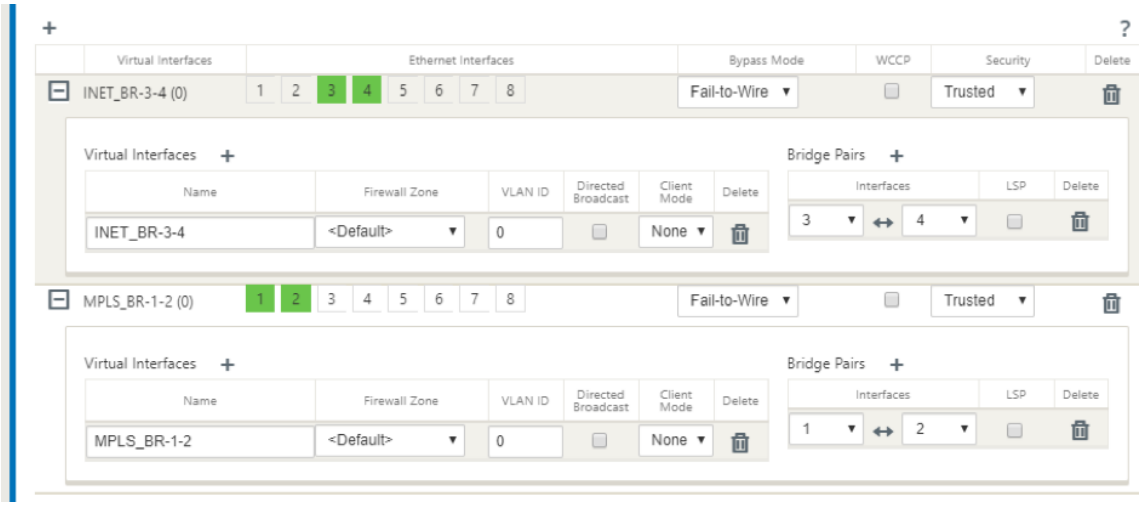
1. Navigate to **Configuration Editor > Sites**, and click **+ Add** button.
2. Keep default settings unless instructed to change.





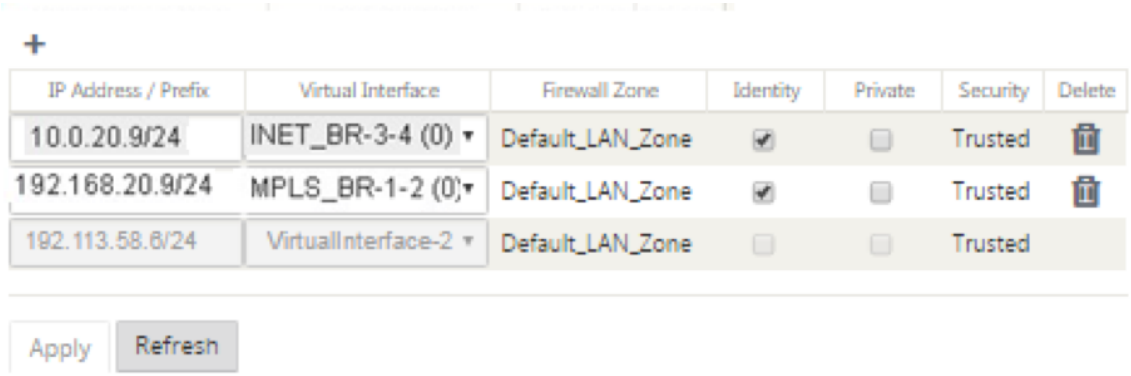
To populate interface groups based on connected Ethernet interfaces

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 topology above and populate the Interface Groups fields as shown below.



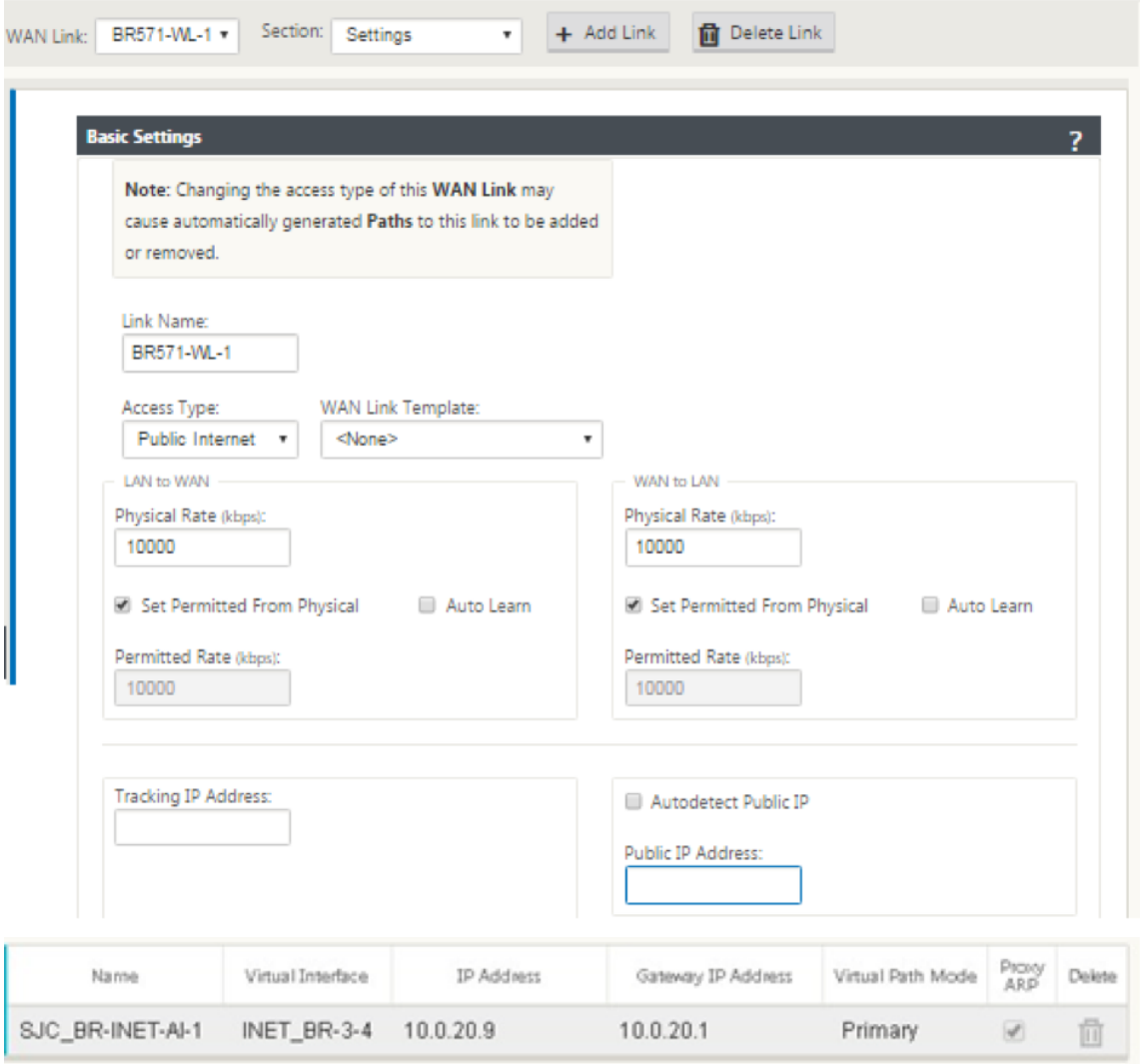
To create Virtual IP (VIP) address for each virtual interface

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.



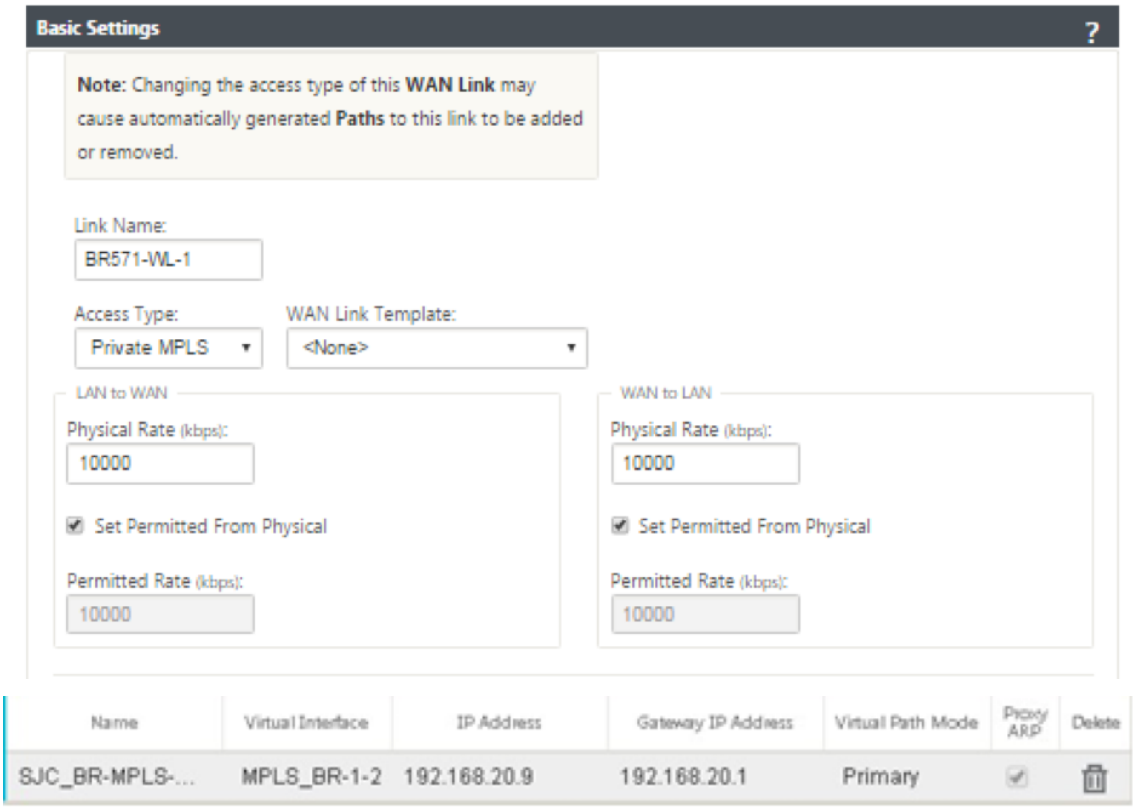
To populate WAN links based on physical rate and not on burst speeds using Internet link

1. Navigate to **WAN Links**, click **+** button to add a WAN Link for the Internet link.
2. Populate Internet link details, including the Auto Detect Public IP address as shown below.
3. Navigate to **Access Interfaces**, click **+** button to add interface details specific for the Internet link.
4. Populate Access Interface for IP address and gateway as shown below.



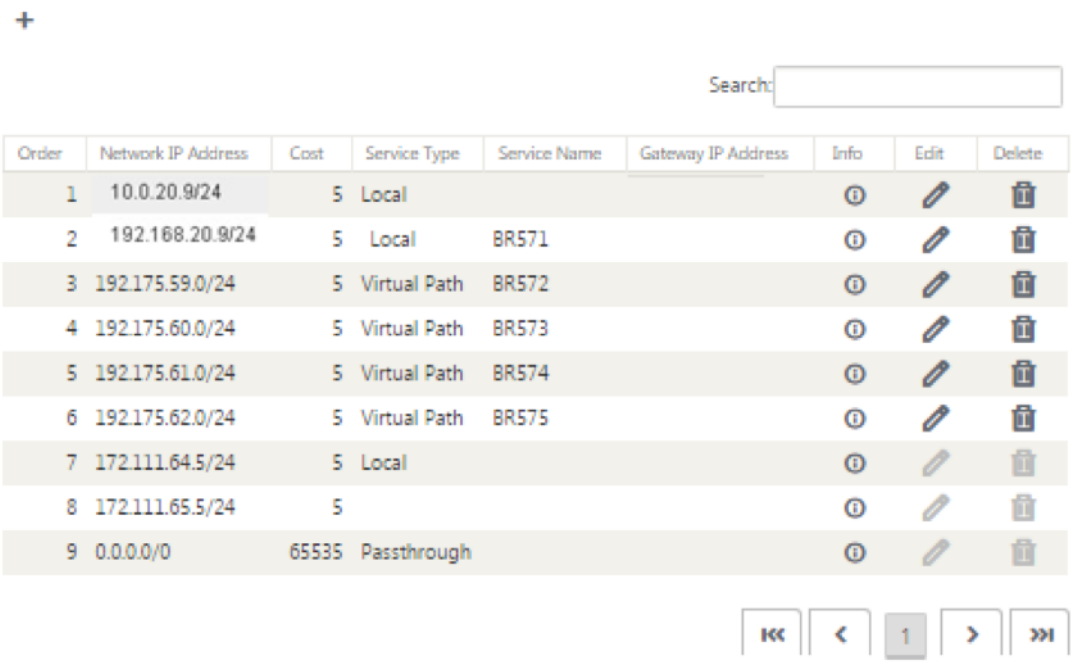
To create MPLS link

1. Navigate to **WAN Links**, click **+** button to add a WAN Link for the MPLS link.
2. Populate MPLS link details as shown below.
3. Navigate to **Access Interfaces**, click **+** button to add interface details specific for the MPLS link.
4. Populate Access Interface for IP address and gateway as shown below.



To populate routes

Routes are auto-created based on above configuration. In case there are more subnets specific to this remote branch office, then specific routes need to be added identifying which gateway to direct traffic to reach those back end subnets.



Virtual inline mode

August 31, 2021

In virtual inline mode, the router uses routing protocol such as PBR, OSPF, or BGP 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 virtual inline mode
- Branch appliance in Inline mode
- Routing protocol must 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) that is, only a single Ethernet interface to be used (Example: Interface 1/5) with bypass mode set to fail-to-block (FTB).
  Citrix SD-WAN appliance must 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.

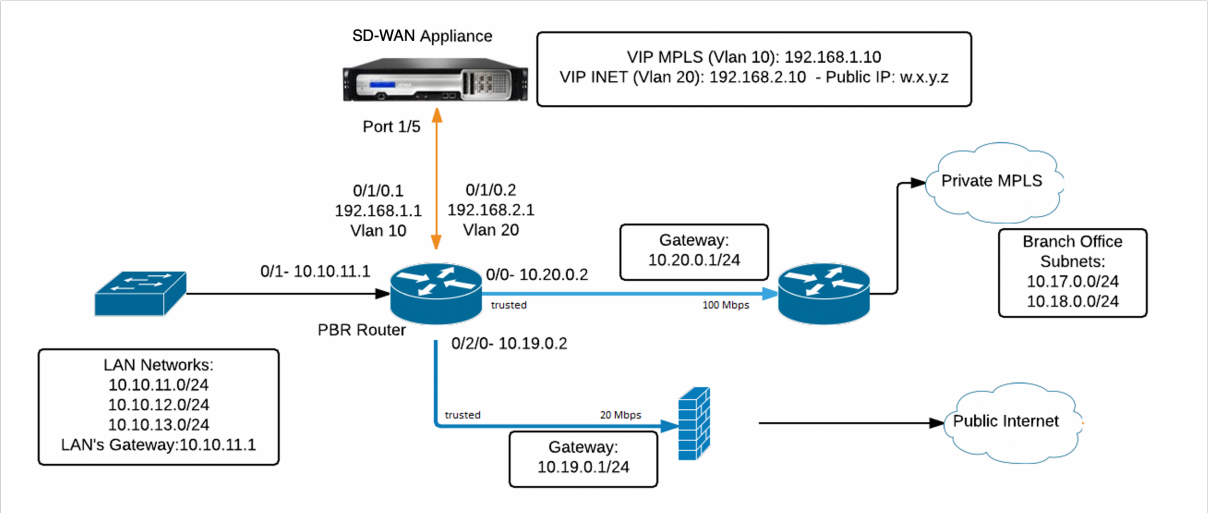
Gather information

Gather the following information required for configuring virtual inline mode:

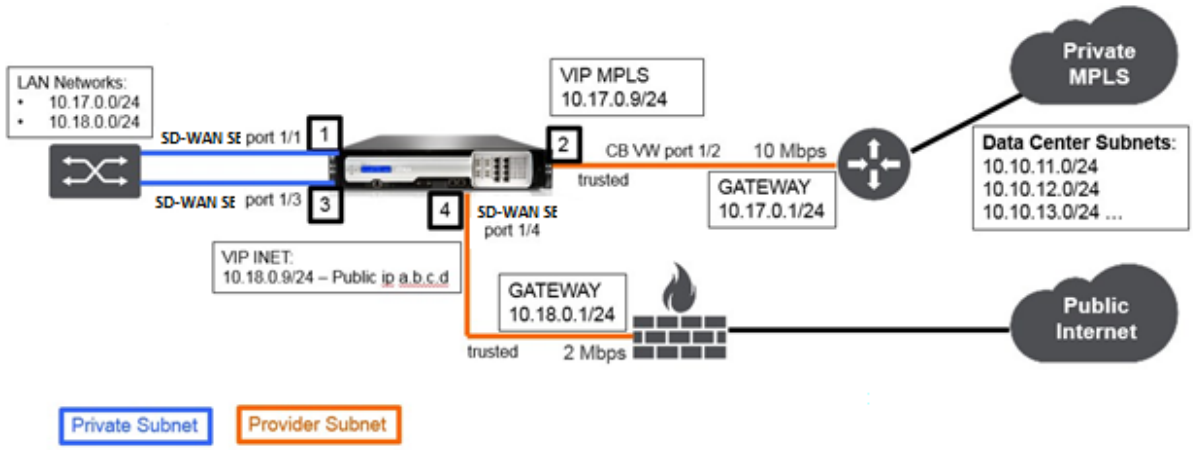
- Accurate network diagram of your local and remote sites including:
  - Local and Remote WAN links and their bandwidths in both directions, their subnets, Virtual IP Addresses and Gateways from each link, Routes, and VLANs.
- Deployment Table

The following is a sample network diagram and deployment table:

Data center topology –Virtual inline mode



Branch topology –inline mode



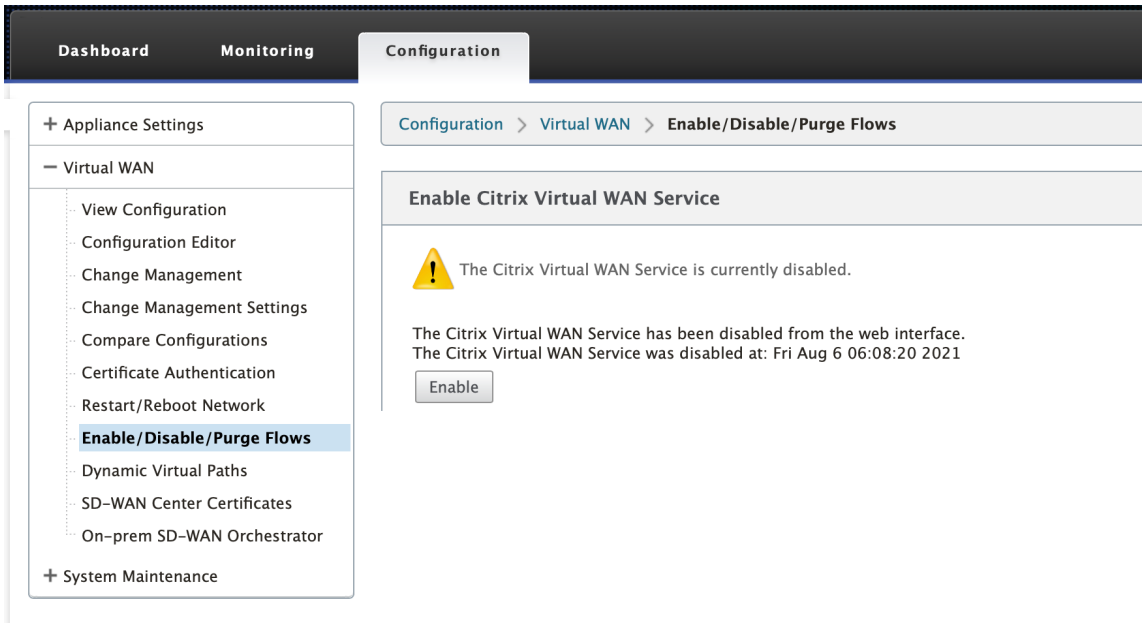
Site Name	Data center Site	Branch Site
Appliance Name	SJC-DC	SJC-BR
Management IP	172.30.2.10/24	172.30.2.20/24
Security Key	If any	If any
Model/Edition	4000	2000
Mode	Virtual Inline Mode	Inline
Topology	2 x WAN Path	2 x WAN Path
VIP Address	192.168.1.10/24 –MPLS, 192.168.2.10/24 –Internet, Public IP 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, and so on) 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: - 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
VLANs	MPLS - VLAN 10, Internet - VLAN 20	None (default 0)

Prerequisites

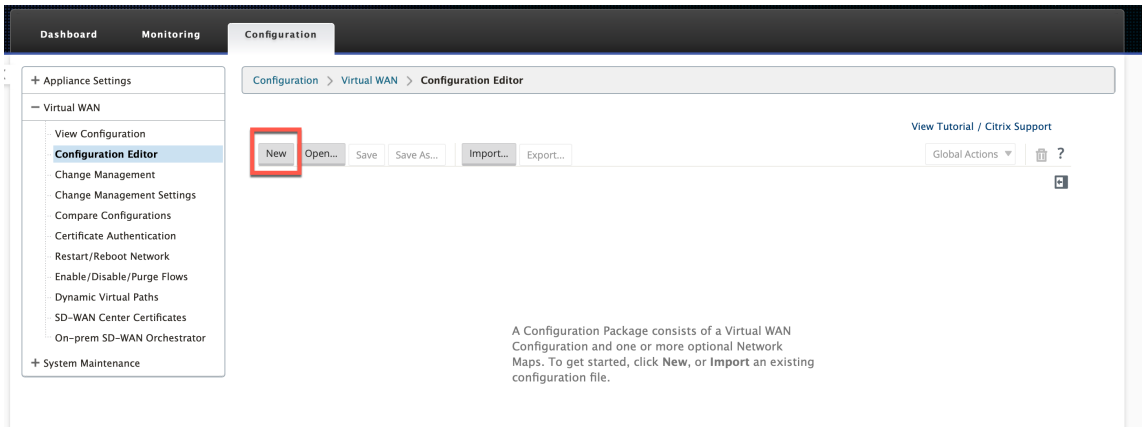
1. In the SD-WAN appliance web management interface, navigate to **Configuration > Appliance Settings > Administrator Interface > Miscellaneous tab** and click **Switch Console**.

   > **Note**
   >
   > If **Switch to Client Console** is displayed, then the appliance is already in MCN mode. You must have only one active MCN in an SD-WAN network.

2. Navigate to **Configuration > Virtual WAN > Enable/Disable/Purge Flows** and click **Enable** in the **Enable Citrix Virtual WAN Service** section.



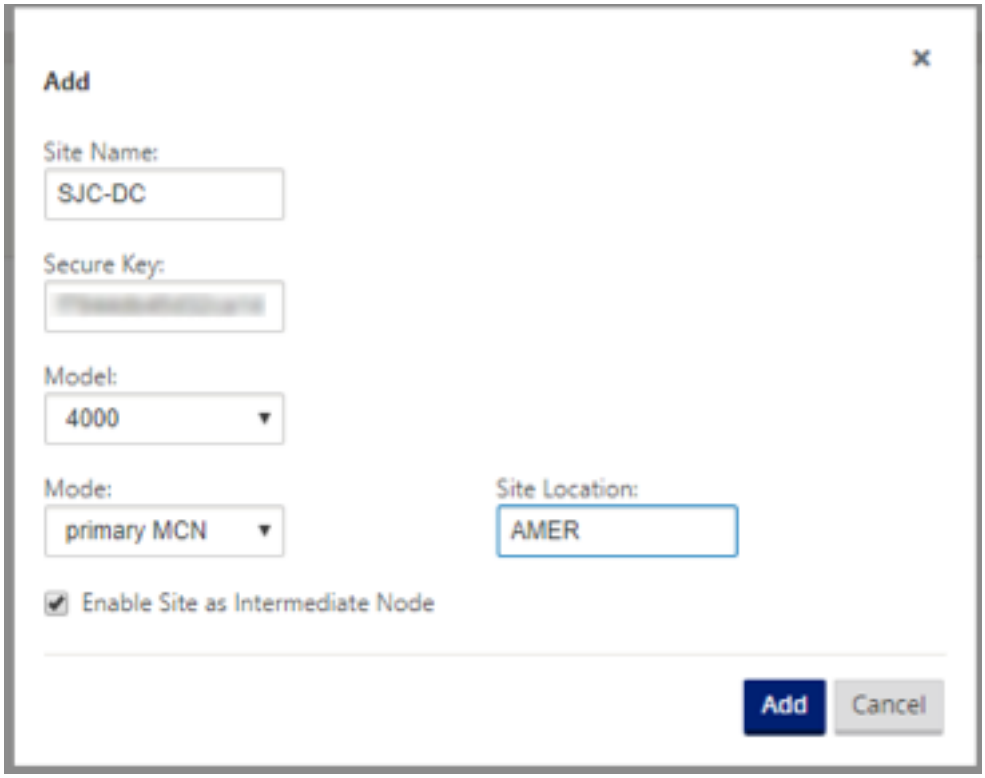
3. Start Configuration by navigating to **Configuration > Virtual WAN > Configuration Editor**. Click **New** to begin the configuration. Clicking **New** creates an initial configuration file having **Untitled_1** as the file name. You can rename [optional] the file later using the **Save As** button.



Data center site - virtual inline mode configuration

Create a data center site

1. Navigate to **Configuration > Virtual WAN > Configuration Editor > Sites** and click **+ Site**.
2. Enter the site name and location. Choose the appliance model from the **Model** drop-down list and **Primary MCN** from the **Mode** drop-down list.
3. Click **Add**.



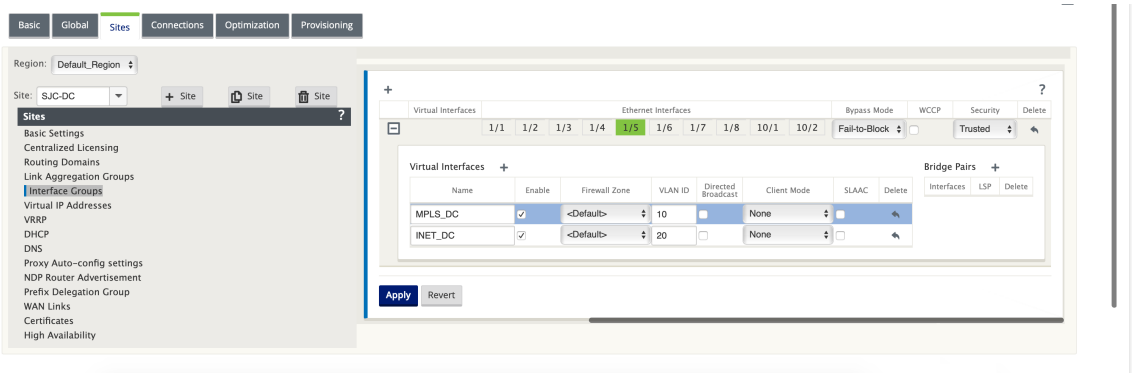
Configure interface groups based on connected Ethernet interfaces

In virtual inline mode configuration, only one Ethernet interface is used, that is, the interface connecting the upstream router providing routing policy implications (Example-Interface 1/5). Bypass mode is set to Fail-to-Block (FTB) since only one Ethernet/physical interface is used per virtual interface. Also, there are no Bridge Pairs.

1. In the **Configuration Editor**, navigate to **Sites > [Site Name] > Interface Groups**. Click **+** to add interfaces intended to be used.
2. Select the Ethernet interface that gets connected to the upstream router and click **+** next to Virtual Interfaces. Add the Virtual Interfaces for both MPLS and INTERNET links. As per the sample topology, add the following:

- Virtual Interface **MPLS** configured on **VLAN 10**
- Virtual Interface **INTERNET** configured on **VLAN 20**

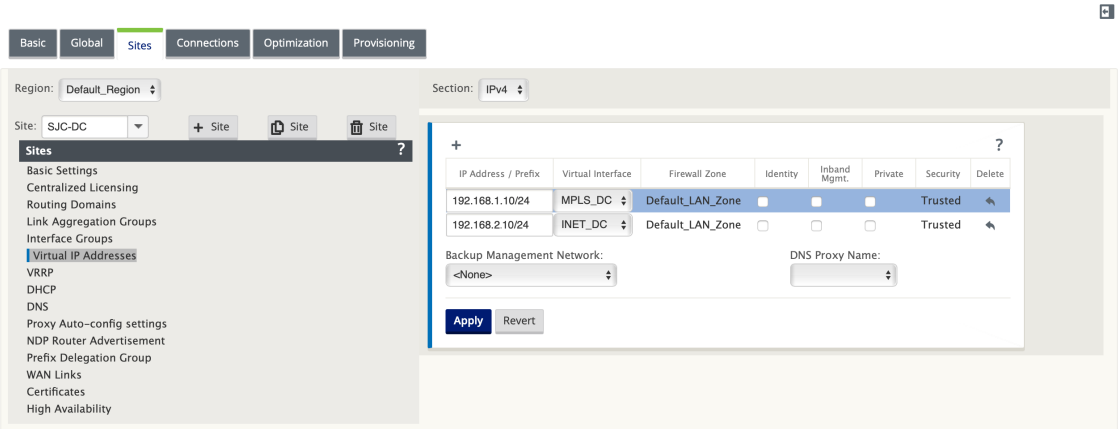
3. Select **Fail-to-Block** from the **Bypass Mode** drop-down list. Click **Apply**.



Create Virtual IP address for each virtual interface

Create a Virtual IP (VIP) Address on the appropriate subnet for each WAN Link. VIPs are used for communication between two SD-WAN appliances in the Virtual WAN environment.

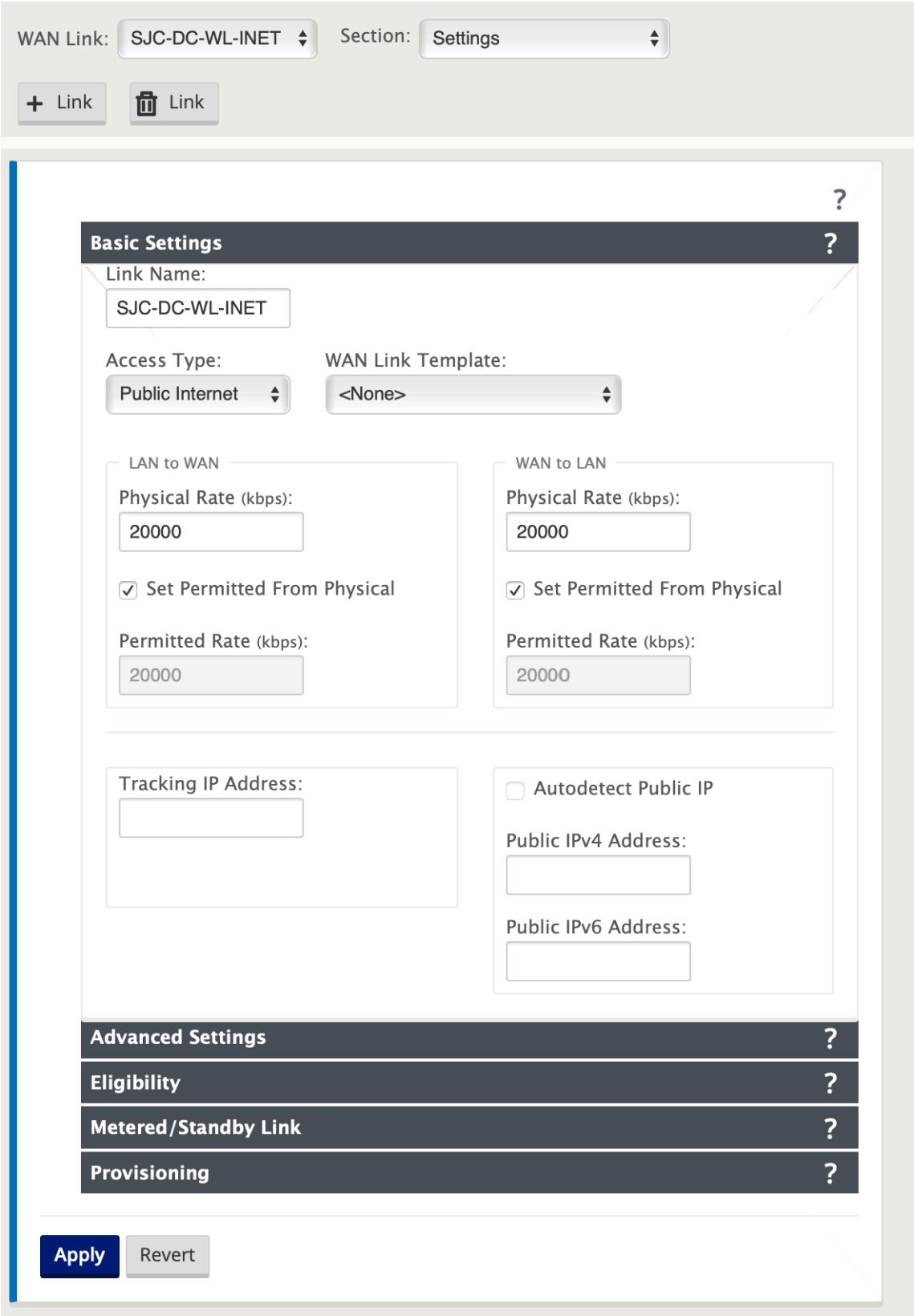
1. In the **Configuration Editor**, navigate to **Sites > [Site Name] > Virtual IP Addresses**. Click **+** to create VIPs.
2. Enter the IP address/prefix and select the corresponding virtual interface for MPLS and Internet.
3. Click **Apply**.



Create Internet WAN link

Create Internet WAN link based on physical rate and not on burst speeds.

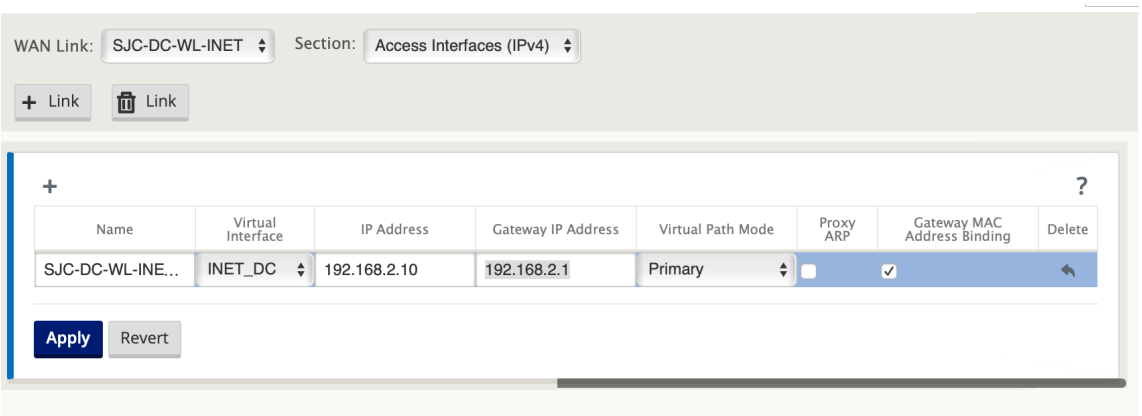
1. In the **Configuration Editor**, navigate to **Sites > [Site Name] > WAN Links** and click **+ Link**. Enter a name and select **Access Type** as **Public Internet**. Click **Add**.
2. Enter the physical rate. Do not select the **Auto Detect Public IP** check box. For the SD-WAN appliance that is configured as MCN, the **Auto Detect Public IP** check box cannot be selected.



3. Select **Access Interfaces** from the **Section** drop-down list and click the **+** button to add interface

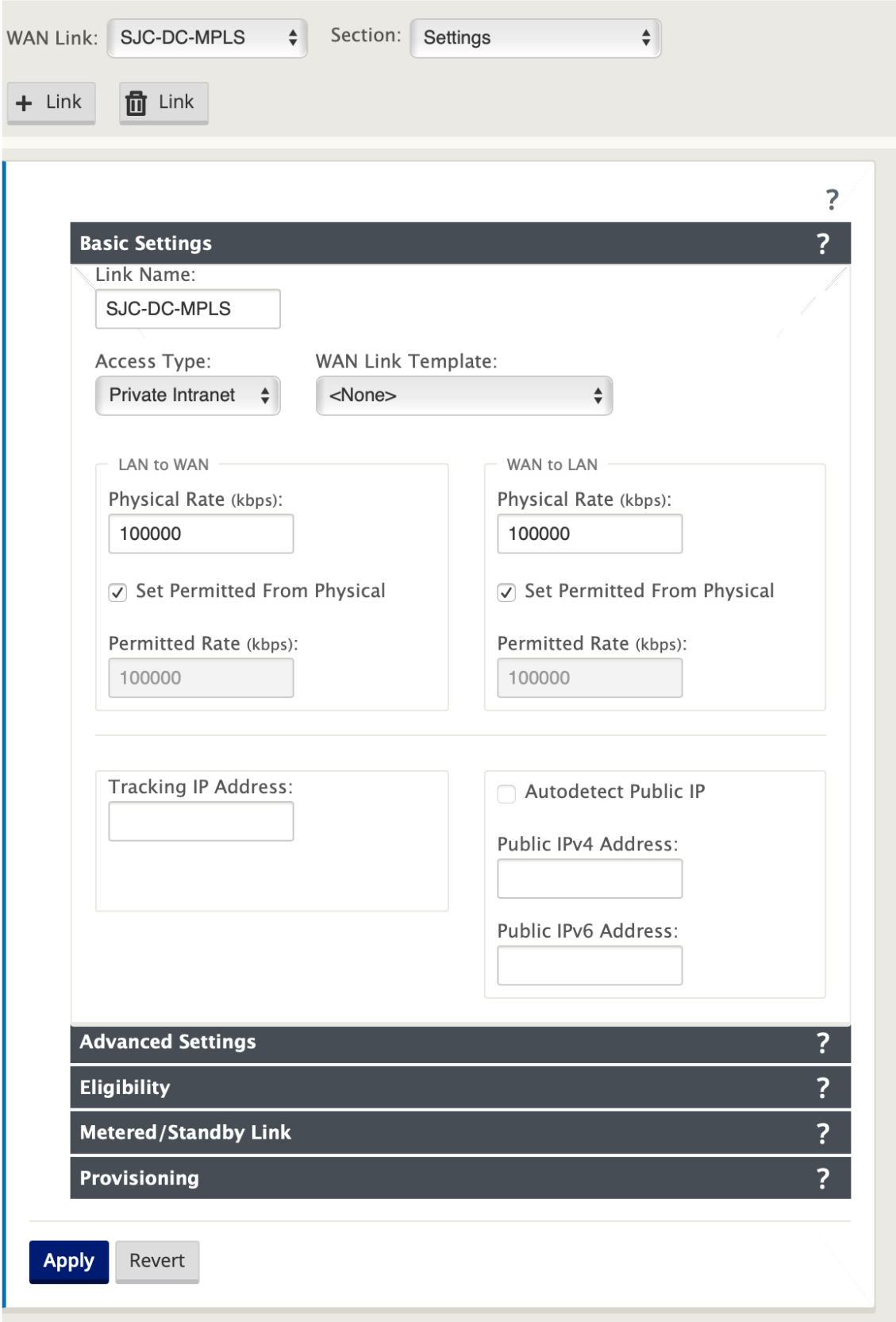
details specific for the Internet link.

4. Enter the Internet WAN virtual IP address and gateway address. The Proxy ARP is not checked for less than two Ethernet interfaces.
5. Click **Apply**.

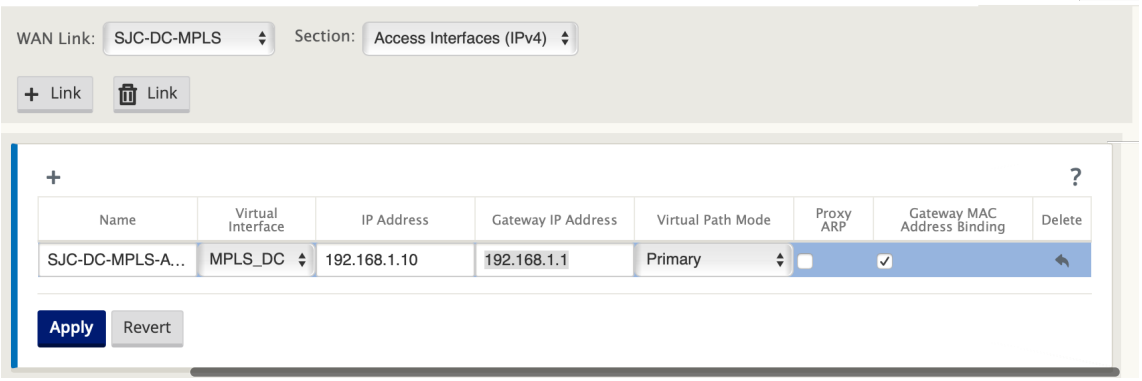


Create MPLS link

1. In the **Sites > [Site Name] > WAN Links** page, select **Settings** from the **Section** drop-down list. Click the **+ Link** button to add a WAN Link for MPLS.
2. Enter the MPLS WAN Link name and select **Access Type** as **Private Intranet**. Click **Add**.
3. Enter the physical rate and other details. Click **Apply**.



4. Select **Access Interfaces** from the **Section** drop-down list and click the **+** button to add interface details specific to the MPLS link.
5. Enter the MPLS Virtual IP address and Gateway address. The Proxy ARP is not checked for less than two Ethernet interfaces.
6. Click **Apply**.



Populate routes

On the data center side, add a route on the SD-WAN appliance on how to reach the LAN Subnets (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, and so on) through any of the physical interfaces.

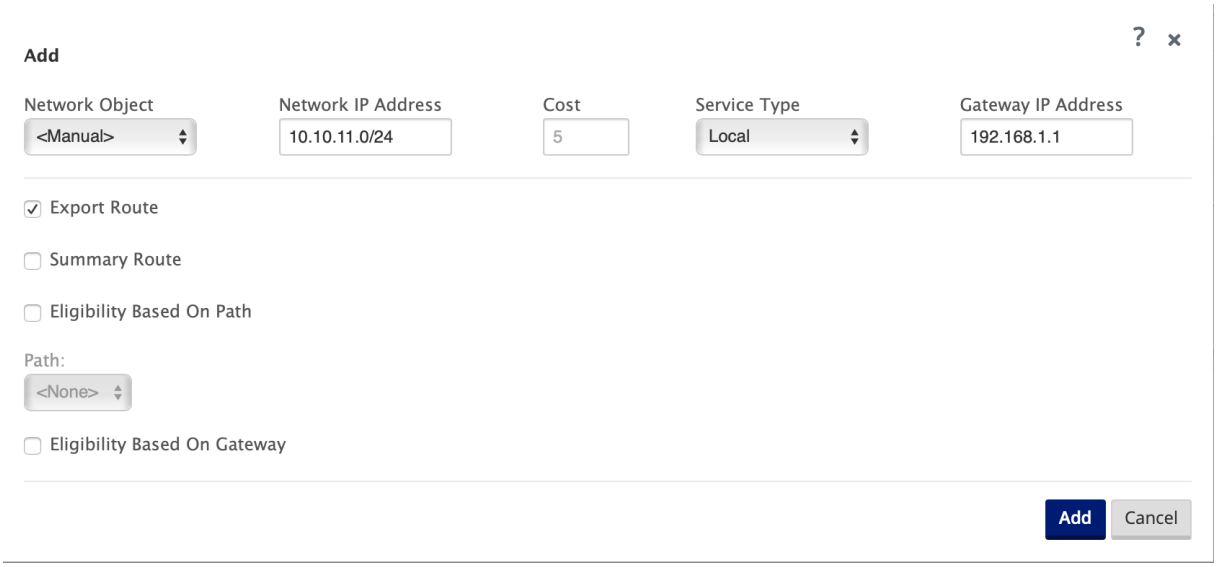
0/1/0.1 –192.168.1.1 on VLAN 10

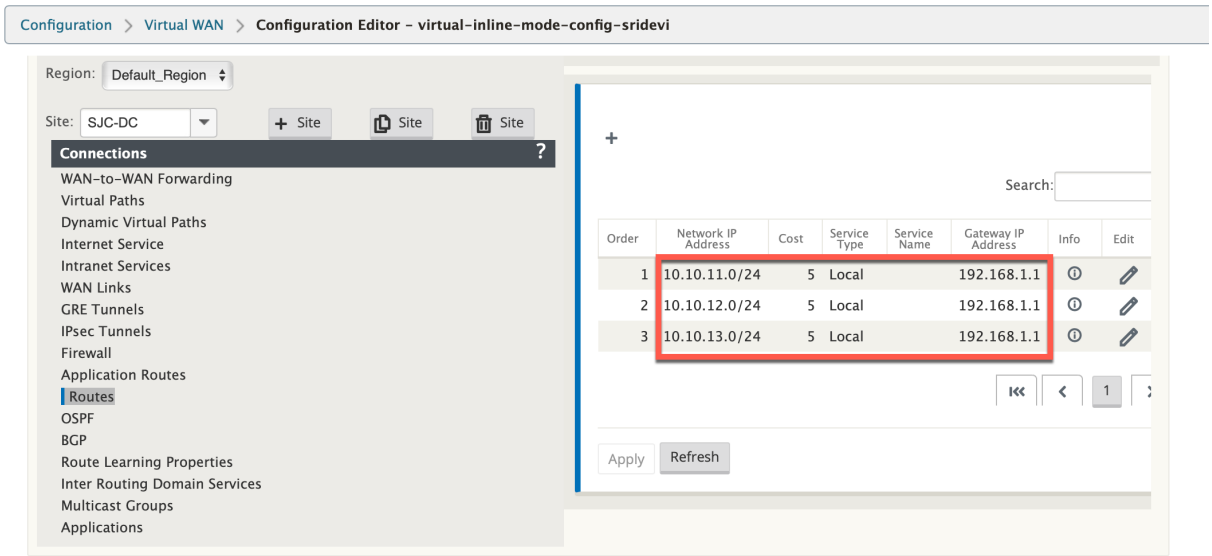
0/1/0.2 –192.168.2.1 on VLAN 20

In this example, the interface 192.168.1.1 is used.

In the **Configuration Editor**, navigate to **Connections > Routes** and click **+** to add the routes.

Enter the **Network IP address**, **Cost**, and **Gateway address**. Click **Add**.

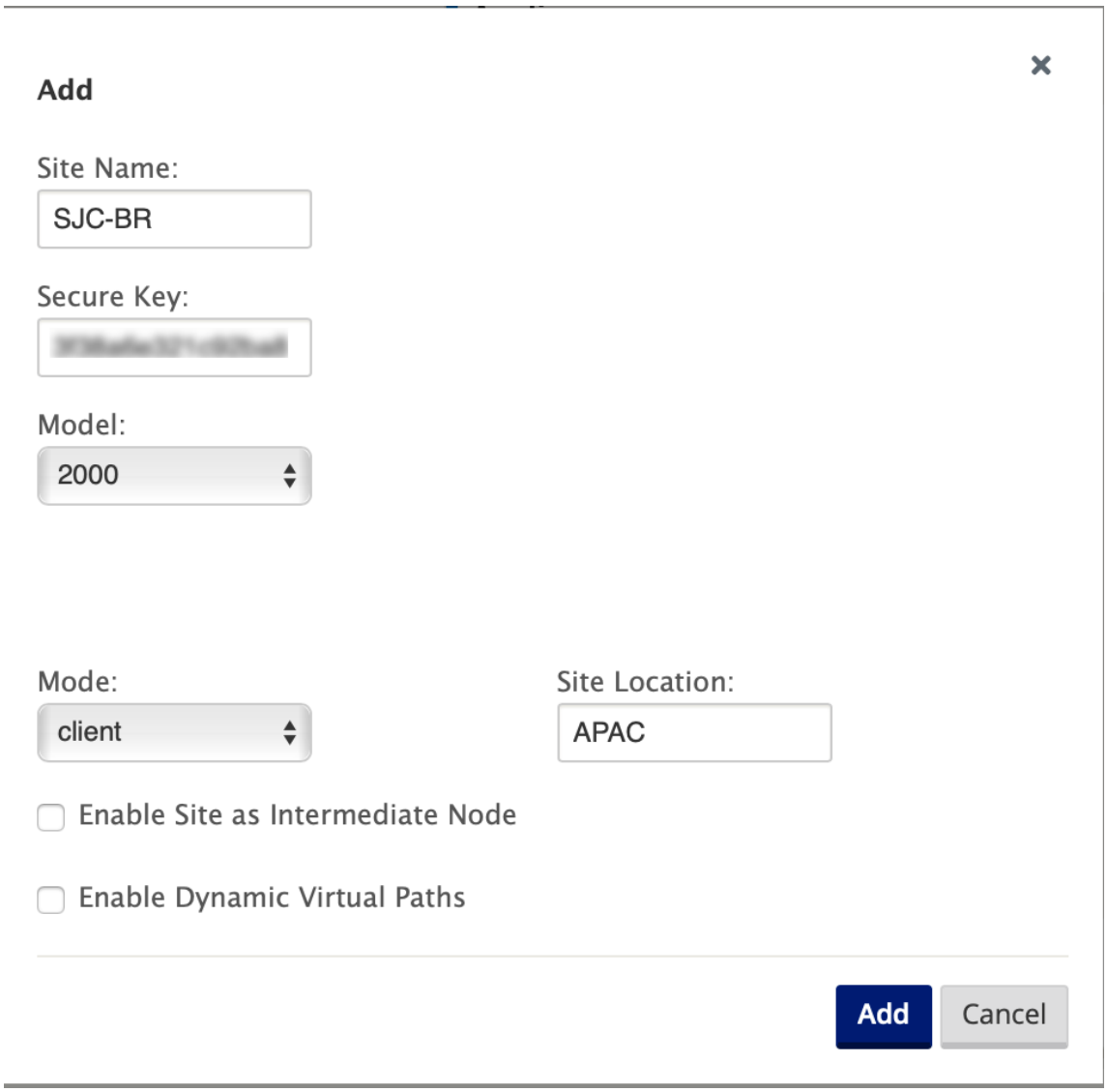




Branch site inline deployment configuration

Create a branch site

1. Navigate to **Configuration Editor > Sites** and click **+ Site**.
2. Enter the site name and location. Choose the appliance model from the **Model** drop-down list and **Client** from the **Mode** drop-down list.
3. Click **Add**.

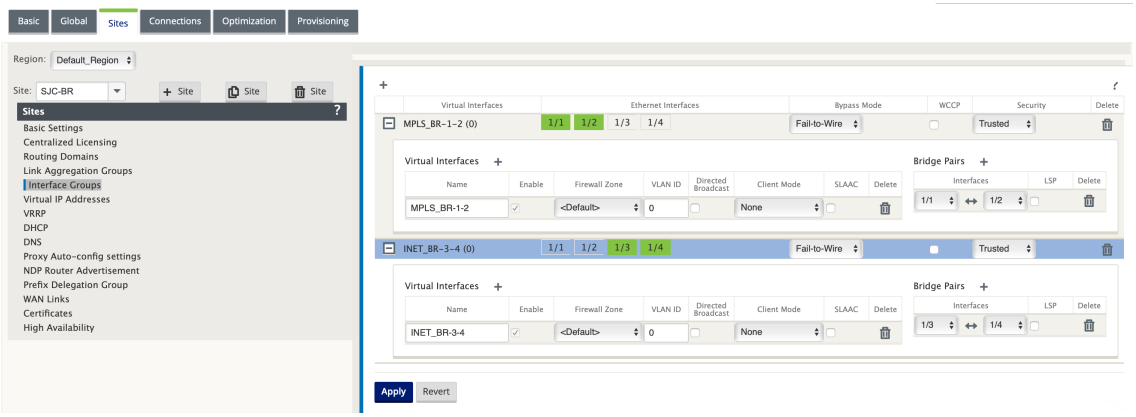


Configure interface groups based on connected Ethernet interfaces

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 interfaces are used; interface pair 1/3, 1/4 and interface pair 1/1 and 1/2.
2. Set the **Bypass mode** to fail-to-wire since two Ethernet/physical interfaces are used per virtual interface. There are two bridge Pairs.
3. Click **+** next to **Virtual Interfaces** and 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 on Bridge Pair 1/1 and 1/2.

4. Click **+** next to **Bridge Pairs** and create the bridge pair by selecting the appropriate interfaces.

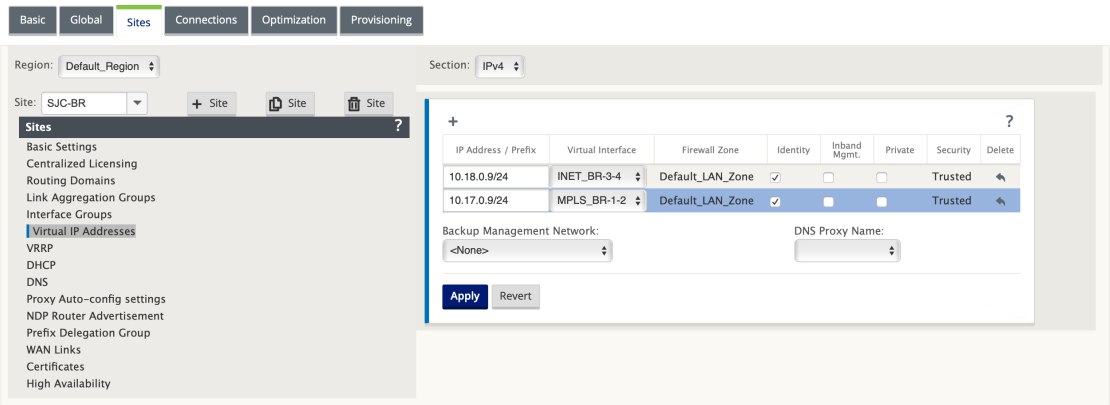
   Refer to the **Branch topology –inline mode** topology diagram under the Prerequisites section and populate the Interface Groups.



Create Virtual IP (VIP) address for each virtual interface

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.

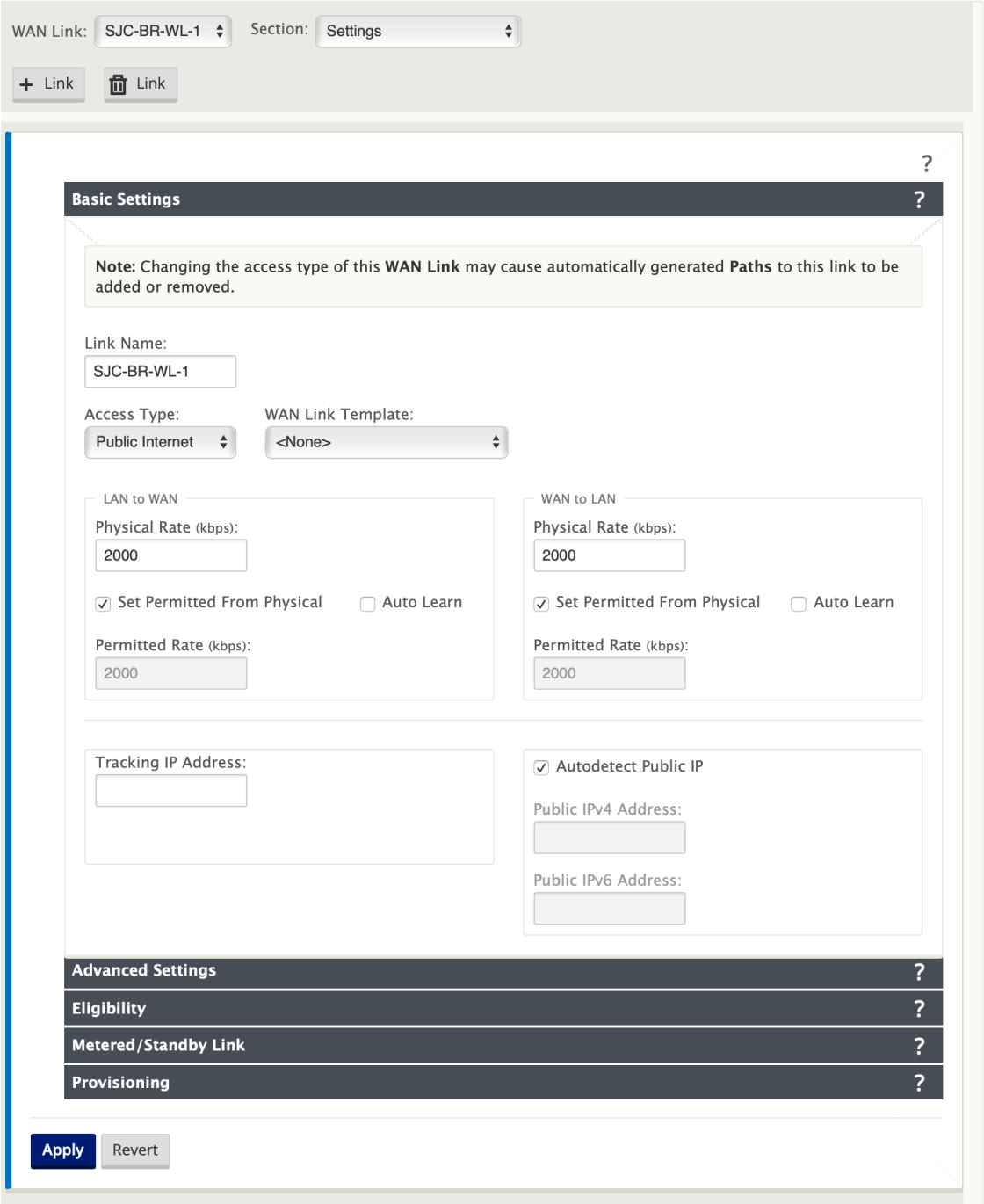
1. In the **Configuration Editor**, navigate to **Sites > [Site Name] > Virtual IP Addresses**. Click **+** to create VIPs.
2. Enter the IP address/prefix and select the corresponding virtual interface for MPLS and Internet.
3. Click **Apply**.

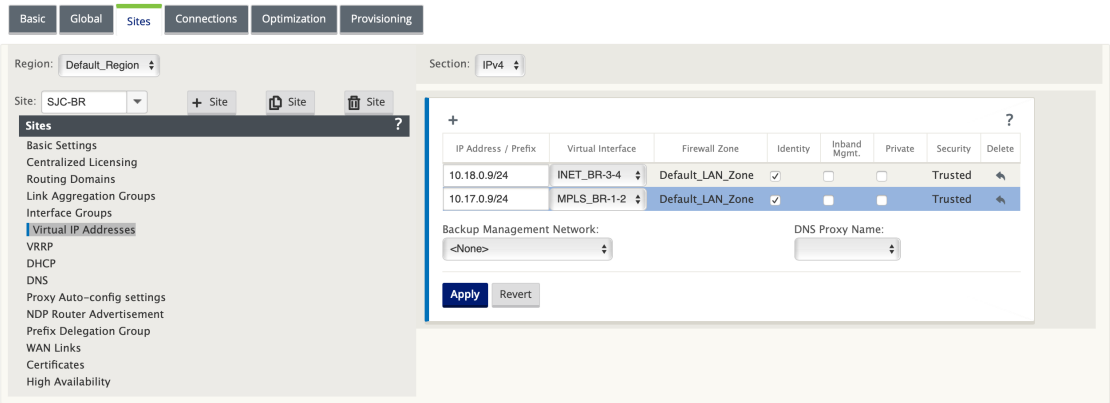


Create Internet WAN link

To populate WAN links based on physical rate and not on burst speeds using Internet link

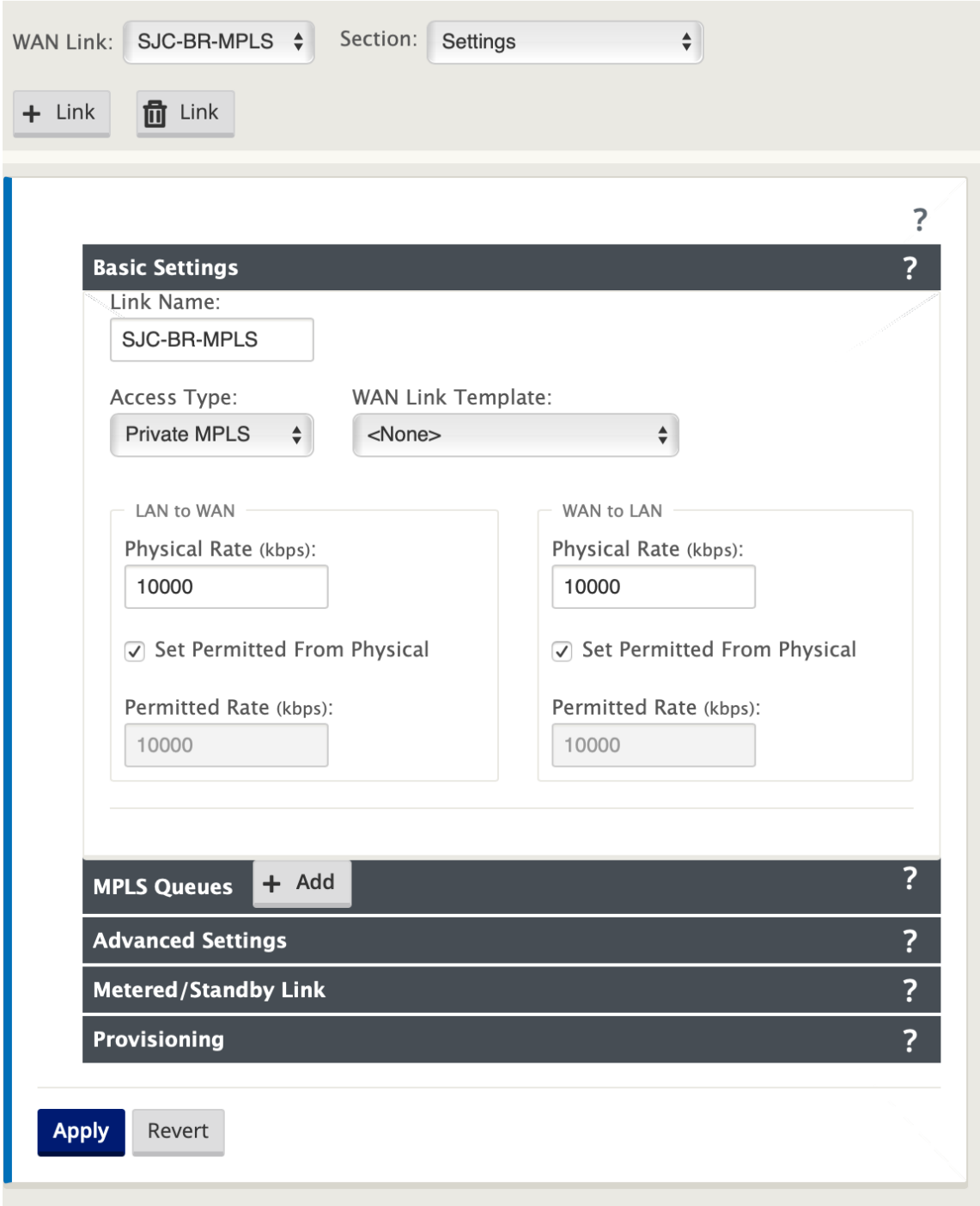
1. Navigate to **WAN Links**, click the **+ Link** button to add a WAN Link for the Internet link. Enter a name and select **Access Type** as **Public Internet**. Click **Add**.
2. Populate Internet link details and select the **Autodetect Public IP address** check box.
3. Select **Access Interfaces** from the **Section** drop-down list and click the **+** to add interface details specific for the Internet link.
4. Enter the Internet WAN virtual IP address and gateway address. The Proxy ARP is not checked for less than two Ethernet interfaces.



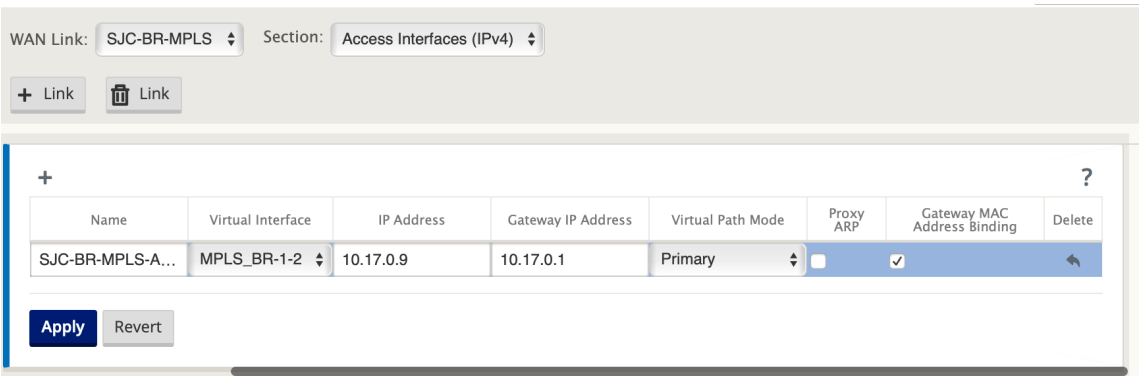


Create MPLS WAN link

1. Navigate to **WAN Links** and select **Settings** from the **Section** drop-down list. Click the **+ Link** button to add a WAN Link for the MPLS link.
2. Enter the MPLS WAN Link name and other details. Select **Access Type** as **Private Intranet**.



3. Select **Access Interfaces** from the **Section** drop-down list and click the **+** button to add interface details specific for the MPLS link.
4. Enter the MPLS Virtual IP address and Gateway address. The Proxy ARP is not checked for less than two Ethernet interfaces.

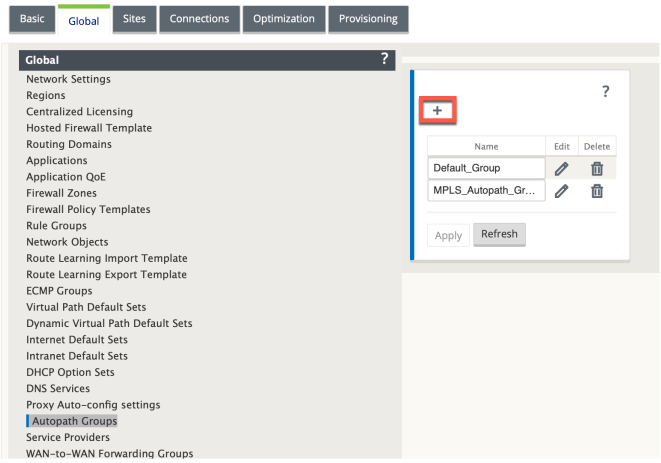


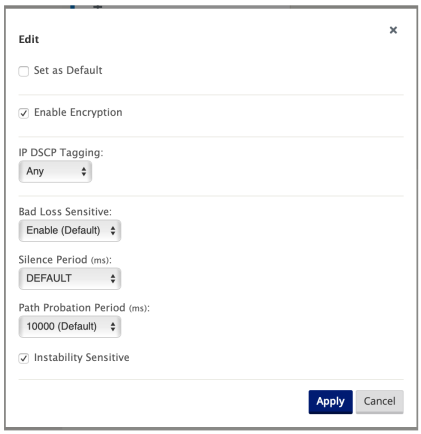
Populate routes

Routes are auto-created based on preceding configuration. If there are more subnets specific to this remote branch office, then specific routes need to be added identifying which gateway to direct traffic to reach those back-end subnets.

Create Autopath groups

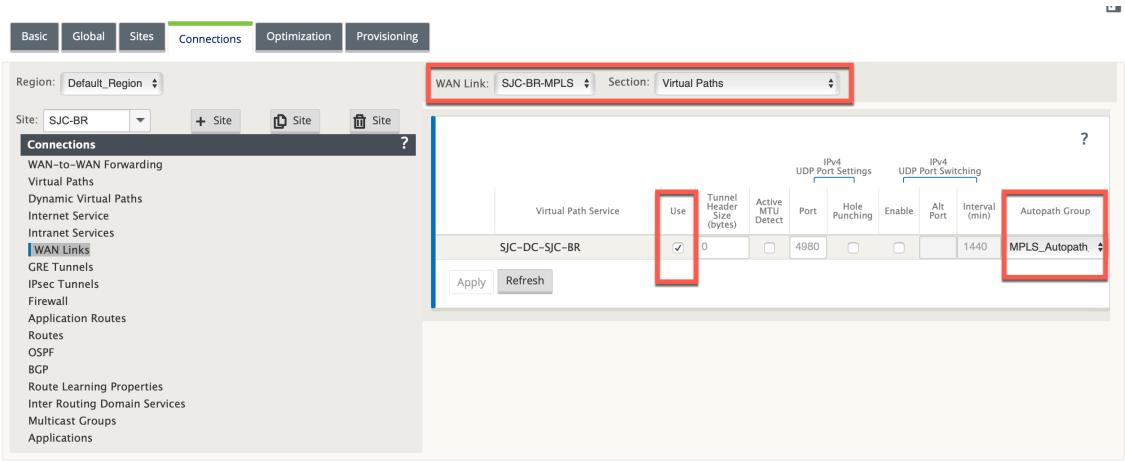
1. In the **Configuration Editor**, navigate to the **Global > Autopath Groups**. Click **+**.
2. Enter a name and click **Apply**.
3. Configure the Autopath Group as per your requirement and click **Apply**.





4. Navigate to **Connections > WAN links**. Select the Internet WAN link from the **WAN Links** drop-down list and **Virtual Paths** from the **Section** drop-down list.
5. Select the **Use** check box and choose the newly created autopath group from the **Autopath Group** check box for the Intranet WAN links at the respective sites (both Data Center and Branch).

No two Autopath Groups can be marked as default. If marked would lead to an audit error.



After manually adding the virtual paths for WAN links with access type as **Private Intranet**, virtual paths get populated under **Paths**.

After completing all the preceding steps, proceed to Preparing the SD-WAN Appliance Packages.

Resolving audit errors

After completing the configuration for Data Center and Branch sites, you will be alerted to resolve the audit errors on both DC and BR sites. Resolve the audit errors (if any).

Build an SD-WAN network

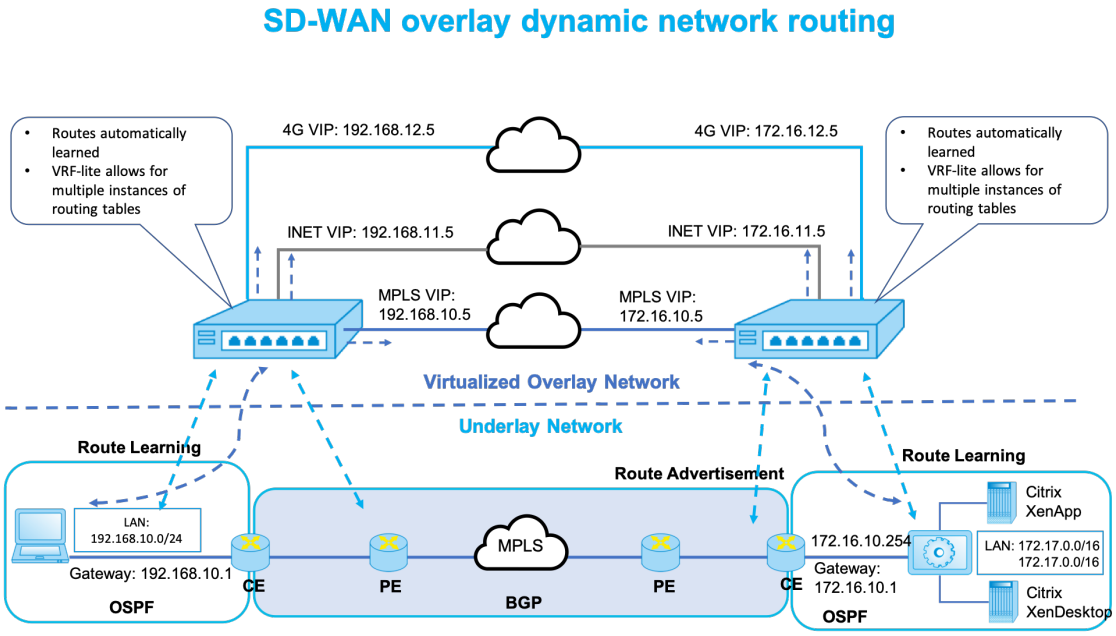
March 12, 2021

To build an SD-WAN overlay network without the need to 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.

SD-WAN routing components and network topology

- 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 Premium (Enterprise) edition

March 12, 2021

The SD-WAN Premium (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 Premium Edition appliances to utilize WAN optimization services.

Citrix SD-WAN Product Platform Editions include the following appliances:

- SD-WAN: SD-WAN Standard Edition appliance

- Premium (Enterprise): SD-WAN Premium Edition appliance
- WANOP: SD-WAN WANOP Edition appliance

To integrate Premium (Enterprise) Edition appliances into an existing distributed WANOP network, you can 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 should 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. The 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 Premium Edition appliance at the Branch site.

Network Topology

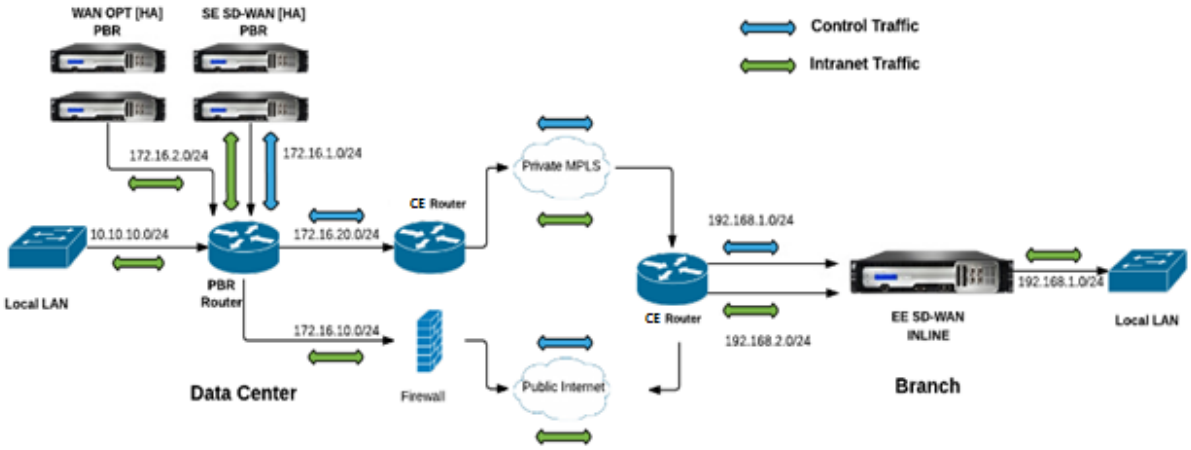
SD-WAN Standard edition and WANOP appliances in PBR deployment:

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 is redirected to the SD-WAN appliance by the PBR Router. The data traffic is 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 is followed in the reverse direction.



SD-WAN Standard Edition in PBR mode and WANOP in Inline Deployment:

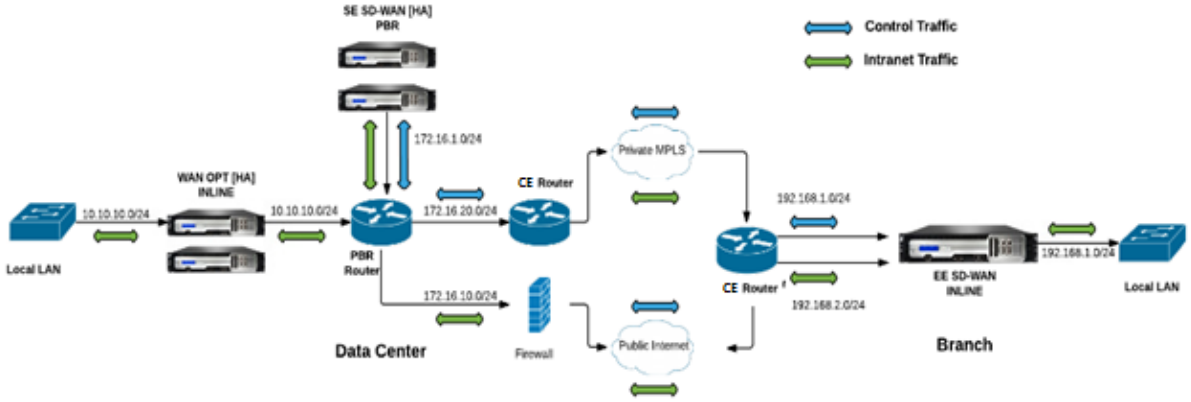
In the below illustration, the SD-WAN appliance at the DC site is deployed in one-arm mode while the WANOP appliance is deployed in inline mode.

The control traffic (Virtual Path traffic) received from WAN at the DC site is redirected to the SD-WAN appliance by the PBR Router. The data traffic is 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 is followed in the reverse direction.



Configuration Steps

1. Configure the SD-WAN Appliance at DC [MCN] to establish Virtual Paths between DC and Branch sites.

See, configuring virtual path service between MCN and clients.

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 one or more WAN Links 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 substeps 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 should be configured to redirect traffic as per the deployment steps provided.

   For more information about configuring WAN Optimization, refer to: Enabling-configuring-wan-optimization.

Two box mode

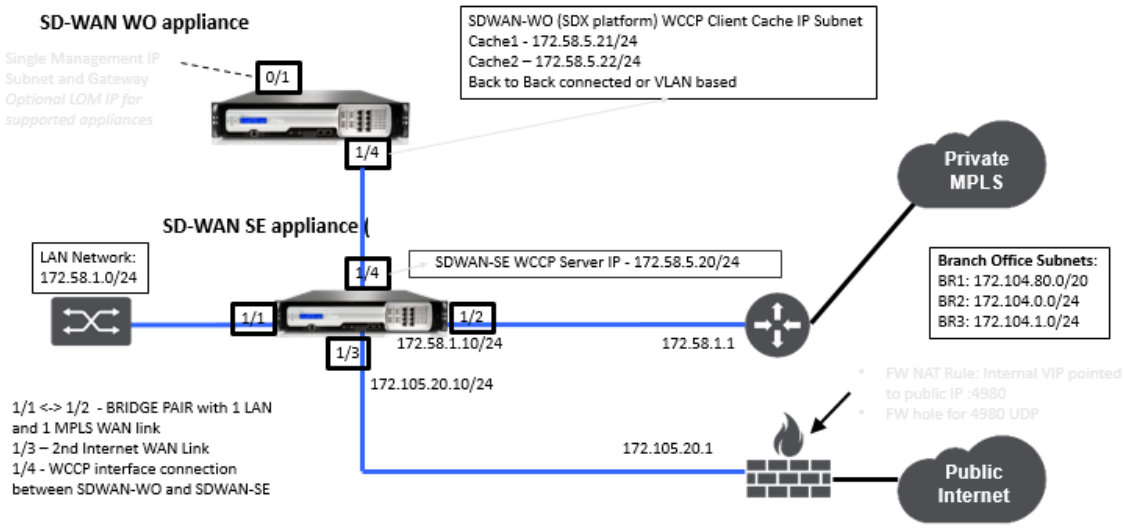
March 12, 2021

Two box mode is a WCCP one-arm based deployment where the SD-WAN SE appliance acts as a WCCP router and the SDWAN-WANOP (4000/5000) appliances act as WCCP clients and help establish WCCP convergence. This way all the virtual path/Intranet service oriented TCP packets reaching the SD-WAN

SE appliance get redirected to the SDWAN-WANOP appliance for optimization benefits by providing both SD-WAN SE and WANOP benefits for the customer traffic.

Two Box mode is supported only on the following appliance models:

- SD-WAN SE appliances –4000, 4100, and 5100
- SD-WAN WANOP appliances –4000, 4100, 5000, and 5100



Note

High Availability and WCCP deployment modes are not accessible when Two Box mode is enabled. However, these deployment modes are available for the user to administer.

Important

- Although the legacy WCCP deployment is disabled when Two Box Mode is enabled, the Service Group convergence can only be verified from the WCCP monitoring page. There is no separate GUI page under the monitoring section for the Two Box Mode.
- If WCCP process running on the Standard Edition appliance reboots multiple times within a short interval of time, for example, 3 times in a minute then Service Group shuts down automatically. In such scenario, to get the WCCP convergence on the WANOP appliance, re-enable the WCCP feature in the WANOP appliance web GUI.
- When there is a change in the WCCP configuration or WAN optimization related to configuration on the Standard Edition appliance, the external WANOP appliance reboots. For example, enabling/disabling the WCCP checkbox in the Interface Group of config editor followed by Change Management process, restarts the WANOP appliance as well.

Note

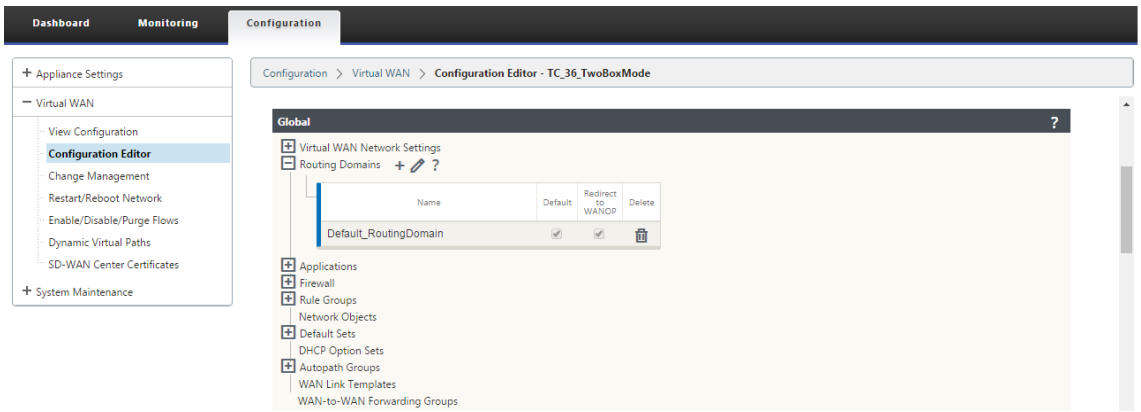
Also, note the following points to consider when implementing the two box mode:

> - 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.

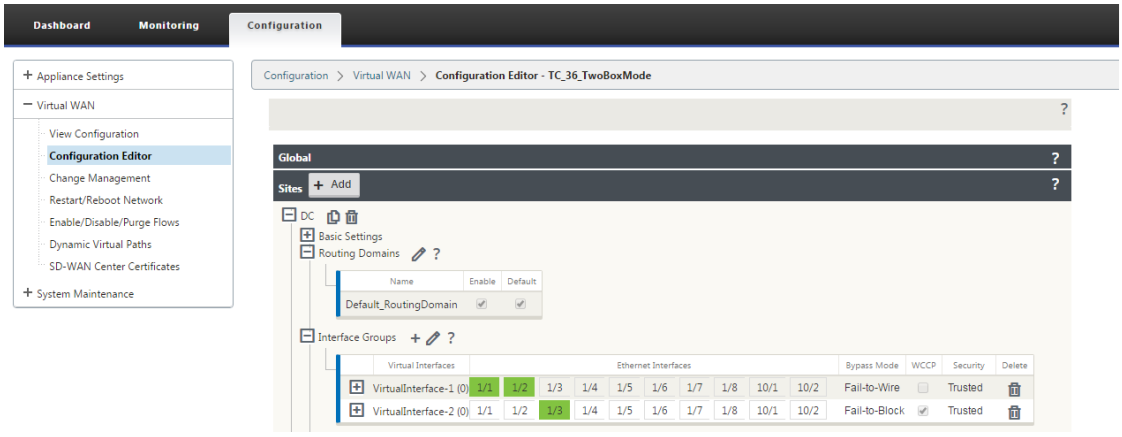
Citrix SD-WAN standard edition

To configure two-box mode solution in the Standard Edition appliance at the DC or Branch site:

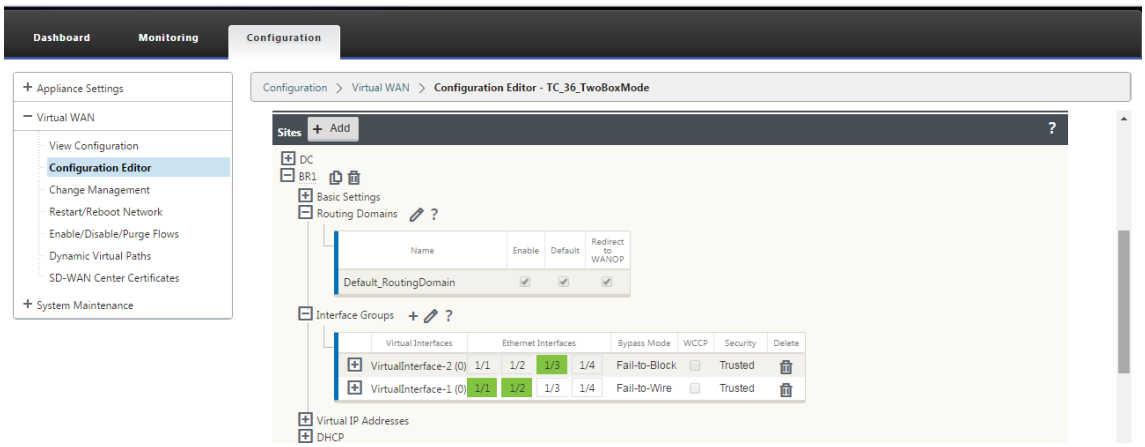
1. In the SD-WAN SE web management interface, go to **Configuration** > **Virtual WAN** > **Configuration Editor**. Open an existing configuration package or create a package.
2. In the chosen configuration package, go to the **Advanced** tab to view the configuration details.
3. Open **Global** settings and expand **Routing Domains** to view that the **Redirect to WANOP** checkbox is enabled.



4. Expand DC to enable **WCCP** for the **Virtual Interface** under **Interface Group** settings that signify which virtual network interface the appliance is 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.

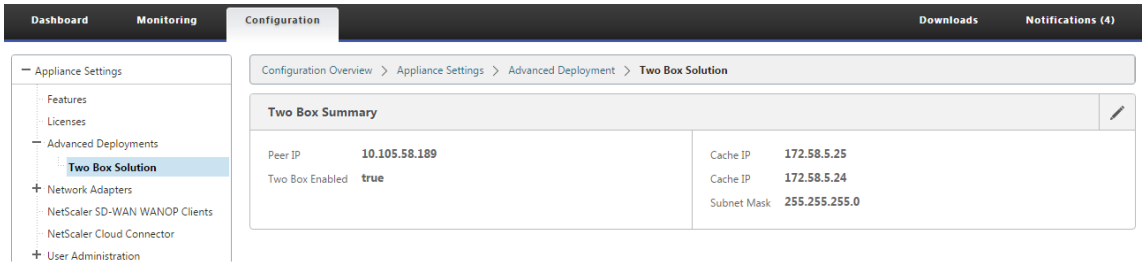


> **Note**
>
> The WCCP listener should be enabled only for those virtual network interfaces which have only ONE Ethernet Interface configured. Do not enable the WCCP Listener on a BRIDGED Pair. It is intended to be enabled on the ONE-ARM interface between the SD-WAN SE and SD-WAN WANOP appliances.

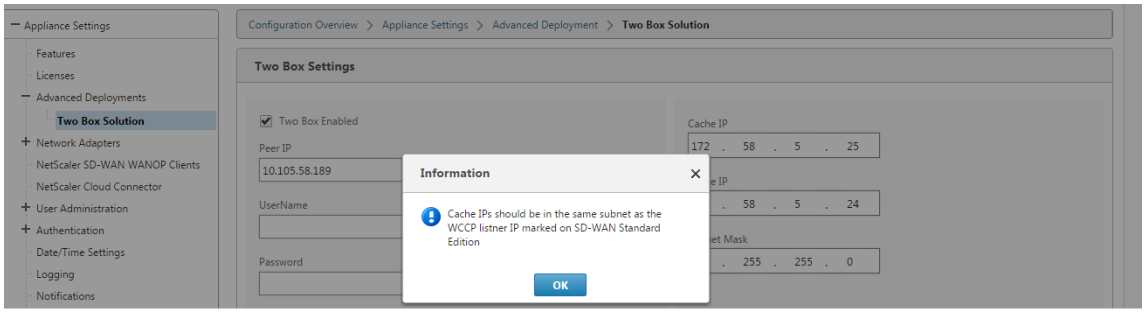
Citrix SD-WAN WANOP configuration

To configure two-box deployment mode in the SD-WAN WANOP appliance web GUI:

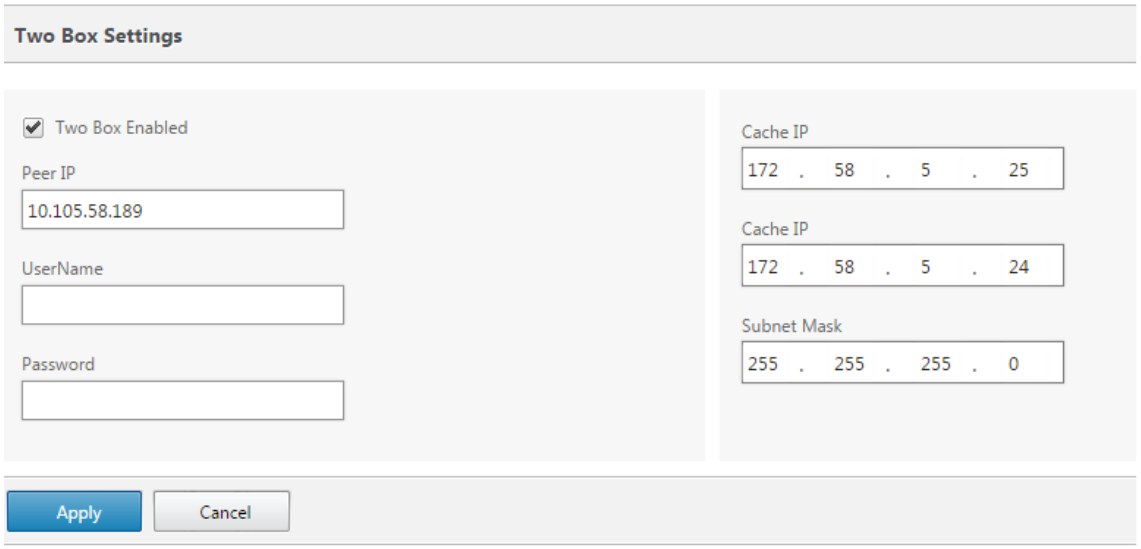
1. In the SD-WAN WANOP web management interface, go to **Configuration** > **Appliance Settings** > **Advanced Deployments** > **Two Box Solution**.



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 SD-WAN Standard Edition appliance IP address.
5. Enter the user credentials and click **Apply**.



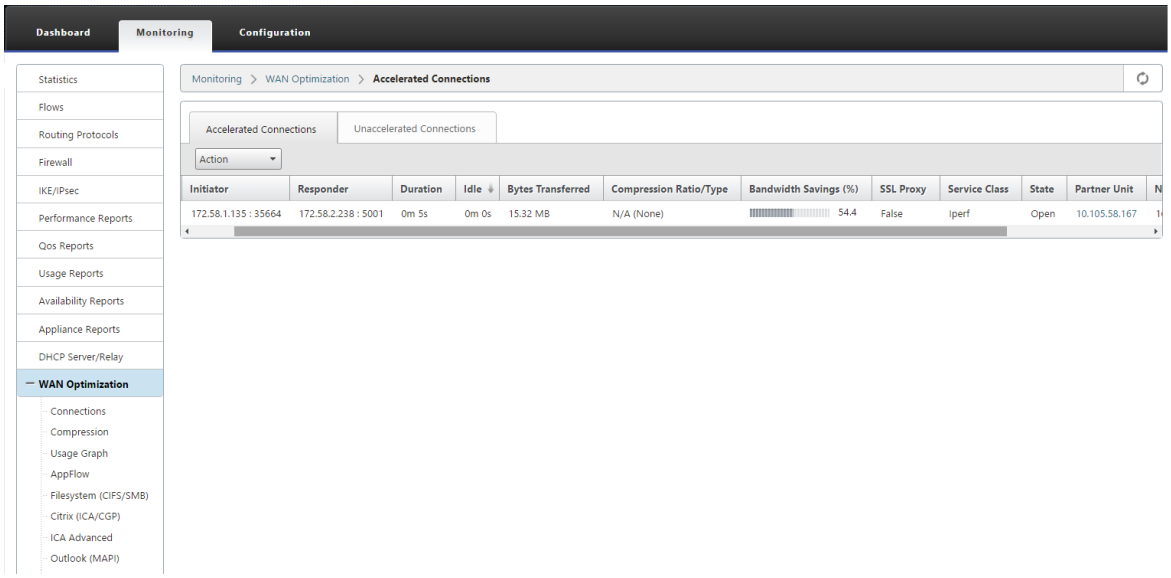
Two box mode configuration and manageability

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

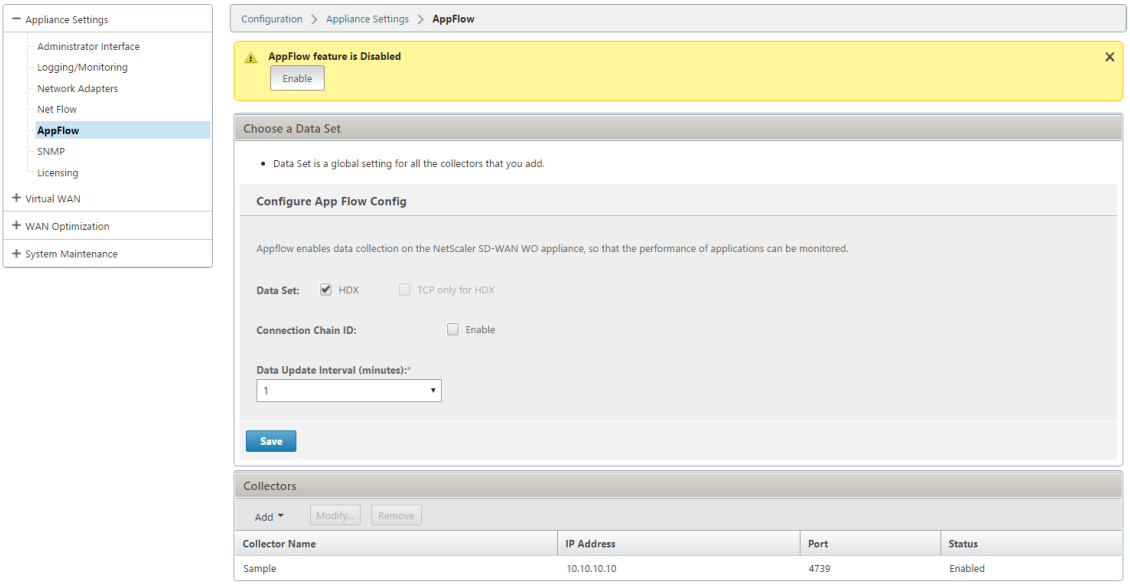
Monitoring

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.



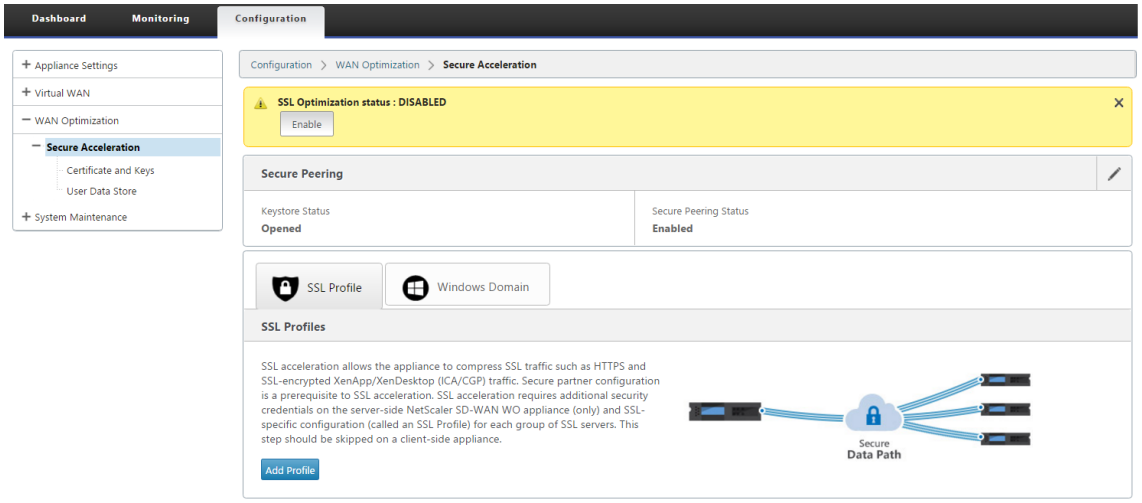
Configuration

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. The configuration done on the SDWAN-SE reflects on the SDWAN-WO configuration, maintaining seamless APPFLOW functionality support.



SD-WAN WANOP already discovered by Citrix Application Delivery Management (ADM), if used in Two Box Mode, should be isolated and not configured using Citrix ADM until this mode is turned off. This is because the configuration of WANOP for traffic processing is managed 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 up-

grade 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

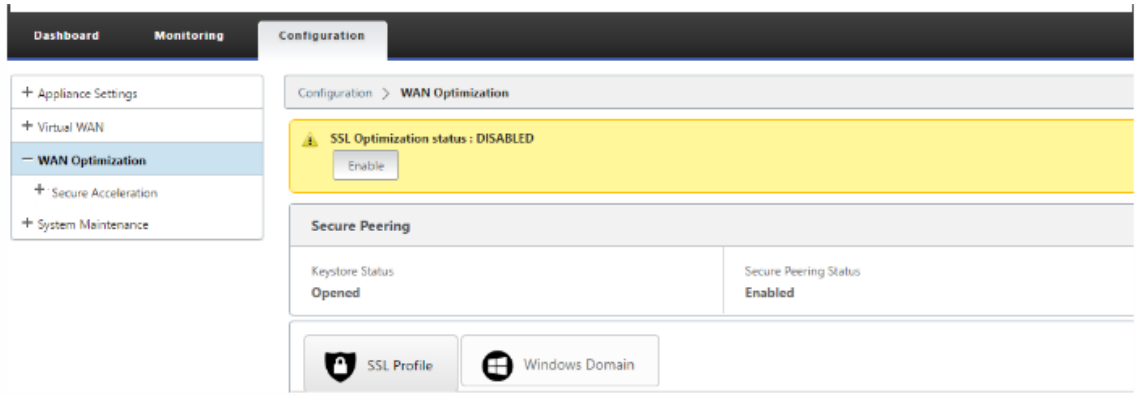
When you enable the two box mode with SD-WAN SE and SDWAN-WANOP appliances, you can view the configuration in the SD-WAN SE appliance similar to how you can view two box configuration with the SD-WAN-EE appliance.

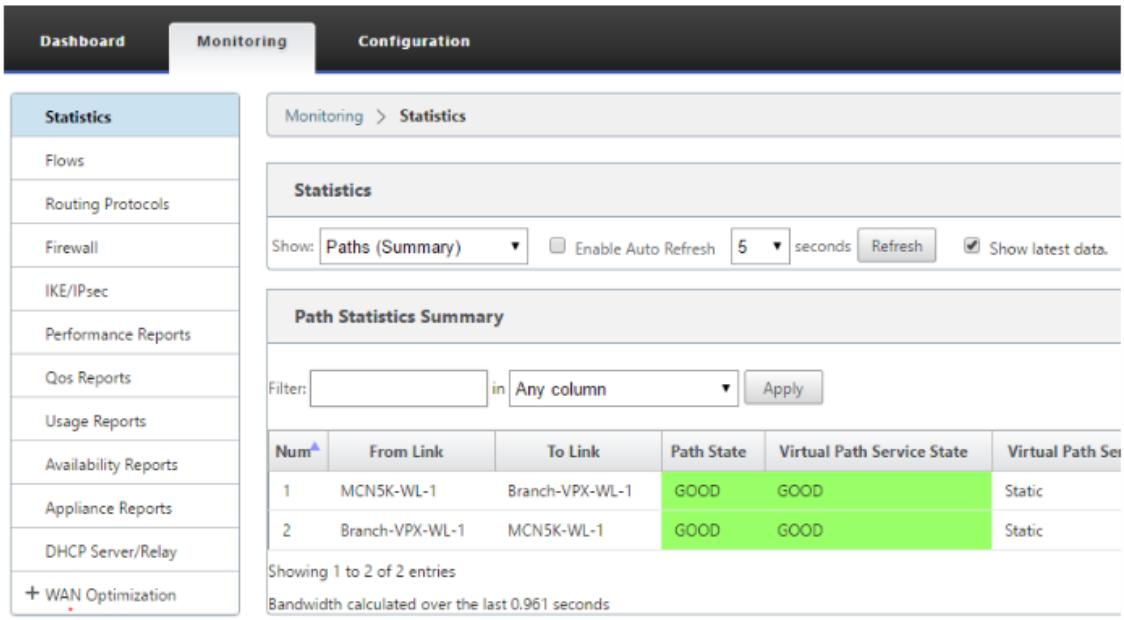
1. Go to **Configuration** > **Virtual WAN** > **WAN Optimization**
2. Appflow node under **Configuration** > **Appliance Settings**
3. WAN Optimization node under Configuration.

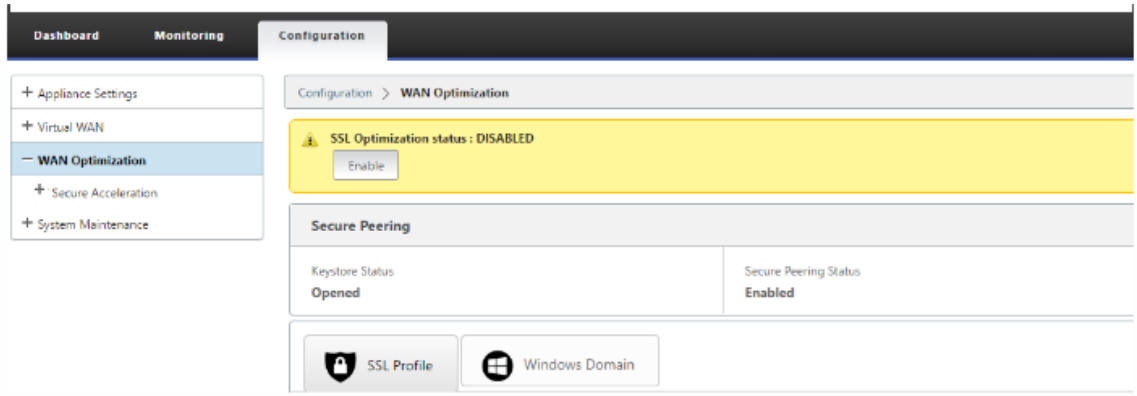
   This information is redirected from the SD-WAN WANOP appliance which is in Two box mode with the SD-WAN SE appliance.

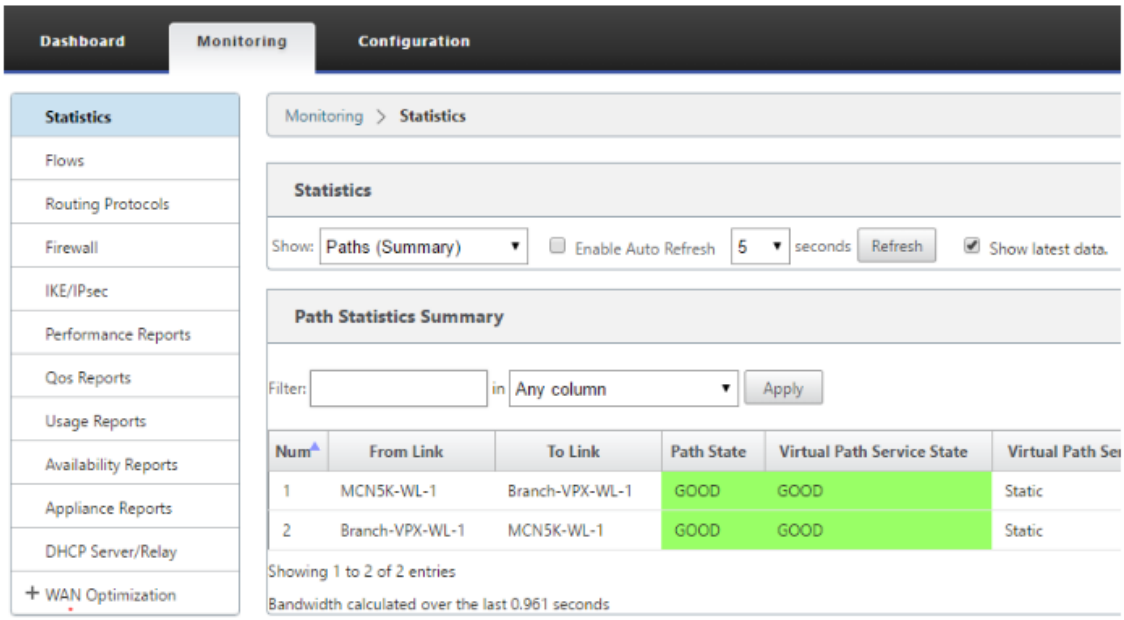
   Configuration related to WANOP, such as SSL Acceleration and AppFlow can now be performed from SD-WAN SE web GUI.

   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 Premium (Enterprise) edition appliance.









Management IP Address Change for SD-WAN WANOP Appliance in Two Box Mode

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. It 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.

Disable two box mode on SD-WAN WANOP appliance

To disable or decouple the SD-WAN WANOP and SD-WAN SE appliances from the Two Box mode:

1. Disable the Two Box mode from SD-WAN WANOP appliance.
2. It is expected to 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

September 23, 2021

This topic covers the High Availability (high availability) deployments and configurations supported by SD-WAN appliances (Standard Edition and Premium (Enterprise) Edition).

Citrix 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 the 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. The Standby appliance monitors the Active 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.

High availability deployment modes

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 the challenges of fail-to-wire. 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**:

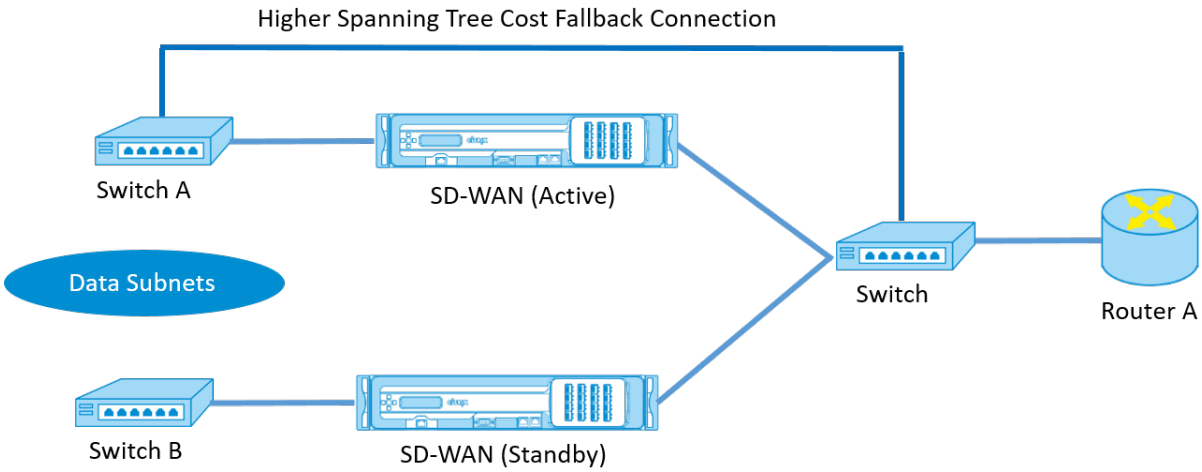
  The active traffic flows even if the virtual path is down, as long as one of the SD-WAN appliances is active. The SD-WAN appliance redirects traffic back to the router as Intranet traffic. However, if both active/standby SD-WAN appliances become inactive, the router tries to redirect traffic to the appliances. IP SLA monitoring can be configured at the router to disable PBR, if the next appliance is not reachable. It allows the router to fall back to perform a route lookup and forward packets appropriately.

Parallel Inline high availability mode:

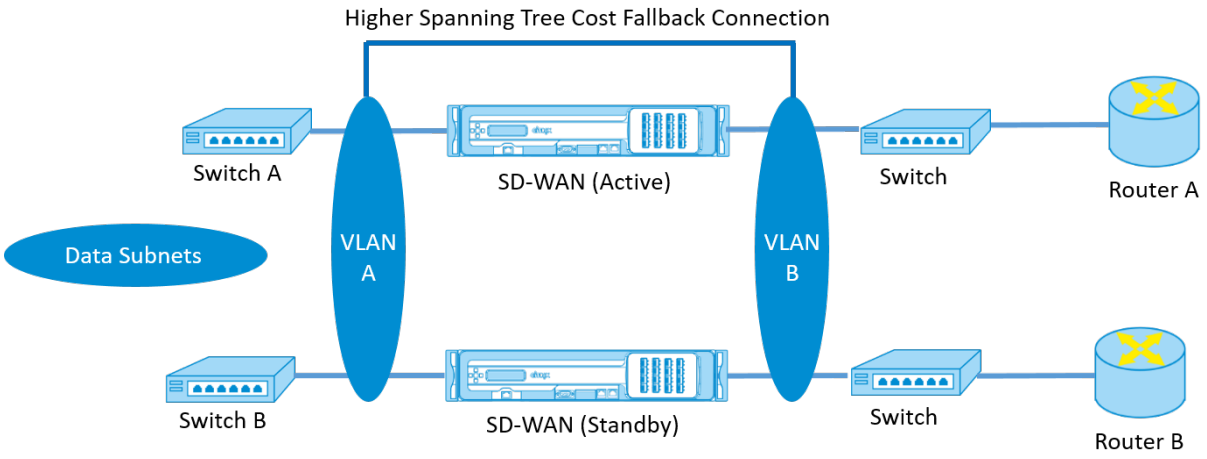
In Parallel Inline high availability mode, the SD-WAN appliances are deployed alongside each other, inline with the data path. Only one path through the Active appliance is used. It is important to note that bypass interface groups are configured to be fail-to-block to avoid bridging loops during a failover.

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 depends on the configured failover time, the default failover time is 1000 ms. However, a failover has a traffic impact of 3-5 seconds. Fall back to the tertiary path impacts traffic for the duration of spanning tree re-convergence. 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.



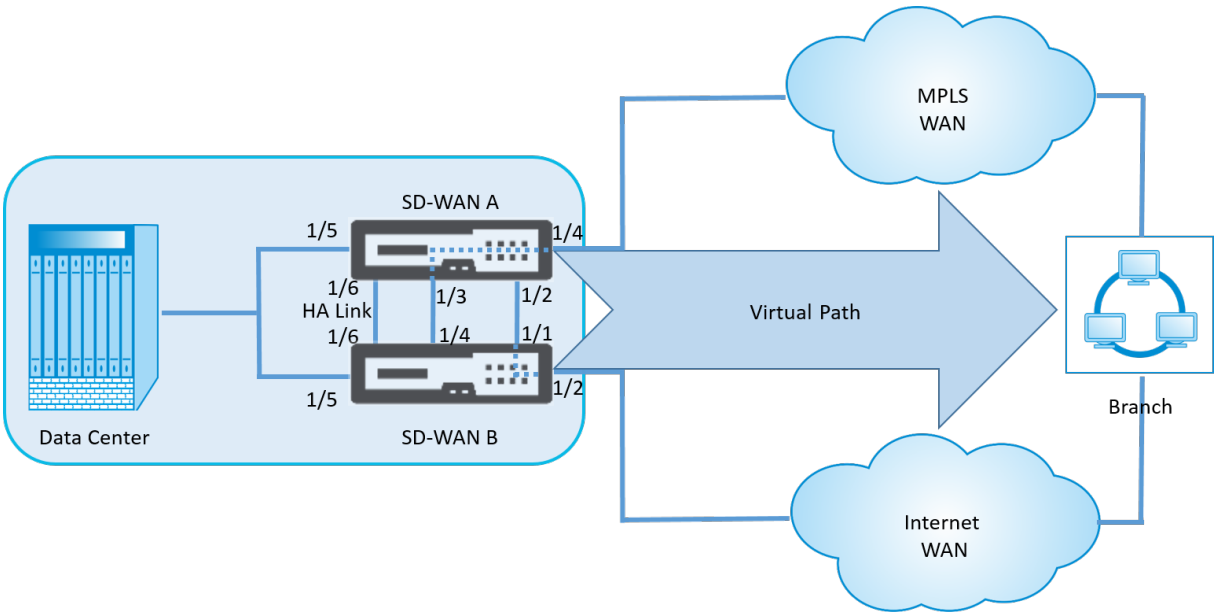
Fail-to-Wire mode:

In fail-to-wire mode, the SD-WAN appliances are inline in the same data path. The bypass interface groups must 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 approximately 10–12 seconds because of the delay in ports to recover from Fail-to-Wire mode.
> - If the high availability connection between the appliances fails, both appliances go into Active state and cause a service interruption. To mitigate the service interruption, assign 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 is used in the hardware appliance pairs for the 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.

The following illustration shows an example of the Fail-to-Wire deployment.



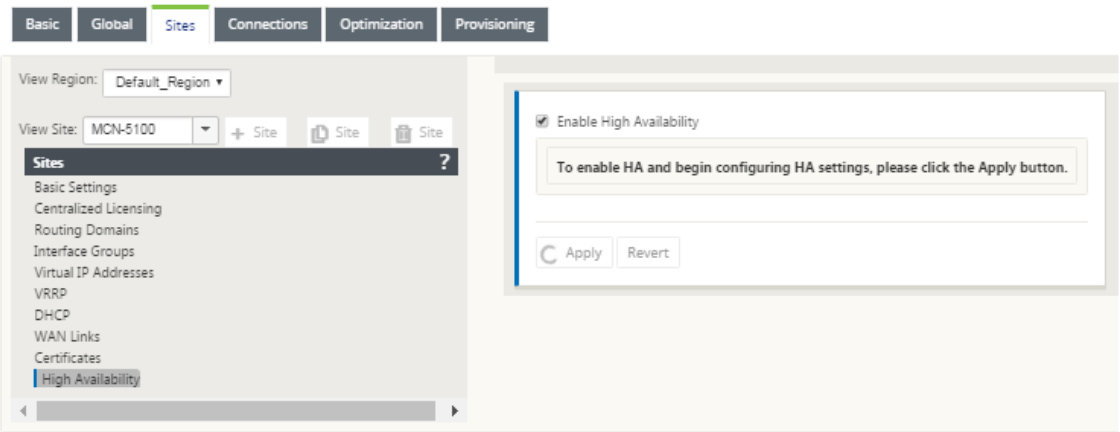
The One-Arm high availability configuration or Parallel Inline high availability configuration is recommended for data centers or Sites that forward a high volume of traffic to minimize disruption during failover.

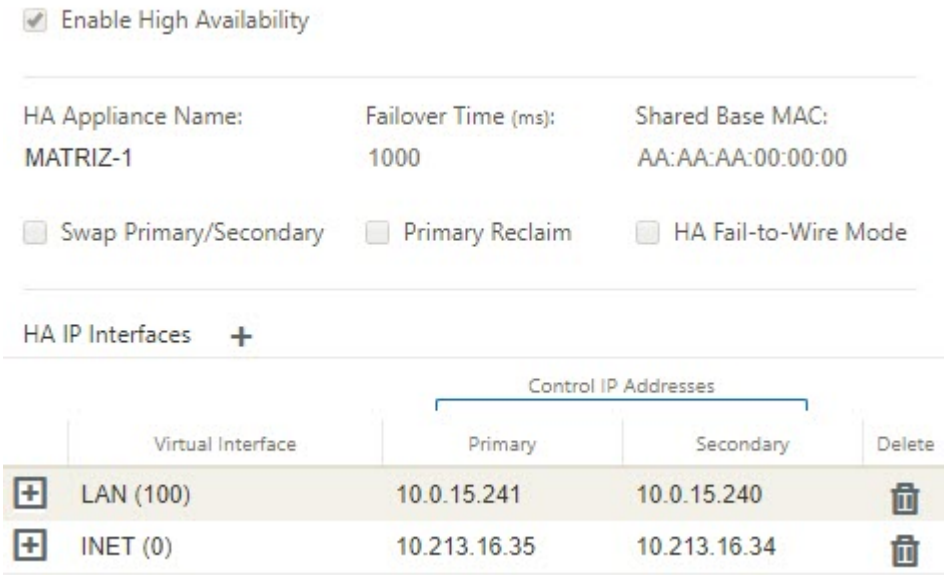
If minimal loss of service is acceptable during a failover, then Fail-to-Wire high availability mode is a better solution. The Fail-to-Wire high availability mode protects against appliance failure and parallel inline high availability protects against all failures. In all scenarios, high availability is valuable to preserve the continuity of the SD-WAN network during a system failure.

Configure high availability

To configure high availability:

1. In the Configuration Editor, navigate to **Sites** > **site name** > **High Availability.** Select **Enable High Availability,** and click **Apply.**





2. Type values for the following parameter:

   - **High availability Appliance Name:** The name of the high availability (secondary) appliance.
   - **Failover Time:** The wait time (in milliseconds) after contact with the primary appliance is lost, before the standby appliance becomes active.
   - **Shared Base MAC:** 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 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 selected, the designated primary appliance reclaims control upon restart after a failover event.
- **High availability Fail-to-Wire Mode:** Select to enable Fail-to-Wire high availability deployment mode.

> **Note**
>
> For hypervisor and cloud based platforms choose the **Disable Shared Base MAC** option to disable the shared virtual MAC address.
>
> 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 promiscu-

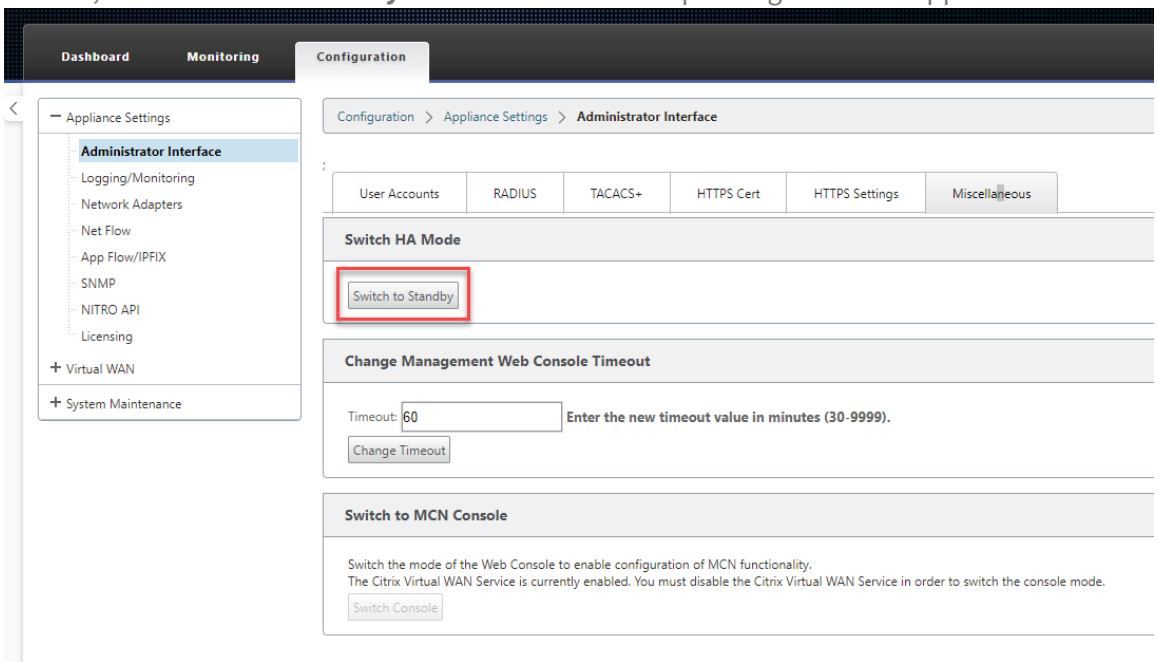
> ous mode is not enabled, you can enable the **Disable Shared Base MAC** option.

Click **+** next to **high availability IP Interfaces to configure interface groups**. Type Values for the following parameters:

- **Virtual Interface** –The Virtual Interface to be used for communication between the appliances in the high availability pair. It monitors the Active appliance for reachability. For One-Arm high availability mode, only one interface group is required.
- **Primary** –The unique Virtual IP address for the primary appliance. The secondary appliance uses the Primary Virtual IP address to communicate with the primary appliance.
- **Secondary** –The unique Virtual IP address for the secondary appliance. The primary appliance uses the Secondary Virtual IP address to communicate with the secondary appliance.

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 and then click **Apply**.

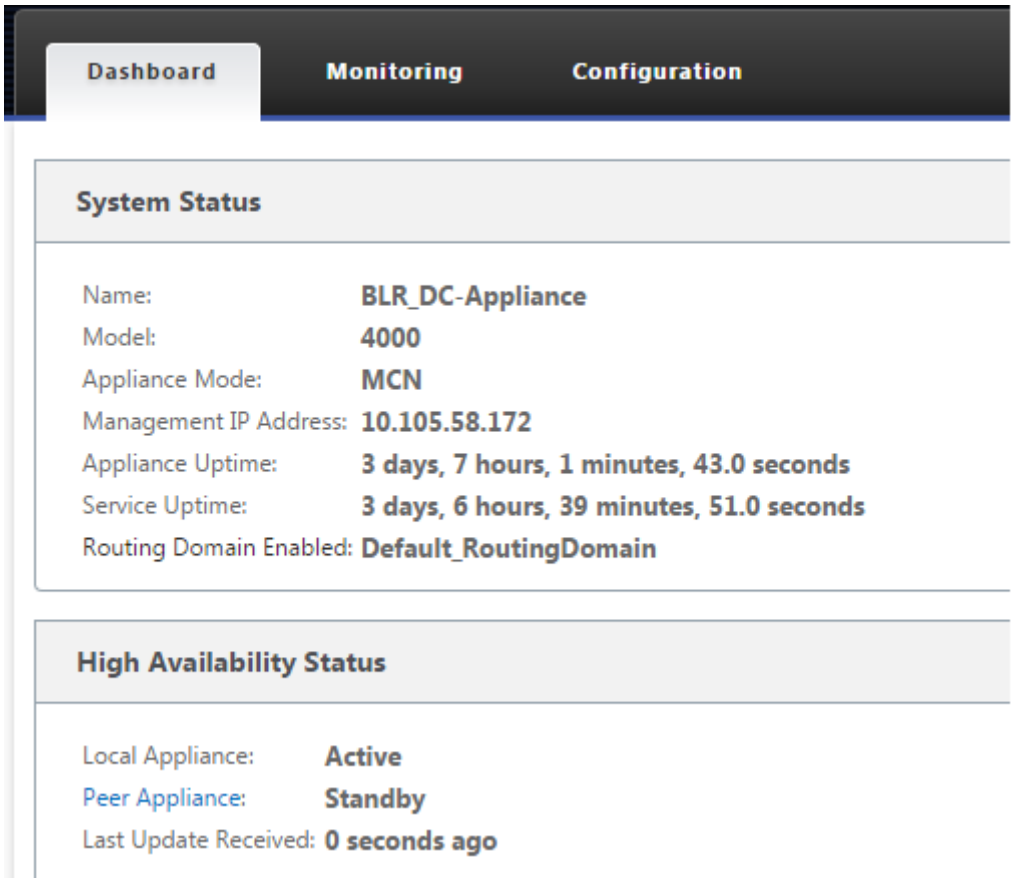
> **Note:**
>
> You can also manually trigger a HA switchover from the appliance. Navigate to **Configuration** > **Appliance Settings** > **Administrator Interface** > **Miscellaneous**. In the Switch HA Mode section, click **Switch to Standby** or **Switch to Active** depending on the HA appliance.

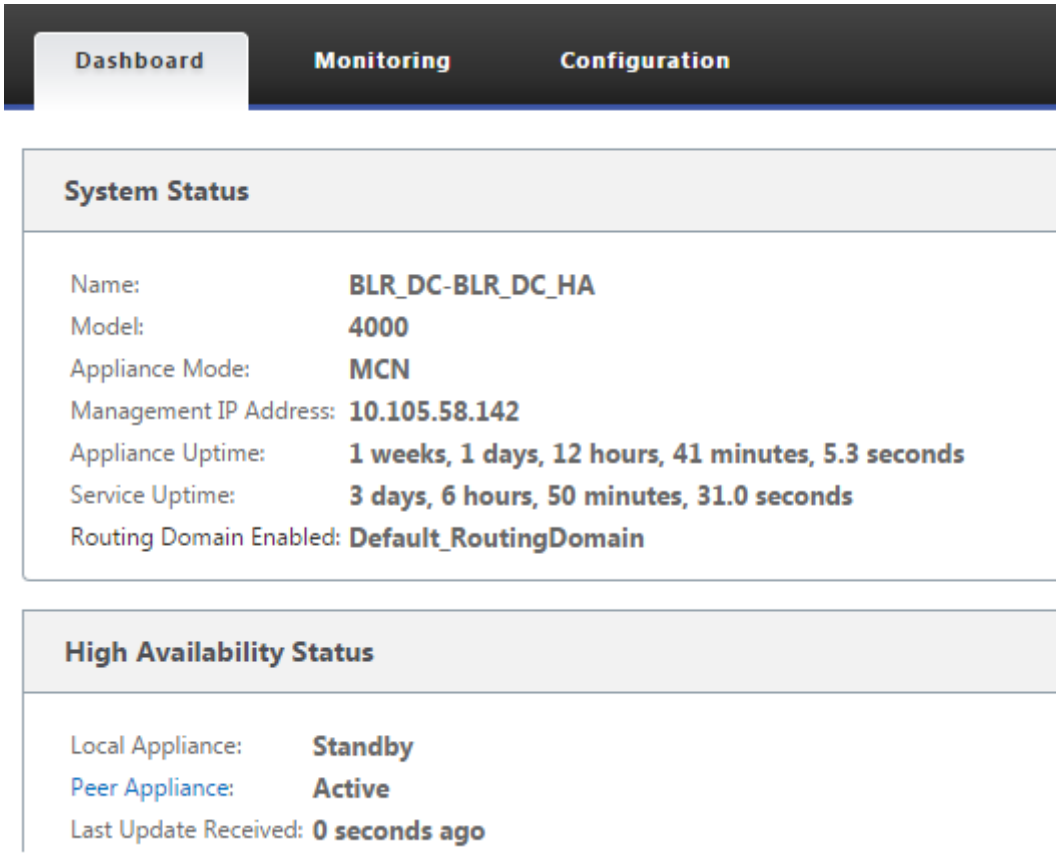


Monitoring

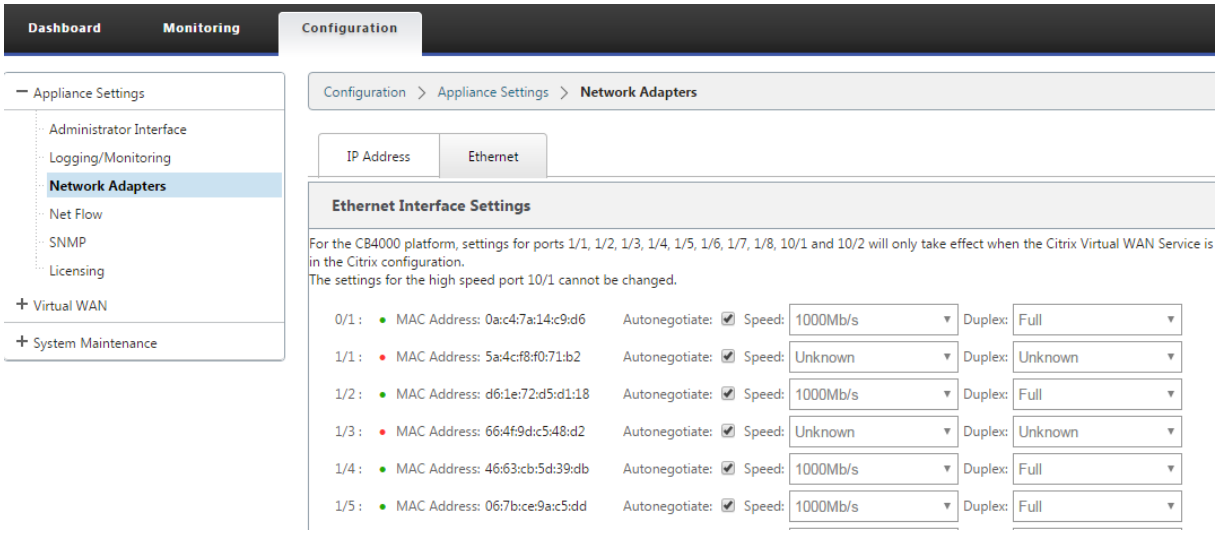
To monitor high availability configuration:

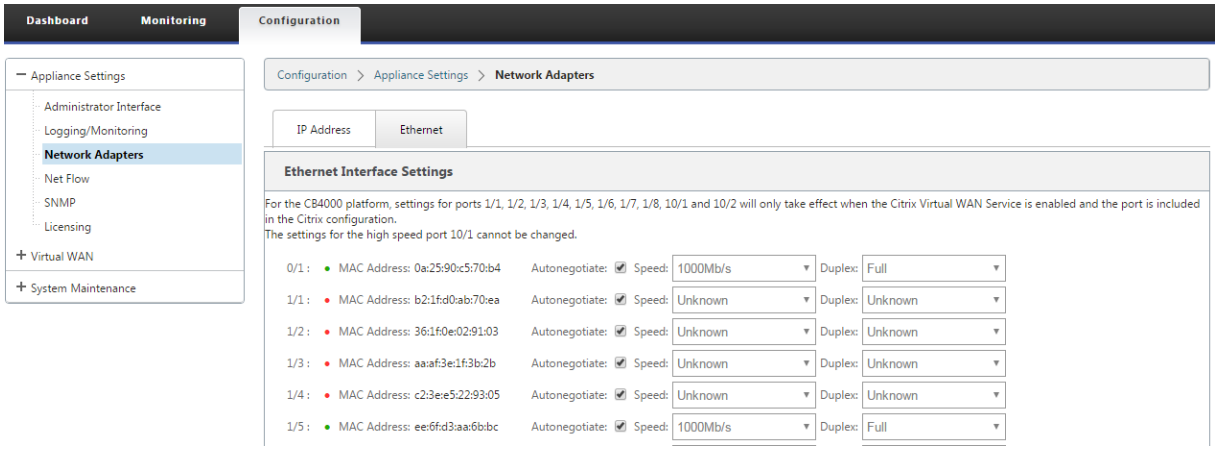
Log in to the SD-WAN web management interface for the Active and Standby appliance's for which high availability is implemented. View high availability status under the **Dashboard** tab.





For Network Adapter details of Active and Standby high availability appliances, navigate to **Configuration** > **Appliance Settings** > **Network Adapters** > **Ethernet** tab.





Troubleshooting

Perform the following troubleshooting steps while configuring the SD-WAN appliance in High Availability (HA) mode:

1. The primary reason for split-brain issue is due to communication problem between the HA appliances.
   - Check if any issue with the connectivity (such as, the ports on both the SD-WAN appliance are up or down) between the SD-WAN appliances.
   - Must disable SD-WAN service on one of the SD-WAN appliances to ensure only one SD-WAN appliance be active.
2. You can verify the HA related logs that is logged into **SDWAN_common.log** file.

   > **NOTE**
   > All the HA related logs is logged with the key word **racp**.

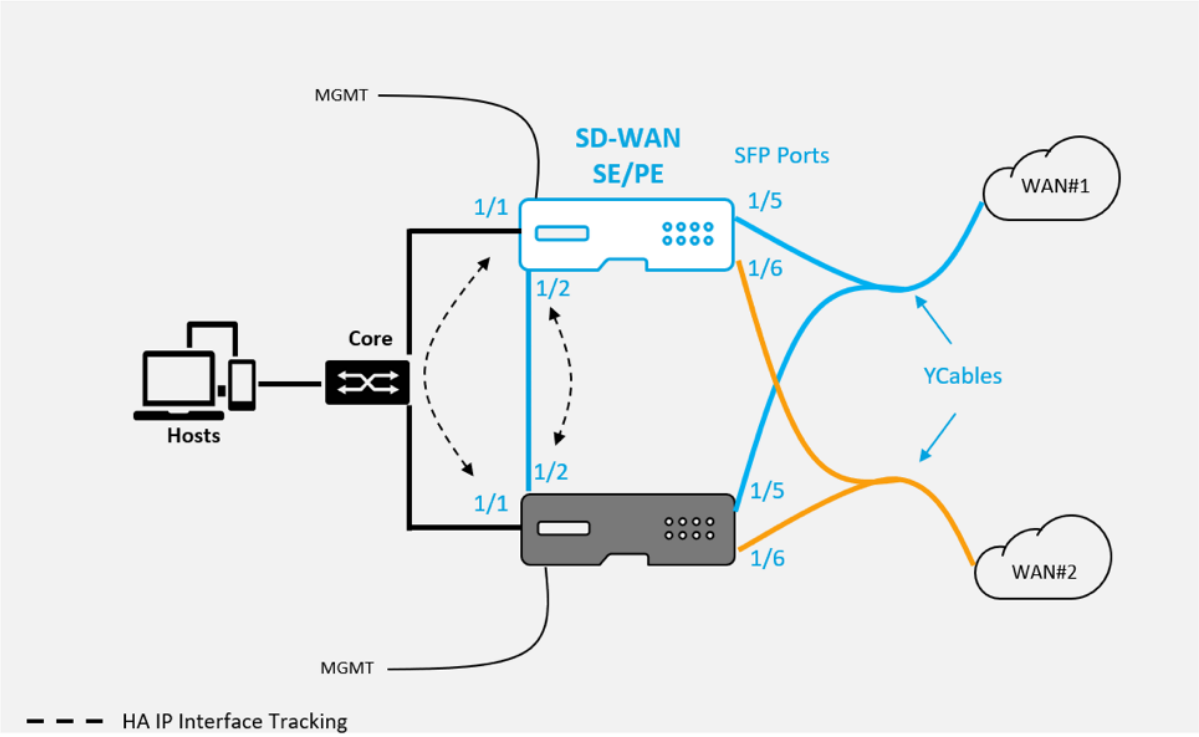
3. You can verify the port related events in **SDWAN_common.log** file (such as, the HA enabled ports goes down or up).
4. For every HA state change, one SD-WAN event is logged. So if the logs are rolled over, you can verify the event logs to get the event details.

Enable Edge Mode High Availability Using Fiber Optic Y-Cable

March 12, 2021

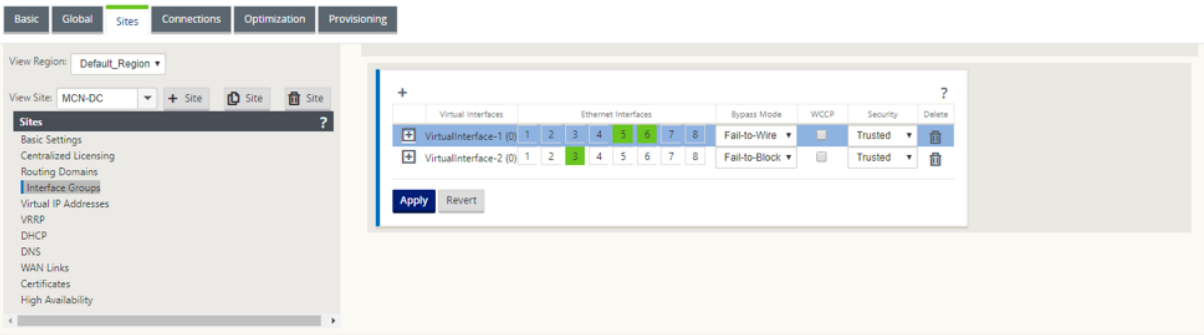
> Note: In release 10.2 version 2, this functionality is applicable to the 1100 SE/PE appliance only.

The following procedure describes the steps to enable High Availability (HA) on 1100 SE/PE appliances deployed in Edge Mode where the handoffs from the WAN link service providers are fiber optic.
The available Small Form-factor Pluggable (SFP) ports on 1100 appliances can be used with fiber optic Y-Cables to enable high availability feature for Edge Mode deployment.
On the 1100 SE/PE appliance the splitter cable split end connects to fiber ports of two 1100 appliances that are configured in HA pair.
The fiber optic Y-Cable has three ends. One end connects to the fiber handoff of the provider and the other two ends connect to SFP ports configured for that WAN link on two 1100 SE/PE appliances deployed in HA pair. The splitter cable is used to divide one incoming signal into multiple signals.



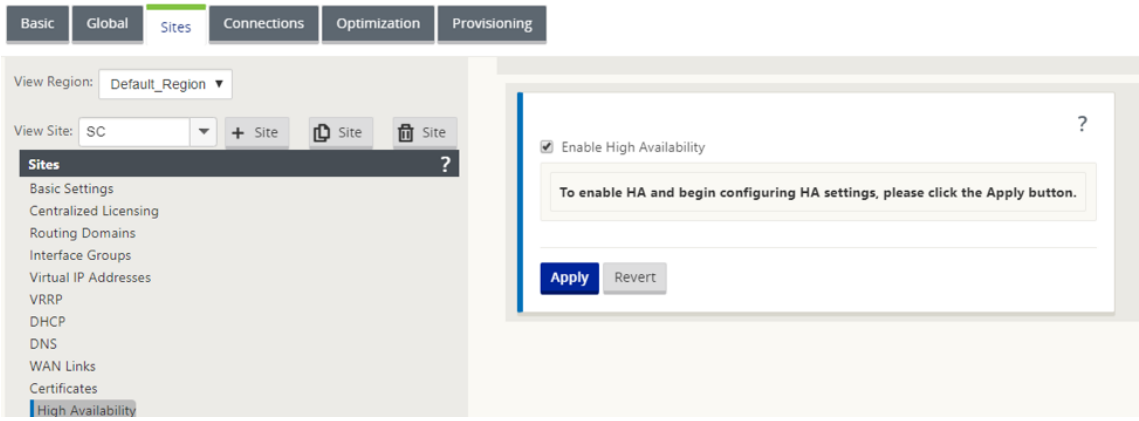
Pre-requisites:

1. On the 1100 SE/PE appliance the ports 1/5 and 1/6 are SFP ports. Connect the splitter ends of the Y cable to any one of these ports on both the appliances in HA pair, see 1100 SE for more information.
2. Add SFP ports to the SD-WAN appliance configuration. Configuring the SFP ports is the same as configuring any network interface ports. For more information, see How to configure interface groups. Adding 1/5 or 1/6 ports to the configuration allows you to enable Y-cable support feature.

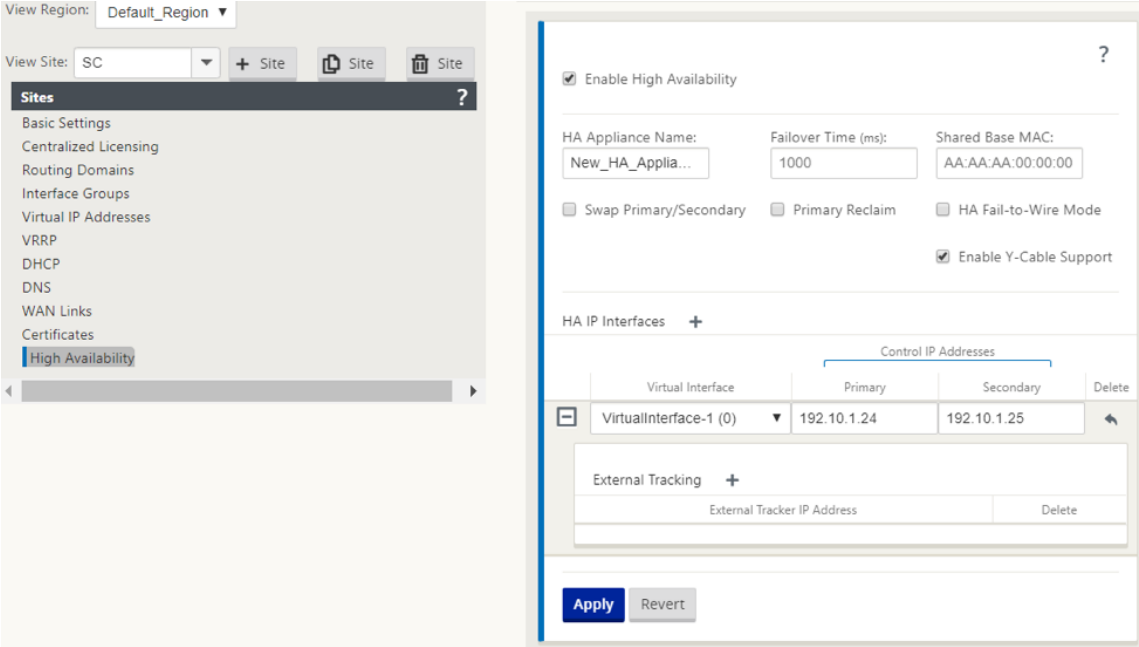


To enable High Availability using Y-cable:

1. In the 1100 SE/PE appliance GUI, navigate to **Configuration > Virtual WAN > Configuration Editor > Sites**. Click **Enable High Availability**.



2. Click **Enable Y-Cable Support**.
3. Add HA IP Interfaces utilizing any other interface besides the interfaces connected to the Y-Cables (e.g. 1/1 LAN facing interface, or 1/2 directly connected interfaces). When the Y-cable feature is enabled, SFP ports cannot be used for the HA IP interfaces.



4. Apply, Stage, and Activate the configuration.

Limitations:

- HA Fail-to-Wire Mode configuration using Y-cable is not supported.
- The SFPs connected to the Y-cable, cannot be used as HA IP interface tracking.
- Software release 10.2.2 or greater, and 11.0 or greater is required to support this deployment.

Zero touch

October 4, 2021

> **Note**
>
> The Zero Touch Deployment service is supported only on select Citrix SD-WAN appliances:
>
> - SD-WAN 110 Standard Edition
> - SD-WAN 210 Standard Edition
> - SD-WAN 410 Standard Edition
> - SD-WAN 2100 Standard Edition
> - SD-WAN 1000 Standard Edition (reimage required)
> - SD-WAN 1000 Enterprise Edition (Premium Edition) (reimage required)
> - SD-WAN 1100 Standard Edition
> - SD-WAN 1100 Premium (Enterprise) Edition

> - SD-WAN 2000 Standard Edition (reimage required)
> - SD-WAN 2000 Enterprise Edition (Premium Edition(reimage required)
> - SD-WAN 2100 Enterprise Edition (Premium Edition)
> - SD-WAN AWS VPX instance

Zero-touch deployment Cloud Service is a Citrix operated and managed cloud-based service which allows discovery of new appliances in the Citrix SD-WAN network, primarily focused on streamlining the deployment process for Citrix SD-WAN at branch or cloud service office locations. The zero-touch deployment Cloud Service is publicly accessible from any point in a network via public Internet access. The zero-touch deployment Cloud Service is accessed over the Secure Socket Layer (SSL) Protocol.

The zero-touch deployment Cloud Services securely communicate with back-end Citrix services hosting stored identification of Citrix customers who have purchased Zero Touch capable devices (for example SD-WAN 410-SE, 2100-SE). The back-end services are in place to authenticate any Zero Touch Deployment request, properly validating association between the Customer Account and the Serial Numbers of Citrix SD-WAN appliances.

ZTD High-Level Architecture and Workflow:

Data Center Site:

Citrix SD-WAN Administrator –A user with Administration rights of the SD-WAN environment with the following primary responsibilities:

- Configuration creation using Citrix 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 Proxy Server Settings for Zero Touch Deployment.

Network Administrator –A user responsible for Enterprise network management (DHCP, DNS, internet, firewall, and so on)

- If necessary, configure firewalls for outbound communication to FQDN ***sdwanzt.citrixnetworkapi.net*** from SD-WAN Center.

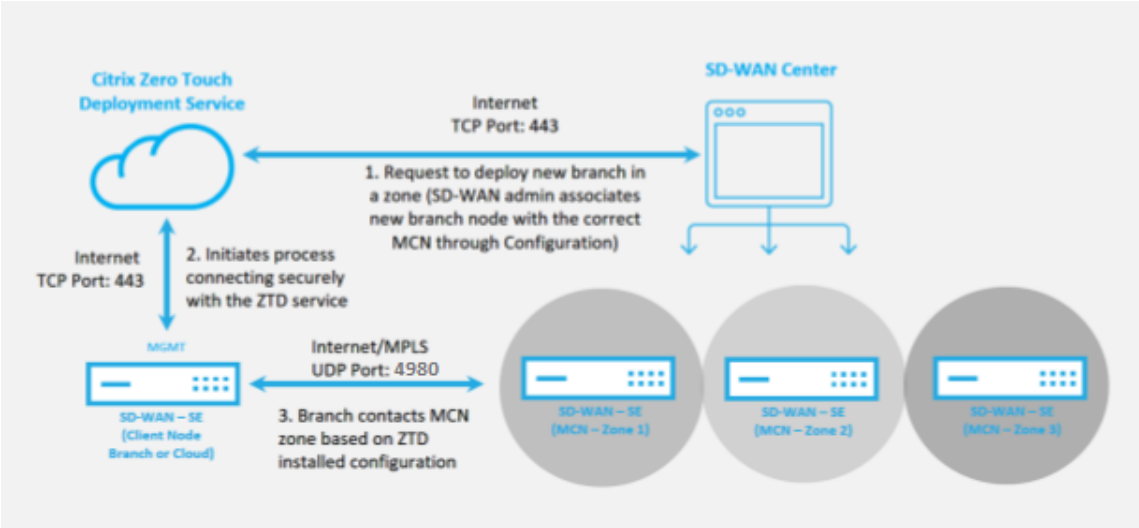
Remote Site:

Onsite Installer –A local contact or hired installer for on-site activity with the following primary responsibilities:

- Physically unpack the Citrix SD-WAN appliance.

- Reimage non-ZTD ready appliances.
  - Required for: SD-WAN 1000-SE, 2000-SE, 1000-EE, 2000-EE
  - Not required for: SD-WAN 410-SE, 2100-SE
- Power cable the appliance.
- Cable the appliance for internet connectivity on the Management interface (for example MGMT, or 0/1).
- Cable the appliance for WAN link connectivity on the Data interfaces (for example apA.WAN, apB.WAN, apC.WAN, 0/2, 0/3, 0/5, and so on).

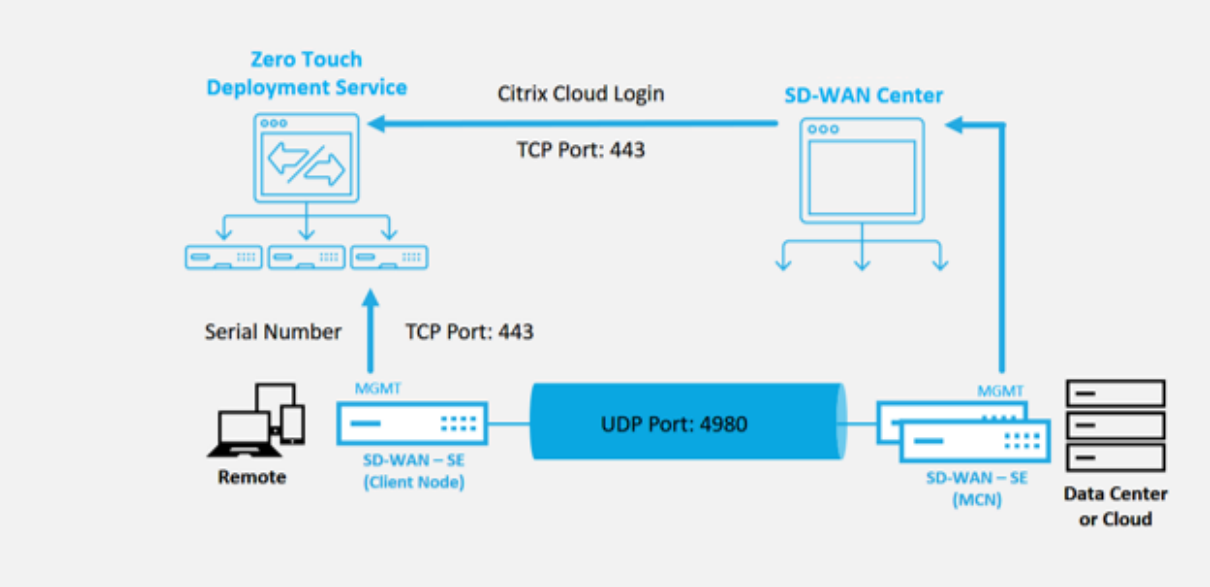
> **Note**
>
> The interface layout is different for each model, so reference the documentation for identification of data and management ports.



The following prerequisites are required before starting any Zero Touch Deployment service:

- Actively running SD-WAN promoted to Master Control Node (MCN).
- Actively running 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 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 SD-WAN Administrator to validate that the underlay network allows Virtual Paths to be established when 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 the 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 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 (Premium) Edition appliances. To use the Zero Touch Deployment Service (or zero-touch deployment Cloud Service), an Administrator must begin by deploying the first 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 automatically initiates the Cloud Service and install the 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 that 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 zero-touch deployment service, the GUI exposes the Zero Touch Deployment options under the **Configuration** tab. Logging into the Zero Touch Service authenticates the Customer ID associated with the particular SD-WAN environment and registers the SD-WAN Center, in addition to unlocking the account for further authentication of zero-touch deployment appliance de-

ployments.

Using the Network Configuration tool in SD-WAN Center, the SD-WAN Administrator will then need to use the templates or clone site capability to build out the SD-WAN Configuration to add new sites. The new configuration is used by the SD-WAN Center to initiate the deployment of zero-touch deployment for the newly added sites. When the SD-WAN Administrator initiates a site for deployment using the zero-touch deployment process, he or she has the option to pre-authenticate the appliance to be used for zero-touch deployment by pre-populating the serial number, and initiating email communication to the on-site installer to begin on-site activity.

The Onsite Installer receives 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 is initiated by the zero-touch deployment Service and progress is monitored by using the activation URL. In the event the remote node to be installed is a cloud instance, opening up the activation URL begins 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 automates the following actions:

Download and Update the zero-touch deployment 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 zero-touch deployment 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 10 Mbps license file for confirmation of Virtual Path establishment to the branch appliance.
- Enable the SD-WAN Service on the branch appliance.

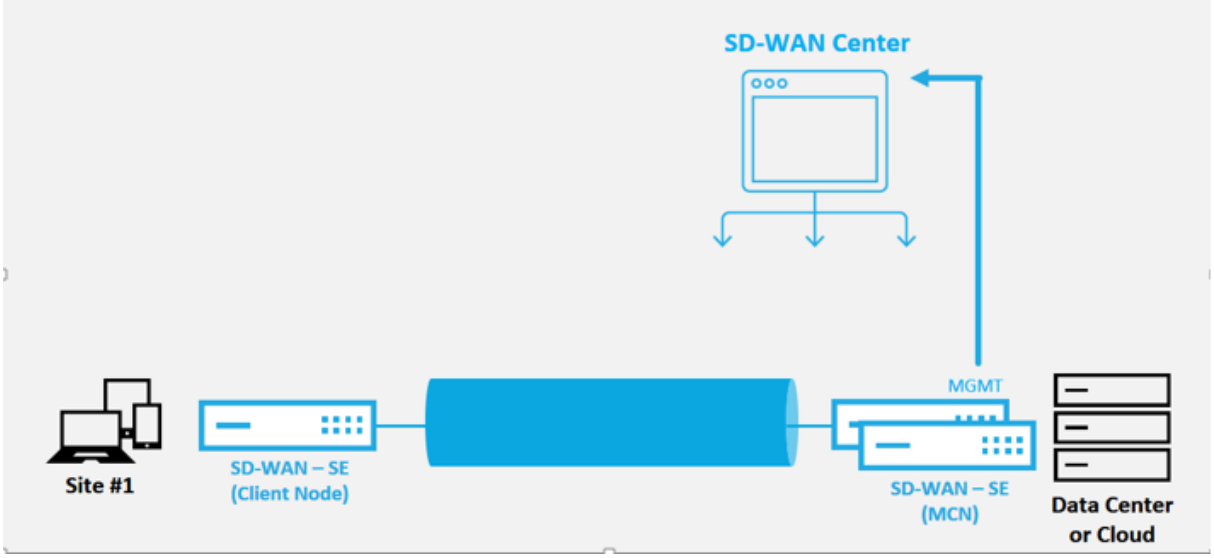
More steps are required of the SD-WAN Administrator to install a permanent license file on the appliance.

> **Note**
>
> While performing a branch configuration that already has the same version of appliance software used in MCN, the zero-touch-deployment process will not download the appliance software file again. This change is applicable for fresh factory shipped appliances, appliances reset to factory

> defaults, and configuration reset administratively. If there is the configuration reset, select the **Reboot after revert** check box to initiate the zero-touch deployment process.

Zero touch deployment device procedure

The following procedure detail the steps required to deploy a new site using the Zero Touch Deployment Service. Have a running MCN and one client node already working with proper communication to SD-WAN Center, and 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:



How to configure zero touch deployment service

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 the existing configuration and save it.
- Log in to Citrix Cloud to enable zero-touch deployment 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 the activation email > Enter the serial number > **Activate** > Appliance is deployed successfully.

To configure Zero Touch Deployment service:

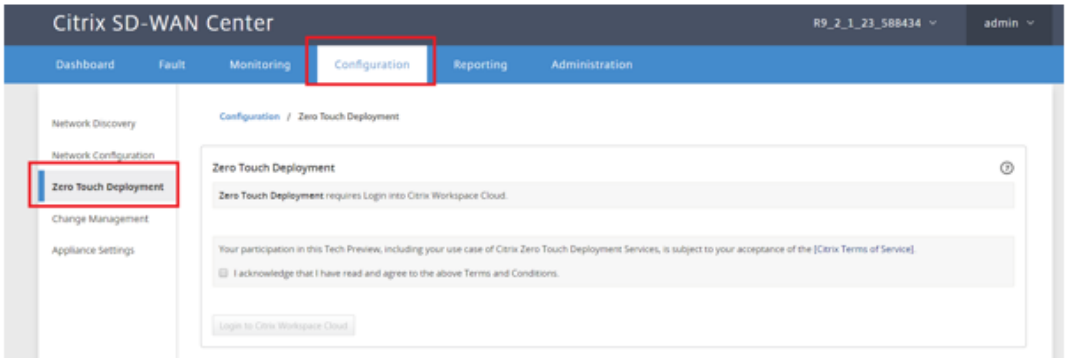
1. Install SD-WAN Center with enabled Zero Touch Deployment capabilities:

   a) Install SD-WAN Center with DHCP assigned IP address.

   b) Verify that 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 SD-WAN Center to the latest SD-WAN software release version.

   d) With proper internet connectivity, the SD-WAN Center initiates the zero-touch-deployment Cloud Service and automatically download and install any firmware updates specific to zero-touch deployment, if this Call Home procedure fails the following Zero Touch Deployment option will not be available in the GUI.

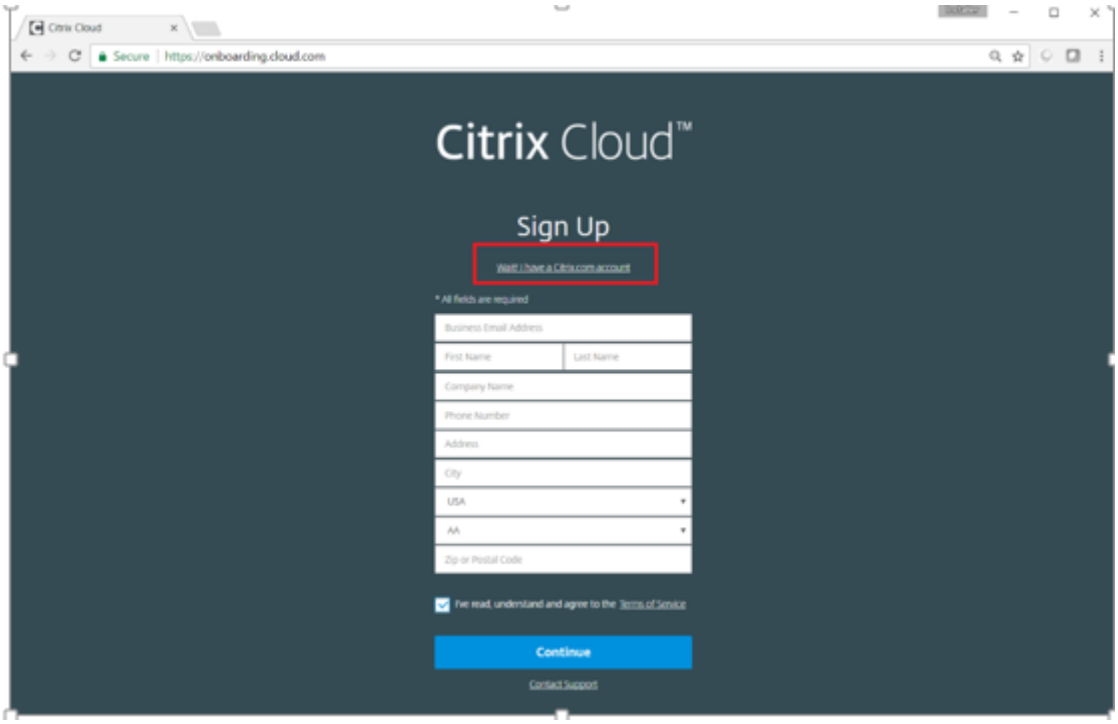


   e) Read the Terms and Conditions, and then select **I acknowledge that I have read and agree to the above Terms and Conditions**.

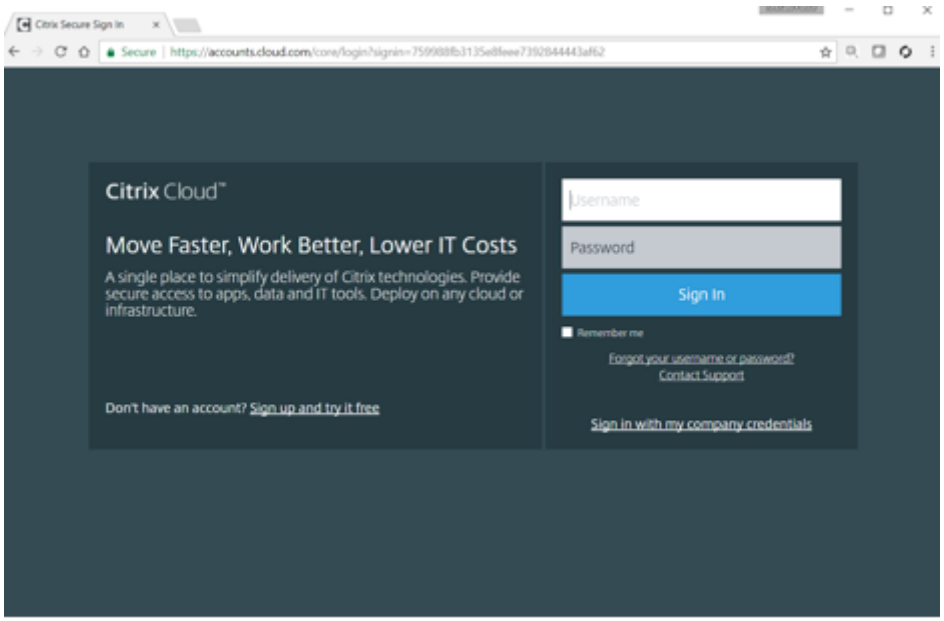
   f) Click the **Login to Citrix Workspace Cloud** button if a Citrix Cloud account has already been created.

   g) Log in 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 must close on its own when it is complete.

2. To create a Cloud Login account follow the below procedure: Open a web browser to https://onboarding.cloud.com
3. Click the link for **Wait, I have a Citrix.com account**.



4. Sign in with an existing Citrix account.



5. Once logged into SD-WAN Center Zero Touch Deployment page, you might notice that no sites are available for zero-touch deployment 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 (for example 410-SE, 2100-SE, Cloud VPX)
6. Update the configuration to add a **new remote** site with a **ZTD capable SD-WAN appliance** using SD-WAN Center Network Configuration.

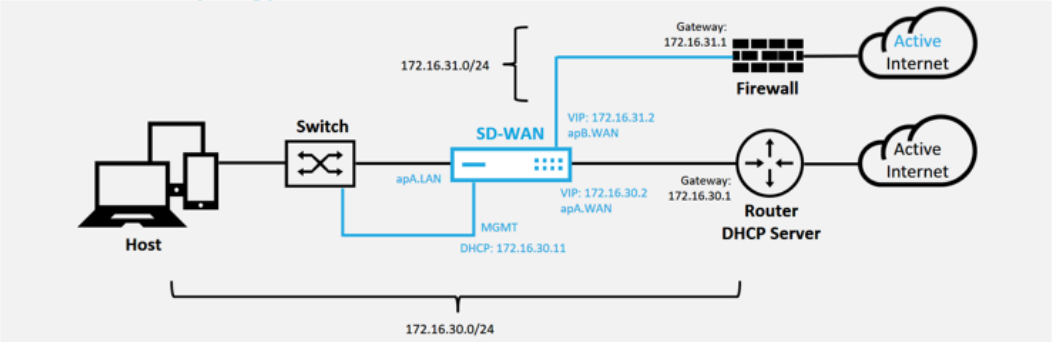
   If the SD-WAN configuration was not built using the SD-WAN Center Network Configuration, import the active configuration from the MCN and begin modifying the configuration using SD-WAN Center. For Zero Touch Deployment capability, the SD-WAN Administrator must build the configuration using SD-WAN Center. The following procedure must 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 (that is, Appliance Model, Interface Groups usage, Virtual IP Addresses, WAN Links with bandwidth and their respective Gateways).

      > **Important**
      >
      > You might notice any site node that has VPX selected as the model is also listed, but currently zero-touch deployment 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 that the web browser is not blocking any pop-up windows during the Citrix Workspace Login

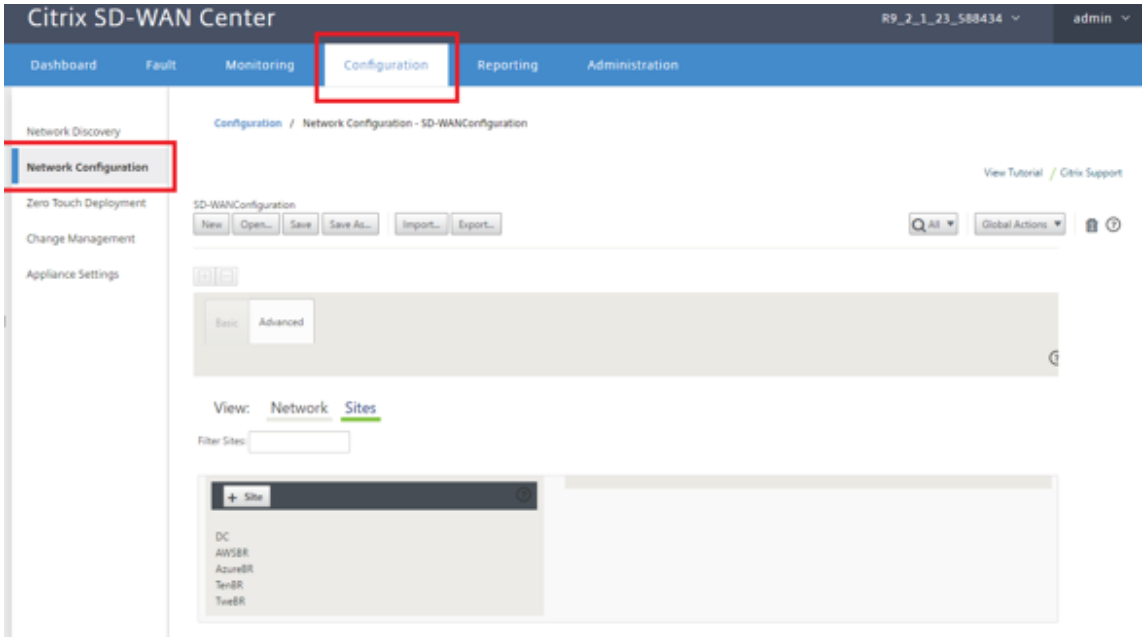
Branch Office Topology



This is an example deployment of a branch office site, the SD-WAN appliance is deployed physically in path of the existing MPLS WAN link across a 172.16.30.0/24 network, and using an existing backup link by enabling it into an active state and terminating that second WAN link directly into the SD-WAN appliance on a different subnet 172.16.31.0/24.

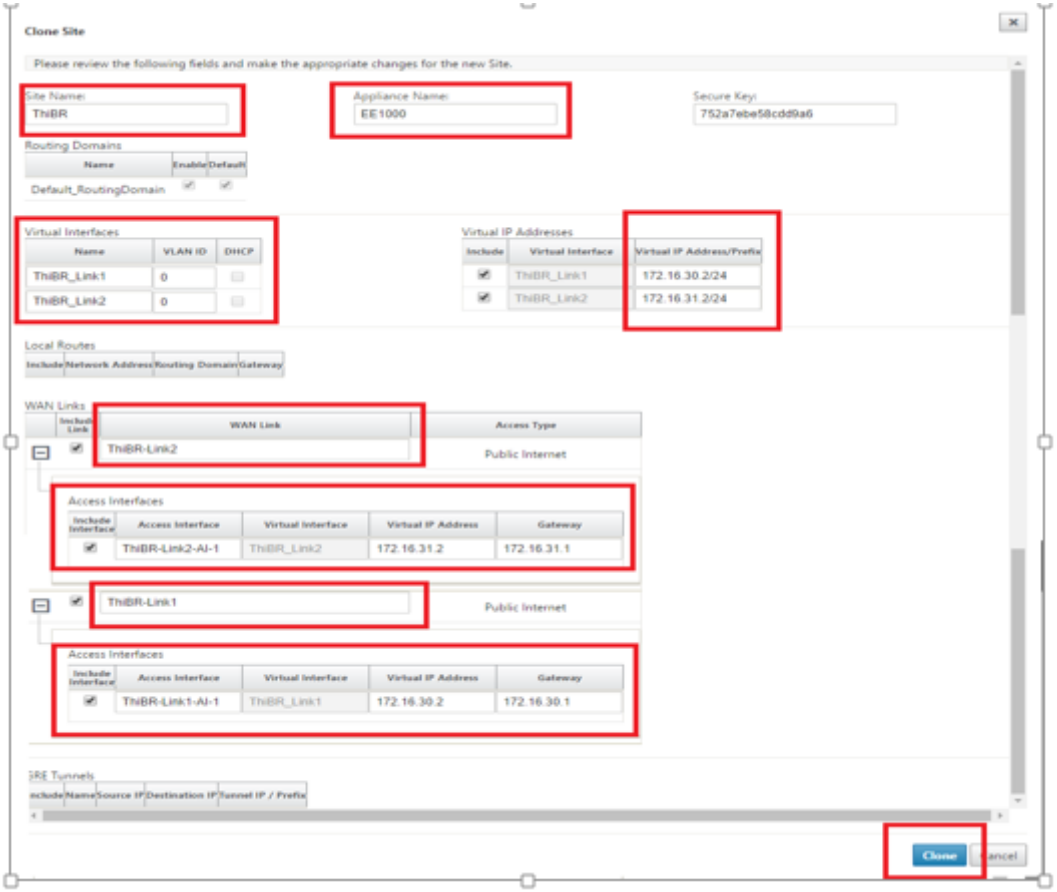
> **Note**
>
> The SD-WAN appliances automatably assign a default IP address of 192.168.100.1/16. With DHCP enabled by default, the DHCP Server in the network might provide the appliance a second IP address in a subnet that overlaps the default. This can possibly result in a routing issue on the appliance where the appliance might fail to connect to the zero-touch deployment Cloud Service. 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 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 might choose to deploy the SD-WAN in Edge or Gateway Mode deployment, eliminating the need for a WAN edge router and firewall, and consolidating the network needs of the edge routing and firewall onto the SD-WAN solution.

7. Open the SD-WAN Center web management interface and navigate to the **Configuration** > **Network Configuration** page.

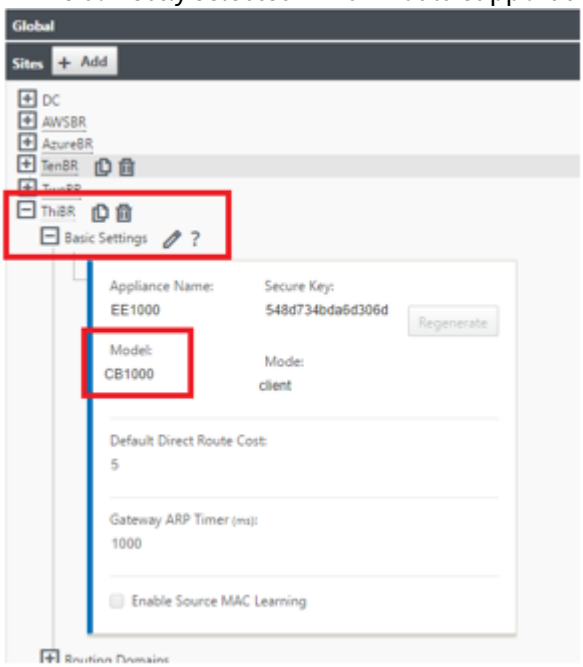


8. Make sure that a working configuration is already in place, or import the configuration from the MCN.
9. Navigate to the Advanced tab to create a site.
10. Open the Sites tile to display the currently configurated sites.
11. Quickly built the configuration for the new site by using the clone feature of any existing site.

12. Populate all the required fields from the topology designed for this new branch site



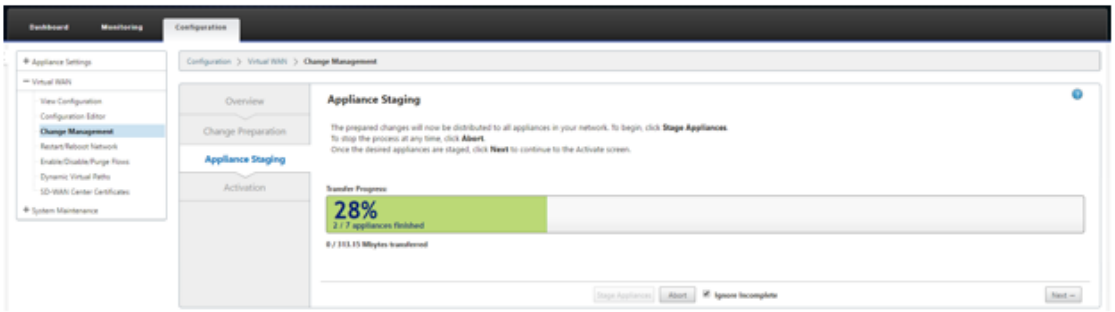
13. After cloning a new site, navigate to the site's **Basic Settings**, and verify that the Model of SD-WAN is correctly selected which would support the zero touch service.



The SD-WAN model for the site can be updated, but do be aware that the Interface Groups might have to be redefined since the updated appliance might have a new interface layout than what was used to clone.

14. 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.

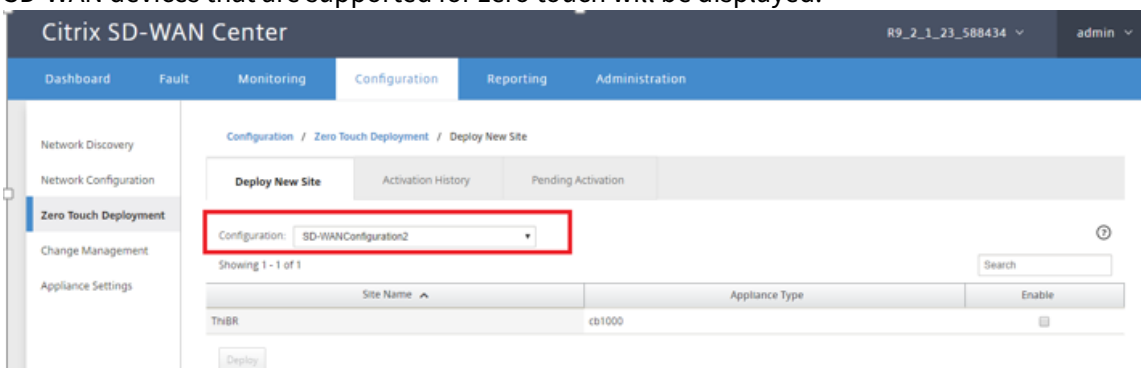
15. Follow the Change Management procedure to properly stage the new configuration, which makes the existing SD-WAN devices aware of the new site to be deployed via zero touch, you must use the "Ignore Incomplete"option to skip attempting to push the configuration to the new site that still must go through the zero-touch deployment workflow.



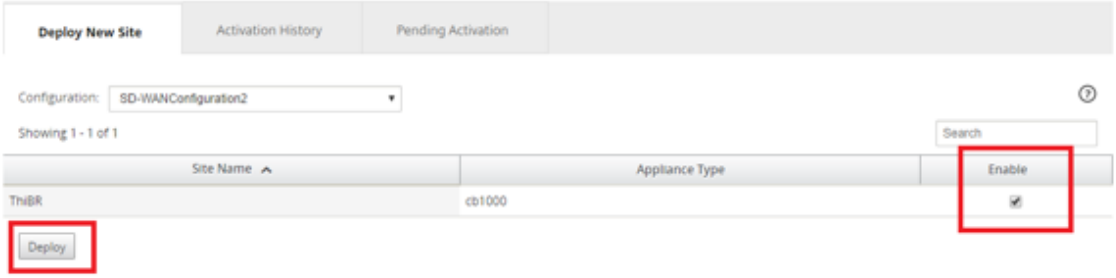
16. Navigate back to the SD-WAN Center Zero Touch Deployment page, and with the new active configuration running, the new site is available for deployment.

17. In the Zero Touch Deployment page, under the **Deploy New Site** tab, select the running network configuration file

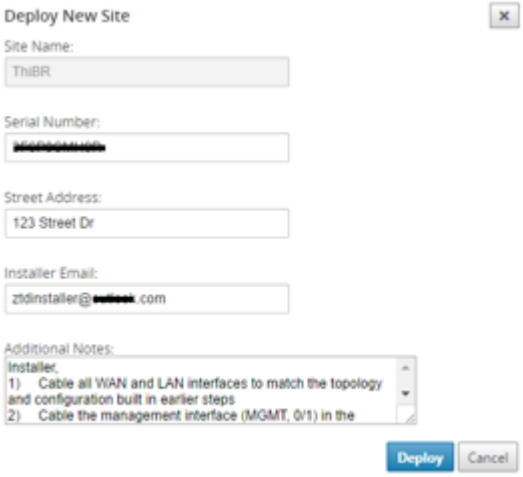
18. After the running configuration file is selected, the list of all the branch sites with undeployed SD-WAN devices that are supported for zero touch will be displayed.



19. Select the branch sites you want to configure for Zero Touch service, click **Enable**, and then **Deploy**.



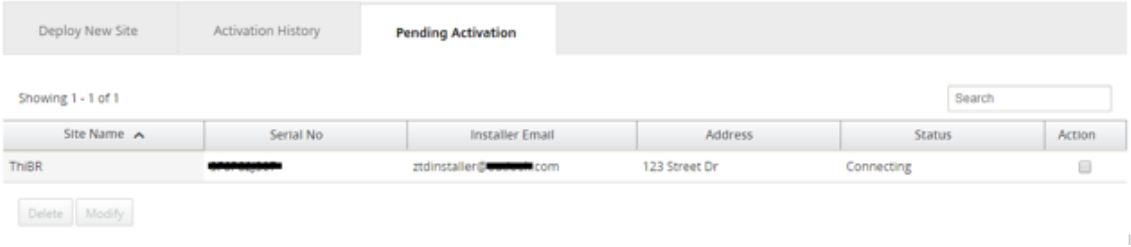
20. A Deploy New Site pop-up window appears, where the Admin can provide the Serial Number, branch site Street Address, Installer Email address, and more Notes, if necessary.



> **Note**
>
> The Serial Number entry field is optional and depending if it is populated or not, results in a change in on-site activity the Installer is responsible for.
>
> ```
> >- If Serial Number field is populated – The installer in not required to enter serial number into the activation URL generated with the deploy site command
> >
> >- If Serial Number field is left black – 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
> ```

21. After clicking the **Deploy** button, a message will appear indicating that “The Site configuration has been deployed.”This action triggers the SD-WAN Center, which was previously registered with the zero-touch deployment Cloud Service, to share the configuration of this particular site to be temporality stored in the zero-touch deployment Cloud Service.

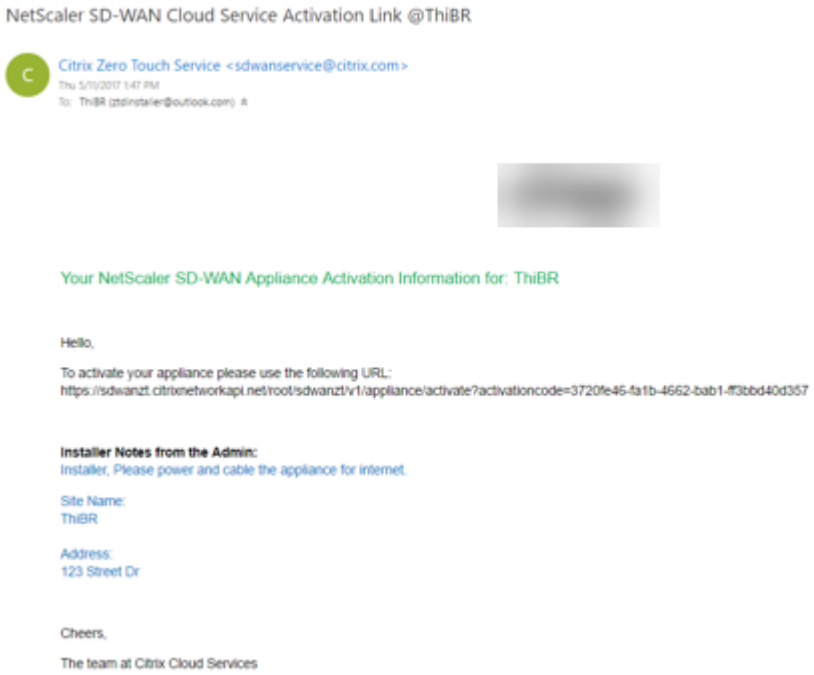
22. Navigate to the Pending Activation tab to confirm that the branch site information populated successfully and was put into a pending installer activity status.



> **Note**
>
> A zero touch deployment in the Pending Activation state can optionally be chosen to Delete or Modify, if information is incorrect. If a Site is deleted from the pending activation page, it becomes 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 becomes invalid.
>
> If the Serial Number field was not populated by the SD-WAN Administrator, the Status Field indicates “Waiting for Installer”instead of “Connecting.”

23. The next series of activities is performed by the On-site Installer.

    a) The Installer verifies the mailbox for the email address that the SD-WAN Administrator used when deploying the site.



    b) Open the zero touch deployment Activation URL in an internet browser window (for example `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 provides 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.

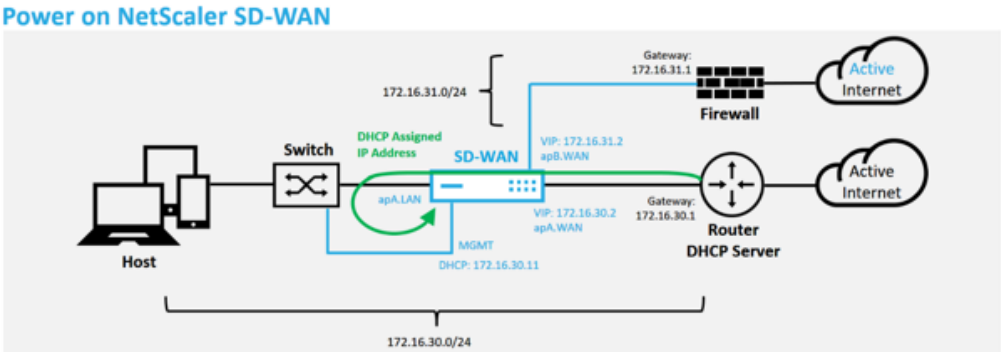
> **Note**
>
> Most appliances will automatically power on when the power cable is attached. Some appliance might have to be powered on using the power switch on the front of the appliance, others might have the power switch on the rear of the appliance. Some power switches require holding the power button until the unit powers up.

24. 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 must be powered up

- DHCP must be available in the existing network to assign management and DNS IP address
- Any DHCP assigned IP address requires connectivity to the internet with the ability to resolve FQDNs
- IP assignment can be configured manually, as long as the other pre-requisites are met

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.

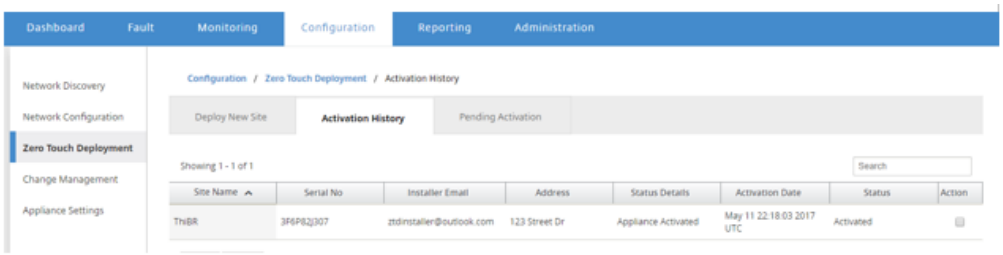


b) As the appliance obtains the web management and DNS IP addresses from the underlay network DHCP Server, the appliance initiates the Zero Touch Deployment Service and download any zero-touch deployment related software updates.

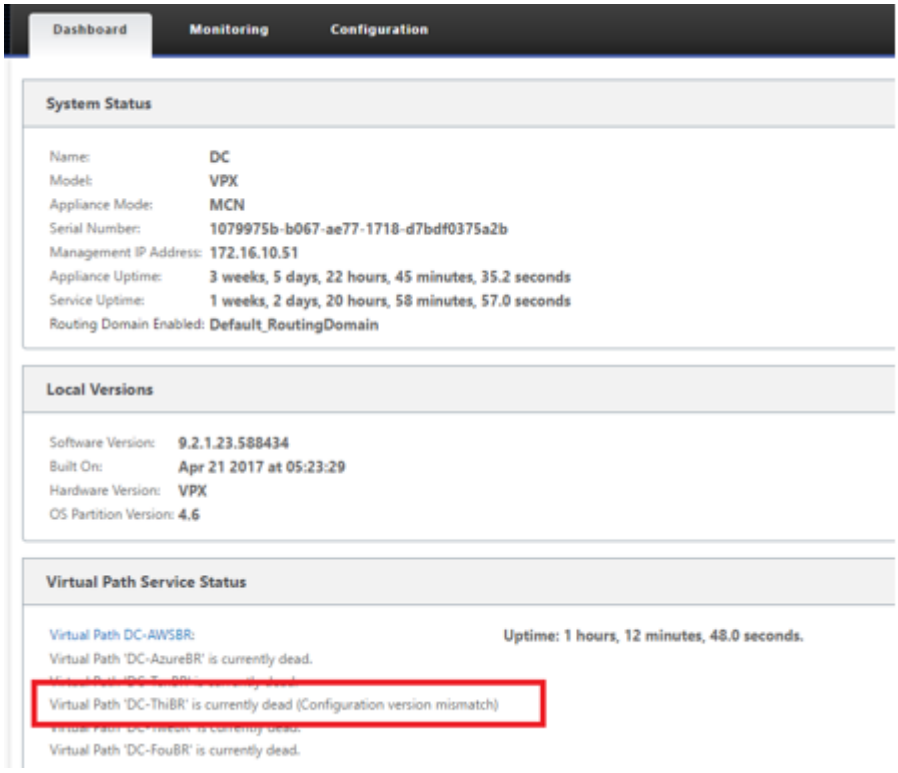
c) With successful connectivity to the zero-touch deployment Cloud Service, the deployment process automatically performs the following:

- Download the Configuration File that is 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

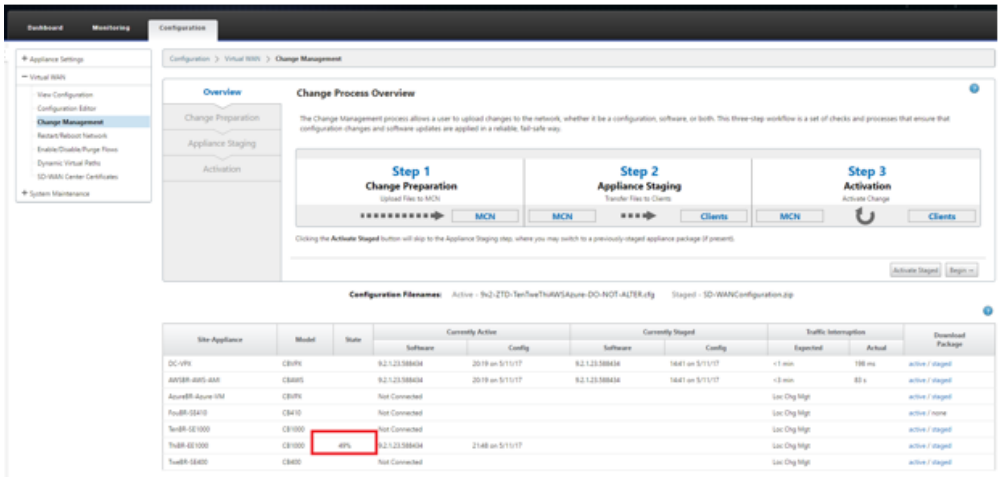
d) Further confirmation can be done in the SD-WAN Center web management interface, the Zero Touch Deployment menu displays successfully activated appliances in the **Activation History** tab.



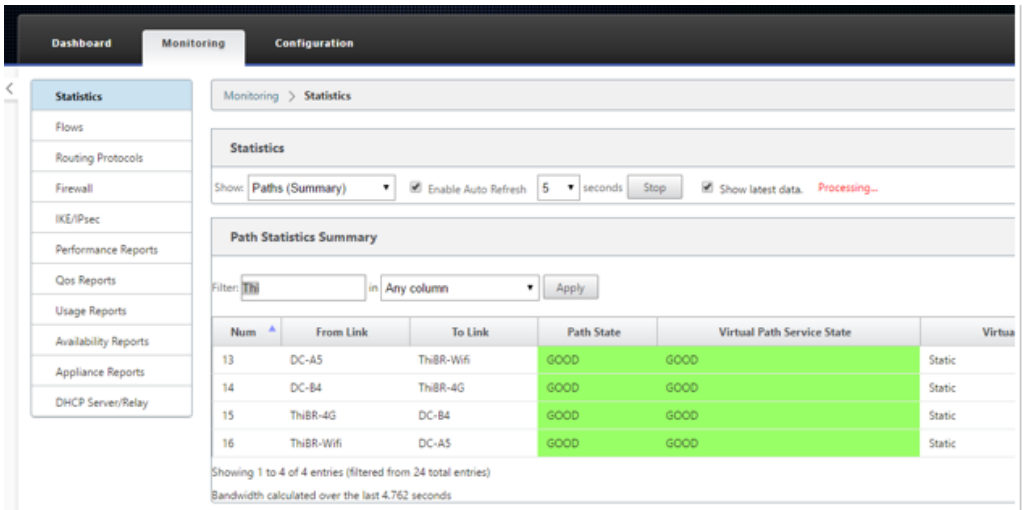
e) The Virtual Paths might not immediately show in a connected state because the MCN might not trust the configuration handed down from the zero-touch deployment Cloud Service, and reports "Configuration version mismatch"in the MCN Dashboard.



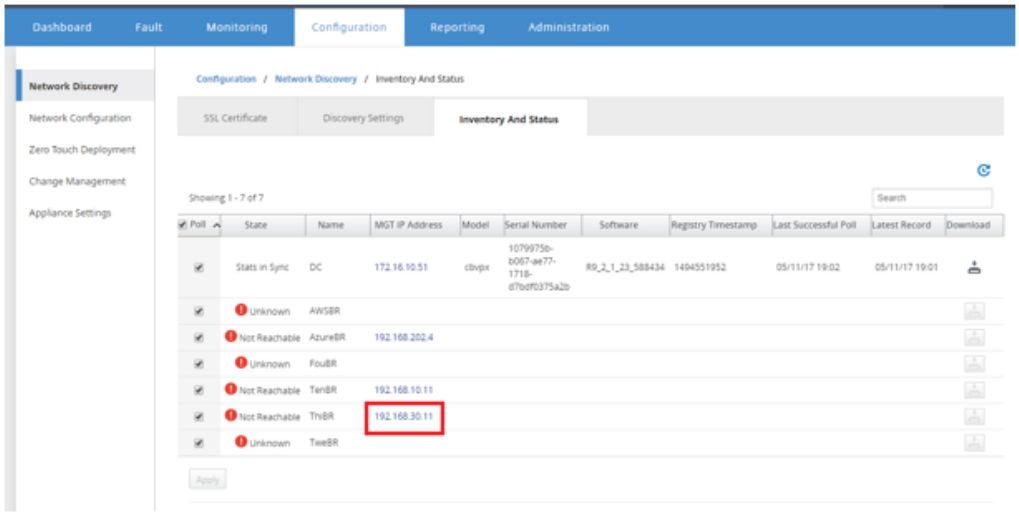
f) The configuration is redelivered to the newly installed branch office appliance and the status is monitored on the **MCN** > **Configuration** > **Virtual WAN** > **Change Management** page (this process can take several minutes to complete).



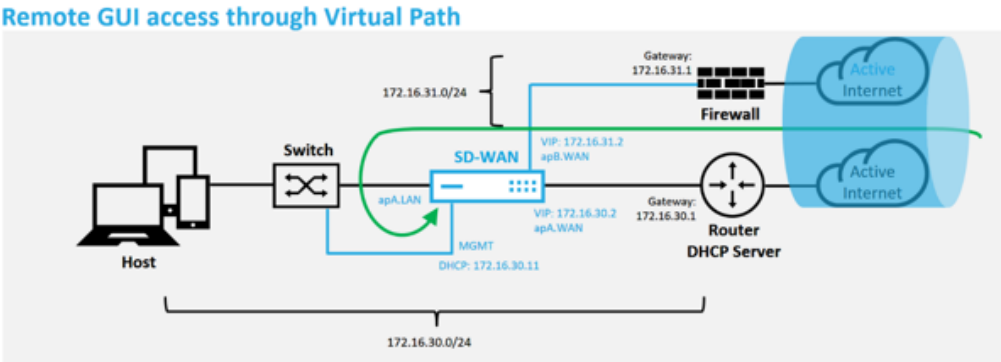
g) The SD-WAN Administrator can monitor the head-end MCN web management page for the established Virtual Paths of the remote site.



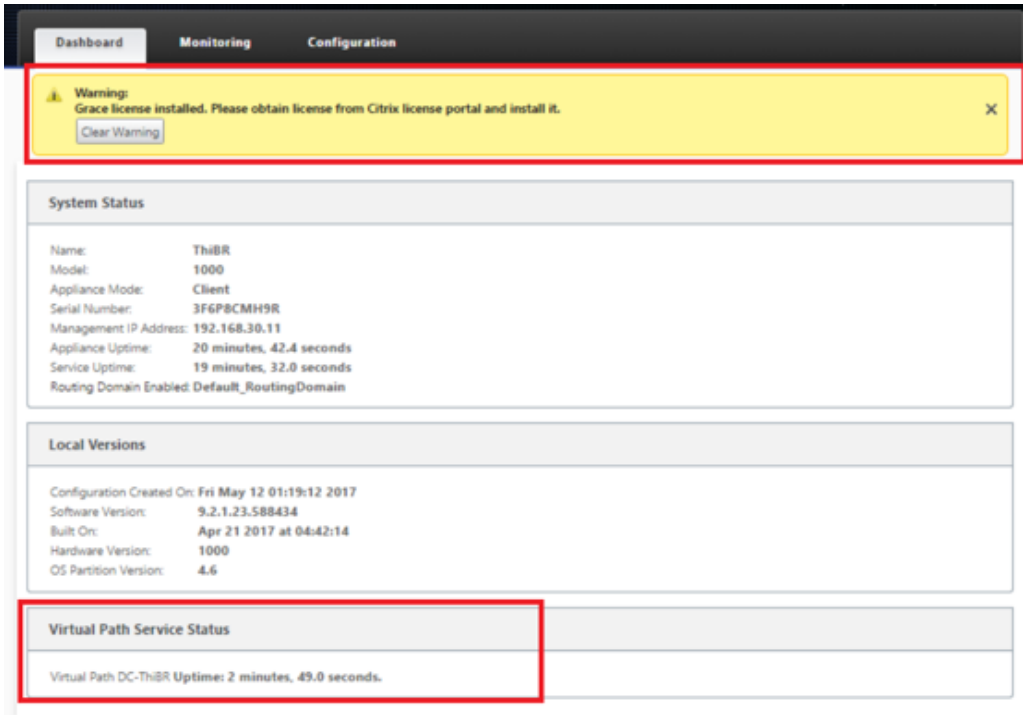
h) SD-WAN Center can also be used to identify the DHCP assigned IP address of the on-site appliance from the **Configuration** > **Network Discovery** > **Inventory and Status** page.



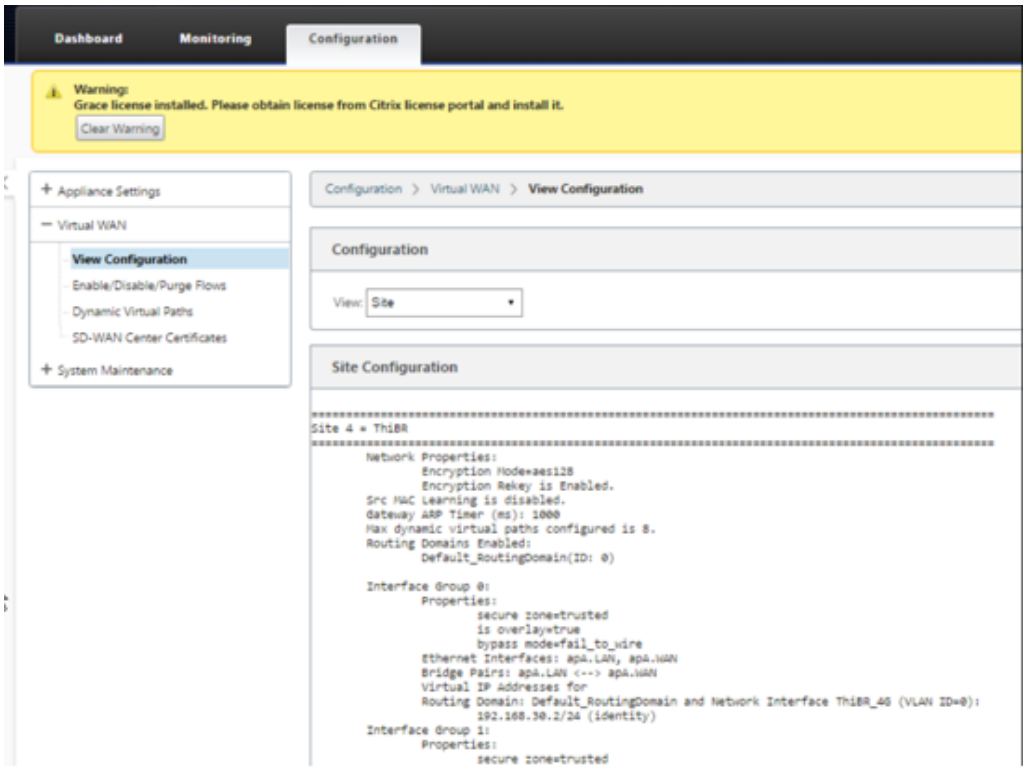
i) At this point the SD-WAN Network Administrator can gain web management access to the on-site appliance using the SD-WAN overlay network.



j) Web management access to the remote site appliance indicates that the appliance has been installed with a temporary Grace License at 10 Mbps, which enables the ability for the Virtual Path Service Status to report as active.

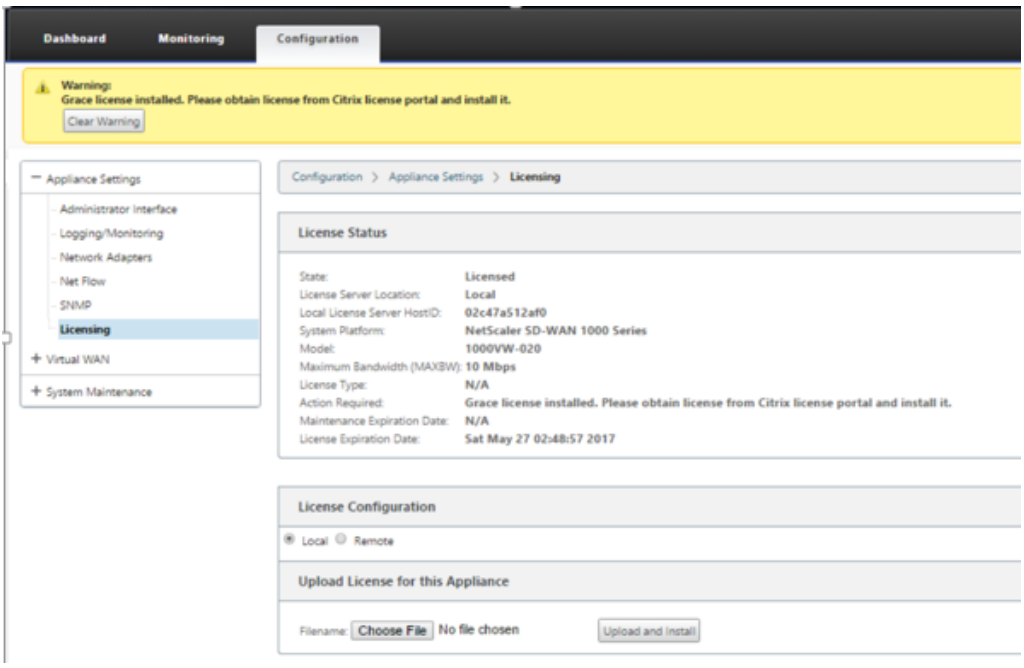


k) The appliance configuration can be validated using the **Configuration** > **Virtual WAN** > **View Configuration** page.



l) The appliance license file can be updated to a permanent license using the **Configu-**

ration > **Appliance Settings** > **Licensing** page.



After uploading and installing the permanent license file, the Grace License warning banner disappears and during the license install process no loss in connectivity to the remote site will occur (zero pings are dropped).

On-prem zero touch

March 12, 2021

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

March 12, 2021

The following sections describe how to deploy ZTD in an AWS environment.

Deploying in AWS:

With 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.

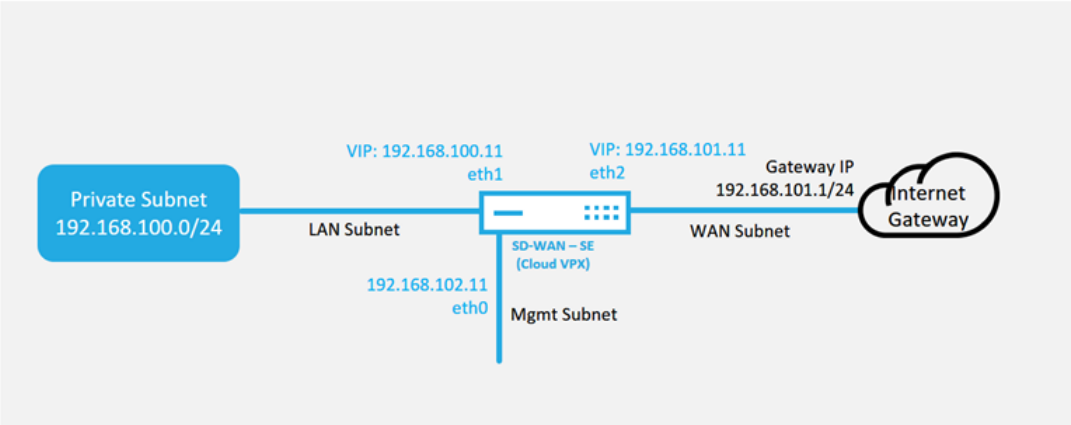
1. Update the configuration to add a new remote site with a ZTD capable SD-WAN cloud device using SD-WAN Center Network Configuration.

   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).

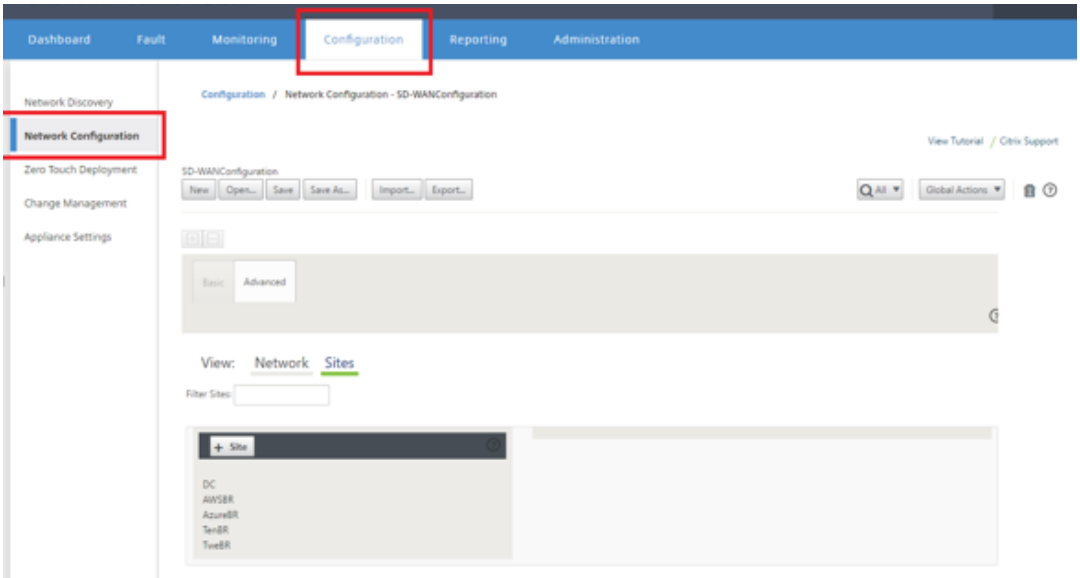
   > **Note**
   >
   > - Cloud deployed SD-WAN instances must be deployed in Edge/Gateway mode.
   > - The template for the cloud instance is limited to three interfaces; Management, LAN, and WAN (in that order).
   > - The available cloud templates for SD-WAN VPX are currently hard-set to obtain the #.#.#.#.11 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 Citrix 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.

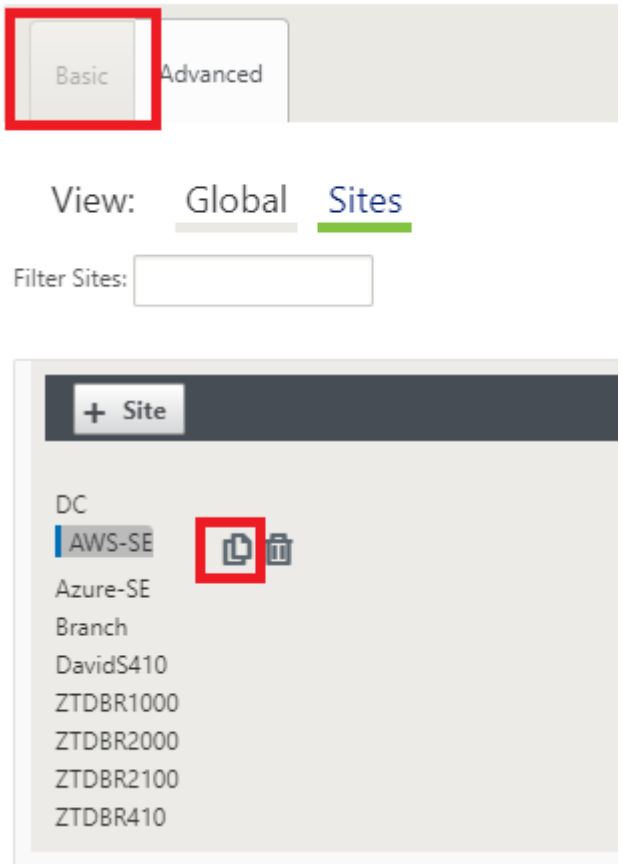


c) Make sure a working configuration is already in place, or import the configuration from the MCN.

d) Navigate to the Basic tab to create a new site.

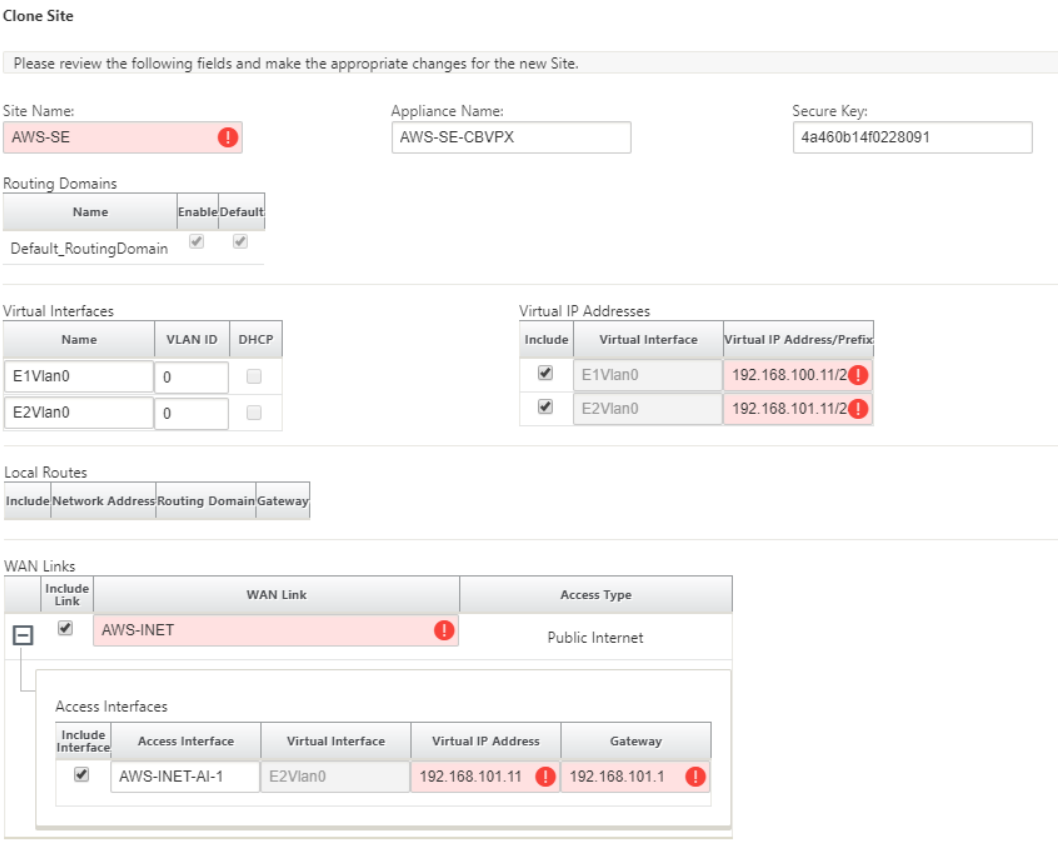
e) Open the Sites tile to display the currently configured sites.

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.

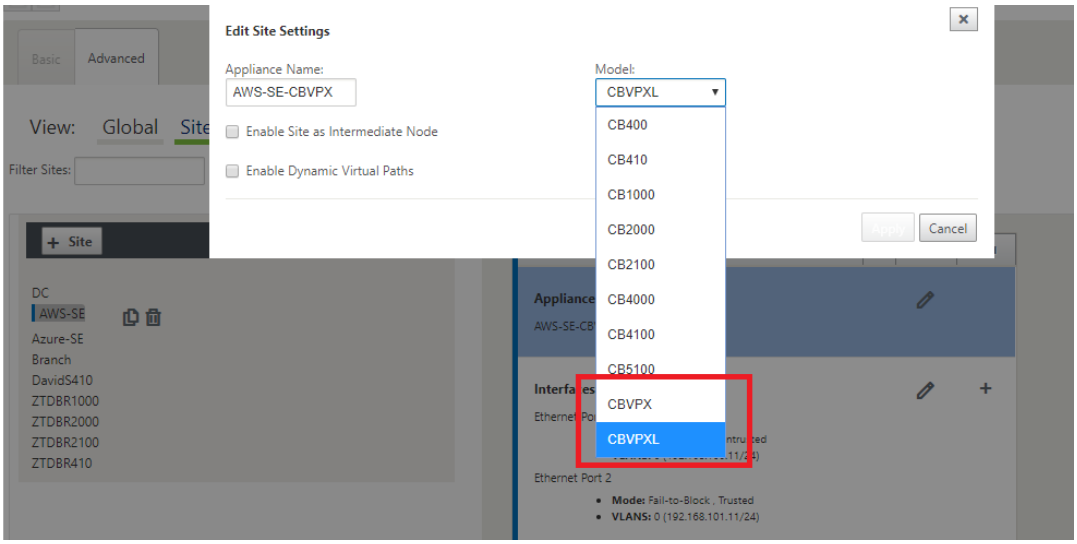


g) Populate all the required fields from the topology designed earlier for this new cloud site

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.



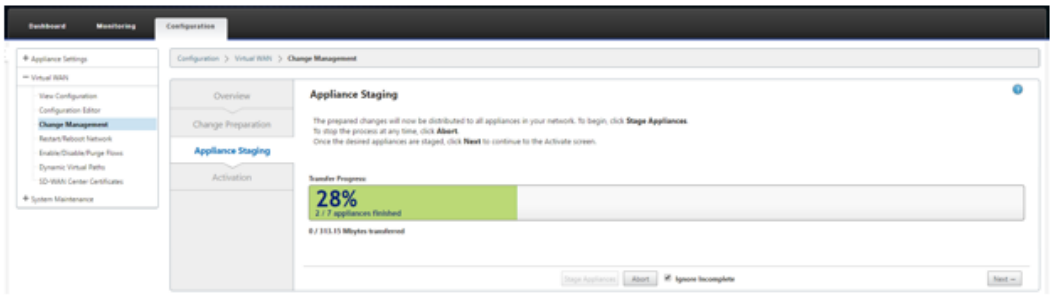
h) After cloning a new site, navigate to the site's **Basic Settings**, and verify that the Model of SD-WAN is correctly selected which would support the zero touch service.



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

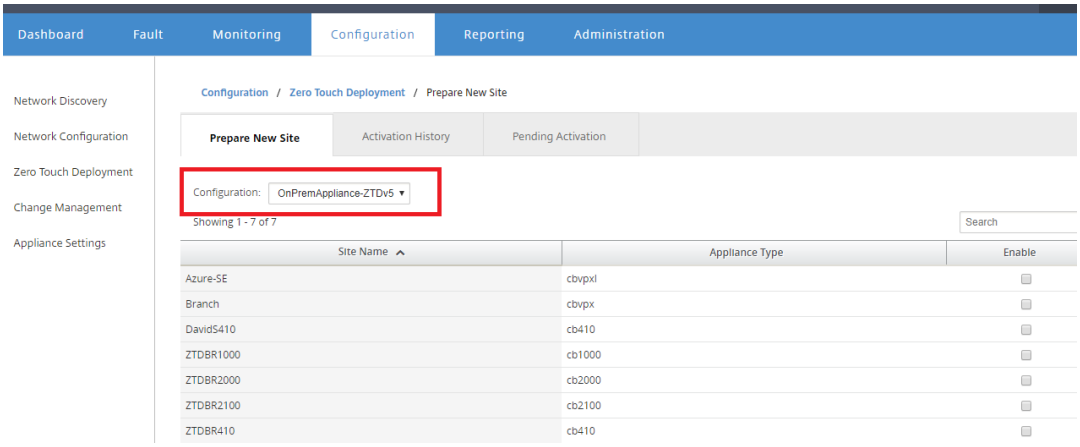
makes the existing SD-WAN devices aware of the new site to be deployed via zero touch, you will need to utilize the *Ignore Incomplete* option to skip attempting to push the configuration to the new site that still needs to go through the ZTD workflow.



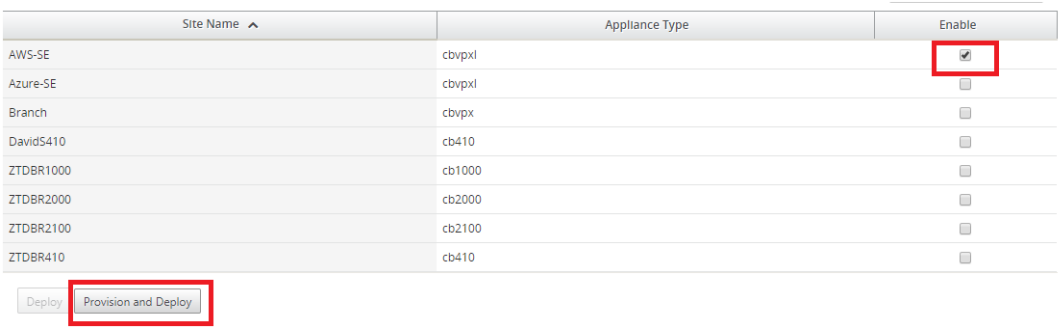
2. Navigate back to the SD-WAN Center Zero Touch Deployment page, and with the new active configuration running, the new site will be available for deployment.

   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 Citrix SD-WAN devices that are supported for zero touch will be displayed.

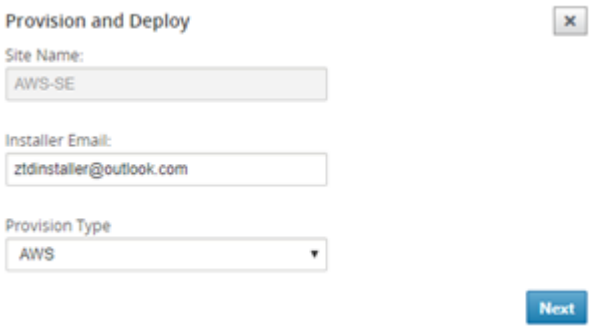


   c) Select the target cloud site you want to deploy using the Zero Touch service, click **Enable**, and then **Provision and Deploy**.

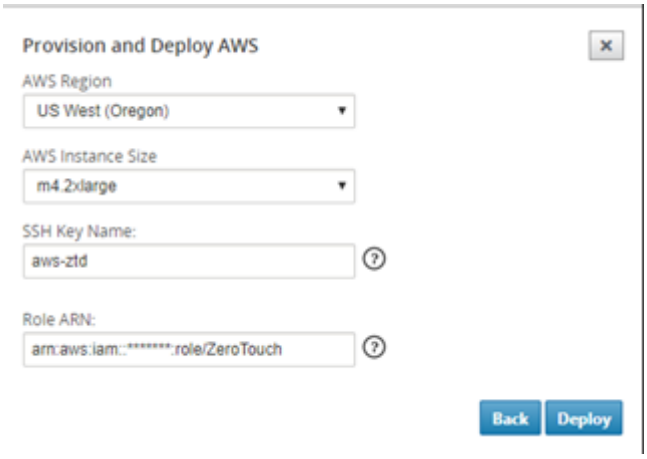


d) A pop-up window will appear, where the Citrix SD-WAN Admin can initiate the deployment for Zero Touch.

Populate an email address where the activation URL can be delivered, and select the **Provision Type** for the desired Cloud.



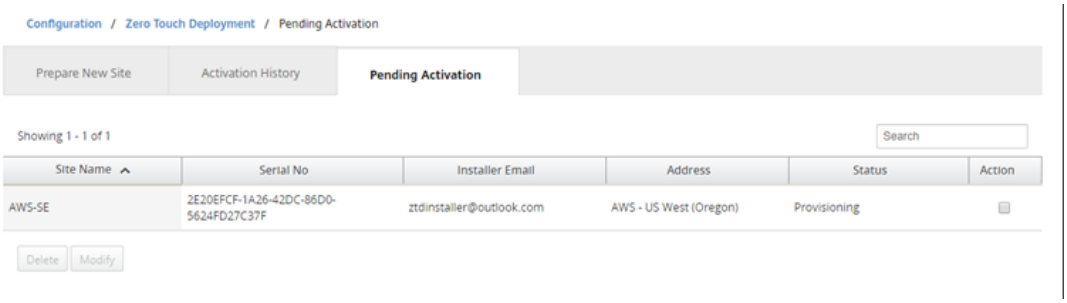
e) After clicking **Next**, Select the appropriate Region, Instance size, populate the SSH Key name and Role ARN fields appropriately.



> **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.

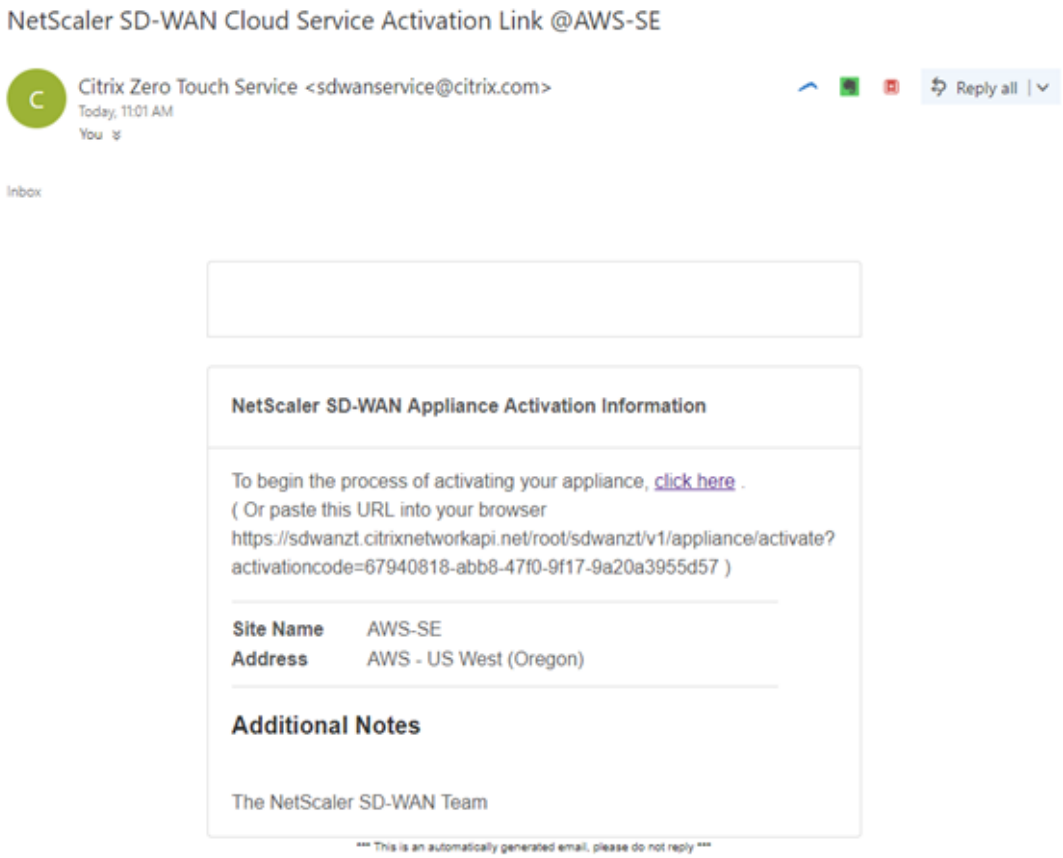
f) Click **Deploy**, triggering the SD-WAN Center, which was previously registered with the ZTD Cloud Service, to share the configuration of this site to be temporality stored in the ZTD Cloud Service.

g) Navigate to the **Pending Activation** tab to confirm that the site information populated successfully and was put into a provisioning status.



3. Initiate the Zero Touch Deployment process as the Cloud Admin.

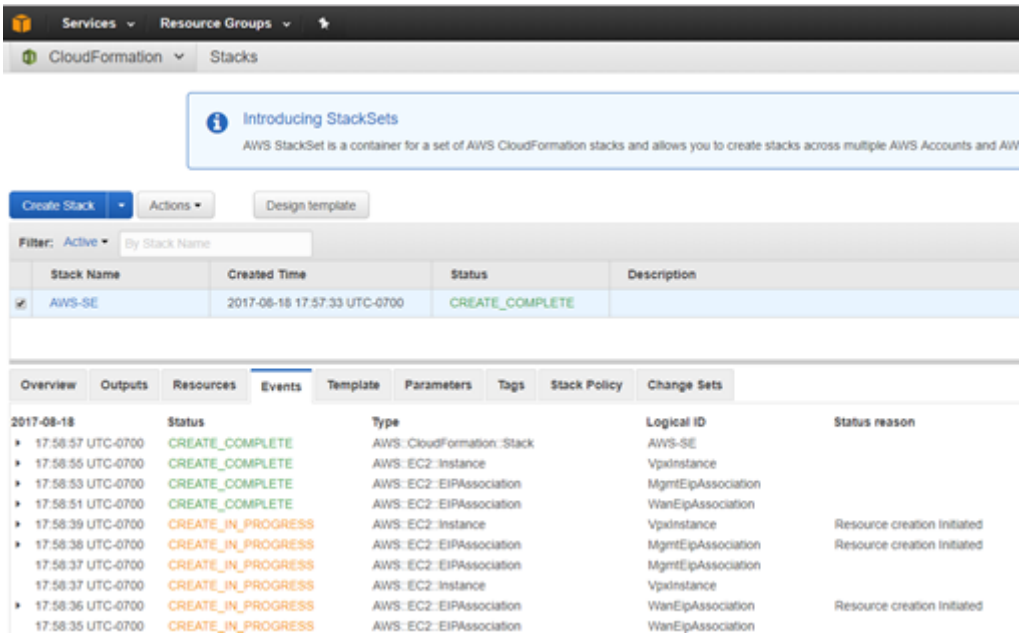
   a) The Installer will need to check the mailbox of the email address the SD-WAN Administrator used when deploying the site.



   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.

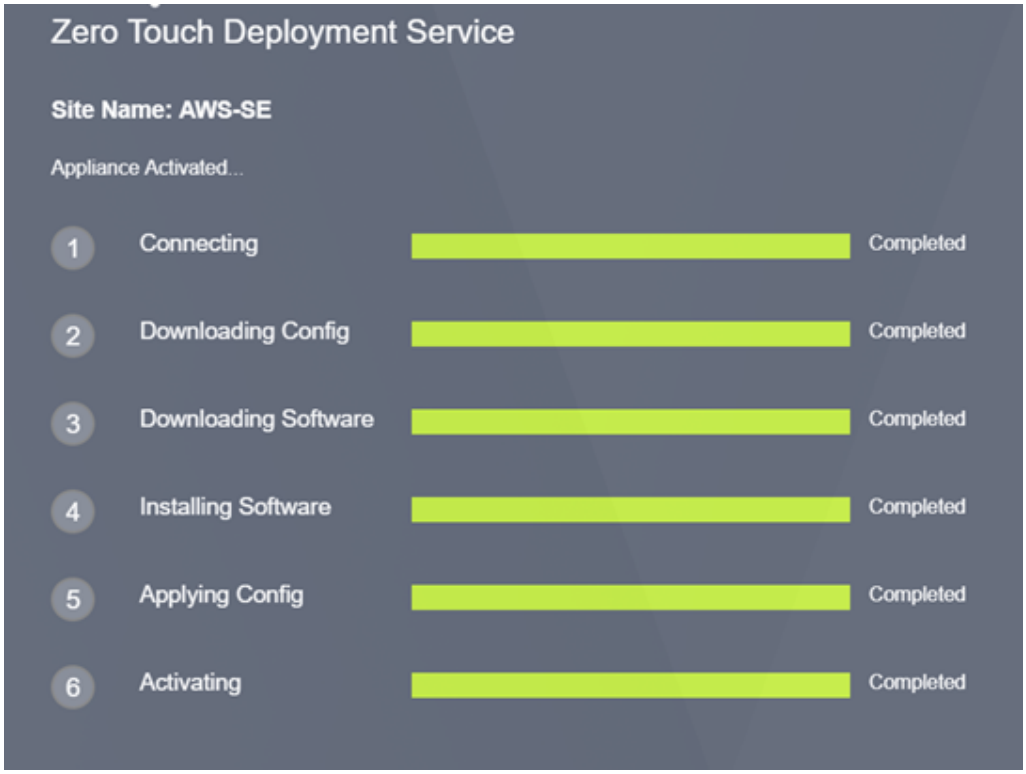


e) Allow the provisioning process ~8-10 minutes and activation another ~3-5 minutes to fully complete.

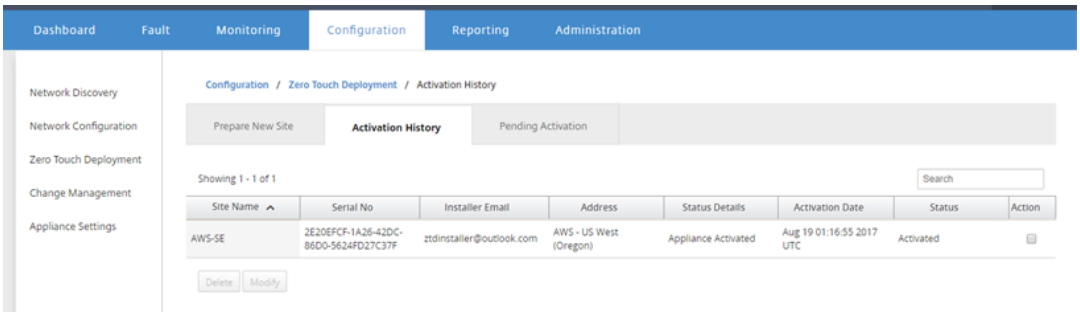
f) With successful connectivity of the SD-WAN cloud instance to the ZTD Cloud Service, the

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

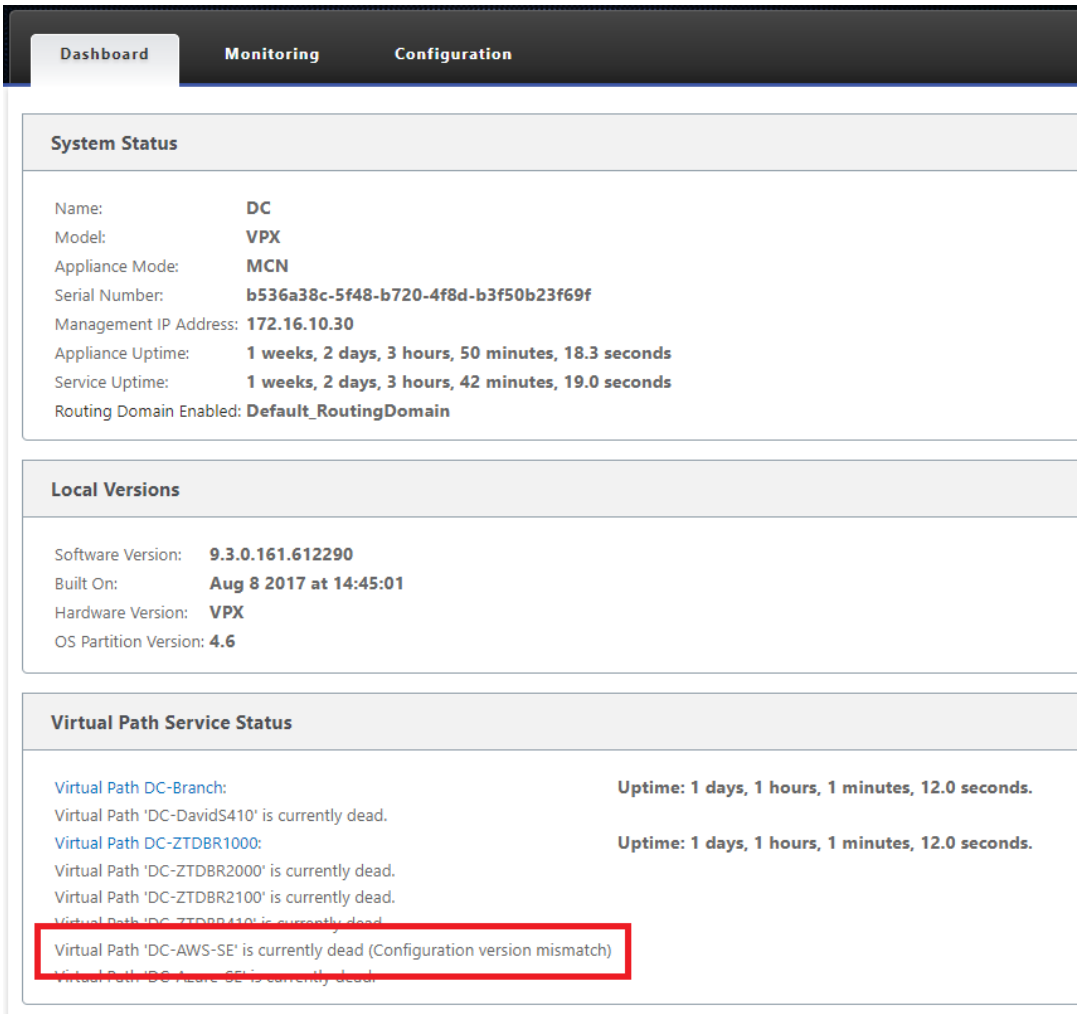


g) Further confirmation can be done in the SD-WAN Center web management interface; the Zero Touch Deployment menu will display successfully activated appliances in the **Activation History** tab.

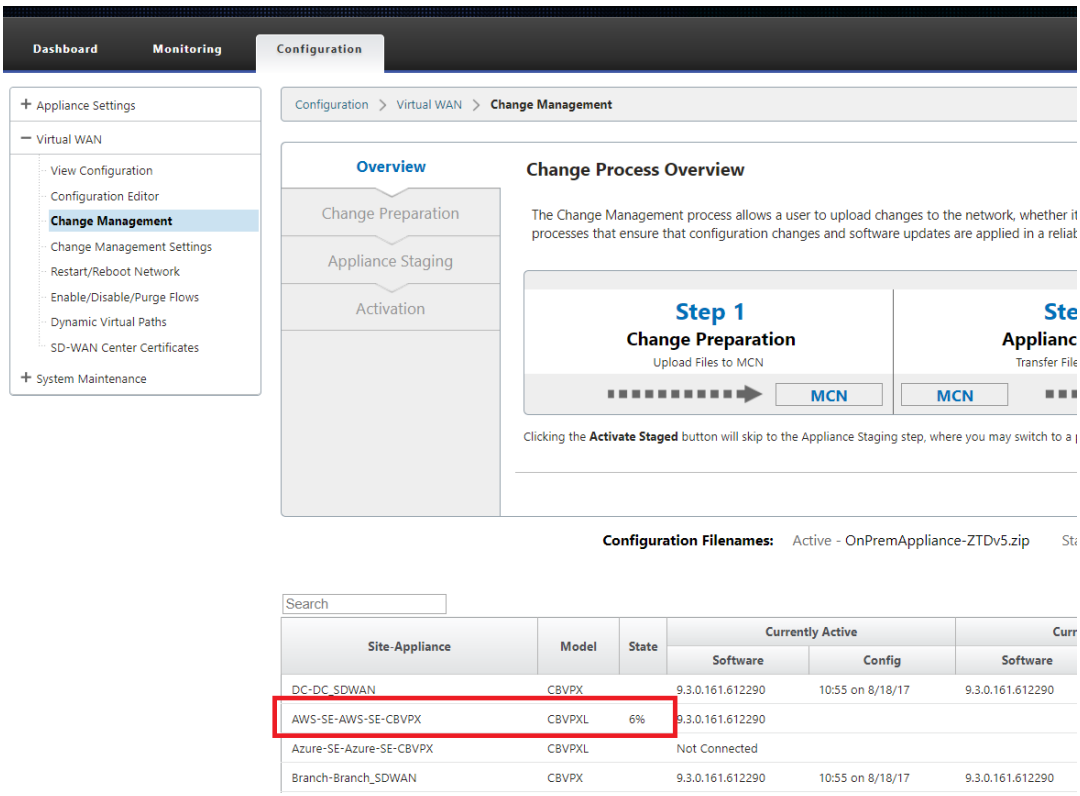


h) The Virtual Paths may not immediately show in a connected state, this is because the MCN

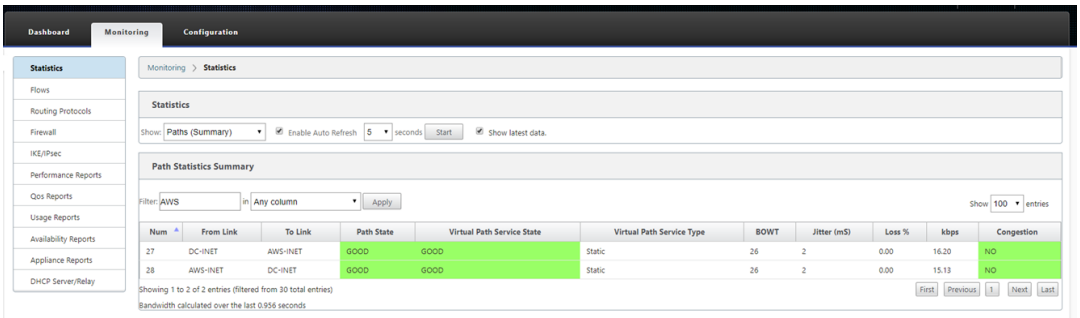
may not trust the configuration handed down from the ZTD Cloud Service, and will report *Configuration version mismatch* in the MCN Dashboard.



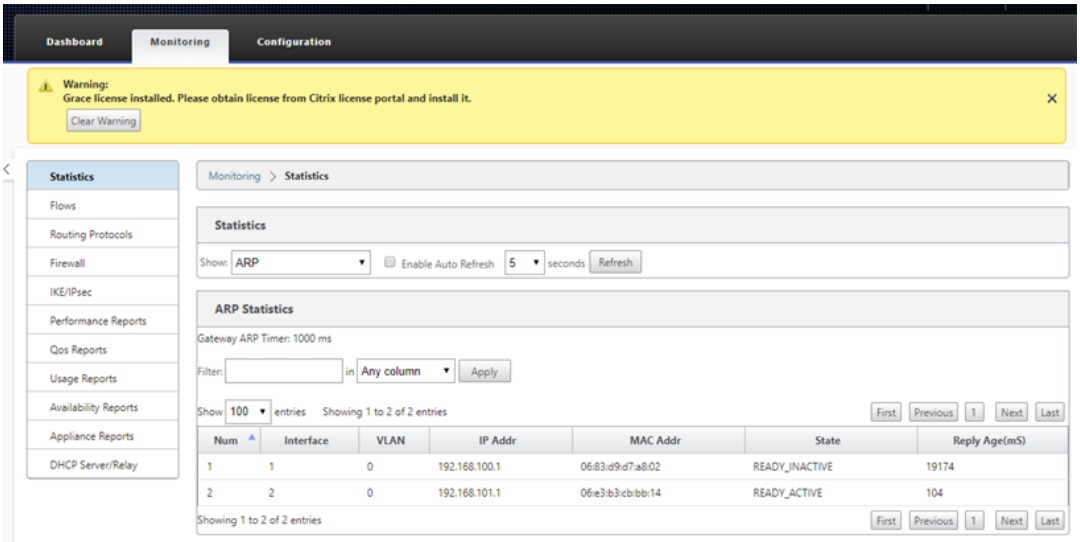
i) The configuration will automatically be redelivered to the newly installed branch office appliance, the status of this can be monitoring on the **MCN** > **Configuration** > **Virtual WAN** > **Change Management** page (depending on the connectivity, this process can take several minutes to complete).



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.



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.



Azure

March 15, 2021

The procedure to deploy zero touch deployment process for cloud instances is slightly different from appliance deployment for zero touch service.

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.

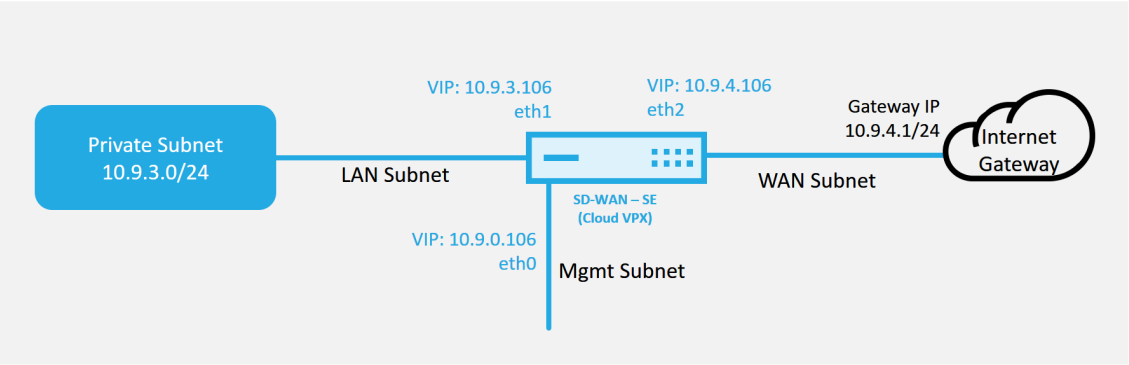
1. Design the new site for SD-WAN cloud deployment by first outlining the details of the new site (i.e. VPX size, Interface Groups usage, Virtual IP Addresses, WAN Link(s) with bandwidth and their respective Gateways).

> **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.

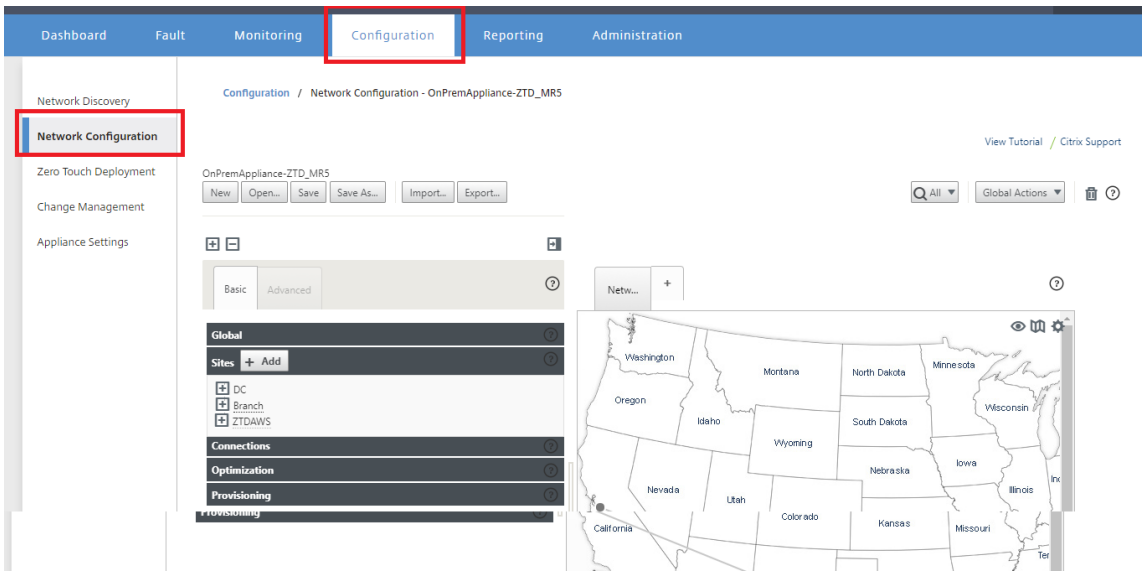
- The Azure site name in the configuration must be all lowercase with no special characters (e.g. ztdazure).

Azure Cloud Topology with NetScaler SD-WAN



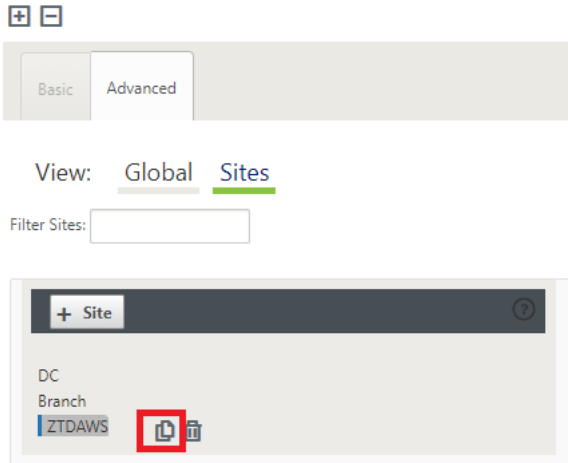
This is an example deployment of a SD-WAN cloud deployed site, the Citrix SD-WAN device is deployed as the edge device servicing a single Internet WAN link in this cloud network. Remote sites will be able to leverage multiple distinct Internet WAN links connecting into this same Internet Gateway for 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.

2. Open the SD-WAN Center web management interface and navigate to the **Configuration** > **Network Configuration** page.



3. Make sure a working configuration is already in place, or import the configuration from the MCN.

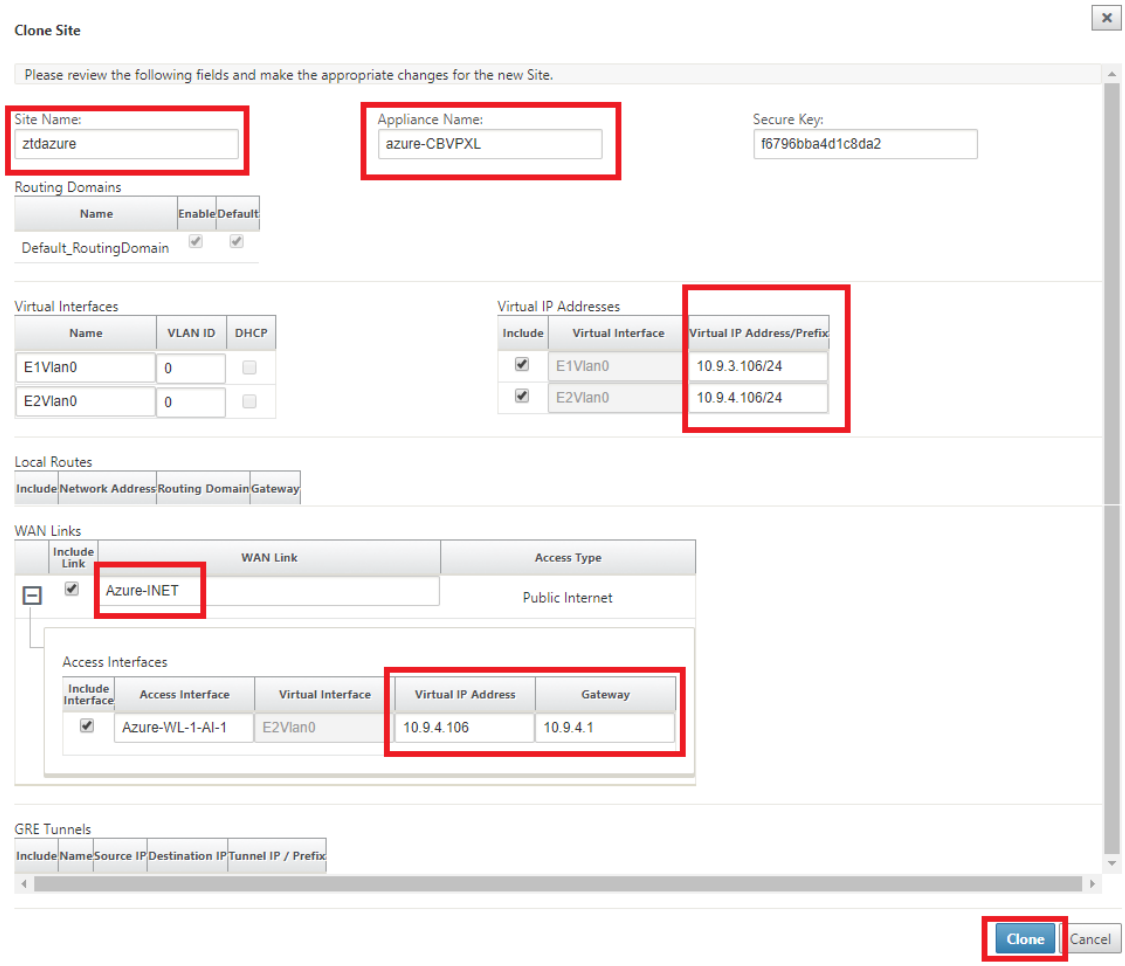
4. Navigate to the Basic tab to create a new site.
5. Open the Sites tile to display the currently configured sites.
6. Quickly built the configuration for the new cloud site by utilizing the clone feature of any existing site, or manually build a new site.



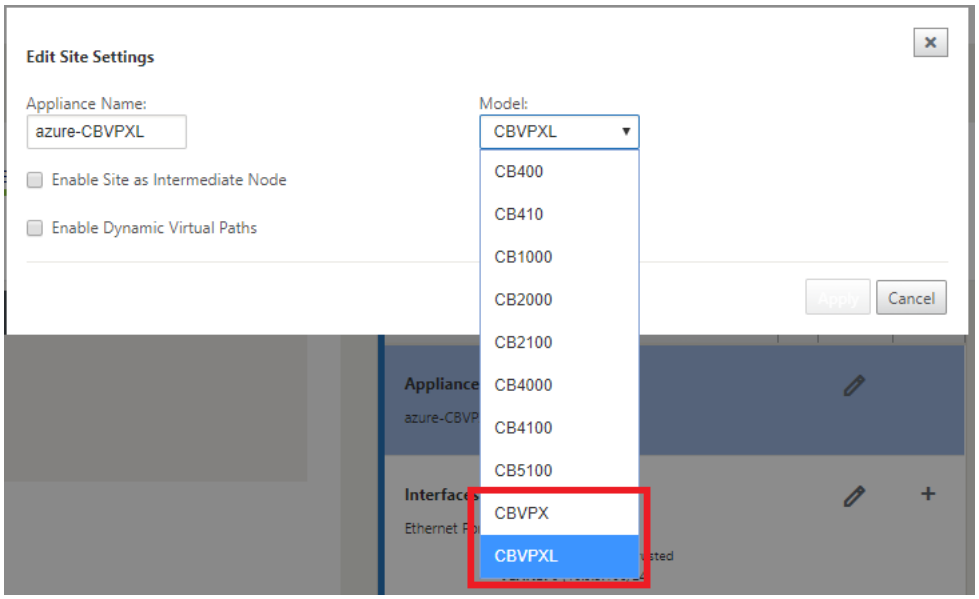
7. Populate all the required fields from the topology designed earlier for this new cloud site.

   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.

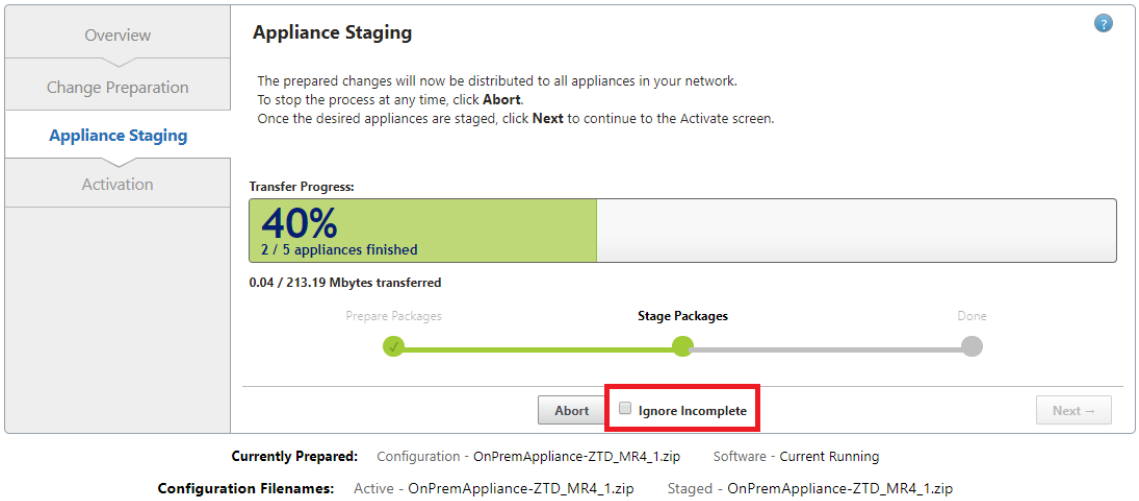
   It is import that the site name be compliant with what Azure expects. The site name must be in all lower case, at least 6 characters, with no special characters, it must confirm to the following regular expression **^[a-z][a-z0-9-]{1,61}[a-z0-9]$.**



8. 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.

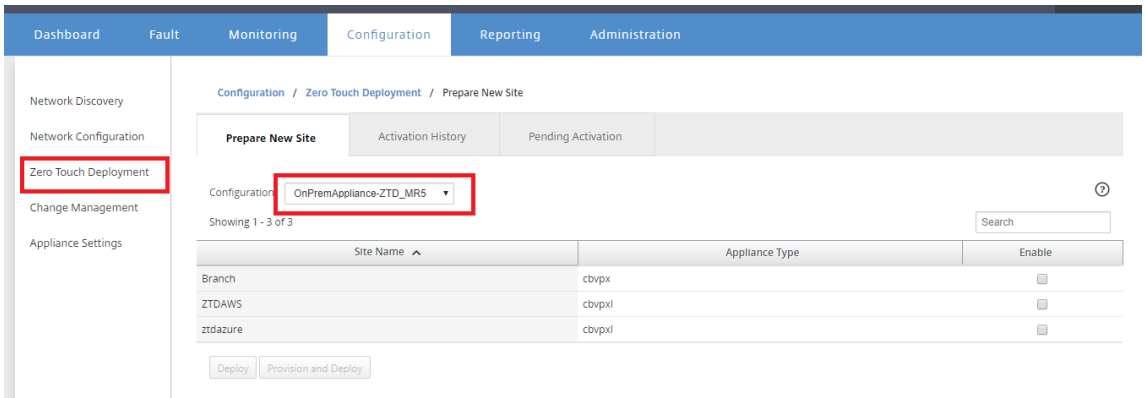


9. Save the new configuration on SD-WAN Center, and use the export to the **Change Management inbox** option to push the configuration using Change Management.
10. Follow the Change Management procedure to properly stage the new configuration, which makes the existing SD-WAN devices aware of the new 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.



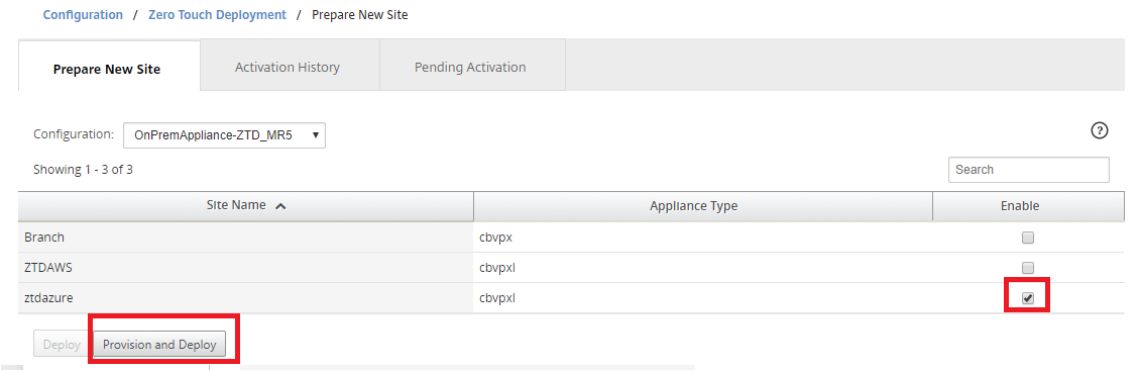
Navigate to the SD-WAN Center's Zero Touch Deployment page, and with the new active configuration running, the new site will be available for SD-WAN Center Provision and Deploy Azure (Step 1 of 2)

1. In the Zero Touch Deployment page, login with your Citrix account credentials. Under the **Deploy New Site** tab, select the running network configuration file.
2. After the running configuration file is selected, the list of all the branch sites with ZTD capable Citrix SD-WAN devices will be displayed.

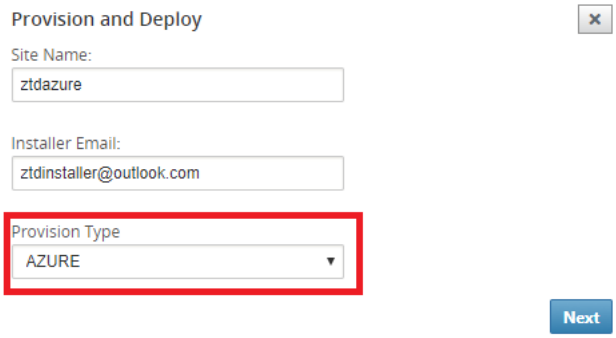


3. Select the target cloud site you want to deploy using the Zero Touch service, click **Enable**, and

then **Provision and Deploy**.

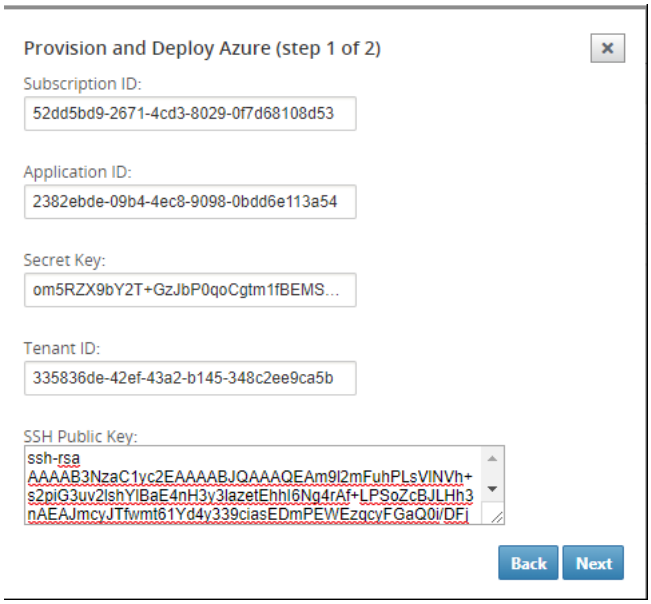


4. A pop-up window will appear, where the Citrix SD-WAN Admin can initiate the deployment for Zero Touch. Validate that the site name complys with the requirements on Azure (lowercase with no special characters). Populate an email address where the activation URL can be delivered, and select Azure as the **Provision Type** for the desired Cloud, before clicking **Next**.

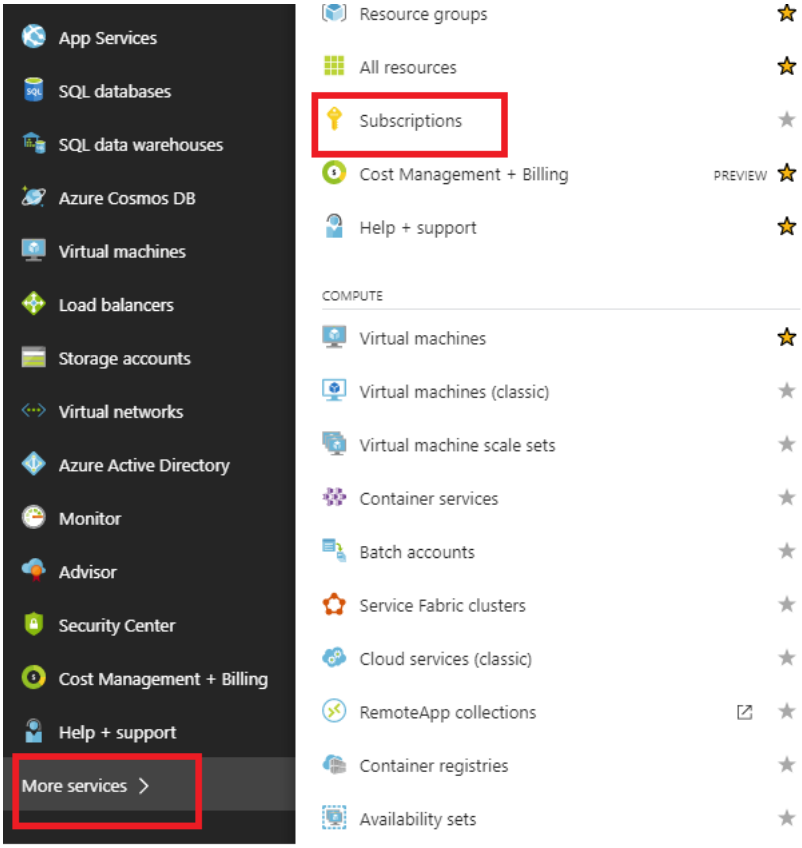


5. After clicking **Next**, the Provision and Deploy Azure (step 1of 2) window will require input of obtained from the Azure account.

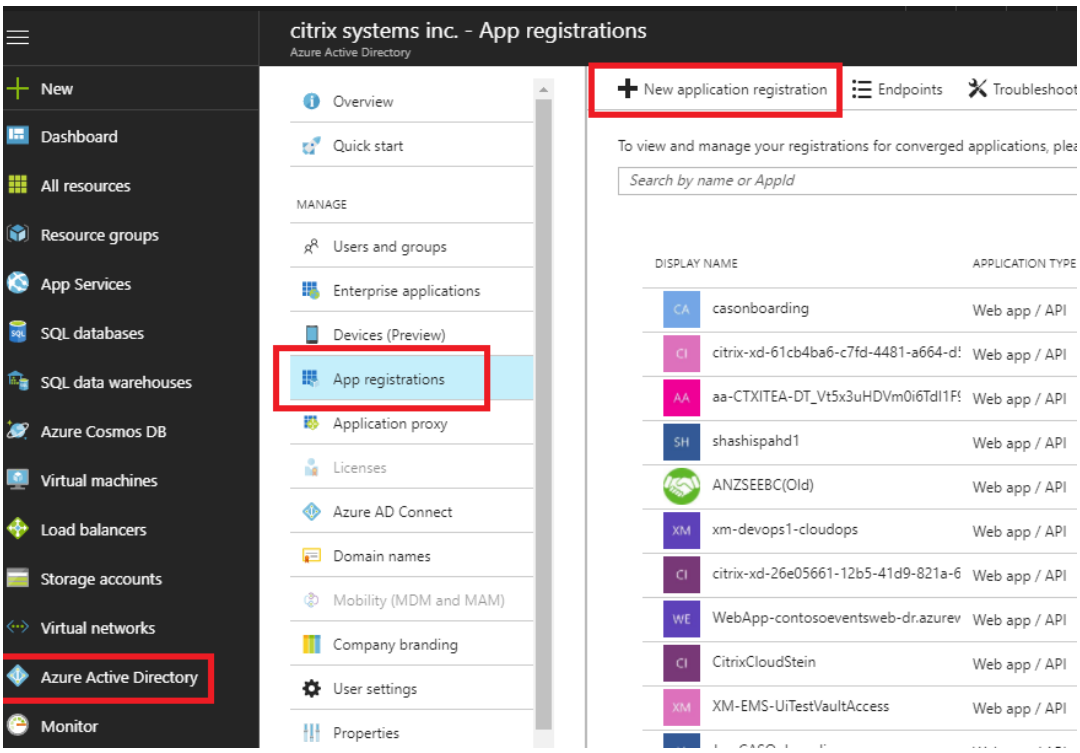
   Copy and paste each required field after obtaining the information from your Azure account. The steps below outline how to obtain the required Subscription ID, Application ID, Secret Key, and Tenant ID from your Azure account, then proceed by clicking **Next**.



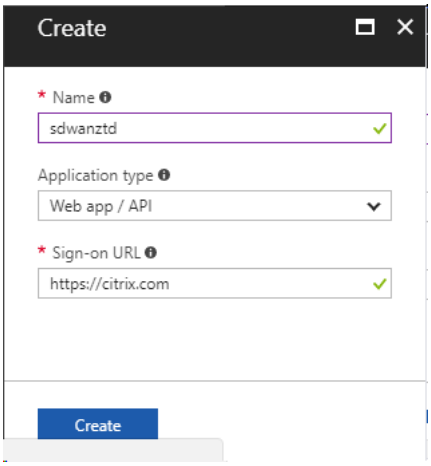
a) On the Azure account, we can identify the required **Subscription ID** by navigating to "More Services"and select **Subscriptions.**



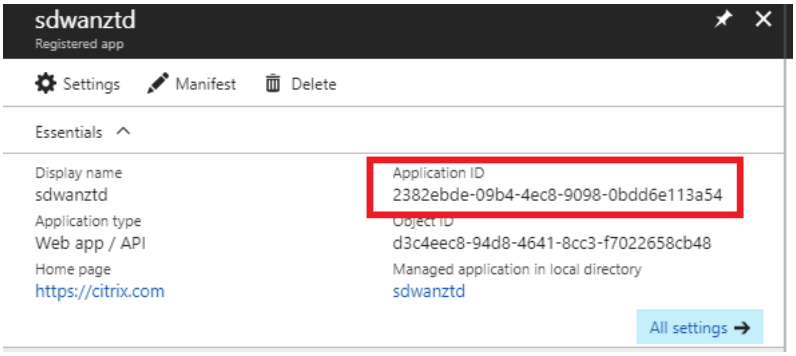
b) To identify the required ***Application ID**, navigate to Azure Active Directory, Application registrations, and click **New application registration.**



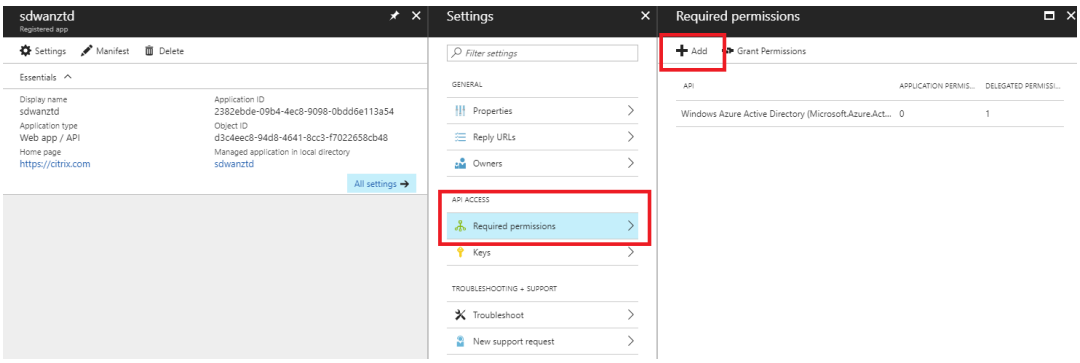
c) In the app registration create menu, enter a Name and a Sign-on URL (this can be any URL, the only requirement is that it must be valid), then click **Create**.



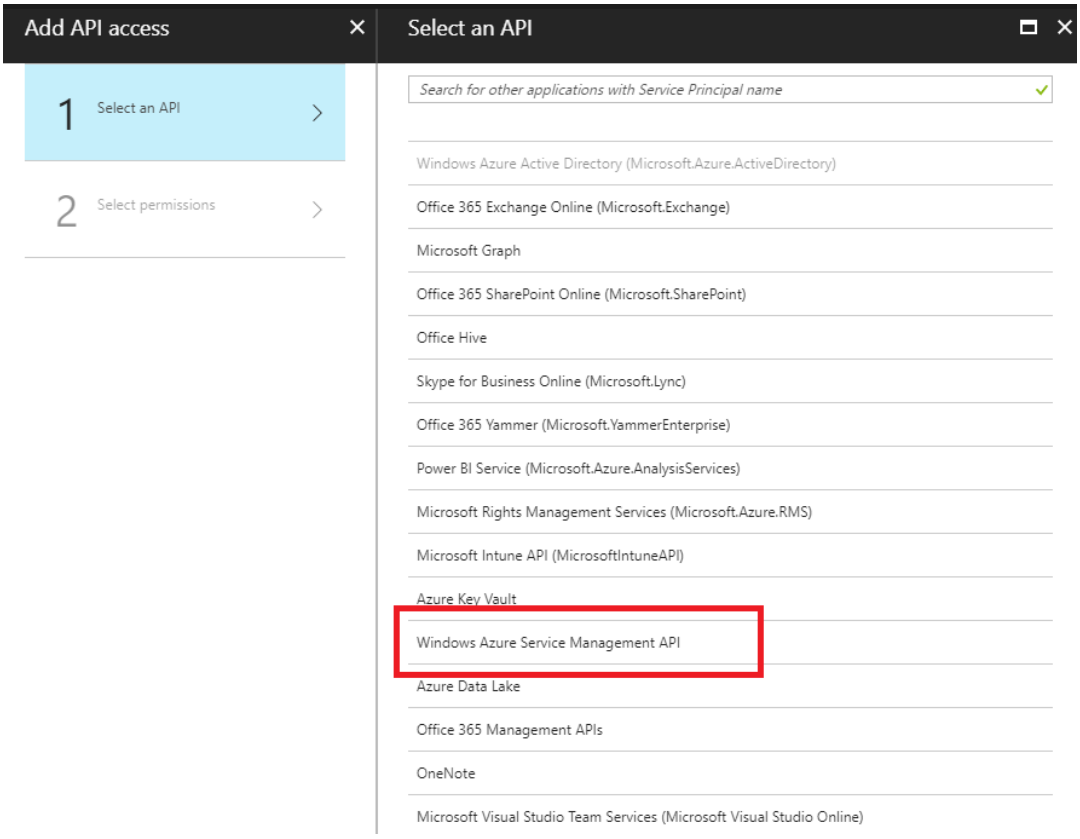
d) Search for and open the newly created Registered App, and note the Application ID.



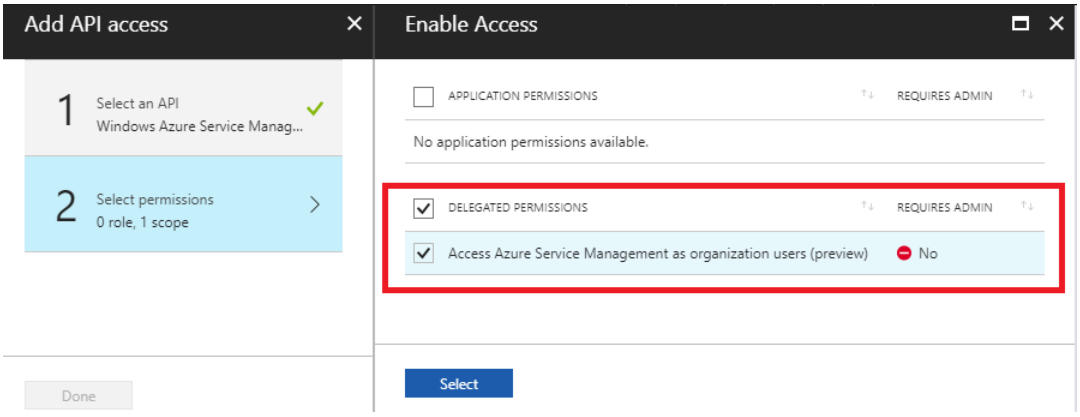
e) Again open the newly created Registration App, and to identify the required *Security Key*, under API Access, select **Required permissions,** to allow a third party to provision and instance. Then select **Add**.



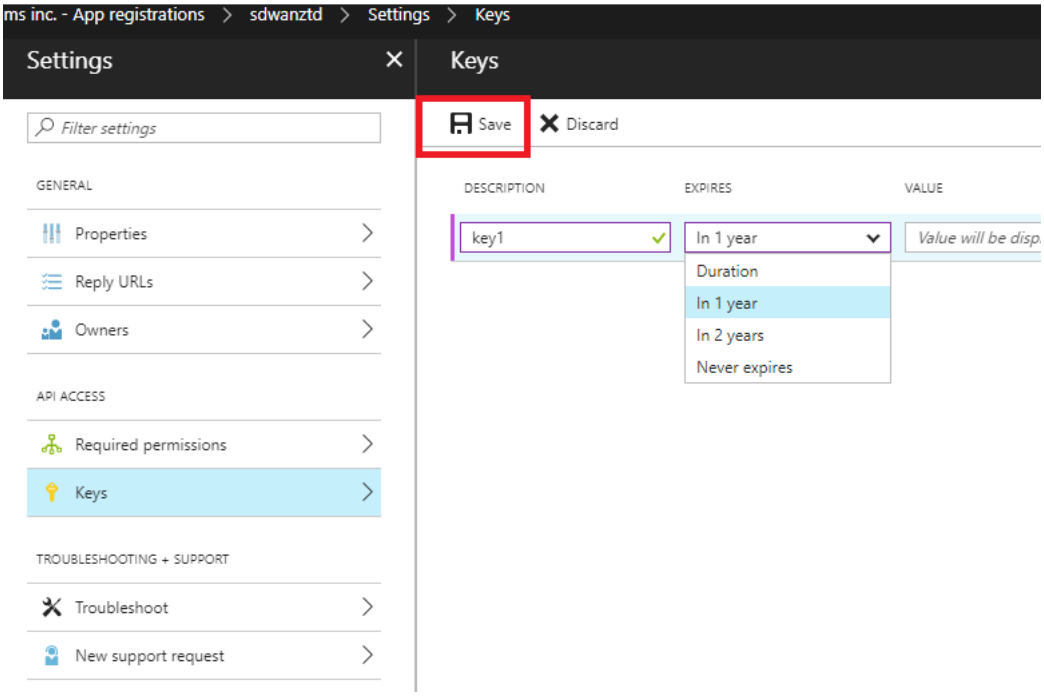
f) When adding the Required permissions, **Select an API,** then highlight **Windows Azure Service Management API.**



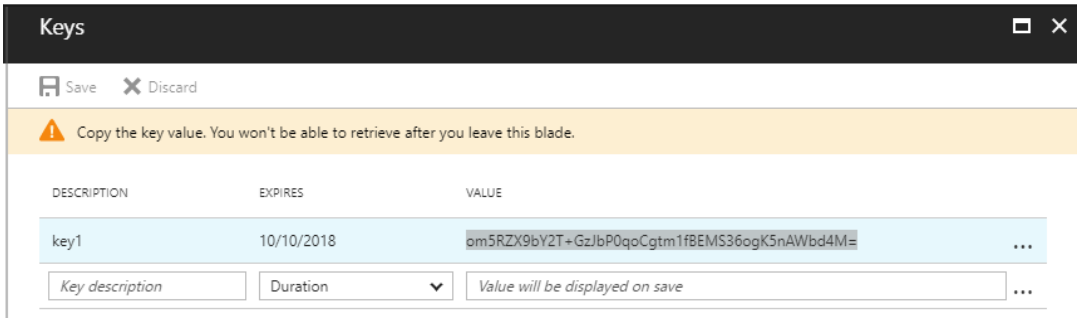
g) Enable **Delegate Permissions** to provision instances, then click **Select** and **Done**.



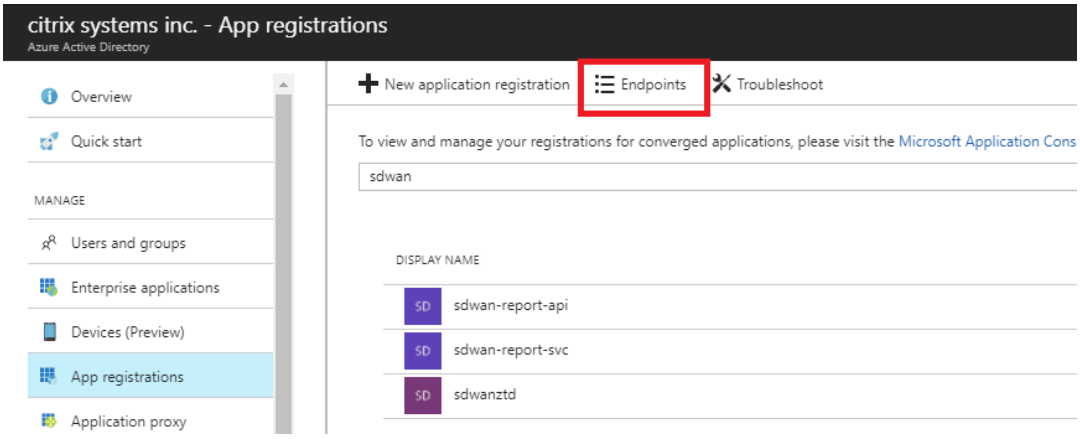
h) For this Registered App, under API Access, select **Keys,** and create a secret **key description** and the desired **duration** for the key to be valid. Then click **Save** which will produce a **secret key** (the key is only required for the provisioning process, it can be deleted after the instance is made available).



i) Copy and save the secret key (note you will not be able to retrieve this later).

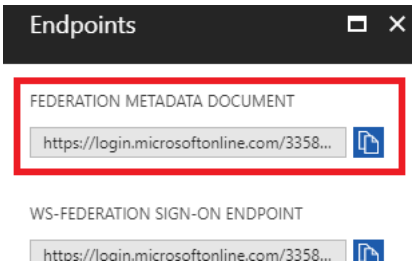


j) To identify the required ***Tenant ID***, navigate back to the App registration pane, and select **Endpoints**.

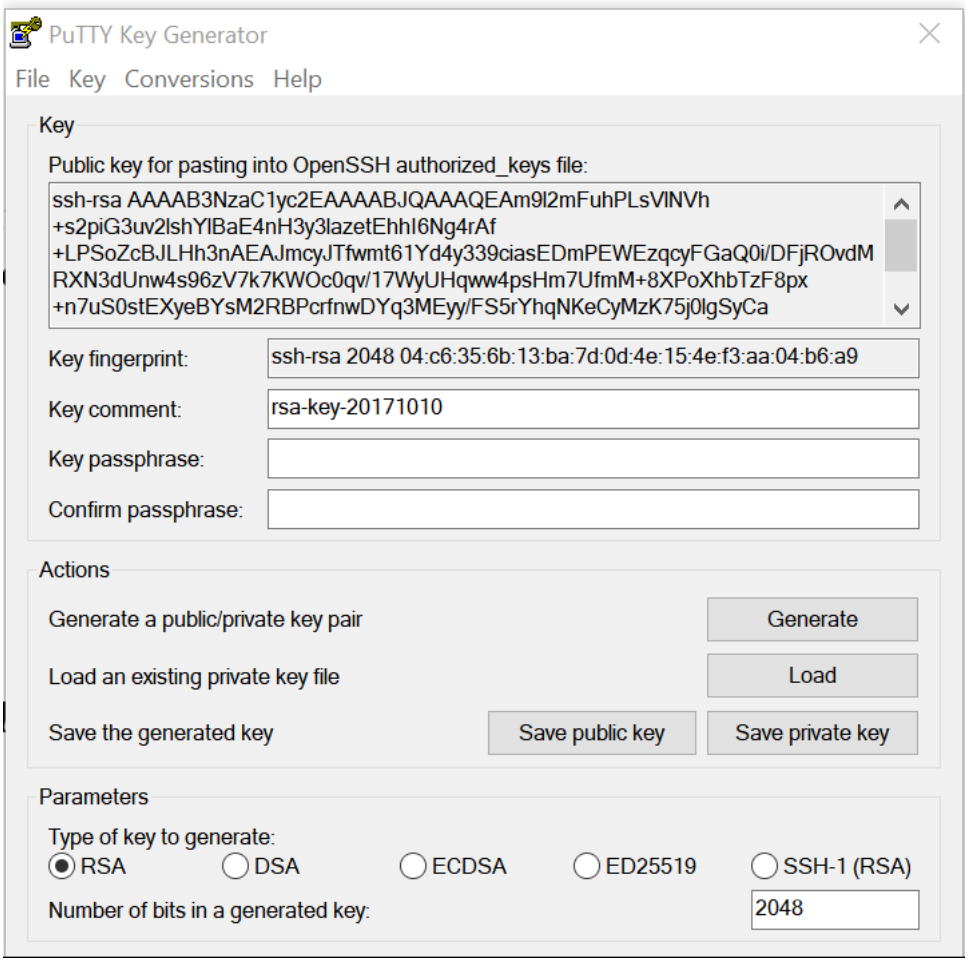


k) Copy the **Federation Metadata Document**, to identify your Tenant ID (note the Tenant ID

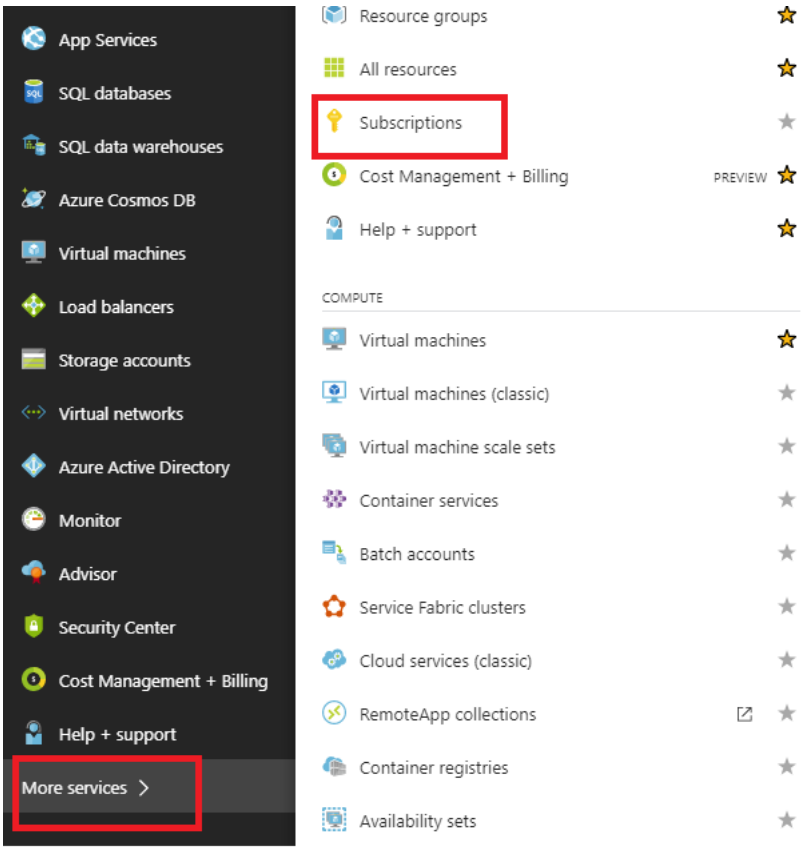
is 36-character string located between the `online.com/` and the `/federation` in the URL).



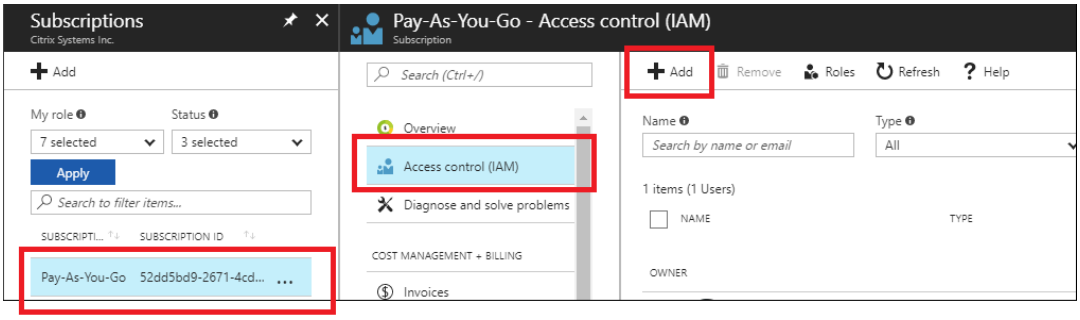
l) The last item required is the ***SSH Public Key***. This can be created using Putty Key Generator or ssh-keygen and will be utilized for authentication, eliminating the need for passwords to log in. The SSH public key can be copied (including the heading ssh-rsa and trailing rsa-key strings). This public key will be shared through SD-WAN Center input to the Citrix Zero Touch Deployment Service.



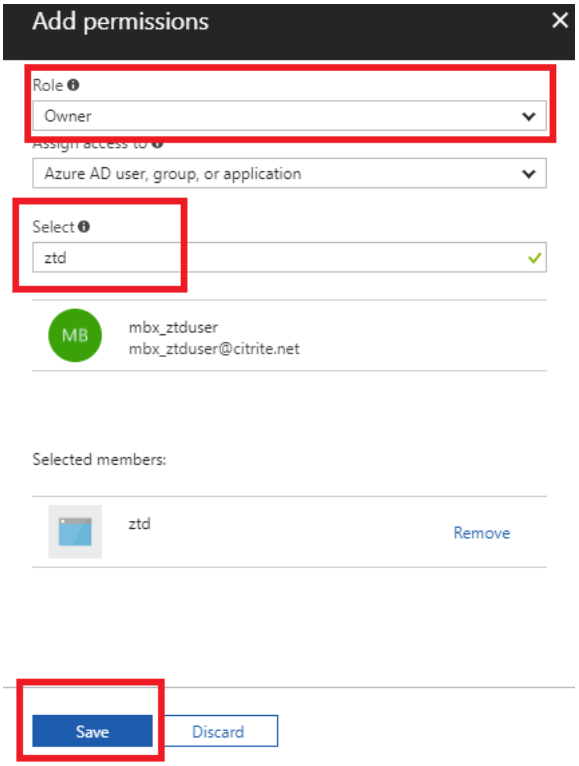
m) Additional steps are required to assign the application a role. Navigate back to More Services, then Subscriptions.



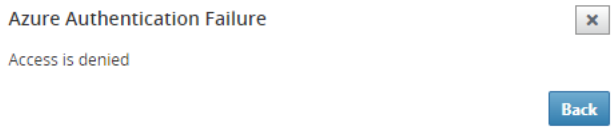
n) Select the active subscription, then **Access control (AIM)**, next click **Add.**



o) 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**.

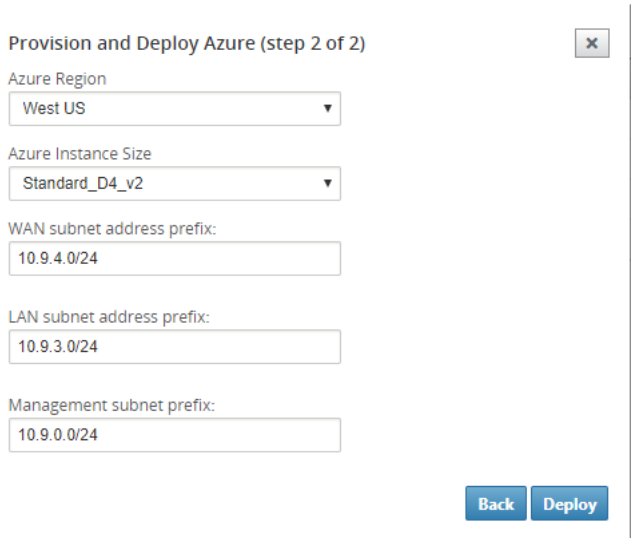


p) After collecting the required inputs and entering them into SD-WAN Center, click **Next**. If the inputs are not correct, you will encounter an authentication failure.

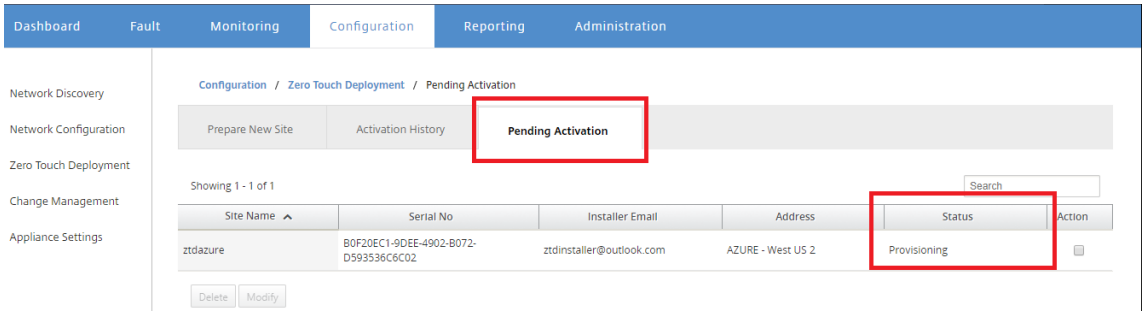


SD-WAN center provision and deploy Azure (Step 2 of 2)

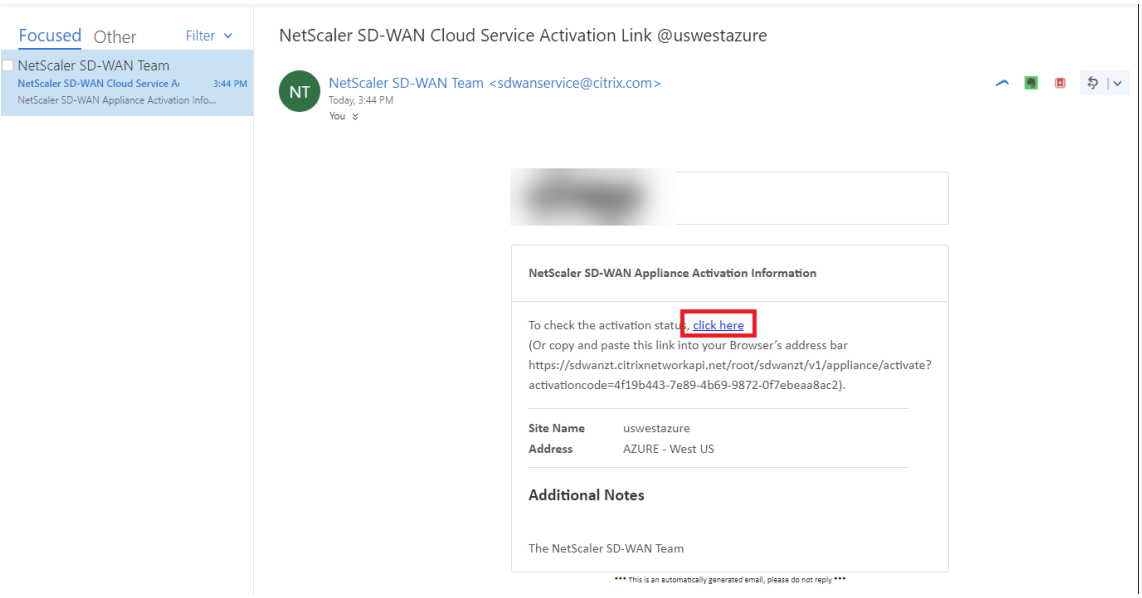
1. Once the Azure authentication is successful, populate the appropriate fields to select the desired Azure Region, and the appropriate Instance Size, then click **Deploy**.



2. Navigating to the **Pending Activation** tab in SD-WAN Center, will help track the current status of the deployment.

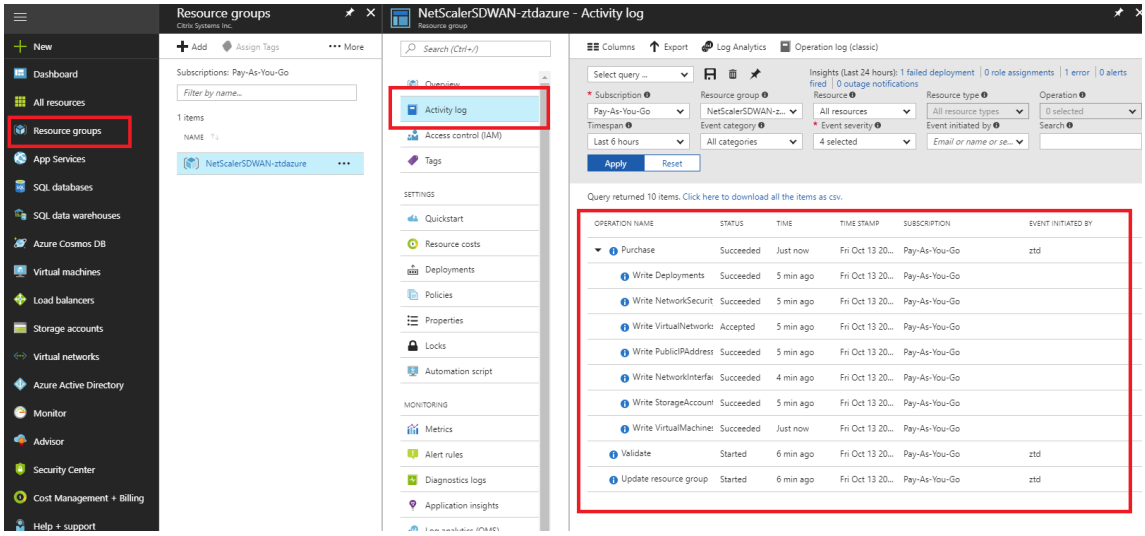


3. An email with an activation code will be delivered to the email address inputted in step 1, obtain the email and open the **activation URL** to trigger the process and check the activation status.

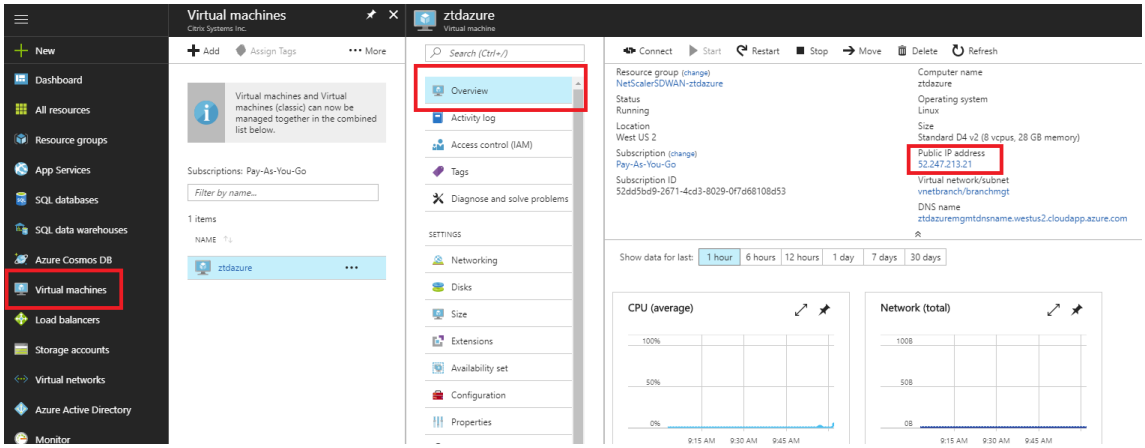


4. An email with an activation URL will be delivered to the email address inputted in step 1. Obtain the email and open the **activation URL** to trigger the process and check the activation status.

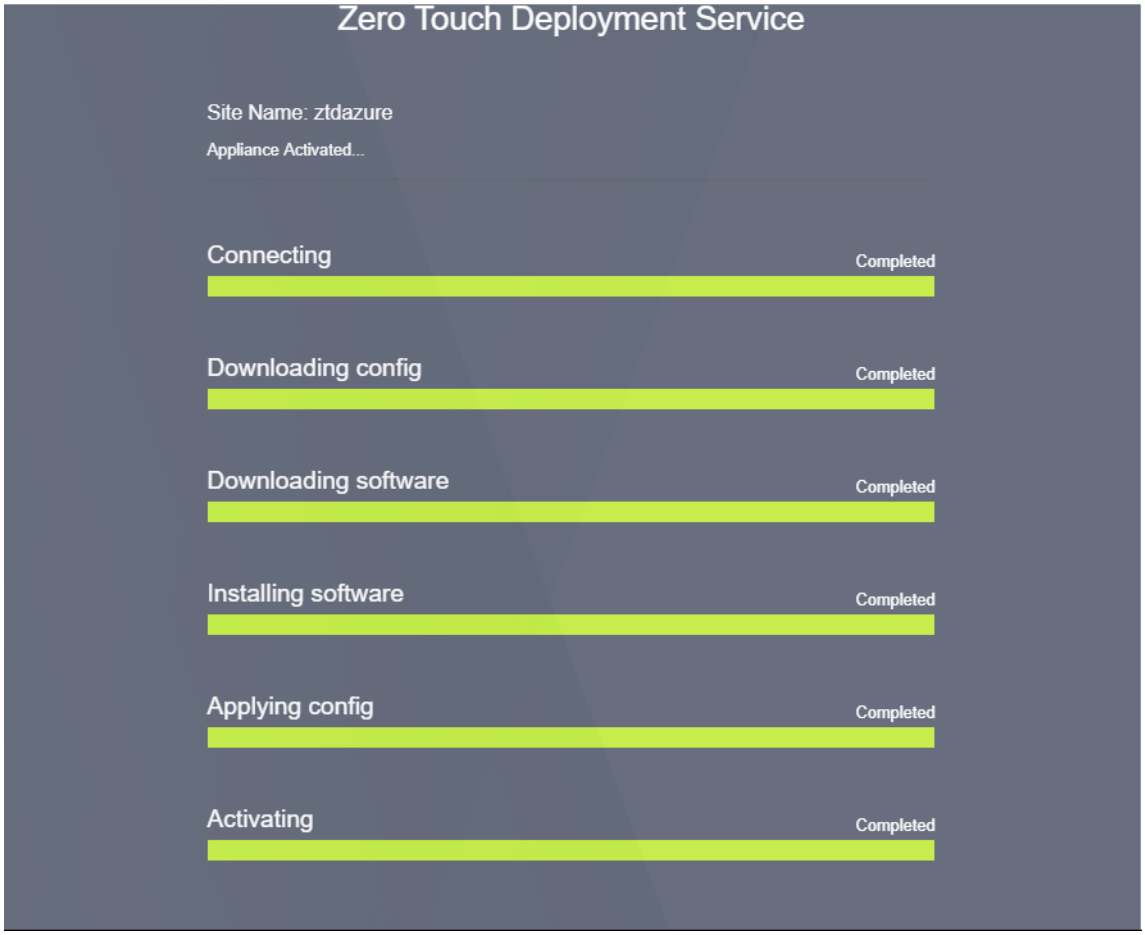
5. It will take a few minutes for the instance to be provisioned by the SD-WAN Cloud Service. You can monitor the activity on the Azure portal, under **Activity log** for the **Resource Group** which is automatically created. Any issues or errors with the provisioning will be populated here, as well as replicated to SD-WAN Center in the Activation Status.



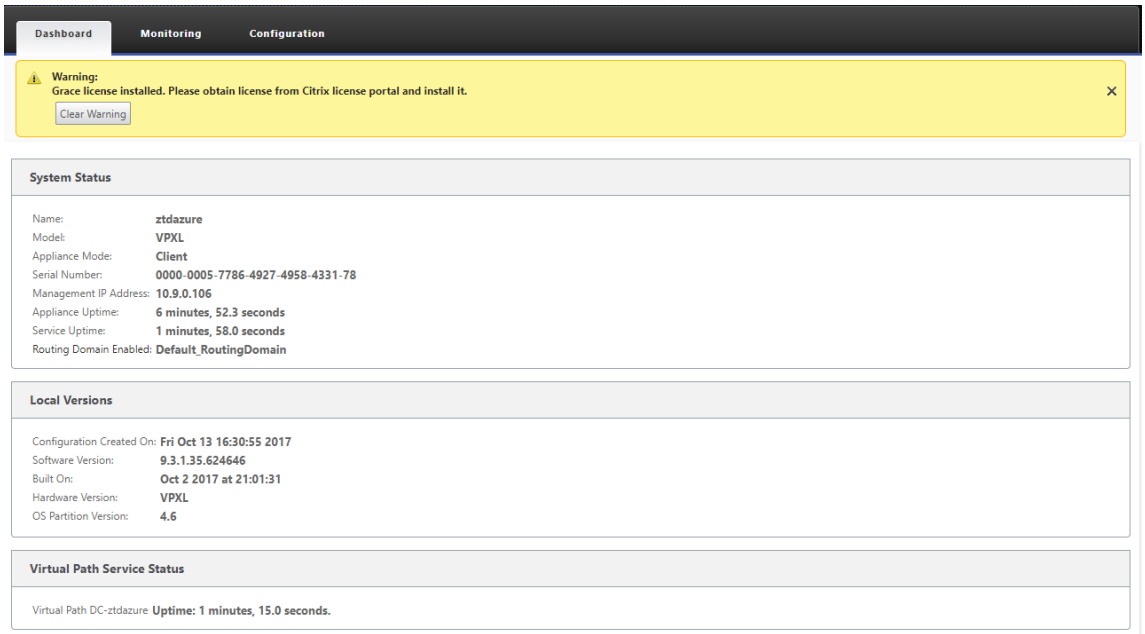
6. In the Azure portal, the successfully launched instance will be available under **Virtual Machines.** To obtain the assigned public IP, navigate to the Overview for the instance.



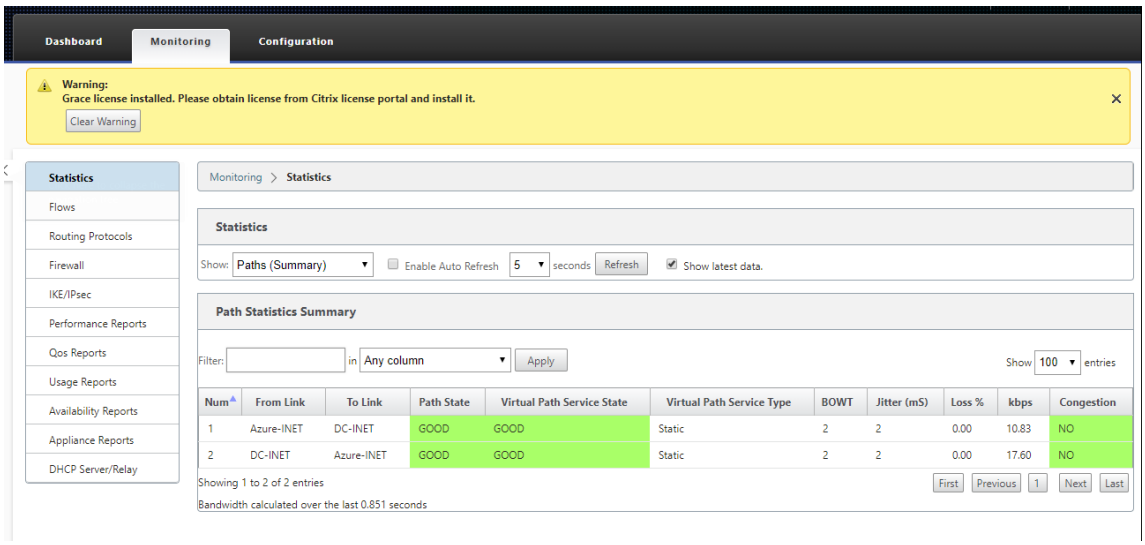
7. After the VM is in a running state, give it a minute before the service will reach out and start the process of downloading the configuration, software and license.



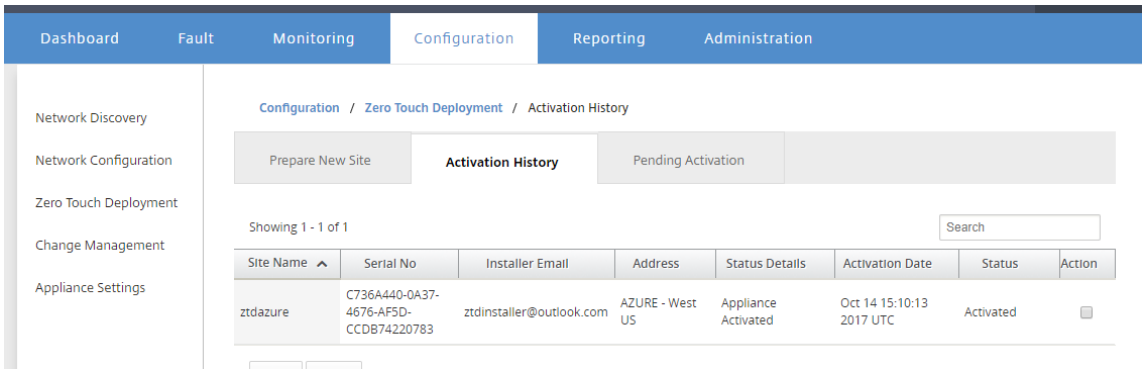
8. After each of the SD-WAN Cloud service steps are automatically complicated, log in to the SD-WAN instances web interface using the public IP obtained from the Azure portal.



9. The Citrix SD-WAN Monitoring Statistics page will identify successful connectivity from the MCN to the SD-WAN instance in Azure.



10. Furthermore, the successful (or unsuccessful) provisioning attempt will be logged in the SD-WAN Center's Activation History page.



Single-region deployment

March 12, 2021

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. RCNs manage traffic between Regions.

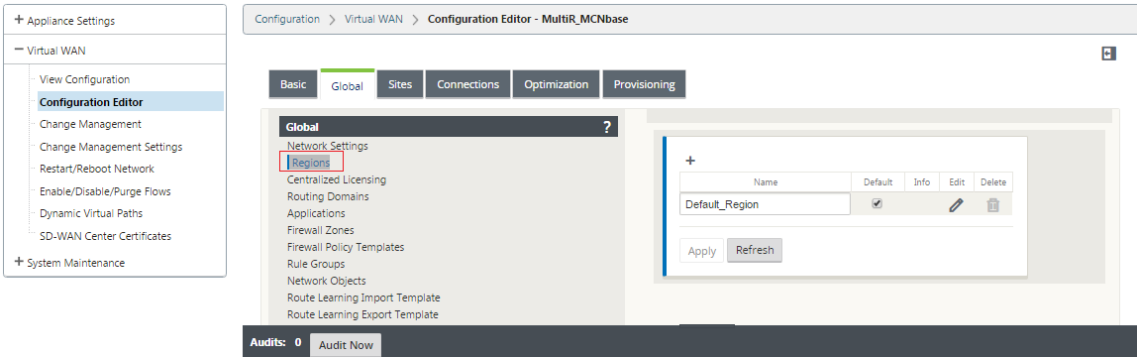
A single-region deployment in an SD-WAN network can support network sites less than 550.

You can configure a 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 a multi-region network with MCN, RCN, Clients, or advanced features, use other configuration options in the configuration editor.

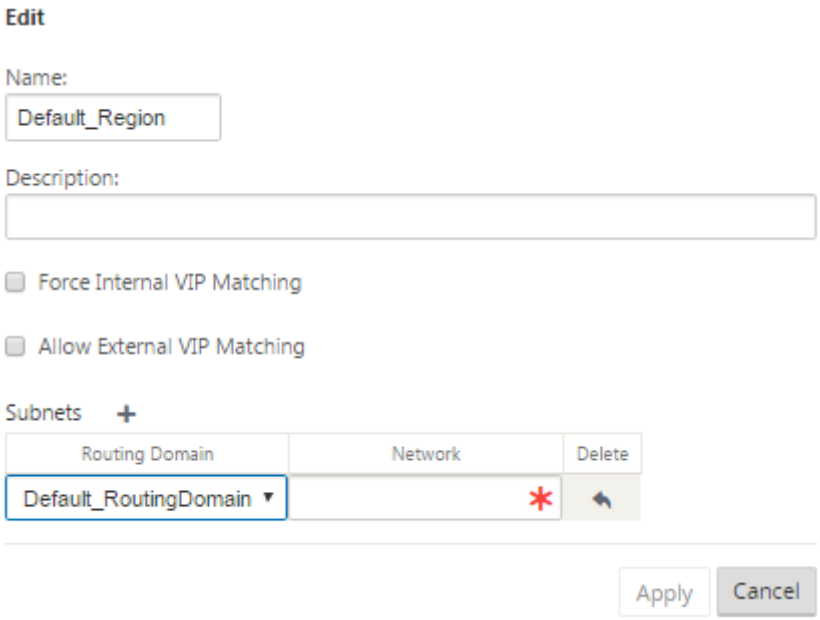
To configure single-region deployment:

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 are forced to match the configured subnets.
   - Allowed External VIP - When enabled, non-private Virtual IP addresses from other regions is allowed to match the configured subnets.
4. Click + to add subnets.



5. Select a **Routing Domain**, enter the **Network** address. Click **Apply**. The network address is the IP address and mask for the subnet.

Multi-region deployment

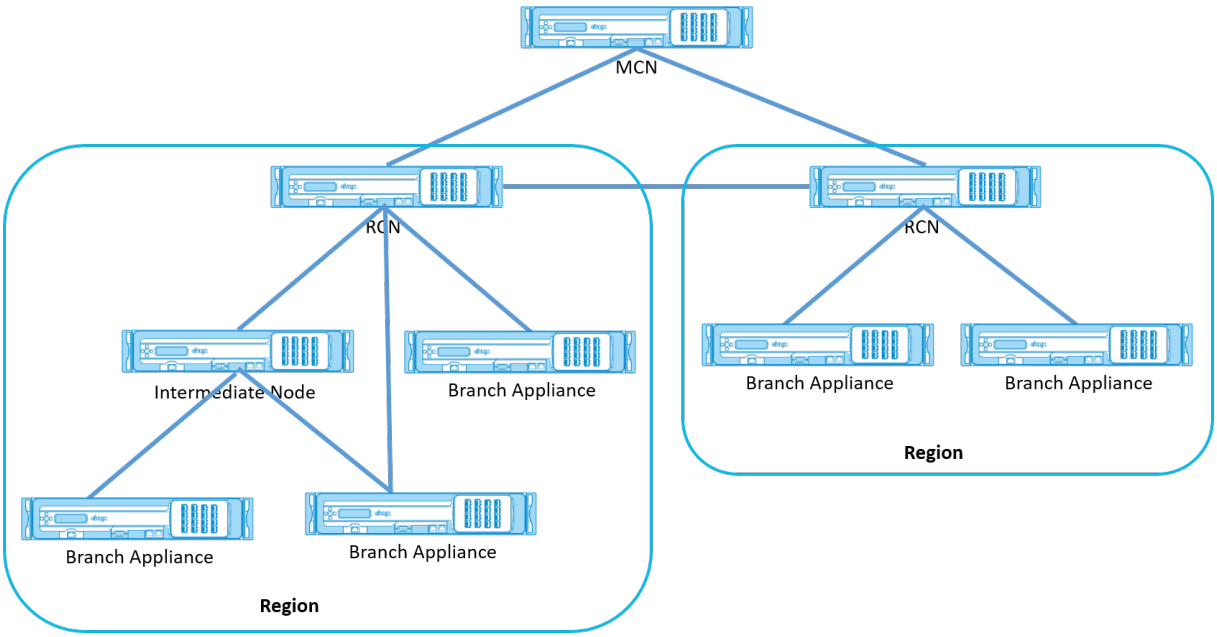
March 12, 2021

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 up to 6000 sites.

Multi-region deployment enables you to fragment a network into regions and set up a tiered network; such as branch (client) > RCN > MCN.

An MCN with a single region can be configured with a 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 following table provides the list of platforms supported for configuring primary and secondary MCN/RCN.

> **NOTE**
>
> - The Premium Edition (PE) appliance is formerly known as the Enterprise Edition (EE).
> - Use the Citrix SD-WAN 210 SE appliance as an MCN only in the SD-WAN Orchestrator managed networks.

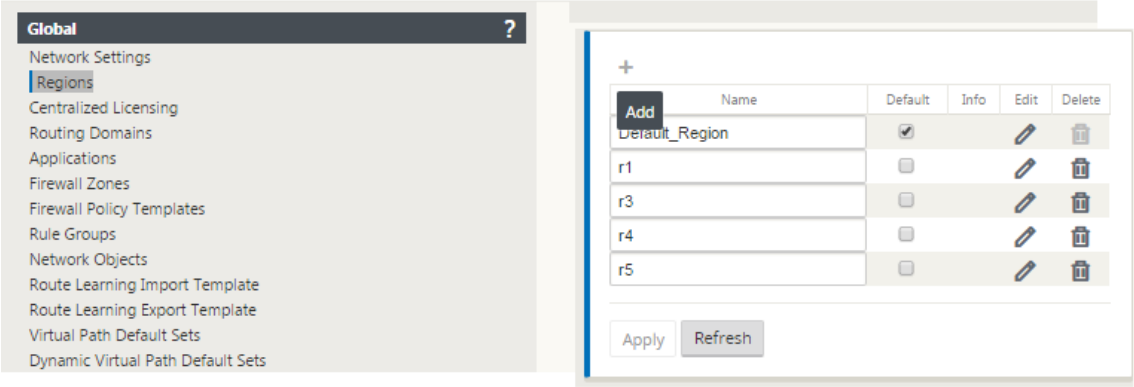
Platform Edition	Primary/Secondary MCN	Primary/Secondary RCN
110-SE	No	No
210-SE	Yes	Yes
400-SE	Yes	No
410-SE	Yes	No
1000-SE, 1000-PE	Yes	No
1100-SE, 1100-PE	Yes	Yes
VPX-SE, VPXL-SE	Yes	Yes
2000-SE, 2100-SE, 2000-PE, 2100-PE, 4000-SE, 4100-SE, 5100-SE, 5100-PE, 6100-SE	Yes	Yes

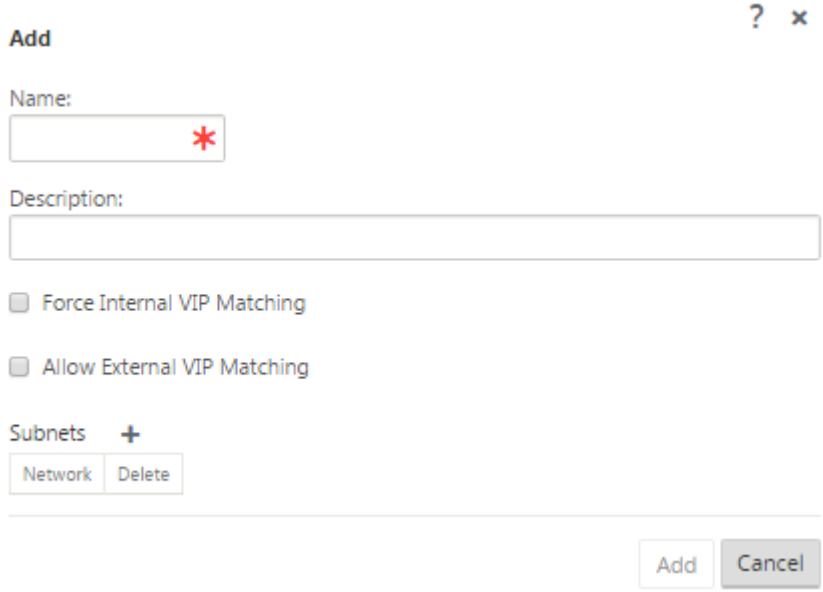
To configure multi-region deployment for an SD-WAN network:

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.



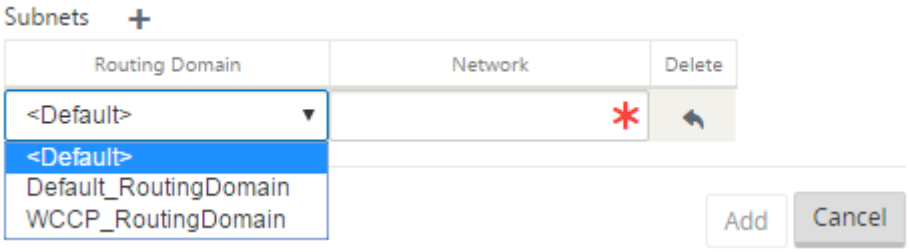


3. Enter a Name and Description for the region.

4. Enable Internal VIP matching based on whether you want **Forced Internal VIP Matching** or **Allow External VIP Matching**.

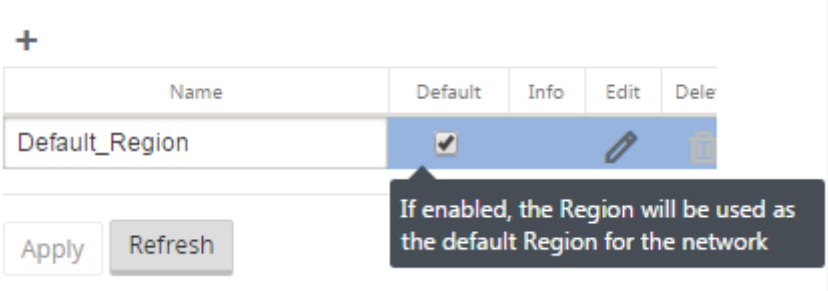
   - Forced Internal VIP: When enabled, all non-private Virtual IP addresses in the Region are forced to match the configured subnets.
   - Allowed External VIP - When enabled, non-private Virtual IP addresses from other regions is allowed to match the configured subnets.

5. Click + to add subnets. Choose a routing domain.



6. Enter a **Network** address. Click **Add.** The network address 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** check box 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 the 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 the change management summary for a 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 25 entries Search

Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	Done	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

Ç

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 - AMEA_r1 Details

Show 25 entries Search

Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
AMEA_r1_vpx01-AMEA_r1_vpx01	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx02-AMEA_r1_vpx02	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx03-AMEA_r1_vpx03	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx04-AMEA_r1_vpx04	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx05-AMEA_r1_vpx05	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx06-AMEA_r1_vpx06	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx07-AMEA_r1_vpx07	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx08-AMEA_r1_vpx08	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx13-AMEA_r1_vpx13	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx14-AMEA_r1_vpx14	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx15-AMEA_r1_vpx15	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx16-AMEA_r1_vpx16	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx17-AMEA_r1_vpx17	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx18-AMEA_r1_vpx18	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx19-AMEA_r1_vpx19	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx20-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx33-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx34-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx35-vpx35	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx36-vpx36	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx37-vpx37	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx38-vpx38	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx39-vpx39	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx40-vpx40	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx49-vpx49	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged

Previous 1 2 Next

> **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."

Configuration guide for Citrix Virtual Apps and Desktops workloads

March 12, 2021

Citrix SD-WAN is a next-generation WAN Edge solution that accelerates digital transformation with flexible, automated, secure connectivity, and performance for SaaS, cloud, and virtual applications to ensure an always-on workspace experience.

Citrix SD-WAN is the recommended and best way for organizations using the Citrix Virtual Apps and Desktops Service to connect to Citrix Virtual Apps and Desktops workloads in the Cloud. For more information, see Citrix blog.

This document focuses on configuring Citrix SD-WAN for connectivity to/from Citrix Virtual Apps and Desktops workloads on Azure.

Benefits

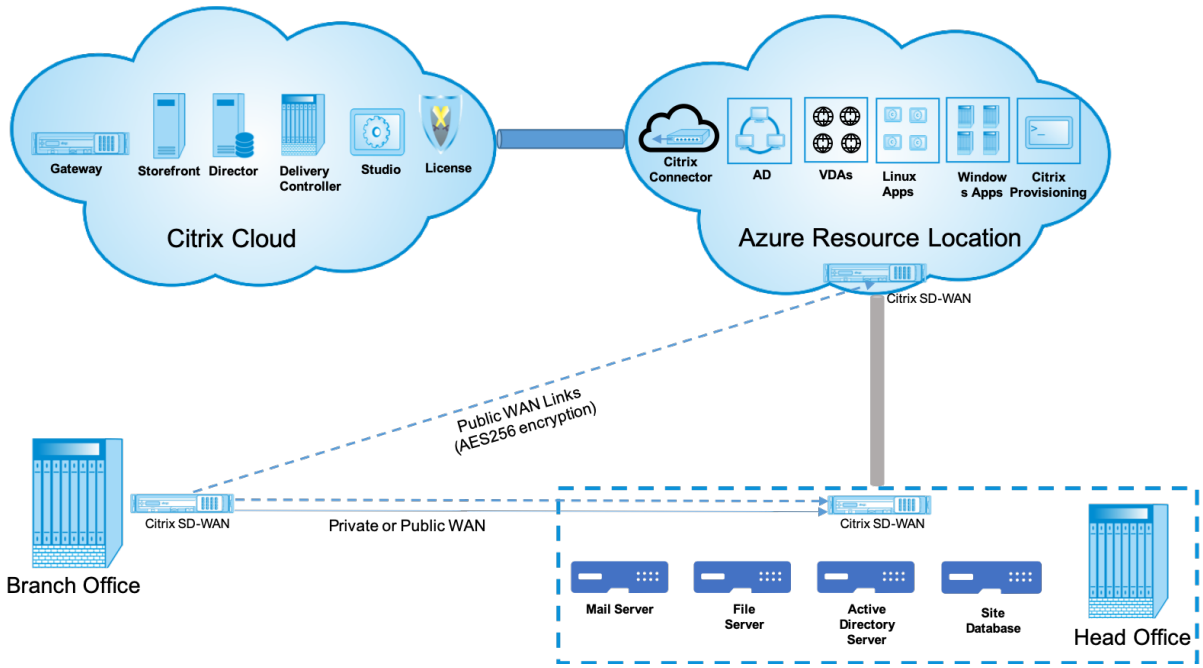
- Easy to set up SD-WAN in Citrix Virtual Apps and Desktops through a guided workflow
- Always-on, high performance connectivity through advanced SD-WAN technologies
- Benefits across all connections (VDA-to-DC, user-to-VDA, VDA-to-cloud, user-to-cloud)
- Reduces latency compared to backhauling traffic to the data center
- Traffic management to ensure Quality of Service (QoS)
  - QoS across HDX/ICA traffic streams (single-port multi-stream HDX AutoQoS)
  - QoS between HDX and other traffic
  - HDX QoS Fairness between users
  - End-to-end QoS
- Link bonding delivers more bandwidth for faster performance
- High Availability with seamless link failover and SD-WAN redundancy on Azure
- Optimized VoIP experience (packet racing for reduced jitter and minimal packet loss, QoS, local break-out for reduced latency)
- Major cost savings and must be faster and easier to deploy compared to Azure ExpressRoute

Pre-requisites

Adhere the following pre-requisites to evaluate and deploy the Citrix Virtual Apps and Desktops workloads capabilities:

- You must have either have an existing SD-WAN network or build a new one.
- You must have a subscription to Citrix Virtual Apps and Desktops Service.
- To make a use of SD-WAN features such as, multi-stream HDX AutoQoS and deep visibility, the Network Location Service (NLS) must be configured for all the SD-WAN sites in your network.
- You must have a DNS server and AD deployed where the client endpoints are present (often co-located in your data center environment) or you can utilize Azure Active Directory (AAD).
- The DNS server must be capable of resolving both internal (private) and external (public) IPs.
- Ensure that the FQDN (sdwan-location.citrixnetworkapi.net) is added to the allowed list in the firewall. This is the FQDN for Network Location Service which is critical in sending traffic over the SD-WAN virtual path. Also, a better way if you are comfortable with whitelisting wild card FQDNs would be to add *.citrixnetworkapi.net to allowed list as this is the subdomain for other Citrix Cloud services such as zero touch provisioning.
- Enroll at sdwan.cloud.com to use the SD-WAN orchestrator for managing your SD-WAN network. SD-WAN Orchestrator is a Citrix Cloud based multitenant management platform for Citrix SD-WAN.

Deployment architecture

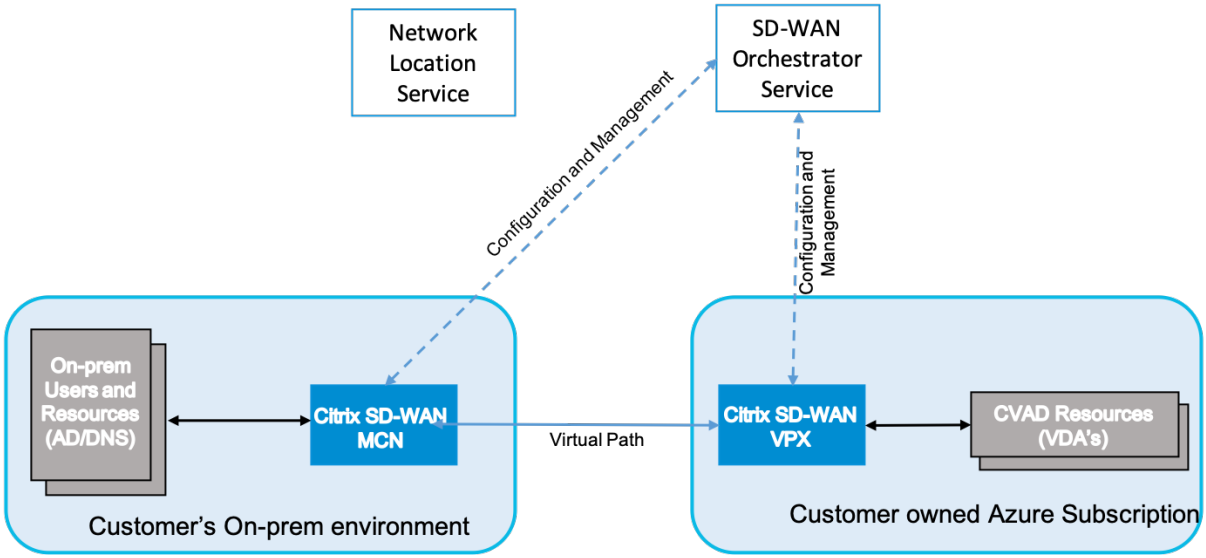


The following entities are required for deployment:

- An on-premises location hosting the SD-WAN appliance which can either be deployed in branch mode or as an MCN (Master control Node). The branch mode or MCN contains the client machines, active directory, and DNS. However, you can also choose to use Azure's DNS and AD. In most scenarios, the on-premises location serves as a data center and houses the MCN.
- **Citrix Virtual Apps and Desktops cloud service** –Citrix Virtual Apps and Desktops provides virtualization solutions that give IT control of virtual machines, applications, and security while providing anywhere access for any device. End users can use applications and desktops independently of the device's operating system and interface.

  Using the Citrix Virtual Apps and Desktops Service, you can deliver secure virtual apps and desktops to any device, and leave most of the product installation, setup, configuration, upgrades, and monitoring to Citrix. You maintain complete control over applications, policies, and users while delivering the best user experience on any device.
- **Citrix connector/cloud connector** - You connect your resources to the service through Citrix Cloud Connector, which serves as a channel for communication between Citrix Cloud and your resource locations. Cloud Connector enables cloud management without requiring any complex networking or infrastructure configuration such as VPNs or IPsec tunnels. Resource locations contain the machines and other resources that deliver applications and desktops to your subscribers.
- **SD-WAN Orchestrator** –Citrix SD-WAN Orchestrator is a cloud-hosted, multitenant management service available to **Do It Yourself** enterprises and Citrix Partners. Citrix partners can use Citrix SD-WAN Orchestrator to manage multiple customers with a single pane of glass, and suitable role-based access controls.
- **Virtual and physical SD-WAN appliances** –This runs as multiple instances within the cloud (VMs) and on-premises in the data center and in the branches (physical appliances or VMs) to provide connectivity among these locations and to/from the public Internet. SD-WAN instance in Citrix Virtual Apps and Desktops is created as a single or a set of virtual appliances (in HA deployment) by provisioning these instances via the Azure Marketplace. SD-WAN appliances in other locations (DC and branches) are created by the customer. All of these SD-WAN appliances are managed (in terms of configuration and software upgrades) by SD-WAN Administrators through SD-WAN Orchestrator.

Deployment and configuration



In a common deployment, a customer would have the Citrix SD-WAN appliance (H/W or VPX) deployed as an MCN in their DC/large office. The customer DC would usually host on-prem users and resources such as AD and DNS servers. In some scenarios the customer can make use of Azure Active Directory services (AADS) and DNS, both of which are supported by Citrix SD-WAN and CMD integration.

Within the customer managed Azure subscription, the customer needs to deploy the Citrix SD-WAN virtual appliance and VDAs. The SD-WAN appliances are managed via SD-WAN Orchestrator. Once the SD-WAN appliance gets configured, it connects to the existing Citrix SD-WAN network and further tasks such as configuration, visibility, and management are handled via SD-WAN Orchestrator.

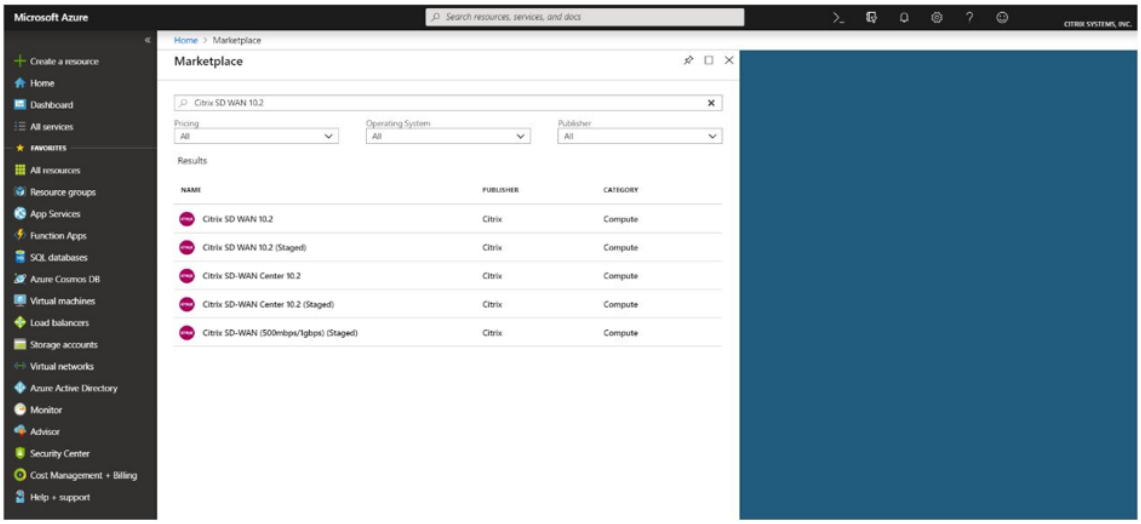
The third component in this integration is the **Network Location Service (NLS)** that allows internal users to bypass the gateway and connect to the VDA's directly, reducing latency for internal network traffic. You can configure NLS manually or through Citrix SD-WAN Orchestrator. For more information, see NLS.

Configuration

Citrix SD-WAN VM is deployed within a specified region (as needed by the customer) and can be connected to multiple branch office locations through MPLS, Internet, or 4G/LTE. Within a Virtual Network (VNET) infrastructure, SD-WAN Standard Edition (SE) VM is deployed in gateway mode. The VNET has routes towards the Azure gateway. The SD-WAN instance has a route towards the Azure gateway for internet connectivity. This route needs to be created manually.

1. In a web browser, go to Azure portal. Log into Microsoft Azure account and search for Citrix SD-WAN Standard Edition.

2. In the search results, choose the Citrix SD-WAN Standard Edition solution. Click **Create** after going through the description and making sure the solution chosen is correct.

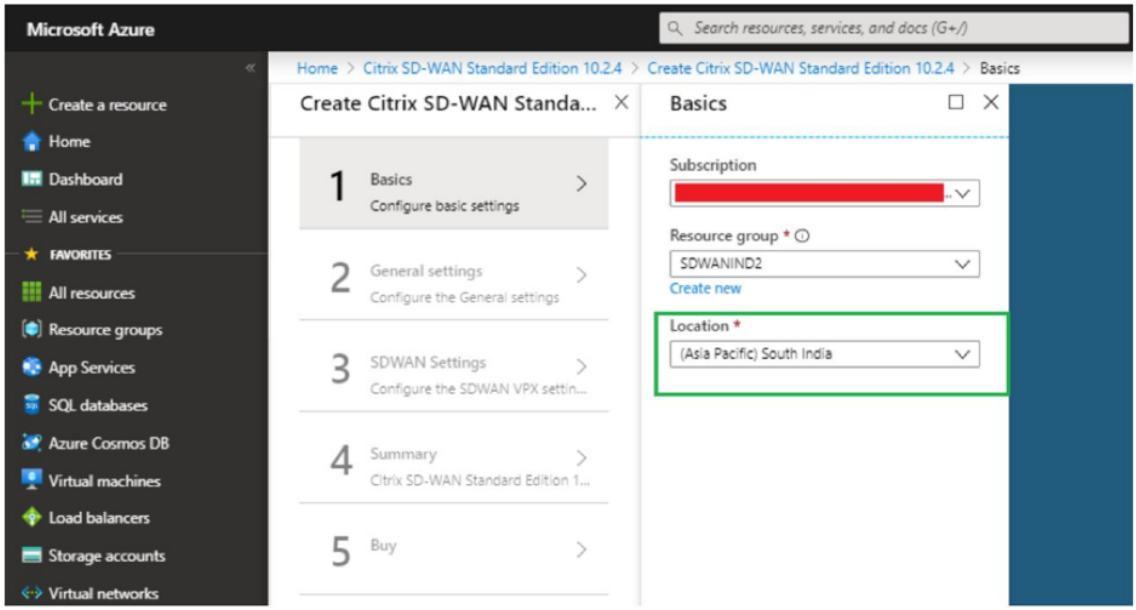


On click of **Create**, a wizard prompting with necessary details to create the virtual machine.

3. In the **Basic settings** page, choose the resource group in which you want to deploy the SD-WAN SE solution.

A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You can decide how you want to allocate resources to resource groups based on your deployment.

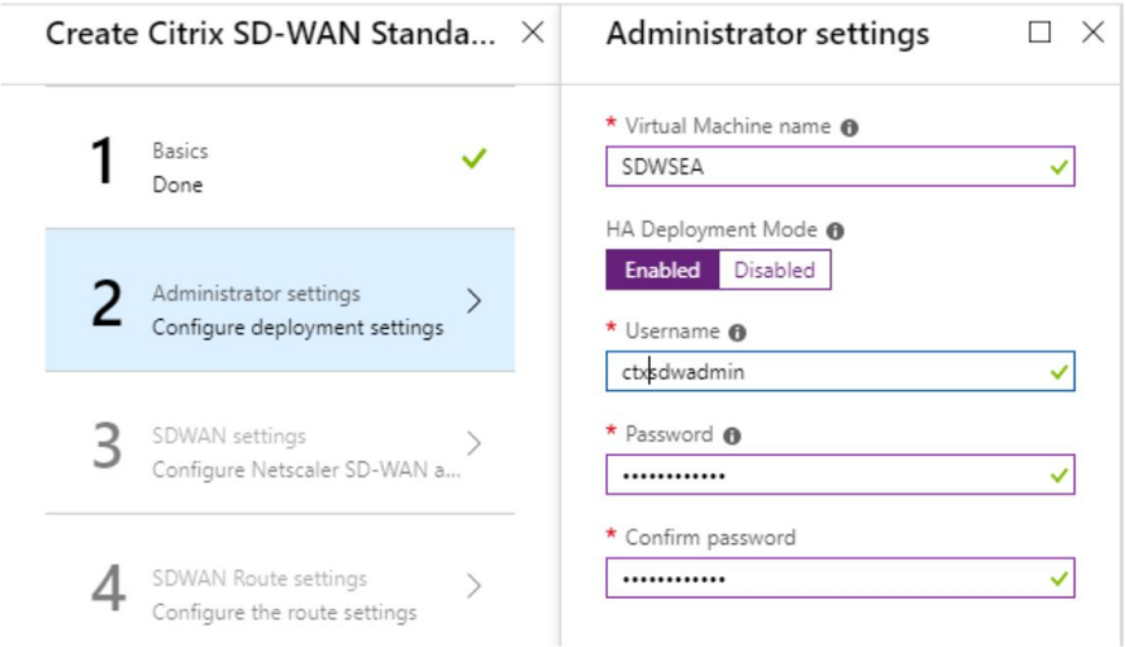
For Citrix SD-WAN, it's recommended that the resource group you choose must be empty. Similarly, pick the Azure region where you want to deploy the SD-WAN instance. The region must be the same as the region in which your Citrix Virtual Apps and Desktops resources are deployed.



4. Under **Administrator settings** page, provide a name for the Virtual Machine. Choose a user name and strong password. The password must consist of an upper-case letter, special character and must be more than nine characters. Click **OK**.

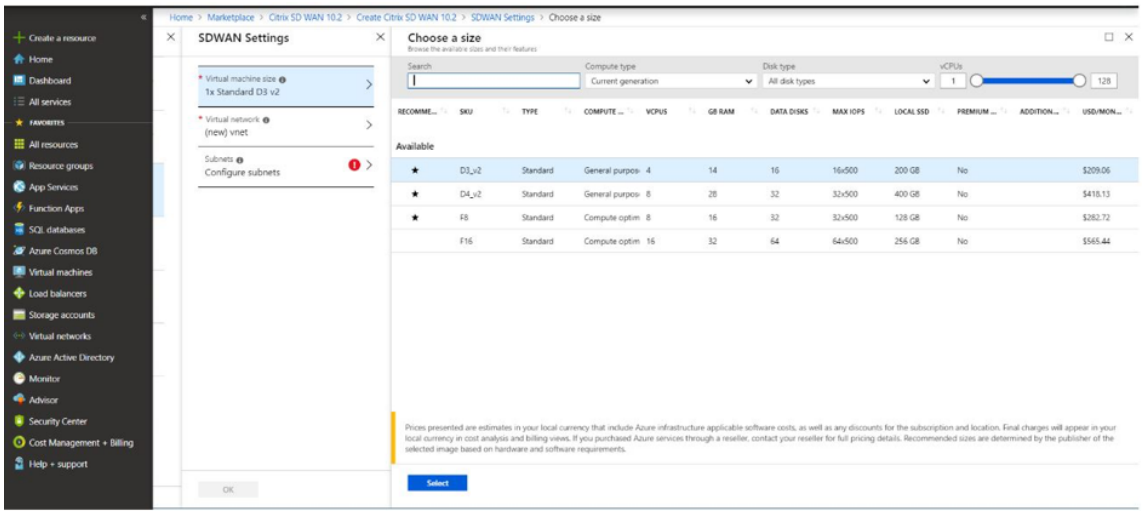
   This password is required to log in to the management interface of the instance as a guest user. To get admin access to the instance, use admin as the user name and the password created while provisioning the instance. If you use the user name created while provisioning the instance, you get read-only access. Also, choose the deployment type here.

   If you want to deploy a single instance then make sure that you choose disabled from the HA Deployment mode option, else pick enabled. For production networks, Citrix always recommends deploying instances in HA mode as it guards your network against failures of the instance.

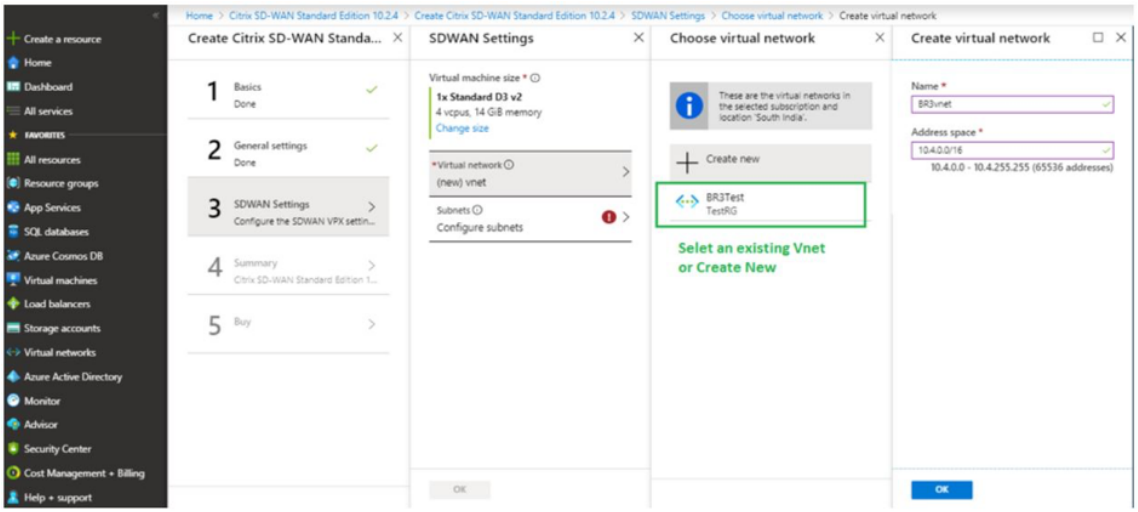


5. Under the **SD-WAN settings** page, choose the instance in which you want to run the image. Choose the following instance type as per your requirement:

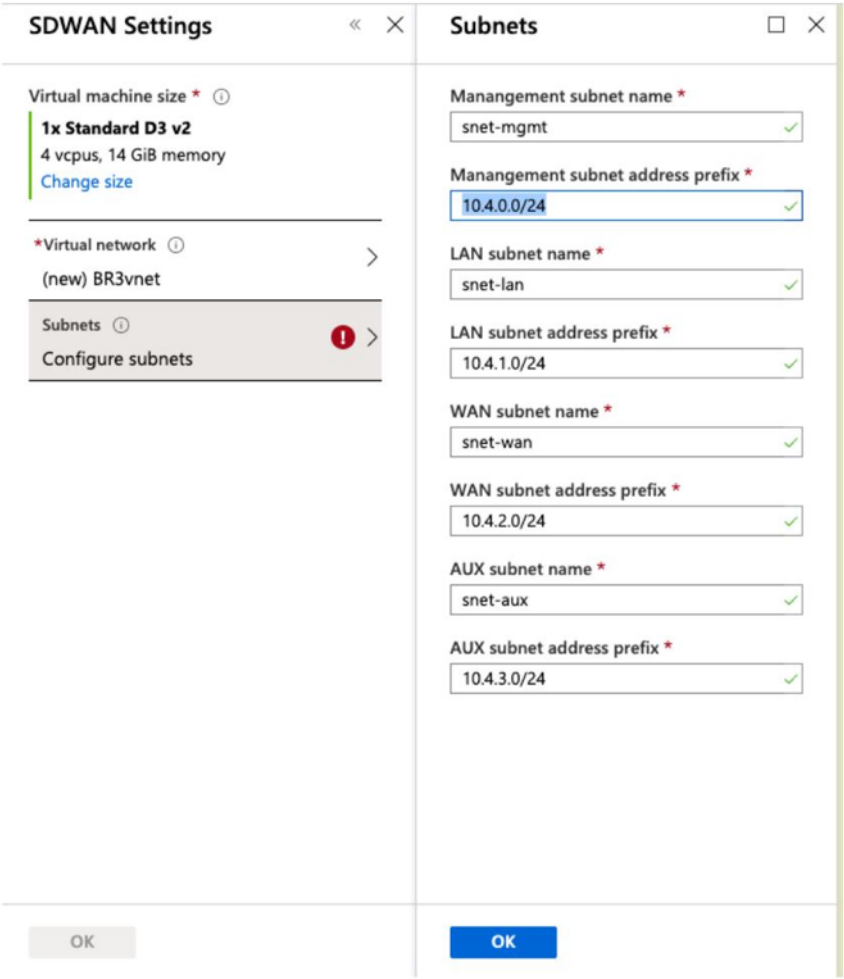
   - Instance type D3_V2 for maximum uni-directional throughput of 200 Mbps with direct connectivity to a maximum of 16 branches.
   - Instance type D4_V2 for maximum uni-directional throughput of 500 Mbps with direct connectivity to a maximum of 16 branches.
   - Instance type F8 standard for maximum uni-directional throughput of 1 Gbps with direct connectivity to a maximum of 64 branches.
   - Instance type F16 standard for maximum uni-directional throughput of 1 Gbps with direct connectivity to a maximum of 128 branches.



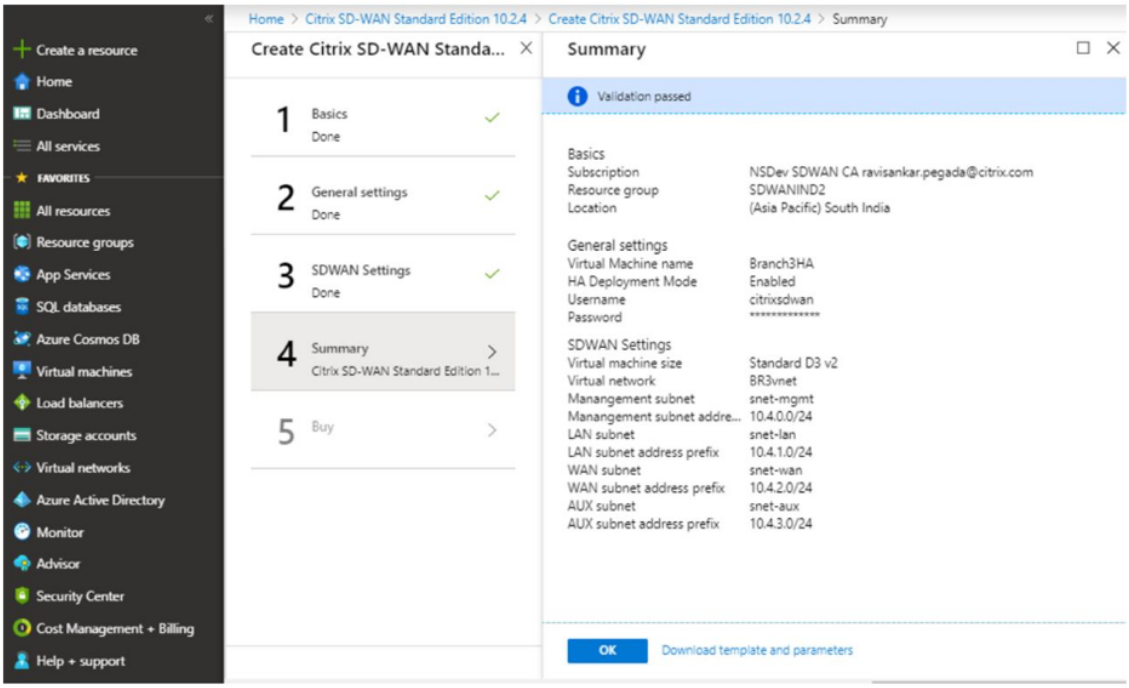
6. Create a new Virtual Network (VNet) or use an existing VNet. This is the most critical step for the deployment as this step chooses the subnets to be assigned to the interfaces of the SD-WAN VPX VM.



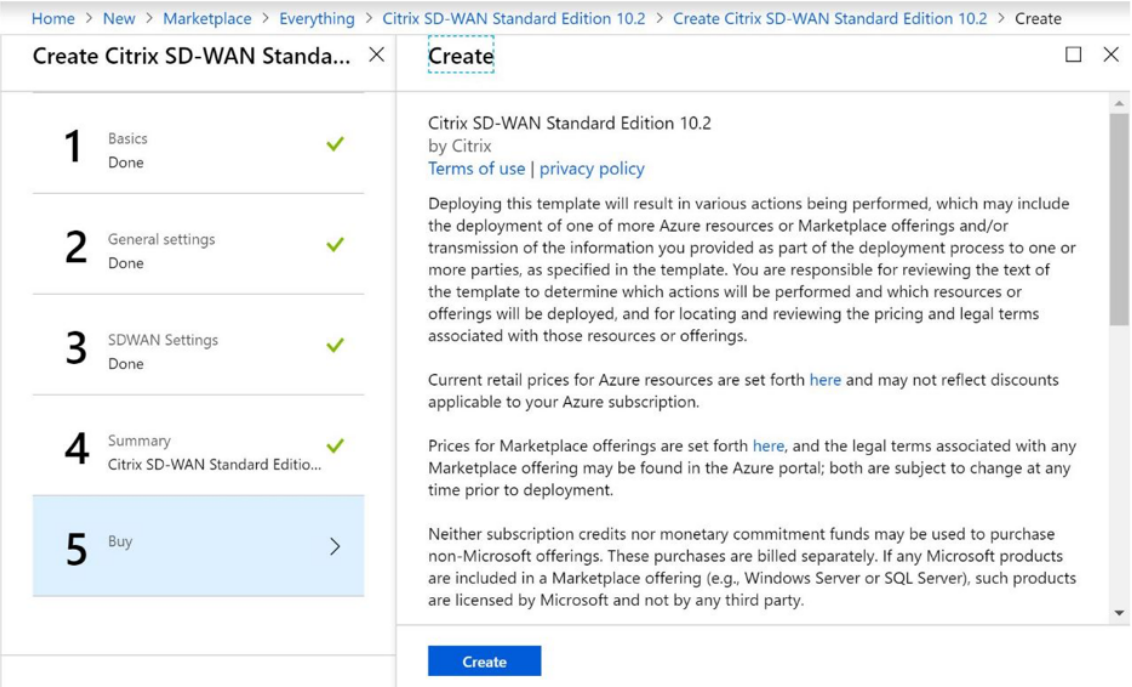
The aux subnet is only needed when you are deploying the instances in HA mode. Ensure that the SD-WAN instance is being deployed in the same VNet as your Citrix Virtual Apps and Desktops resources and is on the same subnet as the LAN interface of the SD-WAN VPX appliance.



7. Verify the configuration in the **Summary** page and click **OK**.



8. On the **Buy** page, click **Create** to start the provisioning process for the instances. It can take around 10 minutes for the instance to get provisioned. You get a notification in the Azure management portal suggesting the success/failure of instance creation.

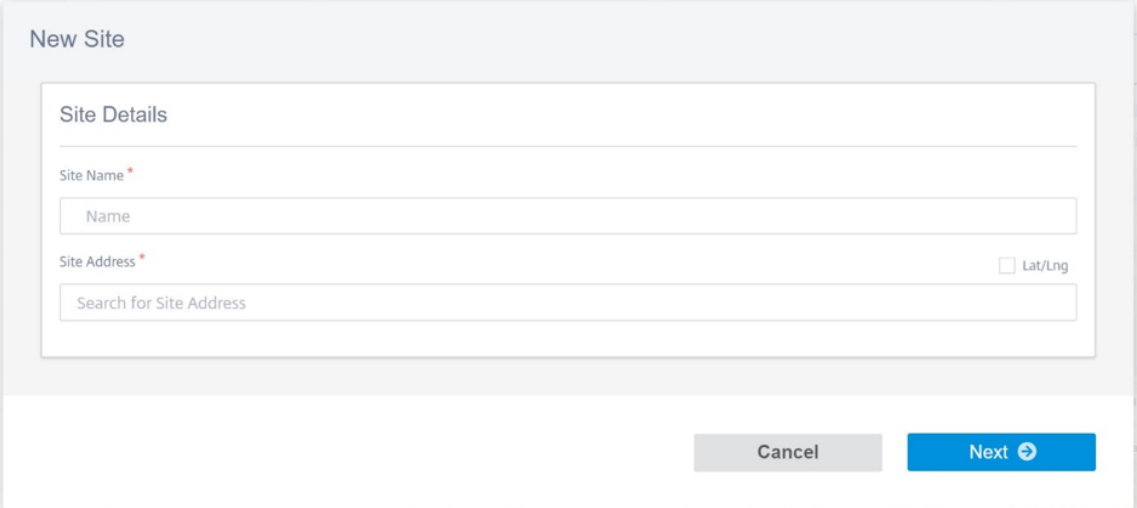


Once the instance is created successfully, fetch the public IP assigned to the management interface of the SD-WAN instance. It can be found under the networking section of the resource group within which the instance has been provisioned. Once retrieved you might use it to log

in to the instance.

> **NOTE**
>
> For admin access, the user name is **admin** and the password is the one that you have set during instance creation.

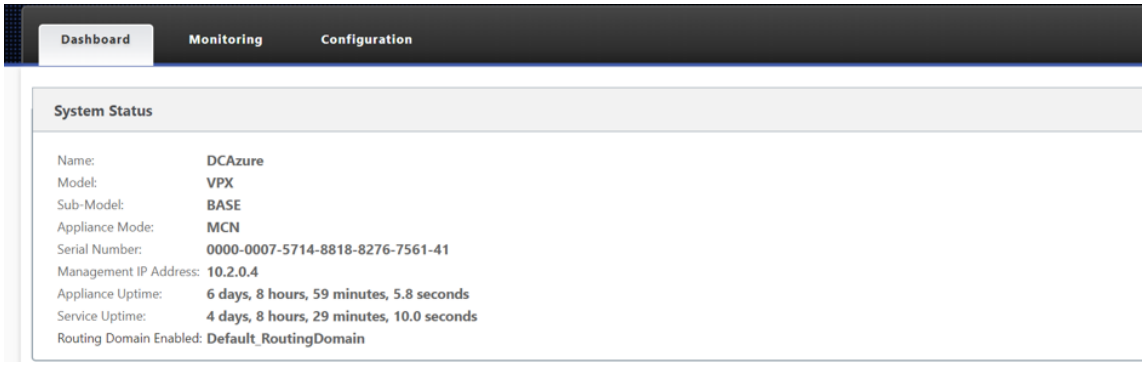
9. Once the site has been provisioned, log into the SD-WAN Orchestrator to configure it. As mentioned in the pre-requisites, you must have the entitlement to SD-WAN Orchestrator to configure the site. If you do not have it yet, refer Citrix SD-WAN Orchestrator Onboarding.
10. If you have an SD-WAN network already, then proceed to creating the configuration for the site that you provisioned in Azure. Otherwise you must create an MCN. For more information, see Network configuration.
11. Once you have access to SD-WAN Orchestrator and already have set up an MCN, login to SD-WAN orchestrator and click the **+New site** to start configuring the SD-WAN VPX appliance (that you have provisioned in Azure).



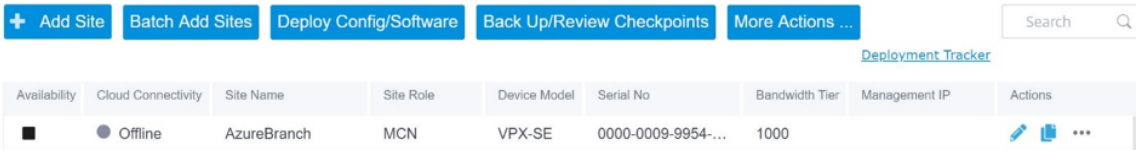
12. Provide a unique site name and enter the address based on the region in which you are provisioning the image. To set up the instance in Azure, refer Basic settings.

> **NOTE**
>
> To fetch the serial number of the instance in Azure, log in to the instance via the public management IP. You can see the serial number on the dashboard screen. If you are configuring instances in HA then both the serial numbers must be captured. Also, while configuring the instance, ensure that the interfaces are chosen as **Trusted**.

13. For fetching the IP addresses associated with LAN and WAN interfaces on Azure. Navigate to the **Azure portal > Resource groups > Resource group** where the SD-WAN is **provisioned >SD-WAN VM > Networking**.



14. Once you are done with the configuration of the instance. Click **Deploy Config/Software** by navigating to **Configuration > Network config Home**.

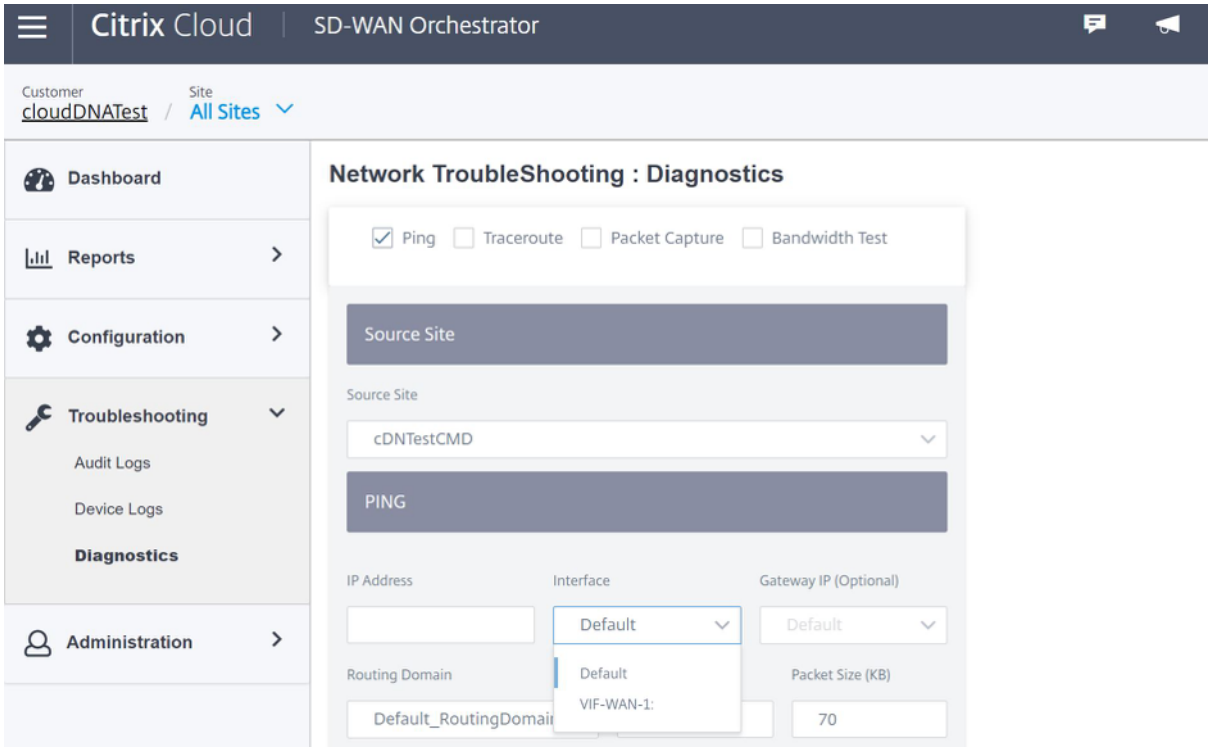


15. If there are no issues and the configuration is accurate, you must have the virtual paths up between the instance in Azure and your MCN once the configuration deployment is run.

Citrix Virtual Apps and Desktops configuration

As highlighted in the Deployment and configuration section, the AD/DNS is present in the on-premises location acting as the DC and in a deployment featuring SD-WAN it presents behind the SD-WAN that is on the LAN network. It is the IP of your AD/DNS that you need to configure here. In case you are making use of Azure Active Directory service/DNS, configure **168.63.129.16** as the DNS IP.

If you are making use of an on-premises AD/DNS.Check if you are able to ping the IP of your DNS from your SD-WAN appliance. You can do this by navigating to **Troubleshooting > Diagnostics**. Check the **Ping** check box and initiate a ping from the LAN interface/Default interface of the SD-WAN appliance to the IP of your AD/DNS.



If the ping succeeds, then it signifies that your AD/DNS can be reached successfully, if not then it means there is routing issue in your network which is preventing reachability to your AD/DNS. If possible, try to host your AD and SD-WAN appliance on the same LAN segment.

In case there is still an issue, get in touch with your network admin. Without completing this step successfully, the catalog creation step will not succeed and you get an error message as **Global DNS IP not configured**.

> **NOTE**
>
> Ensure that the DNS is capable of resolving both internal and external IPs.

Network location service

With the **Network Location** service in Citrix Cloud, you can optimize internal traffic to the apps and desktops you make available to subscribers'workspaces to make HDX sessions faster. Users on both internal and external networks have to connect to VDAs through an external gateway. While this is expected for external users, internal users experience slower connections to virtual resources. The **Network Location** service allows internal users to bypass the gateway and connect to the VDAs directly, reducing latency for internal network traffic.

Configuration

To set up the **Network Location** service, use one of the following methods:

- **Citrix SD-WAN Orchestrator**: For detailed information on configuring NLS using Citrix SD-WAN Orchestrator, see Network location service.
- **Network Location service PowerShell module that Citrix provides**: For detailed information on configuring NLS using PowerShell module, see PowerShell module and configuration.

The network locations share the public IP ranges of the networks where your internal users are connecting from. When subscribers launch Virtual Apps and Desktops sessions from their workspace, Citrix Cloud detects whether subscribers are internal or external to the company network based on the public IP address of the network from which they are connecting.

If a subscriber connects from the internal network, Citrix Cloud routes the connection directly to the VDA, bypassing Citrix Gateway. If a subscriber connects externally, Citrix Cloud routes the subscriber through Citrix Gateway as expected and then redirects the subscriber to the VDA in the internal network.

> **NOTE**
>
> The public IP that needs to be configured in the network location service needs to be the public IP assigned to the WAN links.

Domain name system

March 12, 2021

Domain Name System (DNS) translates human readable domain names to machine-readable IP addresses, and vice versa. Citrix SD-WAN provides the following DNS features:

- DNS Proxy
- DNS Transparent Forwarding

You can configure a DNS proxy or DNS transparent forwarding using the following two types of DNS service:

- **Static DNS service**: Intercepts the DNS requests destined to SD-WAN IP address and forwards it to the specified DNS servers. You can create internal, ISP, google or any other open source DNS service. Static DNS service can be configured at global and site level.
- **Dynamic DNS service**: Intercepts the DNS requests destined to SD-WAN IP address and redirects it to one of the DNS servers learned from the DHCP based WAN links. If the WAN link goes

down another DHCP based WAN links DNS server is chosen. This feature is useful in the deployment where ISPs allow DNS requests only to DNS servers hosted by them. Dynamic DNS service can be configured at site level only. Only one dynamic DNS service is permitted per site.

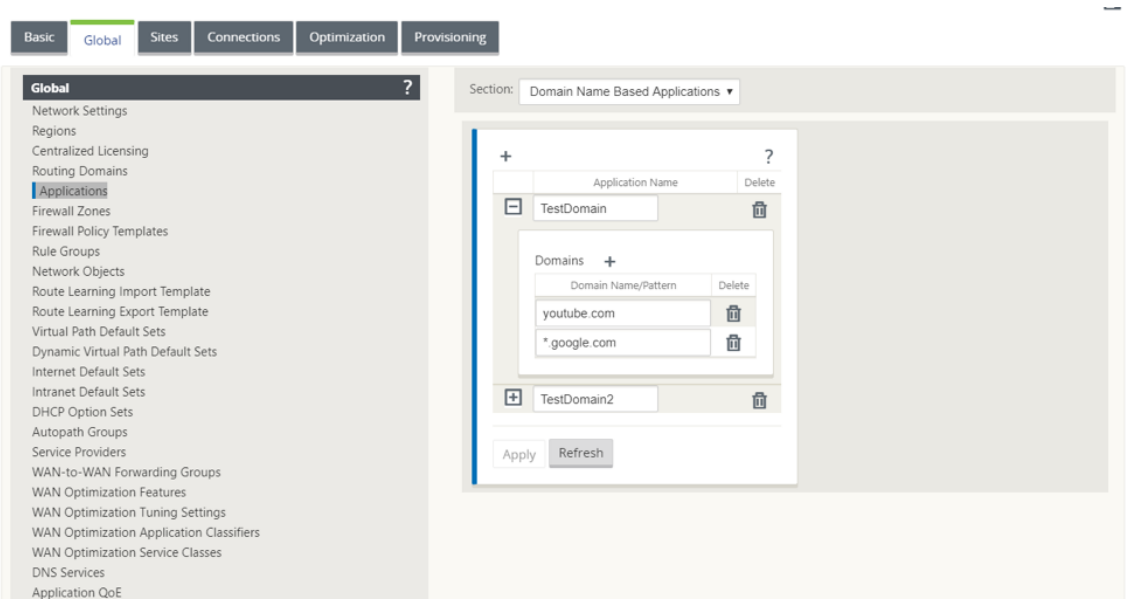
DNS proxy

You can configure a proxy with multiple forwarders that helps steering DNS requests based on application domain names. DNS forwarding works for the requests that are received through UDP connections.

To configure SD-WAN as a DNS Proxy:

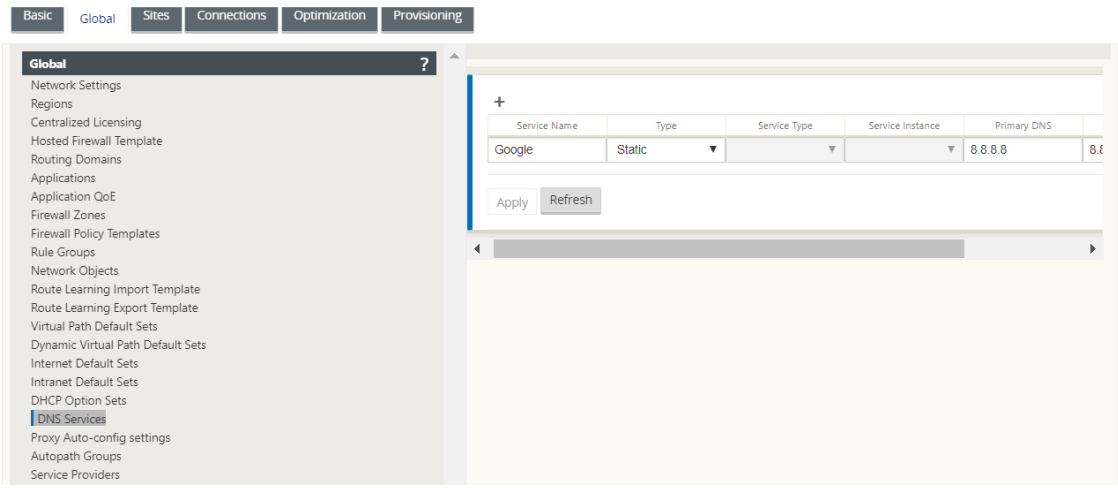
1. Define the domain name based applications. In the Configuration Editor, navigate to **Global > Applications > Domain Name Based Applications**.

   Enter the application name and the required domain names or patterns. You can group several domain names as an application. You can either enter the full domain name or use wild cards at the beginning. For example - *.google.com



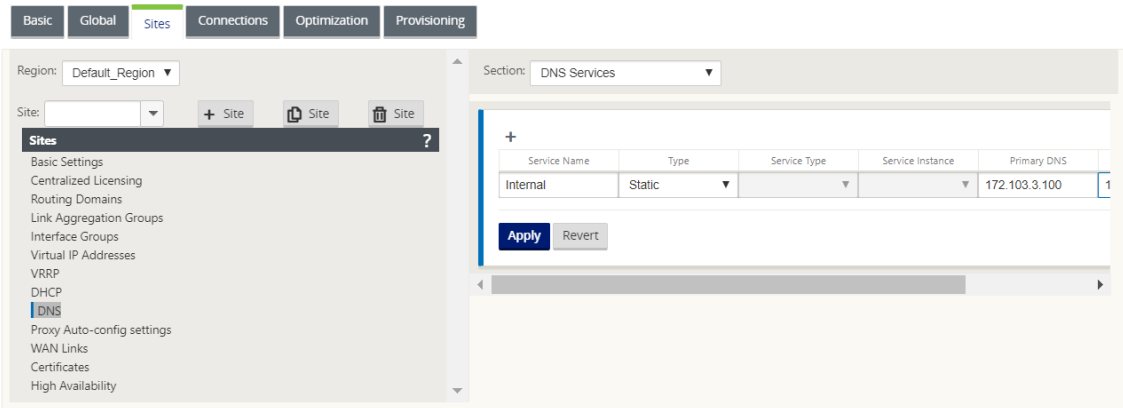
2. Define the required DNS Services. You can define Static or Dynamic DNS service.

   To configure a Static DNS service, navigate to **Global** > **DNS Service**, select the **Type** as **Static**. Enter the **Service Name** and a pair of Primary and Secondary DNS server IP addresses.



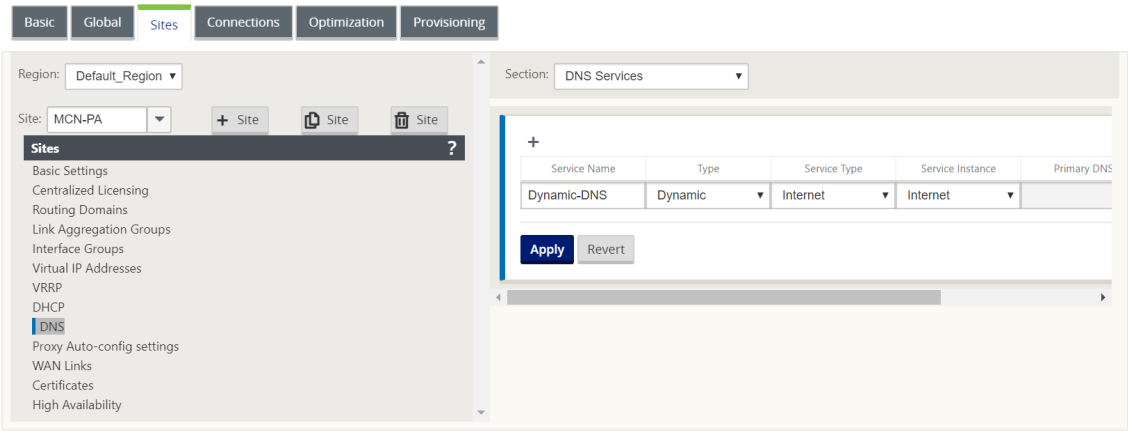
> **Note**
>
> If you have configured Office 365 breakout policy, a Quad9 DNS service is auto created. For more information, see Office 365 Optimization.

Alternatively, you can also define the Static DNS services at individual site level. The site-level DNS service configuration overrides the global configuration. To configure site-specific static DNS service, navigate to **Sites** > **DNS** > **DNS Services** and select the **Type** as **Static**.



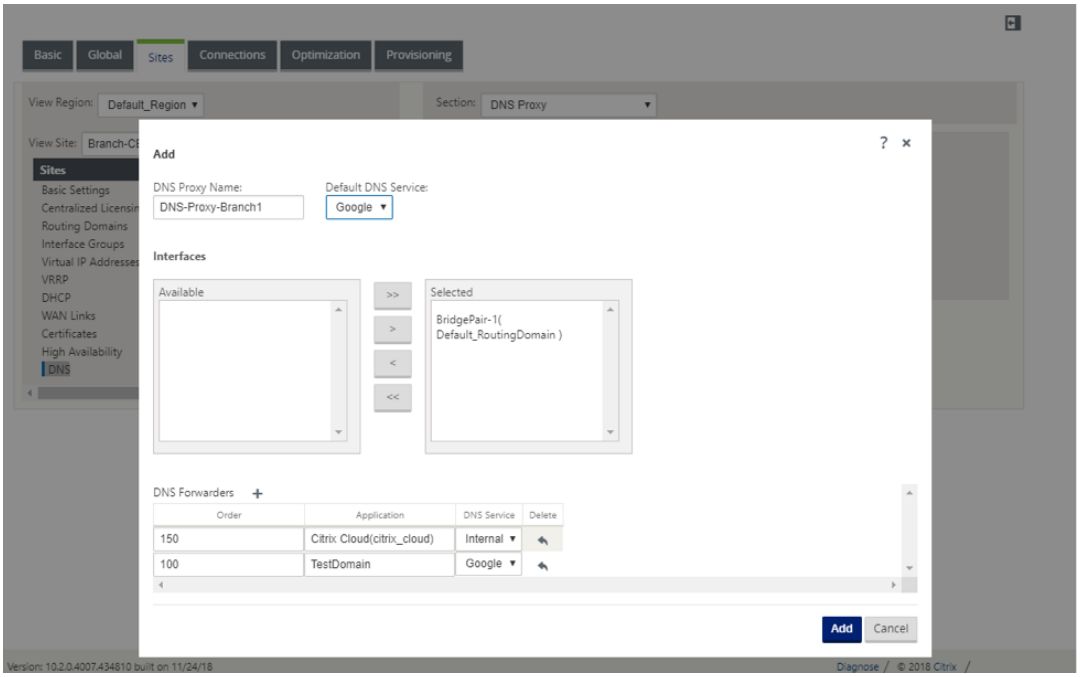
To configure a Dynamic DNS service, navigate to **Sites** > **DNS** > **DNS Services** and select the **Type** as **Dynamic**. Enter the **Service Name** and select **Internet** for **Service Type** and **Service Instance**.

> **Note**
>
> Dynamic DNS service can be configured at site level only. Only one dynamic DNS service is permitted per site.



3. Configure DNS proxy for the site. Navigate to **Sites > DNS > DNS Proxy**. Click **+**. Enter values for the following parameters:

   - **DNS Proxy Name**: Name of the DNS Proxy.
   - **Default DNS Service**: The default DNS Service to which the DNS requests are forwarded to, if none of the applications match in DNS forwarder look-up.
   - **Interfaces**: The interfaces on which the DNS requests are intercepted. Only trusted interfaces are allowed.
   - **DNS Forwarders**: List of DNS forwarders.
     - **Order**: The priority of the forwarder.
     - **Application**: Applications for which DNS requests have to be forwarded to the selected DNS service.
     - **DNS Service**: The DNS service that the DNS requests are forwarded to for the specified application.

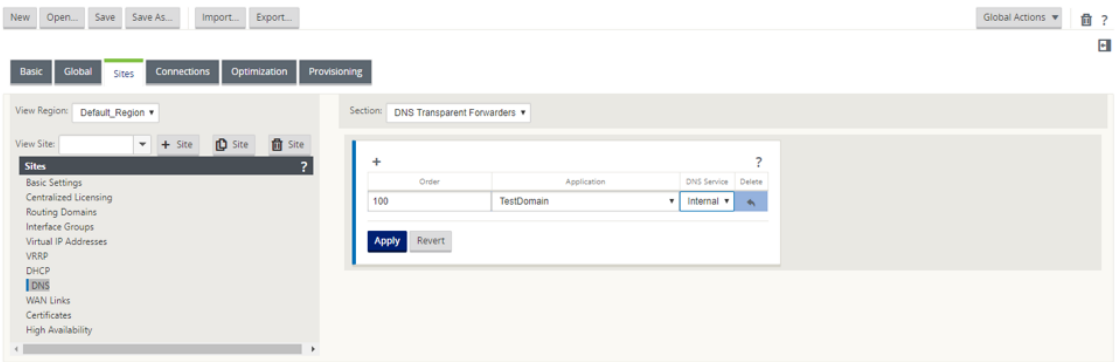


DNS transparent forwarder

Citrix SD-WAN can be configured as a transparent DNS forwarder. In this mode, SD-WAN can intercept DNS requests that are not destined to its IP address and forward them to the specified DNS service. Only the DNS requests coming from local service on trusted interfaces are intercepted. If the DNS requests match any applications in the DNS forwarder list, then it is forwarded to the configured DNS service. DNS forwarding is supported only for requests coming over UDP connections.

To configure SD-WAN as a DNS transparent forwarder:

1. Navigate to **Sites > DNS > DNS Transparent Forwarders**. Click **+**.
2. Enter values for the following parameters:
   - **Order**: The priority of the forwarder.
   - **Application**: Applications for which DNS requests have to be forwarded to the selected DNS service.
   - **DNS Service**: The DNS service that the DNS requests are forwarded to for the specified application.



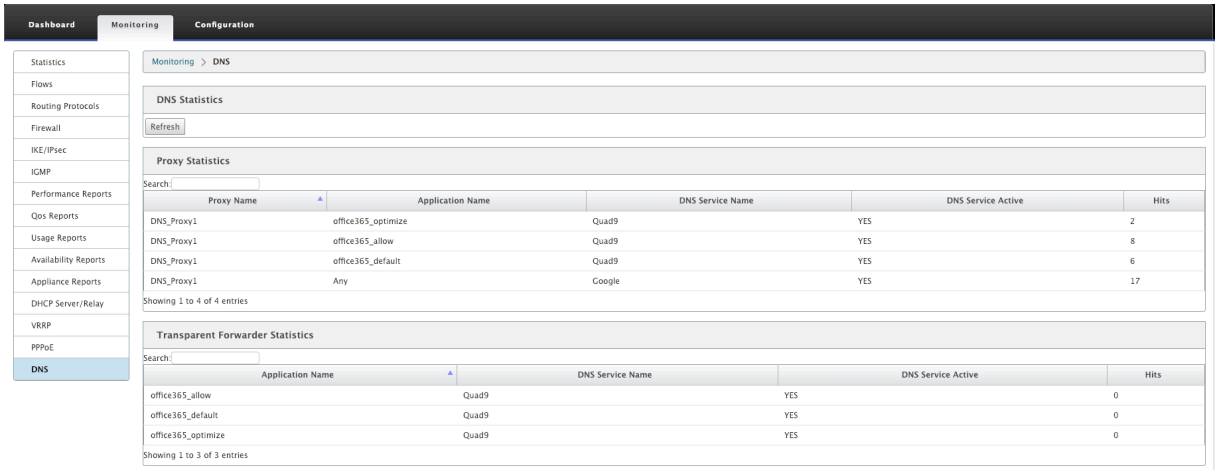
Similarly, continue to add other DNS transparent forwarders as required.

3. Click **Apply**.

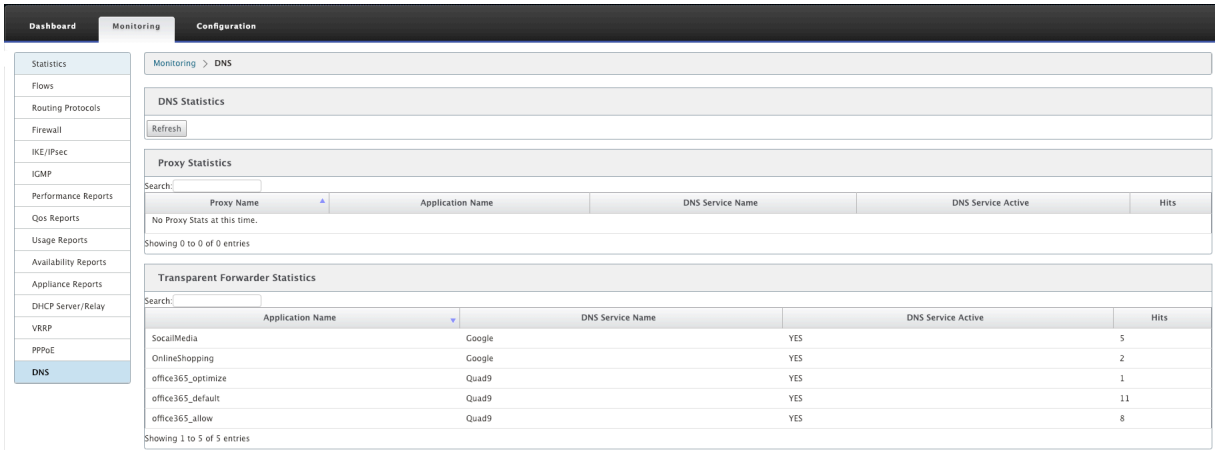
Monitoring

To view Proxy statistics and Transparent forwarder statistics, navigate to **Monitoring > DNS**.
You can view the application name, DNS service name, DNS service status, and the number of hits to the DNS service.

Proxy Statistics



Transparent Forwarder Statistics



DHCP server and DHCP relay

March 12, 2021

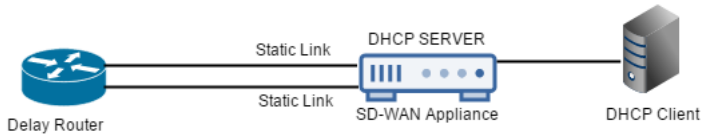
Citrix SD-WAN introduces the ability to use Standard or Premium Edition appliances as either DHCP Servers or DHCP Relay agents. The DHCP server feature allows devices on the same network as the SD-WAN appliance's LAN/WAN interface to obtain their IP configuration from the SD-WAN appliance. The DHCP relay feature allows your SD-WAN appliances to forward DHCP packets between DHCP client and server.

The following are the benefits of using the DHCP server and DHCP relay features:

- Reduce the amount of 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.
- Reduce manual configuration on simple client sites.

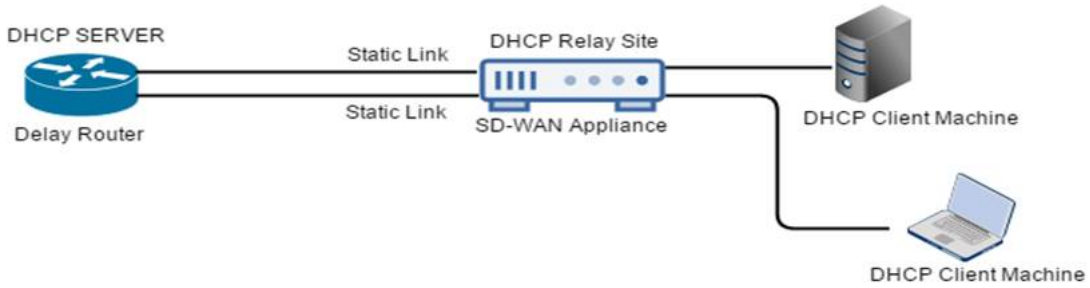
DHCP server

Citrix SD-WAN appliances can be configured as DHCP server. It can assigns and manages IP addresses from specified address pools within the network to DHCP clients. The DHCP server can be configured to assign more 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 forwarded by other DHCP relay agents within the network.



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 of the SD-WAN appliances to relay requests and replies between local DHCP Clients and a remote DHCP Server. It 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.



Configuring DHCP server and DHCP relay

April 14, 2021

Configure DHCP Server and DHCP Relay using the configuration editor

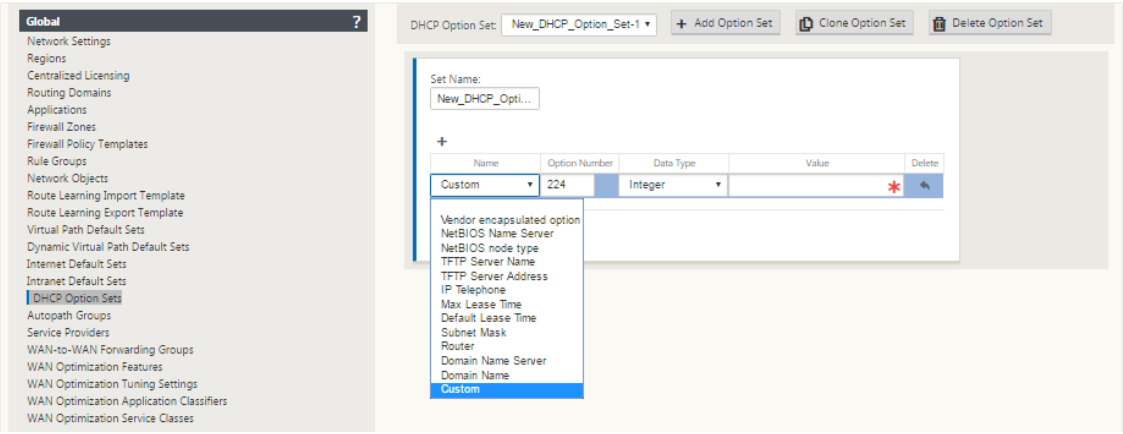
You can configure the DHCP server and DHCP relay settings for the appliances on your network using the configuration editor. The configuration is pushed to the appliances in the SD-WAN network through the change management process.

To configure a site as a DHCP server using the configuration editor:

1. Navigate to **Configuration Editor** > **Sites** > [Site Name] > DHCP > **Server Subnets**. Click **+**.
2. Select a configured Routing Domain, if multiple domains are present.
3. Select the **Virtual interface** to be used to receive the DHCP requests. The IP subnet used by the DHCP server to provides addresses for is auto-populated.

4. Enter the **Domain Name**, **Primary DNS**, and **Secondary DNS**. The DHCP Server forwards this information to the clients.
5. Click **Enable** to enable the subnet.
6. Configure dynamic IP address pools that will be used to allocate IP addresses to clients. Specify the range starting and ending IP address, and select the **Option set**.

> **Note**
>
> The DHCP option sets are groups of DHCP settings that can be applied to individual IP address ranges. To create DHCP option sets, navigate to **Global** > **DHCP Options Sets**. Select the required DHCP options and specify a value for it.



7. Configure individual hosts that require a fixed IP address based on the MAC address. Select the **Fixed IP Address**, **MAC Address**, and **Option Set**.

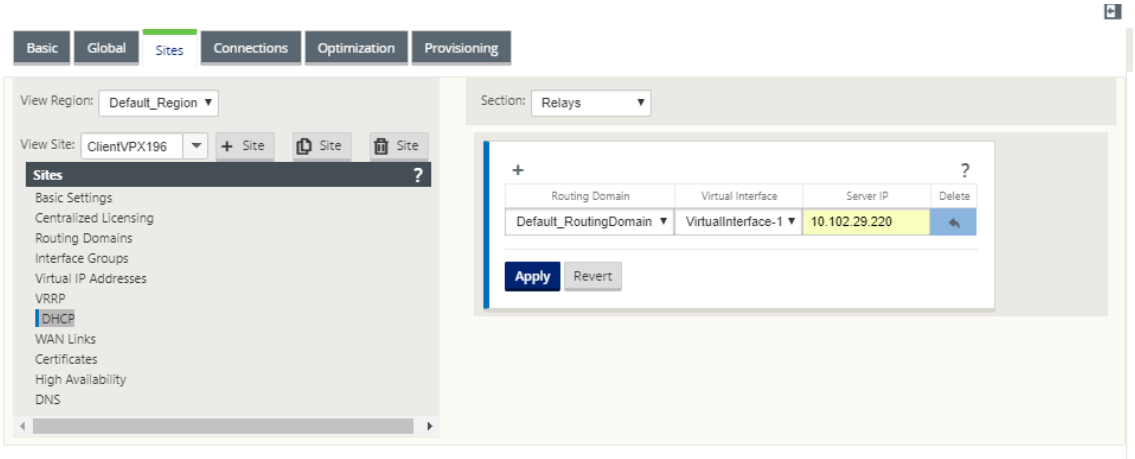
> **Note**
>
> For fixed IP addresses, the **Gateway IP** is set by configuring the **Router** option in the **DHCP option set**.

To configure a site as a DHCP relay using the configuration editor:

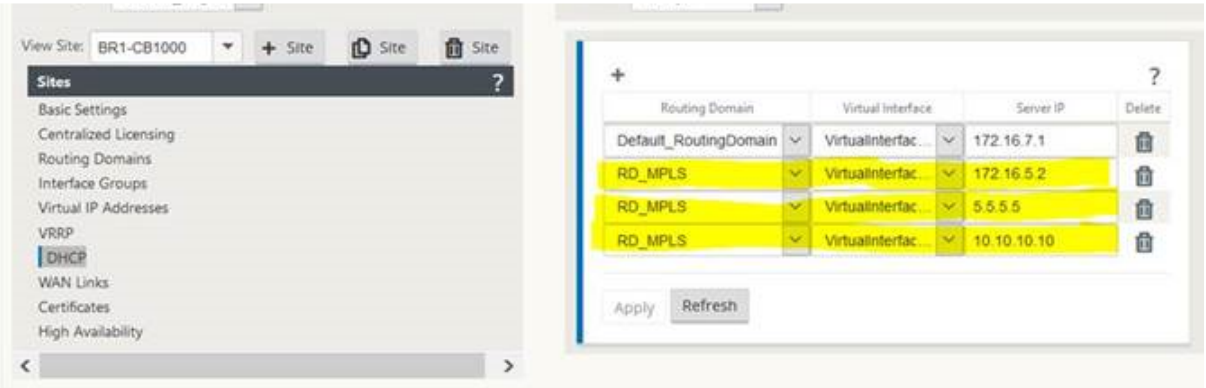
1. Navigate to Configuration **Editor** > **Sites** > [Site Name] > **DHCP** > **Relays**. Click **+**.

> **Note**
>
> You can configure a maximum of 16 DHCP relays.

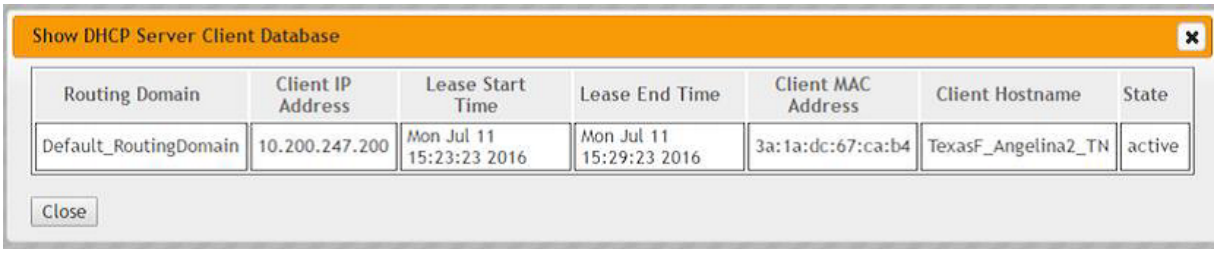
2. Select a configured Routing Domain, if multiple domains are present.
3. Select a Virtual Interface that communicates to a remote DHCP Server.
4. Enter the DHCP Server IP that the relay will use to forward the request and response from the clients.



You can configure a single DHCP Relay using a common Virtual Network Interface and point it to multiple DHCP Servers.



To view a list of Clients from the DHCP Server Database, in the web management interface, navigate to **Monitor** > **DHCP Server/Relay**.



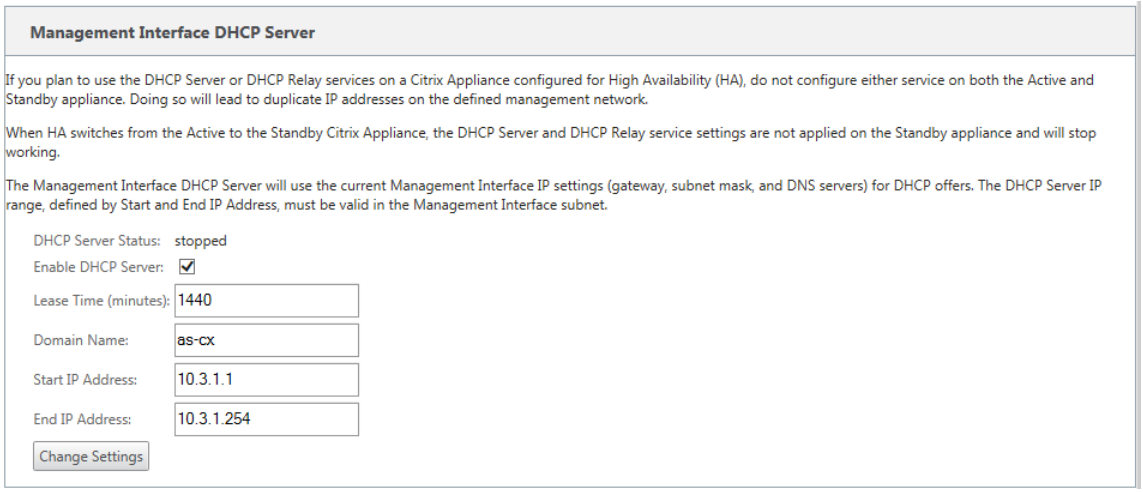
Configuring an SD-WAN appliance as a DHCP server or a DHCP relay using appliance settings

You can manually configure an individual SD-WAN appliance as a DHCP server or a DHCP replay from the appliance settings page.

To enable DHCP server on an SD-WAN appliance:

1. Navigate to **Configuration** > **Appliance Settings** > **Network Adapters**. In the **Network Adapters** page, look for the **Management Interface DHCP Server** pane.
2. Click **Enable DHCP Server** 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.



3. Click **Change Settings** to finish configuring the DHCP Server.

   > **Note**
   >
   > If you plan to use DHCP Server on an SD-WAN appliance configured for High Availability (HA), do not configure the service on both the Active and Standby appliance. Doing so leads to duplicate IP addresses on the defined management network.

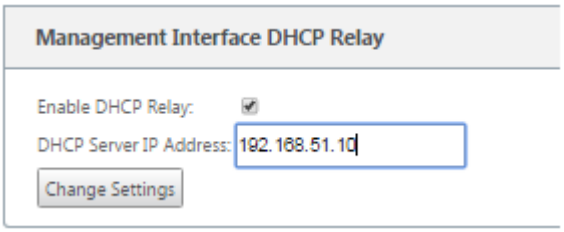
4. Click **Show Client** to view the current DHCP clients, and click **Clear Clients** to release the DHCP Client leases

To enable DHCP relay service on an SD-WAN appliance:

1. Navigate to **Configuration** > **Appliance Settings** > **Network Adapters**. In the **Network Adapters** page, look for the **Management Interface DHCP Relay** pane.

2. Click **Enable DHCP Relay** check box to enable the service. Enter the **DHCP Server IP Address** and click **Change Settings** to begin using your appliance as a DHCP Relay Agent.

> **Note**
>
> If you plan to use the 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 leads to duplicate IP addresses on the defined management network.



WAN link IP address learning through DHCP client

March 12, 2021

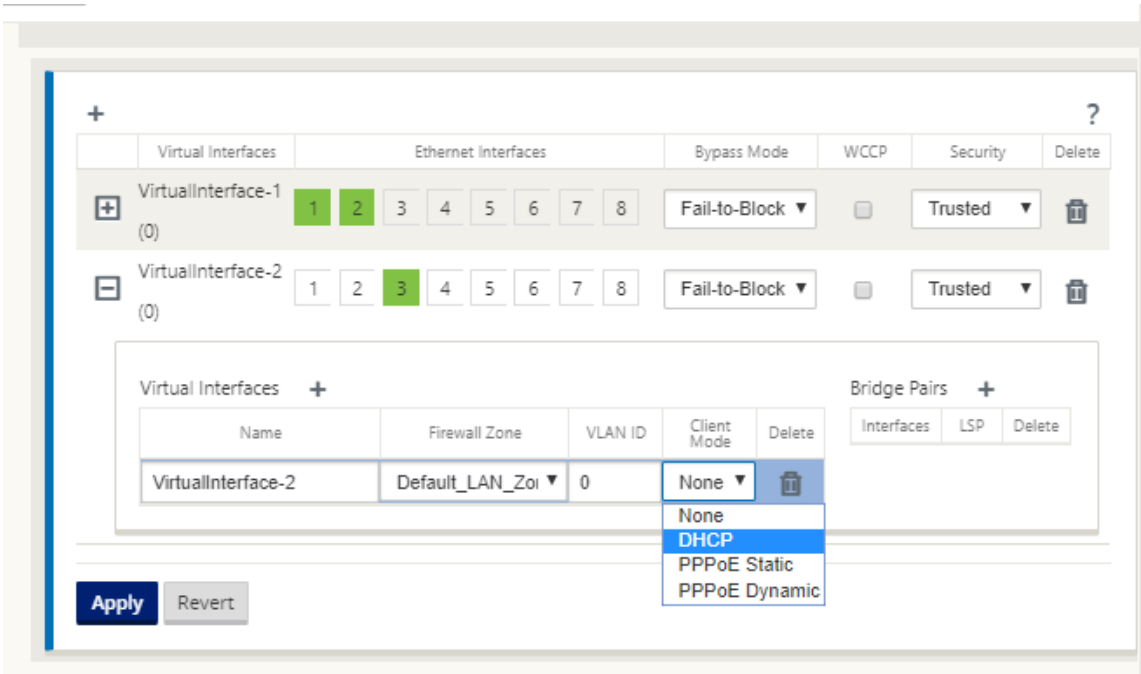
Citrix SD-WAN appliances support WAN Link IP address learning through DHCP Clients. This functionality reduces the amount of manual configuration required to deploy SD-WAN appliances and reduces ISP costs by eliminating the need to purchase static IP addresses. SD-WAN appliances can obtain dynamic IP addresses for WAN Links on untrusted interfaces. This eliminates 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 / non-RCN 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.

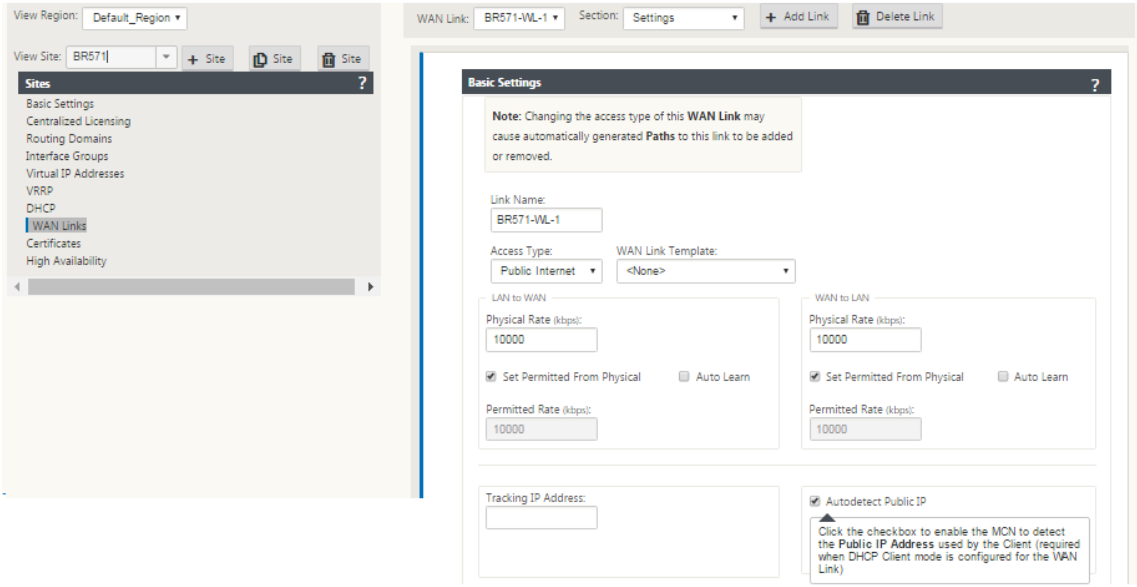
To configure DHCP for an untrusted virtual interface on fail-to-block mode:

1. In the **Configuration Editor**, go to **Sites** > [Site Name] > **Interface Groups** > **Virtual Interfaces**.

> **Note**
>
> The physical interface in the interface group must be a non-bridged pair on a single interface.



2. Select DHCP as the **Client Mode**.
3. Navigate to **WAN Links** > **[WAN Link Name]** > **Settings** > **Basic Settings**.
4. Click the **Autodetect Public IP** check box 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.

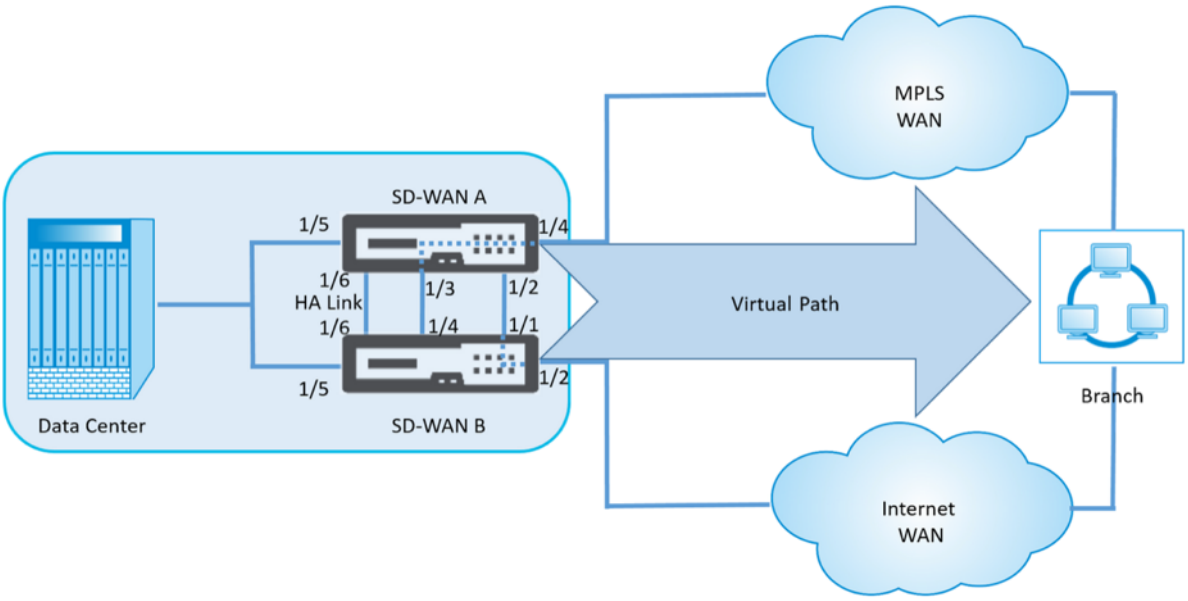


DHCP support on Fail-to-Wire port

Earlier, the DHCP client was only supported on Fail-to-block port. With 11.2.0 release, the DHCP client capability is extended on fail-to-wire port for the branch site with serial High Availability (HA) deployments. This enhancement:

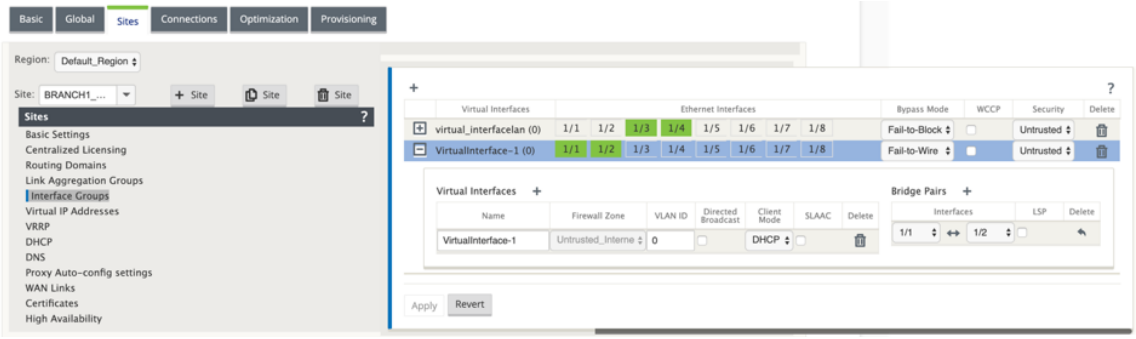
- Allows the DHCP client configuration on untrusted interface group that has fail-to-wire bridge pair and serial HA deployments.
- Allows DHCP interfaces to be selected as part of **Private Intranet WAN links**.

DHCP client is now supported on the private intranet link.



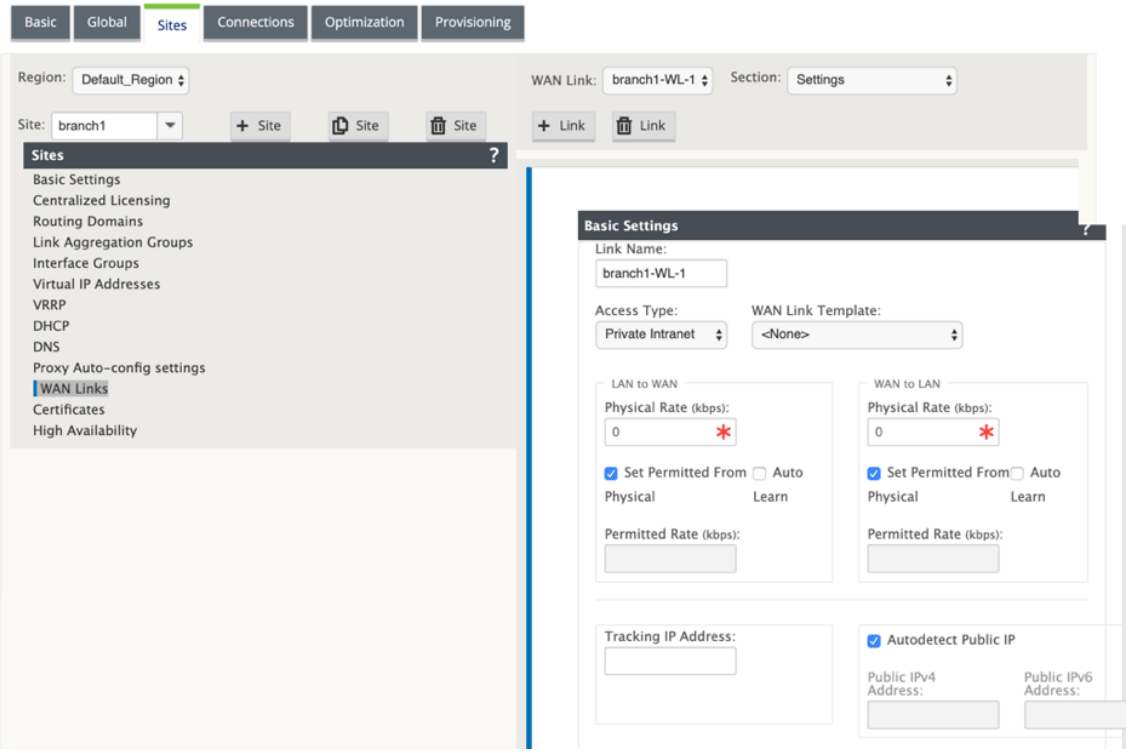
To configure DHCP for an untrusted virtual interface on fail-to-wire mode:

1. In the **Configuration Editor**, go to **Sites > [Site Name] > Interface Groups > Virtual Interfaces**.



2. Select DHCP as the **Client Mode** and add **Bridge Pairs**.
3. Go to **WAN Links >** click **+ >** select **WAN Link Name** from the drop-down list > select **Settings** in the **Section** field **> Basic Settings**.

4. Click the **Autodetect Public IP** check box 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.



> **Note**
>
> A LAN interface must not be connected into the fail-to-wire pair as packets might be bridged between the interfaces.

Monitoring 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 SD-WAN appliance, **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 issues 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	Submit
X2	VLAN350	SFWL4-Inter	10.20.20.53/24	10.20.20.2	86400	71035	4:29 on 1/9/2016	Renew	Submit

Dynamic PAC file customization

March 12, 2021

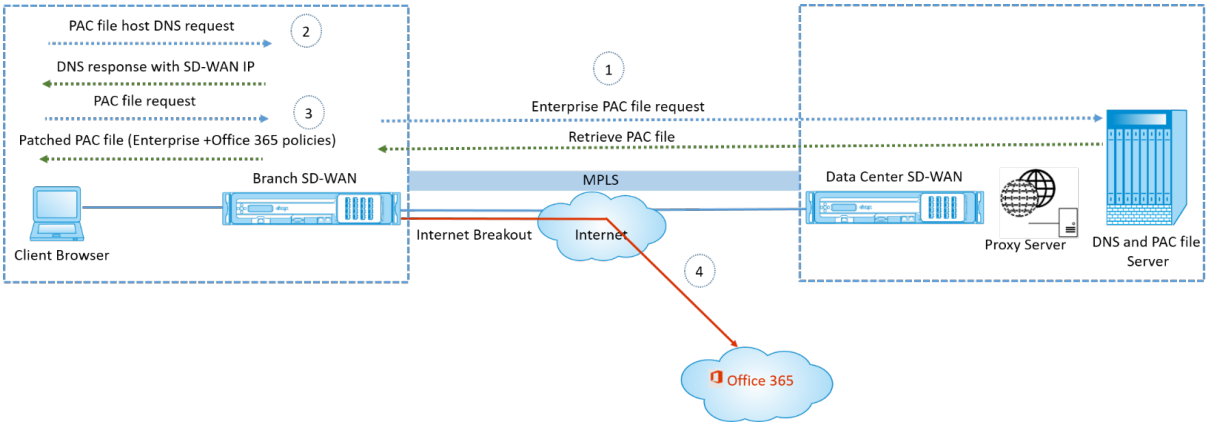
With the increase in enterprise adoption of mission-critical SaaS applications and distributed workforce, it becomes highly critical to reduce latency and congestion. Latency and congestion are inherent in traditional methods of backhauling traffic through the Data Center. Citrix SD-WAN allows direct internet break out of SaaS applications such as Office 365. For more information, see Office 365 Optimization.

If there are explicit web proxies configured on the enterprise deployment all traffic are steered to the web proxy making it difficult for classification and direct internet breakout. The solution is to exclude SaaS application traffic from getting proxied by customizing the enterprise PAC (Proxy Auto-Config) file.

Citrix SD-WAN 11.0 allows proxy bypass and local Internet breakout for Office 365 application traffic by dynamically generating and serving custom PAC file. PAC file is a JavaScript function that defines whether web browser requests go directly to the destination or to a web proxy server.

How PAC file customization works

Ideally, the enterprise network host PAC file on the internal web server, these proxy settings are distributed via group policy. The Client browser requests for PAC files from the enterprise web server. The Citrix SD-WAN appliance serves the customized PAC files for sites where Office 365 breakout is enabled.



1. Citrix SD-WAN periodically requests and retrieves the latest copy of the enterprise PAC file from the enterprise web server. The Citrix SD-WAN appliance patches office 365 URLs to the enterprise PAC file. The enterprise PAC file is expected to have a placeholder (SD-WAN specific tag) where the Office 365 URLs are seamlessly patched.
2. The Client browser raises a DNS request for enterprise PAC file host. Citrix SD-WAN intercepts the request for the proxy configuration file FQDN and responds with the Citrix SD-WAN VIP.
3. The Client browser requests for the PAC file. Citrix SD-WAN appliance serves the patched PAC file locally. The PAC file includes enterprise proxy configuration and Office 365 URL exclusion policies.
4. On receiving a request for Office 365 application, the Citrix SD-WAN appliance performs a direct internet breakout.

Prerequisites

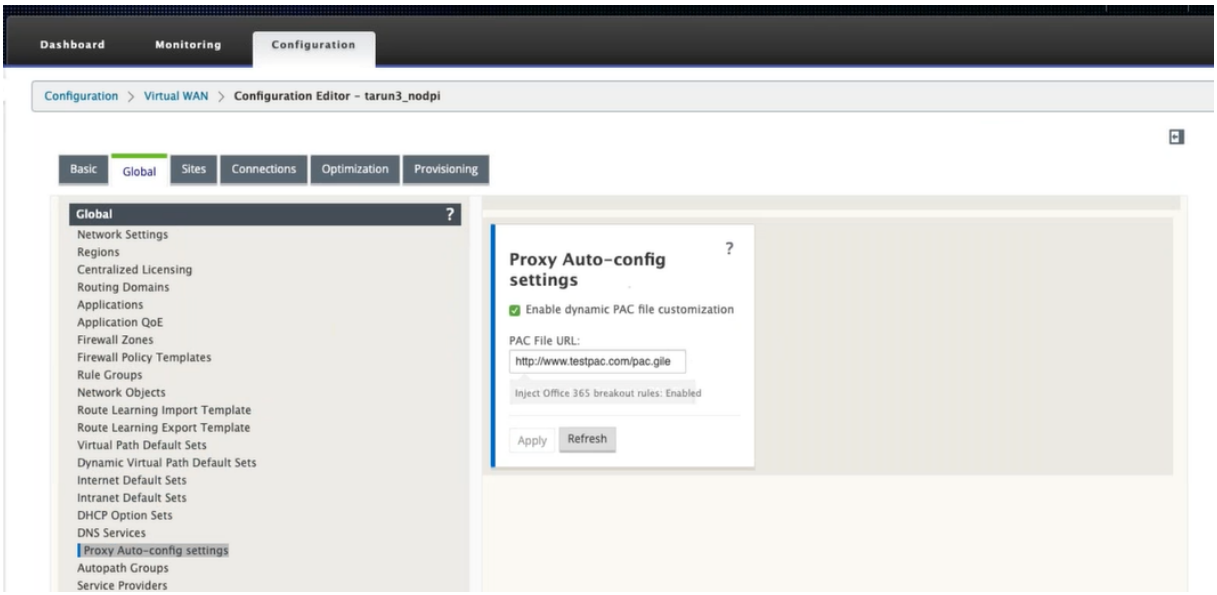
1. The enterprises should have a PAC file hosted.
2. The PAC file should have a placeholder *SDWAN_TAG* or one occurrence of *findproxyforurl* function for patching Office 365 URLs.
3. The PAC file URL should be domain based and not IP based.
4. The PAC file is served only over the trusted identity VIPs.
5. Citrix SD-WAN appliance should be able to download enterprise PAC file over its management interface.

Configure PAC file customization

You can enable PAC file customization globally or at site level.

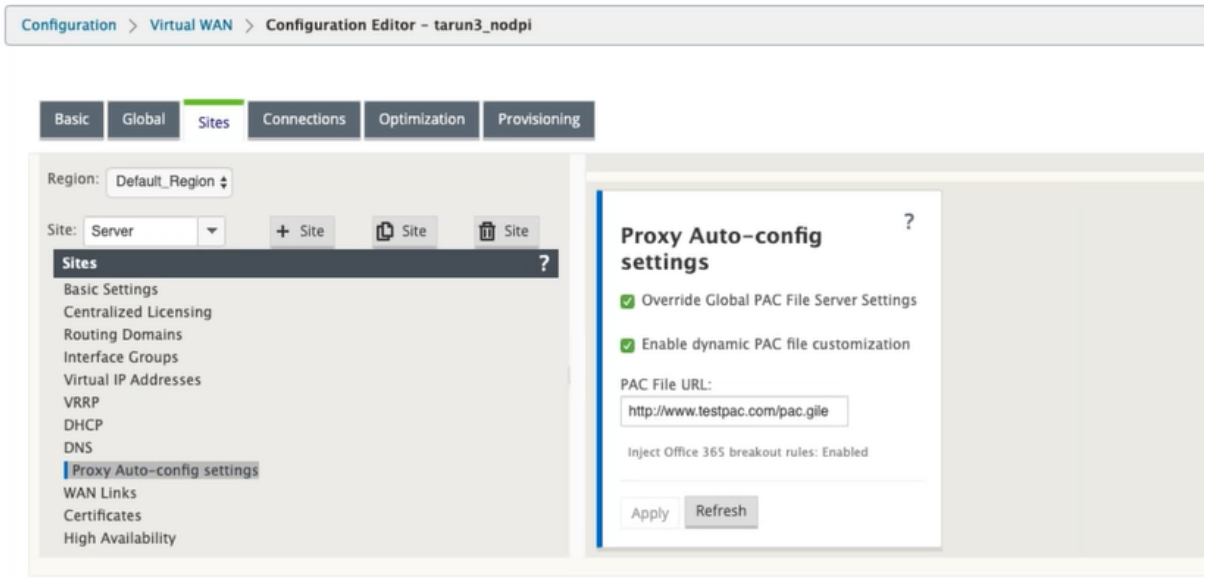
> **Note**
>
> The Office 365 breakout option must be enabled for dynamic PAC file customization. For information on how to enable Office 365 breakout, see Office 365 Optimization.

To configure dynamic PAC file customization globally for all sites, in the configuration editor navigate to **Global** > **Proxy Auto-config settings**.



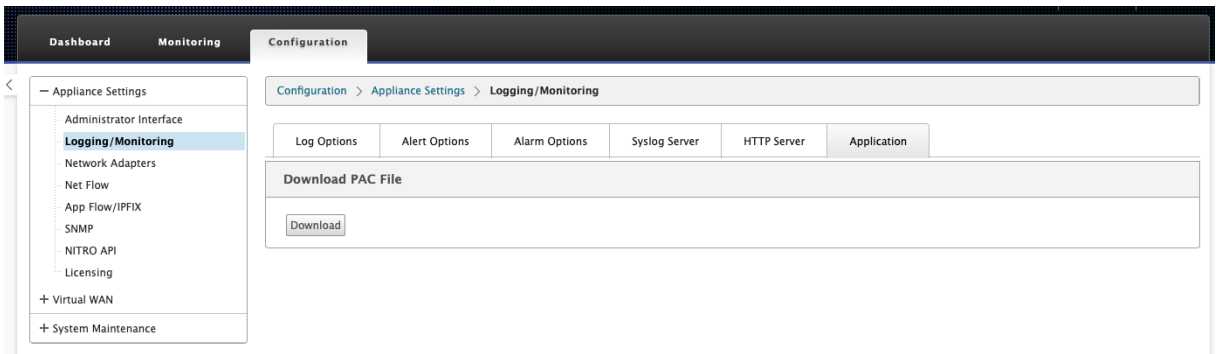
Select **Enable dynamic PAC file customization**. In the **PAC file URL** field, enter the URL of the enterprise PAC file server. The Office 365 breakout rules are dynamically patched to the enterprise PAC file.

To configure dynamic PAC file customization for a site, navigate to **Sites** > [Site] > **Proxy Auto-config settings**. You can also choose to override global PAC file server settings, and specify a different PAC file server URL.

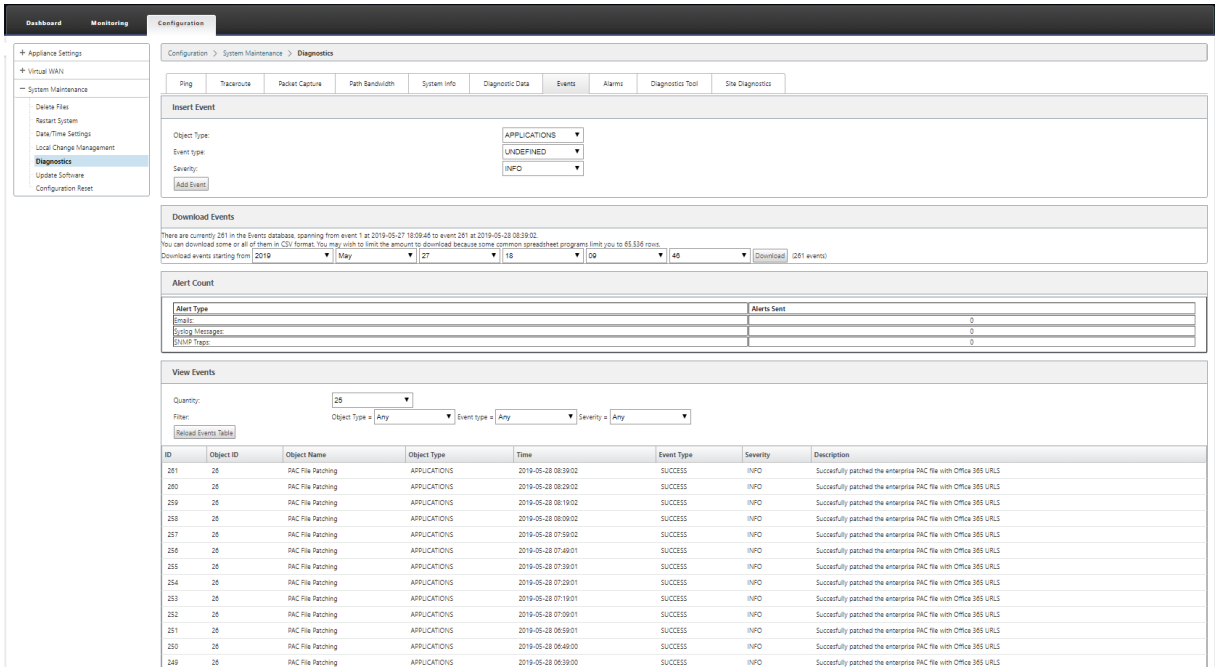


Troubleshooting

You can download the customized PAC file from the Citrix SD-WAN appliance for troubleshooting. Navigate to **Configuration** > **Appliance Settings** > **Logging/Monitoring** > **Application and click Download**.



You can also view the PAC file patching status in the **Events** section, navigate to **Configuration** > **System Maintenance** > **Diagnostics**, click **Events** tab.



Limitations

- HTTPS PAC file server requests are not supported.
- Multiple PAC files in a network are not supported, including PAC files for routing domains or security zones.
- Generating PAC file on Citrix SD-WAN from scratch is not supported.
- WPAD through DHCP is not supported.

GRE tunnel

March 12, 2021

The GRE Tunnel feature allows you to configure Citrix SD-WAN Appliances to terminate GRE tunnels on the LAN or Intranet. 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:

Continuing in the **Sites** view for the new MCN site, click **+** to the left of the **GRE Tunnels** label. The **GRE Tunnels** table for the new site opens. See the GRE topics for more information.

Configuring GRE Tunnels the MCN Site.

Configuring GRE Tunnels for the Branch Site.

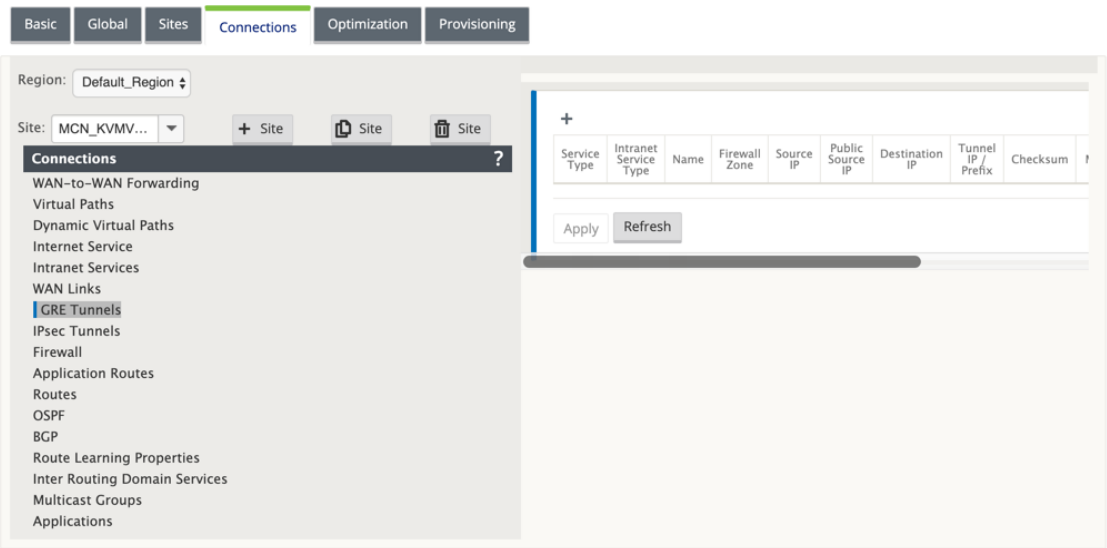
Configure GRE Tunnels for the MCN Site (Optional)

May 28, 2021

The GRE Tunnel feature allows you to configure Citrix SD-WAN appliances to terminate GRE tunnels on the LAN or Intranet. 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:

   - **Service Type** - Choose the service type either Intranet or LAN from the drop-down list.
   - **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 name for the new GRE tunnel or accept the default.
  - Default uses a naming format **Appliance-Tunnel-<number>** - Where *<number>* is the number of GRE Tunnels configured for this site, incremented by one.

- **Intranet Service Type** - For an Intranet service type, choose **Default** or **ZScaler** from the drop-down list.
- **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 are the list of Virtual Interfaces configured for this site. 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 IP address to be used as the source address for packets in the GRE tunnel. The source IP address is the starting point of the GRE tunnel.
  - **Destination IP** –Enter the IP address to be used as the host destination. The destination IP address is the ending point of the GRE tunnel.
  - **Tunnel IP / Prefix** – Enter the IP Address and prefix used for the GRE tunnel interface.
  - **Checksum** – Select the **Checksum** box to enable Checksum for the tunnel GRE header.
  - **Keepalive Period** –Enter the wait time interval (in seconds) between keepalive messages. If configured to 0, no keepalive packets are sent, but the tunnel remains up. The default is 10.
  - **Keepalive Retries** – Enter the number of keepalive retries the Virtual WAN Appliance must 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.

5. To configure more GRE Tunnels, click **+** to the right of the **GRE Tunnels**, and proceed as per the preceding steps.

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

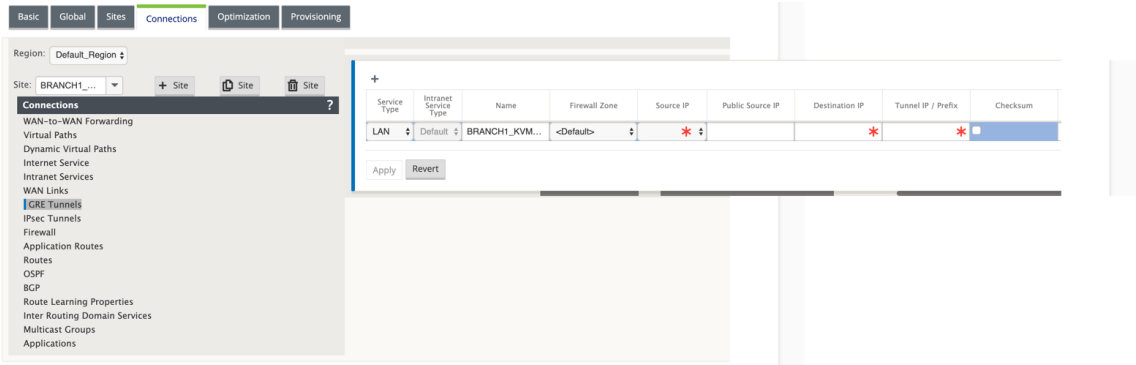
Configure GRE Tunnels for a Branch Site

May 28, 2021

The GRE Tunnel feature allows you to configure Citrix SD-WAN Appliances to terminate GRE tunnels on the LAN or Intranet. 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:

1. Continuing in the connections view for the new branch site, click **GRE Tunnels**. The **GRE Tunnels** view for the new site opens.
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:
   - **Service Type** - Choose the service type either Intranet or LAN from the drop-down list.
   - **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 name for the new GRE tunnel or accept the default.
     - Default uses a naming format **Appliance-Tunnel-<number>** - Where <*number*> is the number of GRE Tunnels configured for this site, incremented by one.
   - **Intranet Service Type** - For an Intranet service type, choose **Default** or **ZScaler** from the drop-down list.
   - **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 are the list of Virtual IP Addresses that you configured for this site.

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 IP address to be used as the source address for packets in the GRE tunnel. The source IP address is the starting point of the GRE tunnel.
- **Destination IP** –Enter the IP address to be used as the host destination. The destination IP address is the ending point of the GRE tunnel.
- **Tunnel IP / Prefix** – Enter the IP Address and prefix used for the GRE tunnel interface.
- **Checksum** – Select the **Checksum** box to enable Checksum for the tunnel GRE header.
- **Keepalive Periods** –Enter the wait time interval (in seconds) between keepalive messages. If configured to 0, no keepalive packets are sent, but the tunnel remains up. The default is 10.
- **Keepalive Retries** – Enter the number of keepalive retries the Virtual WAN Appliance must 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.

5. To configure more GRE Tunnels, click **+** to the right of the **GRE Tunnels** label, and proceed as per the preceding steps.

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

In-band and backup management

April 26, 2021

In-band management

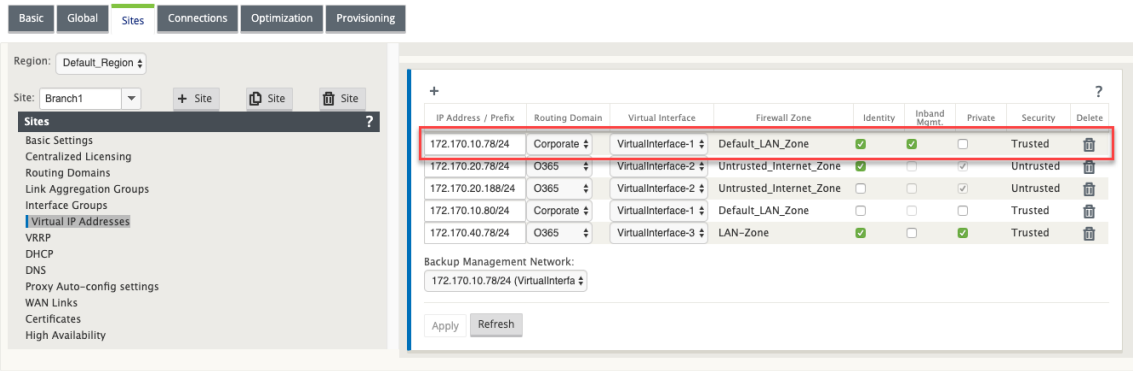
Citrix SD-WAN allows you to manage the SD-WAN appliance in two ways, out-of-band management and in-band management. Out-of-band management allows you to create a management IP using a port reserved for management, which carries management traffic only. In-band management allows you to use the SD-WAN data ports for management. It carries both data and management traffic, without having to configure an addition management path.

In-band management allows virtual IP addresses to connect to management services such as web UI and SSH. You can enable In-band management on multiple trusted interfaces that are enabled to be used for IP services. You can access the web UI and SSH using the management IP and in-band virtual IPs.

To enable in-band management on a virtual IP:

1. In the configuration editor navigate to **Sites** > **Virtual IP Addresses**.
2. Select **Inband Mgmt** for the virtual IPs for which you want to enable in-band management.

   > **Note:**
   >
   > Ensure that the interface security type is **Trusted** and **Identity** is enabled.



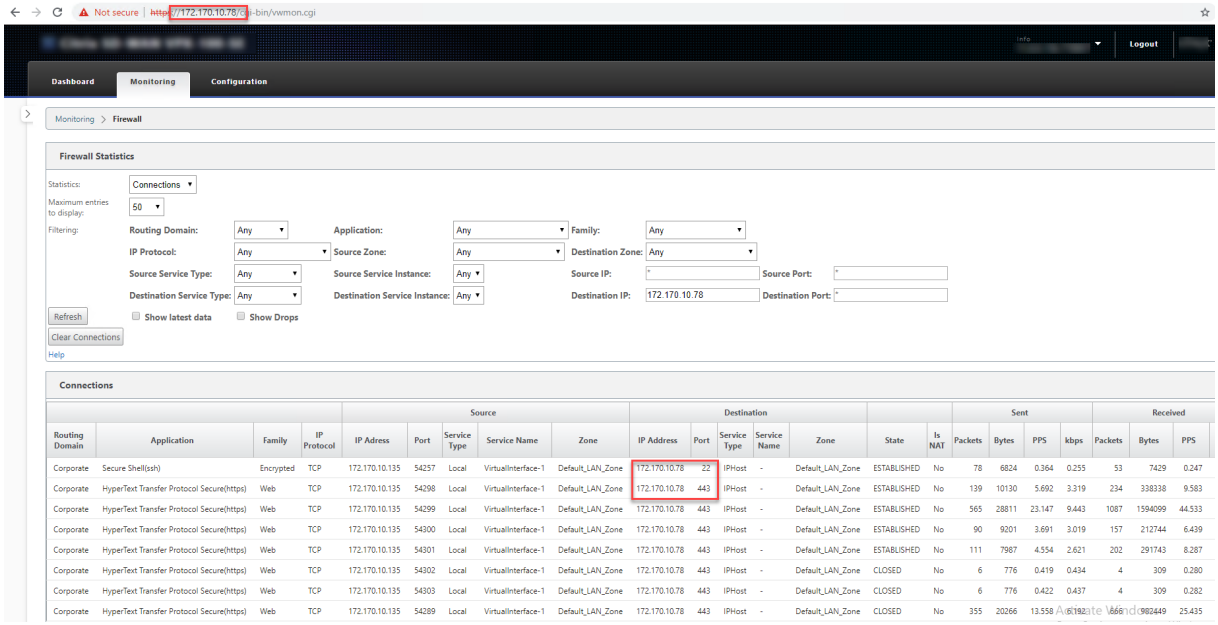
3. Click **Apply**

For detailed procedure on configuring virtual IP address, see How to configure virtual IP.

Monitoring in-band management

In the preceding example, we have enabled in-band management on 172.170.10.78 virtual IP. You can use this IP to access the web UI and SSH.

In the web UI navigate to **Monitoring** > **Firewall**. You can see SSH and web UI accessed using the virtual IP on port 22 and 443 respectively in the **Destination IP address** column.



In-band provisioning

The need to deploy SD-WAN appliances in simpler environments like home or small branches has increased significantly. Configuring separate management access for simpler deployments is an added overhead. Zero-touch deployment (ZTD) along with in-band management feature enables provisioning and configuration management via designated data ports. ZTD is now supported on the designated data ports and there is no need to use a separate management port for ZTD. Citrix SD-WAN also allows to fail over management traffic seamlessly to the management port when the data port goes down and vice versa.

An appliance in factory shipped state, that supports in-band provisioning, can be provisioned by simply connecting the data or management port to the internet. The appliances that support in-band provisioning have specific ports for LAN and WAN. The appliance in factory reset state has a default configuration that allows to establish a connection with the zero-touch deployment service. The LAN port acts as the DHCP server and assigns a dynamic IP to the WAN port that acts as a DHCP client. The WAN links monitor the Quad 9 DNS service to determine WAN connectivity.

> **Note**
>
> In-band provisioning is applicable to SD-WAN 110 SE and SD-WAN VPX platforms only.

Once the IP address is obtained and a connection is established with the zero-touch deployment service the configuration packages are downloaded and installed on the appliance. For information on zero-touch deployment through SD-WAN Center, see Zero Touch Deployment. For information on zero-touch deployment through SD-WAN Orchestrator see, Zero Touch Deployment.

Note: For day-0 provisioning of SD-WAN appliances through the data ports, the appliance software version should be SD-WAN 11.1.0 or higher.

The default configuration of an appliance in factory reset state includes the following configurations:

- DHCP Server on LAN port
- DHCP client on WAN port
- QUAD9 configuration for DNS
- Default LAN IP is 192.168.0.1
- Grace License of 35 days.

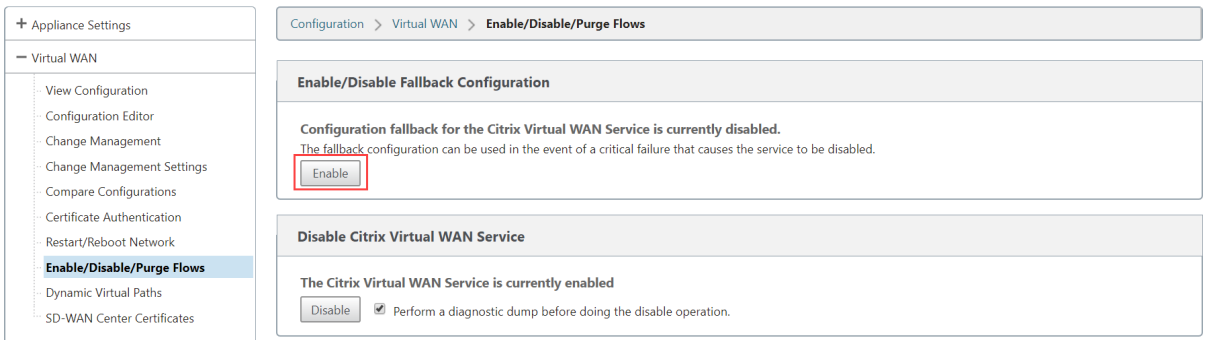
Once the appliance is provisioned, the default configuration is disabled and is overridden by the configuration received from the zero-touch deployment service. If an appliance license or grace license expiries, the default configuration is activated, to ensure that the appliance remains connected to the zero-touch deployment service and receives licenses managed via zero-touch deployment.

Fallback Configuration

Fallback configuration ensures that the appliance remains connected to the zero-touch deployment service if there is link failure, configuration mismatch, or software mismatch. Fallback configuration is enabled by default on the appliances that have a default configuration profile. You can also edit the fallback configuration as per your existing LAN network settings.

Note: After the initial appliance provisioning, ensure that the fallback configuration is enabled for zero-touch deployment service connectivity.

If the fall back configuration is disabled, you can enable it by navigating to **Configuration** > **Virtual WAN** > **Enable /Disable/Purge Flows** > **Enable/Disable Fallback Configuration** and clicking **Enable**.



To customize the fallback configuration as per your LAN network:

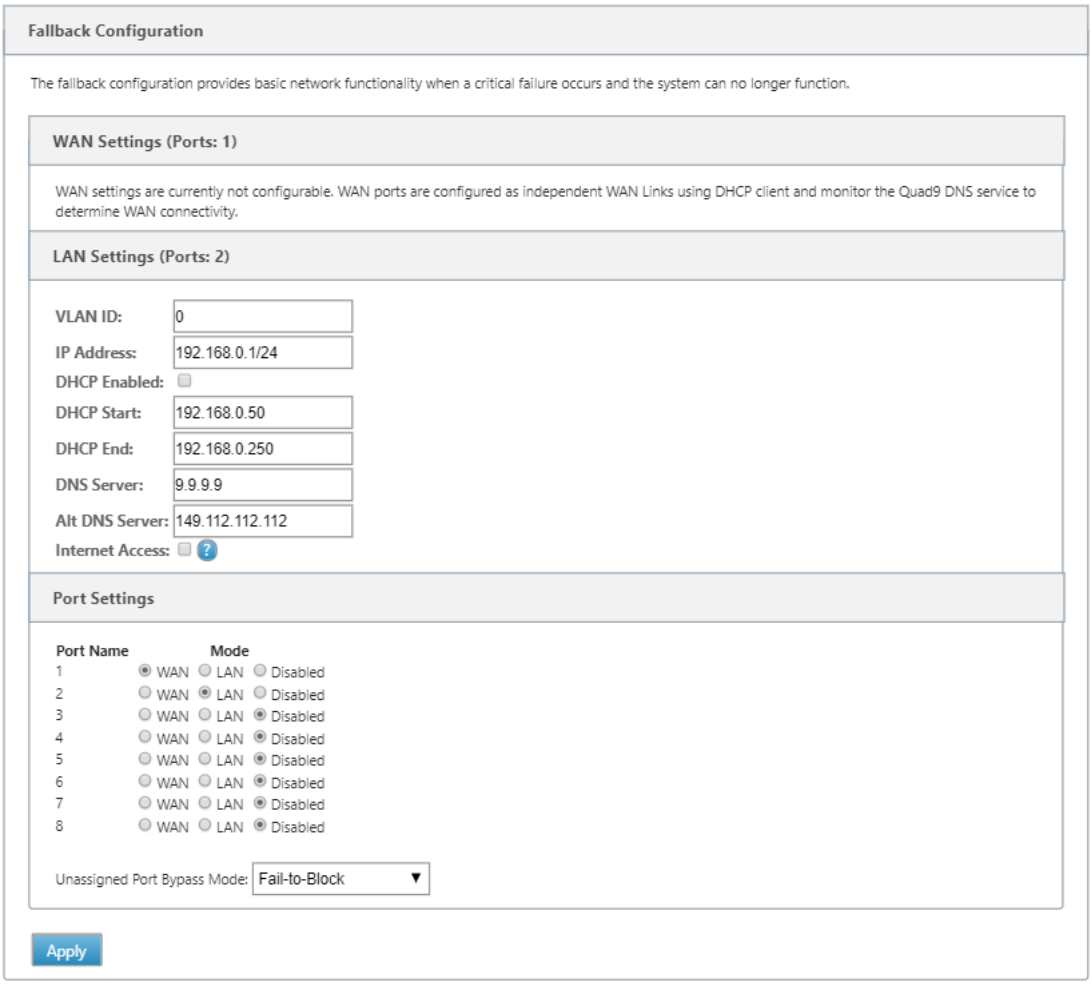
1. Navigate to **Configuration** > **Appliance Settings** > **Fallback Configuration**.

2. Edit values for the following LAN settings as per your network requirements. This is the minimum configuration required to establish a connection with the zero-touch deployment service.

   - **VLAN ID**: The VLAN ID to which the LAN port must be grouped.
   - **IP Address**: The virtual IP address assigned to the LAN port.
   - **DHCP Enabled**: Enables the LAN port as the DHCP server. The DHCP server assigns dynamic IP addresses to the clients on the LAN port.
   - **DHCP Start and DHCP End**: The range of IP addresses which DHCP uses to dynamically assign an IP to the clients on the LAN port.
   - **DNS Server**: The IP address of the primary DNS server.
   - **Alt DNS Server**: The IP address of the secondary DNS server.
   - **Internet Access**: Permit internet access to all LAN clients without other filtering.

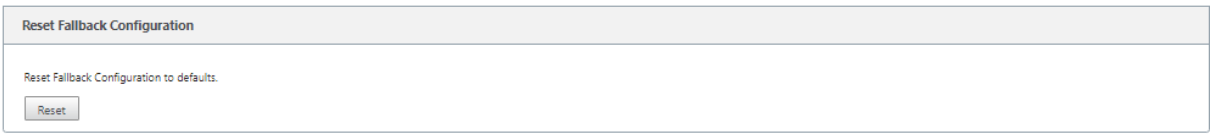
   The following table provides the details of pre-designated WAN and LAN ports for fallback configuration on different platforms:

Platform	WAN Ports	LAN Ports
110	1/2	1/1
110-LTE	1/2, LTE-1	1/1
210	1/4, 1/5	1/3
210-LTE	1/4, 1/5, LTE-1	1/3
VPX	2	1
410	1/4, 1/5, 1/6	1/3 (FTB)
1100	1/4, 1/5, 1/6	1/3 (FTB)



3. Configure the mode for each port. The port can either be LAN port or WAN port or can be disabled. The ports displayed depend on the appliance model. Also, set the port bypass mode to **Fail-to-Block** or **Fail-to-wire**.

To reset the fallback configuration to default configuration at any time, click **Reset**.



Configurable Management or Data port

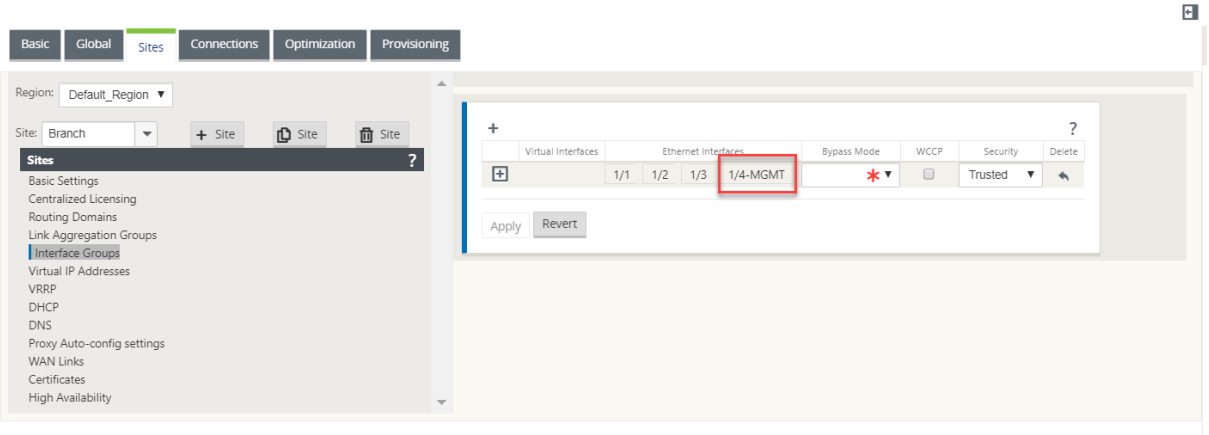
In-band management allows the data ports to carry both data and management traffic, eliminating the need for a dedicated management port. This leaves the management port unused on the low end appliances, which already have low port density. Citrix SD-WAN allows you to configure the management port to operate as either a data port or a management port.

> **Note**
>
> You can convert the management port to data port only on the following platforms.
>
> - Citrix SD-WAN 110 SE/LTE
> - Citrix SD-WAN 210 SE/LTE

On the configuration editor, use the management port in your configuration. After the configuration is activated, the management port is converted to a data port.

> **Note**
>
> You can configure a management port only when in-band management is enabled on other trusted interfaces on the appliance.

To configure a management interface, in the configuration editor navigate to **Sites**, select a site and click **Interface Groups**. The MGMT interface is available to be configured. For more information on configuring interface groups, see How to configure interface groups.



To reconfigure the management port to perform management functionality, remove the configuration. Create a configuration without using the management port and activate it.

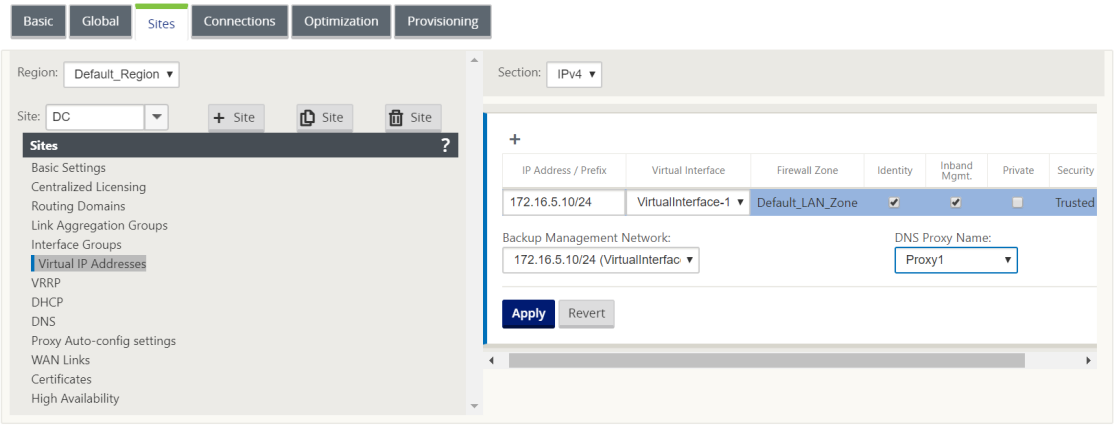
Backup management network

You can configure a virtual IP address as a back-up management network. It is used as the management IP address if the management port is not configured with a default gateway.

> **Note**
>
> If a site has internet service configured with a single routing domain, a trusted interface with identity enabled is selected as the backup management network by default.

To select a virtual IP as a backup management network:

1. In the configuration editor navigate to **Sites** > **Virtual IP Addresses**.
2. Select a virtual IP address as a backup management network.



3. Select the DNS Proxy to which all DNS requests over the in-band and backup management plane is forwarded to.

> **Note**
>
> DNS proxy can be selected only when both In-band Management and Backup Management Network are enabled for a virtual IP.

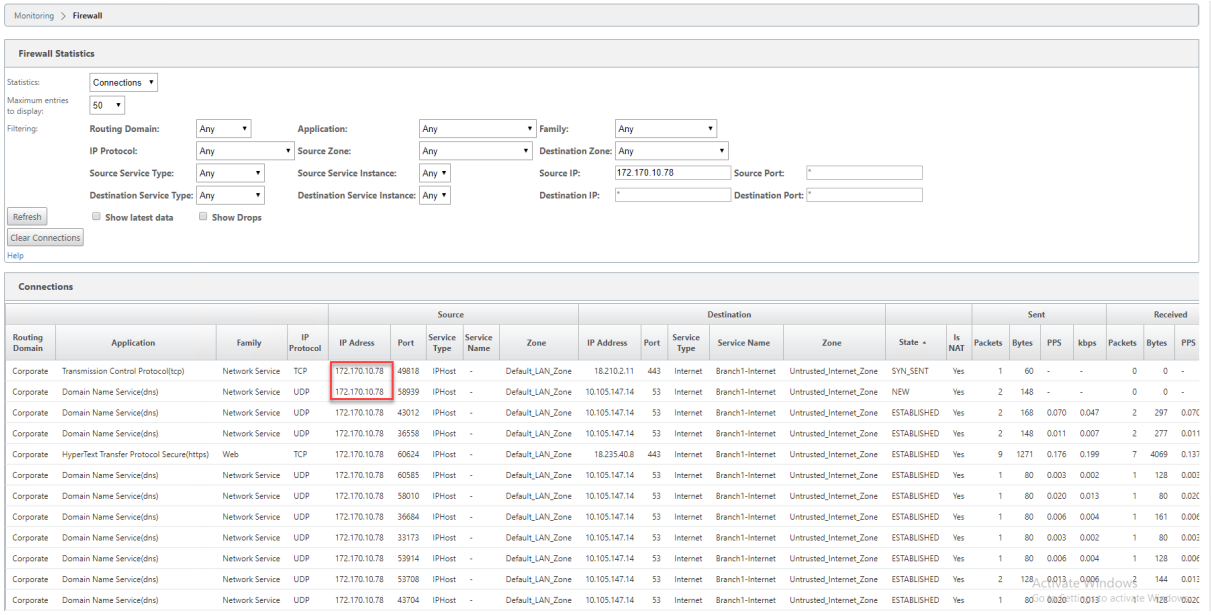
4. Click **Apply**.

For detailed procedure on configuring virtual IP address, see How to configure virtual IP address

Monitoring backup management

In the preceding example, we have selected 172.170.10.78 virtual IP as the backup management network. If the management IP address is not configured with a default gateway, you can use this IP to access the web UI and SSH.

In the web UI navigate to **Monitoring** > **Firewall**. You can see this virtual IP address as the source IP address for SSH and web UI access.



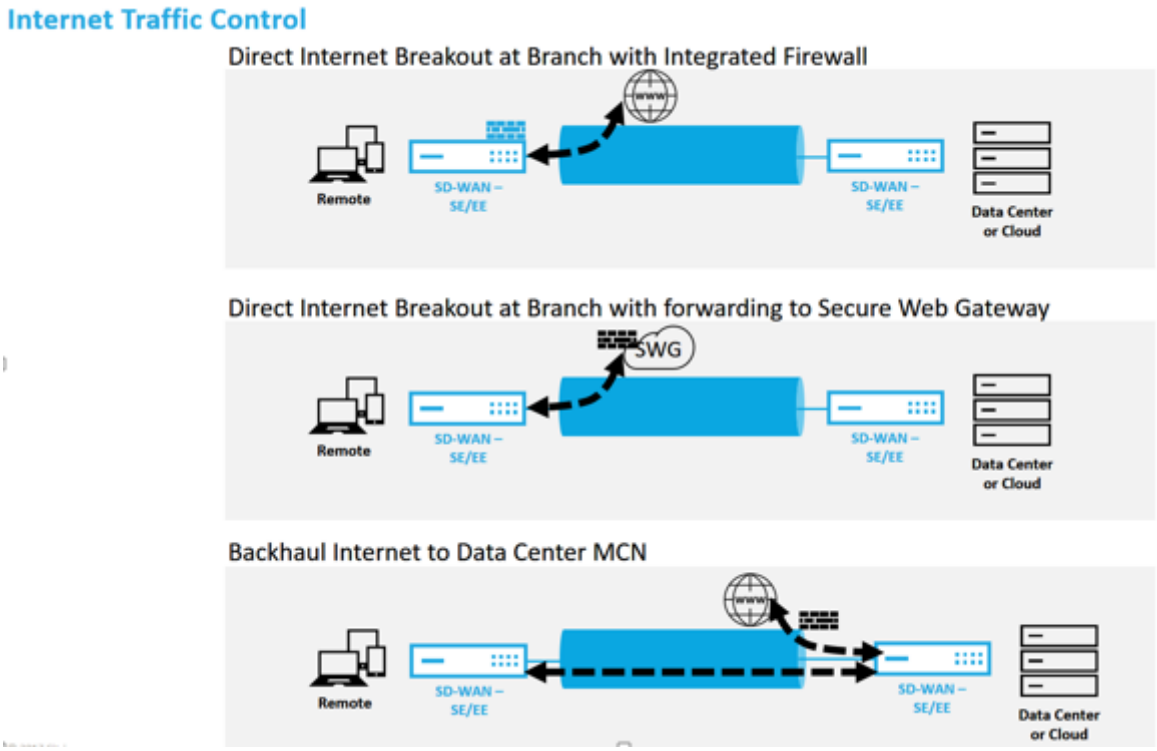
Internet access

March 12, 2021

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 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 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 using multiple Internet WAN links, or optionally, utilizing the Internet WAN links in a primary or secondary configuration.

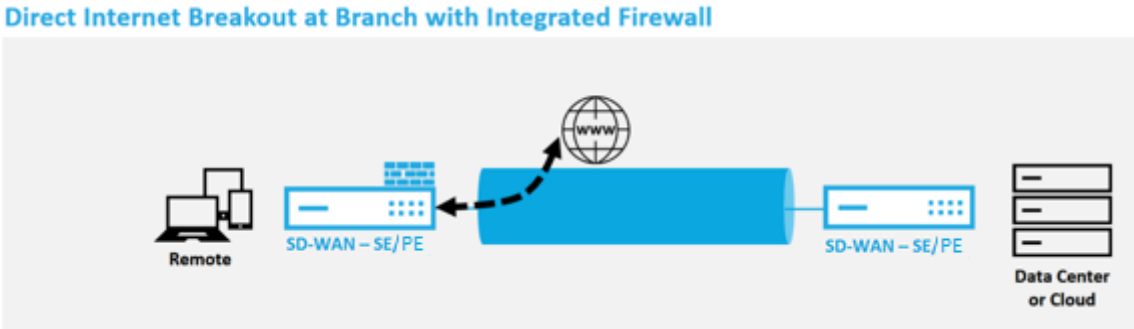
Internet traffic control using the Internet Service on SD-WAN appliances can be configured in the following deployment modes:

- Direct Internet Breakout at Branch with Integrated Firewall
- Direct Internet Breakout at Branch forwarding to Secure Web Gateway
- Backhaul Internet to Data Center MCN



Direct Internet Breakout at Branch with Integrated Firewall

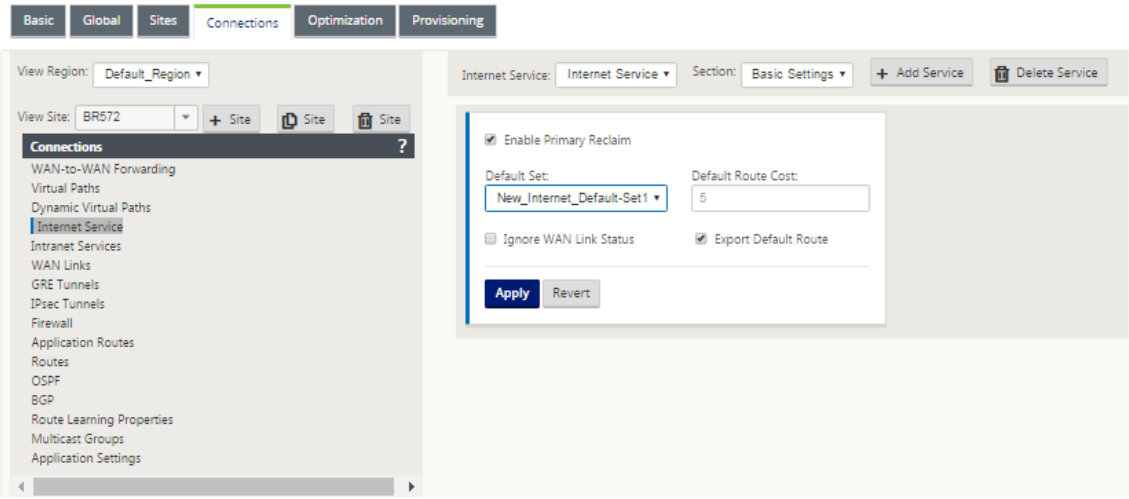
March 12, 2021



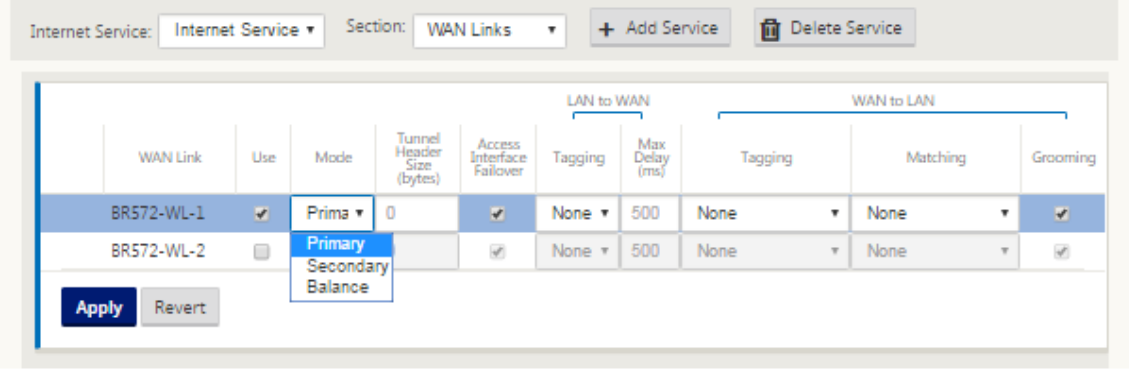
Perform the following steps to enable Internet Service for any site (Client node or MCN):

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

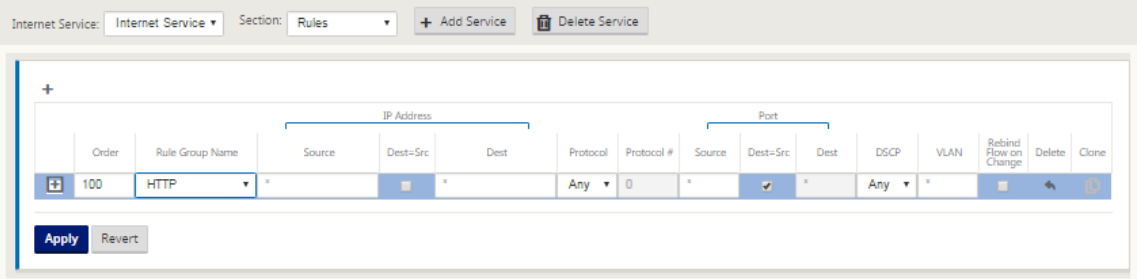
without having to configure each node separately.



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.

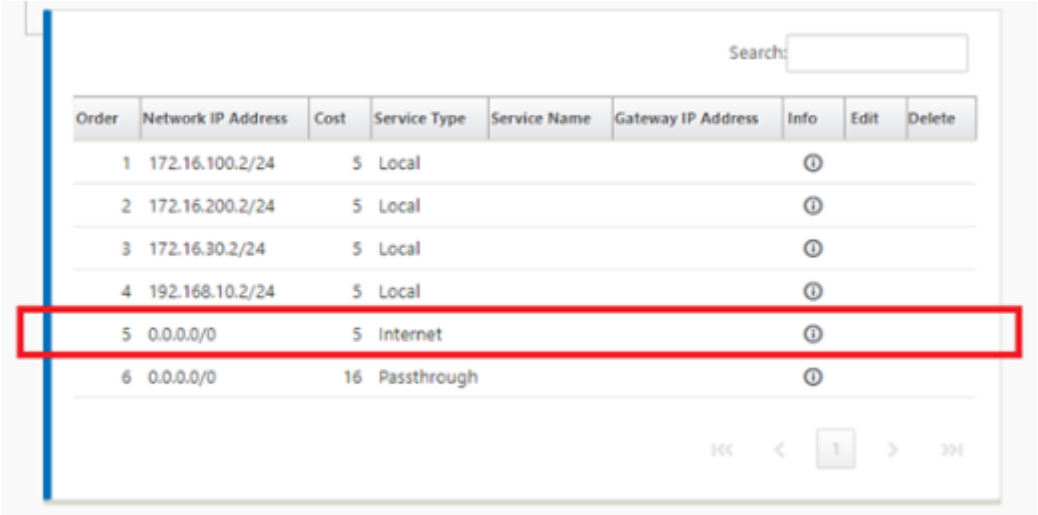


4. Site node specific Rules are available, enabling the capability of customization of each site uniquely overriding any general settings configured in the global default set. Modes include desired delivery over a specific WAN link, or as an Override Service allowing for passthrough or discard of the filtered traffic.

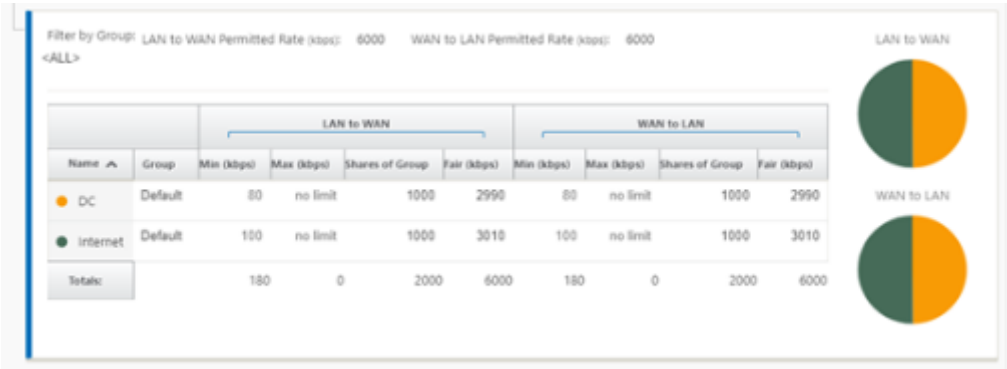


As an Internet Service is created for a node, the Route table for that particular node is auto-

matically 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.



The Internet Service can be utilized in the various deployment modes supported by Citrix SD-WAN.

- Inline Deployment Mode (SD-WAN Overlay)

Citrix 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

Citrix 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.

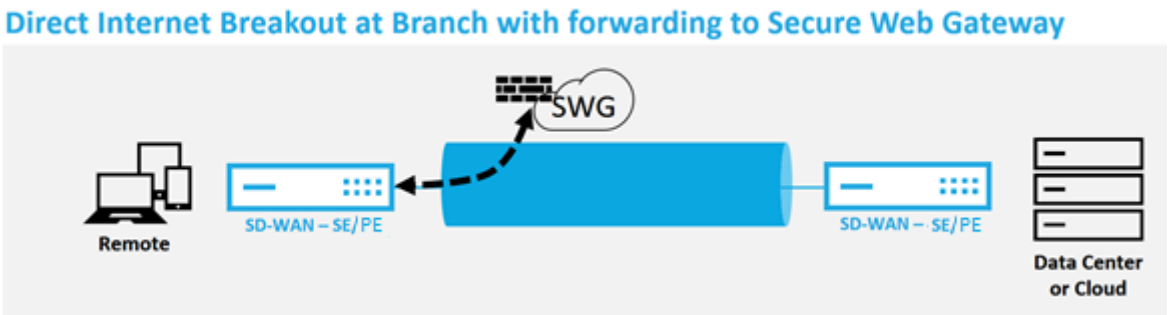
Direct Internet Access with Secure Web Gateway

August 6, 2021

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 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 many 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 using Citrix SD-WAN to the Secure Web Gateway Service. A third-party Secure Web Gateway Service enables granular and central security policy creation to be using 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 more costly security appliances to the network.



Citrix SD-WAN supports the following third party Secure Web Gateway solutions:

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

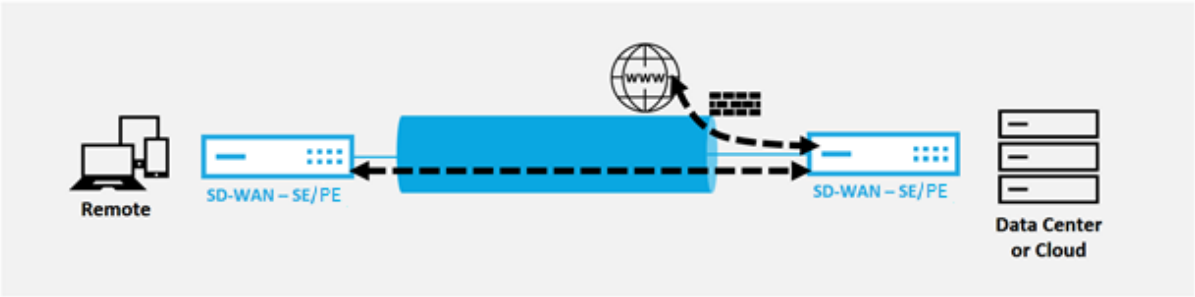
Backhaul Internet

March 12, 2021

The Citrix SD-WAN solution can backhaul Internet traffic to the MCN site or other branch sites. Backhaul indicates that the traffic destined for the Internet is sent back through another predefined site that can access the Internet. It is useful for networks that do not allow Internet access directly because of security concerns or the underlay networks topology. An example would be a remote site that lacks an external firewall where the on-board 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 might be the best 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 for the data center.
- Backhaul of internet traffic consumes bandwidth on the Virtual Path and is accounted for in sizing of WAN links.
- Backhaul of internet traffic might over-subscribe the Internet WAN link at the Data Center.

Backhaul Internet to Data Center MCN



All Citrix SD-WAN devices can terminate up to eight distinct Internet WAN links into a single device. Licensed throughput capabilities for the aggregated WAN links are listed per respective appliance on the Citrix SD-WAN data sheet.

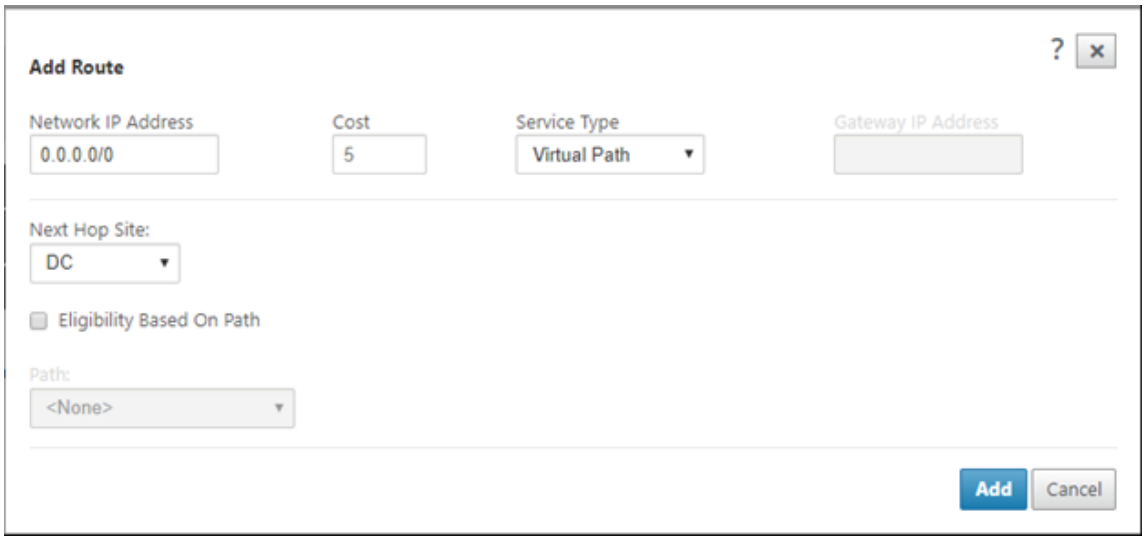
The Citrix SD-WAN solution supports the backhaul of internet traffic with the following configuration.

1. Enable Internet Service at the MCN site node, or any other site note where Internet Service is desired.

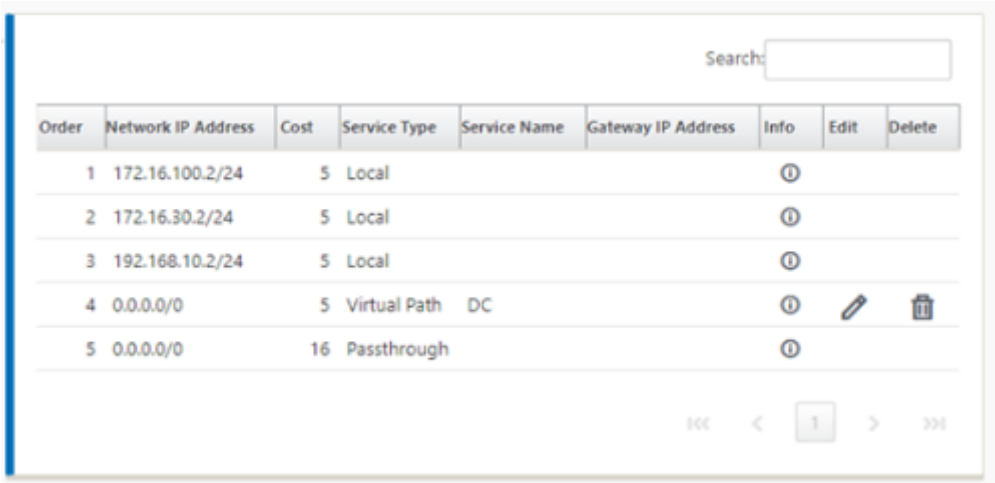
   > **Note**
   >
   > Enable Internet Service and Export routes if all other sites are in the WAN to WAN forward-

> ing group.

2. On the branch nodes where internet traffic is backhauled, manually add a 0.0.0.0/0 route to direct all default traffic to the Virtual Path Service. The next hop is denoted as the MCN, or intermediary site.



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.



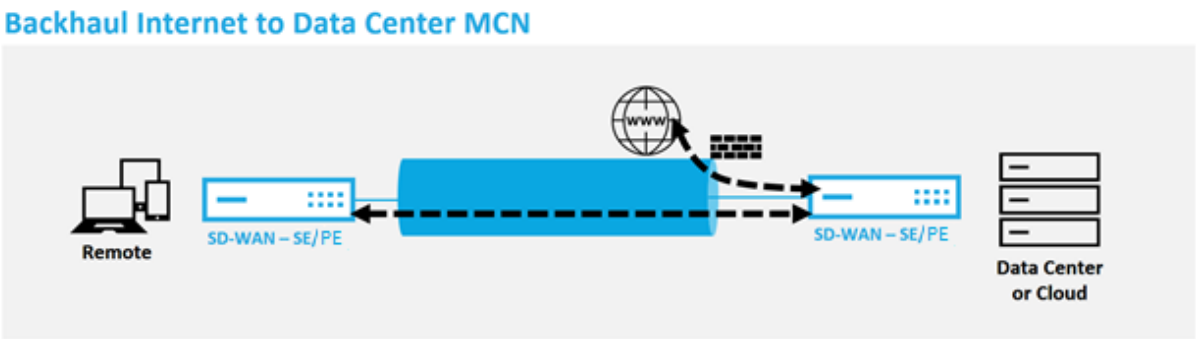
Hairpin Mode

March 12, 2021

With 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 slower traffic. You

can apply 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 more efficient deployment process and more streamlined technical implementation. You can 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 do 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.

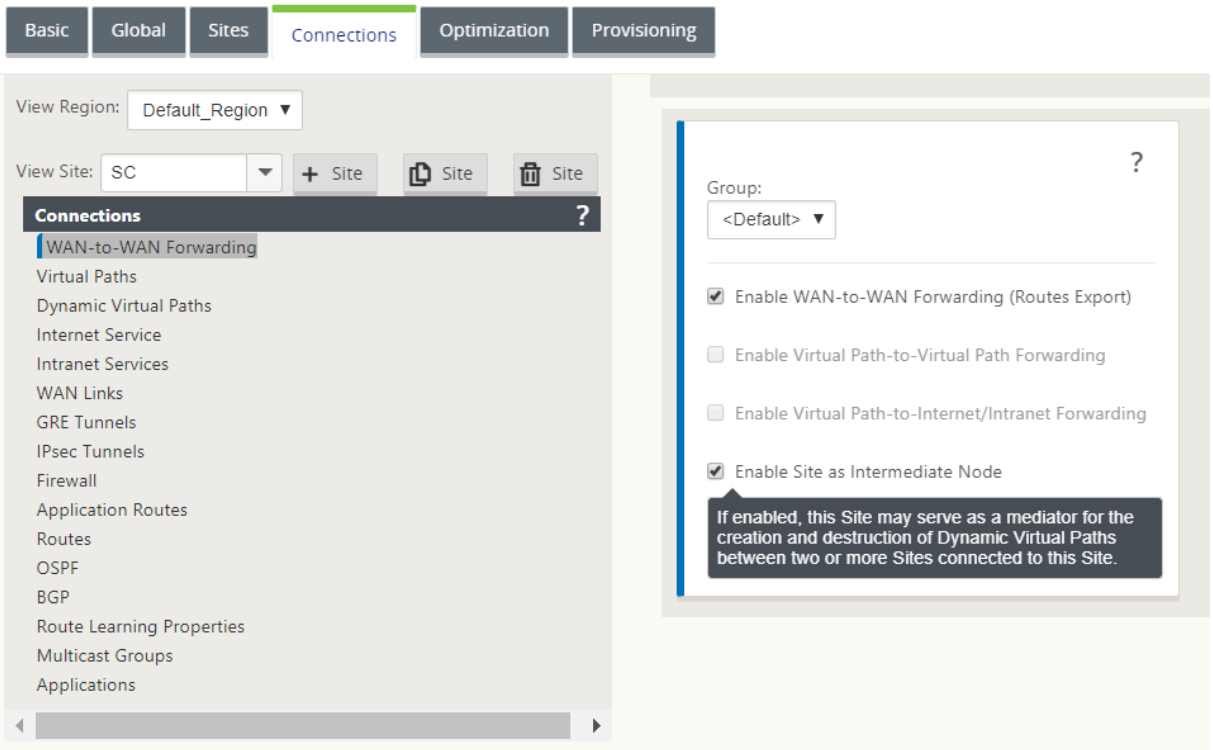
WAN-to-WAN Forwarding and Hairpin deployment have certain differences, namely:

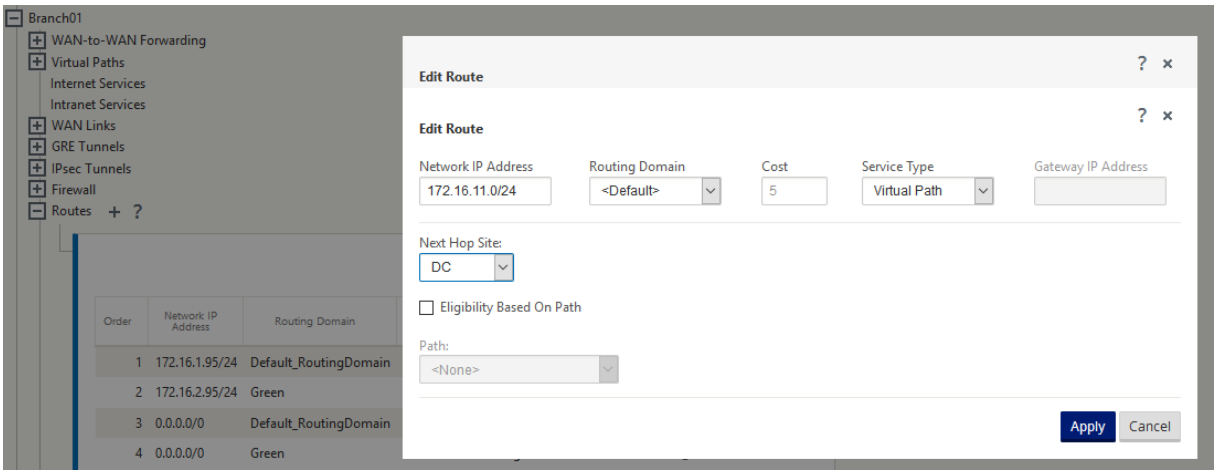
1. Dynamic Virtual Paths are not configured. Always, the intermediate site sees all the traffic between the two sites.
2. Does not participate in WAN-to-WAN Forwarding groups.

   WAN-to-WAN Forwarding and Hairpin deployment are mutually exclusive. Only one of them can be configured at any given point in time.

   Citrix SD-WAN SE/PE 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 Citrix SD-WAN web management interface from the configuration editor.





Hosted firewalls

March 12, 2021

Currently Citrix SD-WAN supports the following hosted firewalls:

- Palo Alto Networks
- Check Point

Palo Alto Networks firewall integration on SD-WAN 1100 platform

March 12, 2021

Citrix SD-WAN supports hosting Palo Alto Networks Next-Generation Virtual Machine (VM)-Series Firewall on the SD-WAN 1100 platform. The following are the supported virtual machine models:

- VM 50
- VM 100

The Palo Alto Network virtual machine series firewall runs as a virtual machine on SD-WAN 1100 platform. The firewall virtual machine is integrated in **Virtual Wire** mode with two data virtual interfaces connected to it. Required traffic can be redirected to the firewall virtual machine by configuring policies on SD-WAN.

Benefits

The following are the primary goals or benefits of Palo Alto Networks integration on the SD-WAN 1100 platform:

- Branch device consolidation: A single appliance that does both SD-WAN and advanced security
- Branch office security with on-prem NGFW (Next Generation Firewall) to protect LAN-to-LAN, LAN-to-Internet, and Internet-to-LAN traffic

Configuration steps

The following configurations are needed to integrate the Palo Alto Networks virtual machine on SD-WAN:

- Provision the Firewall Virtual Machine
- Enable traffic redirection to Security Virtual Machine

> **Note**
>
> Firewall virtual machine must be provisioned first before enabling the traffic redirection.

Provisioning Palo Alto Network virtual machine

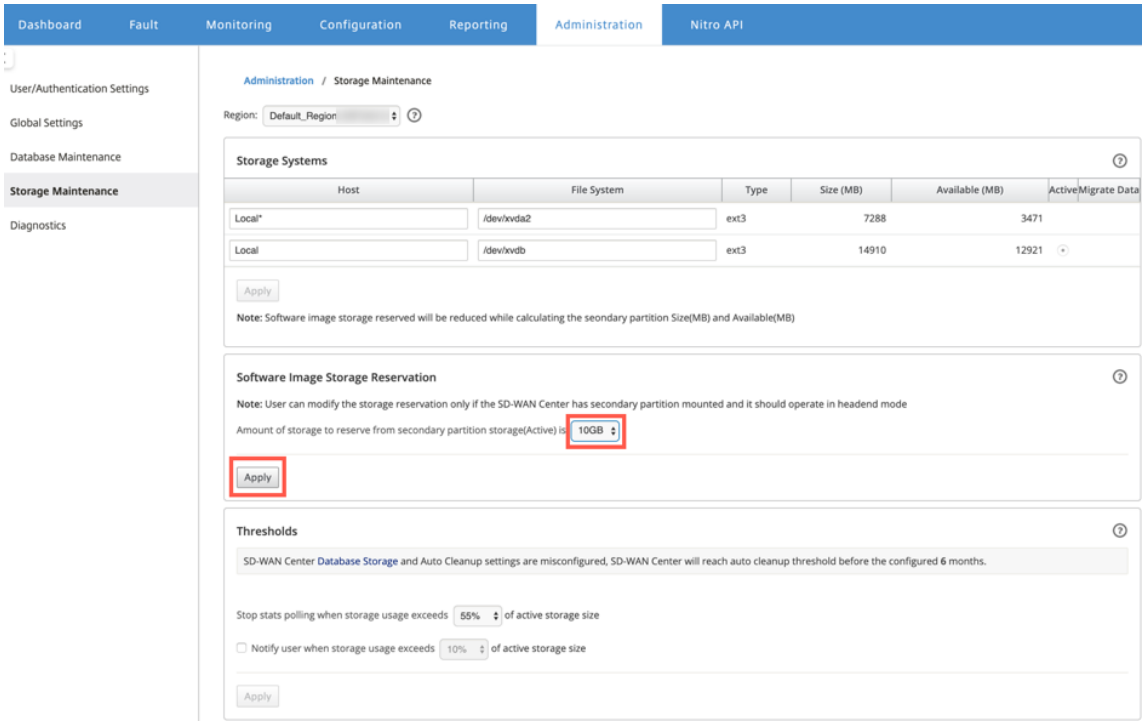
There are two ways to provision the firewall virtual machine:

- Provisioning through SD-WAN Center
- Provisioning through SD-WAN appliance GUI

Firewall virtual machine provisioning through SD-WAN Center

Prerequisites

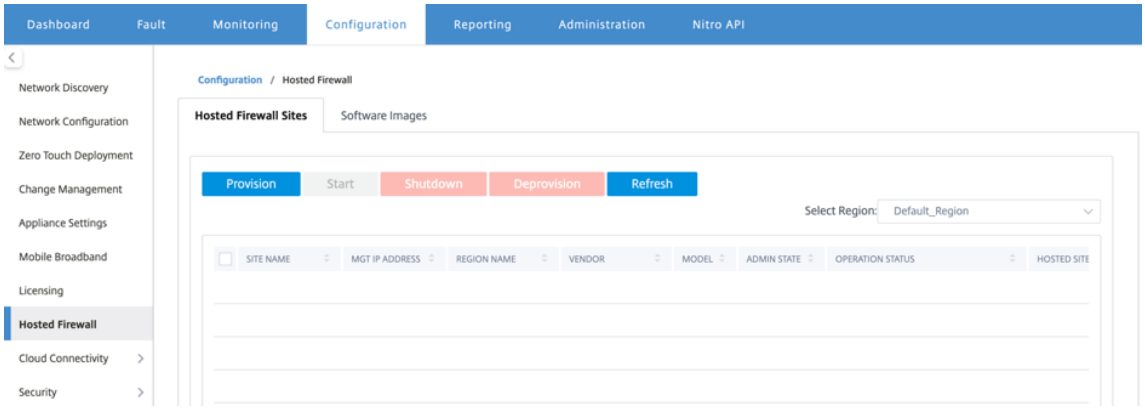
- Add the secondary storage to SD-WAN Center to store the Firewall VM image files. For more information, see System requirements and installation.
- Reserve the storage from the secondary partition for the Firewall VM image files. To configure the storage limit, navigate to **Administration > Storage Maintenance**.
  - Select the required storage amount from the list.
  - Click **Apply**.



> **Note**
>
> Storage is reserved from the secondary partition which is active if the condition is met.

Perform the following steps for provisioning the firewall virtual machine through SD-WAN Center platform:

1. From Citrix SD-WAN Center GUI, navigate to **Configuration >** select **Hosted Firewall**.



You can select the **Region** from the drop-down list to view the provisioned site details for that selected region.

2. Upload the software image.

> **Note**
>
> Ensure that you have enough disk space to upload the software image.

Navigate to **Configuration > Hosted Firewall > Software Images** and select the Vendor name as Palo Alto Networks from the drop-down list. Click or drop the software image file in the box to upload.

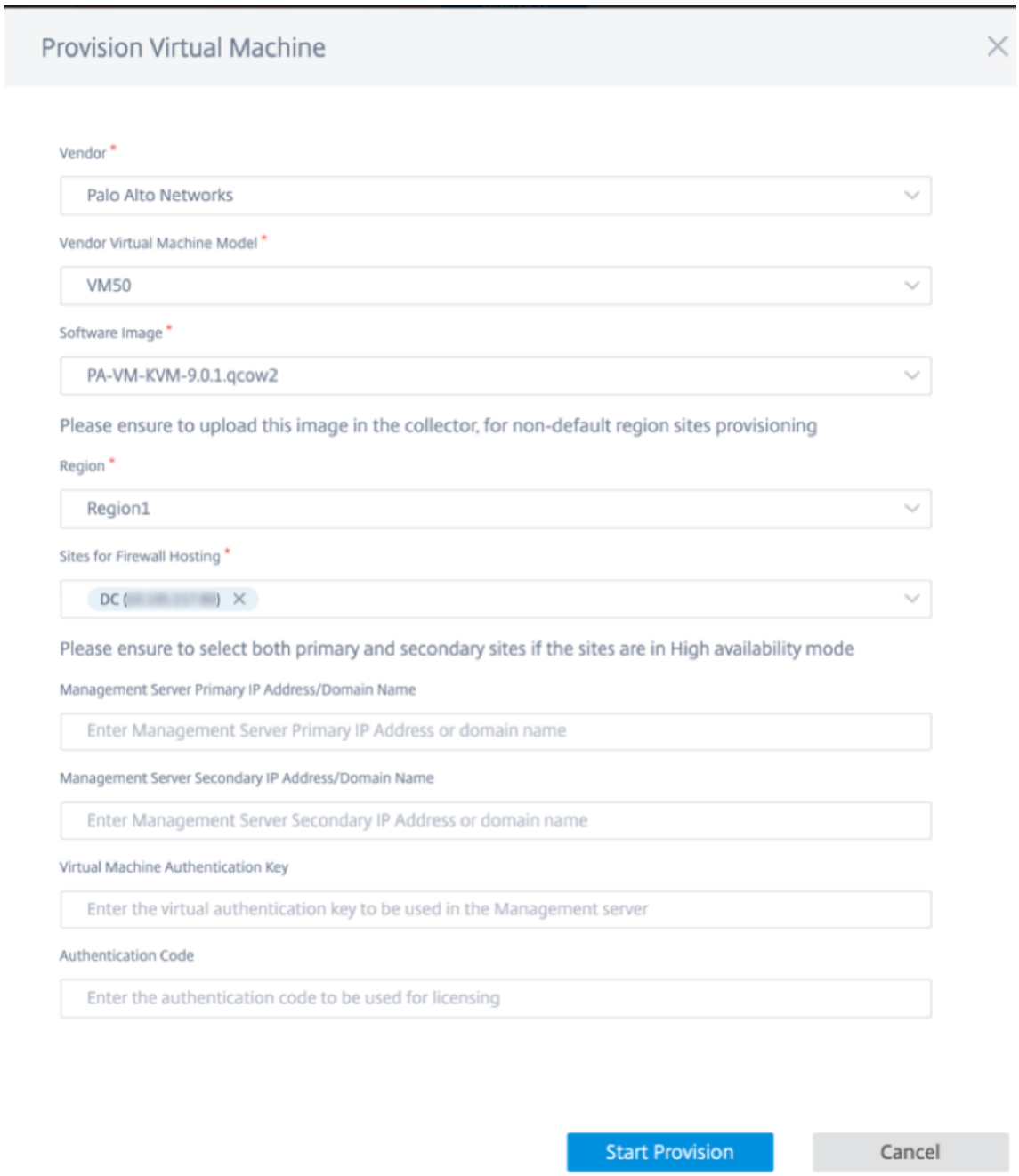
A status bar appears with the ongoing upload process. Do not click **Refresh** or perform any other action until the image file shows 100% uploaded.

- **Refresh**: Click the **Refresh** option to get the latest image file details.

- **Delete**: Click the **Delete** option to delete any existing image file.

> **Note**
>
> - To provision firewall virtual machine on the sites part of non-default region, upload the image file on each of the collector node.
> - Deleting the Palo Alto VM image from SDWAN Center, will delete the image from the SDWAN Center storage, and NOT from the appliance.

3. For provisioning, go back to **Hosted Firewall Sites** tab and click **Provision**.

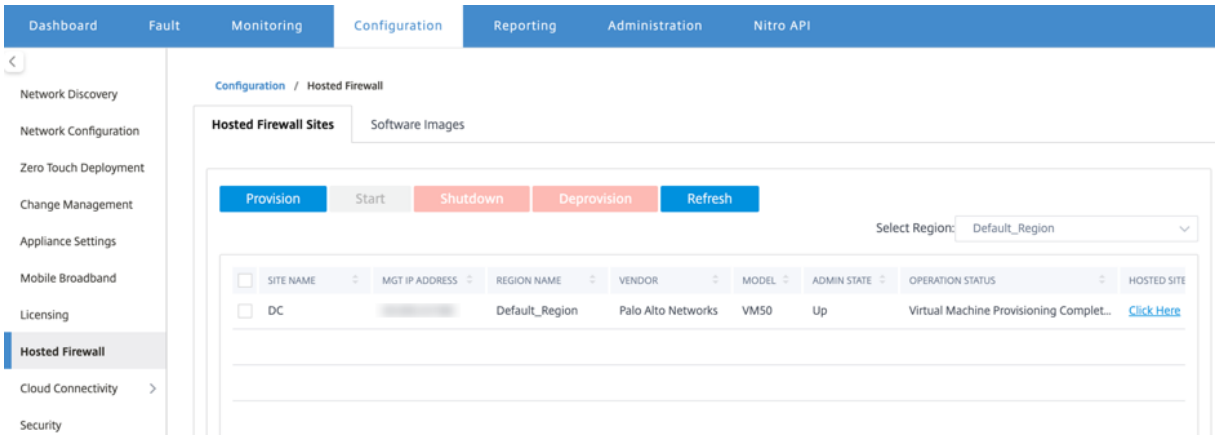


- **Vendor**: Select the **vendor** name as **Palo Alto Networks** from the drop-down list.
- **Vendor Virtual Machine Model**: Select the virtual machine model number from the list.
- **Software Image**: Select the Image file to provision.
- **Region**: Select the region from the list.
- **Sites for Firewall Hosting**: Select sites for the list for firewall hosting. You must select both primary and secondary sites if the sites are in high availability mode.

- **Management Server Primary IP Address/Domain Name**: Enter the management primary IP address or fully qualified domain name (Optional).
- **Management Server Secondary IP Address/Domain Name**: Enter the management server secondary IP address or fully qualified domain name (Optional).
- **Virtual Machine Authentication Key**: Enter the virtual authentication key to be used in the management server.
- **Authentication Code**: Enter the virtual authentication code to be used for licensing.

4. Click **Start Provision**.
5. Click **Refresh** to get the latest status. After the Palo Alto Networks virtual machine is completely bootup, it will reflect on the SD-WAN Center UI.

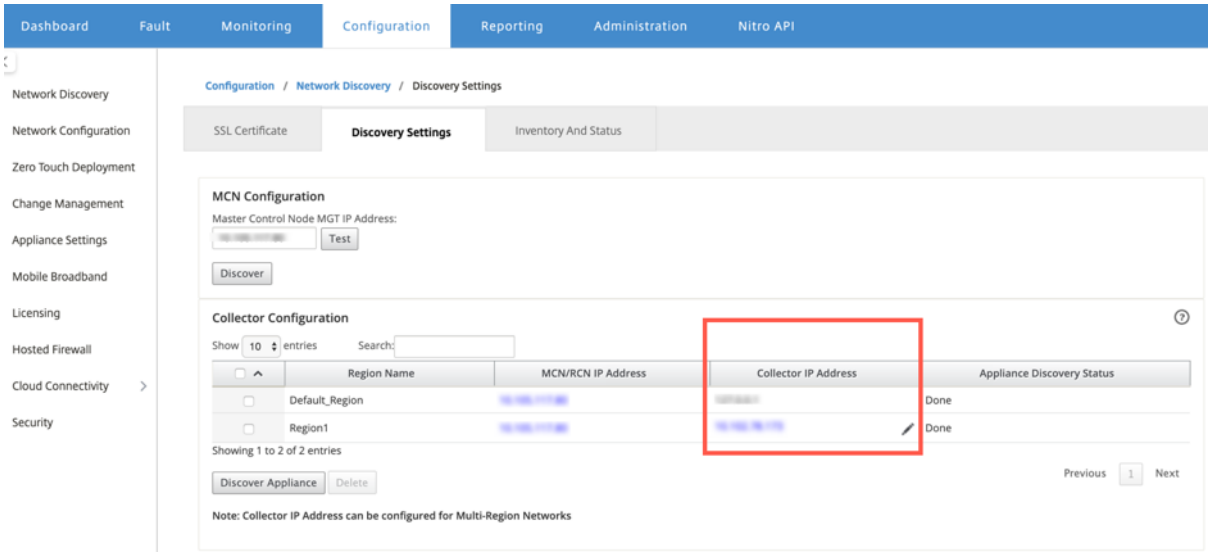
You can **Start, Shutdown,** and **Deprovision** the virtual machine as needed.



- **Site Name**: Displays the site name.
- **Management IP**: Displays the management IP address of the site.
- **Region Name**: Displays the region name.
- **Vendor**: Displays the vendor name (Palo Alto Networks).
- **Model**: Displays the model number (VM50/VM100).
- **Admin State**: State of the vendor virtual machine (Up/Down).
- **Operation Status**: Displays the operational status message.
- **Hosted Site**: Use the **Click Here** link to access the Palo Alto Networks virtual machine GUI.

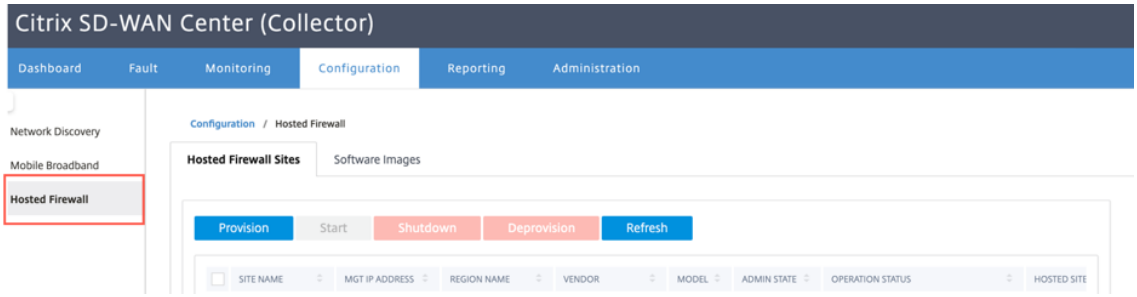
To provision the non-default region sites, you need to upload the software image on the SD-WAN Center Collector. You can provision the Palo Alto Networks both from SD-WAN Center head end GUI or SD-WAN Center Collector.

To get the SD-WAN Center Collector's IP address, navigate to **Configuration > Network Discovery >** select **Discovery Settings** tab.

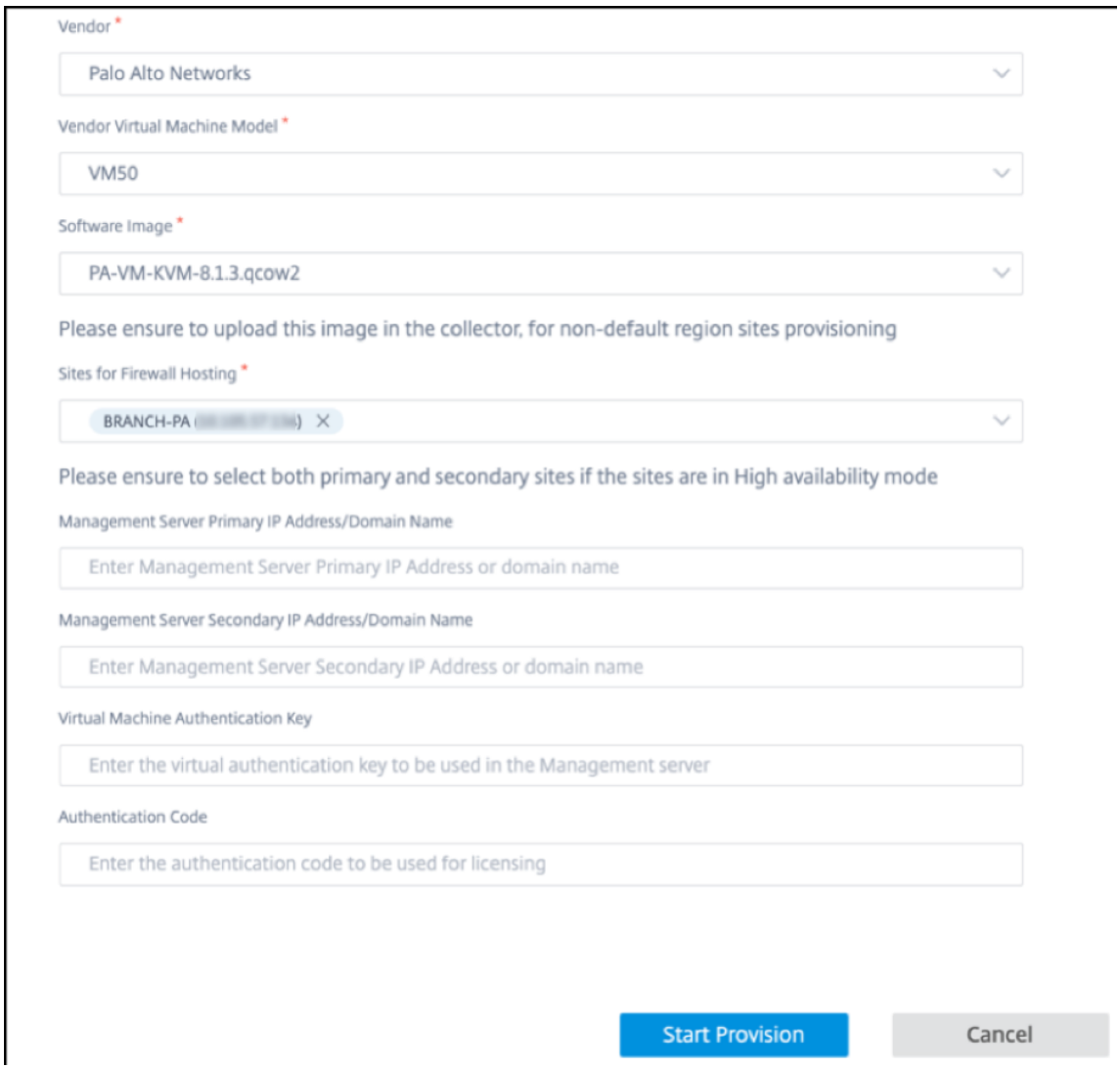


To provision the Palo Alto Networks from SD-WAN Collector:

1. From SD-WAN Collector GUI, navigate to **Configuration >** select **Hosted Firewall**.



2. Go to **Software Images** tab to upload the software image.
3. Click **Provision** under **Hosted Firewall Sites** tab.
4. Provide the following details and click **Start Provision**.



- **Vendor**: Select the **vendor** name as **Palo Alto Networks** from the drop-down list.
- **Vendor Virtual Machine Model**: Select the virtual machine model number from the list.
- **Software Image**: Select the Image file to provision.
- **Region**: Select the region from the list.
- **Sites for Firewall Hosting**: Select sites for the list for firewall hosting. You must select both primary and secondary sites if the sites are in high availability mode.
- **Management Server Primary IP Address/Domain Name**: Enter the management primary IP address or fully qualified domain name (Optional).
- **Management Server Secondary IP Address/Domain Name**: Enter the management server secondary IP address or fully qualified domain name (Optional).
- **Virtual Machine Authentication Key**: Enter the virtual authentication key to be used in the management server.

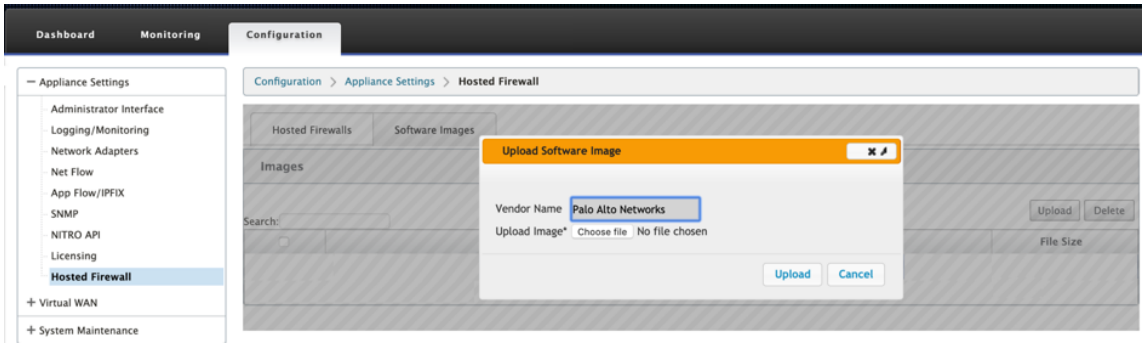
- **Authentication Code**: Enter the virtual authentication code to be used for licensing.

5. Click **Start Provision**.

Firewall virtual machine provisioning through SD-WAN appliance GUI

On SD-WAN platform, provision and boot up the hosted virtual machine. Perform the following steps for provisioning:

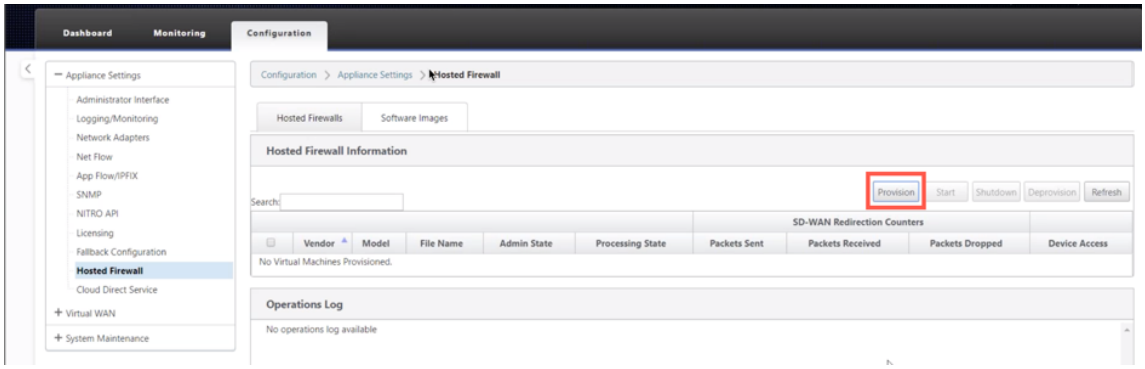
1. From Citrix SD-WAN GUI, navigate to **Configuration >** expand **Appliance Settings >** select **Hosted Firewall**.
2. Upload the software image:
   - Select the **Software Images** tab. Select the Vendor name as **Palo Alto Networks**.
   - Choose the software image file.
   - Click **Upload**.



> **Note**
> Maximum of two software image can be uploaded. Uploading of the Palo Alto Networks virtual machine image might take longer time depending on the bandwidth availability.

   You can see a status bar to track the upload process. The file detail reflects, once the image is uploaded successfully. The image that is used for provisioning cannot be deleted. Do not perform any action or go back to any other page until the image file shows 100% uploaded.

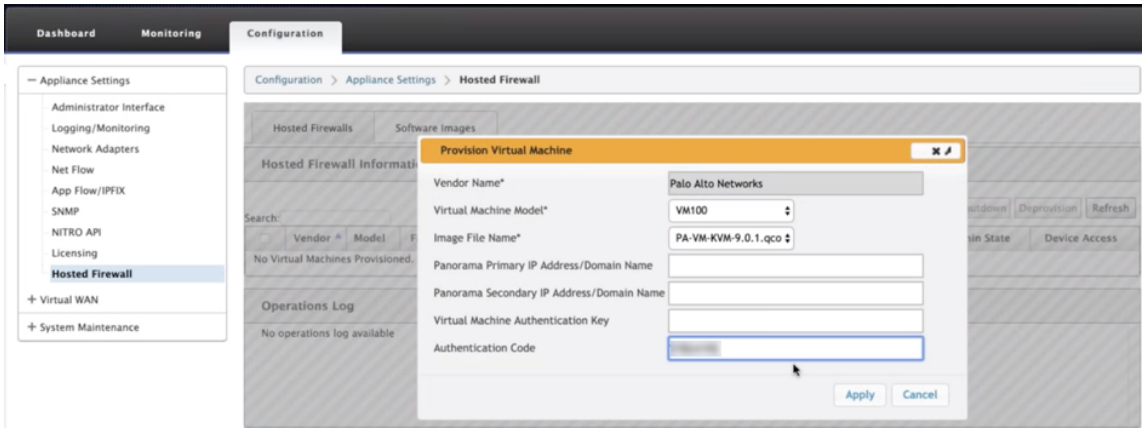
3. For provisioning, select **Hosted Firewalls** tab and click **Provision** button.



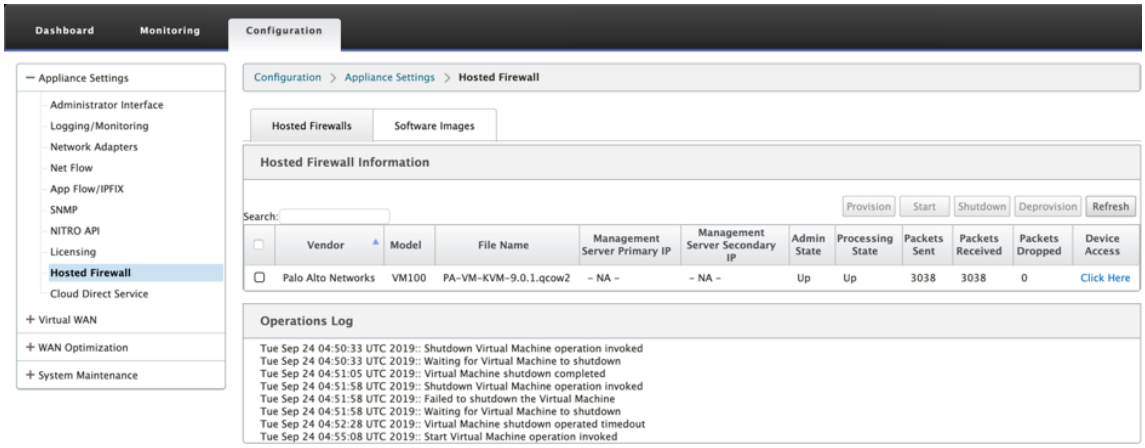
4. Provide the following details for provisioning.

   - **Vendor Name**: Select the Vendor as **Palo Alto Networks**.
   - **Virtual Machine Model**: Select the virtual machine model number from the list.
   - **Image File Name**: Select the Image file.
   - **Panorama Primary IP Address/Domain Name**: Provide the Panorama primary IP address or fully qualified domain name (Optional).
   - **Panorama Secondary IP Address/Domain Name**: Provide the Panorama secondary IP address or fully qualified domain name (Optional).
   - **Virtual Machine Authentication Key**: Provide the virtual machine authentication key (Optional).

     Virtual Machine Authentication Key is needed for automatic registration of the Palo Alto Networks virtual machine to the Panorama.
   - **Authentication Code**: Enter the authentication code (virtual machine license code) (Optional).
   - Click **Apply**.



5. Click **Refresh** to get the latest status. After the Palo Alto Networks virtual machine is completely bootup, it will reflect on the SD-WAN UI with the operations Log detail.



- **Admin State**: Indicates if the virtual machine is up or down.
- **Processing State**: Datapath processing state of the virtual machine.
- **Packet Sent**: Packets sent from SD-WAN to the security virtual machine.
- **Packet Received**: Packets received by SD-WAN from the security virtual machine.
- **Packet Dropped**: Packets dropped by SD-WAN (for example, when the security virtual machine is down).
- **Device Access**: Click the link to get the GUI access to the security virtual machine.

You can **Start, Shutdown,** and **Deprovision** the virtual machine as needed. Use **Click Here** option to access the Palo Alto Networks virtual machine GUI or use your management IP along with 4100 port (management IP: 4100).

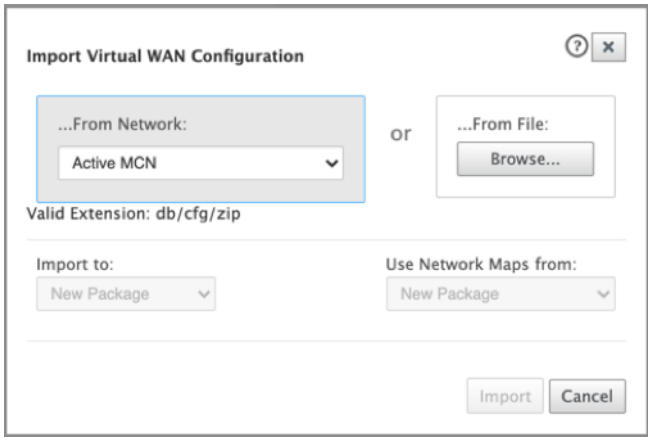
> **Note**
> Always use incognito mode to access the Palo Alto Networks GUI.

Traffic redirection

Traffic redirection configuration can be done both through the Configuration Editor on MCN or Configuration Editor on SD-WAN Center.

To navigate through Configuration Editor on SD-WAN Center:

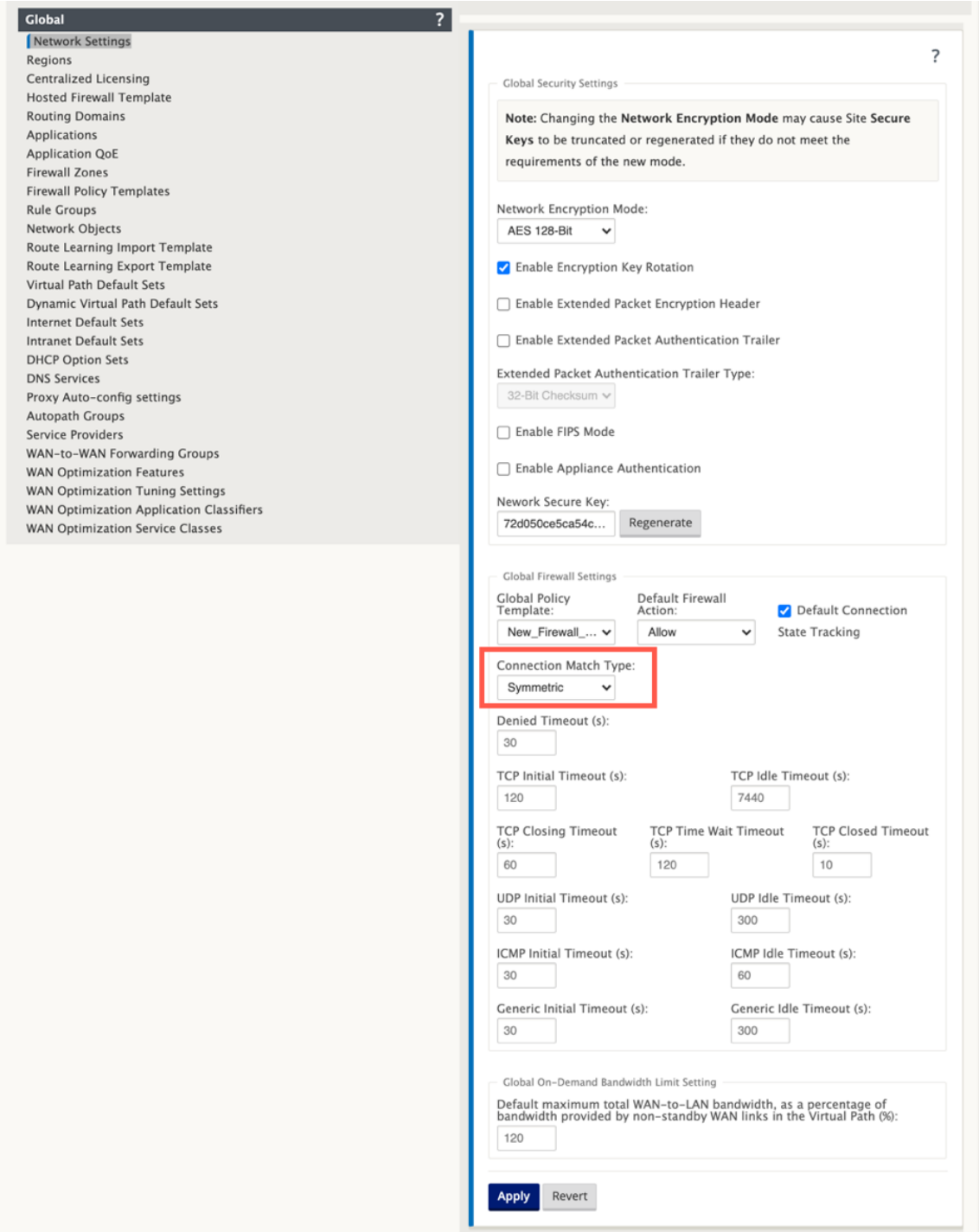
1. Open Citrix SD-WAN Center UI, navigate to **Configuration > Network Configuration Import**. Import the virtual WAN configuration from the active MCN and click **Import**.



Remaining steps are similar as following - the traffic redirection configuration through MCN.

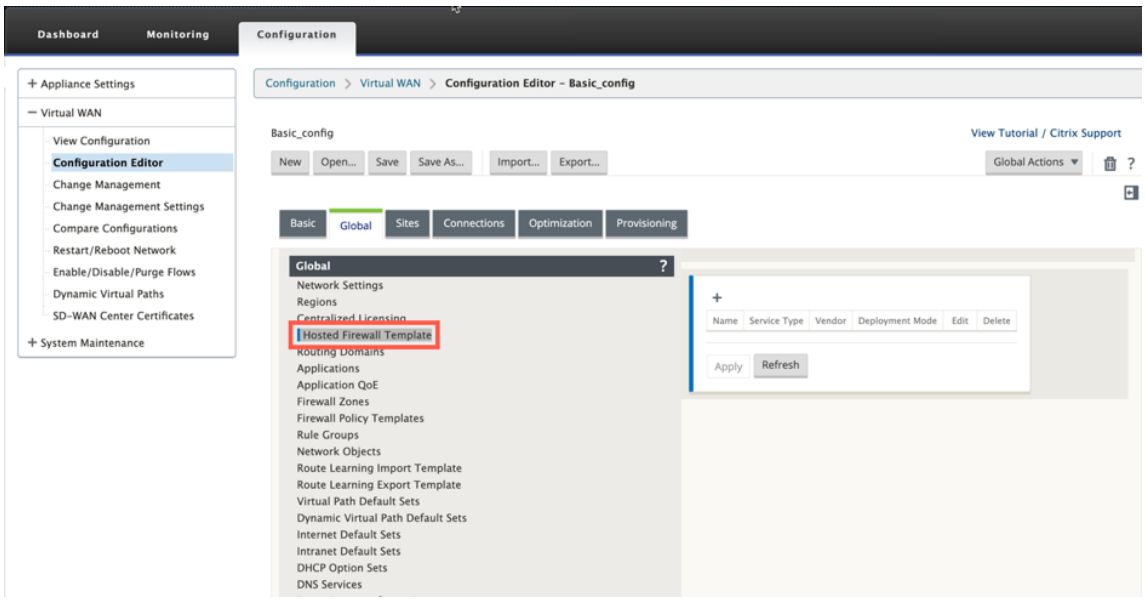
To navigate through Configuration Editor on MCN:

1. Set **Connection Match Type** to **Symmetric** under **Global > Networking Settings**.

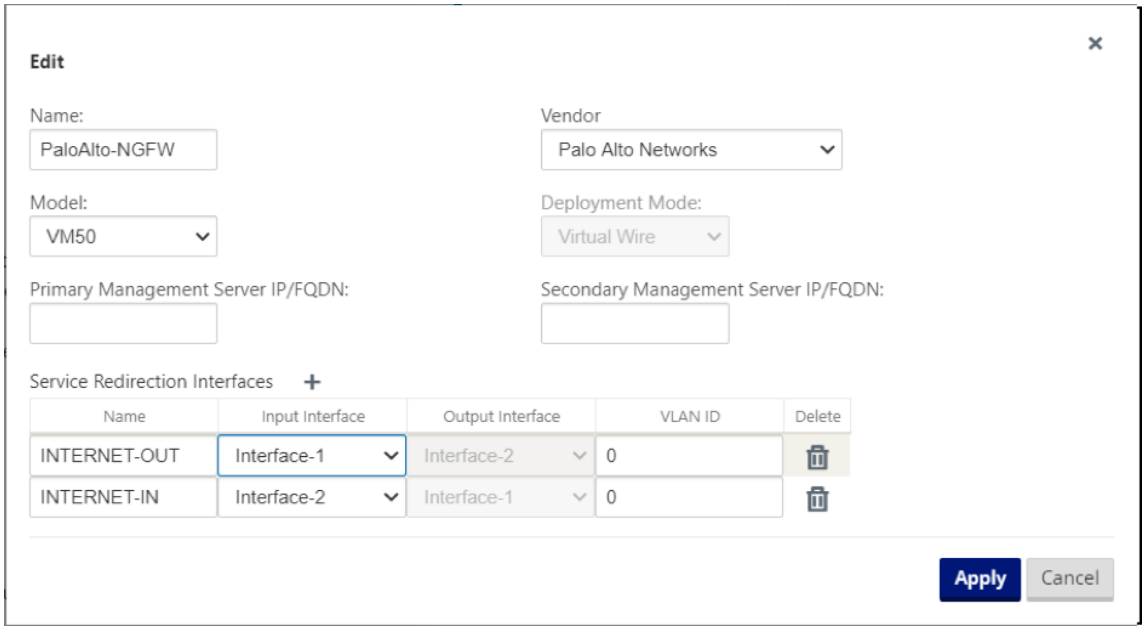


By default, SD-WAN firewall policies are direction specific. The Symmetric match type match the connections using specified match criteria and apply policy action on both directions.

2. Open **Citrix SD-WAN UI**, navigate to **Configuration >** expand **Virtual WAN >** select **Configuration Editor** > select **Hosted Firewall Template** under **Global** section.



3. Click **+** and provide the required information available in the following screenshot to add the **Hosted Firewall** template and click **Add**.



Hosted Firewall Template allows you to configure the traffic redirection to the **Firewall virtual machine** hosted on SD-WAN appliance. The following are the inputs needed to configure the template:

- **Name**: Name of the hosted firewall template.
- **Vendor**: Name of the firewall vendor.
- **Deployment Mode**: The **Deployment Mode** field is auto populated and grayed out. For the **Palo Alto Networks** vendor, the deployment mode is **Virtual Wire**.
- **Model**: Virtual Machine model of the hosted firewall. You can select the virtual machine model number as VM 50/VM 100 for the Palo Alto Networks vendor.

- **Primary Management Server IP/FQDN**: Primary management server IP/FQDN of Panorama.
- **Secondary Management Server IP/FQDN**: Secondary management server IP/FQDN of Panorama.
- **Service Redirection Interfaces**: These are logical interfaces used for traffic redirection between SD-WAN and hosted firewall.

Interface-1, Interface-2 refers to first two interfaces on the hosted firewall. If VLANs are used for traffic redirection then, same VLANs must be configured on the hosted firewall. VLANs configured for traffic redirection are internal to the SD-WAN and hosted firewall.

> **Note**
>
> Redirection input interface has to be selected from connection initiator direction, redirection interface is automatically chosen for the response traffic. For Example, if outbound internet traffic is redirected to hosted firewall on Interface-1 then, response traffic is automatically redirected to hosted firewall on Interface-2. There is no need of Interface-2 in the above example, if there is no internet inbound traffic.

Only two physical interfaces are assigned to host the Palo Alto Networks firewall. If traffic from multiple zones needs to be redirected to the hosted firewall then, multiple subinterfaces can be created using internal VLANs and associated to different firewall zones on the hosted firewall.

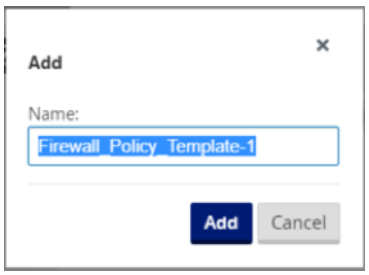
Through SD-WAN firewall policies or site level policies, you can redirect all the traffic to the Palo Alto Networks virtual machine.

> **Note**
>
> SD-WAN firewall policies are auto created to **Allow** the traffic to/from hosted firewall management servers. This avoids redirection of the management traffic that is originated from (or) destined to hosted firewall.

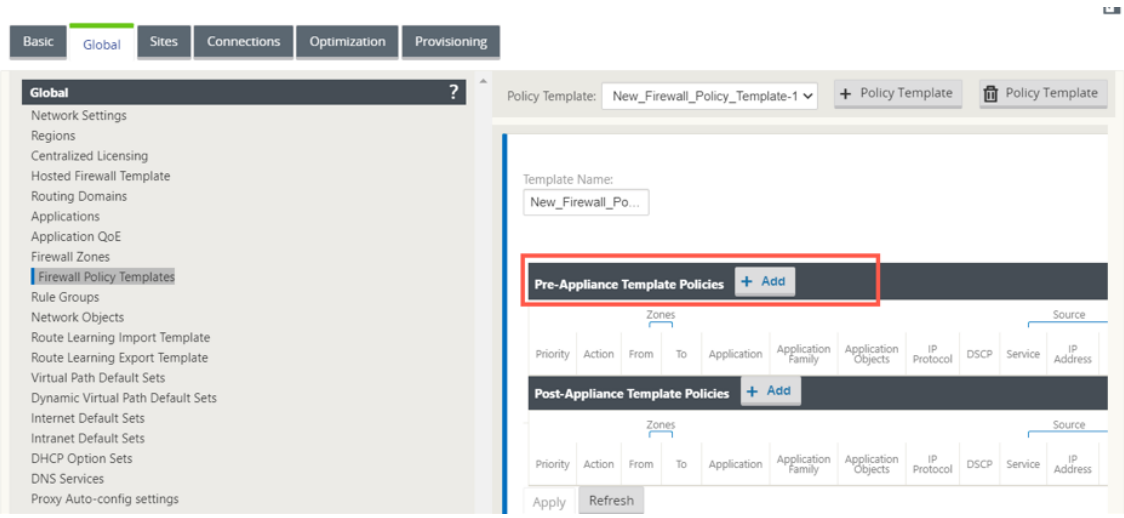
Traffic redirection to firewall virtual machine can be done using SD-WAN firewall policies. There are two methods to create SD-WAN firewall policies - either through firewall policy templates in **Global** section or site level.

Method - 1

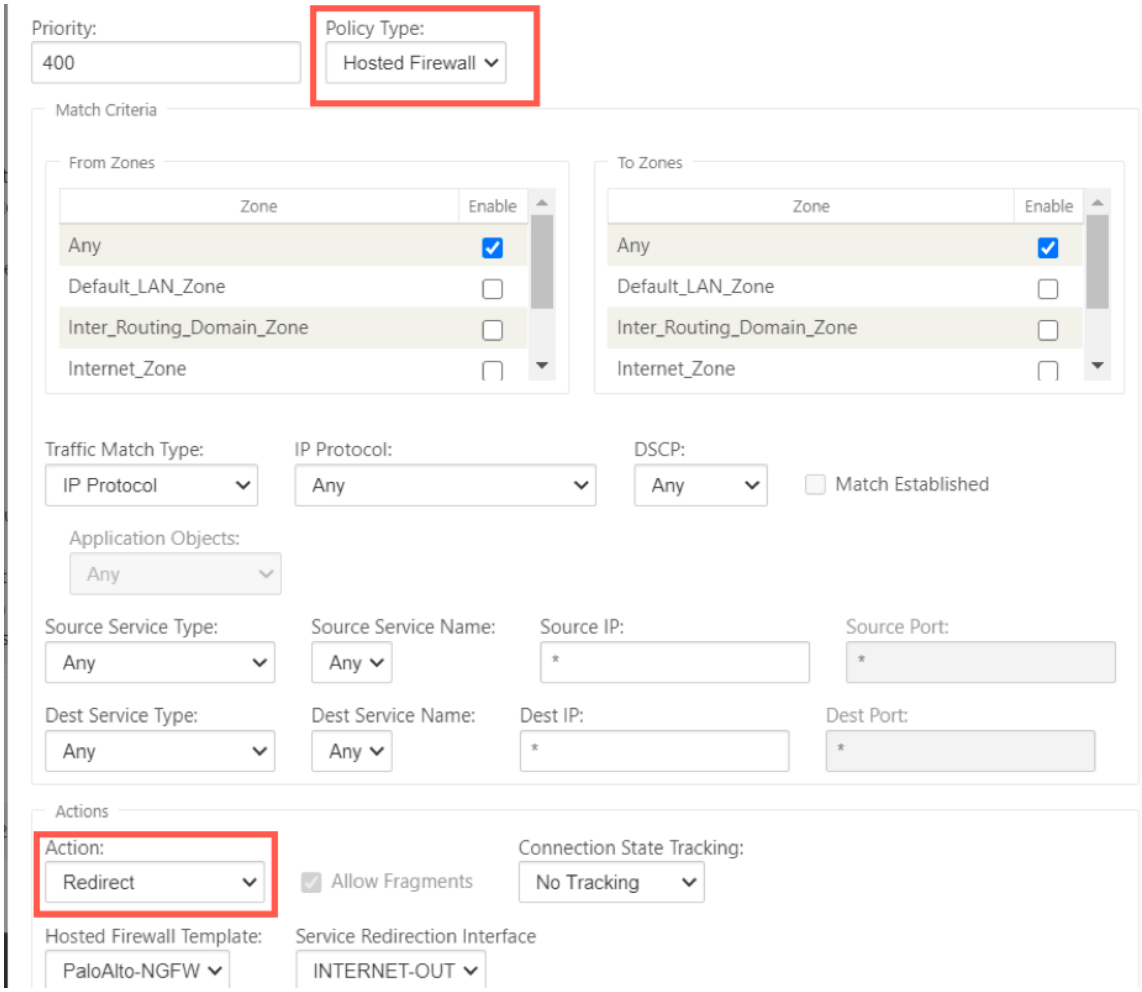
1. From Citrix SD-WAN GUI, navigate to **Configuration >** expand **Virtual WAN > Configuration Editor**. Navigate to the **Global** tab and select **Firewall Policy Templates**. Click **+ Policy Template**. Provide a name to the policy template and click **Add**.



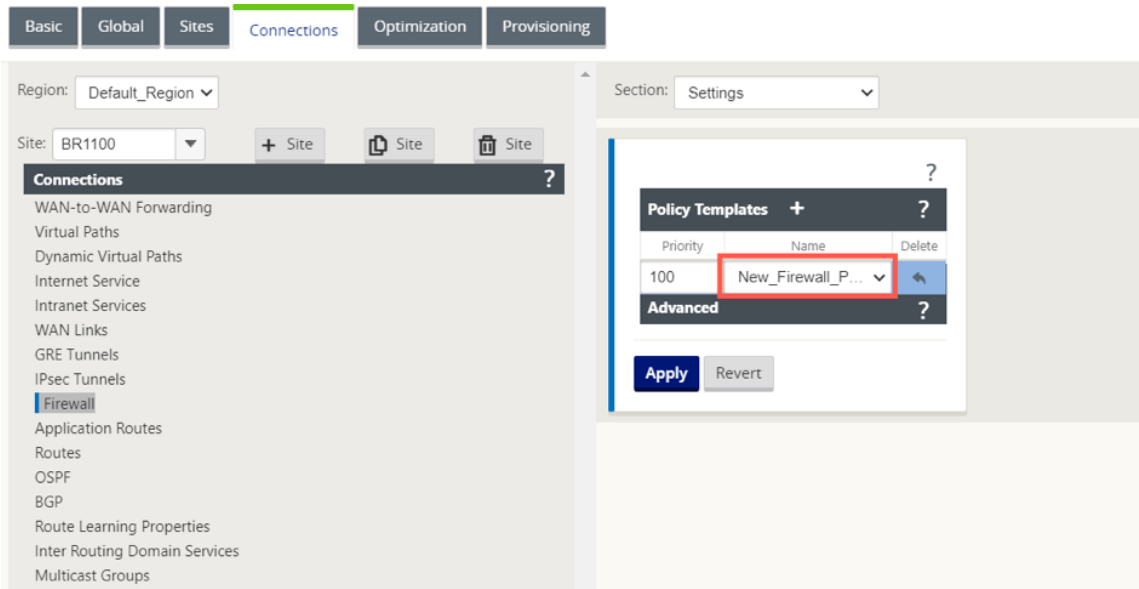
2. Click **+ Add** next to **Pre-Appliance Template Policies**.



3. Change the **Policy Type** to **Hosted Firewall**. The **Action** field is auto filled to **Redirect**. Select the **Hosted Firewall Template** and the **Service Redirection Interface** from the drop-down list. Fill the other match criteria as required.

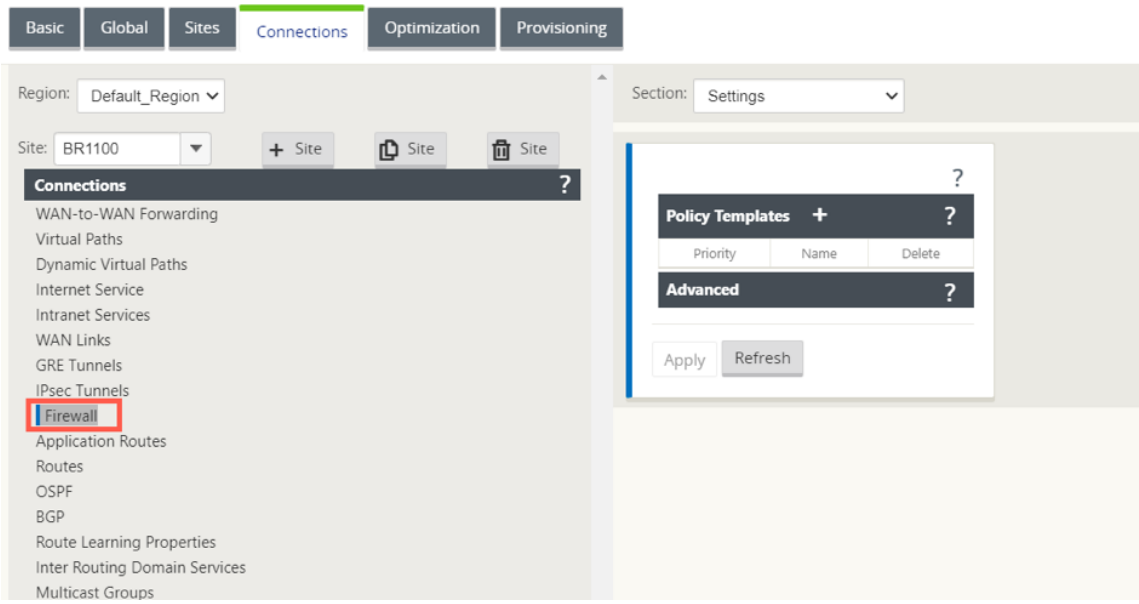


4. Navigate to the **Connections > Firewall**, then select the firewall policy (that you have created) under the name field. Click **Apply**.

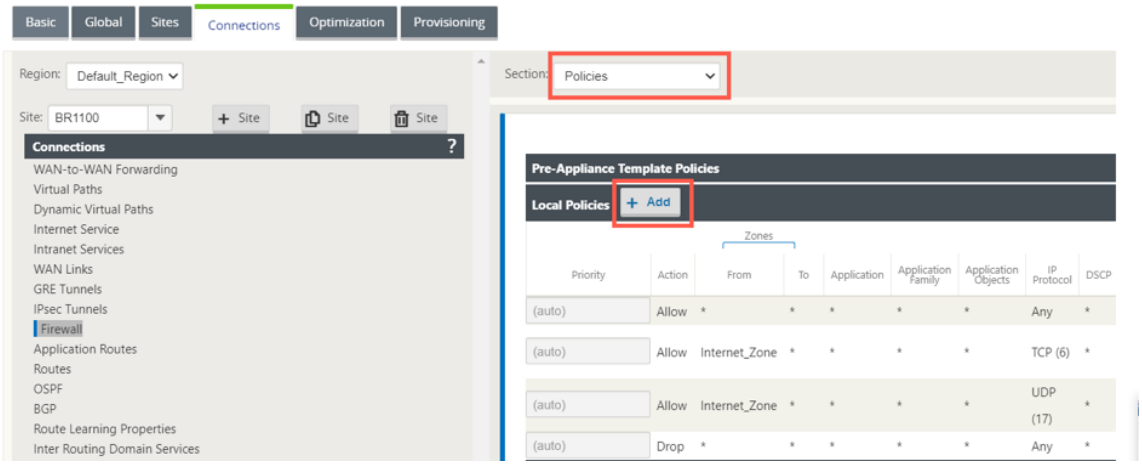


Method - 2

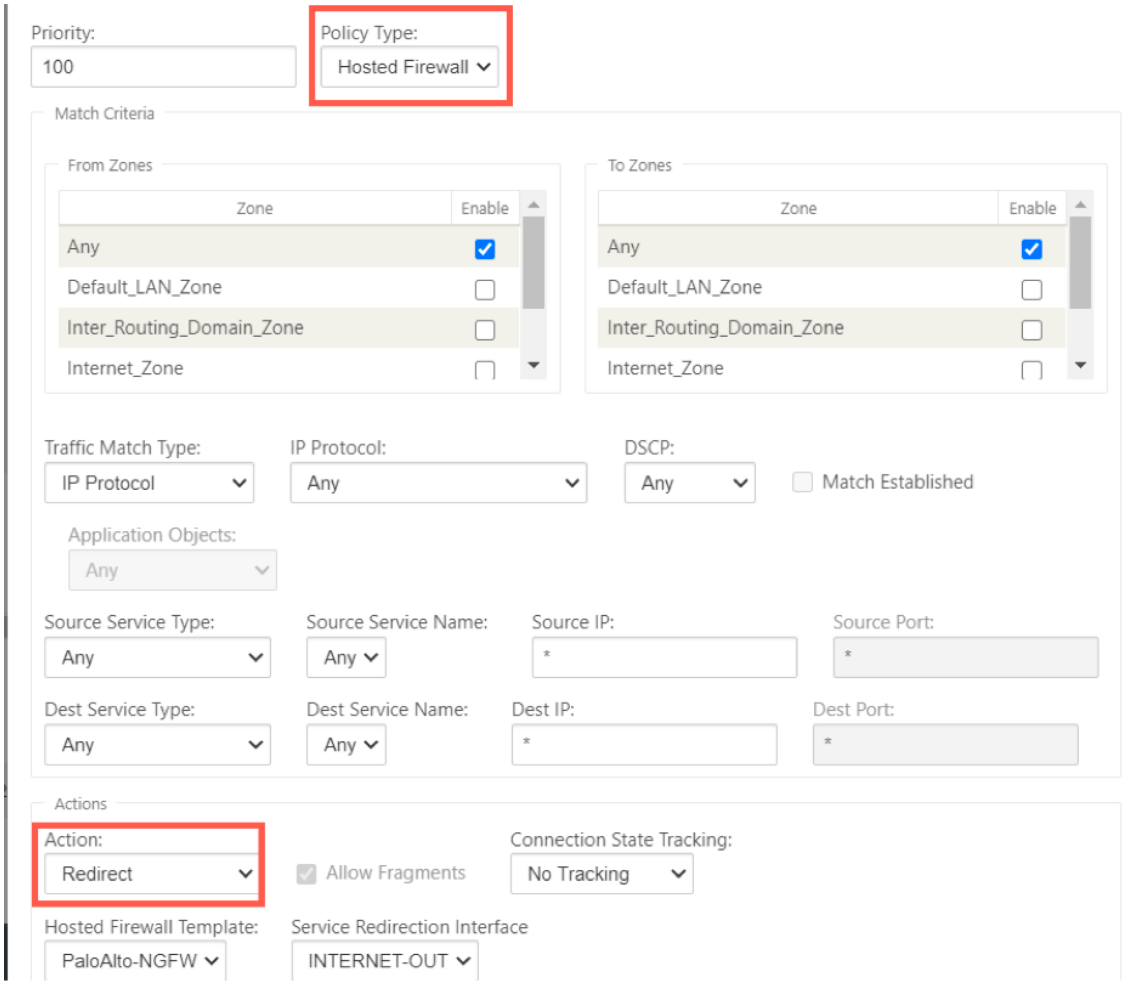
1. To redirect all the traffic, under the **Configuration Editor > Virtual WAN**, navigate to the **Connection** tab and select **Firewall**.



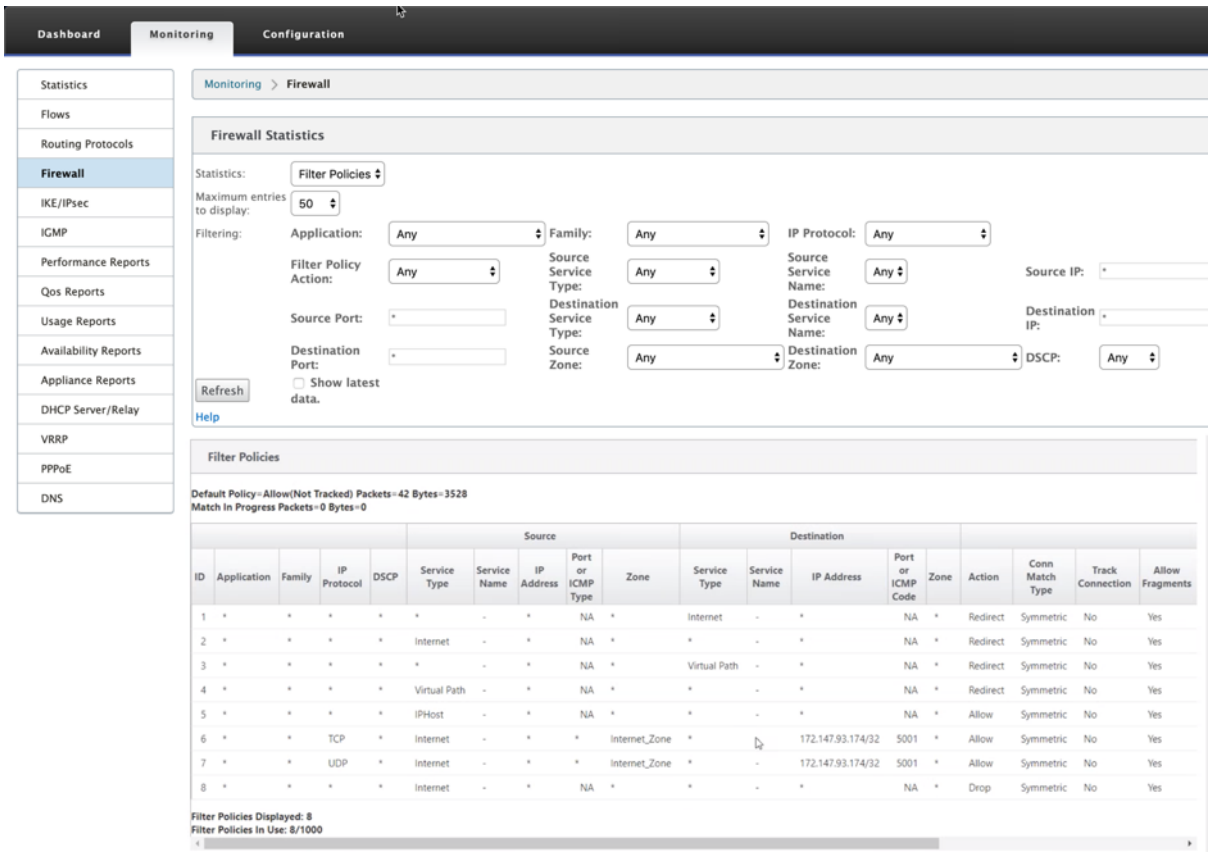
2. Select **Policies** from the **Section** drop-down list and click **+Add** to create a new firewall policy.



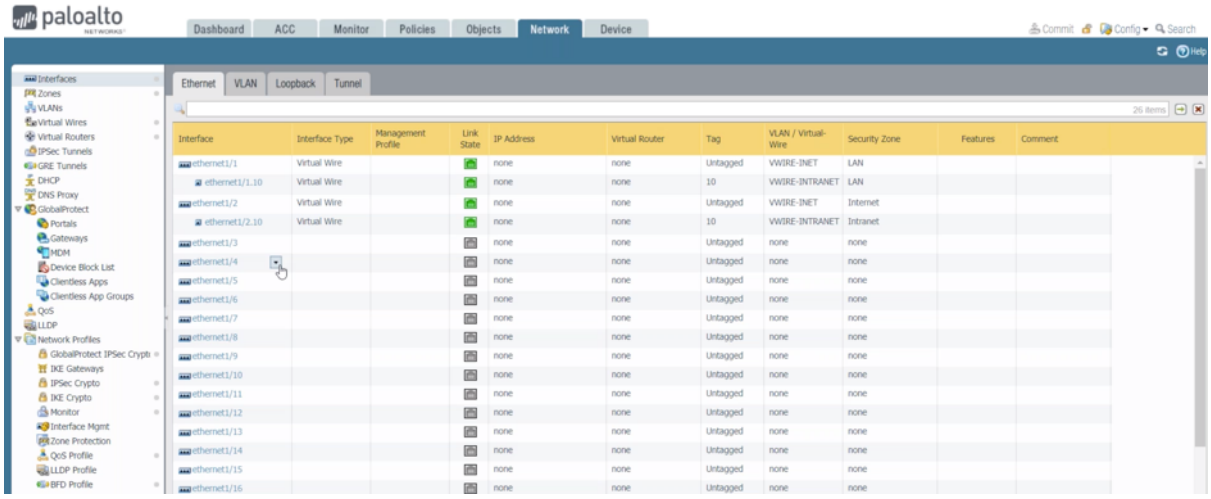
3. Change the **Policy Type** to **Hosted Firewall**. The **Action** field is auto filled to Redirect. Select the **Hosted Firewall Template** and the **Service Redirection Interface** from the drop-down list. Click **Add**.



While all the network configuration is up and running mode, you can monitor the connection under **Monitoring > Firewall >** under **Statistics** list, select **Filter Policies**.



You can verify the mapping between the configuration you did on SD-WAN service chain template and Palo Alto Network configuration using the Palo Alto Networks UI.



NOTE

Palo Alto Networks virtual machine cannot be provisioned if **Cloud Direct** or **SD-WAN WANOP(PE)** is already provisioned on the 1100 appliance.

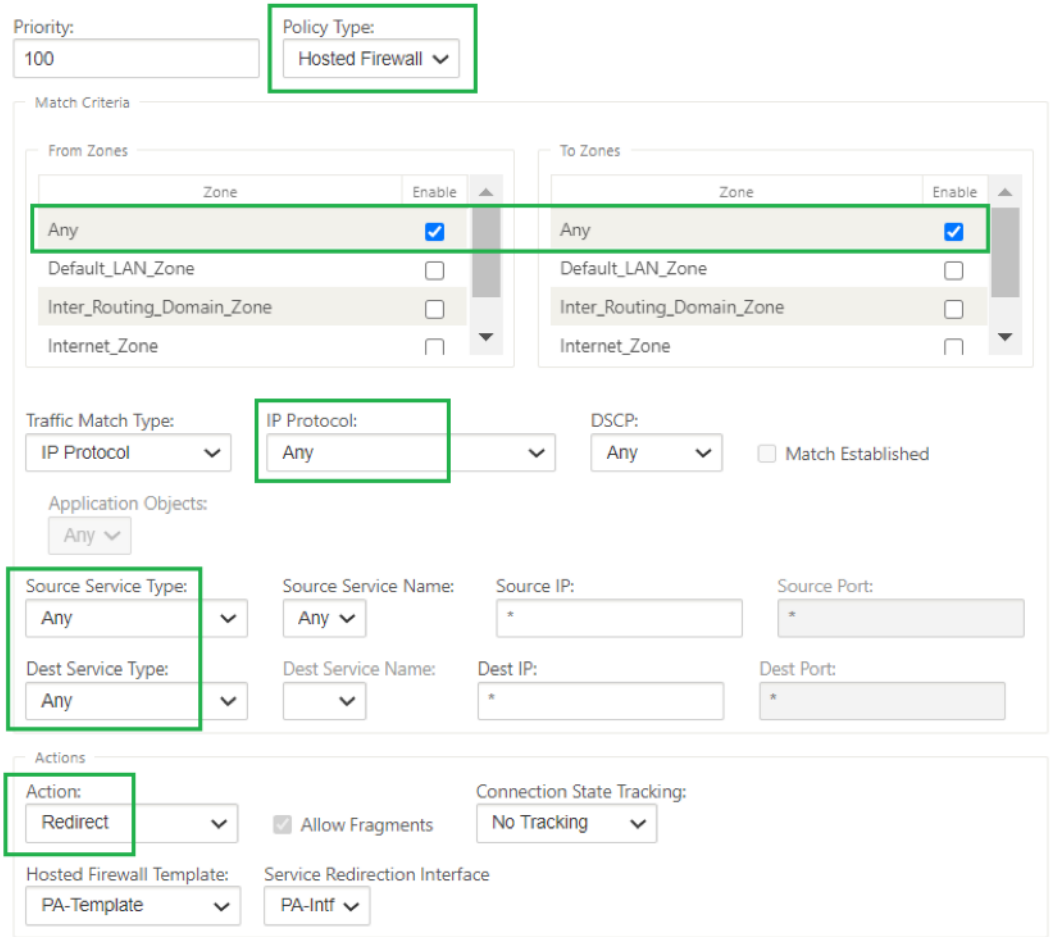
Use-cases –Hosted Firewall on SD-WAN 1100

The following are some of the use case scenarios implemented by using Citrix SD-WAN 1100 appliance:

Use case 1: Redirect all the traffic towards Hosted Firewall

This use case is applicable for small branch use cases where all the traffic is processed by the hosted Next-Generation firewall. Bandwidth requirements must be taken into considerations as the amount of redirected traffic throughput is limited to 100 Mbps.

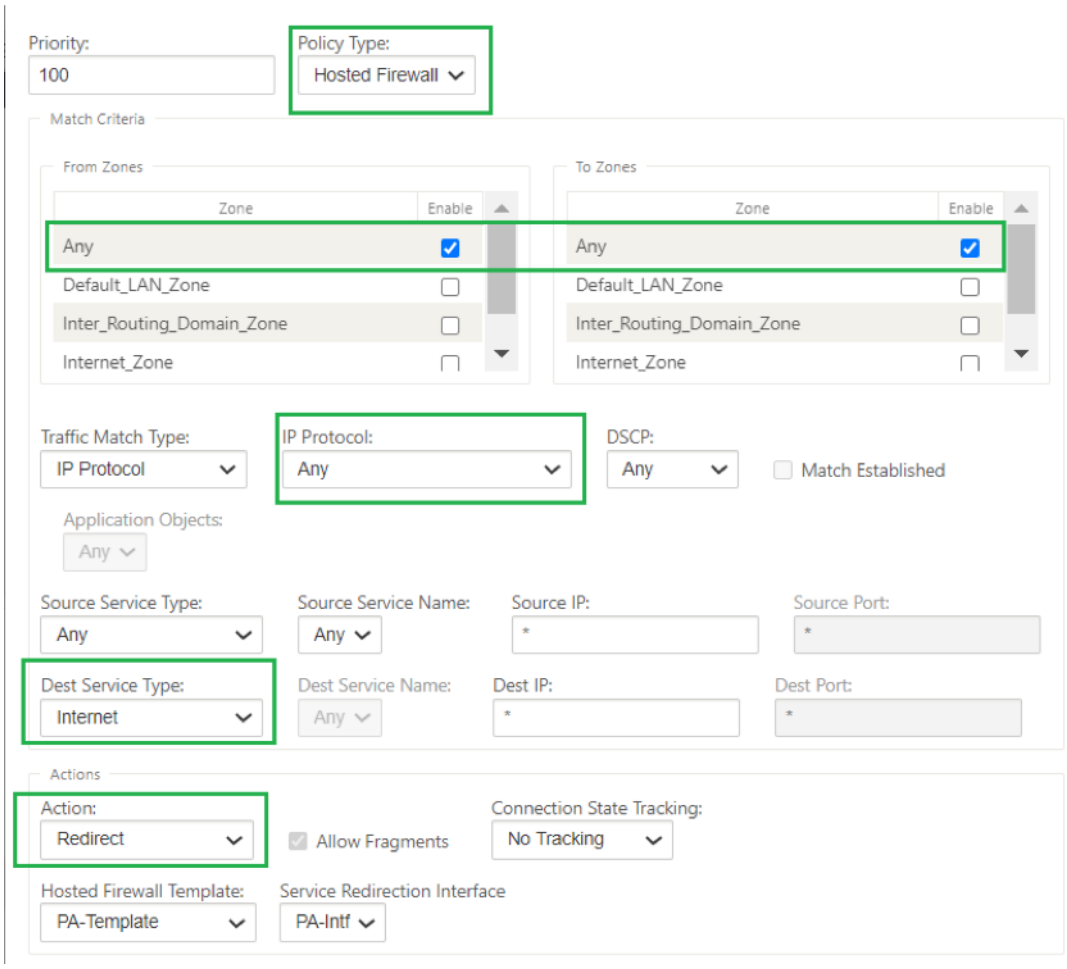
To achieve this, create a firewall rule to match any traffic and with **Action** as **Redirect**, as shown in the following screenshot:



Use case 2: Redirect only Internet traffic towards Hosted Firewall

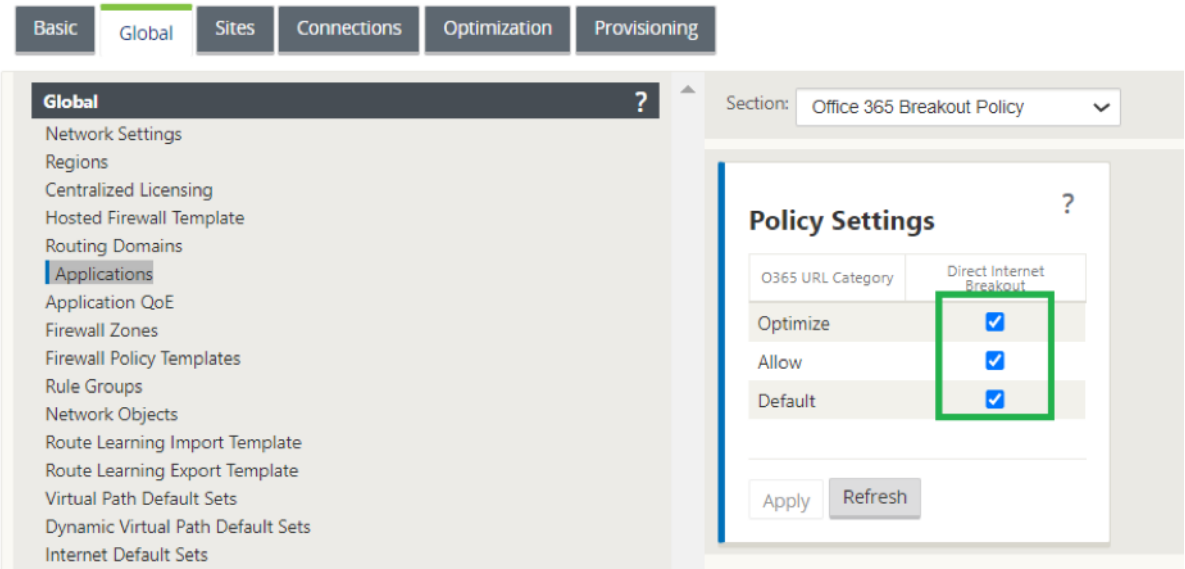
This use case is applicable to any branch sites where Internet bound traffic not exceeding the amount of supported redirected traffic throughput. In this case, Branch to data center traffic is processed by security appliances/service deployed at data centers.

To achieve this, create a firewall rule to match any traffic and with **Action** as **Redirect** as shown in the following screenshot:

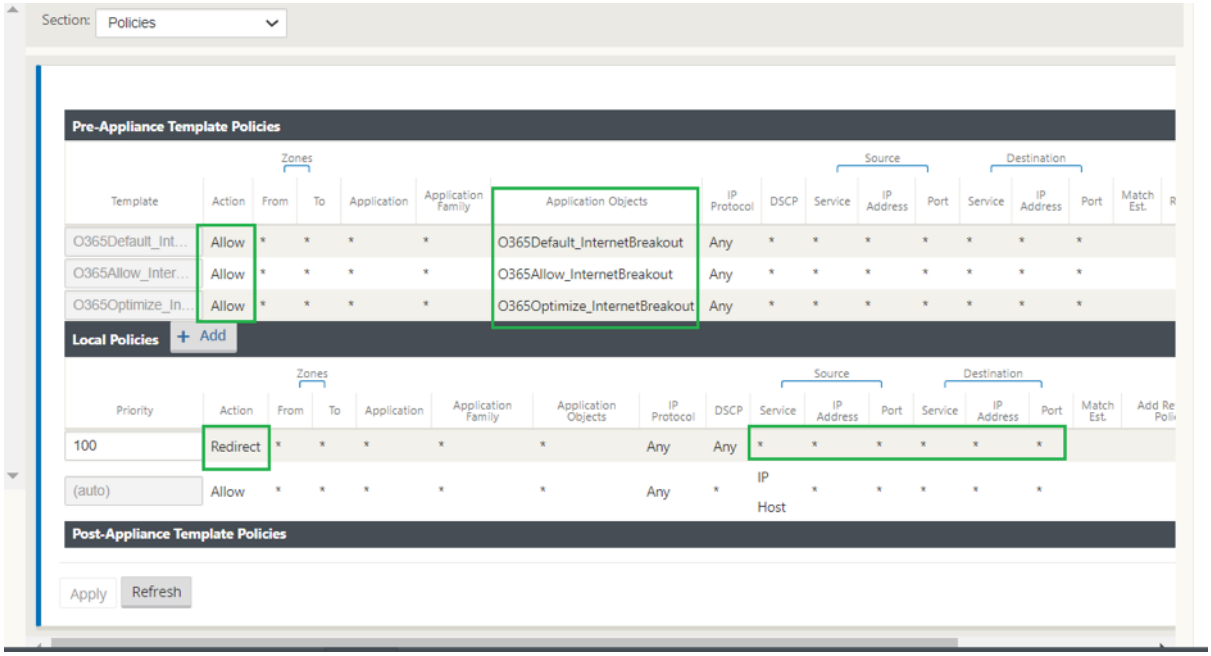


Use case 3: Direct Internet breakout for trusted Internet SaaS applications and redirect remaining all traffic to the Hosted VM

In this use case, a firewall rule is added to perform direct Internet breakout for trusted SaaS applications such as office 365. First enable office 365 break out policy as shown in the following screenshot:



This automatically adds **Pre-Appliance Template Policies** to allow office 365 traffic as shown in the following screenshot. Now add a firewall rule to redirect remaining all traffic to Hosted firewall as mentioned below.



Note

Hosted firewall configuration is independent of Citrix SD-WAN configuration. So, the hosted firewall can be configured as per enterprise security requirements.

Check Point firewall integration on SD-WAN 1100 platform

March 12, 2021

Citrix SD-WAN supports hosting **Check Point CloudGuard Edge** on SD-WAN 1100 platform.

The **Check Point CloudGuard Edge** runs as a virtual machine on SD-WAN 1100 platform. The firewall virtual machine is integrated in Bridge mode with two data virtual interfaces connected to it. Required traffic can be redirected to the firewall virtual machine by configuring policies on SD-WAN.

Benefits

The following are the primary goals or benefits of Check Point integration on the SD-WAN 1100 platform:

- Branch device consolidation: A single appliance that does both SD-WAN and advanced security
- Branch office security with on-prem NGFW (Next Generation Firewall) to protect LAN-to-LAN, LAN-to-Internet, and Internet-to-LAN traffic

Configuration steps

The following configurations are needed to integrate Check Point firewall virtual machine on SD-WAN:

- Provision the Firewall Virtual Machine
- Enable traffic redirection to Security Virtual Machine

> **Note**
>
> Firewall virtual machine must be provisioned first before enabling the traffic redirection.

Provisioning Check Point firewall virtual machine

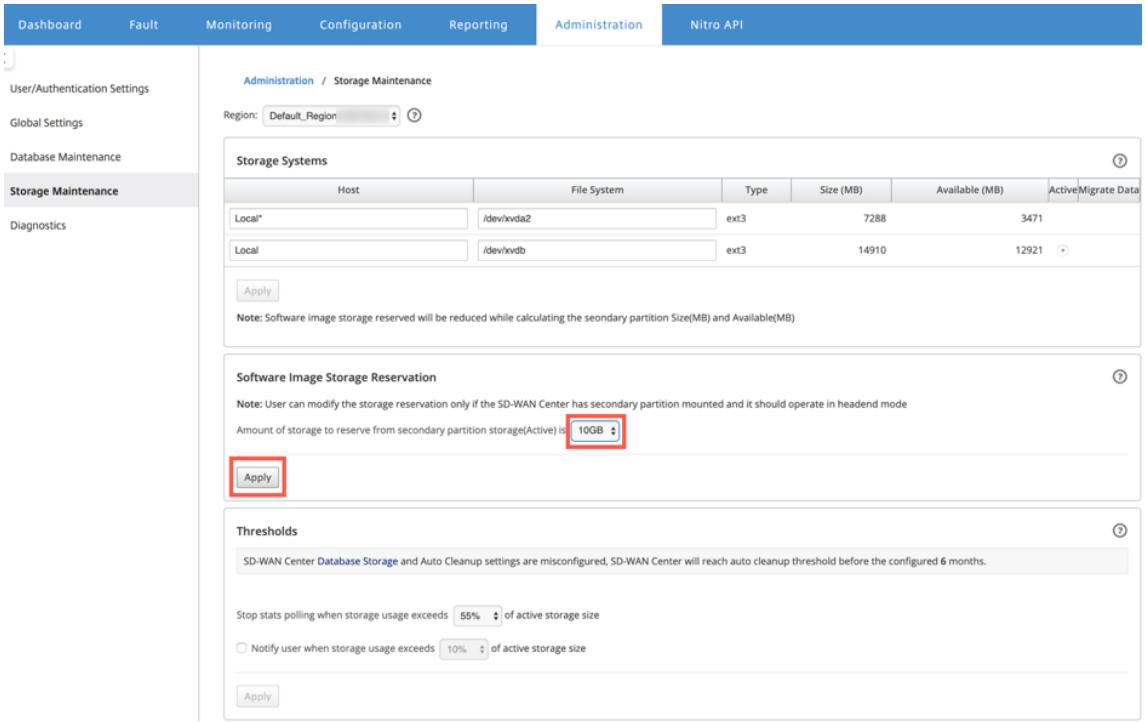
There are two ways to provision the firewall virtual machine:

- Provisioning through SD-WAN Center
- Provisioning through SD-WAN appliance GUI

Firewall virtual machine provisioning through SD-WAN Center

Prerequisites

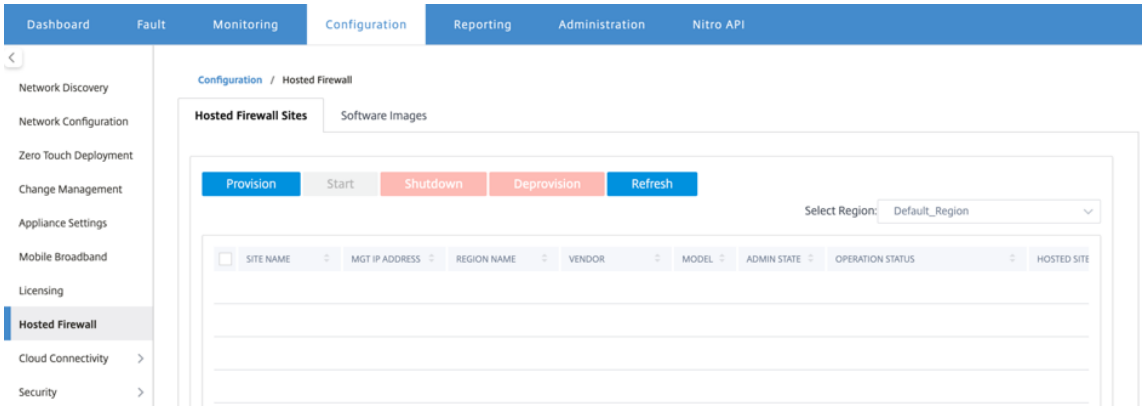
- Add the secondary storage to SD-WAN Center to store the Firewall VM image files. For more information, see System requirements and installation.
- Reserve the storage from the secondary partition for the Firewall VM image files. To configure the storage limit, navigate to **Administration > Storage Maintenance**.
  - Select the required storage amount from the list.
  - Click **Apply**.



> **Note**
>
> Storage is reserved from secondary partition which is active if the condition is met.

Perform the following steps for provisioning the firewall virtual machine through SD-WAN Center platform:

1. From Citrix SD-WAN Center GUI, navigate to **Configuration >** select **Hosted Firewall**.

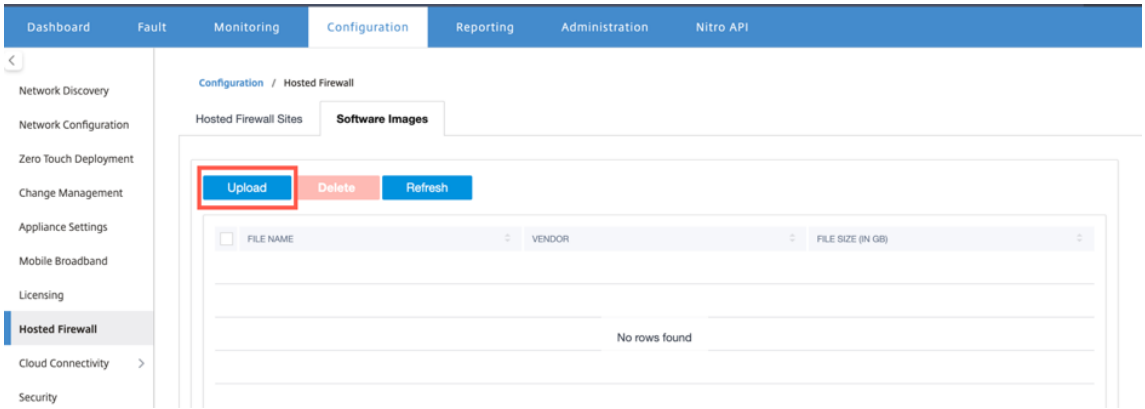


You can select the **Region** from the drop-down list to view the provisioned site details for that selected region.

2. Upload the software image.

> **Note**
>
> Ensure that you have enough disk space to upload the software image.

Navigate to **Configuration > Hosted Firewall > Software Images** and click **Upload**.



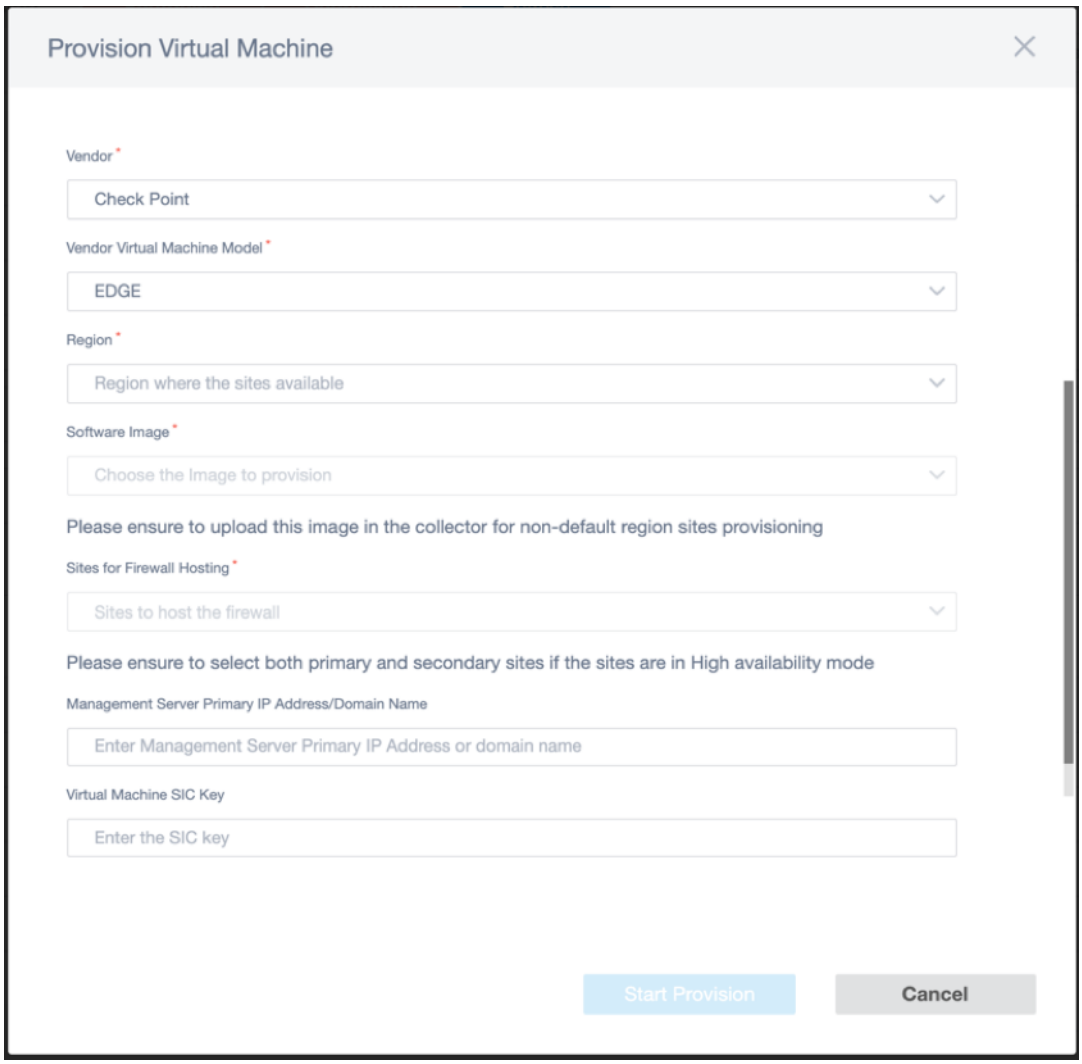
3. Select the Vendor name as **Check Point** from the drop-down list. Click or drop the software image file in the box to upload.

A status bar appears with the ongoing upload process. Do not click **Refresh** or perform any other action until the image file shows 100% uploaded.

- **Refresh**: Click **Refresh** option to get the latest image file details.
- **Delete**: Click **Delete** option to delete any existing image file.

> **Note**
>
> To provision firewall virtual machine on the sites part of non-default region, upload the image file on each of the collector node.

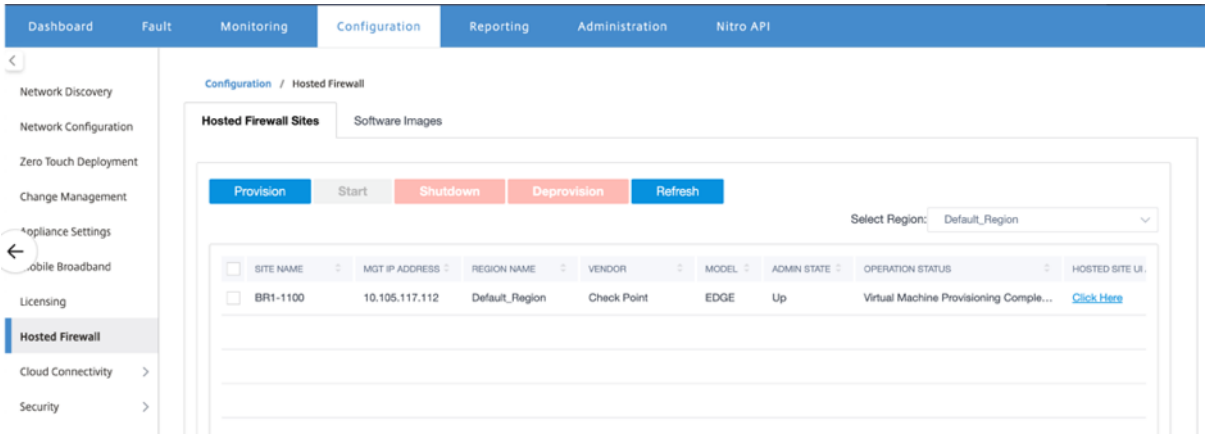
4. For provisioning, go back to **Hosted Firewall Sites** tab and click **Provision**.



- **Vendor**: Select the vendor name as **Check Point** from the drop-down list.
- **Vendor Virtual Machine Model**: The virtual machine model field is auto filled as Edge.
- **Region**: Select the region from the list.
- **Software Image**: Select the Image file to provision.
- **Sites for Firewall Hosting**: Select sites for the list for firewall hosting. You must select both primary and secondary sites if the sites are in high availability mode.
- **Management Server Primary IP Address/Domain Name**: Enter the management primary IP address or fully qualified domain name (Optional).
- **Virtual Machine SIC Key**: Enter the virtual machine Secure Internal Communication (SIC) key. SIC creates trusted connections between **Check Point** components.

5. Click **Start Provision**.
6. Click **Refresh** to get the latest status. After the Check Point virtual machine is completely bootup, it will reflect on the SD-WAN Center UI.

You can **Start, Shutdown,** and **Deprovision** the virtual machine as needed.

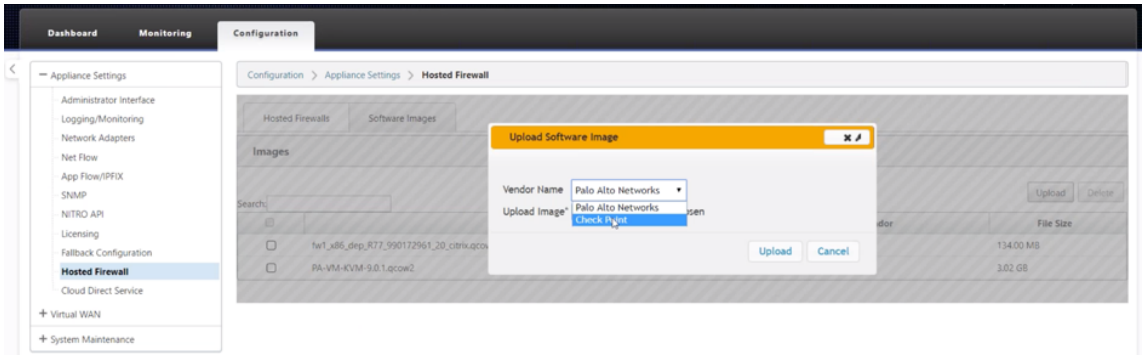


- **Site Name**: Displays the site name.
- **Management IP**: Displays the management IP address of the site.
- **Region Name**: Displays the region name.
- **Vendor**: Displays the vendor name (Check Point).
- **Model**: Displays the model - **Edge**.
- **Admin State**: State of the vendor virtual machine (Up/Down).
- **Operation Status**: Displays the last operation status message.
- **Hosted Site UI Access**: Use the **Click Here** link to access the Check Point virtual machine GUI.

Firewall virtual machine provisioning through SD-WAN appliance GUI

On SD-WAN platform, provision and boot up the hosted virtual machine. Perform the following steps for provisioning:

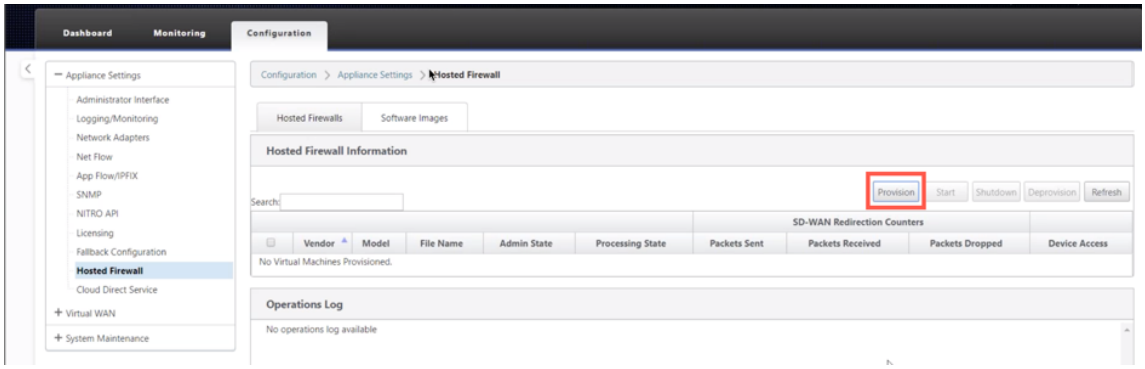
1. From Citrix SD-WAN GUI, navigate to **Configuration > Appliance Settings >** select **Hosted Firewall**.
2. Upload the software image:
   - Select the **Software Images** tab. Select the **Vendor Name** as Check Point.
   - Choose the software image file.
   - Click **Upload**.



> **Note**
>
> Maximum of two images can be uploaded. Uploading of the Check Point virtual machine image might take longer time depending on the bandwidth availability.

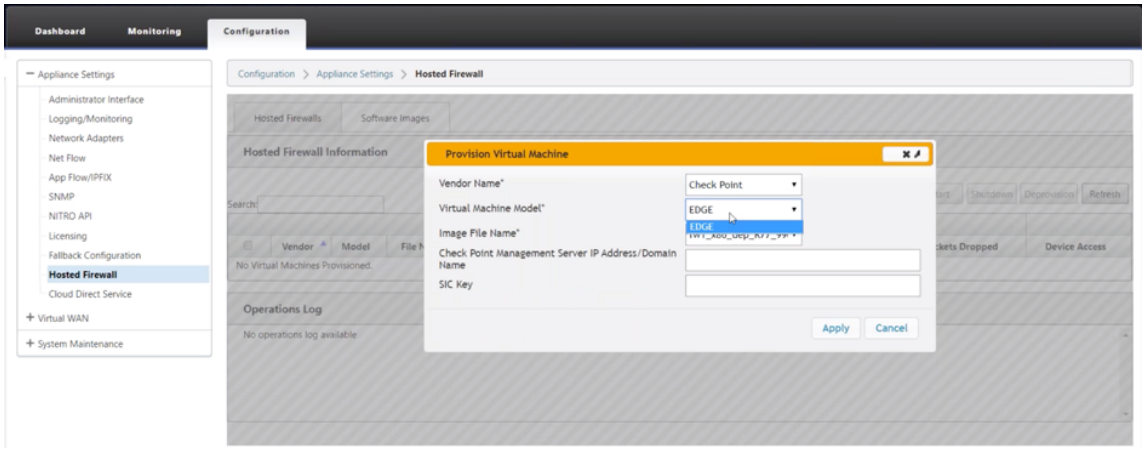
You can see a status bar to track the upload process. The file detail reflects, once the image is uploaded successfully. The image that is used for provisioning cannot be deleted. Do not perform any action or go back to any other page until the image file shows 100% uploaded.

3. For provisioning, select **Hosted Firewall** tab > click **Provision** button.

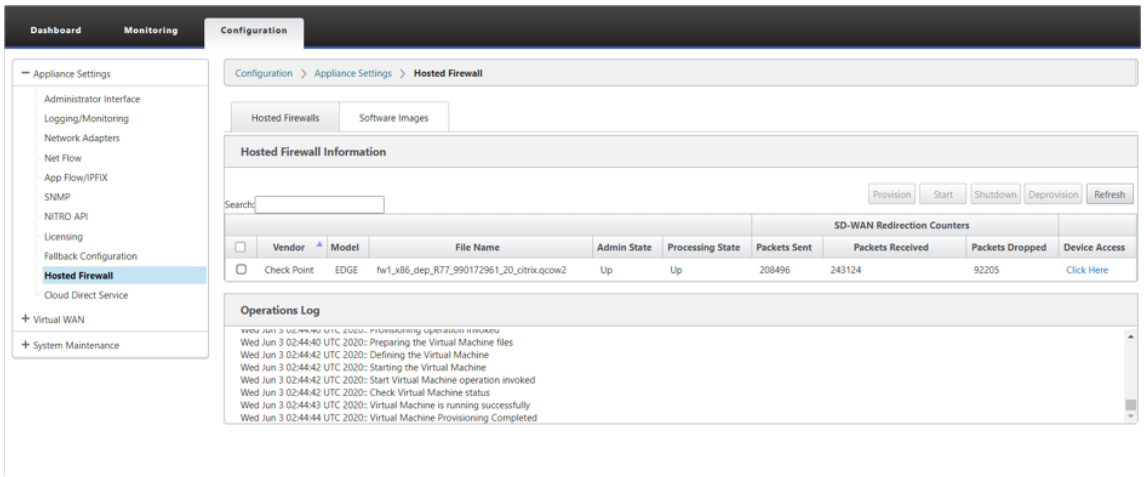


4. Provide the following details for provisioning.

   - **Vendor Name**: Select the **Vendor Name** as Check Point.
   - **Virtual Machine Model**: The virtual machine model is auto filled as **Edge**.
   - **Image File Name**: The image file name is auto-populated.
   - **Check Point Management Server IP Address/Domain**: Provide the check point management server IP address/domain.
   - **SIC Key**: Provide the SIC key (Optional). SIC creates trusted connections between **Check Point** components. Click **Apply**.



5. Click **Refresh** to get the latest status. After the Check Point virtual machine is completely bootup, it will reflect on the SD-WAN UI with the operations Log detail.



- **Admin State**: Indicates if the virtual machine is up or down.
- **Processing State**: Datapath processing state of the virtual machine.
- **Packet Sent**: Packets sent from SD-WAN to the security virtual machine.
- **Packet Received**: Packets received by SD-WAN from the security virtual machine.
- **Packet Dropped**: Packets dropped by SD-WAN (for example, when the security virtual machine is down).
- **Device Access**: Click the link to get the GUI access to the security virtual machine.

You can **Start, Shutdown,** and **Deprovision** the virtual machine as needed. Use **Click Here** option to access the Check Point virtual machine GUI or use your management IP along with 4100 port (management IP: 4100).

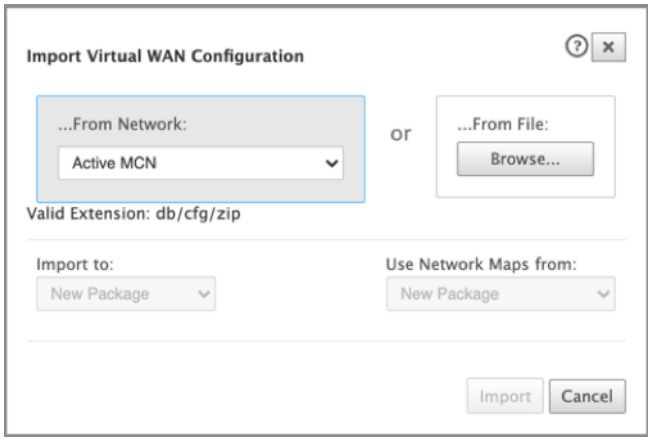
> **Note**
>
> Always use incognito mode to access the Check Point GUI.

Redirect traffic to Edge

Traffic redirection configuration can be done both through the Configuration Editor on MCN or Configuration Editor on SD-WAN Center.

To navigate through Configuration Editor on SD-WAN Center:

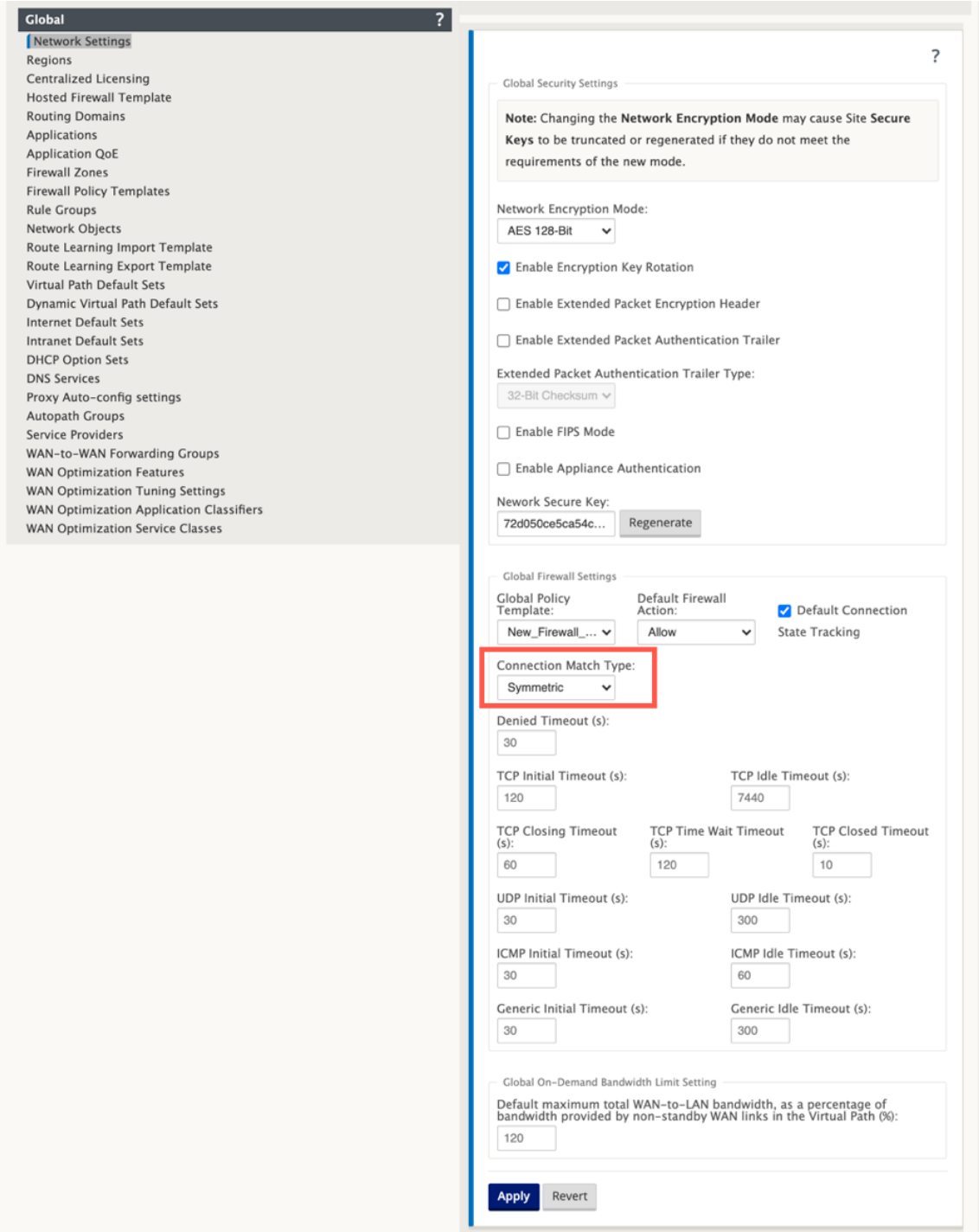
1. Open Citrix SD-WAN Center UI, navigate to **Configuration > Network Configuration Import**. Import the virtual WAN configuration from the active MCN and click **Import**.



Remaining steps are similar as following - the traffic redirection configuration through MCN.

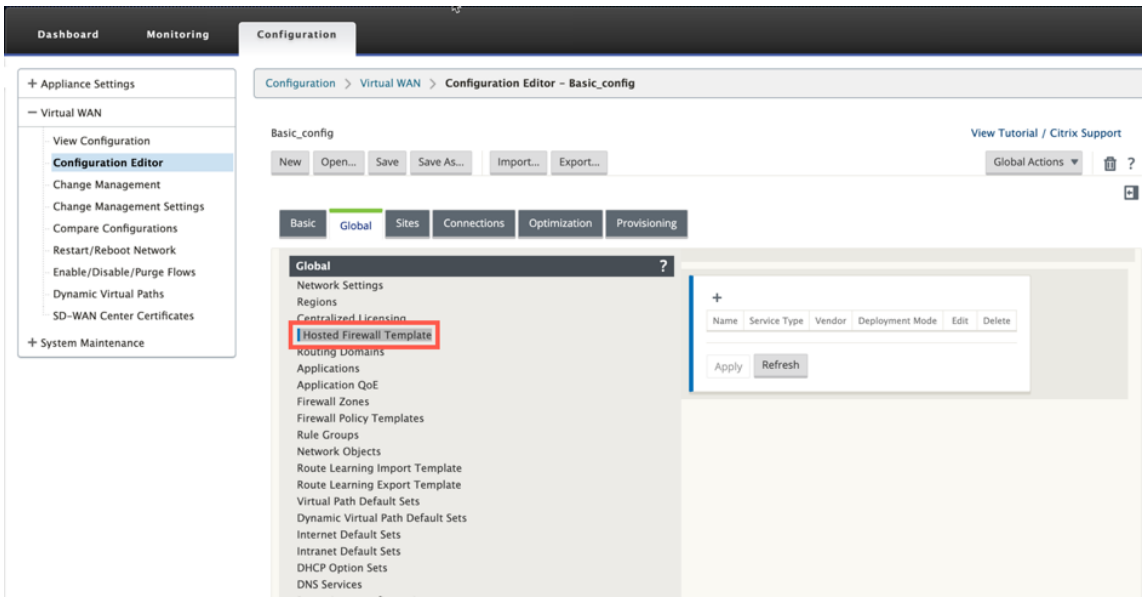
To navigate through Configuration Editor on MCN:

1. Set **Connection Match Type** to **Symmetric** under **Global > Networking Settings**.

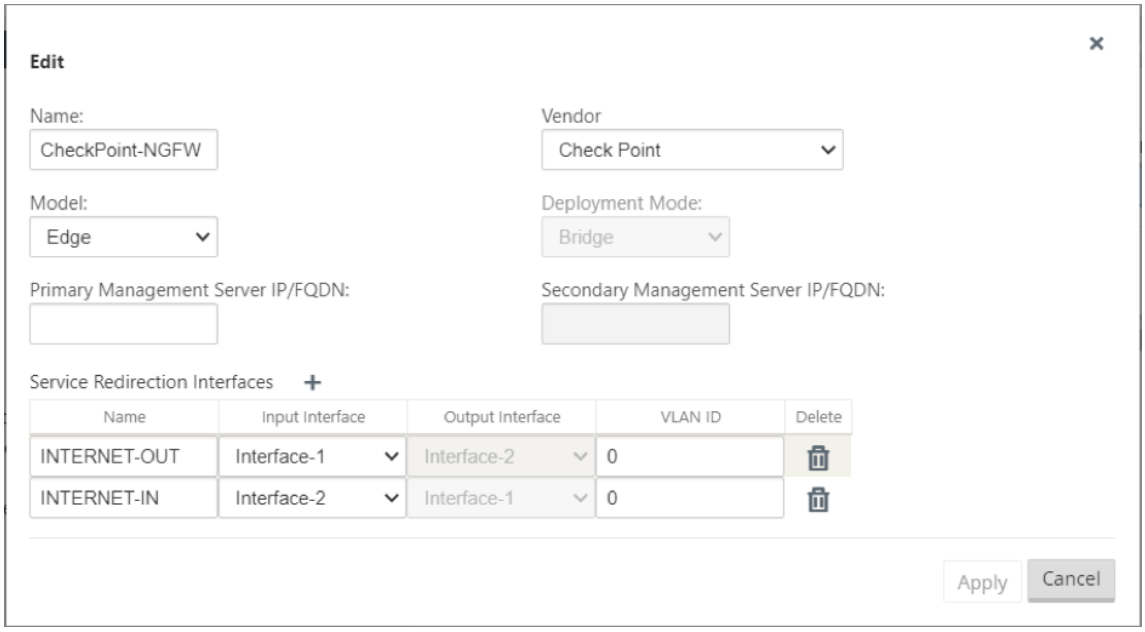


By default, SD-WAN firewall policies are direction specific. The Symmetric match type match the connections using specified match criteria and apply policy action on both directions.

2. Open Citrix SD-WAN UI, navigate to **Configuration >** expand **Virtual WAN >** select **Configuration Editor >** select **Hosted Firewall Template** under **Global** section.



3. Click **+** and provide the required information available in the following screenshot to add the **Hosted Firewall Template**. Click **Add**.



Hosted Firewall Template allows you to configure the traffic redirection to the **Firewall virtual machine** hosted on SD-WAN platform. The following are the inputs needed to configure the template:

- **Name**: The name of the hosted firewall template.
- **Vendor**: The name of the firewall vendor –Check Point.
- **Deployment Mode**: The **Deployment Mode** field is auto populated and grayed out. For the **Check Point** vendor, the deployment mode is **Bridge**.
- **Model**: Virtual Machine model of the hosted firewall. Once you selected the vendor as **Check**

Point, the model field is auto filled with **Edge**.

- **Primary Management Server IP/FQDN**: Primary management server IP/FQDN.
- **Secondary Management Server IP/FQDN**: Secondary management server IP/FQDN.
- **Service Redirection Interfaces**: These are logical interfaces used for traffic redirection between SD-WAN and hosted firewall.

> **Note**
>
> Redirection input interface has to be selected from connection initiator direction, output interface is automatically chosen for the response traffic. For Example, if outbound internet traffic is redirected to hosted firewall on Interface-1 then, response traffic is automatically redirected to hosted firewall on Interface-2. Also, there is no need of Interface-2 if there is no internet inbound traffic.

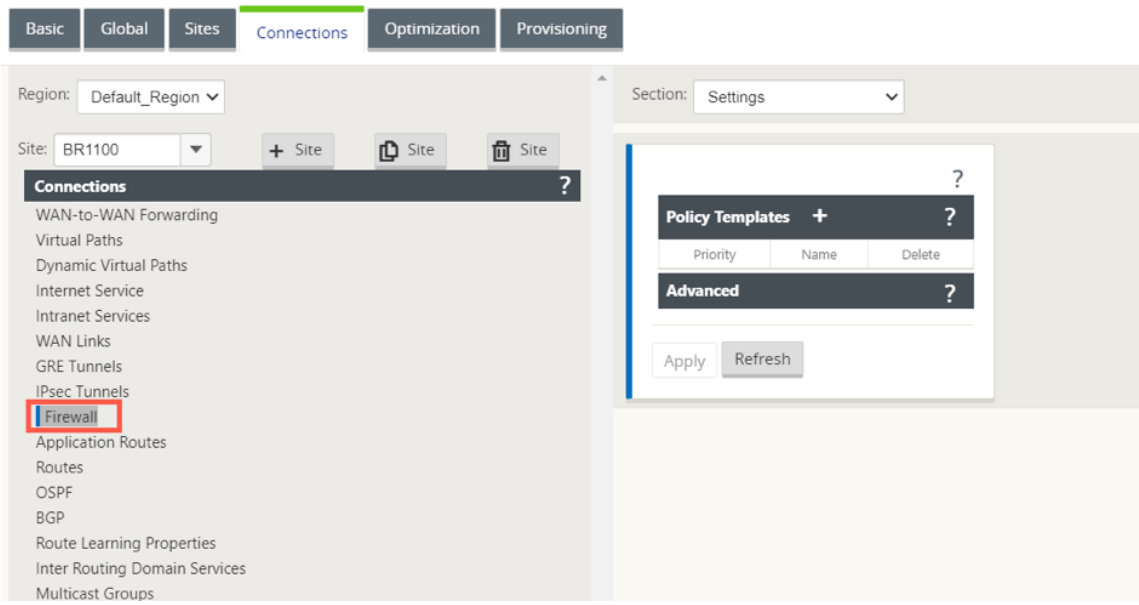
Only two data interfaces are assigned to Check Point virtual machine.

> **Note**
>
> SD-WAN firewall policies are auto created to **Allow** the traffic to/from hosted firewall management servers. This avoids redirection of the management traffic that is originated from (or) destined to the hosted firewall.

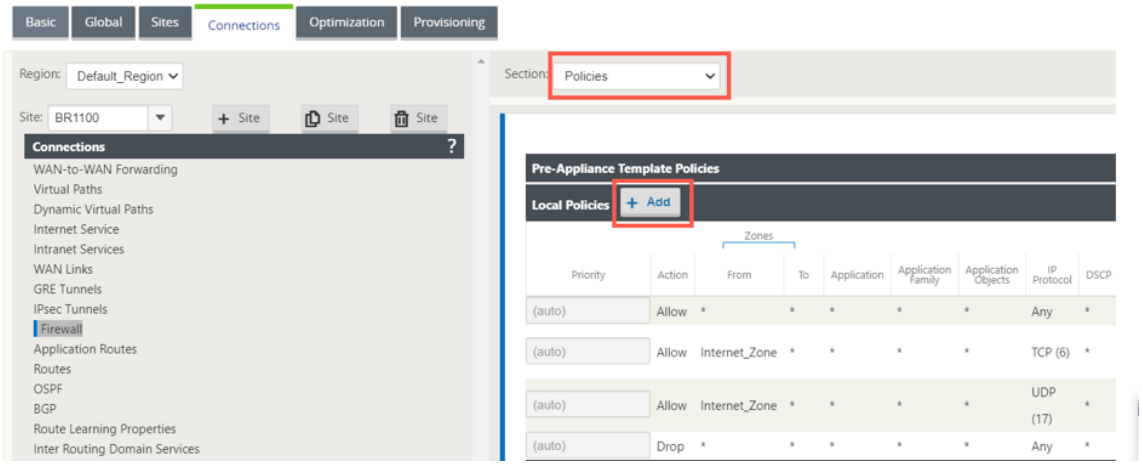
Traffic redirection to firewall virtual machine can be done using SD-WAN firewall policies. There are two methods to create SD-WAN firewall policies - either through firewall policy templates in **Global** section or site level.

Method - 1

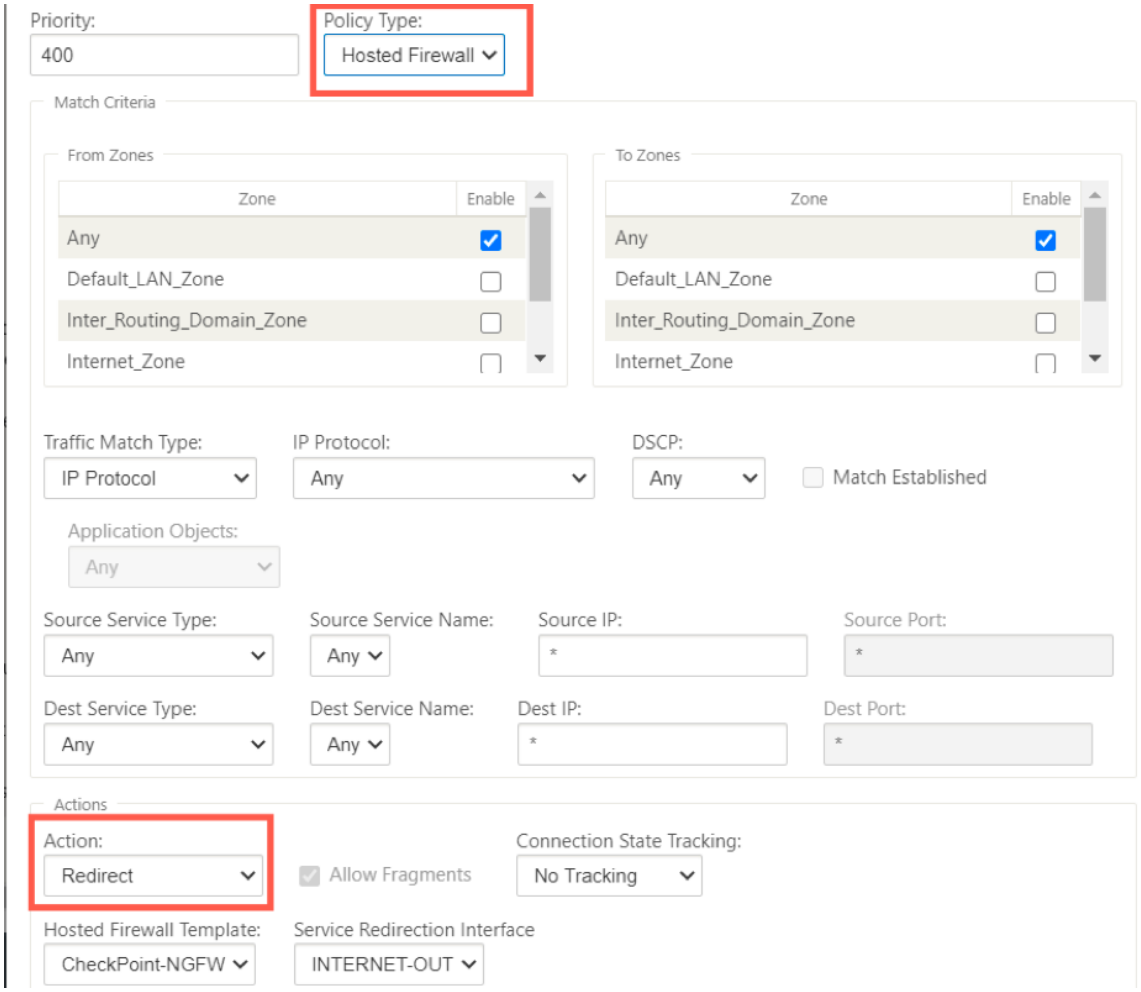
1. From Citrix SD-WAN GUI, navigate to **Configuration >** expand **Virtual WAN > Configuration Editor**. Select **Firewall** under **Connections**.



2. Select **Policies** from the **Section** drop-down list and click **+Add** to create a new firewall policy.

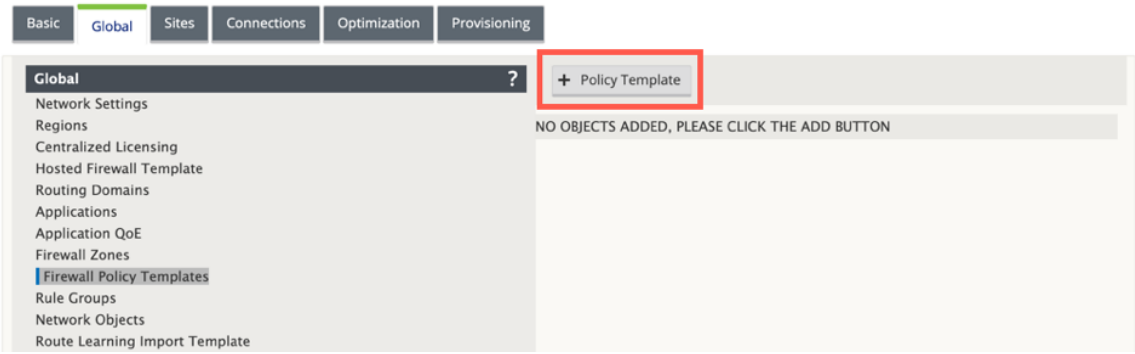


3. Change the **Policy Type** to **Hosted Firewall**. The **Action** field is auto filled to Redirect. Select the **Hosted Firewall Template** and the **Service Redirection Interface** from the drop-down list. Click **Add**.

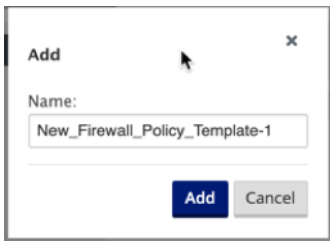


Method - 2

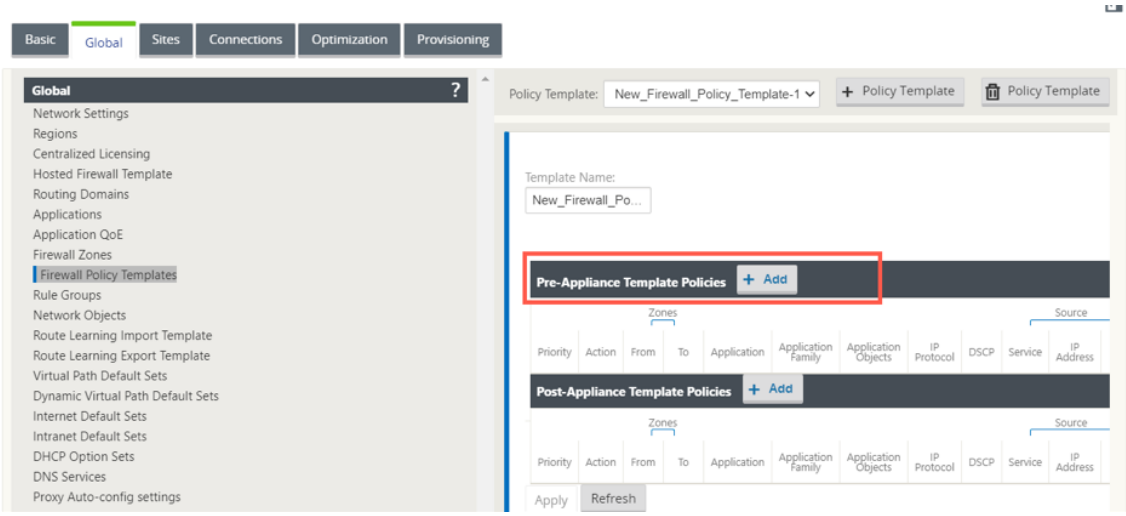
1. Navigate to the **Global** tab and select **Firewall Policy Templates**. Click **+ Policy Template**.



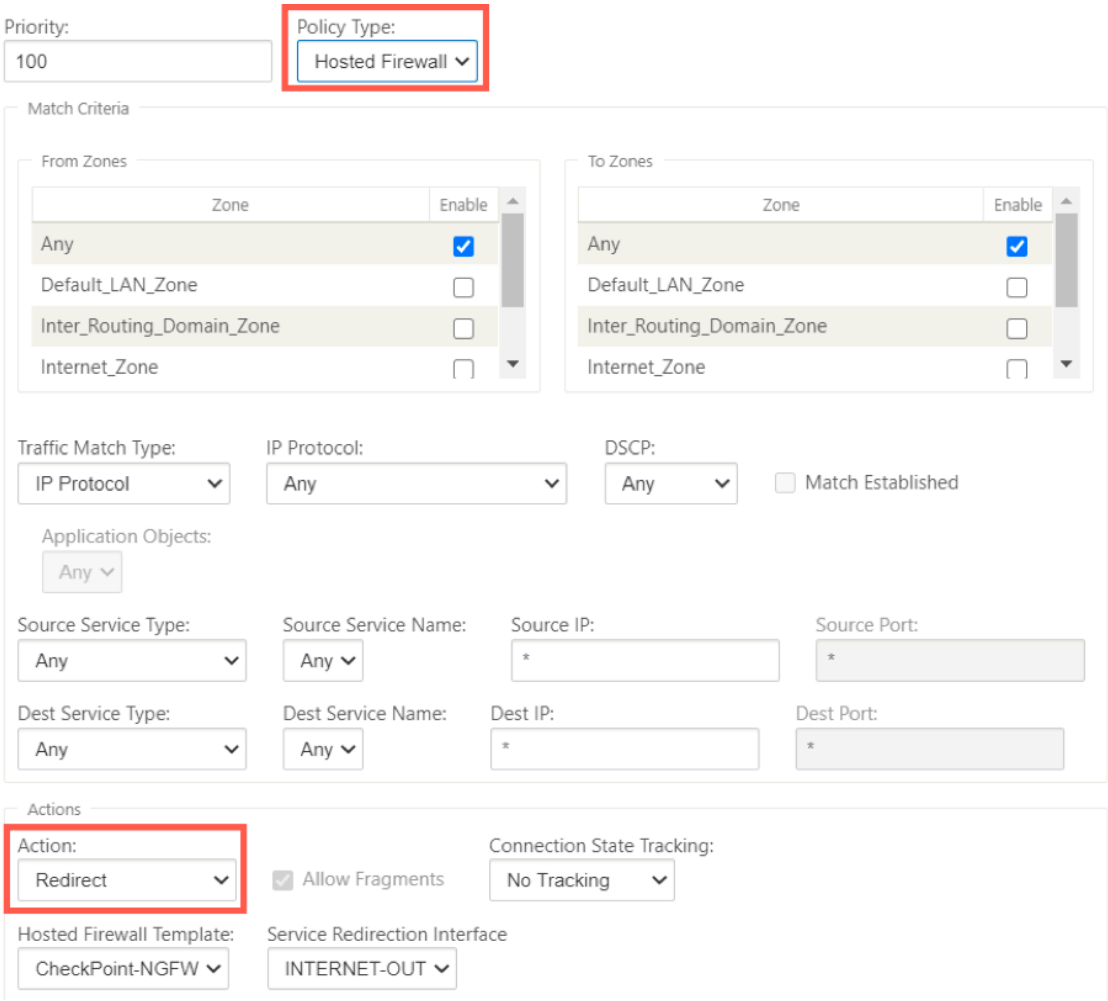
2. Provide the policy template a name and click **Add**.



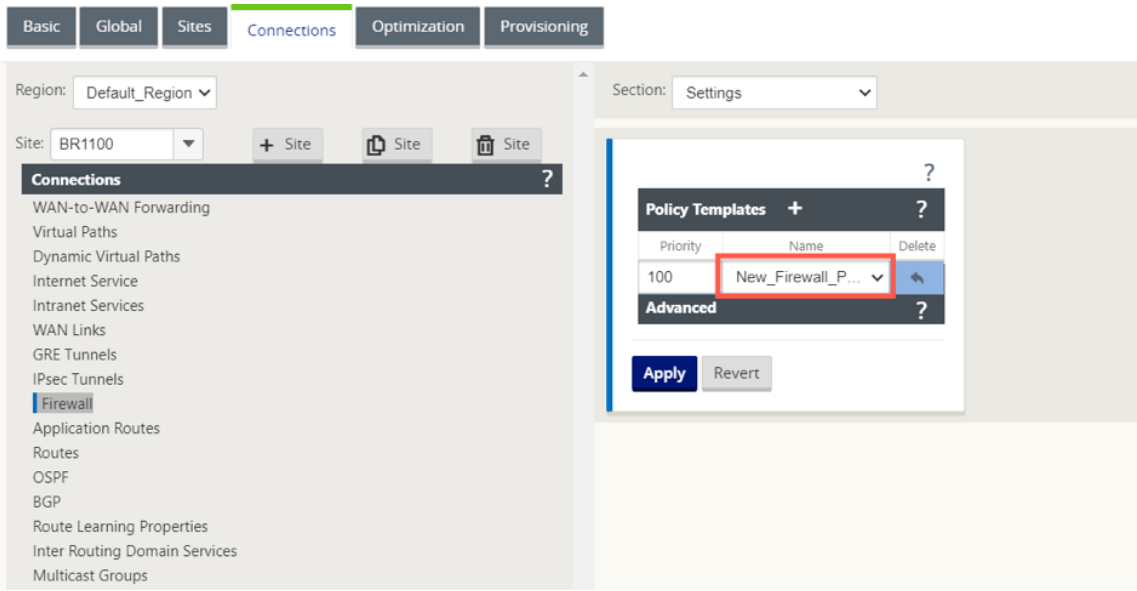
3. Click **+ Add** next to **Pre-Appliance Template Policies**.



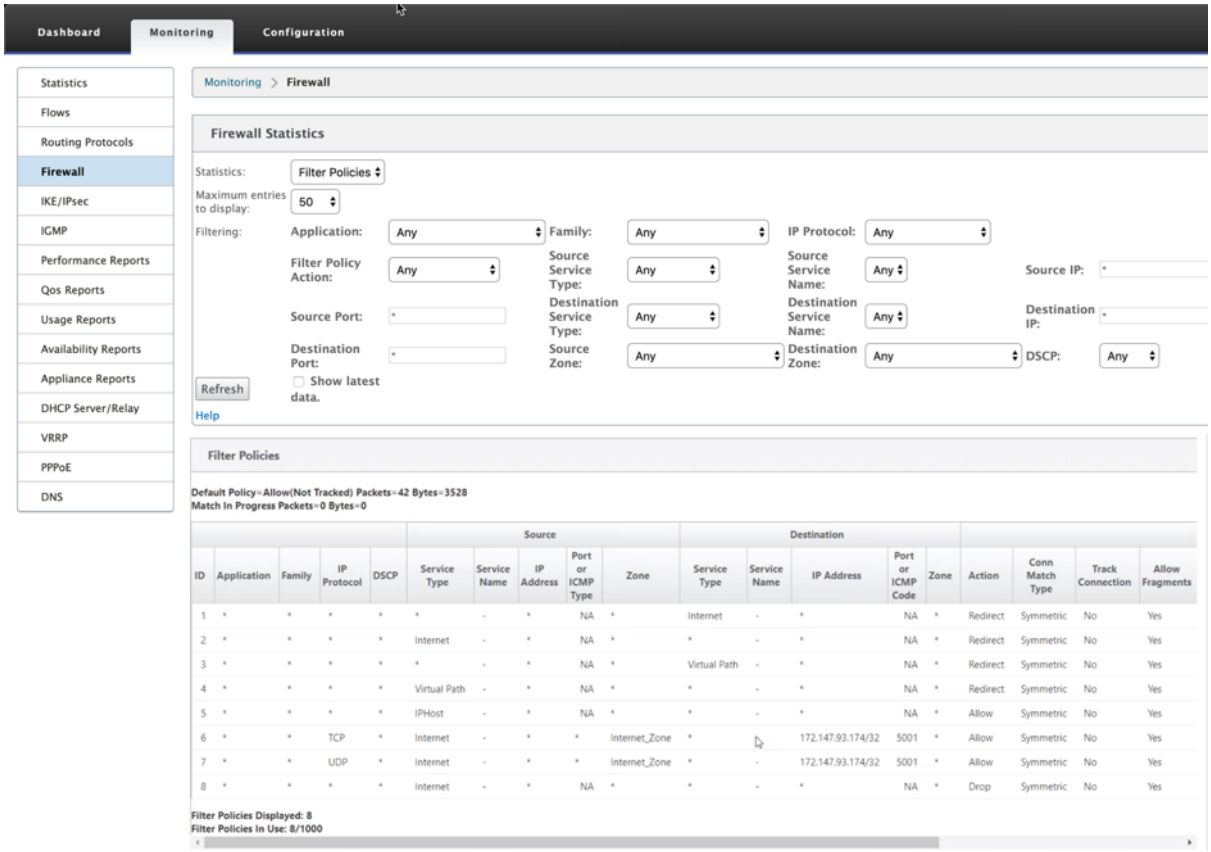
4. Change the **Policy Type** to **Hosted Firewall**. The **Action** field is auto filled to **Redirect**. Select the **Hosted Firewall Template** and the **Service Redirection Interface** from the drop-down list. Click **Add**.



5. Navigate to the **Connections > Firewall**, then select the firewall policy (that you have created) under the name field. Click **Apply**.



While all the network configuration is up and running mode, you can monitor the connection under **Monitoring > Firewall >** under **Statistics** list, select **Filter Policies**.



Link Aggregation Groups

May 24, 2021

The Link Aggregation Groups (LAG) functionality allows you to group two or more ports on your SD-WAN appliance to work together as a single port. This ensures increased availability, link redundancy, and enhanced performance.

Citrix SD-WAN supports simple LAG (ACTIVE-BACKUP). The 802.3ad LACP protocol based negotiations are not supported in the current release. At any time only one port is active and the other ports are in backup mode. The active and backup supports rely on the Data Plane Development Kit (DPDK) package for LAG functionality. The LAG functionality is available only on the following DPDK supported platforms:

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE

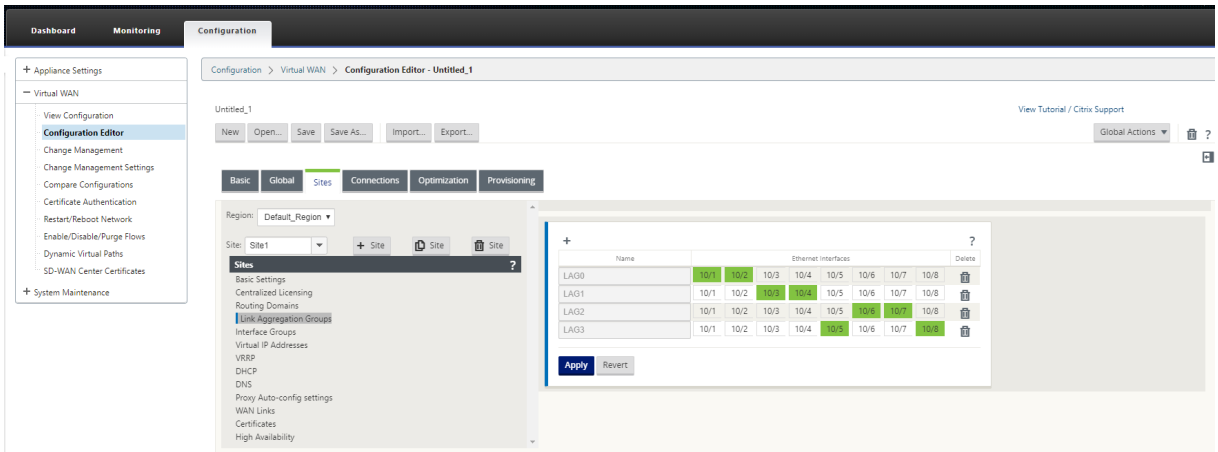
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 4000, 4100, and 5100 SE
- Citrix SD-WAN 6100 SE
- Citrix SD-WAN 2100 SE

> **Note**
>
> The LAG functionality is not supported on VPX/VPXL platforms.

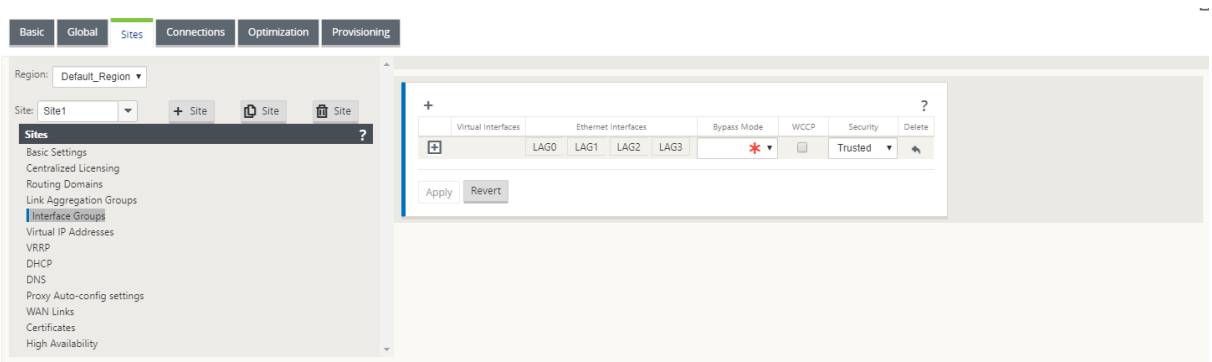
You can create a maximum of four LAGs with a maximum of four ports grouped in each LAG on the Citrix SD-WAN appliances.

> **Note**
>
> For Citrix SD-WAN 210 and 410 appliances, you can create only one LAG with a maximum of three ports grouped in it.

To configure Link aggregation groups, in the **Configuration Editor**, navigate to **Sites** > **Link Aggregation Groups**. You can view all the available physical ports and Ethernet interfaces. Click **+** to create a LAG.



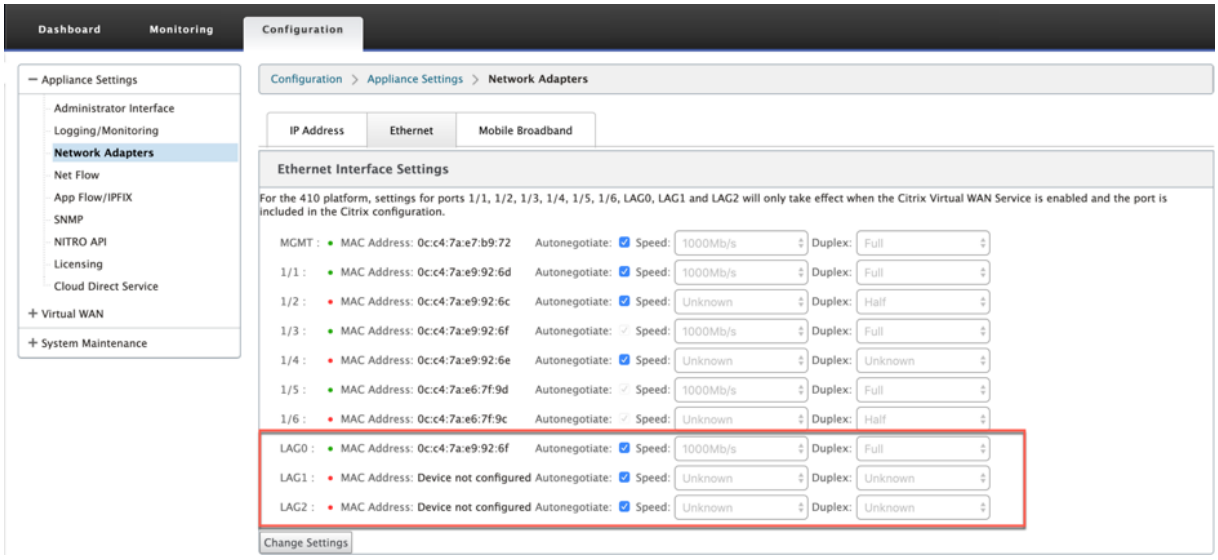
Select the member ports, and click **Apply**. Once the ports are added to the LAG, you can see only the LAGs in the **Interface Group** instead of the member ports.



You can create virtual interfaces using LAGs and these interfaces are further used to configure LAN/WAN links and HA.

> **Note**
>
> The Link State Propagation (LSP) feature is not supported, if LAGs are used as Ethernet interfaces in Interface Groups.

You can view the active and standby LAG ports, navigate to **Configuration** > **Appliance Settings** > **Network Adapters** > **Ethernet**.



> **Note**
>
> You cannot change settings for individual member ports, any configuration changes made to the LAG, is automatically pushed to the member ports.

Link state propagation

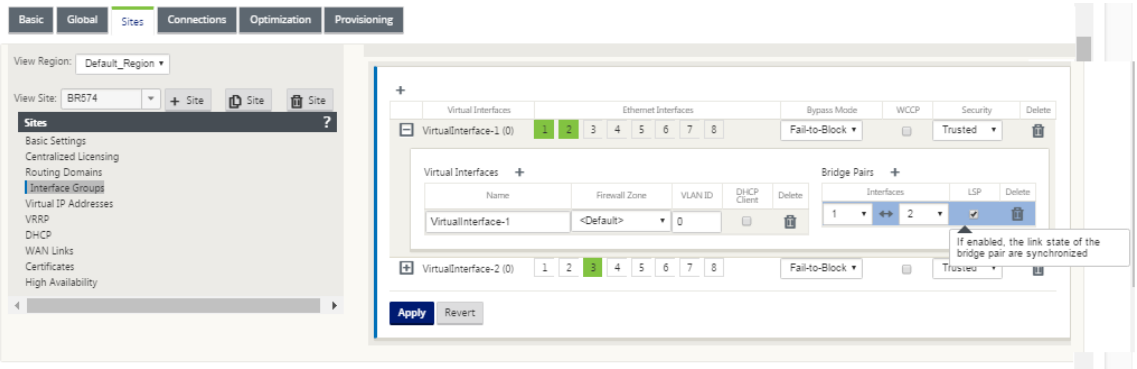
March 12, 2021

The Link state propagation (LSP) 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 automatically becomes active.

How to configure link state propagation

To configure link state propagation:

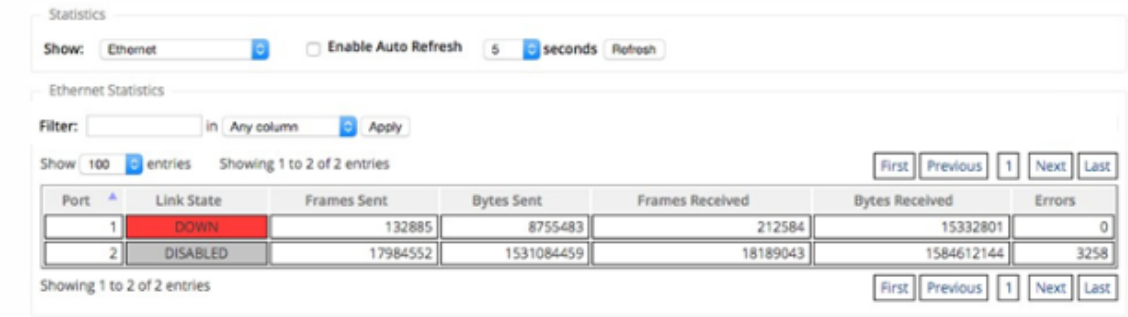
1. Navigate to **Configuration Editor** > **Sites** > **[Site Name]** > **Interface Groups**.
2. Expand **Virtual Interfaces** and under **Bridge Pairs**, click the **LSP** checkbox to enable **Link State Propagation** for a Bridge Pair. Click **Apply** to save the settings.



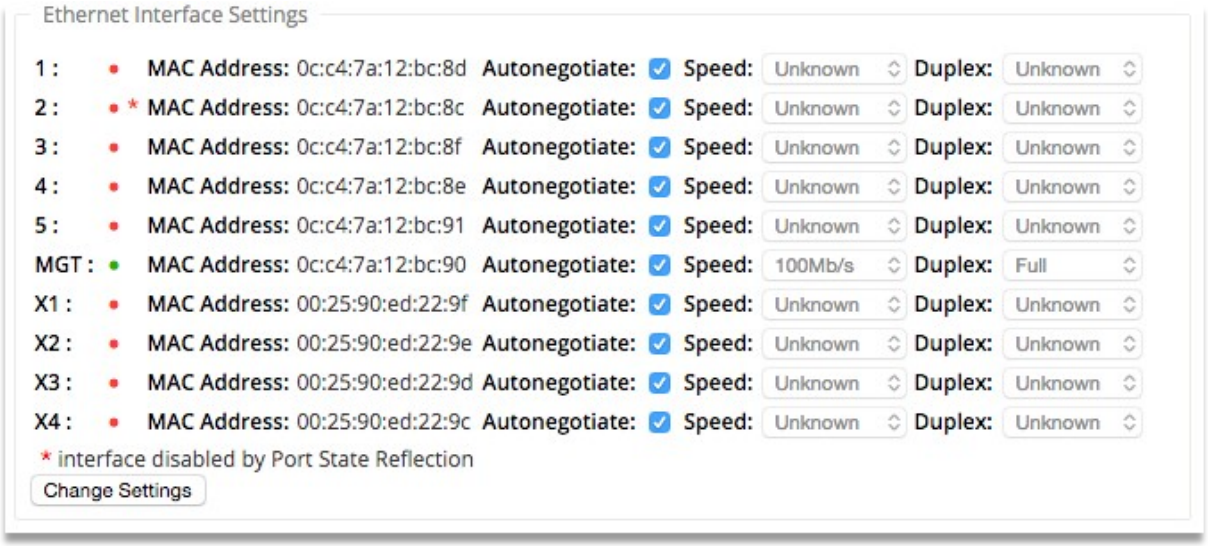
Monitoring link statistics

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 later the WAN side link of the bypass pair is administratively DISABLED.



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.



Metering and Standby WAN Links

March 12, 2021

Citrix 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 (that is, MPLS, Broadband Internet, 4G/LTE) and one of the WAN links is 4G/LTE and might be too costly for a business to allow usage unless it is 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 Cycle (weekly/monthly)
- Start Date
- Standby Mode
- Priority
- 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

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 the SD-WAN Center. A metered path can be formed with 1 or 2 metered links. If a path is formed between two 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 one non-metered path that is in GOOD state, a metered path carries the 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**: The standby link that becomes active when one of the conditions is met.

  When the available bandwidth in the virtual path is less than the configured on-demand bandwidth limit AND there is sufficient usage. Sufficient usage is 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.

- 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

When configuring a standby link, you can specify standby priority and two heartbeat intervals:

- **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.

- **On-Demand** - An on-demand standby path is formed between:
  - a non-standby link and an on-demand standby link
  - 2 on-demand standby links
- **Last-Resort** - 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 are used when the standby path is standby.
- If active heartbeat interval is configured on both links, then the larger of the two values are 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:
  - 50 ms when the path state is GOOD
  - 25 ms when the path state is BAD

On a standby path, the heartbeat interval used depends on the activity state and the path state:

- While inactive, if the 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 goes BAD and then DEAD. If connectivity with the Virtual Path peer is re-established, the path goes 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 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 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 recalculated considering the standby path's MTU. (The Virtual Path's MTU is the smallest path MTU among all active paths within the Virtual Path).

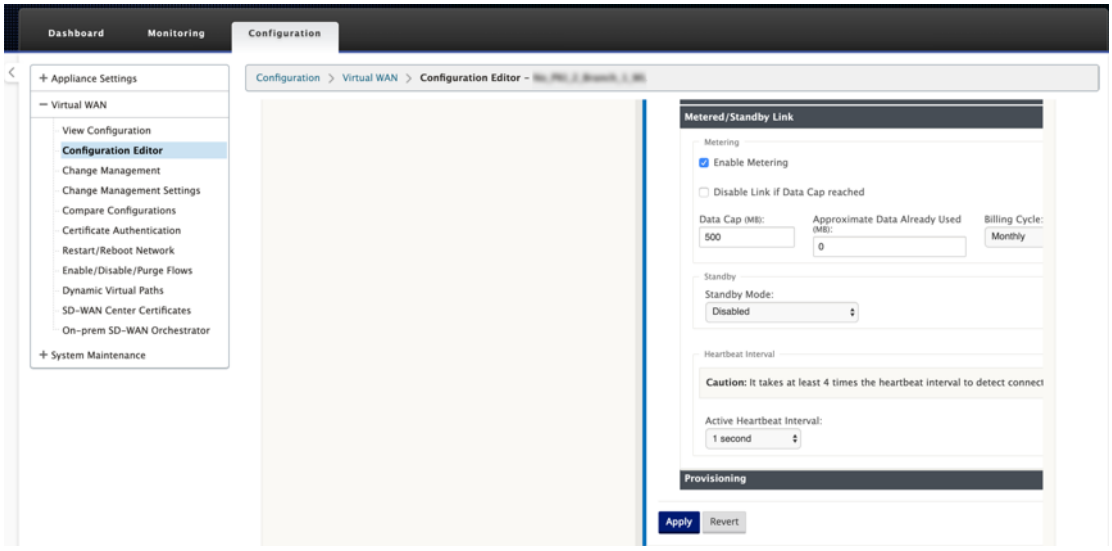
Events and log messages are generated when a standby path transitions between standby and active.

Configuration pre-requisites:

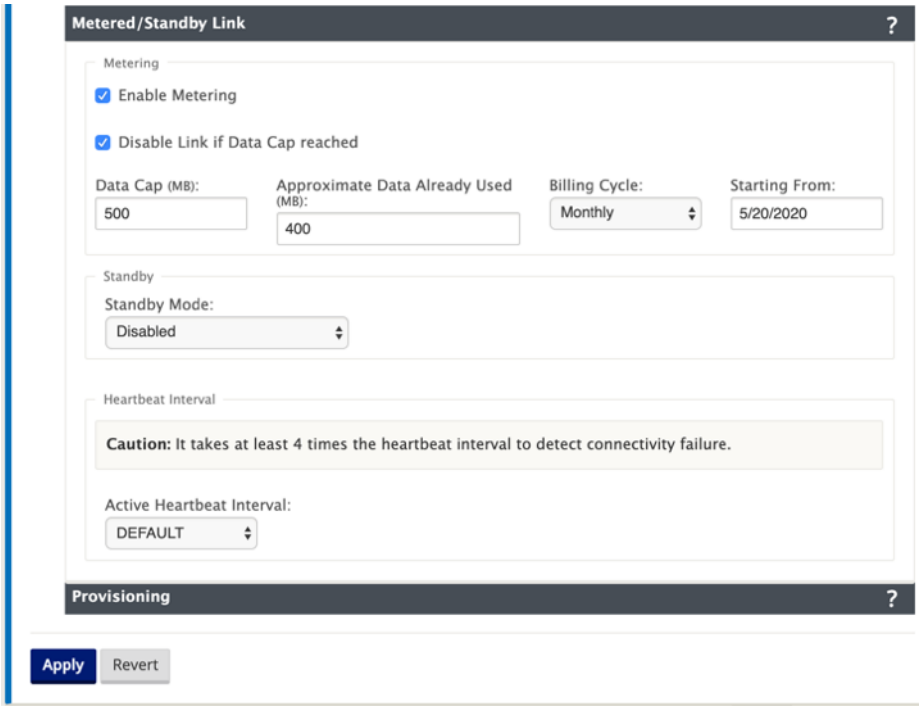
- A meter link might be of any access type.
- All links at a site can be configured with metering enabled.
- A standby link might be of Public Internet or Private Intranet access type. A WAN link of Private MPLS access type cannot be configured as a standby link.
- At least one non-standby link must be configured per site. A maximum of 3 standby links per site is supported.
- Internet/Intranet services might not be configured on on-demand standby links. On-demand standby links support Virtual Path service only.
- Internet service might be configured on a last-resort standby link, but only load balance mode is supported.
- Intranet service might 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 > Virtual WAN >** select **Configuration Editor >** add or select **Sites** from the drop-down list > select **WAN Links >** Click **Metered/Standby Link** tab to expand it.



2. Check the **Enable Metering** check box. You can provide values for Data cap, Billing cycle start date, Approximate Usage Already Used, and the Active heartbeat interval.

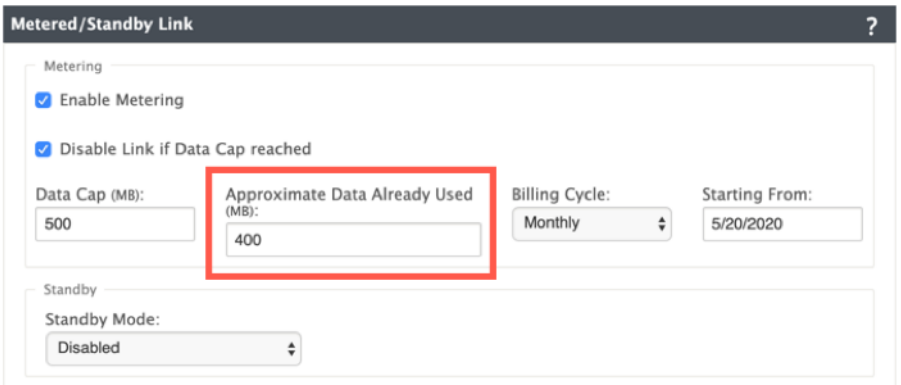


3. Disable Link if Data Cap reached:

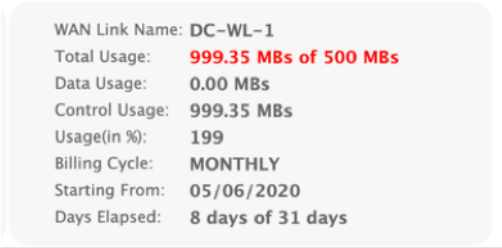
   - If the **Disable Link if Data Cap reached** check box is selected, then the metered link and all its related paths will be disabled until the next billing cycle, if the data usage reaches the data cap.
   - By default, the **Disable Link if Data Cap reached** check box will be unchecked state, where it retains the current mode or state set for the metered link to be continued after the data cap is reached until the next billing cycle.

4. If the metered link is configured, you can provide the approximate data already used in MB for the metered link.

   To track the proper metered link usage, you must enter the approximate usage on the metered link if the link has already been used for some days in the current billing cycle. This approximate usage is only for the first cycle. Total usage since the start date to the current date is calculated and shown in the dashboard.

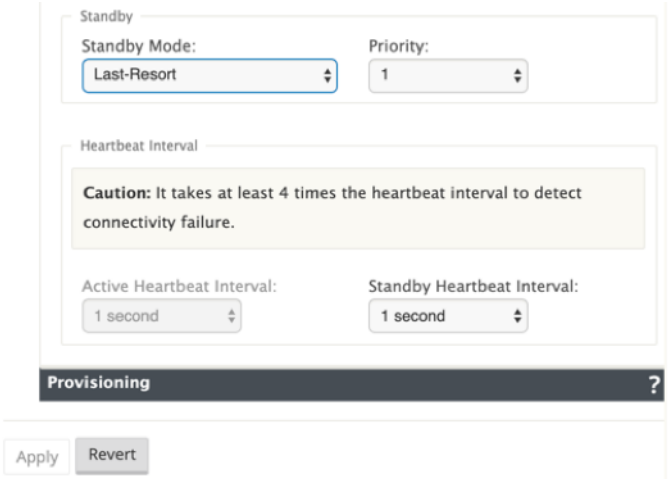


After you perform the configuration update, you can view the usage details on the dashboard.

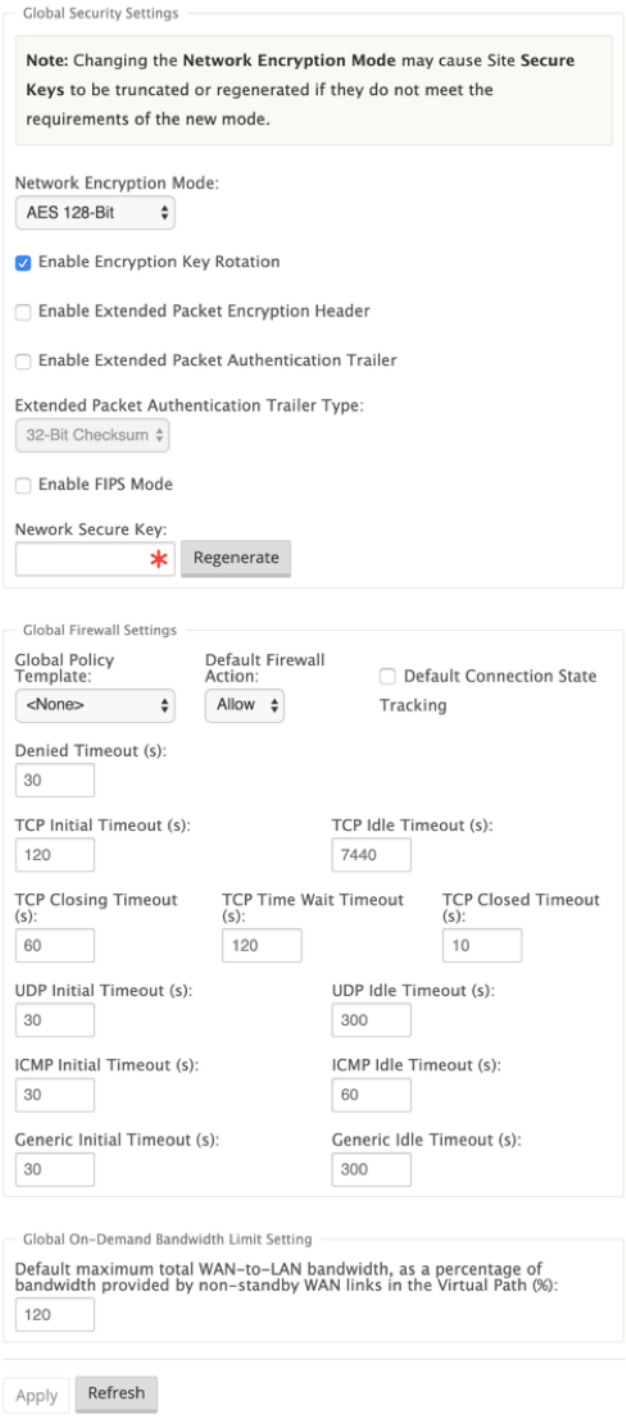


To configure standby links:

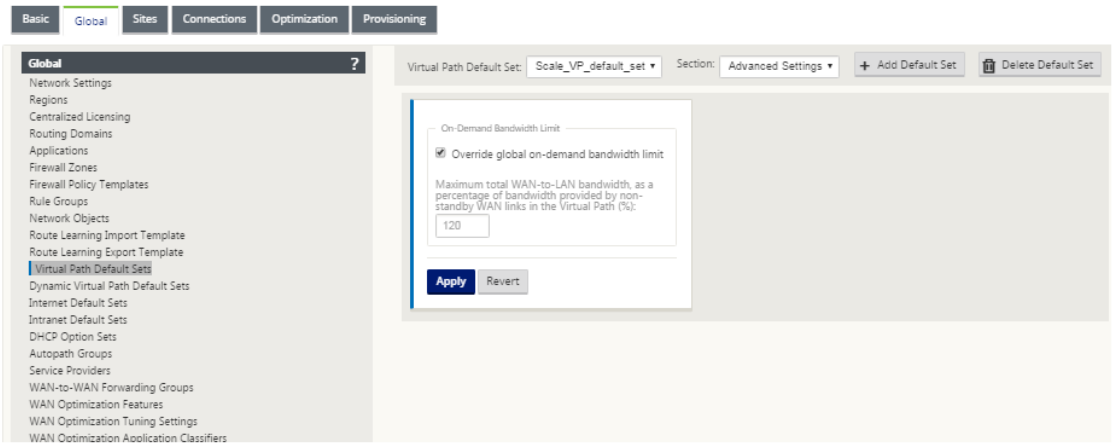
1. By default, the standby mode of a WAN link is disabled. To configure the WAN link as standby, select one of the standby modes (Last-Resort/On-Demand) from the drop-down list.



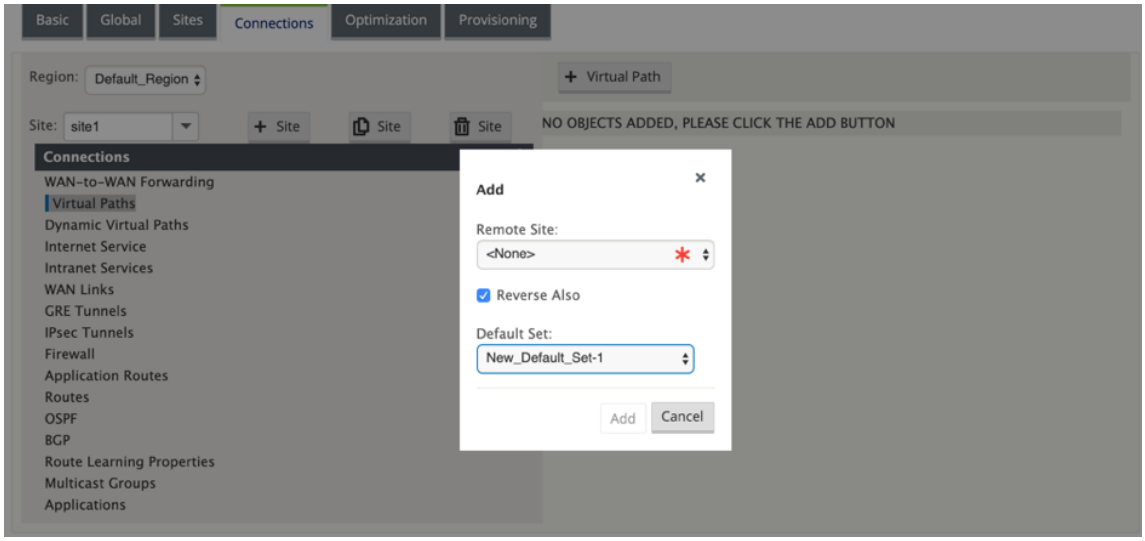
2. Once a standby mode is selected, select the standby priority, active heartbeat interval, and standby heartbeat interval as appropriate. Click **apply** to validate the configuration.
3. If an on-demand standby link is configured, the global default on-demand bandwidth limit (120%) is applied to the 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 attempts to activate on-demand paths to supplement bandwidth.
4. To view or change the global default on-demand bandwidth limit, open the sections **Global** > **Virtual WAN Network** Settings.



5. 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 must be created and the on-demand bandwidth limit in the Advanced Settings can be changed.



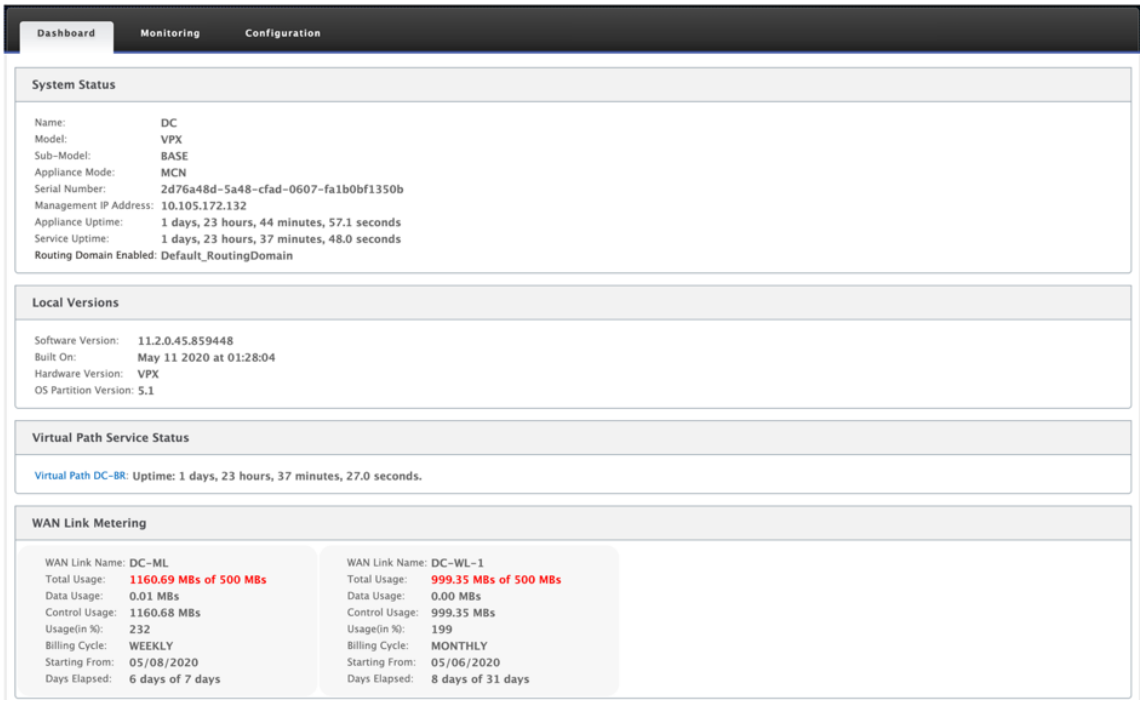
6. To apply settings for a specific Virtual Path, navigate to the section **Connections > Virtual Paths** and click **+ Virtual Path**.



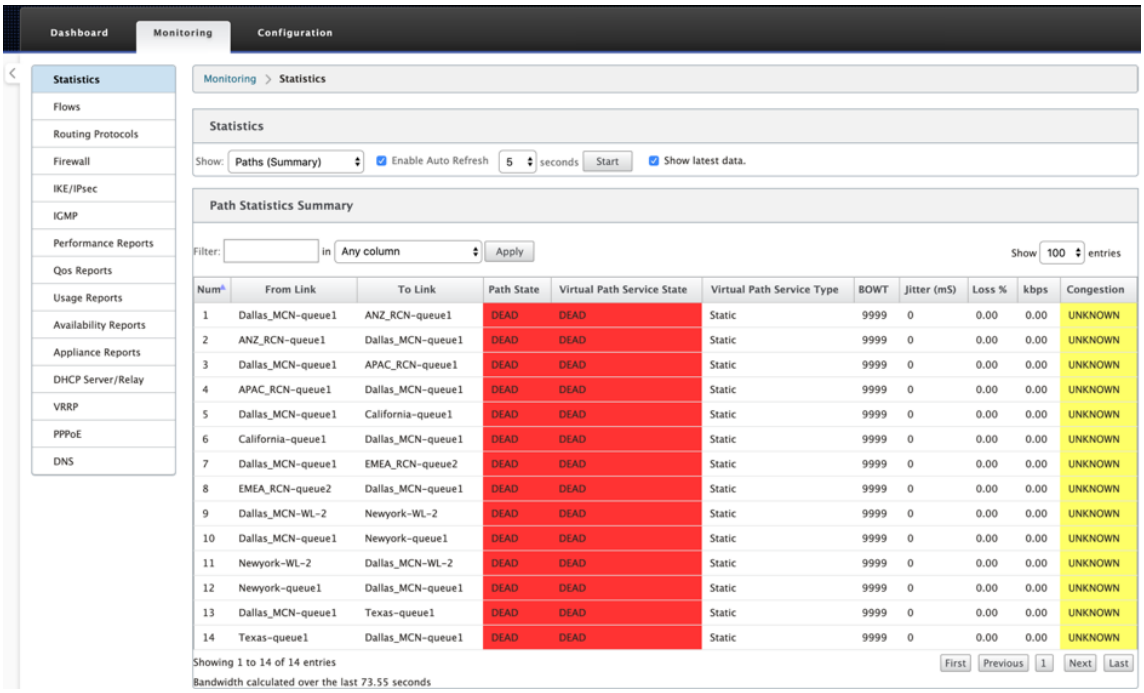
Monitor metered and standby WAN links

- The Dashboard page provides the following **WAN Link Metering** information with the usage values:
  - **WAN Link Name**: Displays the WAN link name.
  - **Total Usage**: Displays the total traffic usage (Data usage + Control usage).
  - **Data Usage**: Displays the usage by user traffic.
  - **Control Usage**: Displays the usage by control traffic.
  - **Usage (in %)**: Displays the used data cap value in percentage (Total Usage/Data Cap) x 100.
  - **Billing Cycle**: Billing frequency (weekly/monthly)
  - **Starting From**: Start date of the billing cycle

– **Days Elapsed**: The time elapsed (in days, hours, minutes, and seconds)

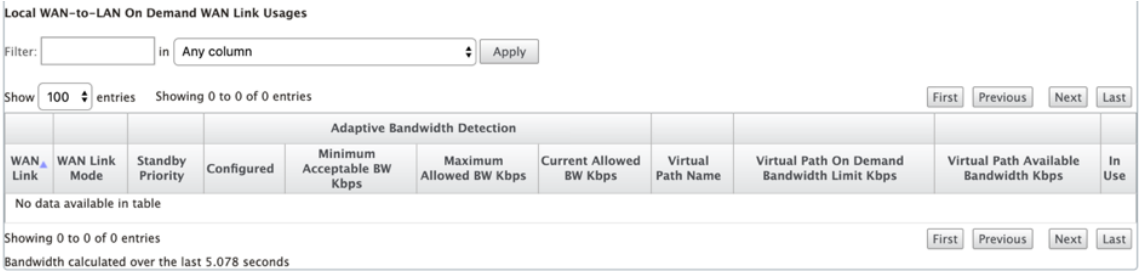


- When path statistics (**Monitoring > Statistics > Paths**) are displayed, metered links and standby links are marked as shown in the screenshot.

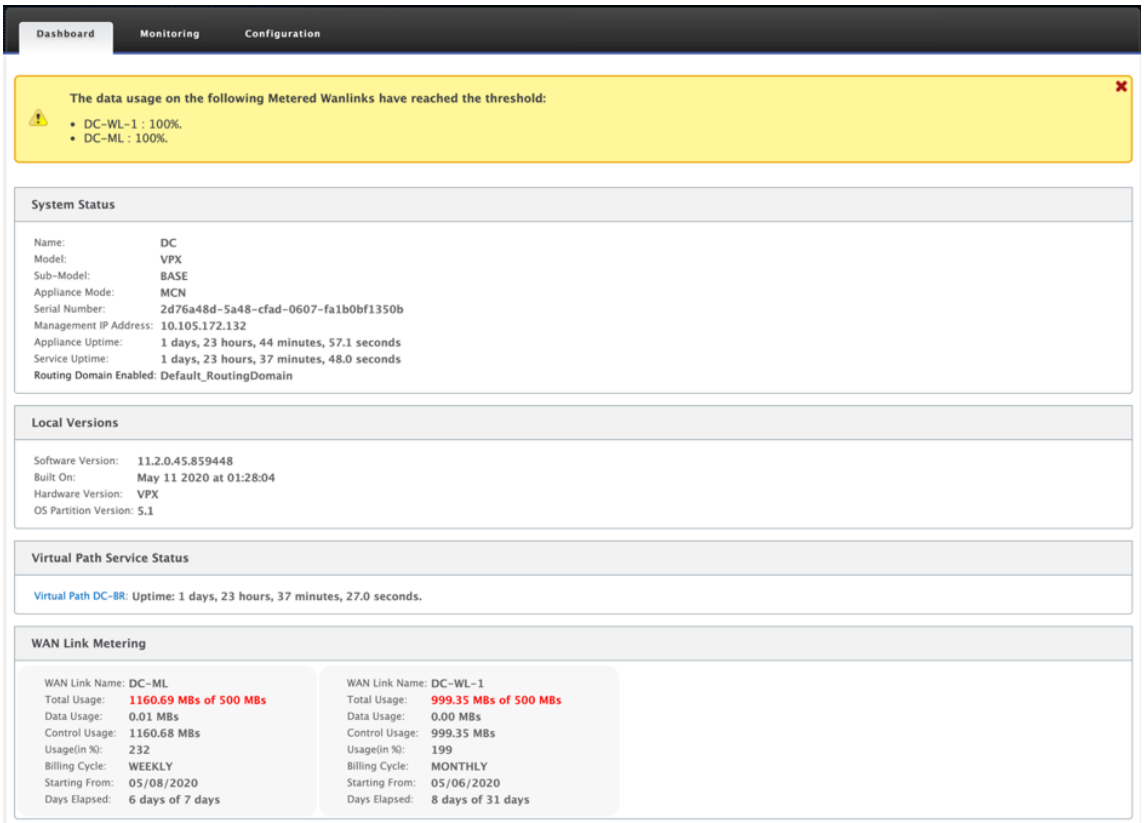


Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	Dallas_MCN-queue1	ANZ_RCN-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
2	ANZ_RCN-queue1	Dallas_MCN-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
3	Dallas_MCN-queue1	APAC_RCN-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
4	APAC_RCN-queue1	Dallas_MCN-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
5	Dallas_MCN-queue1	California-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
6	California-queue1	Dallas_MCN-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
7	Dallas_MCN-queue1	EMEA_RCN-queue2	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
8	EMEA_RCN-queue2	Dallas_MCN-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
9	Dallas_MCN-WL-2	Newyork-WL-2	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
10	Dallas_MCN-queue1	Newyork-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
11	Newyork-WL-2	Dallas_MCN-WL-2	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
12	Newyork-queue1	Dallas_MCN-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
13	Dallas_MCN-queue1	Texas-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
14	Texas-queue1	Dallas_MCN-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN

- 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 extra table showing on-demand bandwidth is displayed at the bottom of the page (**Monitoring > Statistics > WAN Link Usage**).



- 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 is highlighted.

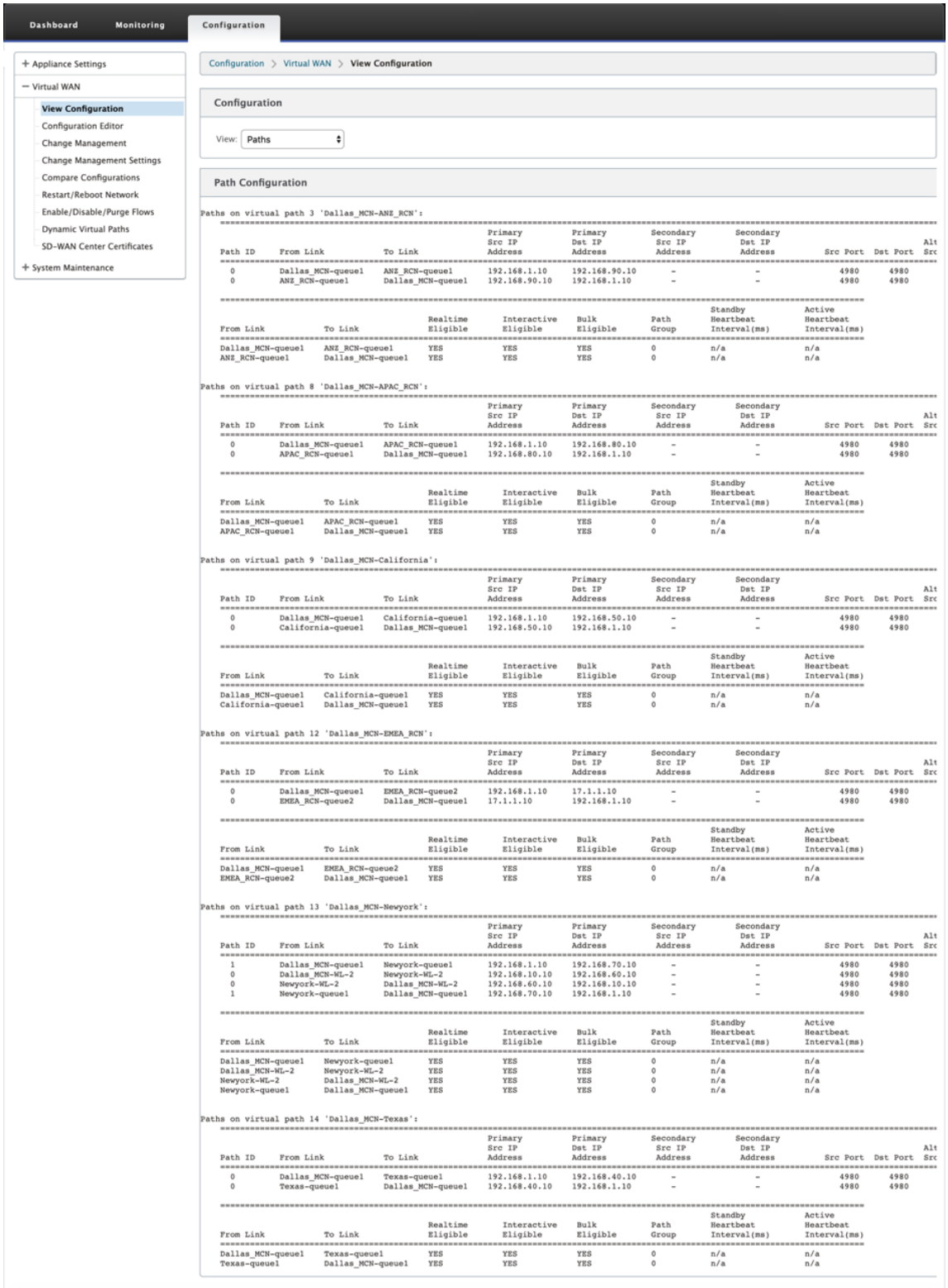


A WAN link usage event is also generated at the appliance when the usage exceeds 50%, 75%, and 90% of the configured data cap.

1. 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-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become standby
24639	1	RL-TB-MCN-WL-1->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become standby
24638	1	RL-TB-CL2-WL-1->RL-TB-MCN-WL-2	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-2 state has changed from BAD to GOOD because notified by peer.
24637	2	RL-TB-MCN-WL-2->RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24636	2	RL-TB-MCN RL-TB-CL2	VIRTUAL PATH	2017-05-26 10:18:27	GOOD	NOTICE	The state of Virtual Path RL-TB-MCN-RL-TB-CL2 has changed from BAD to GOOD
24635	0	RL-TB-CL2-WL-1->RL-TB-MCN-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-1 state has changed from BAD to GOOD because notified by peer.
24634	0	RL-TB-MCN-WL-1->RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24633	3	RL-TB-MCN-WL-2->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become active
24632	1	RL-TB-MCN-WL-1->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become active

2. The configured active and standby heartbeat intervals for each path can be viewed at **Configuration** > **Virtual WAN** > **View Configuration** > **Paths**.



Office 365 optimization

March 12, 2021

The **Office 365 Optimization** features adhere to the Microsoft Office 365 Network Connectivity Principles, to optimize Office 365. Office 365 is provided as a service through several service endpoints (front doors) located globally. To achieve optimal user experience for Office 365 traffic, Microsoft recommends redirecting Office365 traffic directly to the Internet from branch environments and avoiding practices such as backhauling to a central proxy. This is because Office 365 traffic such as Outlook, Word, and so on are sensitive to latency and backhauling traffic introduces more latency resulting in poor user experience. Citrix SD-WAN allows you to configure policies to break out Office 365 traffic to the Internet.

The Office 365 traffic is directed to the nearest Office 365 service endpoint, which exists at the edges of Microsoft Office 365 infrastructure worldwide. Once traffic reaches a front door, it goes over Microsoft's network and reaches the actual destination. This minimizes latency as the round trip time from the customer network to the Office 365 endpoint reduces.

Office 365 endpoints

Office 365 endpoints are a set of network addresses and subnets. Endpoints are segregated into the following three categories:

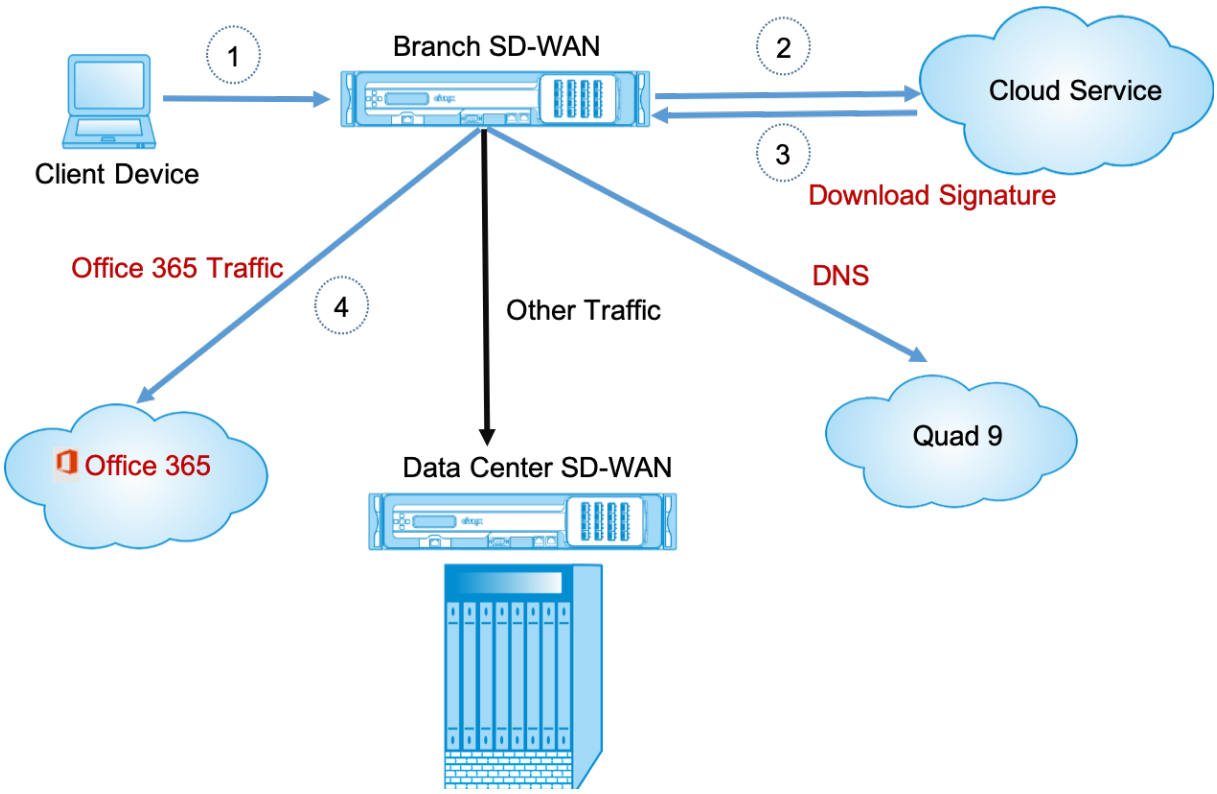
- **Optimize** - These endpoints provide connectivity to every Office 365 service and feature, and are sensitive to availability, performance, and latency. It represents over 75% of Office 365 bandwidth, connections, and volume of data. All the Optimize endpoints are hosted in Microsoft data centers. Service requests to these endpoints should breakout from the branch to the Internet and should not go through the data center.
- **Allow** - These endpoints provide connectivity to specific Office 365 services and features only, and are not so sensitive to network performance and latency. The representation of Office 365 bandwidth and connection count is also lower. These endpoints are hosted in Microsoft data centers. Service requests to these endpoints may breakout from the branch to the Internet or may go through the data center.
- **Default** - These endpoints provide Office 365 services that do not require any optimization, and can be treated as normal Internet traffic. Some of these endpoints may not be hosted in Microsoft data centers. The traffic in this category is not susceptible to variations in latency. Therefore, direct breaking out of this type of traffic does not cause any performance improvement when compared to Internet breakout. In addition, the traffic in this category may not always be Office 365 traffic, hence it is recommended to disable this option when enabling Office 365 breakout in your network.

How Office 365 optimization works

The Microsoft endpoint signatures are updated at most once a day. Agent on the appliance polls the Citrix service (sdwan-app-routing.citrixnetworkapi.net), every day to obtain the latest set of end-point signatures. The SD-WAN appliance polls the Citrix service (sdwan-app-routing.citrixnetworkapi.net), once every day, when the appliance is turned on and Office 365 optimization is enabled. If there are new signatures available, the appliance downloads it and stores it in the database. The signatures are essentially a list of URLs and IPs used to detect Office 365 traffic based on which traffic steering policies can be configured.

> **Note**
>
> First packet detection and classification of Office 365 traffic is performed only if the Office 365 breakout feature is enabled.

When a request for Office 365 application arrives, the application classifier, does a first packet classifier database lookup, identifies, and marks Office 365 traffic. Once the Office 365 traffic is classified, the auto created application route and firewall policies take effect and breaks out the traffic directly to the Internet. The Office 365 DNS requests are forwarded to specific DNS services like Quad9. For more information, see Domain name system.



The signatures are downloaded from Cloud Service (sdwan-app-routing.citrixnetworkapi.net).

Configure Office 365 breakout

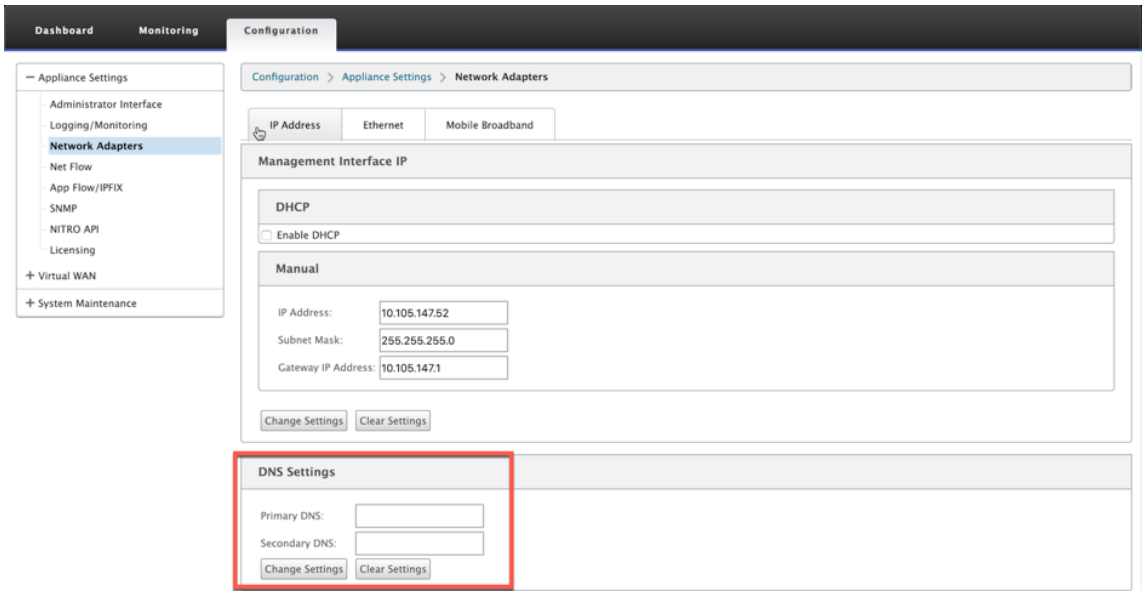
The Office 365 breakout policy allows you to specify which category of Office 365 traffic you can directly break out from the branch. On enabling Office 365 breakout and compiling the configuration, a DNS object, application object, application route, and a firewall policy template is auto-created and applied to branch sites with Internet service.

Prerequisites

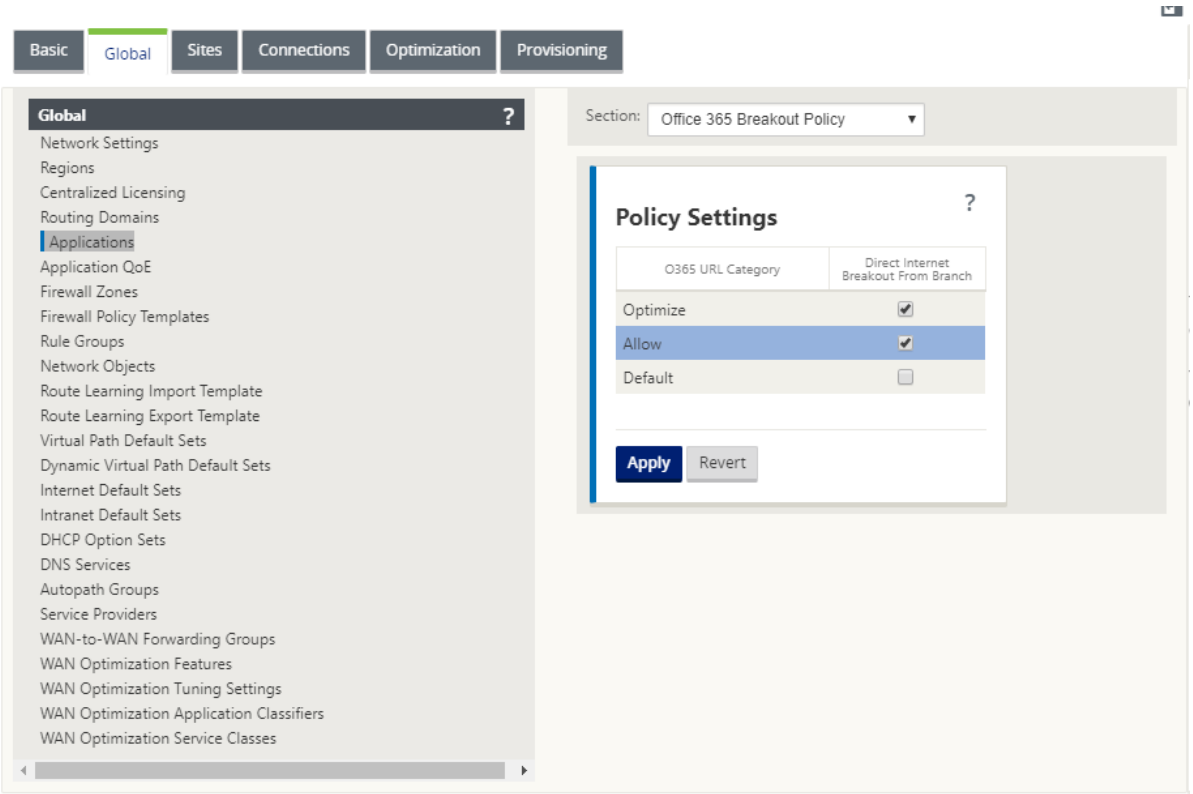
Ensure that you have the following:

1. To perform Office 365 breakout, an internet service has to be configured on the appliance. For more information on configuring internet service, see Internet access.
2. Ensure that the Management interface has internet connectivity.

   You can use the Citrix SD-WAN web interface to configure the management interface settings.
3. Ensure that the management DNS is configured. To configure management interface DNS navigate to **Configuration > Appliance Settings > Network Adapter**. Under the **DNS Settings** section, provide the primary and secondary DNS server detail and click **Change Settings**.

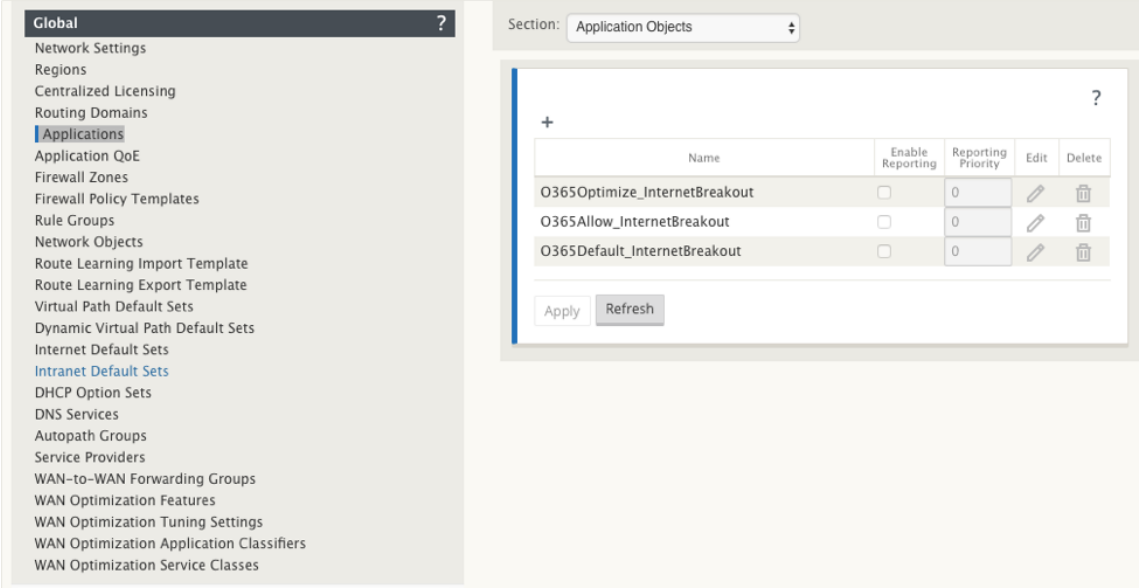


The **Office 365 Breakout Policy** setting is available under global settings, select the required Office 365 category for internet breakout and click **Apply**.

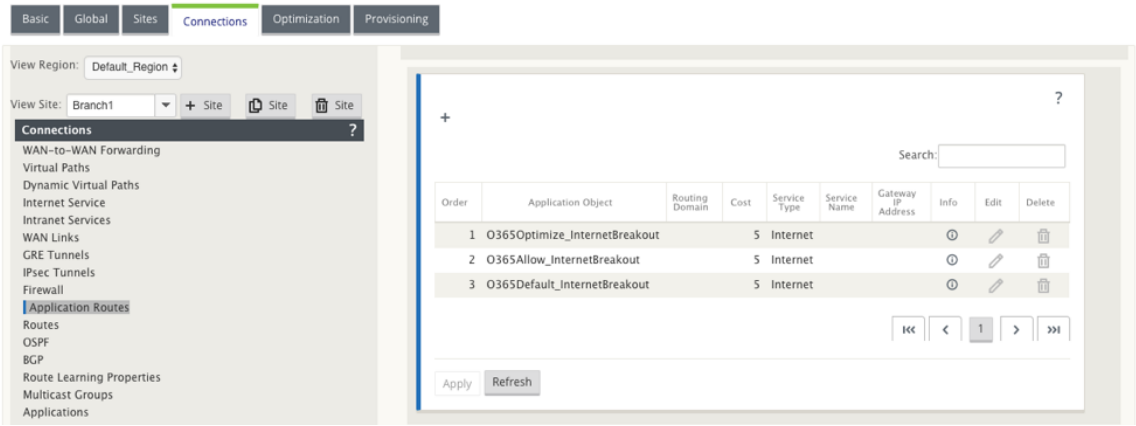


After you configure the Office 365 break out policy settings and compile the configuration. The following settings are auto populated.

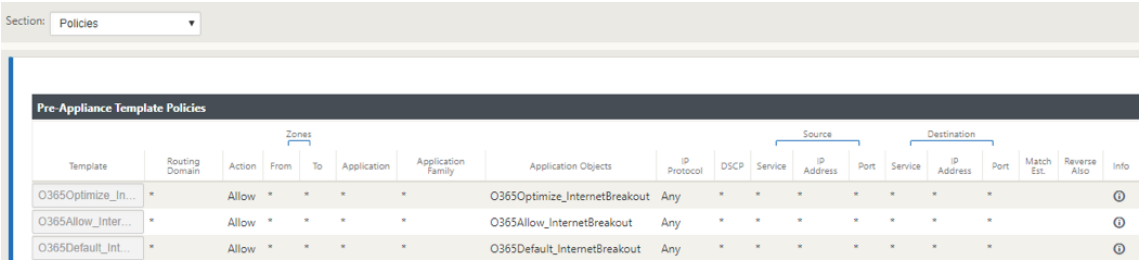
- **DNS object** - The DNS object specifies which type of traffic to be forwarded to the DNS service that the user is configured. The DNS requests are heard on all trusted interfaces, and DNS forwarders are included to direct Office 365 DNS requests to Quad9 service. This forwarder rule takes the highest priority. For more information, see **Domain Name Service** section.
- **Application object** - An application object with the Office 365 category selected by user is created. If you have selected optimize, allow and default categories, the application objects **O365Optimize_InternetBreakout, O365Allow_InternetBreakout** and **O365Default_InternetBreakout** are created.



- **Application route**: An application route is created for each of the Office 365 application objects with Internet Service type.



- **Firewall pre-appliance policy template**: A global pre-appliance policy template is created for each configured Office 365 category. This template is applied to all branch sites that have Internet service. The pre-appliance policy takes priority over local and post appliance policy templates.

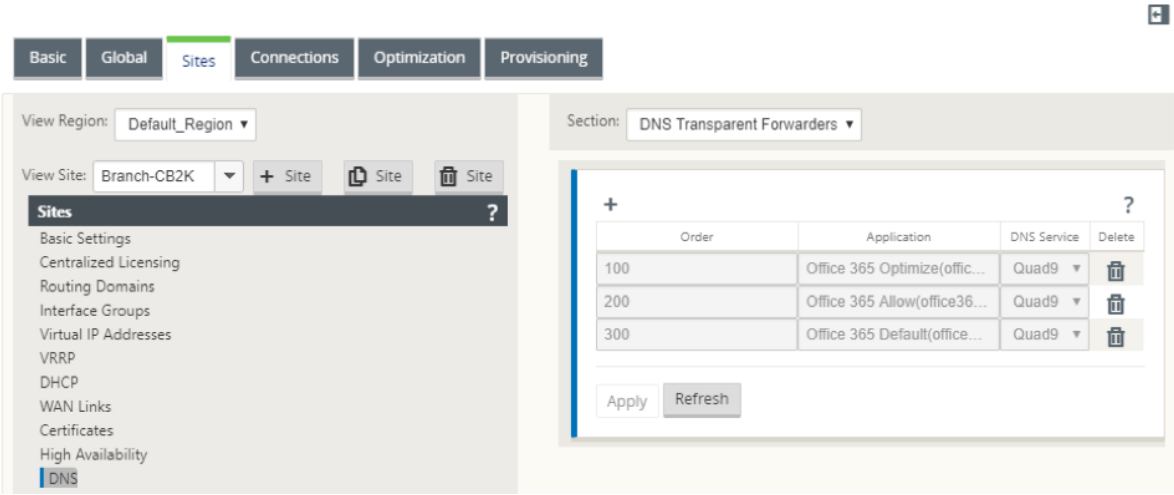


Transparent forwarder for Office 365

The branch breaks out for Office 365 begins with a DNS request. The DNS request going through Office 365 domains have to be steered locally. If Office 365 Internet break out is enabled, the internal DNS routes are determined and the transparent forwarders list is auto populated. Office 365 DNS requests are forwarded to open source DNS service Quad 9 by default. Quad 9 DNS service is secure, scalable, and has multi pop presence. You can change the DNS service if necessary.

Transparent forwarders for Office 365 applications are created at every branch that has Internet service and office 365 breakout enabled.

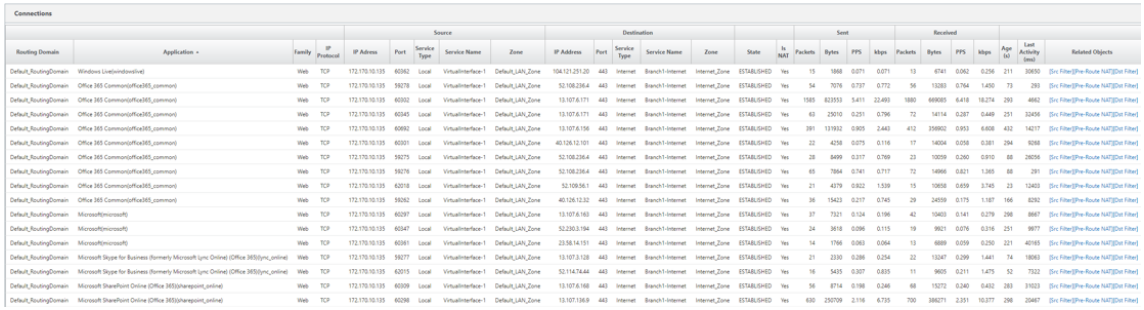
If you are using another DNS proxy or if SD-WAN is configured as the DNS proxy, the forwarder list is auto populated with forwarders for Office 365 applications.



Monitoring

You can monitor the office 365 application statistics in the following SD-WAN statistic reports:

- Firewall Statistics



- Flows

Flows Data

LAN to WAN Flows

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

- DNS Statistics

Dashboard | Monitoring | Configuration

Statistics
Flows
Routing Protocols
Firewall
IKE/IPsec
ICMP
Performance Reports
Qos Reports
Usage Reports
Availability Reports
Appliance Reports
DHCP Server/Relay
VRRP
PPPoE
DNS

Monitoring > DNS

DNS Statistics

Refresh

Proxy Statistics

Search:

Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
DNS_Proxy1	office365_optimize	Quad9	YES	2
DNS_Proxy1	office365_allow	Quad9	YES	8
DNS_Proxy1	office365_default	Quad9	YES	6
DNS_Proxy1	Any	Google	YES	17

Showing 1 to 4 of 4 entries

Transparent Forwarder Statistics

Search:

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

Showing 1 to 3 of 3 entries

- Application Route Statistics

Monitoring > Statistics

Statistics

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

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

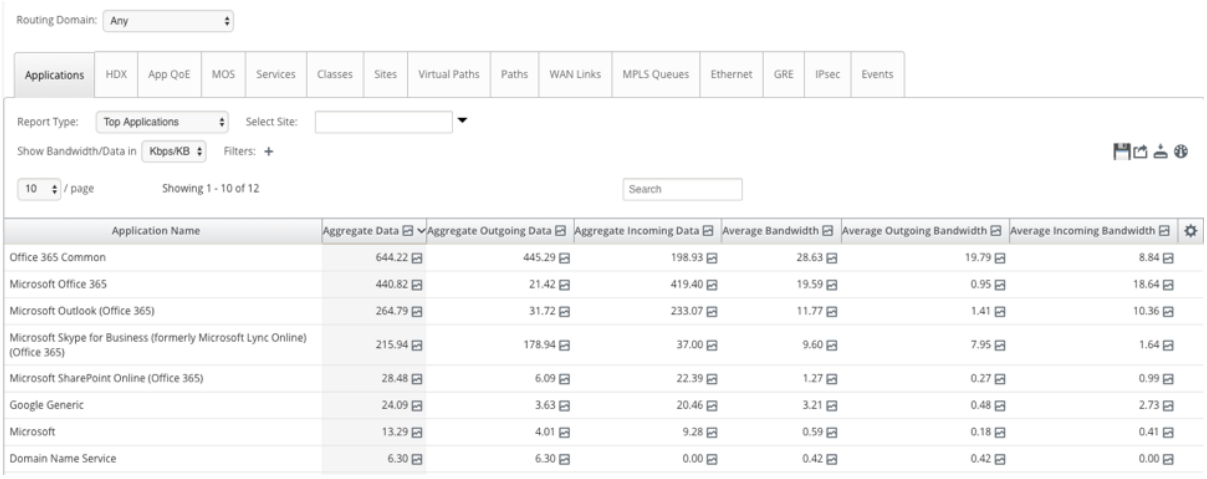
Filter: in Any column Apply

Show 100 entries Showing 1 to 3 of 3 entries First Previous 1 Next Last

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

Showing 1 to 3 of 3 entries First Previous 1 Next Last

You can also view Office 365 application statistics in the SD-WAN Center Application report.

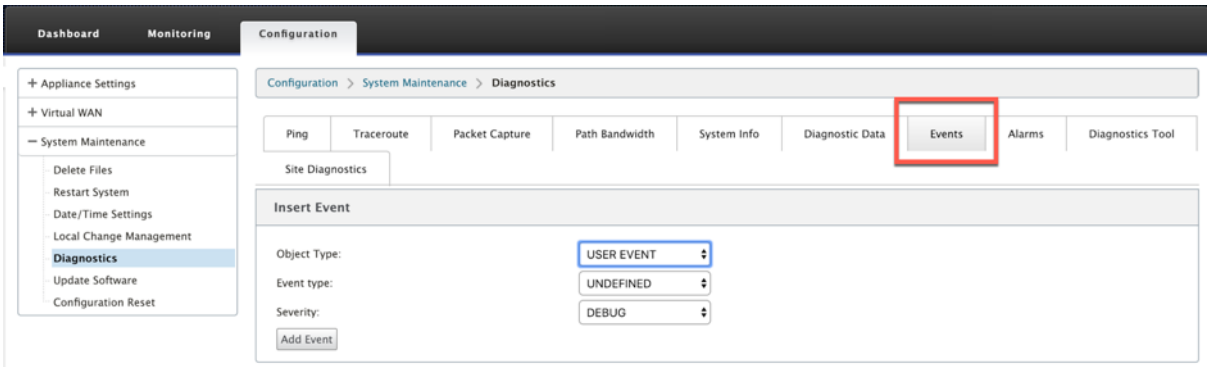


Application Name	Aggregate Data	Aggregate Outgoing Data	Aggregate Incoming Data	Average Bandwidth	Average Outgoing Bandwidth	Average Incoming Bandwidth
Office 365 Common	644.22	445.29	198.93	28.63	19.79	8.84
Microsoft Office 365	440.82	21.42	419.40	19.59	0.95	18.64
Microsoft Outlook (Office 365)	264.79	31.72	233.07	11.77	1.41	10.36
Microsoft Skype for Business (formerly Microsoft Lync Online) (Office 365)	215.94	178.94	37.00	9.60	7.95	1.64
Microsoft SharePoint Online (Office 365)	28.48	6.09	22.39	1.27	0.27	0.99
Google Generic	24.09	3.63	20.46	3.21	0.48	2.73
Microsoft	13.29	4.01	9.28	0.59	0.18	0.41
Domain Name Service	6.30	6.30	0.00	0.42	0.42	0.00

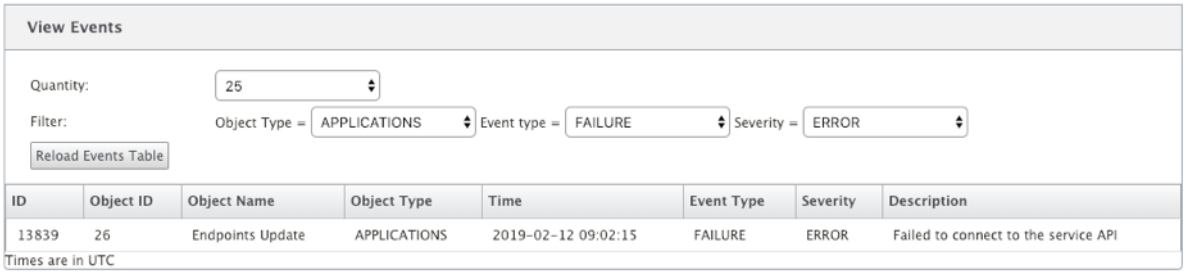
Troubleshooting

You can view the service error in the **Events** section of the SD-WAN appliance.

To check the errors, navigate to **Configuration > System Maintenance > Diagnostics**, click **Events** tab.

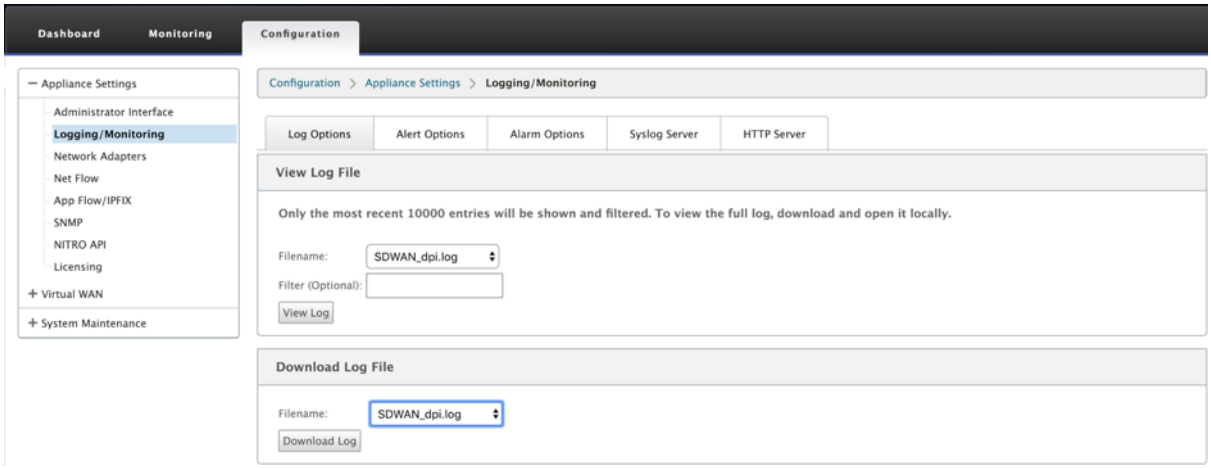


If there is an issue in connecting to the Citrix service (sdwan-app-routing.citrixnetworkapi.net), then the error message reflects under the **View Events** table.



The connectivity errors are also logged to **SDWAN_dpi.log**. To view the log, navigate to **Configuration > Appliance Settings > Logging/ Monitoring > Log Options**. Select the **SDWAN_dpi.log** from the drop-down list and click View **Log**.

You can also download the log file. To download the log file, select the required log file from the drop-down list under the **Download Log file** section and click **Download Log**.



Limitations

- If Office 365 breakout policy is configured, deep packet inspection is not performed on connections destined to the configured category of IP addresses.
- The auto created firewall policy and application routes are uneditable.
- The auto created firewall policy has the lowest priority and is uneditable.
- The route cost for the auto created application route is five. You can override it with a lower cost route.

Office 365 beacon service

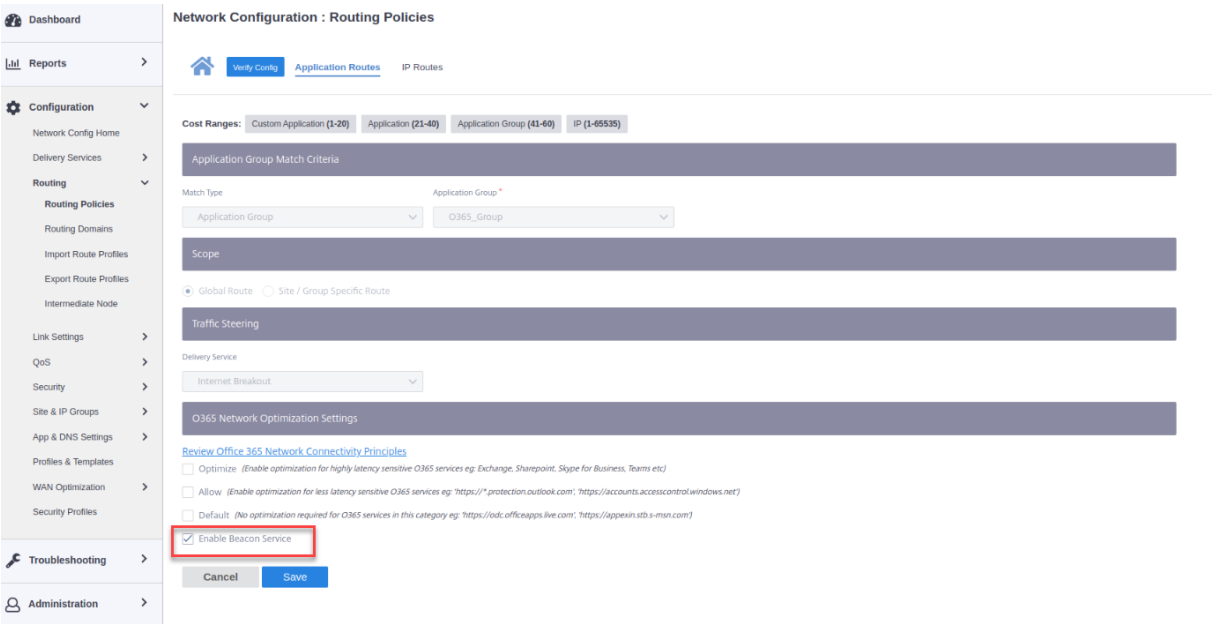
Microsoft provides Office 365 beacon service to measure Office 365 reachability through the WAN links. The beacon service is basically a URL - sdwan.measure.office.com/apc/trans.png, which is probed at regular intervals. Probing is done on each appliance for every internet enabled WAN link. With each probe, an HTTP request is sent to the beacon service and an HTTP response is expected. The HTTP response confirms the availability and reachability of Office 365 service.

Citrix SD-WAN allows you to not only perform beacon probing, but also determines the latency to reach Office 365 endpoints through each WAN link. The latency is the round trip time taken to send a request and get a response from the Office 365 beacon service over a WAN link. This enables network administrators to view the beacon service latency report and manually choose the best internet link for direct Office 365 breakout. Beacon probing is enabled only through SD-WAN Orchestrator. By default, beacon probing is enabled on all Internet enabled WAN links when Office 365 break-out is enabled through Orchestrator.

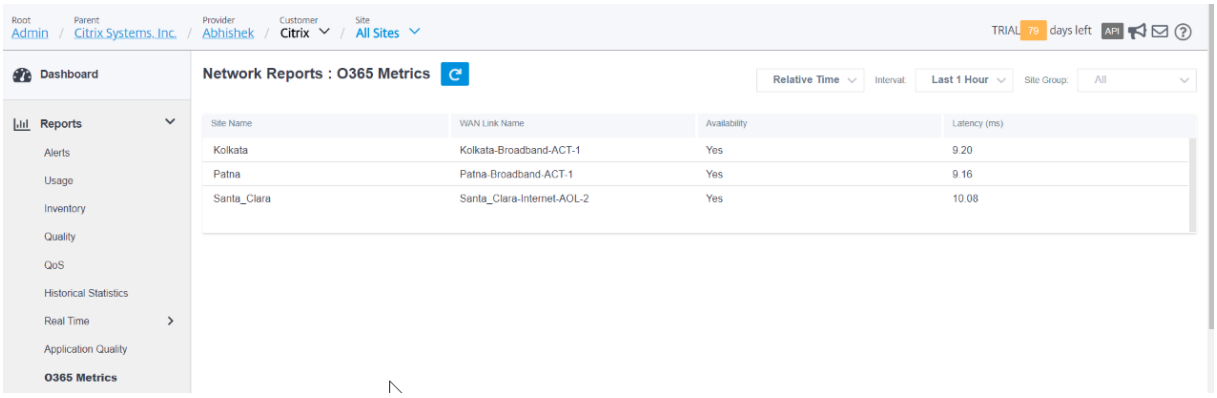
> **Note**
>
> Office 365 beacon probing is not enabled on metered links.

You can choose to disable Office 365 beacon probing and view latency reports on the SD-WAN Orchestrator. For more information, see Office 365 optimization.

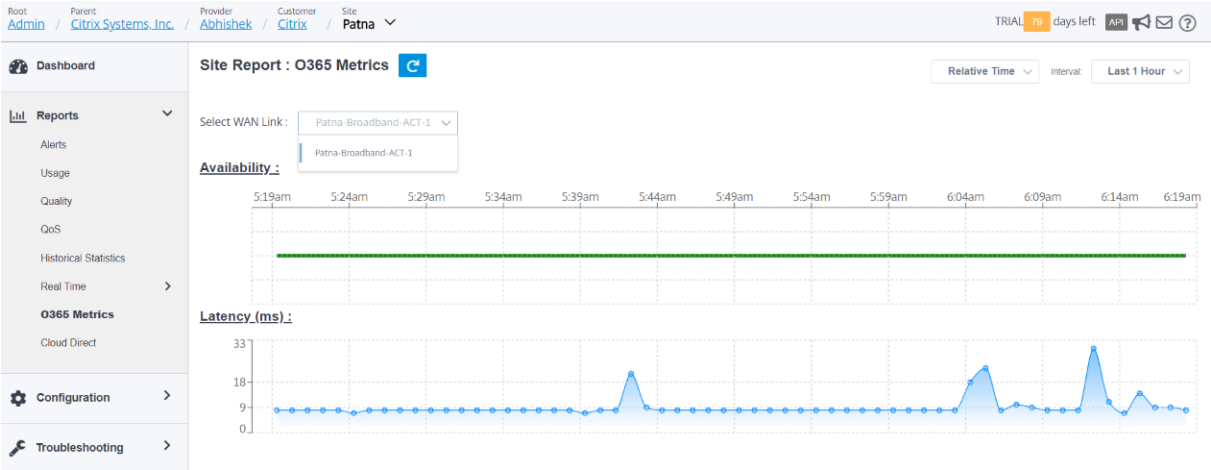
To disable Office 365 beacon service, in SD-WAN Orchestrator, at network level navigate to **Configuration** > **Routing** > **Routing Policies** > **O365 Network Optimization Settings** and uncheck **Enable Beacon Service**.



To view the beacon probing availability and latency reports, in SD-WAN Orchestrator, at network level navigate to **Reports** > **O365 Metrics**.



To view a detailed site level report of beacon service, in SD-WAN Orchestrator, at site level navigate to **Reports** > **O365 Metrics**.



Citrix Cloud and Gateway service optimization

March 12, 2021

With the **Citrix Cloud and Gateway Service optimization** feature enhancement, you can detect and route traffic destined for Citrix Cloud and Gateway Service. You can create policies to either break the traffic out to internet directly or, to send it via a backhaul route over virtual path. In the absence of this feature, when the default route is virtual path, gateway service will hairpin back to the customer's Data Center and then would go out to Internet adding unnecessary latency. In addition to that, you now get visibility into Citrix Gateway service and Citrix Cloud traffic and can create QoS policies to prioritise it over virtual path.

The **Citrix Cloud and Gateway Service breakout** feature is enabled by default in Citrix SD-WAN software version 11.2.1 and above.

From 11.2.1 release, you can now enable the first packet detection, classification, and selective routing (direct Internet breakout or over the virtual path) of the traffic destined for Citrix Cloud and Citrix Gateway Service (control and data).

> **Note**
>
> - You can configure the Citrix Cloud and Gateway Service optimization only through Citrix SD-WAN Orchestrator. For more information, see Gateway service optimization.
> - **Citrix SD-WAN Orchestrator traffic optimization** is introduced from Citrix SD-WAN software version 11.2.3 or higher. The goal is to provide a more granular classification, and thus, separately identify Citrix SD-WAN Orchestrator traffic and other dependent services'traffic

> from Citrix Cloud, and provide an Internet breakout option. As a result, customers can now choose to optimize only the Citrix SD-WAN Orchestrator traffic.

Citrix Cloud and Gateway Service categories

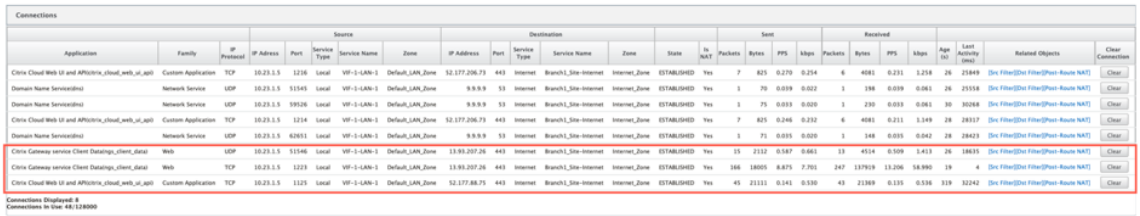
Following are the traffic categories used for classification and optimization purposes:

- **Citrix Cloud**: Enable to detect and route traffic destined for Citrix Cloud Web UI and APIs.
  - Citrix SD-WAN Orchestrator and dependant critical services:
    - **Citrix SD-WAN Orchestrator**: Enables direct internet breakout of heartbeat and other traffic required to establish and maintain connectivity between Citrix SD-WAN appliance, and Citrix SD-WAN Orchestrator.
    - **Citrix Cloud Download Service**: Enables direct internet breakout for download of appliance software, configuration, scripts, and so on onto the Citrix SD-WAN appliance.
- **Citrix Gateway Service**: Enable to detect and route traffic (control and data) destined for Citrix Gateway Service.
  - **Gateway Service Client Data**: Enables direct internet breakout of ICA data tunnels between clients and Citrix Gateway Service. It requires high bandwidth and low latency.
  - **Gateway Service Server Data**: Enables direct internet breakout of ICA data tunnels between Virtual Delivery Agents (VDAs) and Citrix Gateway Service. It requires high bandwidth and low latency and only relevant in VDA resource locations (VDA to Citrix Gateway Service connections).
  - **Gateway Service Control Traffic**: Enables direct internet breakout of the control traffic. No specific QoS considerations.
  - **Gateway Service Web Proxy Traffic**: Enables direct internet breakout of the Web proxy traffic. It requires high bandwidth but latency requirements might vary.

Monitoring

You can monitor the Gateway service statistics in the following SD-WAN statistic reports:

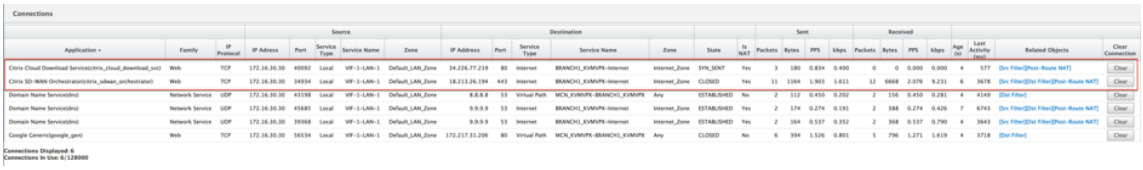
- Firewall Statistics



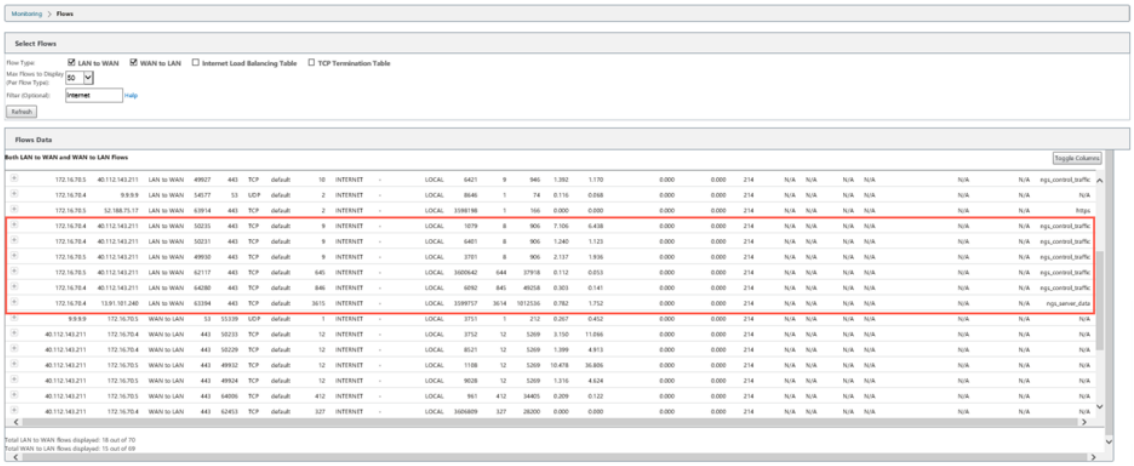
Connections

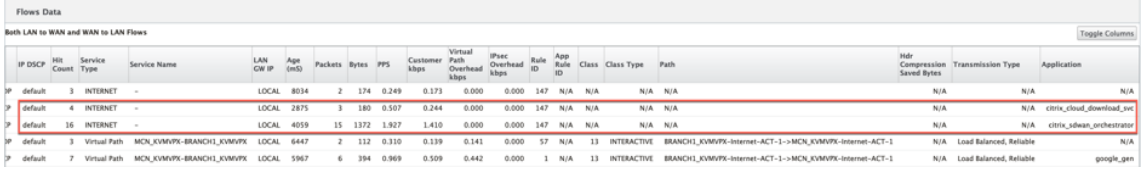
			Source					Destination							Sent				Received							
Application	Family	IP Protocol	IP Adress	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT?	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS	kbps	Age (s)	Last Activity (ms)	Related Objects	Clear Connection
Citrix Cloud Web UI and APIs(citrix_cloud_web_ui_api)	Custom Application	TCP	10.23.1.5	1216	Local	VIF-1-LAN-1	Default_LAN_Zone	52.177.206.73	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	7	825	0.270	0.254	6	4081	0.231	1.258	26	25849	[Src Filter][Dst Filter][Post-Route NAT]	Clear
Domain Name Service(dns)	Network Service	UDP	10.23.1.5	51545	Local	VIF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	1	70	0.039	0.022	1	198	0.039	0.061	26	25558	[Src Filter][Dst Filter][Post-Route NAT]	Clear
Domain Name Service(dns)	Network Service	UDP	10.23.1.5	59526	Local	VIF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	1	75	0.033	0.020	1	230	0.033	0.061	30	30268	[Src Filter][Dst Filter][Post-Route NAT]	Clear
Citrix Cloud Web UI and APIs(citrix_cloud_web_ui_api)	Custom Application	TCP	10.23.1.5	1214	Local	VIF-1-LAN-1	Default_LAN_Zone	52.177.206.73	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	7	825	0.246	0.232	6	4081	0.211	1.149	28	28317	[Src Filter][Dst Filter][Post-Route NAT]	Clear
Domain Name Service(dns)	Network Service	UDP	10.23.1.5	62651	Local	VIF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	1	71	0.035	0.020	1	148	0.035	0.042	28	28423	[Src Filter][Dst Filter][Post-Route NAT]	Clear
Citrix Gateway service Client Data(ngs_client_data)	Web	UDP	10.23.1.5	51546	Local	VIF-1-LAN-1	Default_LAN_Zone	13.93.207.26	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	15	2112	0.587	0.661	13	4514	0.509	1.413	26	18635	[Src Filter][Dst Filter][Post-Route NAT]	Clear
Citrix Gateway service Client Data(ngs_client_data)	Web	TCP	10.23.1.5	1223	Local	VIF-1-LAN-1	Default_LAN_Zone	13.93.207.26	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	166	18005	8.875	7.701	247	137919	13.206	58.990	19	4	[Src Filter][Dst Filter][Post-Route NAT]	Clear
Citrix Cloud Web UI and APIs(citrix_cloud_web_ui_api)	Custom Application	TCP	10.23.1.5	1125	Local	VIF-1-LAN-1	Default_LAN_Zone	52.177.88.75	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	45	21111	0.141	0.530	43	21369	0.135	0.536	319	32242	[Src Filter][Dst Filter][Post-Route NAT]	Clear

Connections Displayed: 8
Connections In Use: 48/128000



- Flows





- DNS Statistics

Monitoring > DNS

DNS Statistics

Refresh

Proxy Statistics

Search:

Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
Default	office365_optimize	Quad9	YES	0
Default	citrix_cloud_web_ui_api	Quad9	YES	4
Default	ngs_client_data	Quad9	YES	14
Default	ngs_server_data	Quad9	YES	0
Default	ngs_control_traffic	Quad9	YES	2286
Default	ngs_web_proxy	Quad9	YES	0
Default	Any	azureDNS	YES	51490

Showing 1 to 7 of 7 entries

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
citrix_cloud_web_ui_api	Quad9	YES	0
ngs_client_data	Quad9	YES	0
ngs_control_traffic	Quad9	YES	0
ngs_server_data	Quad9	YES	0
ngs_web_proxy	Quad9	YES	0
office365_optimize	Quad9	YES	0

Showing 1 to 6 of 6 entries

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
citrix_cloud_download_svc	Quad9	YES	1
citrix_sdwan_orchestrator	Quad9	YES	1

Showing 1 to 2 of 2 entries

- Application Route Statistics

Monitoring > Statistics

Statistics

Show: Application Routes ☐ Enable Auto Refresh 5 seconds Refresh ☑ Clear Counters on Refresh

Application Route Statistics

Maximum allowed routes: 64000

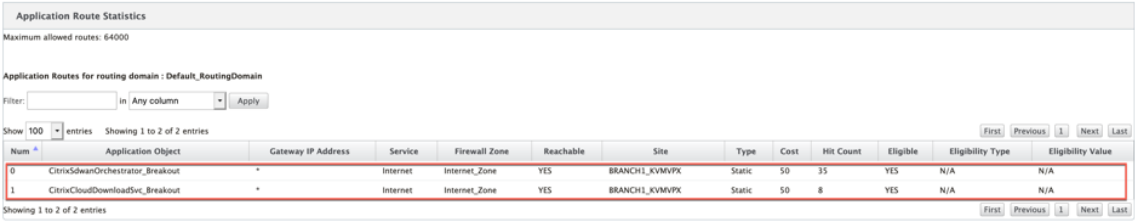
Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 6 of 6 entries First Previous 1 Next Last

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

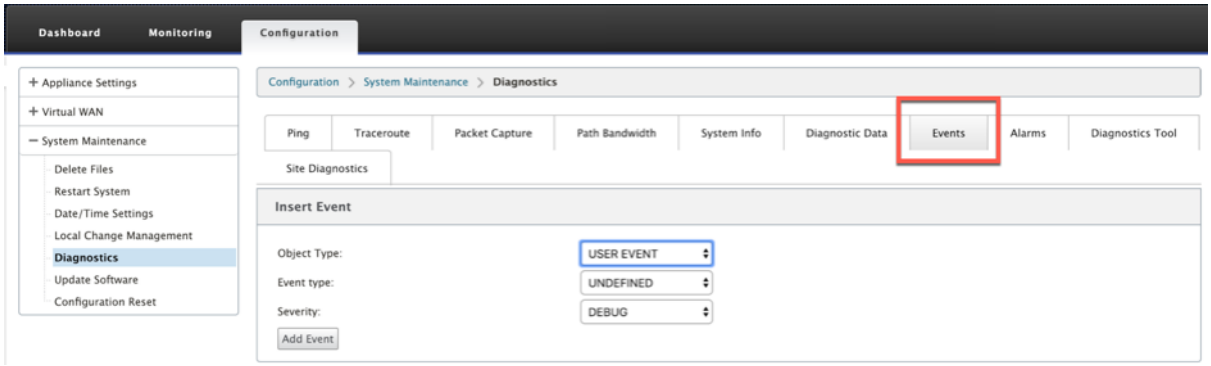
Showing 1 to 6 of 6 entries First Previous 1 Next Last



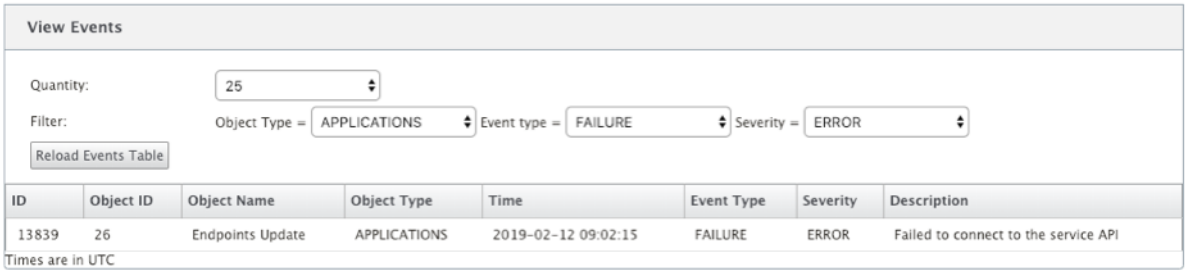
Troubleshooting

You can view the service error in the **Events** section of the SD-WAN appliance.

To check the errors, navigate to **Configuration > System Maintenance > Diagnostics**, click **Events** tab.

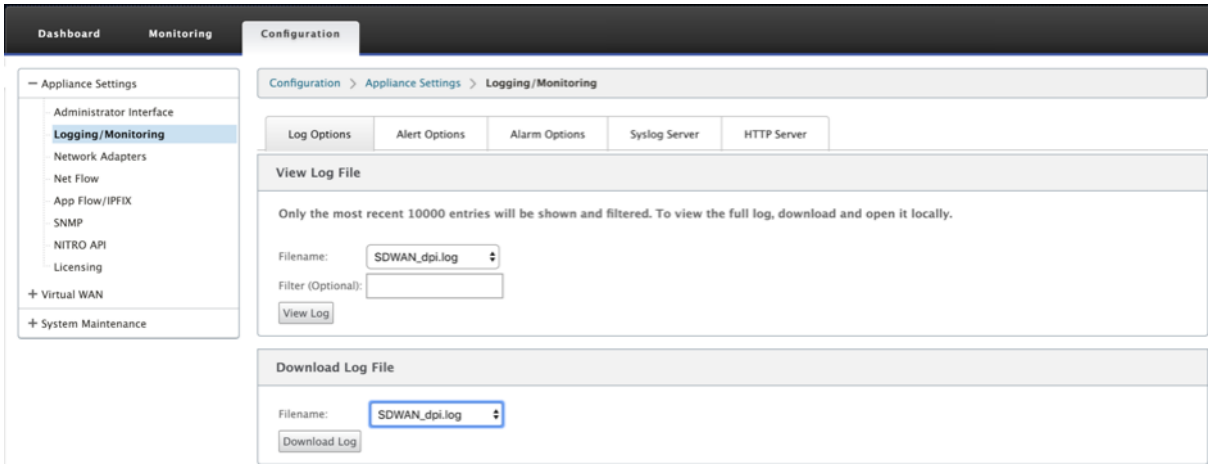


If there is an issue in connecting to the Citrix service (sdwan-app-routing.citrixnetworkapi.net), then the error message reflects under the **View Events** table.



The connectivity errors are also logged to **SDWAN_dpi.log**. To view the log, navigate to **Configuration > Appliance Settings > Logging/ Monitoring > Log Options**. Select the SDWAN_dpi.log from the drop-down list and click **View Log**.

You can also download the log file. To download the log file, select the required log file from the drop-down list under the **Download Log file** section and click **Download Log**.



Citrix SD-WAN Orchestrator for On-premises configuration on Citrix SD-WAN appliance

August 13, 2021

Citrix SD-WAN Orchestrator for On-premises is the on-premises software version of the Citrix SD-WAN Orchestrator service. Citrix SD-WAN Orchestrator for On-premises provides a single-pane of glass management platform for Citrix partners to manage multiple customers centrally, with suitable role based access controls.

You can establish a connection between your Citrix SD-WAN appliance and the Citrix SD-WAN Orchestrator for On-premises by enabling Orchestrator connectivity and specifying the Citrix SD-WAN Orchestrator for On-premises identity.

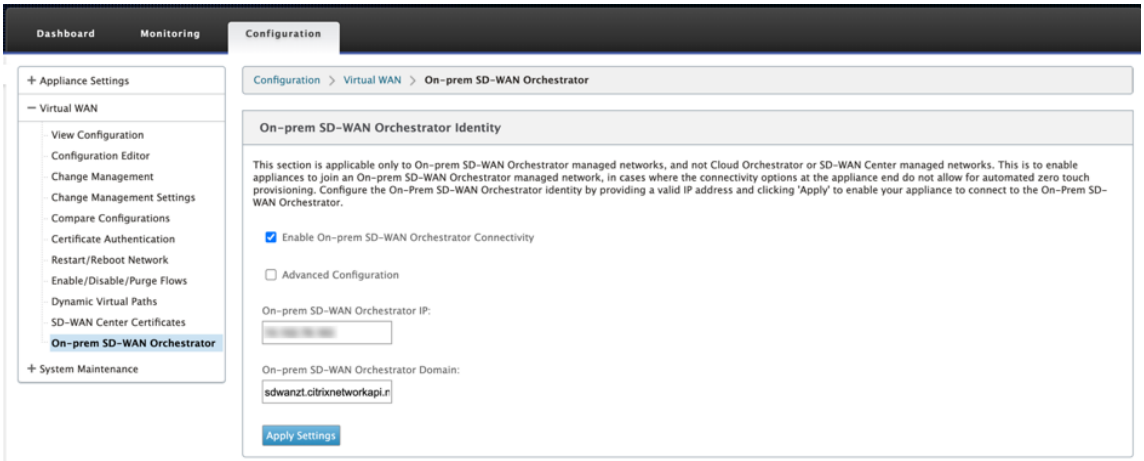
> **Note**
>
> - Cloud Orchestrator Zero-Touch Deployment will not work if the **On-prem SD-WAN Orchestrator configuration on SD-WAN appliance** feature is configured on the SD-WAN appliances.
> - Citrix SD-WAN Orchestrator for On-premises on the SD-WAN appliance is lost, if the Citrix SD-WAN Orchestrator for On-premises configuration on the SD-WAN appliance configured in the Citrix SD-WAN release 11.3.0 is downgraded to release 10.2.7. Downgrading from release 11.3.0 to release 10.2.7 is not supported. The workaround is to reconfigure the Citrix SD-WAN Orchestrator for On-premises identity after the downgrade.
> - After downgrading the SD-WAN appliance from 11.3.0 to 11.1.1/11.2.0/10.2.7 software version, you must apply identity settings again on the Citrix SD-WAN appliance UI. If any issues related to the Citrix SD-WAN Orchestrator for On-premises configuration or SD-WAN

> appliance connectivity, disable the Citrix SD-WAN Orchestrator for On-premises connectivity and then enable the Citrix SD-WAN Orchestrator for On-premises connectivity again.

To enable Citrix SD-WAN Orchestrator for On-premises connectivity with Citrix SD-WAN 11.2.1 release onwards:

1. In the appliance UI, navigate to **Configuration** > **Virtual WAN** > **On-prem SD-WAN Orchestrator**.
2. Select **Enable On-prem SD-WAN Orchestrator Connectivity** check box.

   > **Note**
   >
   > From Citrix SD-WAN 11.2.1 release onwards, the **SD-WAN Appliance and On-prem SD-WAN Orchestrator Certificates, On-prem SD-WAN Orchestrator Domain, Authentication Type,** and **Advanced Configuration** options are introduced.



3. Enter either the Citrix SD-WAN Orchestrator for On-premises IP address or Domain or both (IP address and domain) for configuration.

   If the customer configures only Domain, then they must ensure to add DNS record in their Local DNS server and must configure DNS Server IP Address on SD-WAN Appliances. To configure, navigate to **Configuration > Network Adapters > IP Address**.

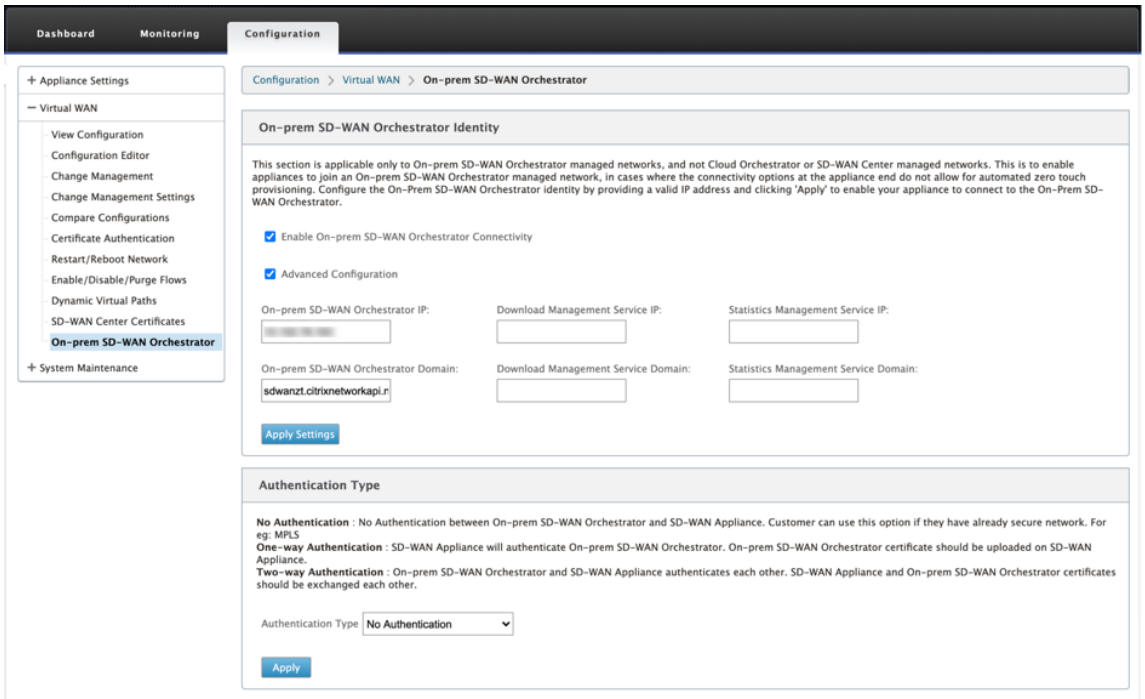
   For example, if the Citrix SD-WAN Orchestrator for On-premises domain is configured as **citrix.com**. then you must create a DNS record in the DNS Server for the below FQDN and Citrix SD-WAN Orchestrator for On-premises IP Address:

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

   In advanced configuration:

For example: If the Citrix SD-WAN Orchestrator for On-premises domain is configured as **citrix.com**, the Download Management Service Domain is configured as **download.citrix.com**, and the Statistics Management Service Domain is configured as statistics.citrix.com, then you must create a DNS record in the DNS Server for the below FQDN and corresponding IP Address:

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



Citrix SD-WAN Orchestrator for On-premises might support running services like download, statistics on an independent server instance, to enable better scalability for large networks. You can select the **Advanced Configuration** and configure the **Download Management Service and Statistic Management** service.

Select the **Advanced Configuration** check box and provide the following details:

- **Download Management Service IP/Domain**: Provide the IP address /domain that helps offload SD-WAN software and configuration download aspects, to an independent server instance, to enable better scalability for large networks.
- **Statistic Management Service IP/Domain**: Provide the IP address/domain that helps offload collection and management of SD-WAN statistics from devices, to an independent server instance, to enable better scalability for large networks.

4. Select the **Authentication Type**. The following are the authentications types that are supported between the SD-WAN appliance and the Citrix SD-WAN Orchestrator for On-premises connectivity:

- **No Authentication** –No authentication between the Citrix SD-WAN Orchestrator for On-premises and the SD-WAN appliance, and there is no need to use the **SD-WAN Appliance** or **On-prem SD-WAN Orchestrator Certificate**. But you can use this option if you have a secure network such as MPLS.
- **One-way Authentication** –On selecting the **One-way Authentication** type, you must upload the Citrix SD-WAN Orchestrator for On-premises certificate. Download the certificate from the Citrix SD-WAN Orchestrator for On-premises and click **Upload**. SD-WAN appliance trusts the Citrix SD-WAN Orchestrator for On-premises using the uploaded certificates.
- **Two-way Authentication** –Citrix SD-WAN Orchestrator for On-premises and Appliance certificates have to be exchanged with each other. For **Two-way Authentication**, you must regenerate, download, and upload the SD-WAN appliance certificate on the Citrix SD-WAN Orchestrator for On-premises. SD-WAN appliance and Citrix SD-WAN Orchestrator for On-premises trusts each other using the exchanged certificates.

> **Note**
>
> It is recommended to use only One-way Authentication or Two-way Authentication. In the case of No Authentication, ensure that the DNS is secure from DNS attacks.

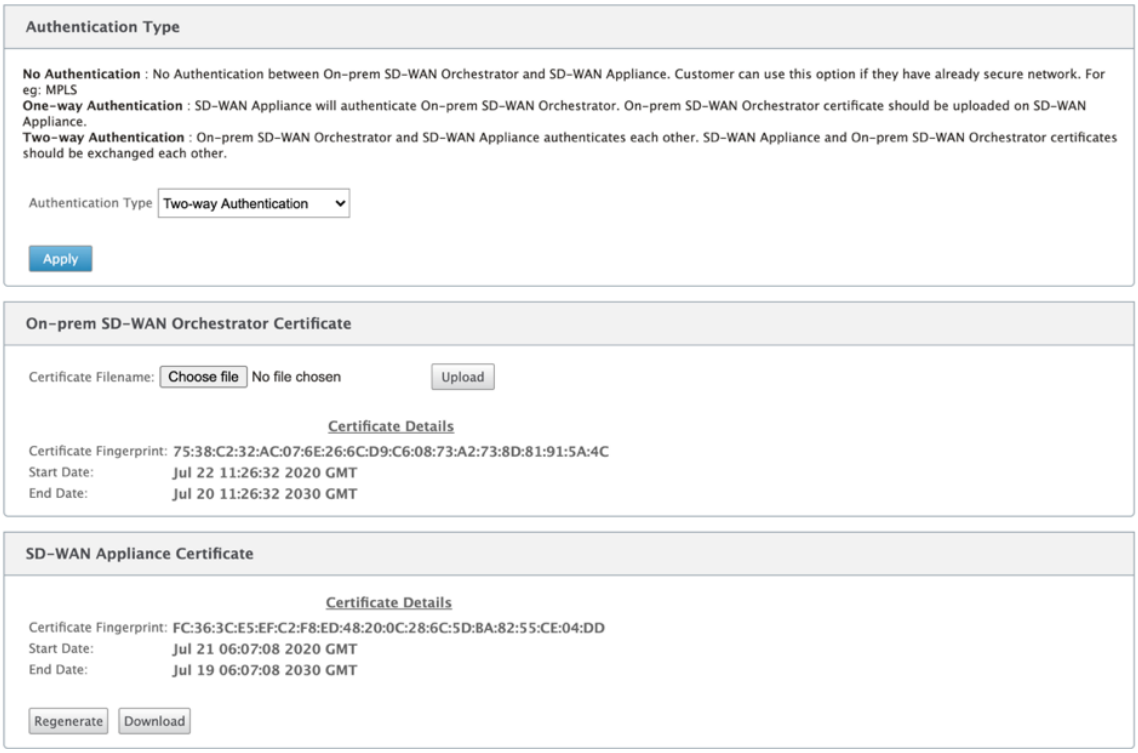
If the Citrix SD-WAN Orchestrator for On-premises **Authentication Type** is disabled, then Appliance can connect to the Citrix SD-WAN Orchestrator for On-premises either via **No Authentication** or **One-way Authentication** or **Two-way Authentication** mode.

If the Citrix SD-WAN Orchestrator for On-premises **Authentication Type** is enabled, then Appliance can only connect to the Citrix SD-WAN Orchestrator for On-premises via **Two-way Authentication**.

While disabling **Authentication Type** in Citrix SD-WAN Orchestrator for On-premises from enable state, existing appliances in One-way Authentication mode goes to disconnected state. Customers have to change the appliance Authentication Type to Two-way Authentication and upload the SD-WAN Appliance certificate to the Citrix SD-WAN Orchestrator for On-premises to get it connected.

> **Note**
>
> - Generated certificates are X509 self-signed certificates.
> - Customer must regenerate the certificates if the certificate is expired or compromised.
> - Validity of the certificate is 10 years.
> - You can view the certificate details such as, fingerprint, start date, and end date
> - Customer must ensure that the certificates are regenerated and exchanged between Citrix SD-WAN Orchestrator for On-premises and SD-WAN appliance to avoid loss of

> appliance connectivity with Citrix SD-WAN Orchestrator for On-premises.



5. Click **Apply Settings**.

To disable the Citrix SD-WAN Orchestrator for On-premises connectivity clear **Enable On-prem SD-WAN Orchestrator Connectivity** option and click **Apply Settings**. To convert Citrix SD-WAN Orchestrator for On-premises managed network to either Cloud Orchestrator or MCN Managed network, you need to disable Citrix SD-WAN Orchestrator for On-premises Connectivity and must perform the configuration reset. To reset configuration, navigate to **Configuration > System Maintenance > Configuration Reset**.

Deploy Citrix SD-WAN appliances running on software versions 10.2.7, 11.1.1, or 11.2.0 with Citrix SD-WAN Orchestrator for On-premises

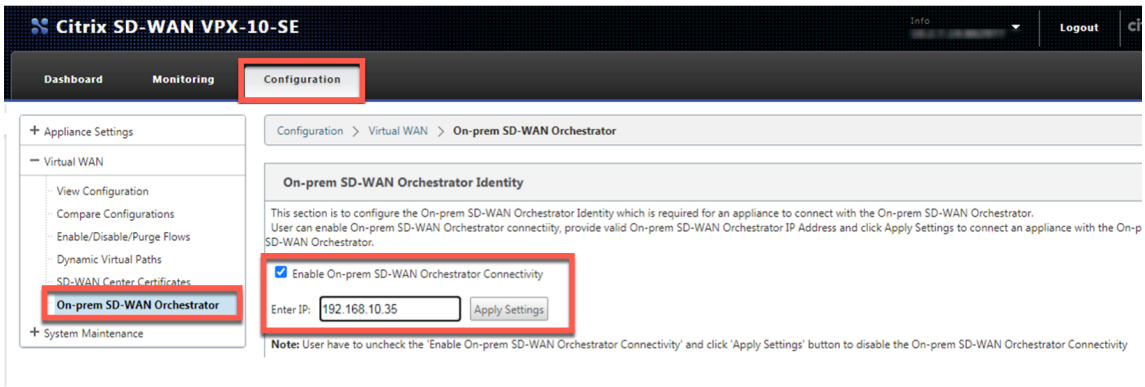
> **NOTE**
>
> To deploy Citrix SD-WAN appliances with software versions 10.2.7, 11.1.1, or 11.2.0, you need Citrix SD-WAN Orchestrator for On-premises version 11.1 or later.

1. For each Citrix SD-WAN appliance with software version 10.2.7, 11.1.1 or 11.2.0, log in to the appliance web interface and perform the following:

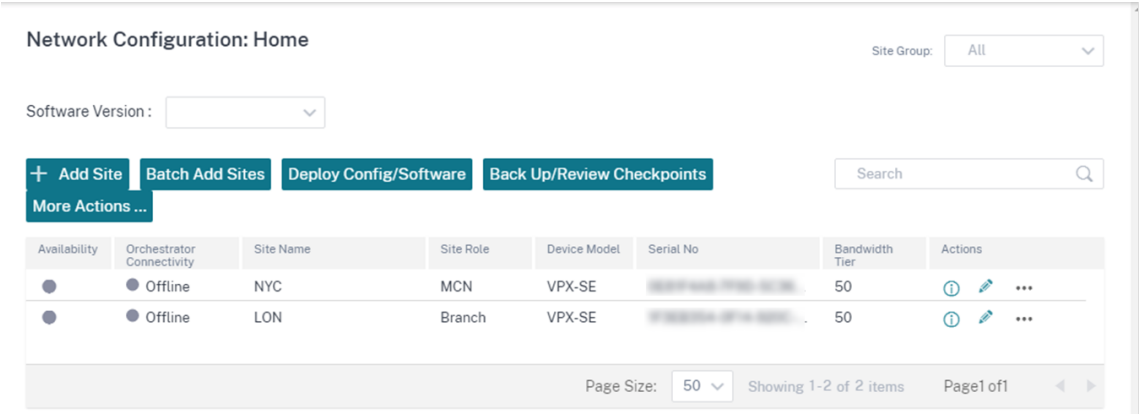
   a) Navigate to **Configuration > Virtual WAN > On-prem SD-WAN Orchestrator** and select the **Enable On-prem SD-WAN Orchestrator Connectivity** check box.

b) Enter the IP address of Citrix SD-WAN Orchestrator for On-premises.

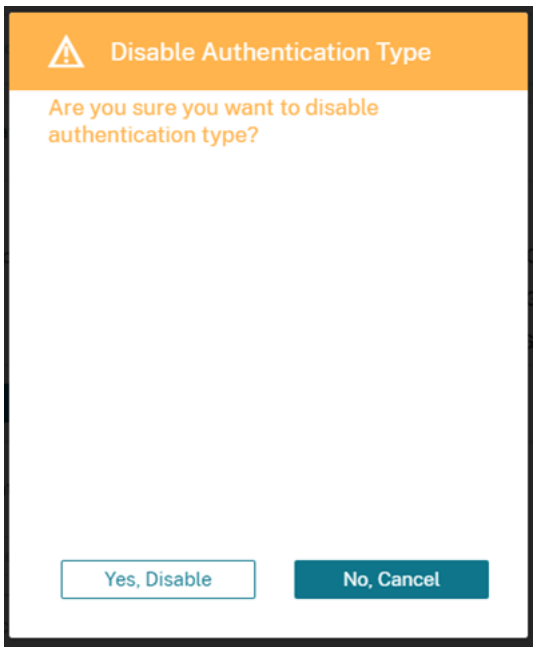
c) Click **Apply Settings**.

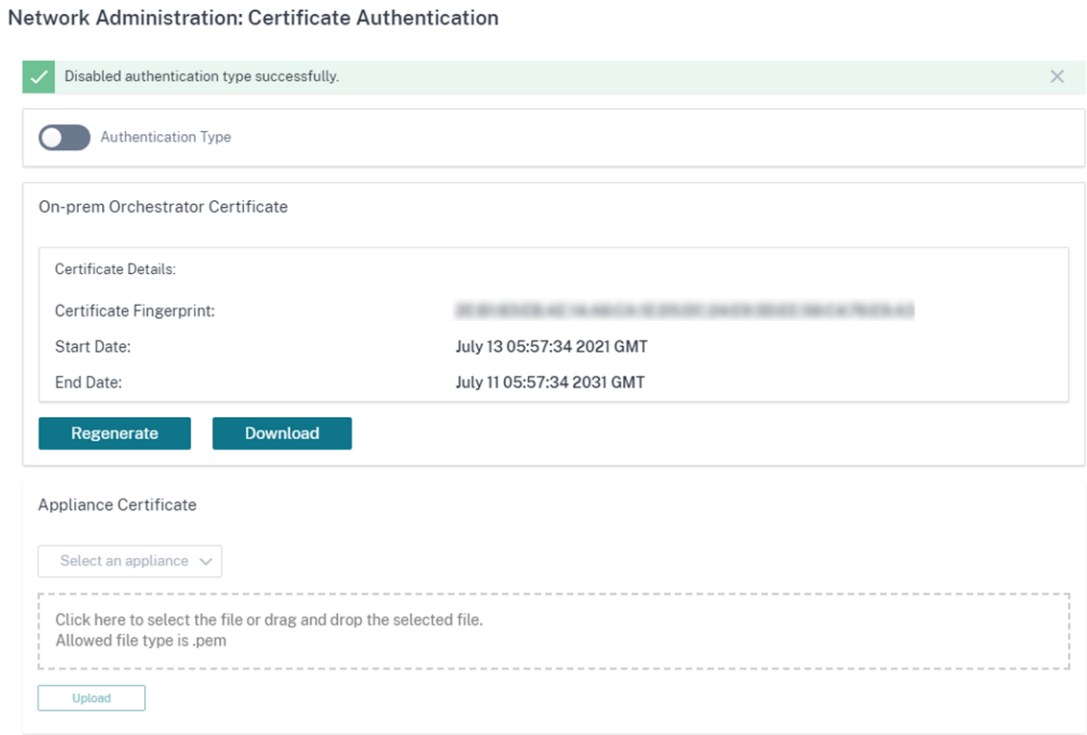


2. Log in to Citrix SD-WAN Orchestrator for On-premises UI. Create a site and build the configuration. Enter the serial number of each Citrix SD-WAN appliance in its respective site configuration. Save the configuration.

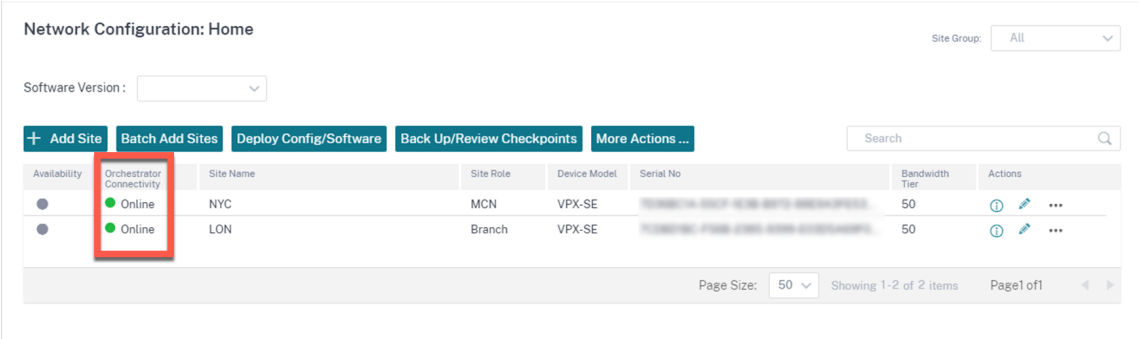


3. Navigate to **Administration > Certificate Authentication** and turn the **Authentication Type** toggle to **OFF**. Click **Yes, Disable** to approve the **Disabled Authentication Type** pop-up.

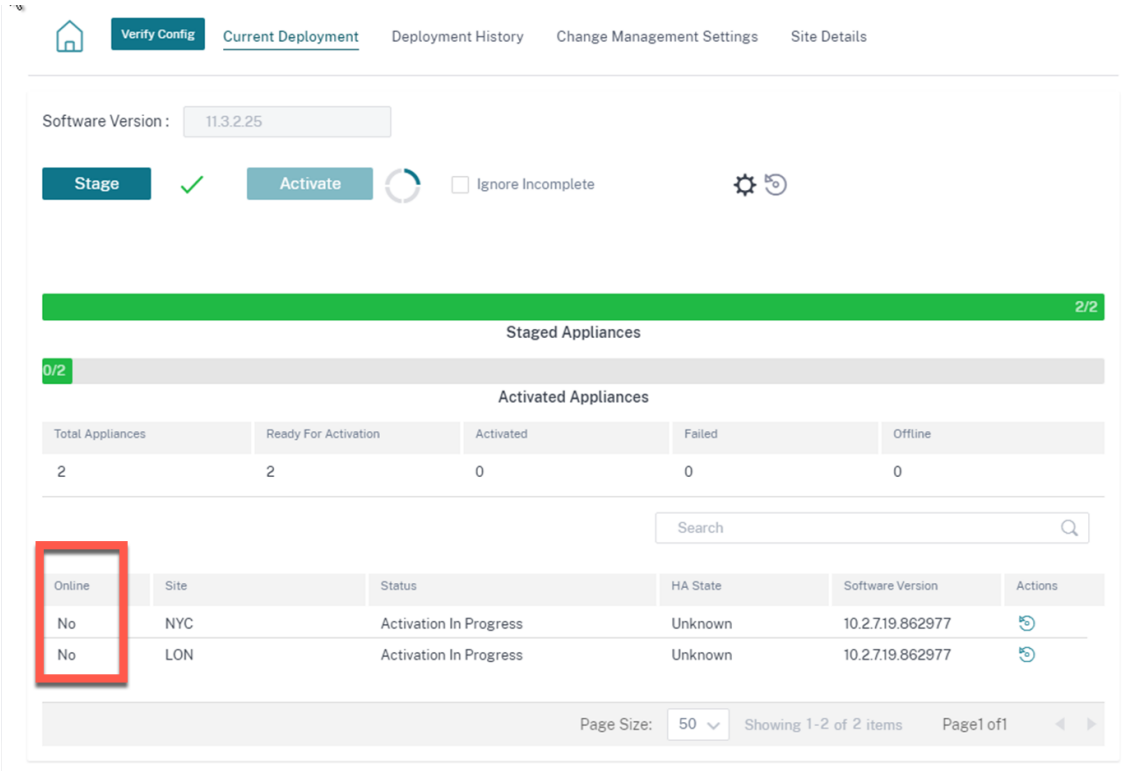




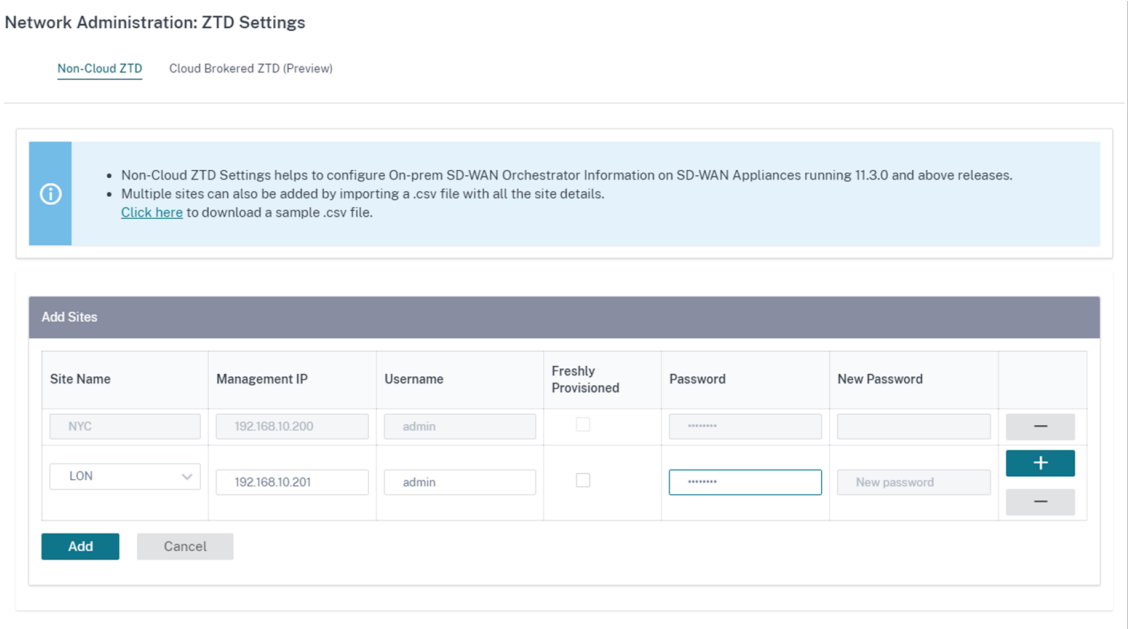
4. In the **Configuration > Network Config Home** page, SD-WAN appliances show as **Online** under the **Cloud Connectivity** column. This is due to Certificate Authentication disabled on Citrix SD-WAN Orchestrator for On-premises and SD-WAN appliances enabled for Citrix SD-WAN Orchestrator for On-premises connectivity with the appropriate IP address. Allow a couple minutes for the devices to be reported as Online.



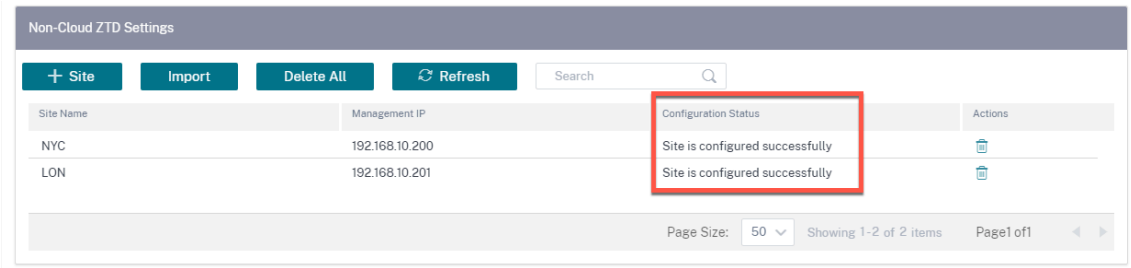
5. Select a published software version (11.3.0 or higher) and click **Deploy Config/Software**. For more details on selecting the published software version, see Software. **Stage** and **Activate** the sites. After activation, the appliances show **No** in the **Online** column.



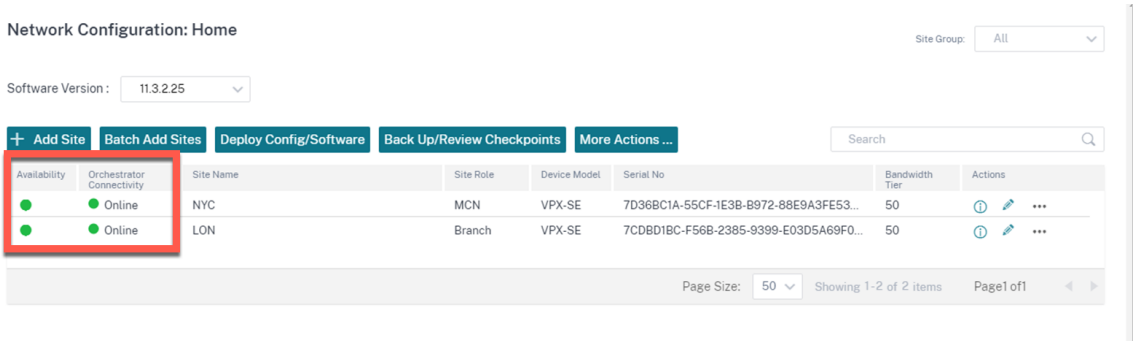
6. Navigate to **Administration > ZTD Settings > Non-Cloud ZTD**. Click **+Site** and add a site. Enter the management IP and login credentials for each appliance. Click **+** to add more sites. Click **Add**.



7. Click **Refresh** to monitor the configuration status. When the site is successfully configured, the **Configuration Status** column displays **Site is configured successfully**.



8. Navigate to the **Configuration > Network Config Home** page. Successfully configured sites show as **Online** under the **Orchestrator Connectivity** column.



9. Follow the same process to add any additional sites. Performing the preceding steps does not impact any existing site deployments.

PPPoE Sessions

March 12, 2021

Point-to-Point Protocol over Ethernet (PPPoE) connects multiple computer users on an Ethernet local area network to a remote site through common customer premises appliances, for example; Citrix SD-WAN. PPPoE allows users to share a common Digital Subscriber Line (DSL), cable modem, or wireless connection to the Internet. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol, which supports multiple users in a local area network. The PPP protocol information is encapsulated within an Ethernet frame.

Citrix SD-WAN appliances use PPPoE to provide support Internet service provider (ISP) to have ongoing and continuous DSL and cable modem connections unlike dialup connections. PPPoE provides each user-remote site session to learn each other's network addresses through an initial exchange called "discovery". After a session is established between an individual user and the remote site, for example, an ISP provider, the session can be monitored. Corporations use shared Internet access over DSL lines using Ethernet and PPPoE.

Citrix SD-WAN act as a PPPoE client. It authenticates with PPPoE server and obtains dynamic IP address, or uses static IP address to establish PPPoE connections.

The following is required to establish successful PPPoE sessions:

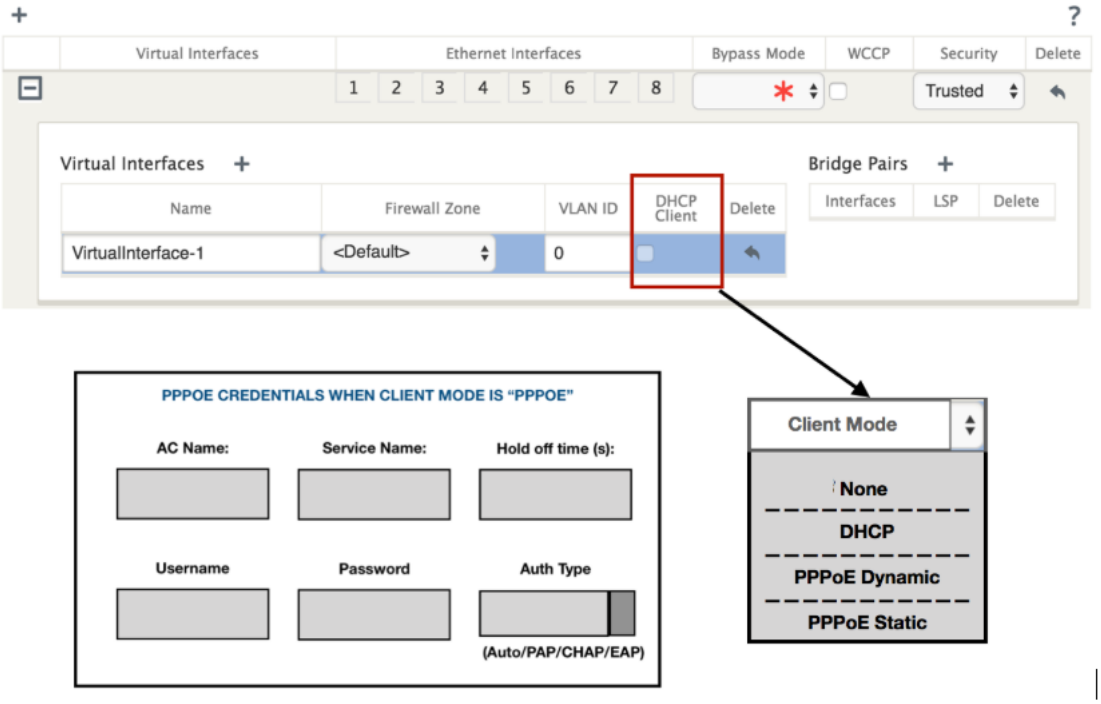
- Configure virtual network interface (VNI).
- Unique credentials for creating PPPoE session.
- Configure WAN link. Each VNI can have only one WAN link configured.
- Configure Virtual IP address. Each session obtains a unique IP address, dynamic, or static based on the provided configuration.
- Deploy appliance in bridge mode to use PPPoE with static IP address and configure the interface as "trusted."
- Static IP is preferred to have a configuration to force the server proposed IP; if different from the configured static IP, otherwise an error can occur.
- Deploy appliance as an Edge device to use PPPoE with dynamic IP and configure the interface as "untrusted."
- Authentication protocols supported are, PAP, CHAP, EAP-MD5, EAP-SRP.
- Maximum number of multiple sessions depends on the number of VNIs configured.
- Create multiple VNIs to support Multiple PPPoE sessions per interface group.

> **Note**:
>
> Multiple VNIs are allowed to create with same 802.1Q VLAN tag.

Limitations for PPPoE configuration:

- 802.1q VLAN tagging is not supported.
- EAP-TLS authentication is not supported.
- Address/Control compression.
- Deflate Compression.
- Protocol field compression negotiation.
- Compression Control Protocol.
- BSD Compress Compression.
- IPv6 and IPX protocols.
- PPP Multi Link.
- Van Jacobson style TCP/IP header compression.
- Connection-ID compression option in Van Jacobson style TCP/IP header compression.
- PPPoE is not supported on LTE interfaces

To facilitate PPPoE configuration, **DHCP Client** option is replaced with a new option called the **Client Mode** in the SD-WAN web management interface under **Sites** configuration.



The following table describes the Client Mode PPPoE configuration options available on an MCN and branch SD-WAN appliance, respectively.

MCN

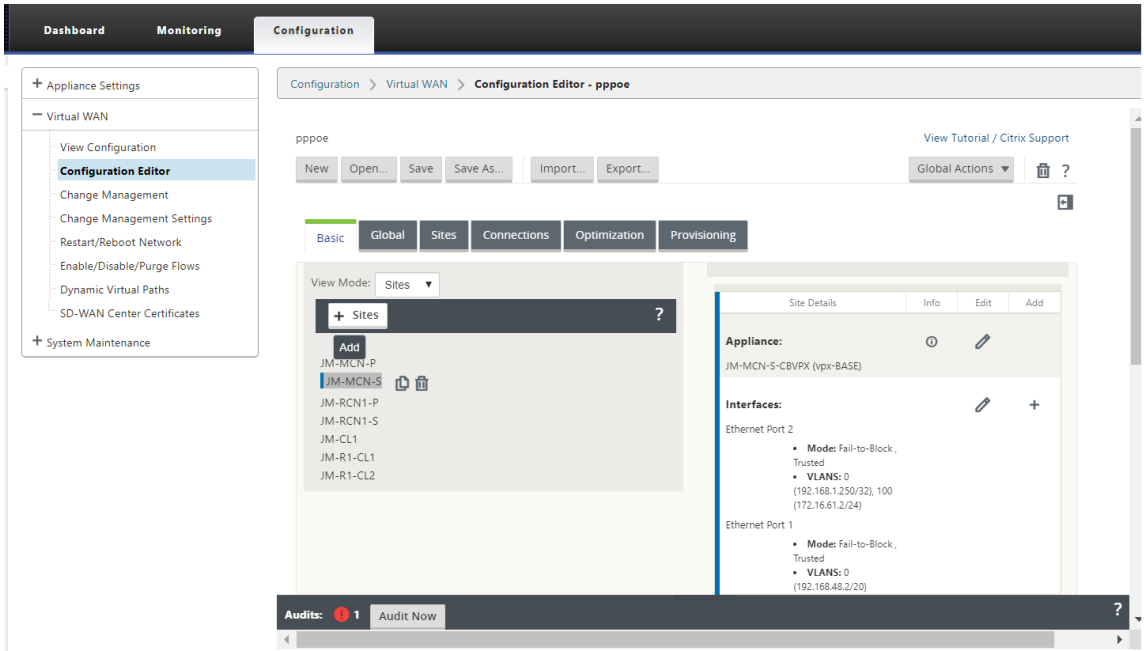
- None
- PPPoE Static

Branch

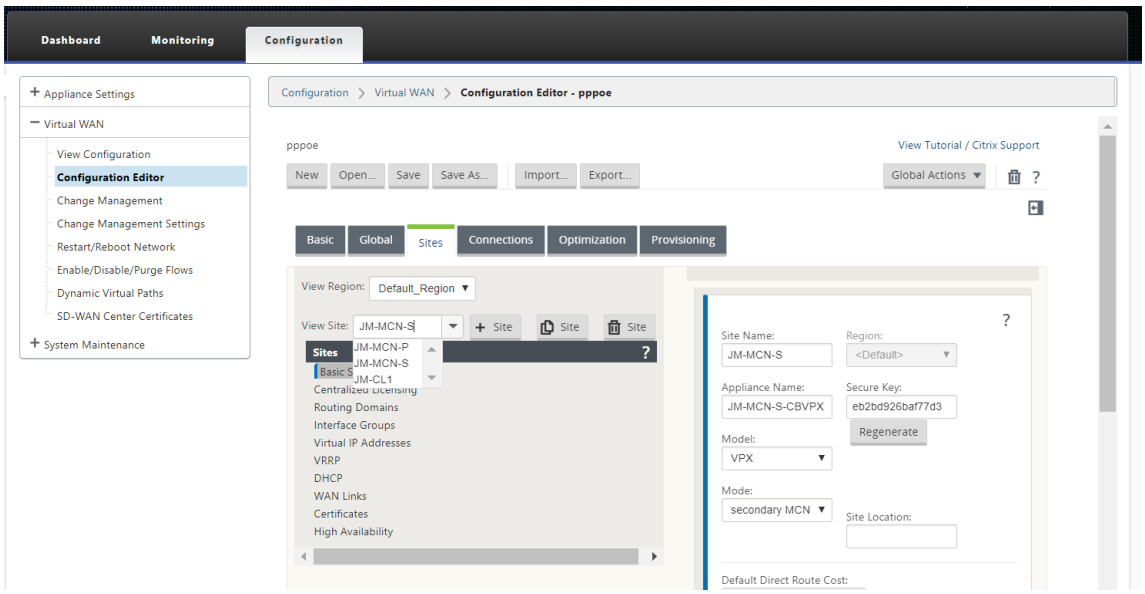
- None
- PPPoE Static
- PPPoE Dynamic
- DHCP

Configure MCN appliance

1. In the SD-WAN MCN appliance GUI, navigate to **configuration** > **Virtual WAN** > **Configuration Editor**. Add site under the **Basic** tab. For more information, refer to the branch node configuration at, configure mcn.



2. After the new site is created, open the **Sites** tab. Select the newly created site from the **View Site** drop-down list.

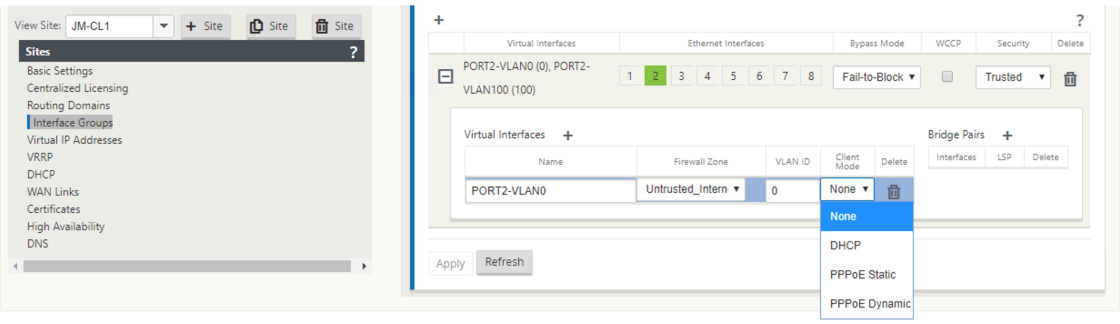


3. Select **Interface Groups** for the MCN site. Do the following:

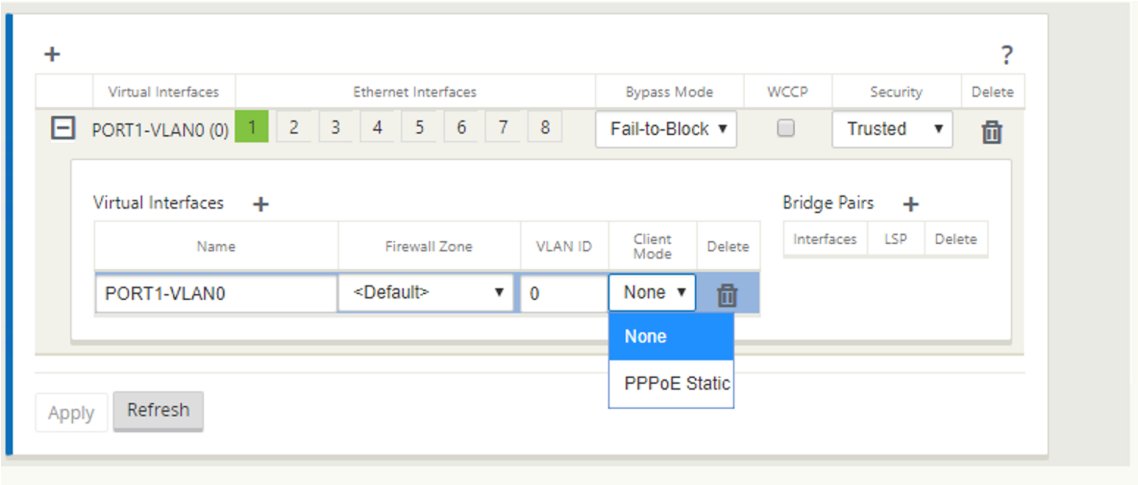
   - Add Virtual Interfaces.
   - Configure Ethernet Interfaces.
   - Configure Bypass Mode.
   - Choose **WCCP**, if necessary.
   - Choose Security –Trusted/Untrusted.

   For virtual interface:

   - Configure Name, Firewall Zone, VALN ID, and Client Mode.
   - A VNI configured with multiple interfaces can have only one interface used for PPPoE connectivity.
   - If a VNI configured with multiple interfaces and a PPPoE connectivity is changed to a different interface, then the monitor page can be used to stop the existing session and start a new session, then a new session can be established over the new interface.

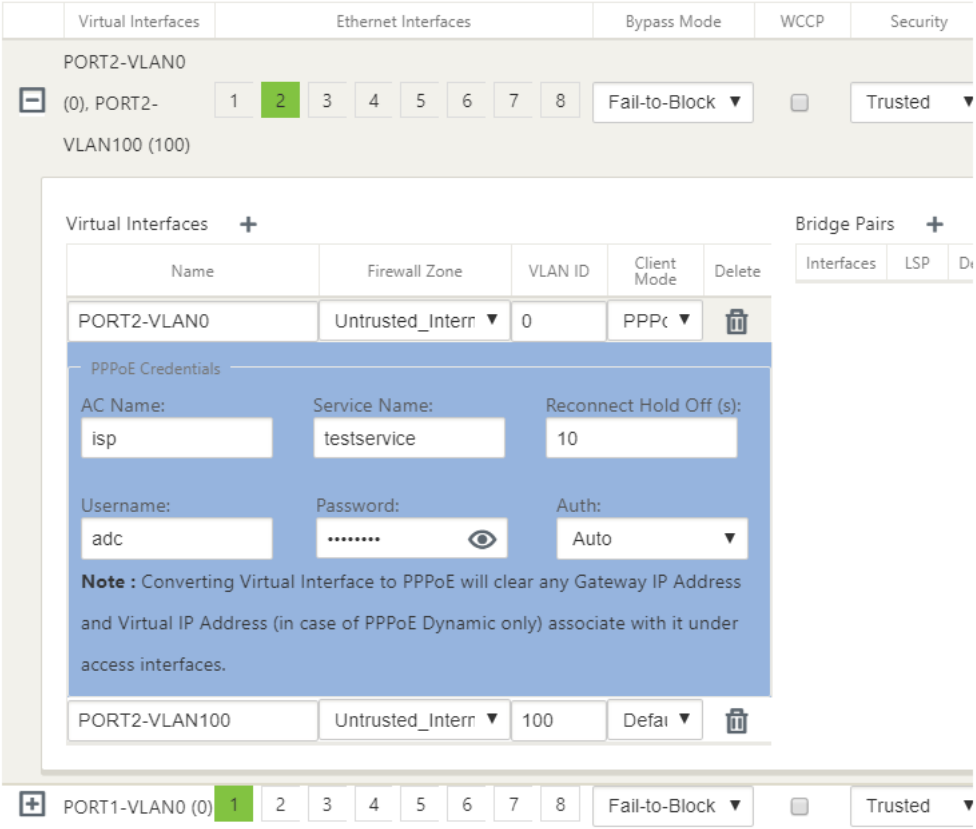


4. Select **PPPoE Static or None** based on your network configuration requirement for the Client Mode option on the MCN appliance. The following more options are displayed.

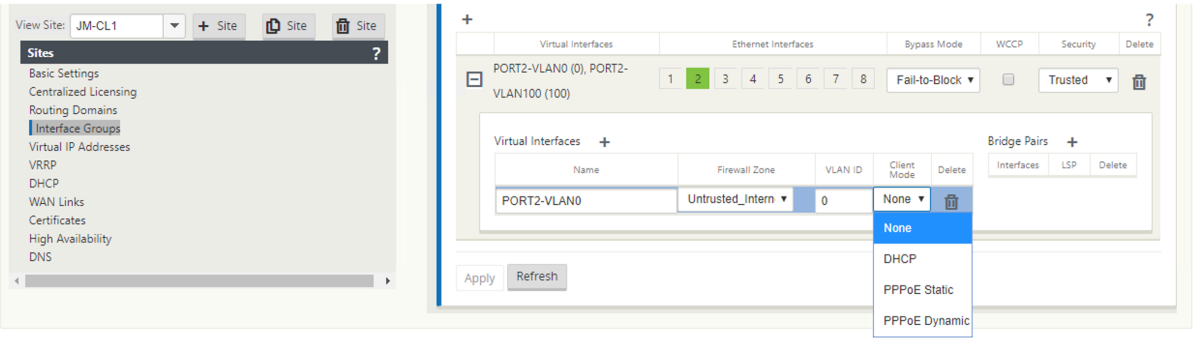


Configure the following PPPoE parameters and click **Apply**.

- Access Concentrator (AC) Name field.
- Service Name.
- Hold-off reconnect time (default is to reconnect immediately, '0')
- Authentication type - (AUTO/PAP/CHAP/EAP).
  - When Auth option is set to Auto, the SD-WAN appliance honors the supported authentication protocol request received from the server.
  - When Auth option is set to PAP/CHAP/EAP, then only specific authentication protocols are honored. If PAP is in the configuration and server sends an authentication request with CHAP, the connection request is rejected. If server does not negotiate with PAP, an authentication failure occurs.
- CHAP includes –CHAP, Microsoft CHAP, and Microsoft CHAPv2.
- EAP supports EAP-MD5.
- Username and password.



The following figure displays the PPPoE client mode options for a branch SD-WAN appliance. If PPPoE Dynamic is selected, the VNI is required to be “Untrusted.”

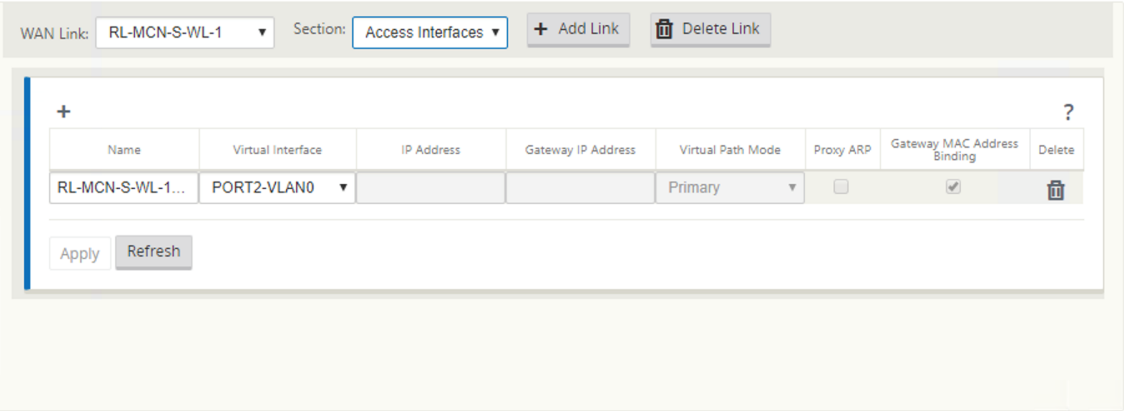


Configure WAN links

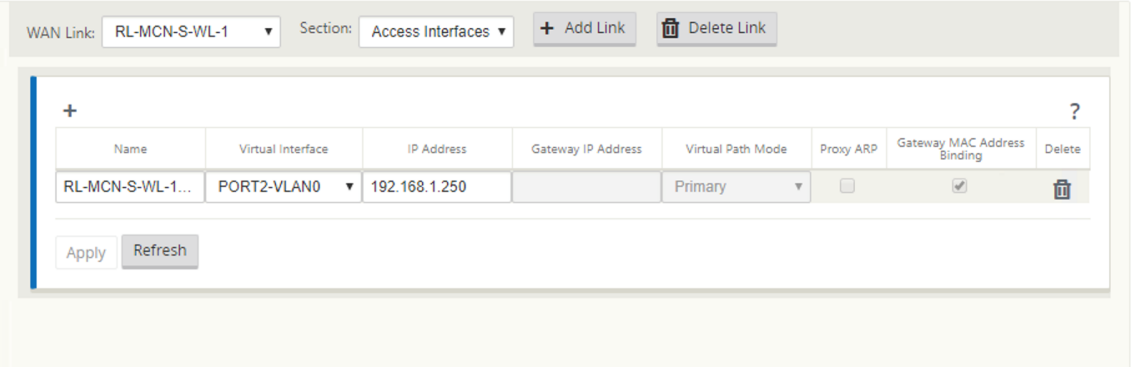
1. In the SD-WAN GUI, navigate to **Sites > WAN Links**. Only one WAN link creation is allowed per PPPoE static or dynamic VNI. The WAN link configuration varies depending on the VNI selection of the Client Mode.
2. If the VNI is configured with PPPoE dynamic client mode:
   - IP address and Gateway IP address fields become inactive.

- Virtual path mode is set to “Primary.”
- Proxy ARP cannot be configured.

By default, Gateway MAC Address Binding is selected.



3. If the VNI is configured with PPPoE static client mode, configure the IP address.



> **Note**:
>
> If the server does not honor the configured static IP address and offers a different IP address, an error occurs. The PPPoE session tries to re-establish connection periodically, until the server accepts the configured IP address.

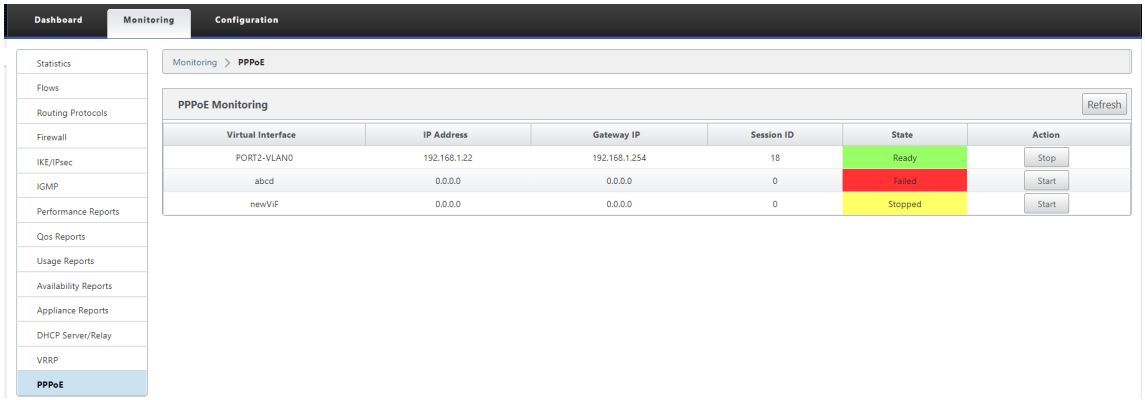
Monitor PPPoE sessions

You can monitor PPPoE sessions by navigating to the **Monitoring > PPPoE** page in the SD-WAN GUI.

The PPPoE page provides status information of the configured VNIs with the PPPoE static or dynamic client mode. It allows you to manually start or stop the sessions for troubleshooting purposes.

- If the VNI is up and ready, the **IP and Gateway IP** columns shows the current values in the session. It indicates that these are recently received values.
- If the VNI is stopped or is in failed state, the values are last received values.

- Hovering mouse over Gateway IP column shows the MAC address of the PPPoE Access Concentrator from where the Session and IP is received.
- Hovering mouse over the “state”value shows a message, which is more useful for a “Failed” state.



The **State** column displays the status of the PPPoE session using three color codes; green, red, yellow, and values. The following table describes the states and descriptions. You can hover over the states to obtain descriptions.

PPPoE session type	Color	Description
Configured	Yellow	A VNI is configured with PPPoE. This is an initial state.
Dialing	Yellow	After a VNI is configured, the PPPoE session state moves to dialing state by starting the PPPoE discovery. Packet information is captured.
Session	Yellow	VNI is moved from Discovery state to Session state. waiting to receive IP, if dynamic or waiting for acknowledgement from server for the advertised IP, if static.
Ready	green	IP packets are received and VNI and associated WAN link is ready for use.

PPPoE session type	Color	Description
Failed	red	PPP/PPPoE session is terminated. The reason for the failure can be due to Invalid Configuration or fatal error. The session attempts to reconnect after 30 seconds.
Stopped	yellow	PPP/PPPoE session is manually stopped.
Terminating	yellow	An intermediate state terminating due to a reason. This state automatically starts after certain duration (5 seconds for normal error or 30 secs for a fatal error).
Disabled	yellow	The SD-WAN service is disabled.

Troubleshooting PPPoE session failures

On the Monitoring page, when there is a problem in establishing a PPPoE session:

- Hovering mouse over the Failed status shows the reason for the recent failure.
- To establish a fresh session or for troubleshooting an active PPPoE session, use the monitoring->PPPoE page and restart the session.
- If a PPPoE session is stopped manually, it cannot be started until either it is manually started and a configuration change is activated, or service is restarted.

A PPPoE session might fail due to the following reasons:

- When SD-WAN fails to authenticate itself to the peer due to incorrect username/password in the configuration.
- PPP negotiation fails - negotiation does not reach the point where at least one network protocol is running.
- System memory or system resource issue.
- Invalid/bad configuration (wrong AC name or service name).
- Failed to open serial port due to operating system error.
- No response received for the echo packets (link is bad or server is not responding).

- There were several continuous unsuccessful dialing sessions with in a minute.

After 10 consecutive failures, the reason for the failure is observed.

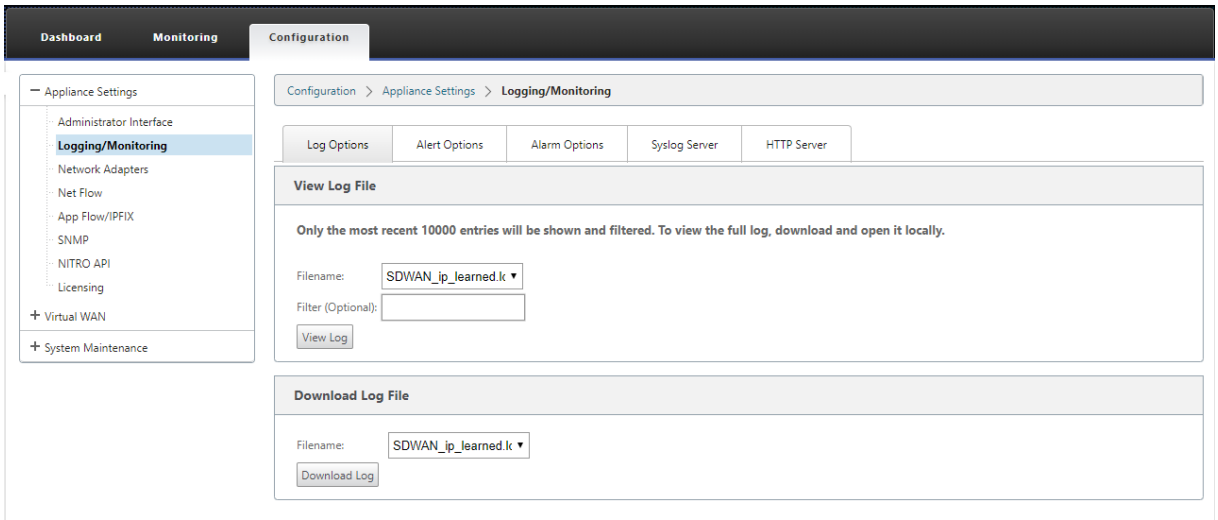
- If the failure is normal, it restarts immediately.
- If the failure is an error then restart reverts for 10 seconds.
- If the failure is fatal the restart reverts for 30 seconds before restarting.

LCP Echo request packets are generated from SD-WAN for every 60 seconds and failure to receive 5 echo responses is considered as link failure and it re-establishes the session.

PPPoE log file

The *SDWAN_ip_learned.log* file contains logs related to PPPoE.

To view or download the *SDWAN_ip_learned.log* file from the SD-WAN GUI, navigate to **Appliance Settings** > **Logging/Monitoring** > **Log Options**. View or download the *SDWAN_ip_learned.log* file.



Quality of service

March 12, 2021

The network between office locations and the data center or cloud must transport a multitude of applications and data, including high quality video or real-time voice. Bandwidth sensitive applications stretch the network's capabilities and resources. Citrix SD-WAN provides guaranteed, secure, measurable, and predictable network services. This is achieved by managing the delay, jitter, bandwidth, and packet loss on the network.

The Citrix SD-WAN solution includes a sophisticated application Quality-of-Service (QoS) engine that accesses the application traffic and prioritizes critical applications. It also understands the requirements for 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.

Classes

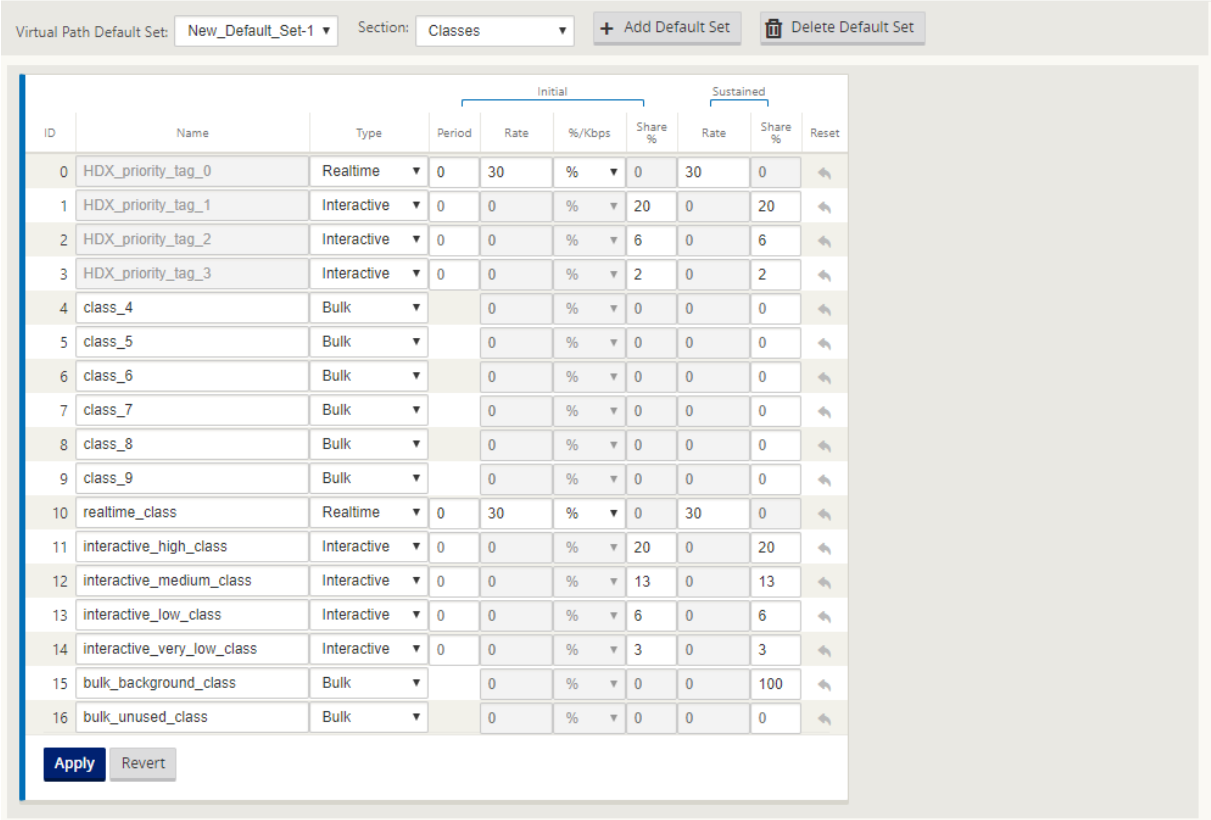
October 12, 2021

The Citrix SD-WAN configuration provides a default set of application and IP/Port based QoS policies that are applied to all traffic going over Virtual Paths. These settings can be customized to fit the deployment needs.

Classes are useful to prioritize the traffic. Application and IP/Port based QoS policies classify traffic and put it into appropriate classes specified in the configuration.

For more information on application QoS and IP address/port based QoS, see Rules by application name and Rules by IP address and port number respectively.

The SD-WAN provides 17 classes (IDs: 0–16). Following is the default configuration of all the 17 classes.



ID	Name	Type	Initial Period	Initial Rate	Initial %/Kbps	Initial Share %	Sustained Rate	Sustained Share %	Reset
0	HDX_priority_tag_0	Realtime	0	30	%	0	30	0	
1	HDX_priority_tag_1	Interactive	0	0	%	20	0	20	
2	HDX_priority_tag_2	Interactive	0	0	%	6	0	6	
3	HDX_priority_tag_3	Interactive	0	0	%	2	0	2	
4	class_4	Bulk		0	%	0	0	0	
5	class_5	Bulk		0	%	0	0	0	
6	class_6	Bulk		0	%	0	0	0	
7	class_7	Bulk		0	%	0	0	0	
8	class_8	Bulk		0	%	0	0	0	
9	class_9	Bulk		0	%	0	0	0	
10	realtime_class	Realtime	0	30	%	0	30	0	
11	interactive_high_class	Interactive	0	0	%	20	0	20	
12	interactive_medium_class	Interactive	0	0	%	13	0	13	
13	interactive_low_class	Interactive	0	0	%	6	0	6	
14	interactive_very_low_class	Interactive	0	0	%	3	0	3	
15	bulk_background_class	Bulk		0	%	0	0	100	
16	bulk_unused_class	Bulk		0	%	0	0	0	

The following are the different types of classes:

- **Real-time**: 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 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. The interaction is typically between a client and a server. The communication might not need high bandwidth but is sensitive to loss and latency.
- **Bulk**: Used for high bandwidth traffic and applications that can tolerate high latency. Applications that handle file transfer and need high bandwidth are categorized as bulk class. These applications involve little human interference and are mostly handled by the systems themselves.

Bandwidth sharing among classes

Bandwidth is shared among classes as follows:

- **Real-time**: Traffic hitting real-time classes are guaranteed to have low latency and bandwidth is capped to the class share when there is competing traffic.
- **Interactive**: Traffic hitting the interactive classes get remaining bandwidth after serving real-time traffic and the available bandwidth is fair shared among the interactive classes.

- **Bulk**: Bulk is best effort. Bandwidth left over after serving real-time and interactive traffic is given to bulk classes on a fair share basis. Bulk traffic can starve if real-time and interactive traffic utilizes all the available bandwidth.

> **Note**
>
> Any class can use all available bandwidth when there is no contention.

The following example explains the bandwidth distribution based on the class configuration:

Consider there is an aggregated bandwidth of 10 Mbps over Virtual Path. If the class configuration is

- Real-time: 30%
- Interactive High: 40%
- Interactive Medium: 20%
- Interactive Low: 10%
- Bulk: 100%

The bandwidth distribution outcome is

- Real-time traffic gets 30% of 10Mbs (3 Mbps) based on the need. If it needs less than 10%, then the rest of the bandwidth is made available to the other classes.
- Interactive classes share the remaining bandwidth on fair share basis (4 Mbps: 2 Mbps: 1 Mbps).
- Anything leftover when real-time, interactive traffic is not fully using their shares is given to the Bulk class.

To customize classes:

1. If Virtual Path Default Sets are in use, classes can be modified under **Global > Virtual Path Default Sets**.

   > **Note**
   >
   > You can also modify classes at the Virtual Path level (**Connections -> Virtual Paths -> Classes**)

2. Click **Add Default Set**, enter a name for the default set, and click **Add**. In the **Section** field, select **Classes**.
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 (Real-time, Interactive, or Bulk).
5. For real-time 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 or percentage at which packets leave the queue during the initial period.
- **Sustained Rate**: Maximum rate or percentage at which the packets leave the queue after the initial period.

6. For interactive classes, you can specify the following attributes:
   - **Initial Period**: The time period, in milliseconds, during which to apply the initial percentage of the available bandwidth before switching to the sustained percentage. Typically, 20 ms.
   - **Initial Share %**: The maximum share of virtual-path bandwidth remaining after serving real-time during the initial period.
   - **Sustained Share %**: The maximum share of virtual-path bandwidth remaining after serving real-time traffic after the initial period.
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 after serving real-time and interactive traffic.
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

March 12, 2021

Rules by IP address and port number feature helps you to create rules for your network and take certain Quality of Service (QoS) decisions based on the rules. You can create custom rules for your network. For example, you can create a rule as –If source IP address is 172.186.30.74 and destination IP address is 172.186.10.89, set **Transmit mode** as Persistent Path and **LAN to WAN Class** as 10(real-time_class)".

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.

You can create rules locally at a site level or at the global level. If more than one site requires the same rule, you can create a template for rules globally under **Global > Virtual Path Default Sets > Rules**.

The template can then be attached to the sites where the rules need to be applied. Even if a site is associated with the globally created rule template, you can create site specific rules. In such cases, site specific rules take precedence and override the globally created rule template.

Create rules by IP address and port number

1. In the SD-WAN Configuration Editor, navigate to **Global** > **Virtual Path Default Sets.**

   > **Note**
   >
   > You can create rules at site level by navigating to **Sites > Connections > Virtual Paths > Rules**.

2. Click **Add Default Set**, enter a name for the default set, and click **Add**. In the Section field, select **Rules** and 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 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 applications. 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 based on the parameters listed as follows. 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**
     >
     > If the **Dest=Src** check box is selected, the source IP address will also be used for the destination IP address.

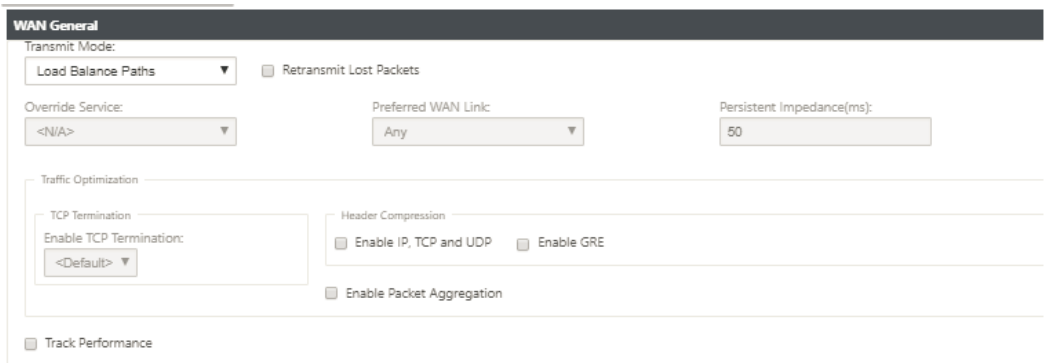
   - **Protocol**: Protocol to match against the traffic.
   - **Source Port**: Source port number or port range to match against the traffic.
   - **Destination Port**: Destination port number or port range to match against the traffic.

> **Note**
>
> If the **Dest=Src** check box is selected, the source port will also be used for the destination port.

- **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 populates 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 is sent through the best path until that path is used. Leftover packets are sent through the next best path.
     - **Persistent Path**: Traffic for the flow remains 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 overrides to a different service. In the Override Service field, select the service type to which the service overrides. For example, a virtual path service can 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. The round-trip time for acknowledgment of packets is reduced, 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 the wait time on which 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 the performance attributes of this rule in a session data base (for example, loss, jitter, latency, and bandwidth).

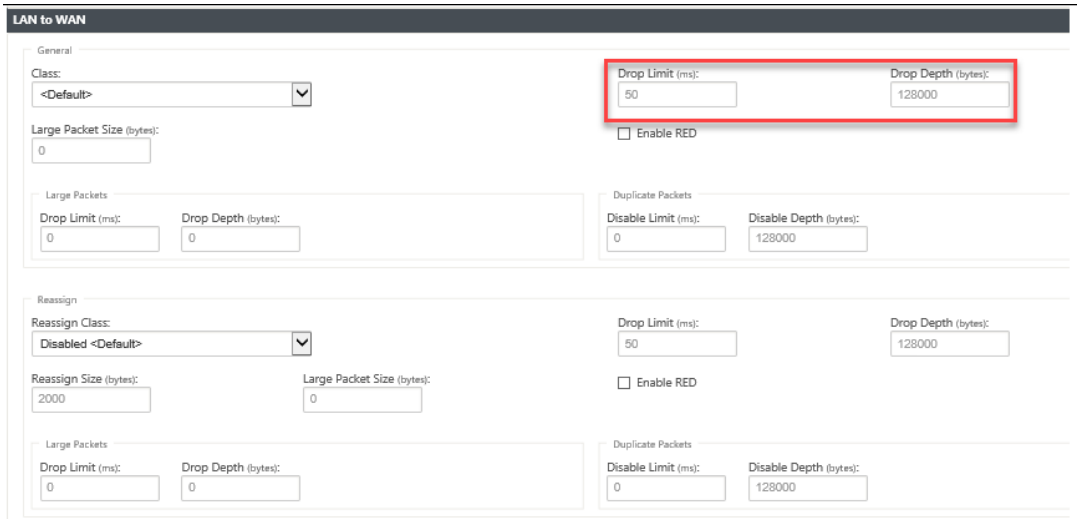


10. Click the **LAN to WAN** tile, to configure LAN to WAN behavior for this rule.

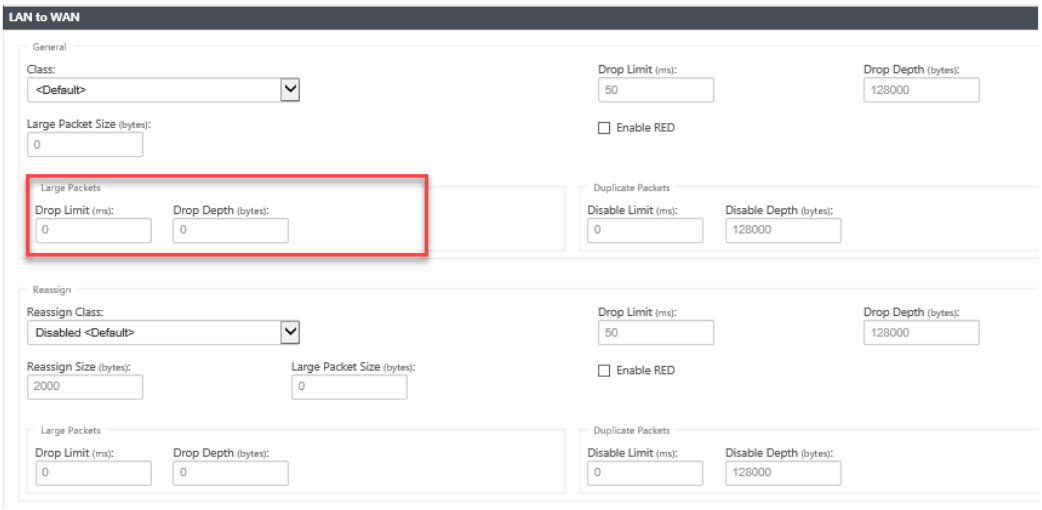
- **Class**: Select a class with which to associate this rule.

> **Note**
>
> You can also customize classes before applying rules, for more information, see How to Customize Classes.

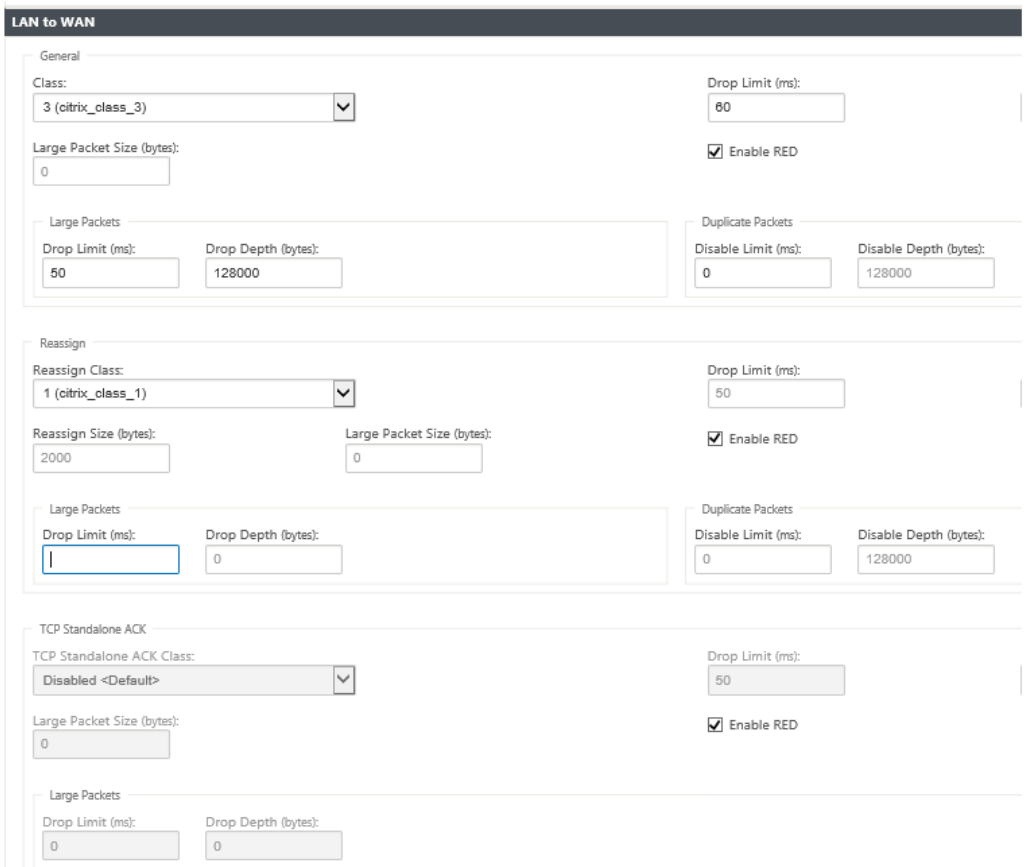
- **Large Packet Size**: Packets smaller than or equal to this size are assigned the **Drop Limit** and **Drop Depth** values specified in the fields to the right of the **Class** field.



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.

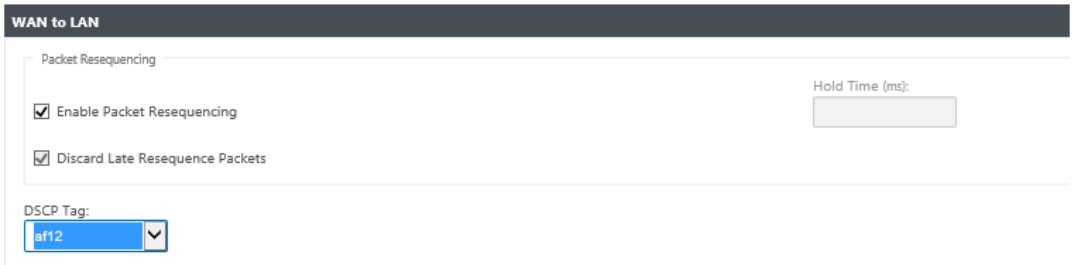


- **Drop Limit**: Length of time after which packets waiting in the class scheduler are dropped. Not applicable for a bulk class.
- **Drop Depth**: Queue depth threshold after which packets are dropped.
- **Enable RED**: Random Early Detection (RED) ensures fair sharing of class resources by discarding 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 acknowledgments are mapped during large file transfers.



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.



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.

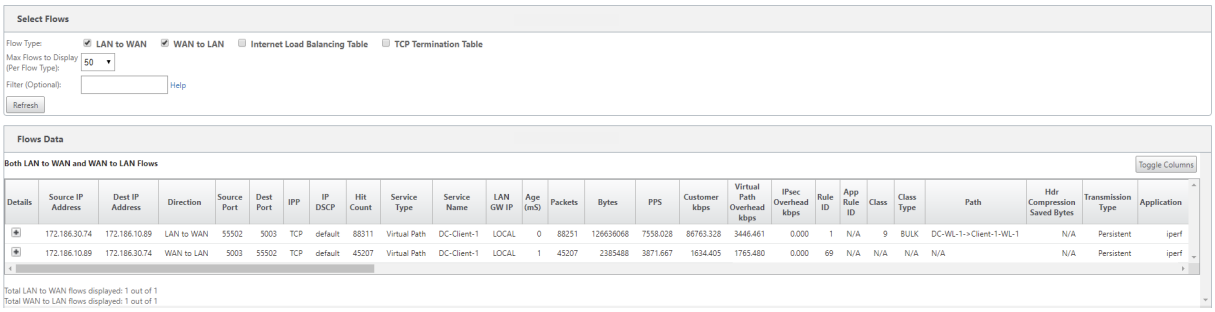
13. Click **Apply**.

> **Note**
>
> Save the configuration, export it to the change management inbox, and initiate the change management process.

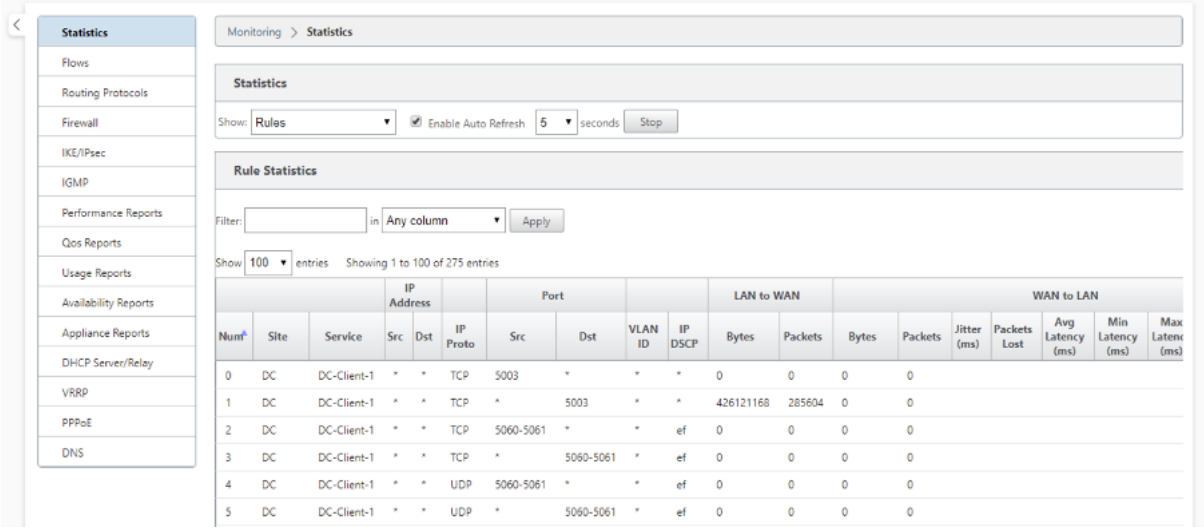
Verify rules

In the Configuration Editor, navigate to **Monitoring > Flows**. Select **Flow Type** field located in the **Select Flows** section at the top of the **Flows** page. Next to the **Flow Type** field there is a row of check boxes for selecting the flow information you want to view. Verify if the flow information is according to the configured rules.

Example:
The rule "If source IP address is 172.186.30.74 and destination IP address is 172.186.10.89, set **Transmit mode** as Persistent Path"shows the following **Flows Data**.



In the Configuration Editor, navigate to **Monitoring > Statistics** and verify the configured rules.



Rules by application name

March 12, 2021

The Application classification feature allows the Citrix 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 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 Aggregation	Enable Packet Resequencing	Resequence Hold Time (ms)	Discard Late Resequencing Packets	Drop Limit (ms)	Drop Depth (bytes)	Enable RED	Disable Limit (ms)	Disable Depth (bytes)
HDX_Priority_0	0 (HDX_priority_tag_0)	Load Balance Path	True	False	True	250	True	350	30000	True	0	128000

Rule	Class	Transmit Mode	Retransmit Lost Packets	Enable Packet Aggregation	Enable Packet Resequencing	Resequence Hold Time (ms)	Discard Late Resequencing Packets	Drop Limit (ms)	Drop Depth (bytes)	Enable RED	Disable Limit (ms)	Disable Depth (bytes)
HDX_Priority_1	1 (HDX_priority_tag_1)	Load Balance Path	True	False	True	250	True	350	30000	True	0	128000
HDX_Priority_2	2 (HDX_priority_tag_2)	Load Balance Path	True	False	True	250	True	350	30000	True	0	128000
HDX_Priority_3	3 (HDX_priority_tag_3)	Load Balance Path	True	False	True	250	True	350	30000	True	0	128000
HDX	11 (interactive_high_class)	Load Balance Path	True	False	True	250	True	350	30000	True	0	128000

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 are applied to the packets. After DPI classification, the application rule attributes such as Class, transmit mode 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.

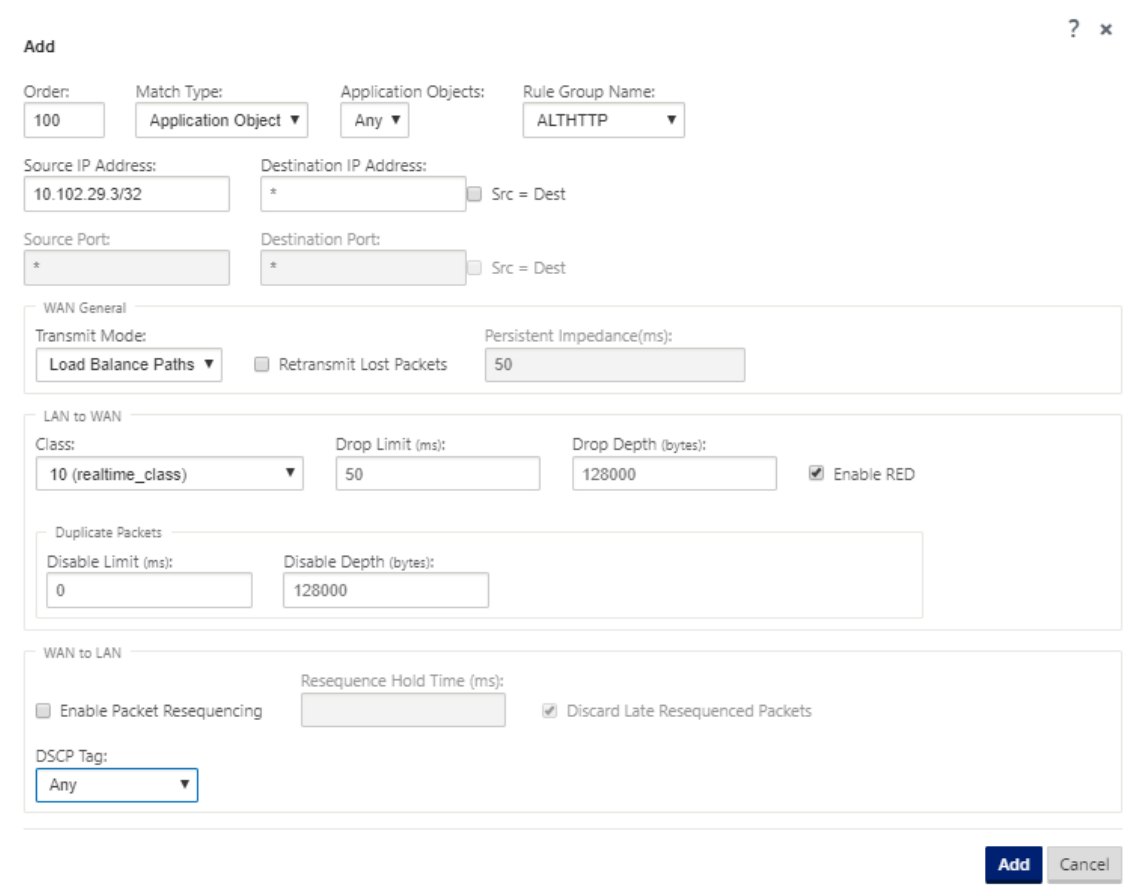
For example, consider you have specified an application rule for a webmail application such as Google Mail that uses the SMTP protocol. The IP rule set for SMTP protocol is applied initially before DPI classification. After parsing the packets and classifying it as belonging to Google Mail application, 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** and 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.**



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 object 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 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 custom applications 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 Customize 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.

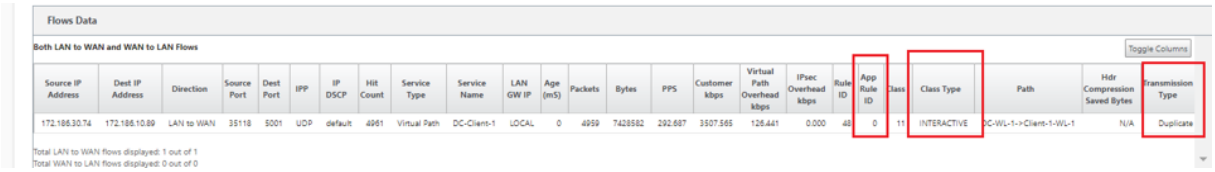
9. Configure the following WAN to LAN behavior for this rule:

   - **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**.

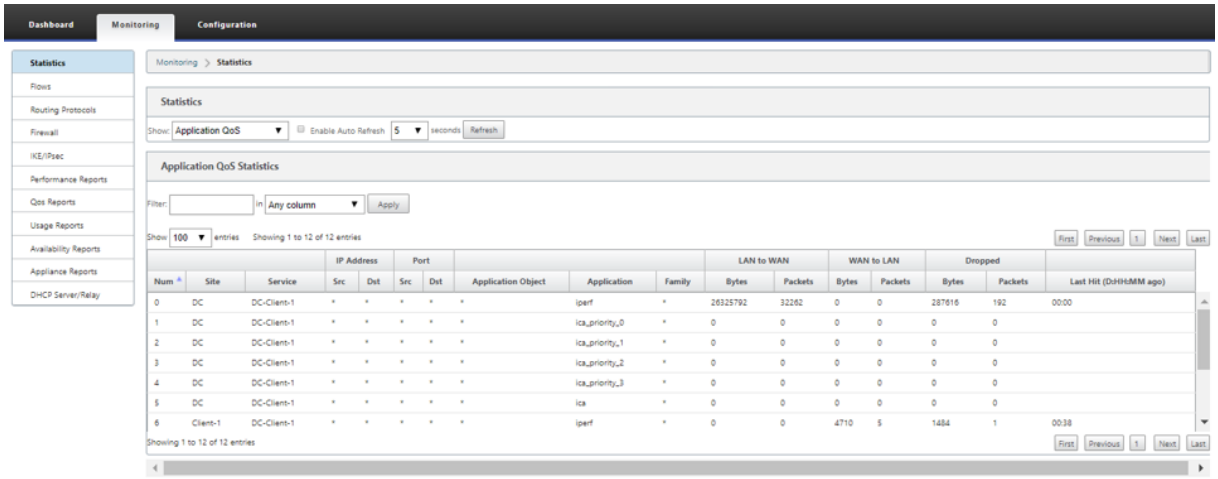
To confirm if application rules are applied to traffic flow, navigate to **Monitoring** > **Flows**.

Make a note of the app rule id and check if the class type and transmission mode are as per your rule configuration.



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

You can use application objects to define custom applications based on the following match types:

- IP protocol
- Application name
- Application family

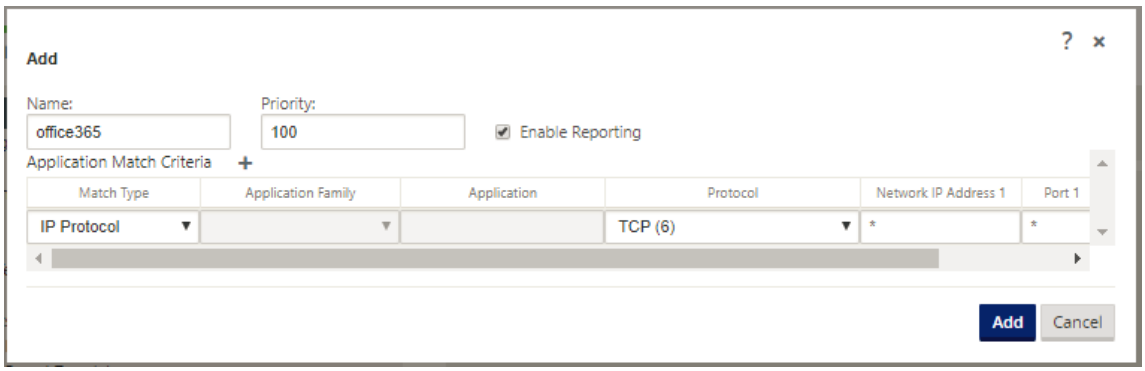
The DPI classifier analyzes the incoming packets and classifies it as applications based on the specified match criteria. You can use these classified custom applications in QoS, firewall, and application routing.

> **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 Application report.

To create custom applications:

1. In the Configuration Editor, navigate to **Global** > **Applications** > **Custom Applications** and click **+**.



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, Application report.
   - **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

March 12, 2021

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**.

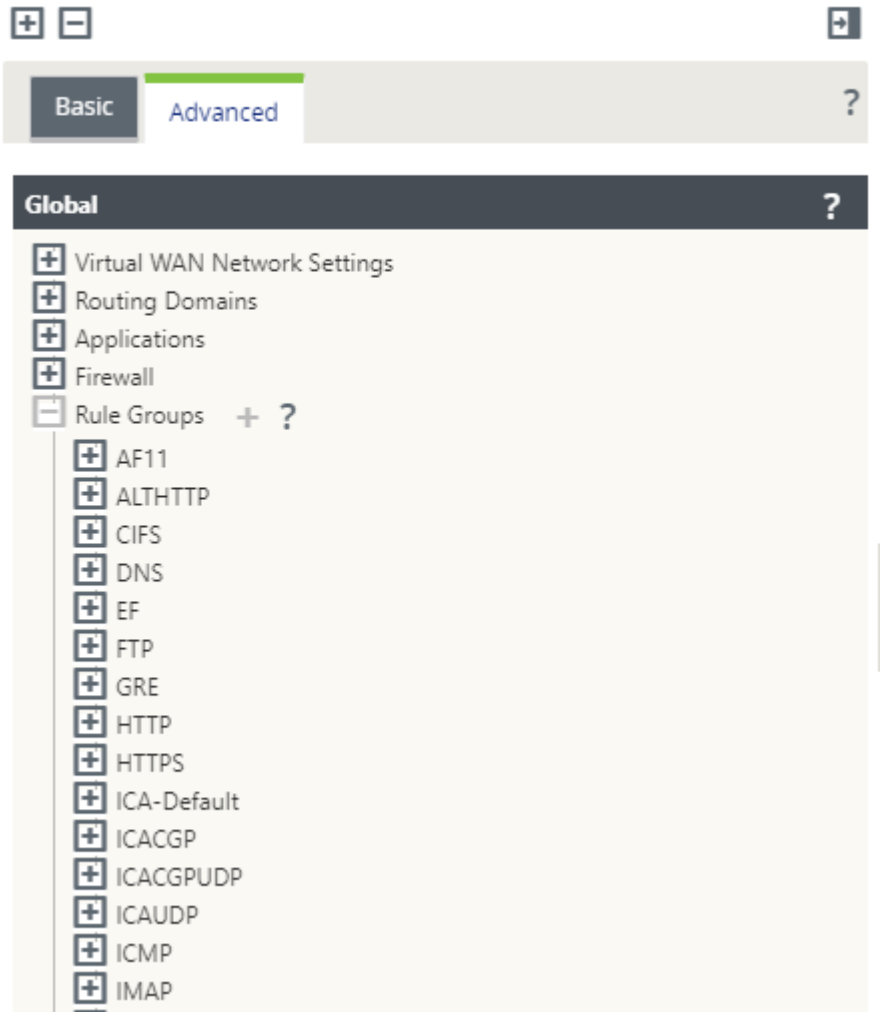
The mean opinion score (MOS) is a numerical measure of the quality of the experience that an application delivers to end users. It is primarily used for VoIP applications. In SD-WAN, MOS is also used to assess the quality of non-VoIP applications by judging the traffic as if it were a VoIP call.

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 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** .



5. Click **Apply**.

> **Note**
>
> - You can also enable MOS estimation for the default applications, by selecting **Enable MOS**.
> - Enable the Track Performance option under Rules to estimate MOS for applications and display it in SD-WAN Center. For more information. see MOS for Applications.

Application classification

March 12, 2021

The Citrix SD-WAN appliances perform deep packet inspection (DPI) to identify and classify applications using the following techniques:

- DPI library classification
- Citrix-proprietary Independent Computing Architecture (ICA) classification
- Application vendor APIs (for example Microsoft REST APIs for Office 365)
- Domain name based application classification

DPI library classification

The Deep Packet Inspection (DPI) library recognizes thousands of commercial applications. It enables real-time discovery and classification of applications. Using the DPI technology, the SD-WAN appliance analyses the incoming packets and classifies the traffic as belonging to a particular application or application family. Application classification for each connection takes a few packets.

To enable DPI library classification, in the **Configuration Editor**, navigate to **Global > Applications > DPI Settings** and select the **Enable Deep Packet Inspection** check box.

ICA classification

Citrix SD-WAN appliances can also identify and classify Citrix HDX traffic for virtual apps and desktops. Citrix SD-WAN recognizes the following variations of the ICA protocol:

- ICA
- ICA-CGP
- Single Stream ICA (SSI)
- Multi-Stream ICA (MSI)
- ICA over TCP
- ICA over UDP/EDT
- ICA over non-standard ports (including Multi-Port ICA)
- HDX Adaptive Transport
- ICA over WebSocket (used by HTML5 Receiver)

> **Note**
>
> Classification of ICA traffic delivered over SSL/TLS or DTLS is not supported in SD-WAN Standard Edition but is supported in SD-WAN Premium Edition and SD-WAN WANOP Edition.
>
> Classification of network traffic is done during initial connections or flow establishment. Therefore, pre-existing connections are not classified as ICA. Classification of connections is also lost when the connection table is cleared manually.
>
> Framehawk traffic and Audio-over-UDP/RTP are not classified as HDX applications. They are re-

> ported as either “UDP”or “Unknown Protocol.”
>
> Since release 10 version 1, the SD-WAN appliance can differentiate each ICA data stream in multi-stream ICA even in a single-port configuration. Each ICA stream is classified as a separate application with its own default QoS class for prioritization.
>
> - For Multi-Stream ICA functionality to work properly, you must have SD-WAN Standard Edition 10.1 or above, or SD-WAN Premium Edition.
> - For HDX user based reports to be shown on SDWAN-Center, you must have SD-WAN Standard Edition or Premium Edition 11.0 or above.
>
> Minimum software requirements for HDX information virtual channel:
>
> - A Current Release of Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop), since the prerequisite functionality was introduced in XenApp and XenDesktop 7.17 and is not included in the 7.15 Long-Term Service Release.
> - A version of the Citrix Workspace app (or its predecessor, Citrix Receiver) that supports multi-stream ICA and the HDX Insights information virtual channel, CTXNSAP. Look for **HDX Insight with NSAP VC** and Multiport/Multi-stream ICA in the Citrix Workspace app Feature Matrix. See the currently supported release versions at HDX Insights.
> - From 11.2 release onwards, packet duplication is now enabled by default for HDX real-time traffic when multi-stream ICA is in use.

Once classified, the 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:

- Independent Computing Architecture (Citrix)(ICA)
- ICA Real-time (ica_priority_0)
- ICA Interactive (ica_priority_1)
- ICA Bulk-Transfer (ica_prority_2)
- ICA Background(ica_priority_3)

For more information, see Rules by Application Name

If you are running a combination of software that does not support Multi-Stream ICA over a single port, then to perform QoS you must configure multiple ports, one for each ICA stream.
To classify HDX on non-standard ports as configured in XA/XD server policy, you must add those ports in ICA port configurations. Also, to match traffic on those ports to valid IP rules, you must update the 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 a 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 Citrix Application Delivery Management.

To enable ICA based classification, in the **Configuration Editor**, navigate to **Global > Applications > DPI Settings** and select the **Enable Deep Packet Inspection for Citrix ICA Applications** check box.

Application vendor API based classification

Citrix SD-WAN supports the following application vendor API based classification:

- Office 365. For more information, see Office 365 optimization.
- Citrix Cloud and Citrix Gateway service. For more information, see Gateway Service Optimization.

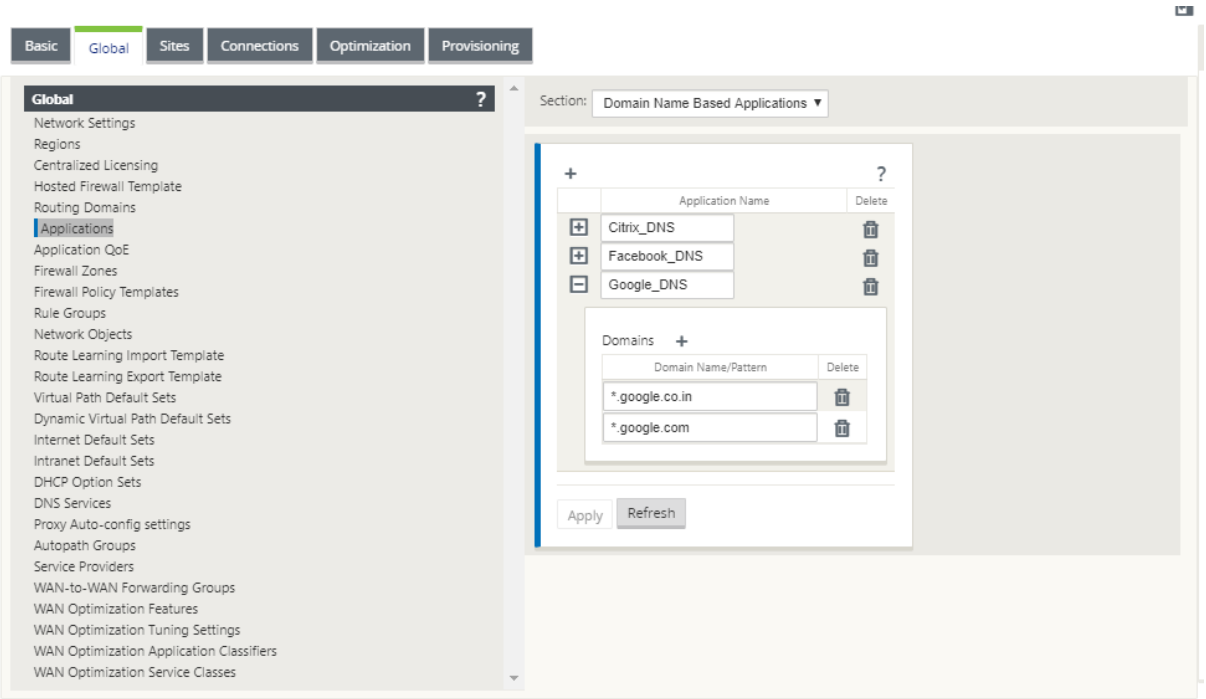
Domain name based application classification

The DPI classification engine is enhanced to classify applications based on the domain name and patterns. After the DNS forwarder intercepts and parses the DNS requests, the DPI engine uses IP classifier to perform first packet classification. Further DPI library and ICA classification are done and the domain name based application ID is appended.

The Domain name based application feature allows you to group several domain names and treat it as a single application. Making it easier to apply firewall, application steering, QoS, and other rules. A maximum of 64 domain name based applications can be configured.

To define domain name based applications, in the Configuration Editor, navigate to **Global** > **Applications** > **Domain Name Based Applications**. Enter an application name and add the required domain names or patterns. You can either enter the full domain name or use wild cards at the beginning. The following domain name formats are allowed:

- example.com
- *.example.com



The classified domain name based applications are used in configuring the following:

- DNS Proxy
- DNS Transparent forwarder
- Application objects
- Application Routes
- Firewall policy
- Application QoS Rules
- Application QoE

Limitations

- If there are no DNS request/response corresponding to a domain name based application, the DPI engine does not classify the domain name based application and hence does not apply the application rules corresponding to the domain name based application.
- If an Application Object is created such that the port range includes port 80 and/or port 443, with a specific IP address match type that corresponds to a domain name based application, the DPI engine does not classify the domain name based application.
- If explicit web proxies are configured, you have to add all the domain name patterns to the PAC file, to ensure that the DNS response does not always return the same IP address.
- The domain name based application classifications are reset on configuration upgrade. Reclassification happens based on pre 11.0.2 release classification techniques such as DPI library classification, ICA classification and Vendor application APIs based classification.

- The application signatures learned (destination IP addresses) by domain name based application classification are reset on configuration update.
- Only the standard DNS queries and their responses are processed.
- AAAA records or IPv6 records are not supported.
- DNS response records split over multiple packets are not processed. Only DNS responses in a single packet are processed.
- DNS over TCP is not supported.
- Only top-level domains are supported as domain name patterns.

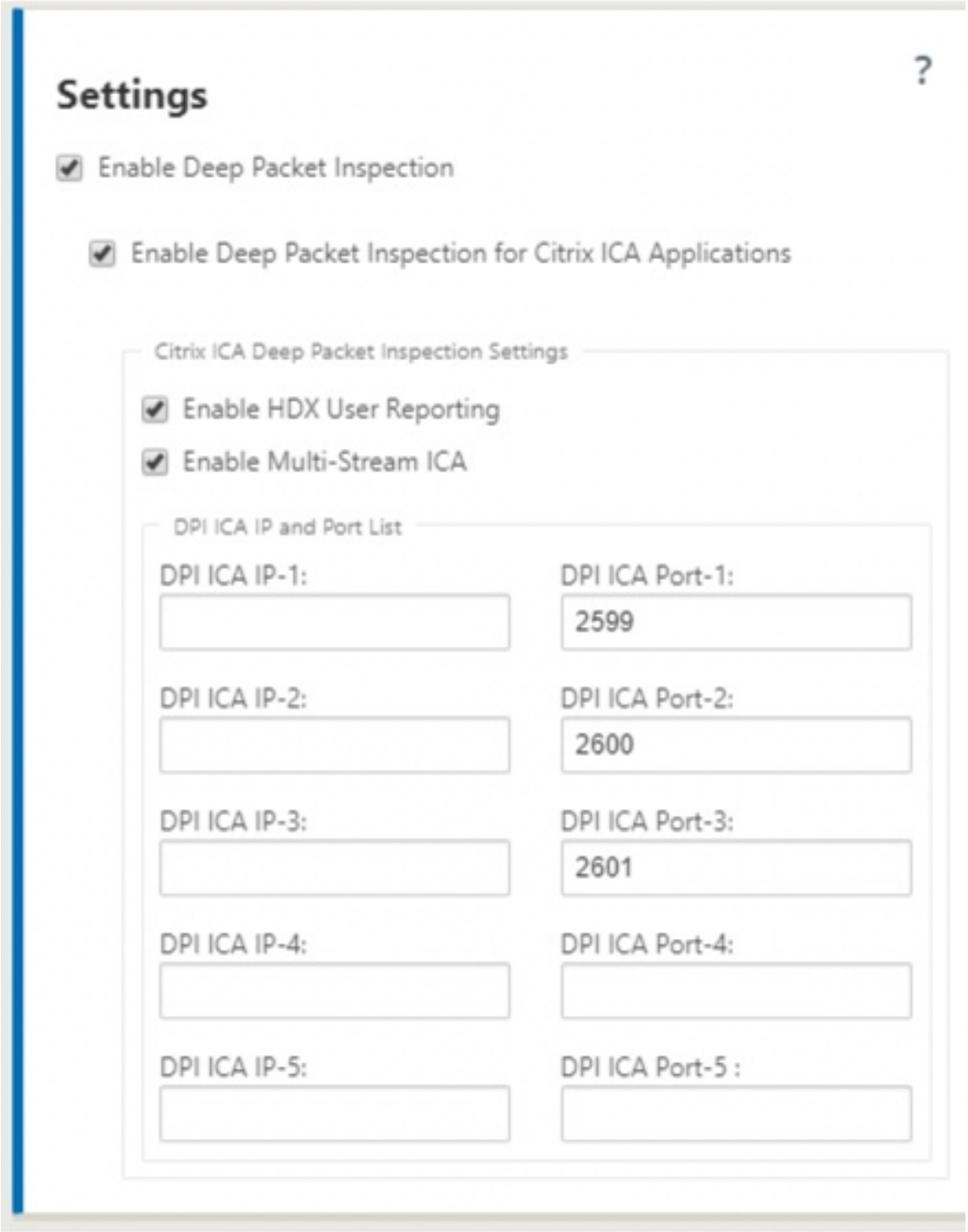
Classifying encrypted traffic

Citrix SD-WAN appliance 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 might 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:

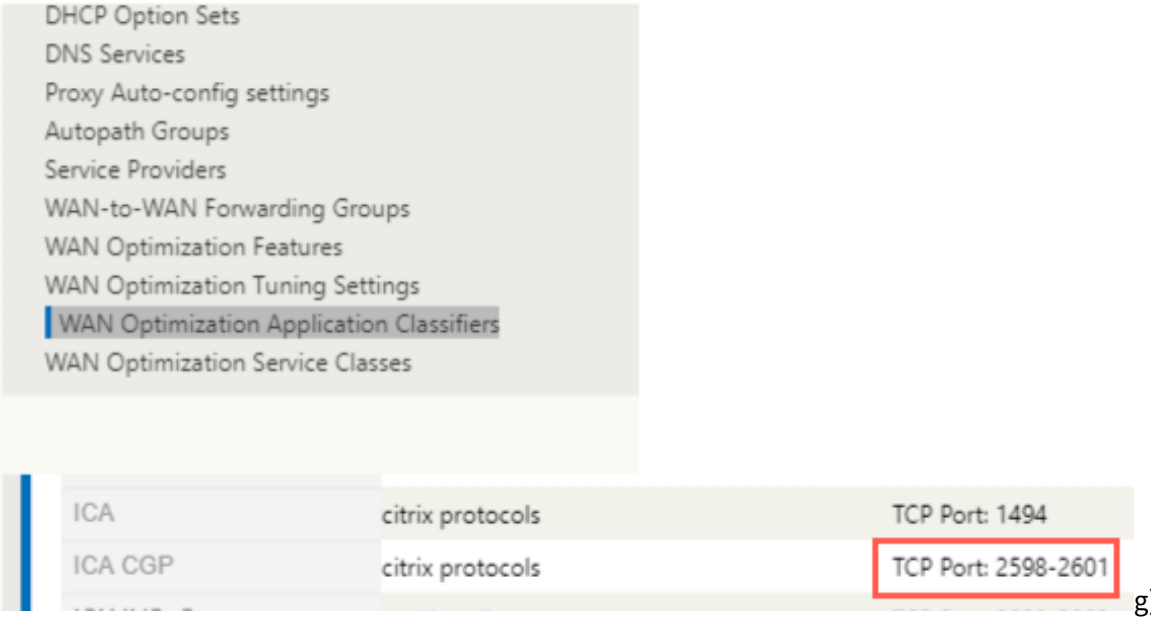
1. In the **Configuration Editor**, click **Global** > **Applications** > **Settings**.



Note

If you add extra ICA port for multiport deployment, these ports must be added in Wan optimization application classifiers. Otherwise the traffic on the three extra ports will not forwarded to WANOP. Only the default 2598 port is forwarded if ICA is configured to opti-

> mize.

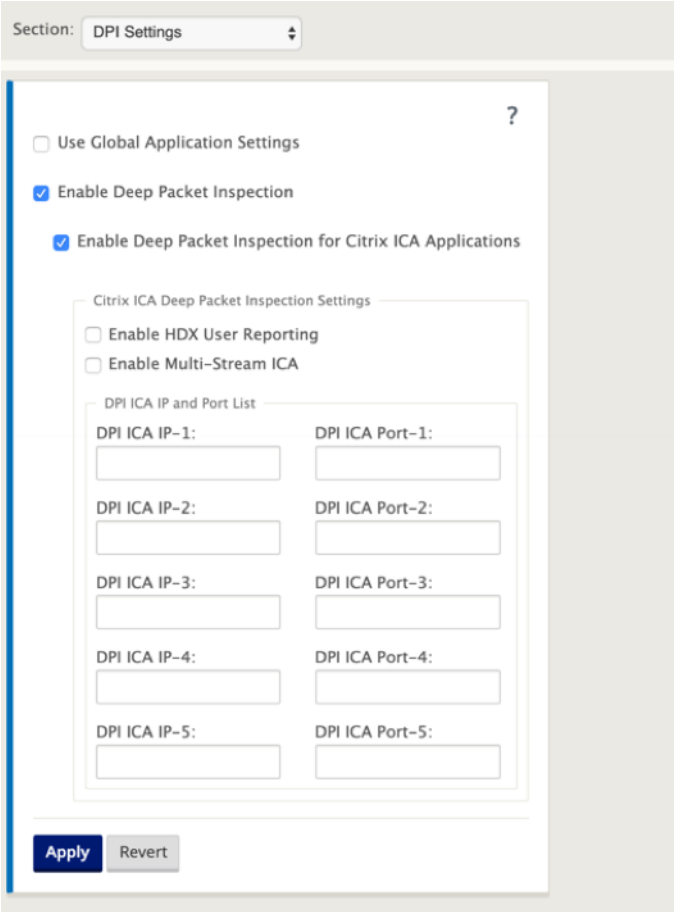


2. Select **Enable Deep Packet Inspection**. This enables application classification on the appliance. You can, view, and monitor application statistics on the SD-WAN Center. For more information, see Application report.

   > **Note**
   >
   > By default, **Enable Deep Packet Inspection** collects 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 might still be classified and QoE calculated but statistics on SD-WAN center is not available. You can, view, and monitor ICA application statistics on the SD-WAN Center. This option is enabled by default. For more information, see HDX Reports.

4. Select **Enable HDX User Reporting** to generate newly added user based reports (HDX Summary, HDX User Sessions, and **HDX Apps**) and these reports are available in SD-WAN Center. This is not applicable for the **HDX Site Stats** report. This option is available at the global and site level similar to enable DPI option. To **Enable HDX User Reporting** at site level, in the **Configuration Editor**, click **Connections > Applications**.



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.

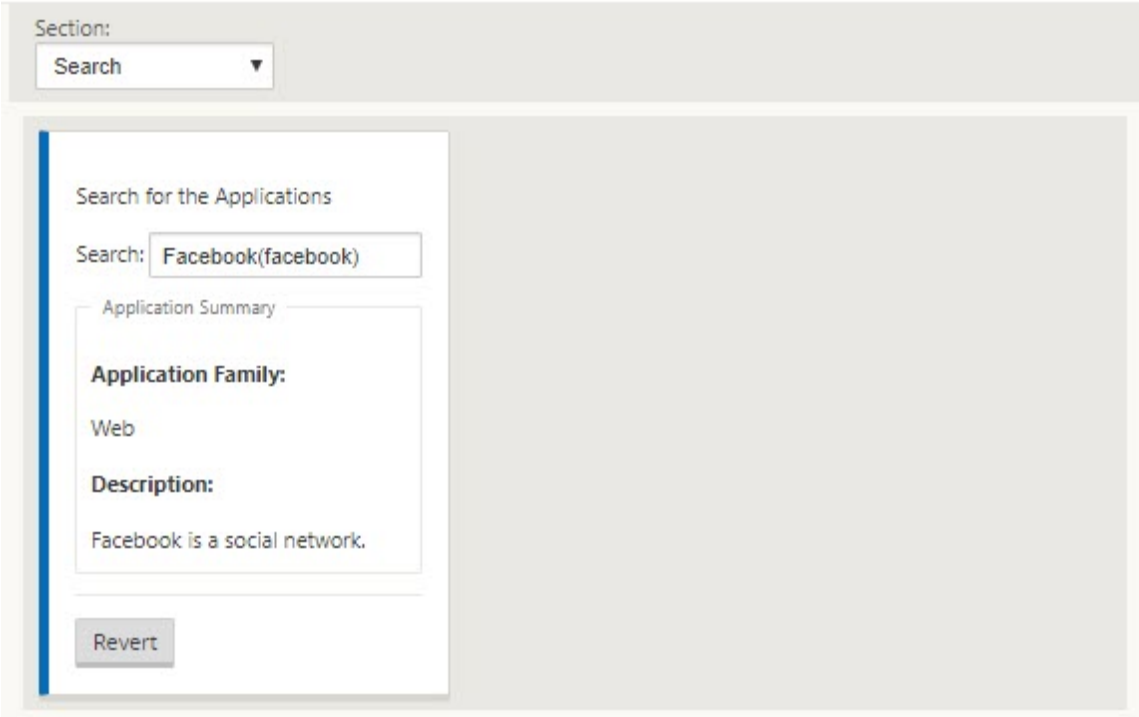
Search applications

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 click enter.

   A brief description of the Application and the Application Family name appears.



The following features use application as a match type:

- Firewall policy
- Application QoS Rules
- Application QoE

> **Note**
>
> For information on applications that the SD-WAN appliance can identify using Deep Packet Inspection, see Application Signature Library.

Application Objects

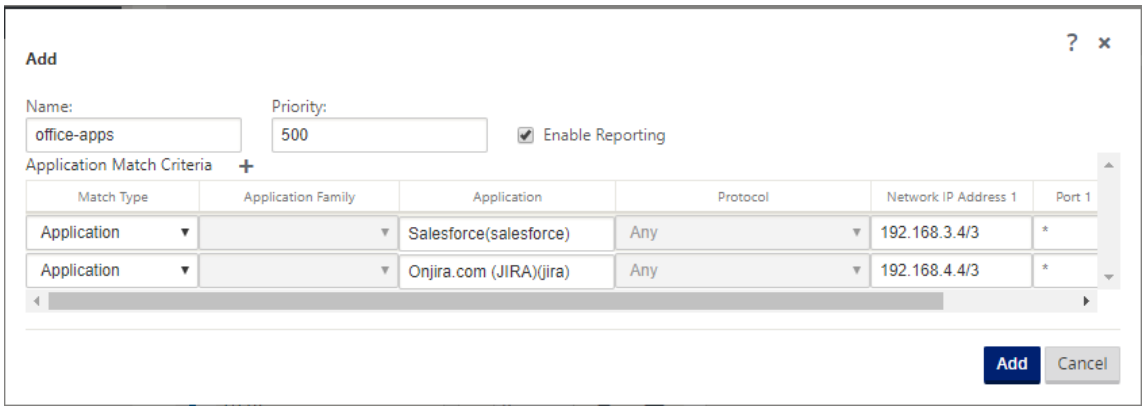
Application objects enable you to group different types of match criteria into a single object that can be used in firewall policies and application steering. IP Protocol, Application, and Application Family are the available match types.

The following features use application object as a match type:

- Application Routes
- Firewall policy
- Application QoS Rules
- Application QoE

To create an application object:

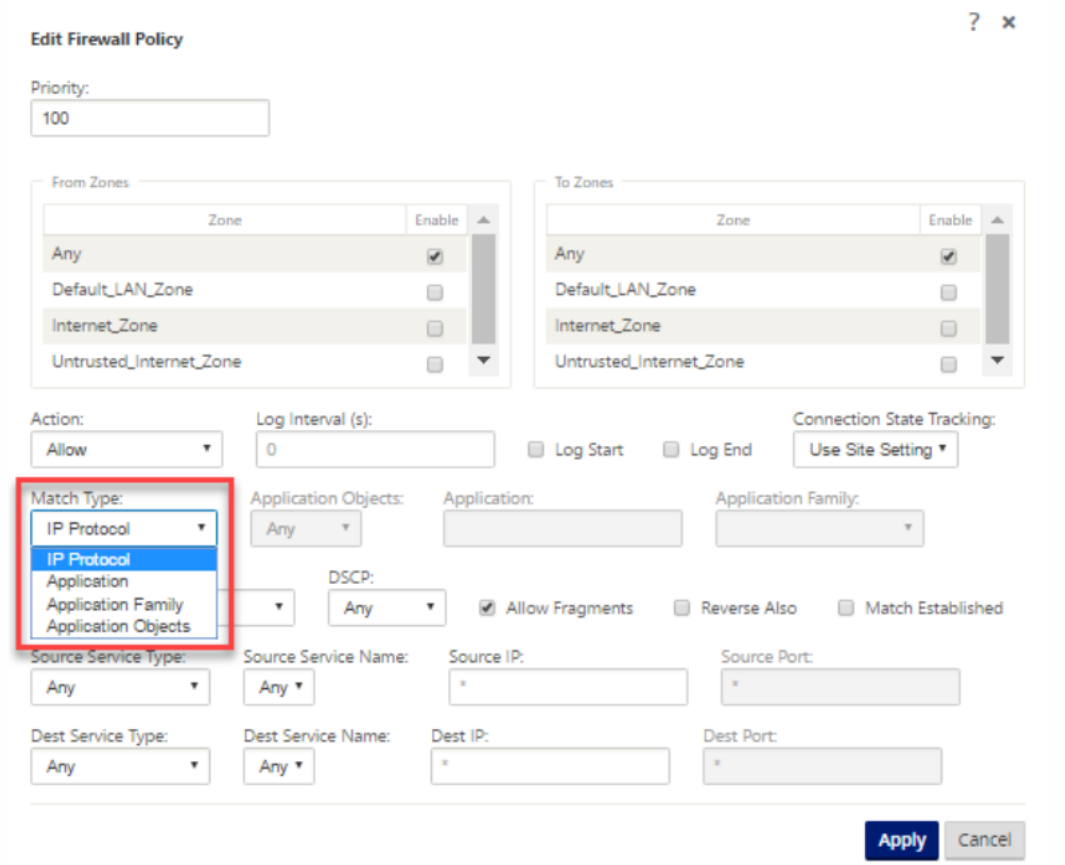
1. In the Configuration Editor, click **Global** > **Applications** > **Application Objects**.
2. Click **Add** and, in the **Name** field, enter a name for the object.



3. Select **Enable Reporting** to enable viewing custom application reports in Citrix SD-WAN Center. For more information see, Application Report.
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 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, application families or domain names enables you to use the application, application families, and application objects as match types to filter traffic and apply firewall policy and rules. It applies for all Pre, Post, and local policies. For more information about firewall, see Stateful Firewall and NAT Support.



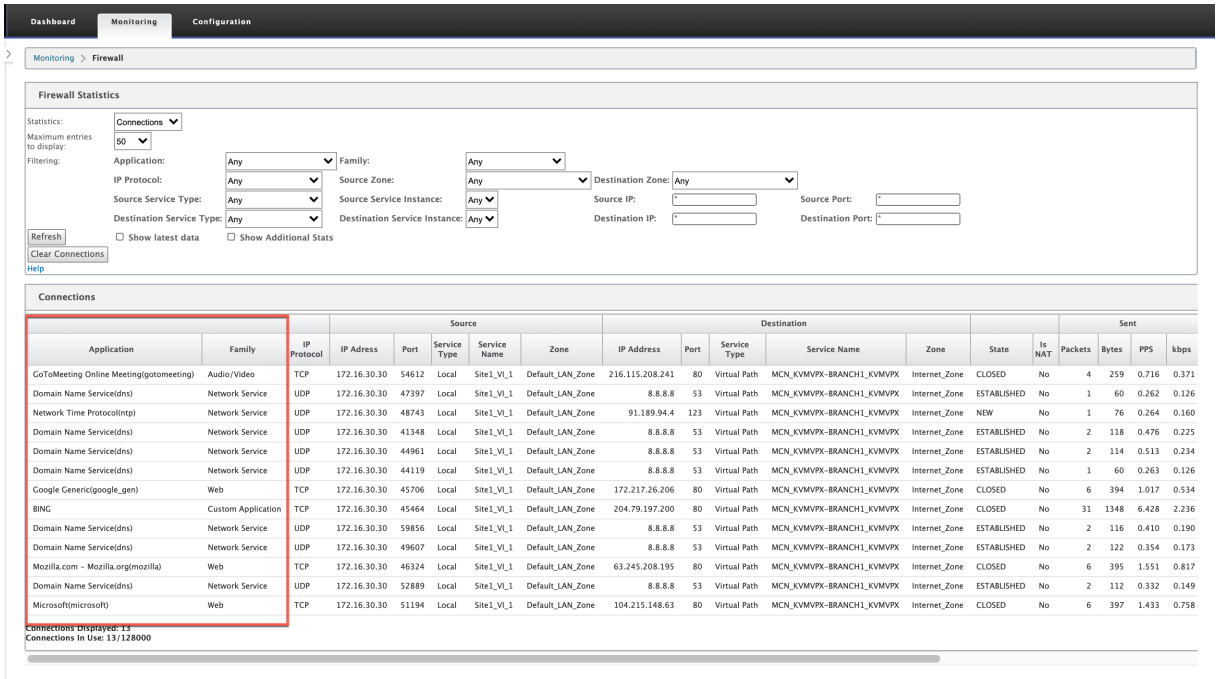
Viewing Application Classification

After enabling application classification, you can view the application name and application family details in the following reports:

- Firewall connection Statistics
- Flows information
- Application statistics

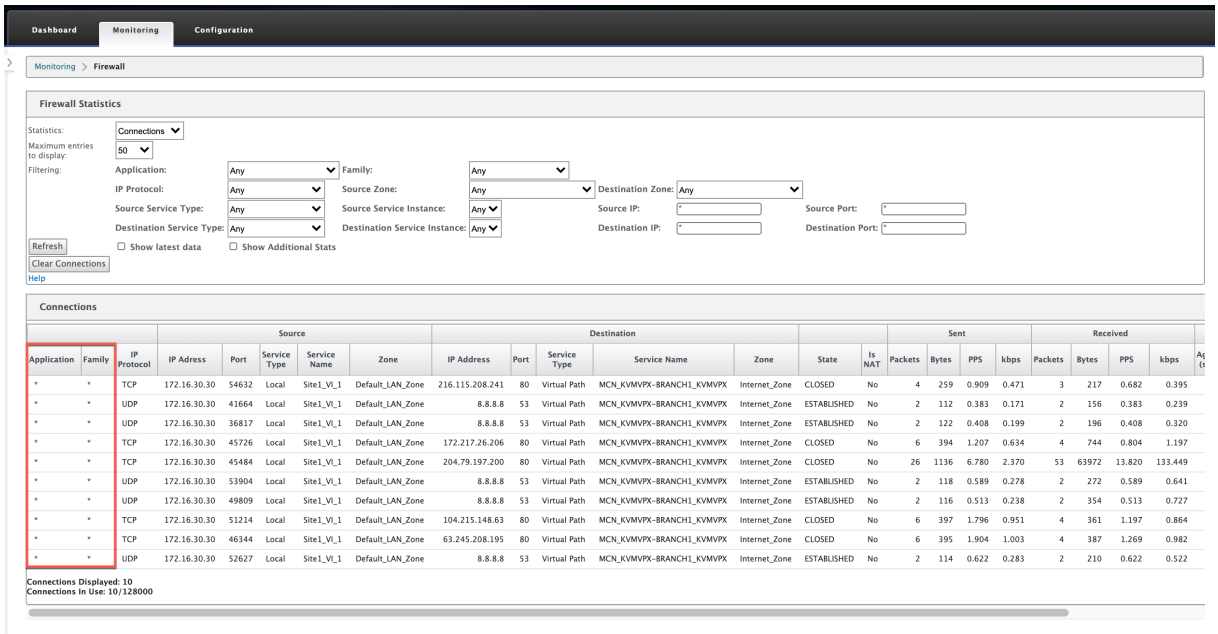
Firewall connection statistics

In the **Configuration Editor**, navigate to **Monitoring > Firewall**. Under **Connections** section, the **Application** and **Family** columns list the applications and its associated family.



Application	Family	IP Protocol	Source IP Adress	Source Port	Source Service Type	Source Service Name	Source Zone	Destination IP Address	Destination Port	Destination Service Type	Destination Service Name	Destination Zone	State	Is NAT	Sent Packets	Sent Bytes	Sent PPS	Sent kbps
GoToMeeting Online Meeting(gotomeeting)	Audio/Video	TCP	172.16.30.30	54612	Local	Site1_VI_1	Default_LAN_Zone	216.115.208.241	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	4	259	0.716	0.371
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	47397	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	1	60	0.262	0.126
Network Time Protocol(ntp)	Network Service	UDP	172.16.30.30	48743	Local	Site1_VI_1	Default_LAN_Zone	91.189.94.4	123	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	NEW	No	1	76	0.264	0.160
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	41348	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	118	0.476	0.225
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	44961	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	114	0.513	0.234
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	44119	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	1	60	0.263	0.126
Google Generic(google_gen)	Web	TCP	172.16.30.30	45706	Local	Site1_VI_1	Default_LAN_Zone	172.217.26.206	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	6	394	1.017	0.534
BING	Custom Application	TCP	172.16.30.30	45464	Local	Site1_VI_1	Default_LAN_Zone	204.79.197.200	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	31	1348	6.428	2.236
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	59856	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	116	0.410	0.190
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	49607	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	122	0.354	0.173
Mozilla.com – Mozilla.org(mozilla)	Web	TCP	172.16.30.30	46324	Local	Site1_VI_1	Default_LAN_Zone	63.245.208.195	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	6	395	1.551	0.817
Domain Name Service(dns)	Network Service	UDP	172.16.30.30	52889	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	112	0.332	0.149
Microsoft(microsoft)	Web	TCP	172.16.30.30	51194	Local	Site1_VI_1	Default_LAN_Zone	104.215.148.63	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	6	397	1.433	0.758

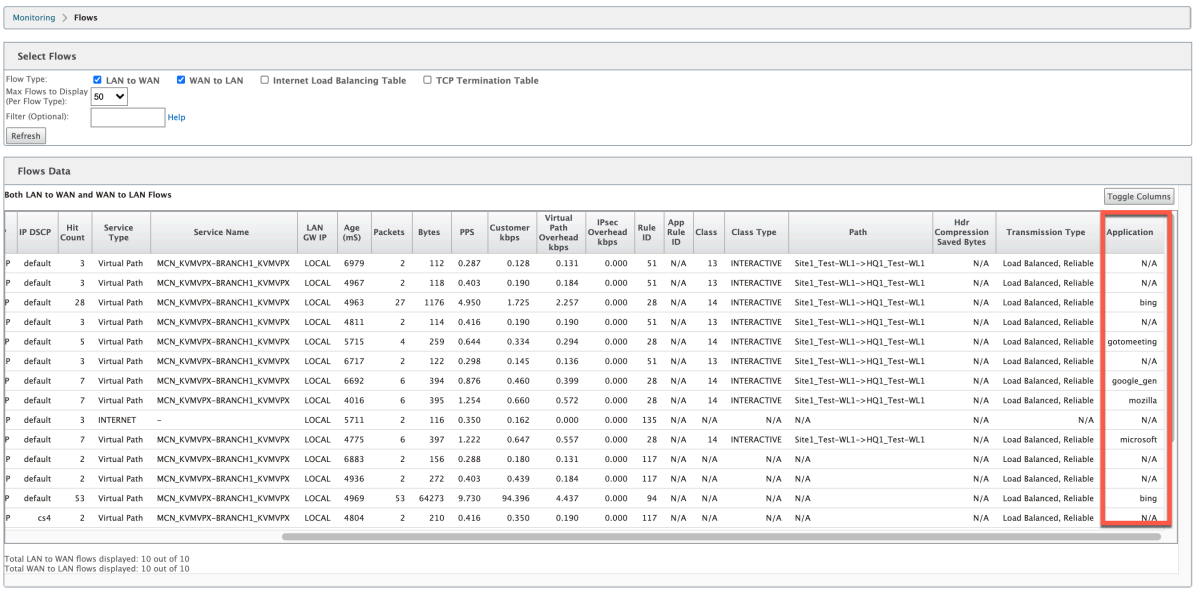
If you do not enable application classification, the **Application** and **Family** columns do not show any data.



Application	Family	IP Protocol	Source IP Adress	Source Port	Source Service Type	Source Service Name	Source Zone	Destination IP Address	Destination Port	Destination Service Type	Destination Service Name	Destination Zone	State	Is NAT	Sent Packets	Sent Bytes	Sent PPS	Sent kbps	Received Packets	Received Bytes	Received PPS	Received kbps
*	*	TCP	172.16.30.30	54632	Local	Site1_VI_1	Default_LAN_Zone	216.115.208.241	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	4	259	0.909	0.471	3	217	0.682	0.395
*	*	UDP	172.16.30.30	41664	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	112	0.383	0.171	2	156	0.383	0.239
*	*	UDP	172.16.30.30	36817	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	122	0.408	0.199	2	196	0.408	0.320
*	*	TCP	172.16.30.30	45726	Local	Site1_VI_1	Default_LAN_Zone	172.217.26.206	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	6	394	1.207	0.634	4	744	0.804	1.197
*	*	TCP	172.16.30.30	45484	Local	Site1_VI_1	Default_LAN_Zone	204.79.197.200	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	26	1136	6.780	2.370	53	63972	13.820	133.449
*	*	UDP	172.16.30.30	53904	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	118	0.589	0.278	2	272	0.589	0.641
*	*	UDP	172.16.30.30	49809	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	116	0.513	0.238	2	354	0.513	0.727
*	*	TCP	172.16.30.30	51214	Local	Site1_VI_1	Default_LAN_Zone	104.215.148.63	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	6	397	1.796	0.951	4	361	1.197	0.864
*	*	TCP	172.16.30.30	46344	Local	Site1_VI_1	Default_LAN_Zone	63.245.208.195	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	6	395	1.904	1.003	4	387	1.269	0.982
*	*	UDP	172.16.30.30	52627	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	114	0.622	0.283	2	210	0.622	0.522

Flows Information

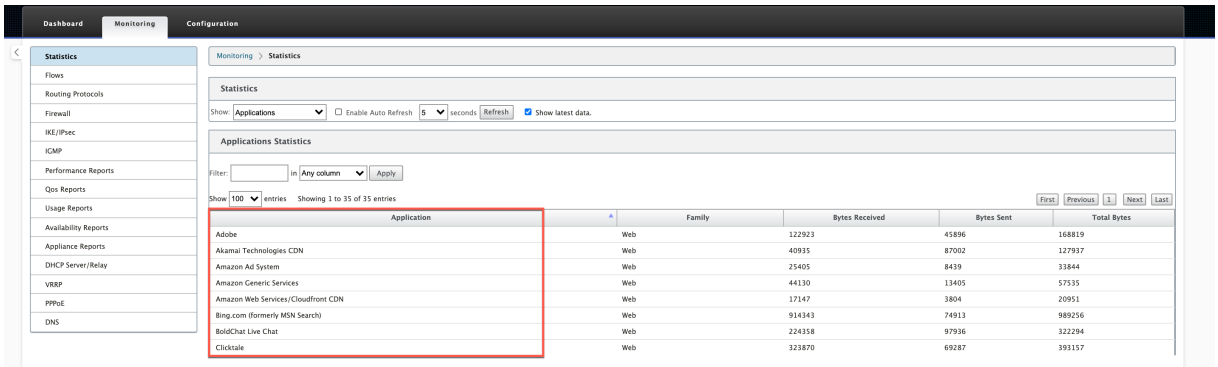
In the **Configuration Editor**, navigate to **Monitoring > Flows**. Under **Flows Data** section, the **Application** column lists the application details.



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

Application statistics

In the **Configuration Editor**, navigate to **Monitoring > Statistics**. Under **Application Statistics** section, the **Application** column lists the application details.



Troubleshooting

After enabling application classification, you can view the reports under the **Monitoring** section and ensure that they show application details. For more information, see Viewing Application Classification.

If there is any unexpected behavior, collect the STS diagnostics bundle while the issue is being observed, and share it with the Citrix Support team.

The STS bundle can be created and downloaded using **Configuration > System Maintenance > Diagnostics > Diagnostic Information**.

QoS fairness (RED)

March 12, 2021

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 enable 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, Citrix 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 allows 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 800 ms 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.

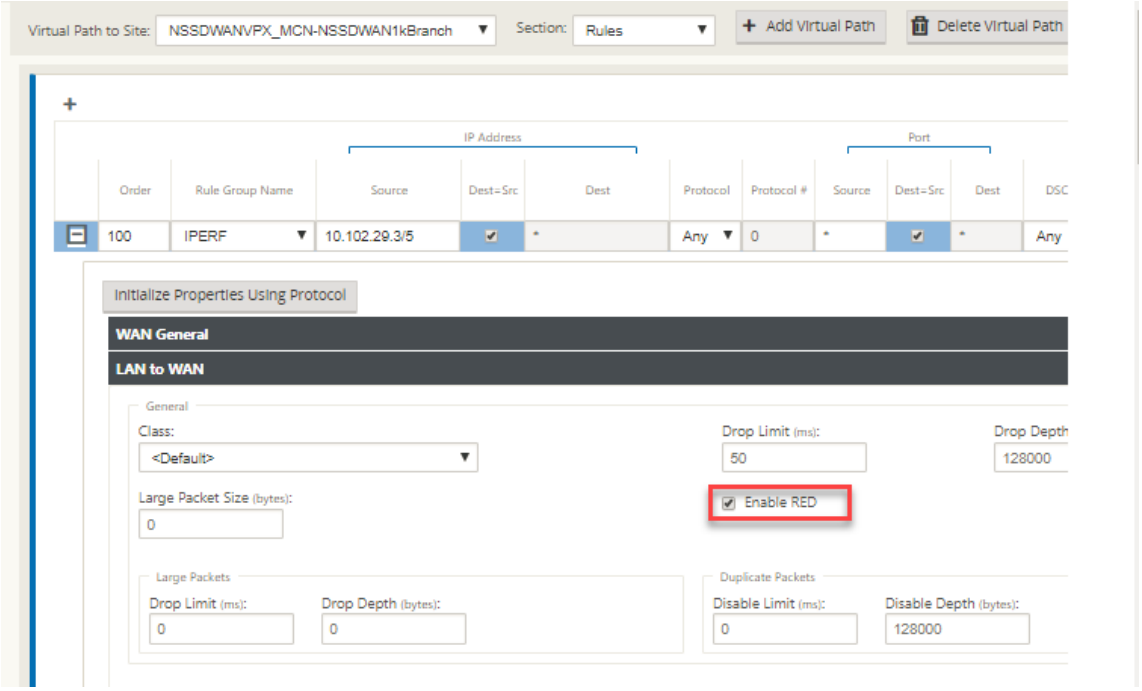
How to use RED

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 both the 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.



MPLS queues

March 12, 2021

This feature simplifies creating SD-WAN configurations when adding a Multiprotocol Layer 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 (that is, Access Type) is available. When a new Private MPLS Access Type is selected, you can define the 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 the 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, contact Citrix Support for assistance.

Configure 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 WAN Link 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 the DSCP tags match.

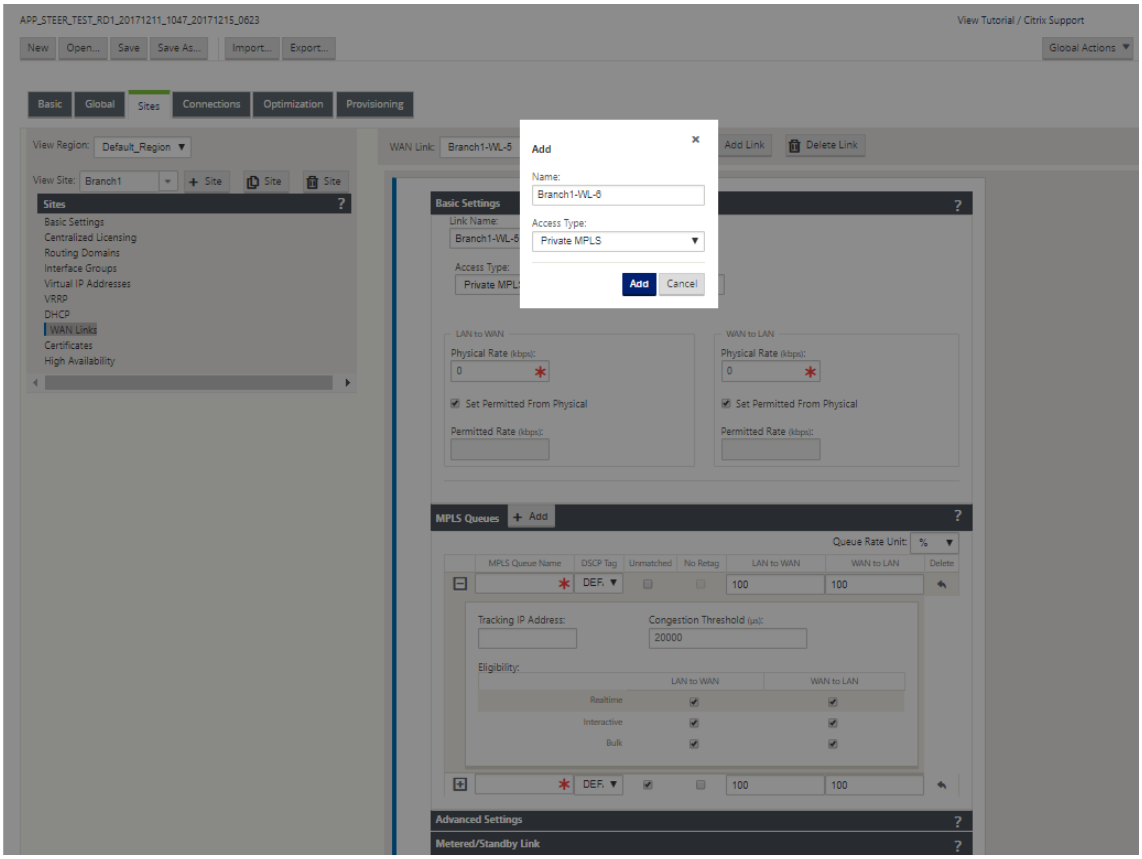
5. Ensure that the same Autopath Group is configured at the MCN and Client.
6. Verify that the Paths for the WAN Link are built automatically.
7. Assign Intranet Service to a specific queue, if needed.

> **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 a 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 the defined tags within the configuration file are mapped to this queue and the bandwidth defined for this queue.
LAN to WAN Permitted Rate (kbps)	The amount of bandwidth that SD-WAN devices are permitted to use for upload, which cannot exceed the defined physical upload rate of the WAN Link.

Field	Description
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 more 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 throttles packet transmission to avoid more 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.

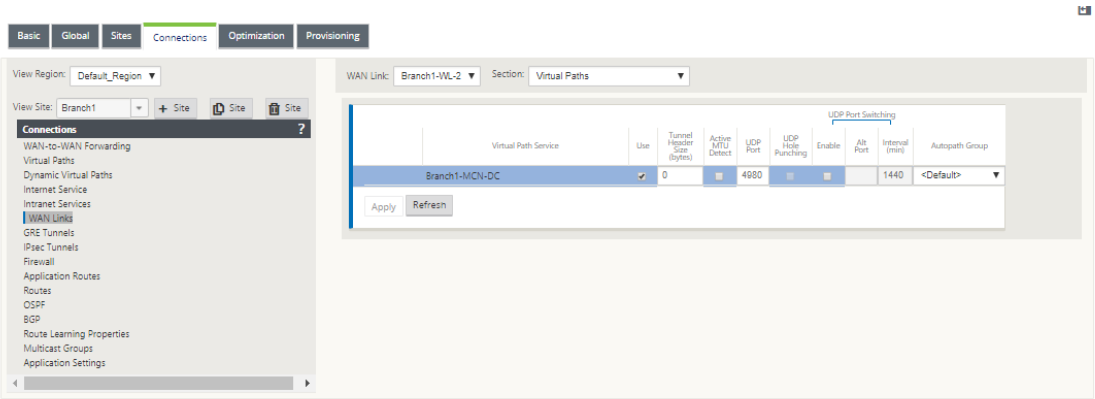
Define WAN Link properties for private MPLS

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 can 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 the 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 automatically generates 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 is in 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 help with troubleshooting.

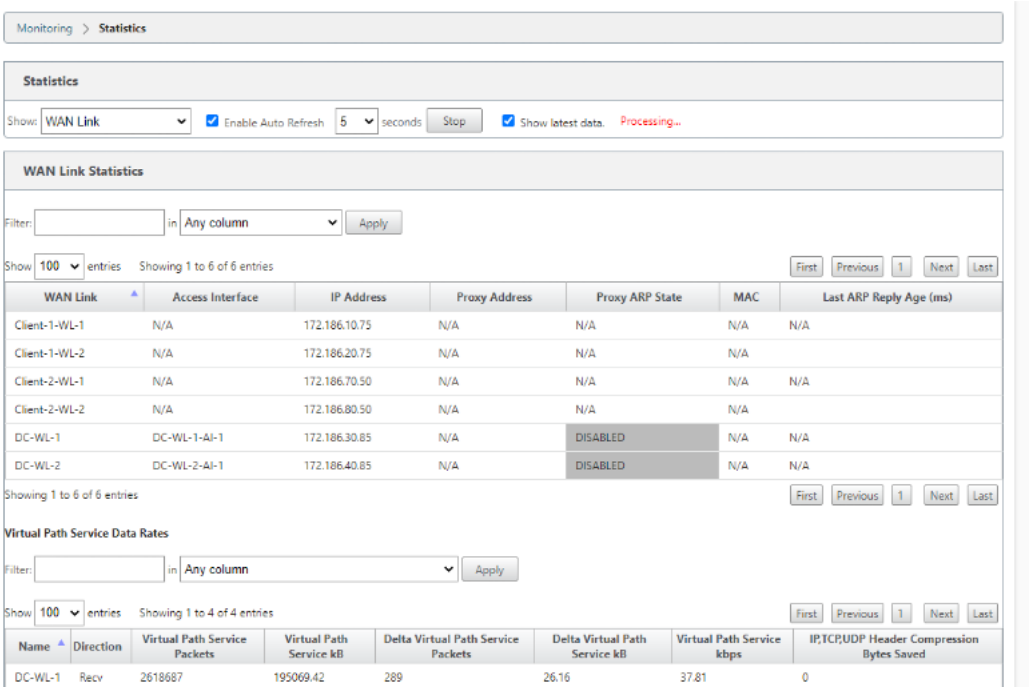
View permitted rate

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

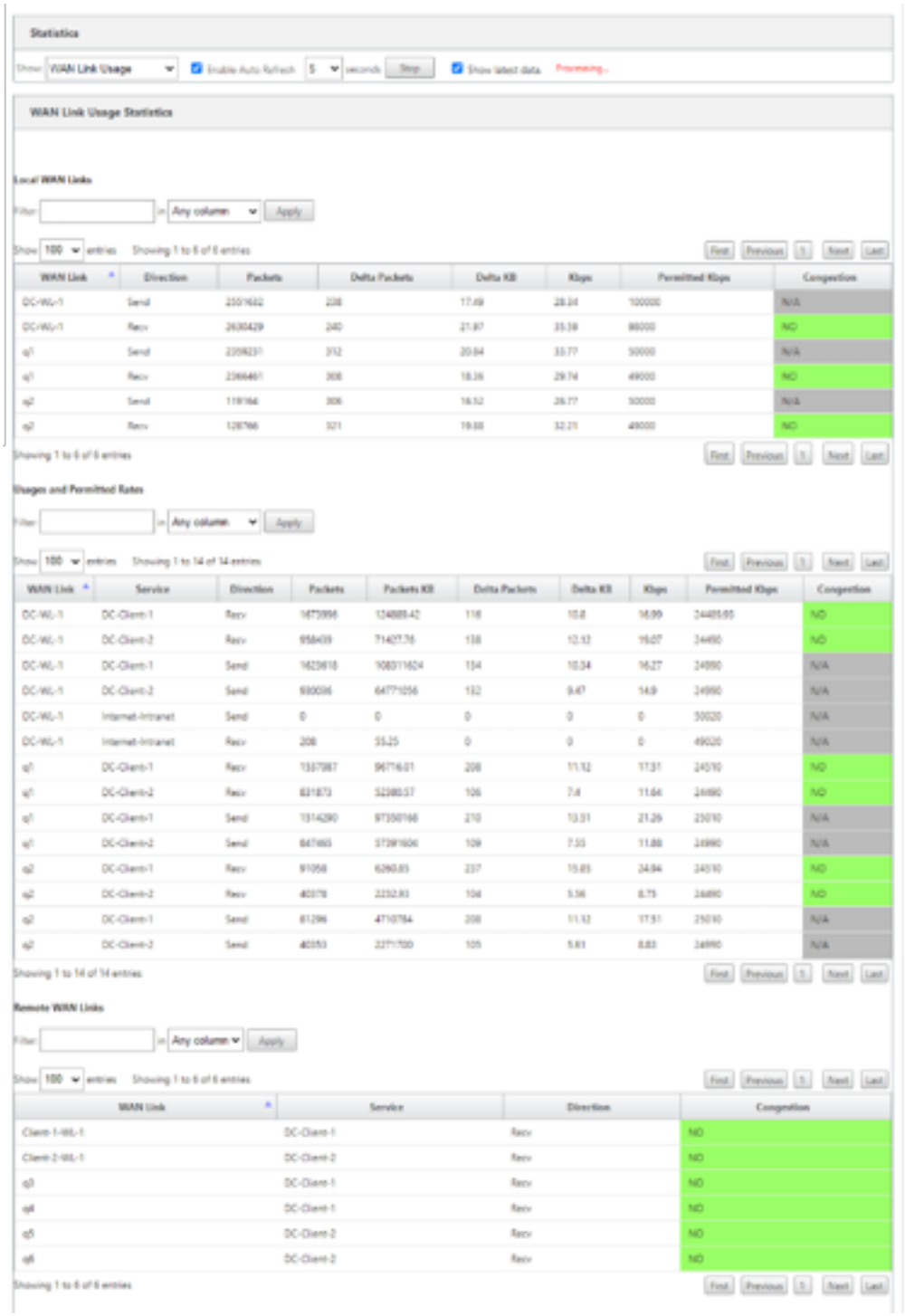
Path Service, Intranet Service, or Internet Service will fluctuate over time, in response to congestion, user demand, and Fair Shares, but will always be greater than or equal to the Minimum Reserved Bandwidth for the Service.

Monitor WAN link

Go to **Monitor** > **Statistics**, and select **WAN Link** from the **Show** drop-down list.

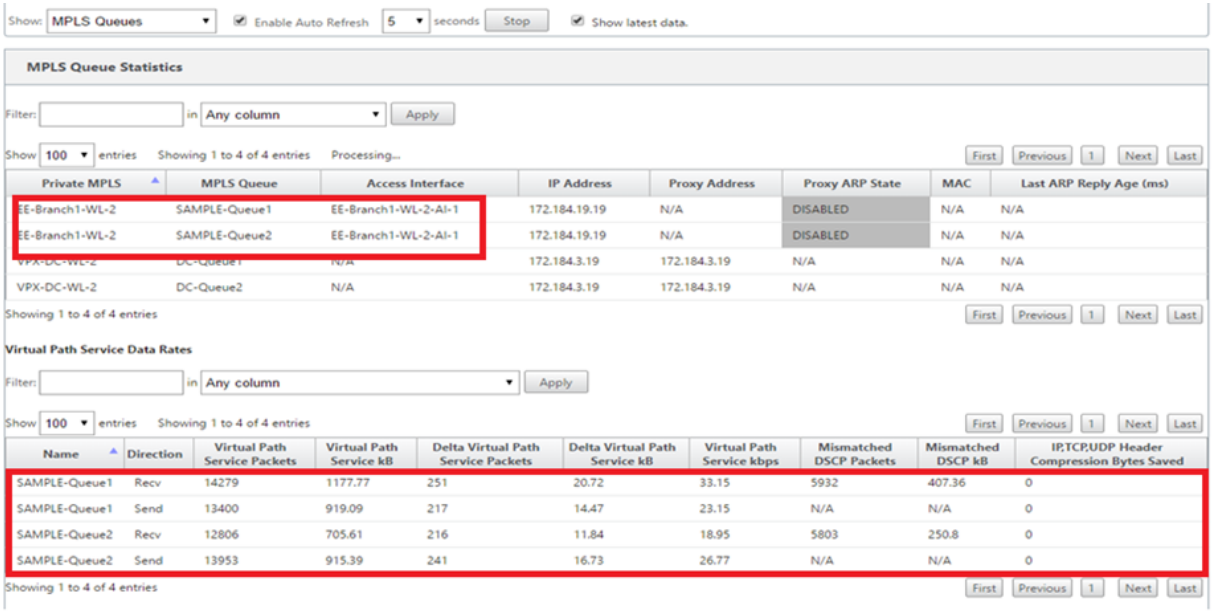


Go to **Monitor > Statistics**, and select **WAN Link Usage** from the **Show** drop-down list.



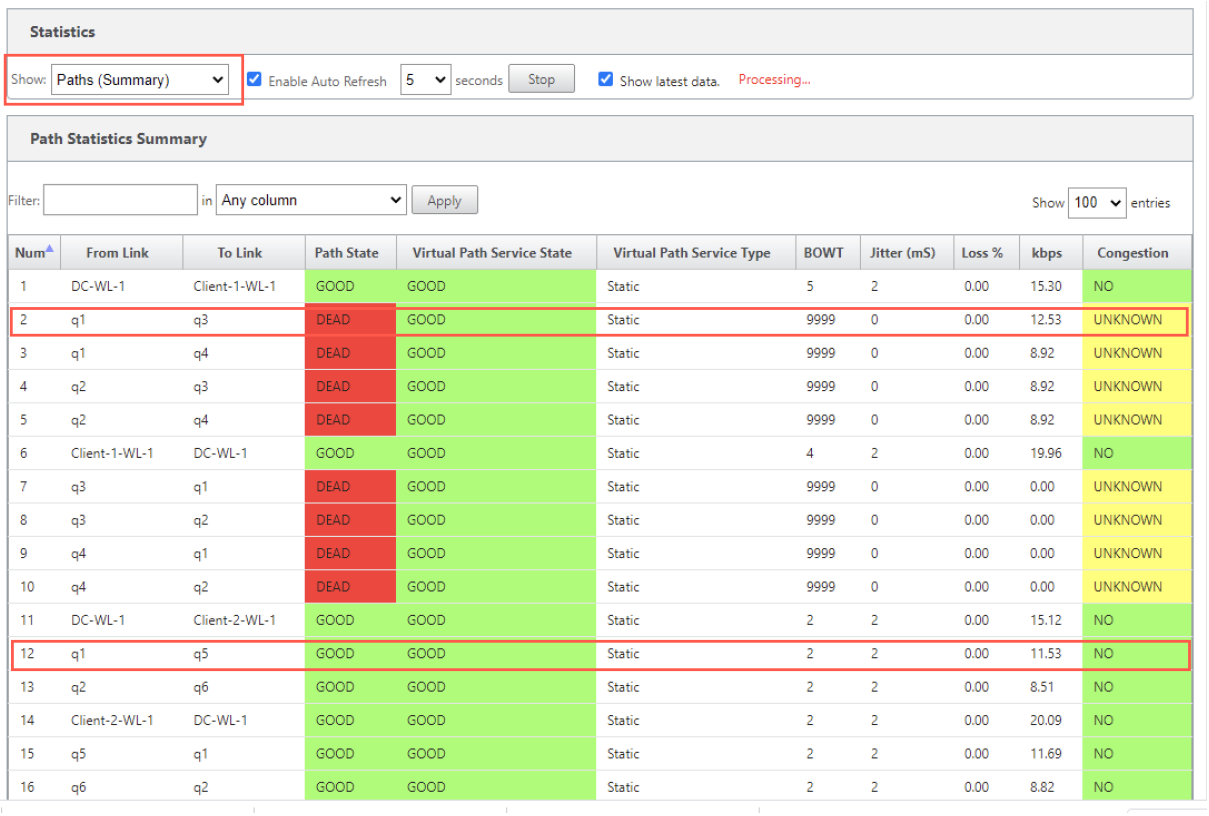
Monitor MPLS queues

Go to **Monitor** > **Statistics**, and select **MPLS Queues** from the **Show** drop-down list.



Troubleshooting MPLS queues

To check the status of MPLS queues, navigate to **Monitor > Statistics** and select **Paths (summary)** from the **Show** drop-down list. In the following example, the path from MPLS queue “q1”to “q3”is in DEAD state and shown in red. The path from MPLS queue “q1”to “q5”is in GOOD state and shown in green.



Num	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	DC-WL-1	Client-1-WL-1	GOOD	GOOD	Static	5	2	0.00	15.30	NO
2	q1	q3	DEAD	GOOD	Static	9999	0	0.00	12.53	UNKNOWN
3	q1	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
4	q2	q3	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
5	q2	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
6	Client-1-WL-1	DC-WL-1	GOOD	GOOD	Static	4	2	0.00	19.96	NO
7	q3	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
8	q3	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
9	q4	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
10	q4	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
11	DC-WL-1	Client-2-WL-1	GOOD	GOOD	Static	2	2	0.00	15.12	NO
12	q1	q5	GOOD	GOOD	Static	2	2	0.00	11.53	NO
13	q2	q6	GOOD	GOOD	Static	2	2	0.00	8.51	NO
14	Client-2-WL-1	DC-WL-1	GOOD	GOOD	Static	2	2	0.00	20.09	NO
15	q5	q1	GOOD	GOOD	Static	2	2	0.00	11.69	NO
16	q6	q2	GOOD	GOOD	Static	2	2	0.00	8.82	NO

For detailed information on paths, select **Paths (Detailed)** from the **Show** drop-down list. The information on paths such as reason for the state, duration, source port, destination port, MTU are available

In the following example, the path from MPLS queue “q1”to “q3”is in DEAD state and the reason is PEER. The path from MPLS queue “q3”to “q1”is dead and the reason is SILENCE. The following table provides the list if available reasons and its descriptions.

Reason	Description
GATEWAY	The path is DEAD as the appliance cannot reach or detect the gateway
SILENCE	The path is BAD or DEAD because the appliance has not received packets from the peer site
LOSS	The path is BAD due to packet loss
PEER	The peer site is reporting the path is BAD

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

Path Statistics Advanced

Filter: in Any column Apply

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

Num	From Link	To Link	Congestion	Path State	Reason	Duration (S)	Virtual Path Service State	Src Port	Dst Port	MTU	BOWT	Jitter (mS)	Packets Received	OOO	Loss %	kbps	Virtual Path Service Type
1	DC-WL-1	Client-1-WL-1	NO	GOOD	N/A	386	GOOD	4980	4980	1488	5	2	116	0	0.00	13.79	Static
2	q1	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	108	0	0.00	12.75	Static
3	q1	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
4	q2	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
5	q2	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
6	Client-1-WL-1	DC-WL-1	NO	GOOD	N/A	21325	GOOD	4980	4980	N/A	4	2	126	0	0.00	17.45	Static
7	q3	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
8	q3	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
9	q4	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
10	q4	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
11	DC-WL-1	Client-2-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	130	0	0.00	14.41	Static
12	q1	q5	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	111	0	0.00	11.69	Static
13	q2	q6	NO	GOOD	N/A	234	GOOD	4980	4980	1488	2	2	107	0	0.00	8.72	Static
14	Client-2-WL-1	DC-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	142	0	0.00	19.40	Static
15	q5	q1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	110	0	0.00	11.27	Static
16	q6	q2	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	107	0	0.00	8.50	Static

To check the access interface and IP address associated with the MPLS queues, select **Access Interfaces** from the **Show** drop-down list.

Show: Access Interfaces | Enable Auto Refresh 5 seconds Stop | Show latest data. Processing...

Access Interface Statistics

Filter: in Any column Apply

Show 100 entries Showing 1 to 3 of 3 entries First Previous 1 Next Last

WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
DC-WL-1	DC-WL-1-AI-1	172.186.30.85	N/A	N/A	N/A	N/A
q1	DC-WL-2-AI-1	172.186.40.85	N/A	N/A	N/A	N/A
q2	DC-WL-2-AI-1	172.186.40.85	N/A	N/A	N/A	N/A

Showing 1 to 3 of 3 entries First Previous 1 Next Last

Virtual Path Service Data Rates:

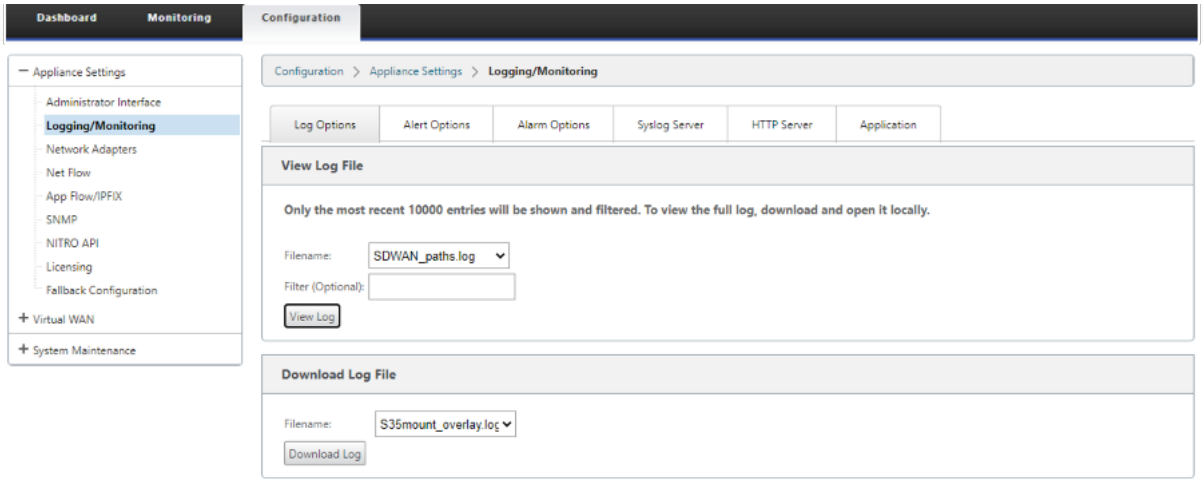
Filter: in Any column Apply

Show 100 entries Showing 1 to 12 of 12 entries First Previous 1 Next Last

WAN Link	Access Interface	Service Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Virtual Path Service kbps	IP,TCP,UDP Header Compression Bytes Saved
DC-WL-1	DC-WL-1-AI-1	DC-Client-2	Recv	953815	71018.84	147	13.04	21.11	0
DC-WL-1	DC-WL-1-AI-1	DC-Client-1	Recv	1670099	124524.23	112	10.56	17.1	0
DC-WL-1	DC-WL-1-AI-1	DC-Client-2	Send	925756	62940.27	137	10.22	16.55	0
DC-WL-1	DC-WL-1-AI-1	DC-Client-1	Send	1619424	105451.88	141	11.16	18.07	0
q1	DC-WL-2-AI-1	DC-Client-1	Recv	1530107	96340.46	202	10.82	17.52	0
q1	DC-WL-2-AI-1	DC-Client-2	Recv	828314	52130.2	103	7.21	11.68	0
q1	DC-WL-2-AI-1	DC-Client-1	Send	1507265	94613.25	205	13.25	21.46	0
q1	DC-WL-2-AI-1	DC-Client-2	Send	843865	55794.07	104	7.3	11.81	0

You can download the log files for further troubleshooting. Navigate to **Configuration > Logging/-**

Monitoring and select **SDWAN_paths.log** or **SDWAN_common.log** from the **Log Options** tab.



Reporting

March 12, 2021

Application QoE

Multiple Net Flow Collectors

Application QoE

March 12, 2021

Application QoE is a measure of Quality of Experience of applications in the SD-WAN network. It measures the quality of applications that flow through the virtual paths between two SD-WAN appliances. The **Application QoE** score is a value between 0 and 10. The score range that it falls in determines the quality of an application.

Quality	Range
Good	8–10
Fair	4–8
Poor	0–4

Application QoE score can be used to measure quality of applications and identify problematic trends.

You can define the quality thresholds for real-time and interactive appliances using QoE profiles, and map these profiles to applications or applications objects.

> **Note**:
>
> To monitor Application QoE, it is essential to enable Deep Packet Inspection. For more information, see Application classification

Real-time application QoE

The Application QoE calculation for real-time applications uses a Citrix innovative technique, which is derived from MOS score.

The default threshold values are:

- Latency threshold: 160 ms
- Jitter Threshold: 30 ms
- Packet loss threshold: 2%

A flow of a real-time application that meets the thresholds for latency, loss, and jitter is considered to be of good quality.

QoE for Real-time applications is determined from the percentage of flows that meet the threshold divided by the total number of flow samples.

QoE for Real-time = (No of flow samples that meet the threshold / Total no of flow samples) * 100

It is represented as QoE score ranging from 0 to 10.

You can create QoE profiles with custom threshold values and apply to applications or application objects.

> **Note**:
>
> The QoE value can be zero if the network conditions are outside of the configured thresholds for real-time traffic.

Interactive application QoE

The Application QoE for interactive applications uses a Citrix innovative technique based on packet loss and burst rate thresholds.

Interactive applications are sensitive to packet loss and throughput. Therefore, we measure the packet loss percentage, and the burst rate of ingress and egress traffic in a flow.

The configurable thresholds are:

- Packet loss percentage.
- Percentage of expected egress burst rate in comparison to the ingress burst rate.

The default threshold values are:

- Packet loss threshold: 1%
- Burst rate: 60%

A flow is of good quality if the following conditions are met:

- The percentage loss for a flow is less that the configured threshold.
- The egress burst rate is at least the configured percentage of ingress burst rate.

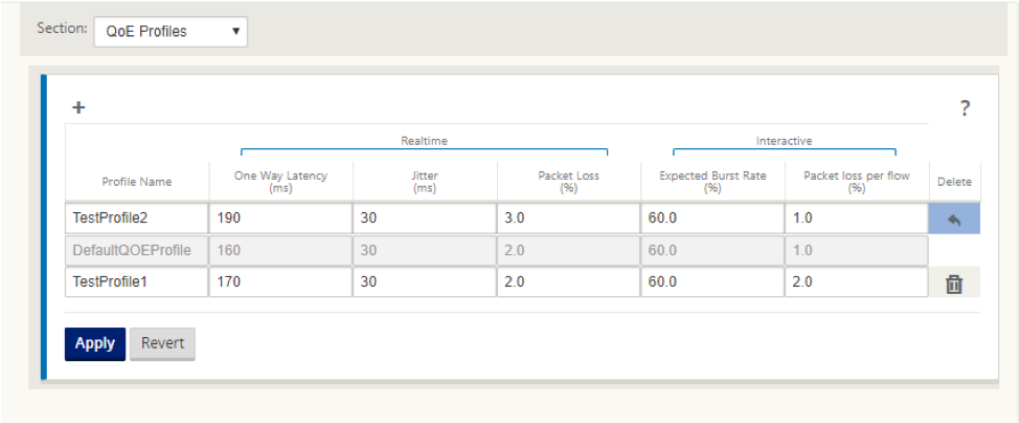
Configuring application QoE

Map application or application objects to default or custom QoE profiles.
You can create custom QoE profiles for real-time and interactive traffic.

To create custom QoE profiles:

1. In the Configuration Editor, navigate to **Global > Application QoE > QoE Profiles** and click **+**.
2. Enter value for the following parameters:
    - **Profile Name**: A name to identify the profile that sets thresholds for real-time and interactive traffic.
    - **Real-time**: Configure thresholds for traffic flows that hit the real-time QoS policy. A flow of a real-time application that meets that below thresholds for latency, loss, and jitter is considered to be of good quality.
        - **One Way latency**: The latency threshold in milliseconds. The default QoE profile value is 160 ms.
        - **Jitter**: The jitter threshold in milliseconds. The default QoE profile value is 30 ms.
        - **Packet Loss**: The percentage of packet loss. The default QoE profile value is 2%.
    - **Interactive**: Configure thresholds for traffic flows that hit the interactive QoS policy. A flow of an interactive application that meets that below threshold for burst ratio and packet loss is considered to be of good quality.
        - **Expected Burst Rate**: The percentage of expected burst rate. The egress burst rate should be at least the configured percentage of ingress burst rate. The default QoE profile value is 60%.

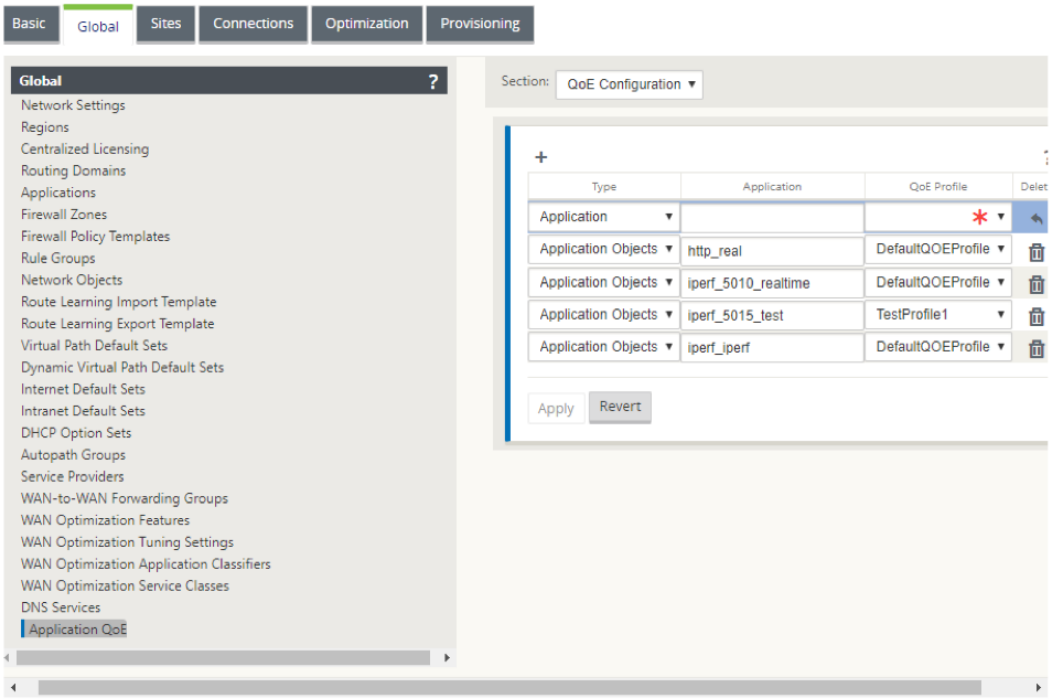
– **Packet loss per flow**: The percentage of packet loss. The default QoE profile value is 1%.



3. Click **Apply**.

To map applications or application objects with QoE profiles:

1. In the Configuration Editor, navigate to **Global > Application QoE > QoE Configuration** and click **+**.
2. Select values for the following parameters:
   - **Type**: A DPI application or an application object.
   - **Application**: Search and select an application or application object based on the selected Type.
   - **QoE Profile**: Select a QoE profile to map to the application or application object.



3. Click **Apply**.

You can map up to 10 applications or application objects with QoE profiles. You can view the Application QoE reports on SD-WAN Center. For more information see, the Application QOE report report.

HDX QoE

March 12, 2021

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, are measured between the two SD-WAN appliances located at the client and server side and not measured between the client or the server appliances themselves. Latency, jitter, and packet drop are measured at the flow level and it can be different from the statistics at the link level. The end host (client or server) application might 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 might increase latency and jitter a bit.

Default configuration for HDX traffic enables SD-WAN to retransmit 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 Citrix 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 Citrix SD-WAN Center. For more information see, 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 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 might 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 can 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 can take up to 2 minutes to show as closed in ICA_Summary.*
> - *QoE of TCP sessions and UDP sessions might not be the same on the same path due to the*

> *inherent different between TCP and UDP.*
> - *If one user launches two virtual desktops, the number of users is countered as two.*

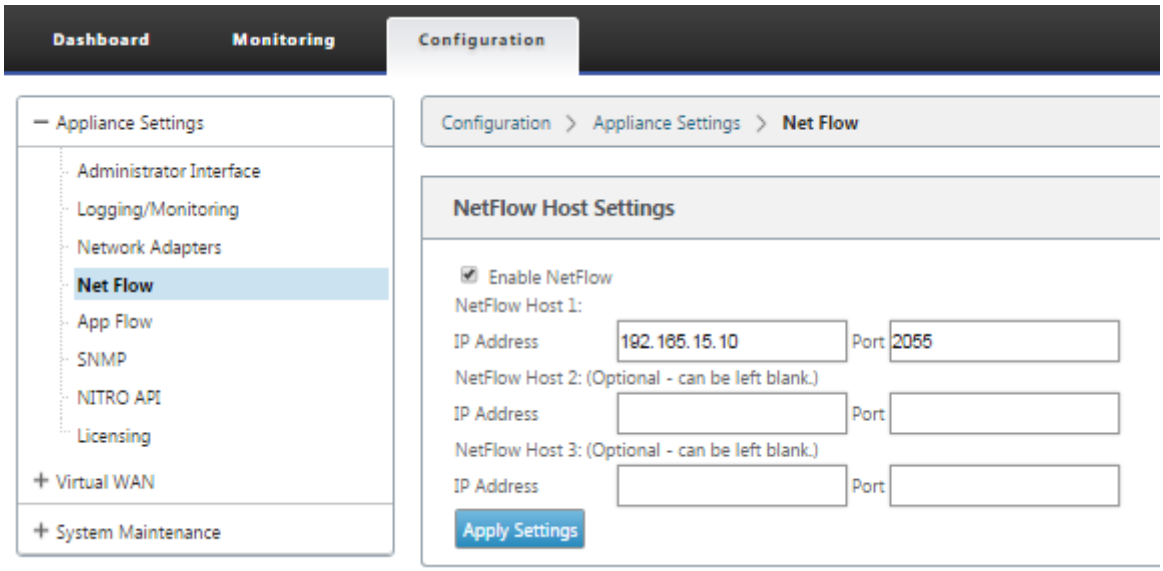
Multiple Net Flow Collectors

August 31, 2021

Net Flow Collectors 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 Net Flow version 5 statistical data to the configured Net Flow collector. Citrix SD-WAN provides Net Flow support for traffic flows that are obscured by the transport reliable protocol. Devices on the WAN edge of the solution lose capability to collect Net Flow records since only the SD-WAN encapsulated UDP packets are displayed. Net Flow is supported on the Citrix SD-WAN Standard and Premium (Enterprise) Edition appliances.

To configure Net Flow Hosts:

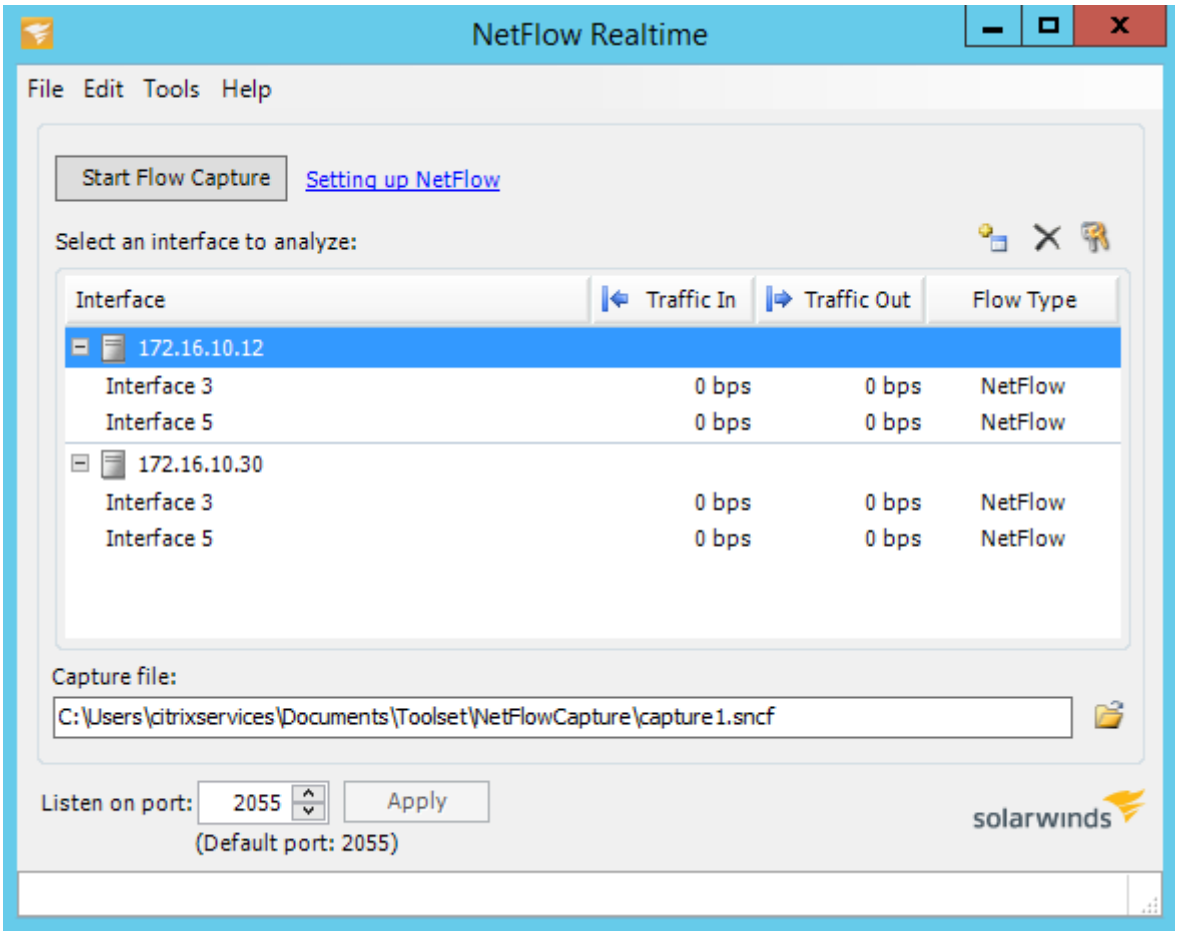
Navigate to **Configuration > Appliance Settings > Net Flow > Netflow Host Settings** page. Click the **Enable NetFlow checkbox**, and enter the **IP Address**, and **Port** numbers for up to three Net flow Hosts, then click **Apply Settings to** save the changes.

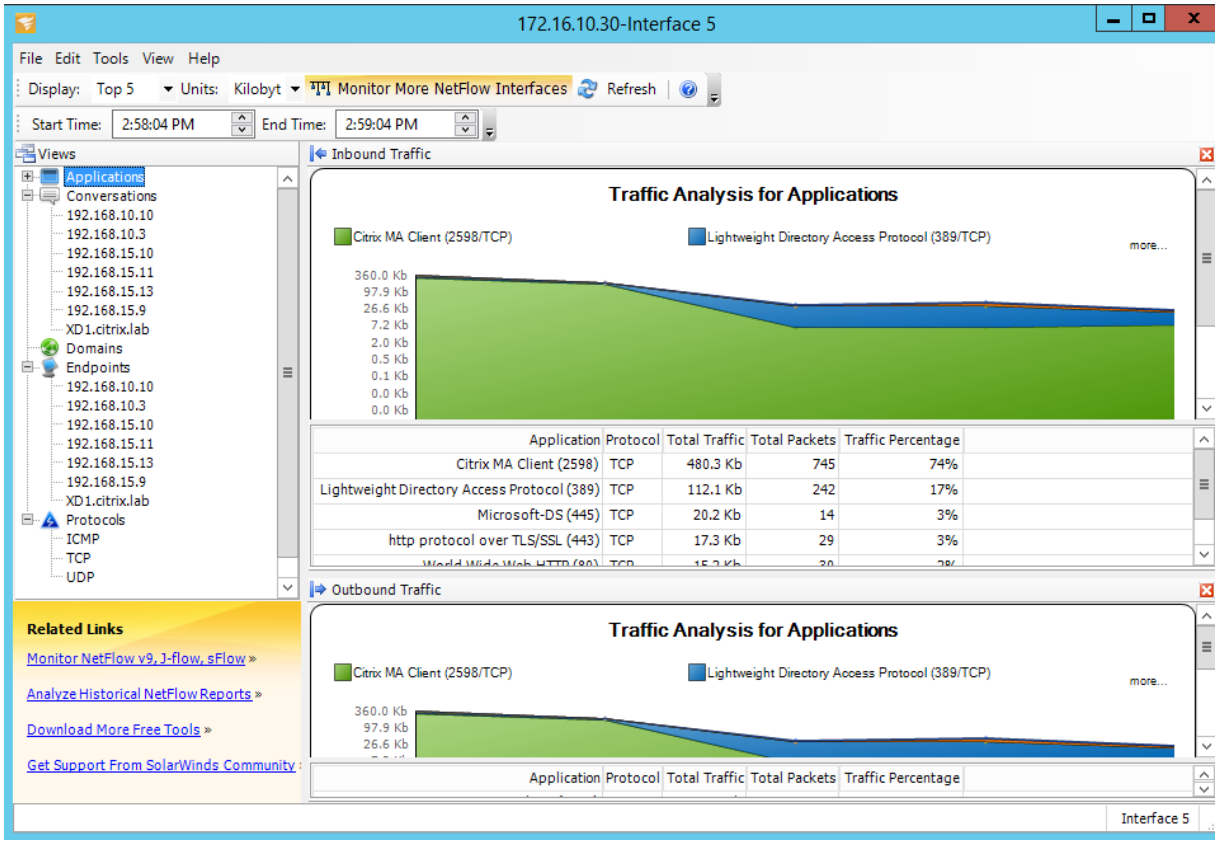


NetFlow Export

Net Flow data is exported from the management port of the SD-WAN device. On your Net Flow collector tool, the SD-WAN devices are listed as the configured management IP address, if SNMP is not

configured. The interfaces are listed as one for incoming and a second for outgoing (Virtual Path traffic).





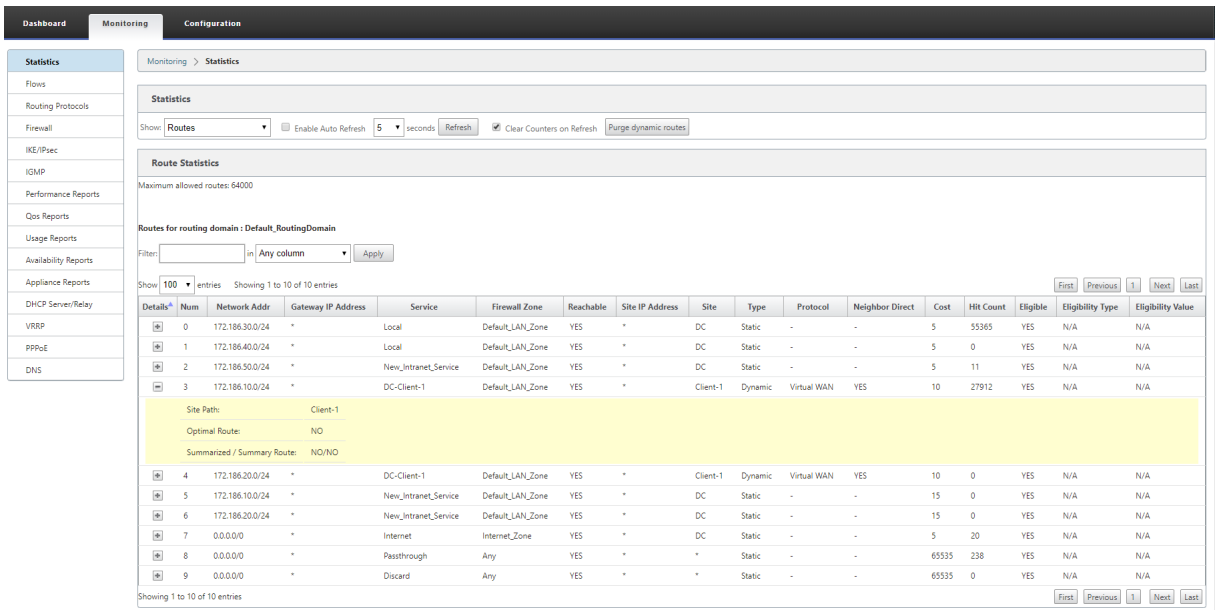
NetFlow Limitations

- With Netflow enabled on SD-WAN Standard and Premium 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 round trip time (RTT), latency, jitter, and other performance metrics in the flow data is not possible. From the security side, without TCP flags, the Net Flow collector cannot determine if there are FIN, ACK/RST, or SYN scans occurring.

Route statistics

March 12, 2021

To view route statistics of your SD-WAN appliances, in the SD-WAN GUI navigate to **Monitoring** > **Statistics** > **Routes**.



You can view the following parameters:

- **Network Address**: The Network address and subnet mask of the route.
- **Details**: Click + to display the following information.
  - **Site Path**: Site Path is a source of truth metric for the received prefix. It is used in situations where WAN to WAN forwarding is enabled on multiple devices and in mesh deployment. Multiple such prefixes are received and the administrators are able to judge the prefix attributes by viewing the site path.

    For example, consider a simple topology of Branch1, Branch2, and MCN along with a Geo MCN. Branch1 has a prefix 172.16.1.0/24 and has to get to Branch2. Geo MCN and MCN have WAN to WAN forwarding enabled.

    The prefix 172.16.1.0/24 can get to Branch2 via Branch1-MCN-Branch2, Branch1-Geo-Branch2, and Branch1-MCN-Geo-Branch2. For each of these distinct prefixes the routing table is updated with their site path metric. The site path metric indicates the origin of the route prefix and the cost involved to get to Branch2.
  - **Optimal Route**: Optimal route indicates whether the route is the optimal route to reach that subnet compared to all other routes. This optimal route is exported to other sites.
  - **Summarized/ Summary Route**: A summary route is a route configured explicitly by an administrator to summarize multiple prefixes that fall in the supernet. Summarized routes are the prefixes that fall under the summary route.

For example, assume that we have a summary route 172.16.0.0/16. This is a summary route only and not a summarized route. A summary route has Summary 'YES'and Summarized 'NO'. If there are few other subnets like 172.16.1.0/24, 172.16.2.0/24 and 172.16.3.0/24, these three routes fall under the summary route or the supernet and hence are called summarized routes. A summarized route has Summarized 'YES'and Summary 'NO'.

- **Gateway IP Address**: The IP address of the gateway/route used to reach this route.
- **Service**: The type of Citrix SD-WAN service.
- **Firewall Zone**: The firewall zone used by the route.
- **Reachable**: Is the route reachable or not.
- **Site IP Address**: The IP address of the site.
- **Site**: The name of the site.
- **Type**: Type of a route depends upon the source of the route learning. The routes on the LAN side and routes entered manually during configuration are Static routes. Routes learned from the SD-WAN or dynamic routing peers are Dynamic routes.
- **Protocol**: The protocol of the prefixes.
  - **Local**: Local virtual IPs of the appliance.
  - **Virtual WAN**: Prefixes learned from peer SD-WAN appliances.
  - **OSPF**: Prefixes learned from OSPF dynamic routing peer.
  - **BGP**: Prefixes learned from BGP dynamic routing peer.
- **Neighbor Direct**: Indicates whether the subnet is connected to the branch from which the route came to the appliance.
- **Cost**: The cost used to determine the best path to a destination network.
- **Hit Count**: The number of times a route was hit to forward a packet to that subnet.
- **Eligible**: Indicates that the route is eligible and is used for forwarding or routing the packets to the prefix hit during traffic processing.
- **Eligibility Type**: The following two eligibility types are available.
  - **Gateway eligibility**: Determines if the gateway is reachable or not.
  - **Path eligibility**: Determines if the path is DEAD or NOT DEAD.
- **Eligibility Value**: The value selected for the gateway or the path in the configuration while the route is created in the system. For instance a route can be called eligible based on a path MCN-WL-1->BR1-WL-2. So the eligibility value for this route in the routes section is the value MCN-WL-1->BR1-WL-2.

Routing

March 12, 2021

Dynamic Routing

Citrix SD-WAN introduces support for well known Routing protocols under the **Dynamic Routing** feature. This feature facilitates the 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, Citrix SD-WAN provides more control over which SD-WAN routes are advertised to routing neighbors rather and which routes are received from routing neighbors, rather than advertising and accepting 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.
- Import Filters are used to accept or not accept routes which are received using OSPF and BGP neighbors based on specific match criteria.

Route filtering is implemented on LAN routes and Virtual Path routes in an SD-WAN network (Data Center/Branch) and is advertised to a non-SD-WAN network through using BGP and OSPF.

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.

Citrix SD-WAN (release version 10.0 and later) 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 the 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

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

‘

dynamic_routing?

‘

SD-WAN Overlay Routing

March 12, 2021

Citrix 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 applying route tables that overlay the existing underlay network. SD-WAN route tables can fully replace or coexist with the existing routing infrastructure.

Citrix SD-WAN appliances measure the paths available unidirectionally in terms of availability, loss, latency, jitter and congestion characteristics, and select the best path on a per-packet basis. This means that the path chosen from Site A to Site B, need not necessarily be the path chosen from Site B to Site A. The best path at a given time is selected independently in each direction. Citrix SD-WAN offers packet-based path selection for rapid adaptation to any network changes. SD-WAN appliances can detect path outages after just two or three missing packets, allowing seamless subsecond failover of application traffic to the next-best WAN path. SD-WAN appliances recalculate every WAN link status in about 50 ms. The following article provides detailed routing configuration within the Citrix SD-WAN network.

Citrix 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. The following are the main service types in use:

- **Local 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** –Denotes any local route learned from a remote SD-WAN site that 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** –Denotes routes that are reachable through a private WAN link (MPLS, P2P, VPN, and so on). 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 must 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 Intranet Service. 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 route 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.

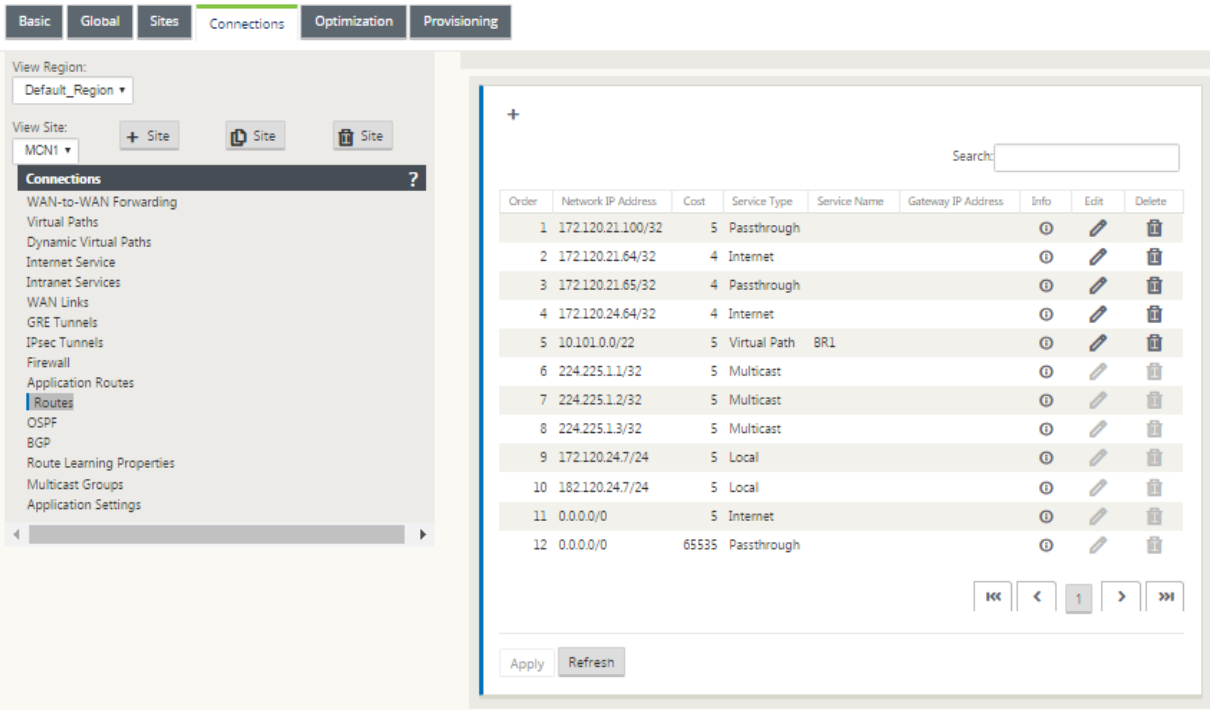
- **Passthrough** –This service acts as a last resort or override service when an appliance is in-line mode. If a destination IP address fails to match with any other route, then the SD-WAN appliance simply forwards it onto the WAN link next hop. A default route: 0.0.0.0/0 cost of 16 pass-through

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 is limited as much as possible.

> **Note**
>
> Passthrough can be useful when conducting a POC to avoid having to configure numerous routings, however be 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 the path. You must have an Intranet service or local route as a catch all route, otherwise the traffic is 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:



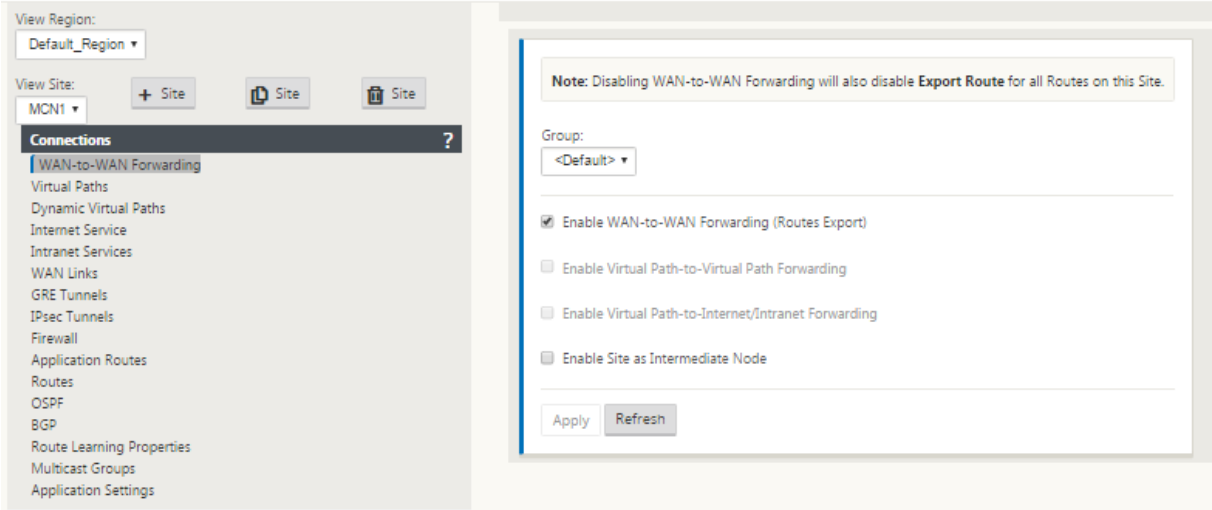
Route table entries are populated from different inputs:

- Configured Virtual IP Address (VIP) auto-populate as Service Type Local route. The Configuration Editor prevents the same VIP assignment to different site nodes.
- Internet Services enabled at a local site auto-populate a default route (0.0.0.0/0) locally for direct internet breakout.

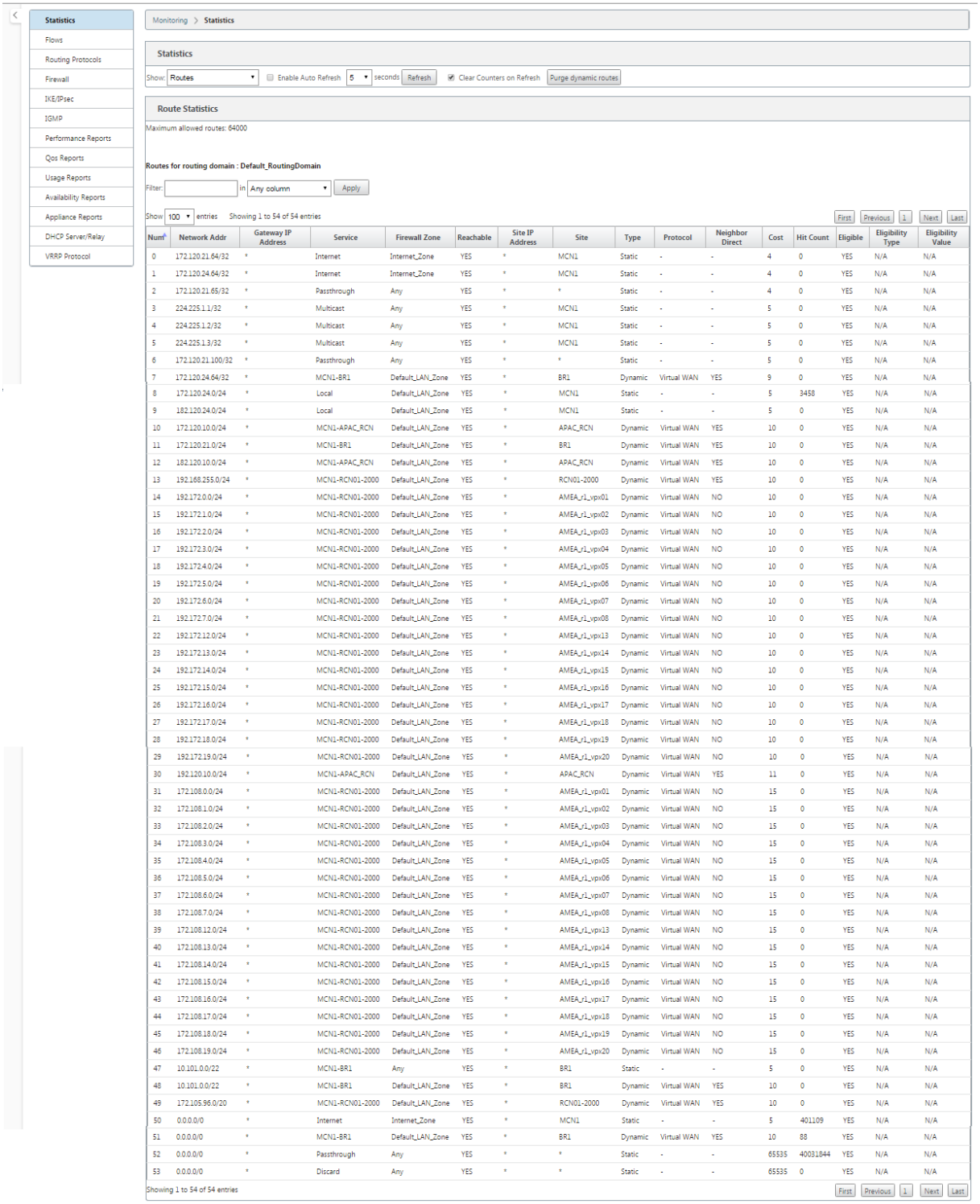
- Admin defined static routes on a per site basis, which will also be defined as a Service Type Local route.
- A default (0.0.0.0/0) catches all route with cost 16 defined as Passthrough

Administrators can configure one of the preceding 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 (refer the following table for default route costs). Also, 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. For client node routes to be visible to another client nodes WAN to WAN Forwarding must be enabled at the MCN node.



With WAN-to-WAN Forwarding (Routes Export Template) enabled under Global settings, the MCN site shares 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 list.

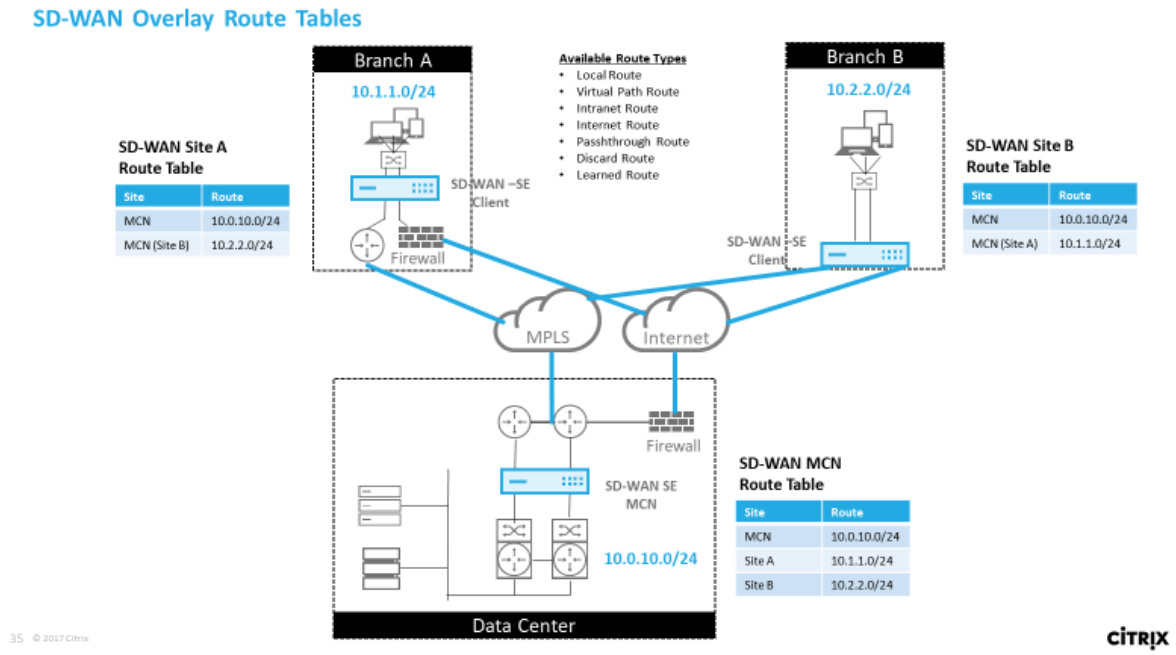


Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.120.21.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
1	172.120.24.64/32	*	Internet	Internet_Zone	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

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 following 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.



How Citrix SD-WAN Traffic Matches on Defined Routes

The match process for defined routes on Citrix SD-WAN is based on the longest prefix match for the destination subnet (similar to a router operation). The more specific the route, the higher the change on it being matched. Sorting is done in the following order:

1. Longest prefix matches
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 as follows:

- 192.168.1.0/24 Cost 5
- 192.168.1.64/26 Cost 10

A packet destined for the 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, and so on), and the next hop IP.

Citrix 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 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 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 processed by the rule engine and a flow is created in the flow database.

Citrix SD-WAN Routing Protocol Support

Citrix 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. Citrix 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). Also,

SD-WAN can be deployed in “learn only”mode where SD-WAN can receive routes but not advertise routes back to the underlay. This is useful when introducing the SD-WAN solution into a network where the routing infrastructure is complex or uncertain.

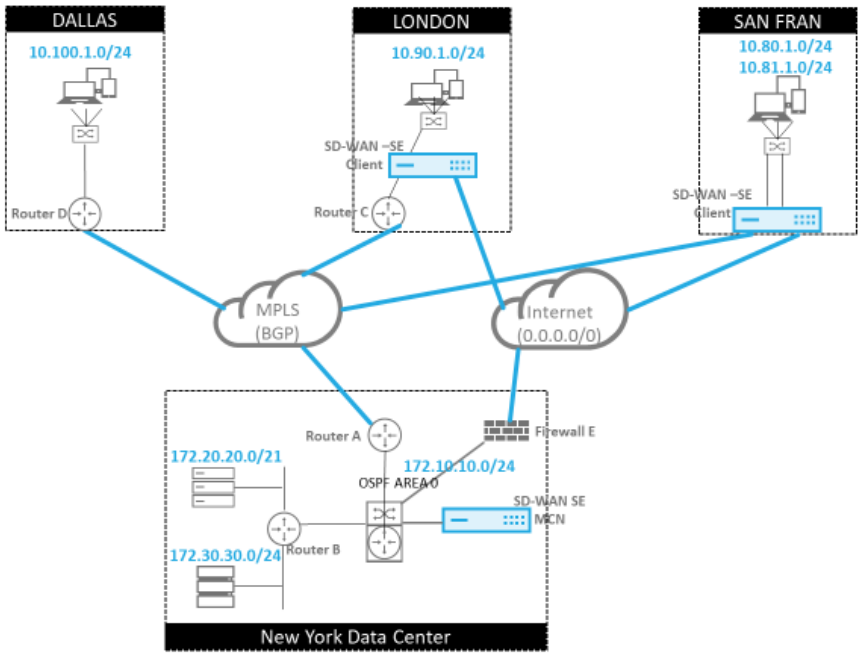
> **Important**
>
> It is easy to leak the unwanted route, if you are not careful.

The SD-WAN Virtual Path route table works as an External Gateway Protocol (EGP), 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 IGPs 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 interoperate 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:



In this example, we examine a routing protocol use case. The preceding network has four locations; New York, Dallas, London, and San Francisco. We 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 must 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 data center, even though the London and San Francisco Branches have a path to the internet.

The San Francisco site also must be noted not to have a router. SD-WAN is 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 is 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.

Review 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). The route costs indicate that 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:

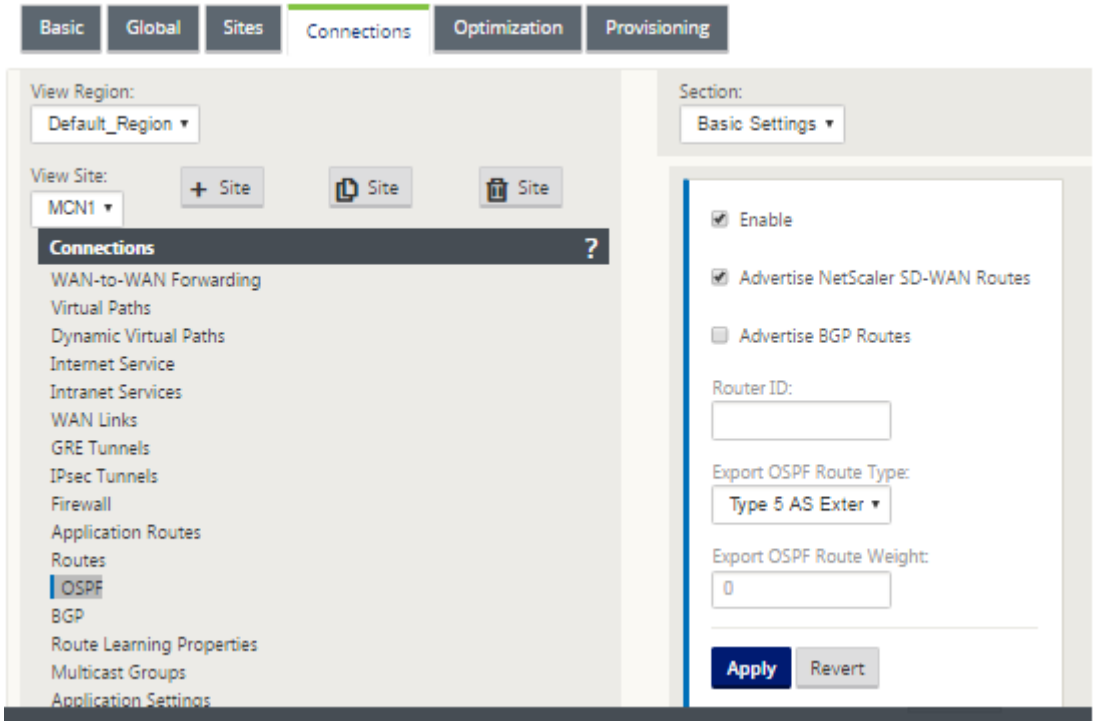
For the Dallas WAN Router (D) all routes are learned across the MPLS.

```
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 is

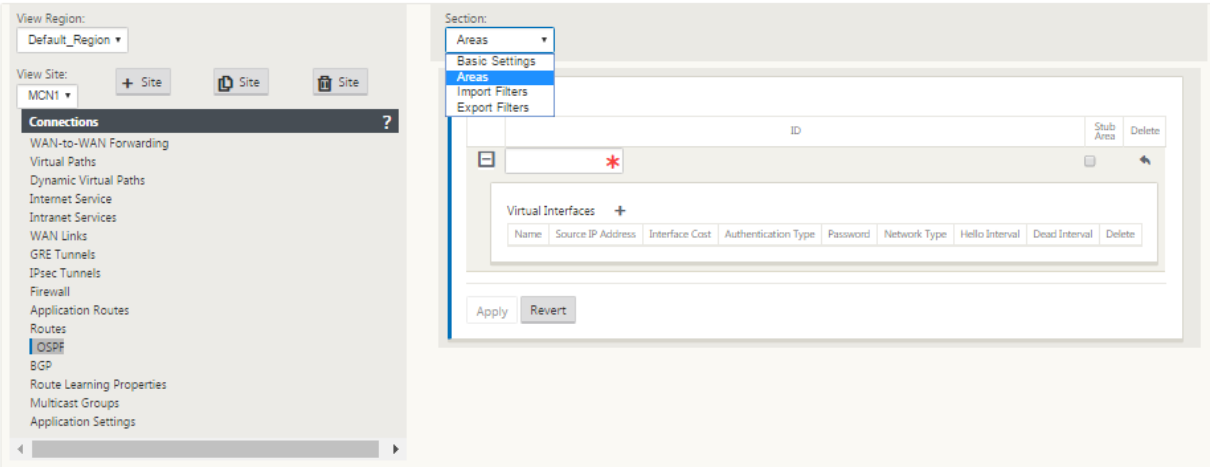
> not advertised in any routing protocol.

In Citrix 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 the SD-WAN routing table is considered external to the OSPF protocol and so OSPF will prefer a route learned internal (intra-area), therefore the routes advertised by SD-WAN might not take precedence.

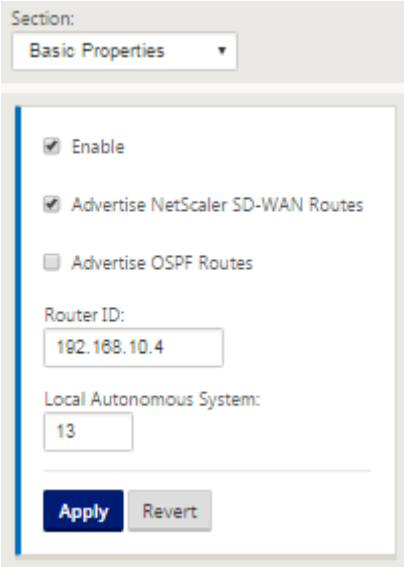
When OSPF is used across the WAN (that is, MPLS networks), then this can be changed to Type one intra-area. OSPF areas can be configured as shown below.

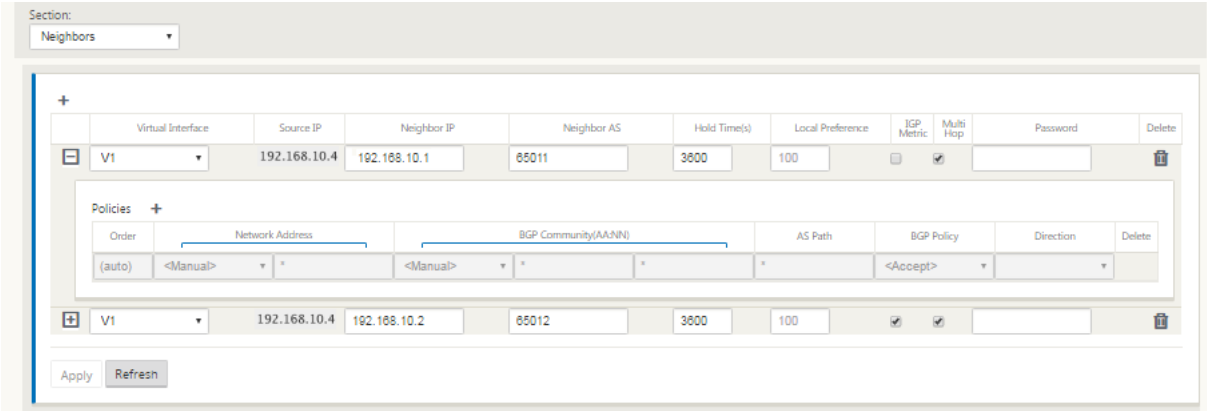


Area 0 added with the local network derived from the Virtual Interface (172.10.10.0), all other settings were left default.

For the new San Francisco site, we must 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.





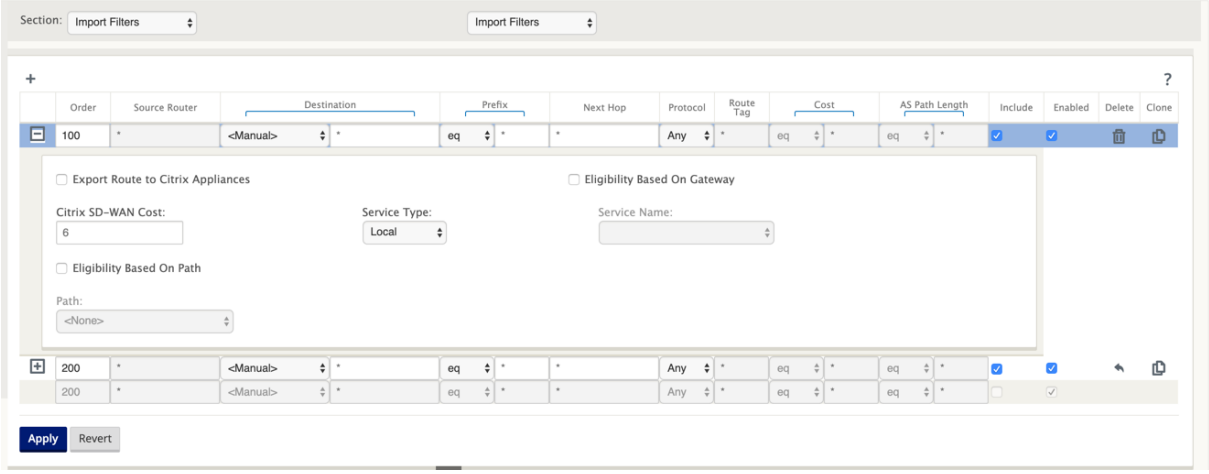
The eBGP peers with each other location. Each ASN is different.

It is important to understand how the 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 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 New York can still reach San Francisco over

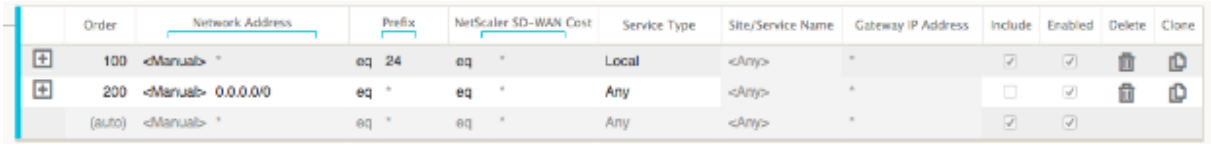
the Virtual Path overlay network. We also want to learn from eBGP reachability to all sites in case the SD-WAN Virtual Path overlay goes down and the environment must fall back to using just the MPLS. We also do not want to readvertise anything SD-WAN learns from eBGP to the SD-WAN routers. To accomplish this, the filters must be configured as follows:

- Import all routes from eBGP. Do not readvertise/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 not to readvertise the routes. Any route matching any prefix SD-WAN has learned across the Virtual Paths.



After the Citrix 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 Citrix SD-WAN route table can be viewed on the **Monitoring** > **Statistics** > **Show Routes** page.

San Francisco Citrix SD-WAN:

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

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

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	10.81.1.0/24	10.80.1.20	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
1	10.80.1.0/24	*	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
2	192.168.10.0/24	*	Local	YES	*	SFO	Static	-	-	5	122	YES	N/A	N/A
3	172.10.10.0/24	*	NYC-SFO	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
4	172.30.30.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
5	172.20.20.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
6	172.10.10.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	192.168.10.3	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	10.90.1.0/24	192.168.10.2	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
9	172.20.20.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
10	10.100.1.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
11	172.30.30.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
12	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
13	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

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

Citrix SD-WAN 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 the New York Data Center. This route is being learned in two ways:

- As a Virtual Path route (Number 3), service = NYC-SFO with a cost of 5 and type static. This is a local subnet advertised by SD-WAN appliance in New York. It is static in that it is either di-

rectly 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.

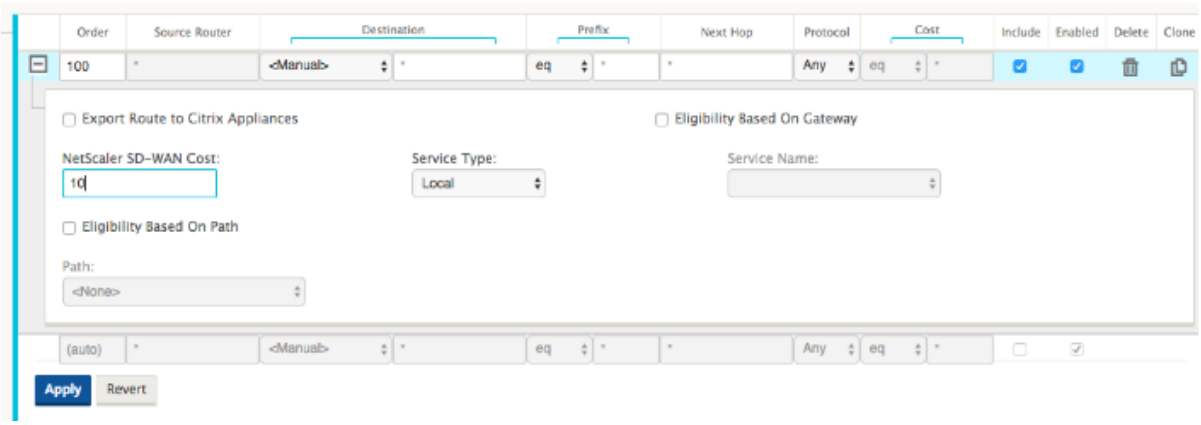
- As an advertised route through BGP (Number 6), with a cost of 6. This is now considered a fallback route.

Since the prefix is equal and the cost is different, SD-WAN uses the Virtual Path route unless it becomes unavailable in which case the fallback route is learned through BGP.

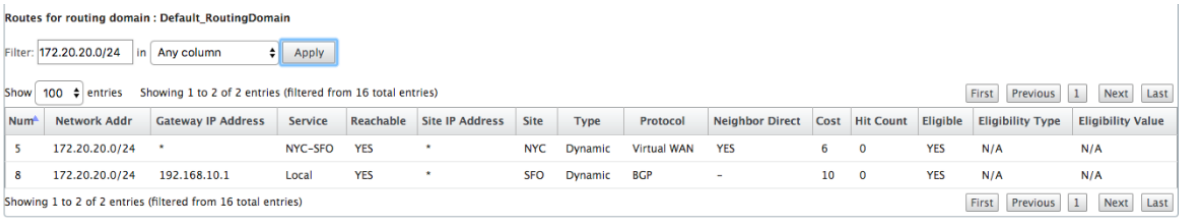
Now, let us consider the route 172.20.20.0/24.

- This is learned as a Virtual Path route (Number 9) but has a type of dynamic and a cost of 6. This means that 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 might be preferred over the Virtual Path route.

To ensure correct routing, we must increase the BGP route cost to make sure if we have a Virtual Path route and it is 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. Use the filter option to focus the displayed list.



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 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) First Previous 1 Next Last

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

Showing 1 to 4 of 4 entries (filtered from 16 total entries) First Previous 1 Next Last

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 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 to advertise 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> 192.168.65.0/24	eq *	*	Any	eq *	☐	☑		
200	*	<Manual> 192.168.10.0/24	eq *	*	Any	eq *	☐	☑		
300	*	<Manual> *	eq *	*	Any	eq *	☑	☑		
(auto)	*	<Manual> *	eq *	*	Any	eq *	☐	☑		

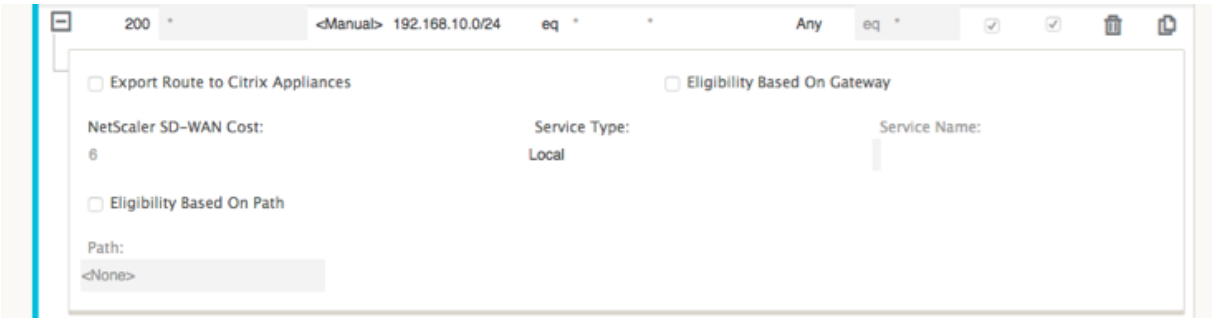
☐ Export Route to Citrix Appliances ☐ Eligibility Based On Gateway

NetScaler SD-WAN Cost: 6 Service Type: Local Service Name:

☐ Eligibility Based On Path

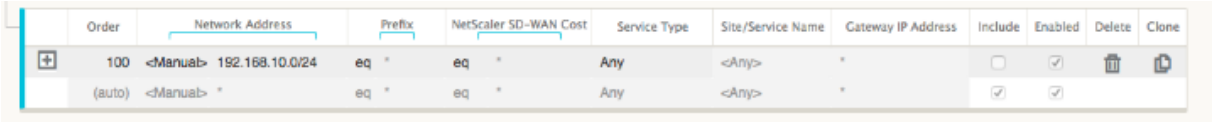
Path: <None>

The New York SD-WAN site imports all routes for the management network. This can be ignored. We can focus on filter 200.



Filter 200 is used to import 192.168.10.0/24 (our MPLS core) for reachability but not to export it to the virtual path. Select the **Include** check box and ensure that the **Export Route to Citrix Appliances** check box is cleared. All other routes are then included.

For the export filters, we can exclude the route for 192.168.10.0/24. This is because, as a directly connected subnet in the San Francisco site, we cannot filter this route out at the source, so it is suppressed at this end.



Now let us review the refreshed route table starting at the core route in the 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 Apply

Show 100 entries Showing 1 to 11 of 11 entries First Previous 1 Next Last

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

We can see the correct routes for both the local subnets learned via OSPF, a route to the Dallas site learned from the MPLS Router A and the remote subnets for the San Francisco and London sites. 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 might 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. 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 that the Virtual Path is rerouted 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 4,980 packets at the SD-WAN appliance to prevent the Virtual Path from coming back to itself.

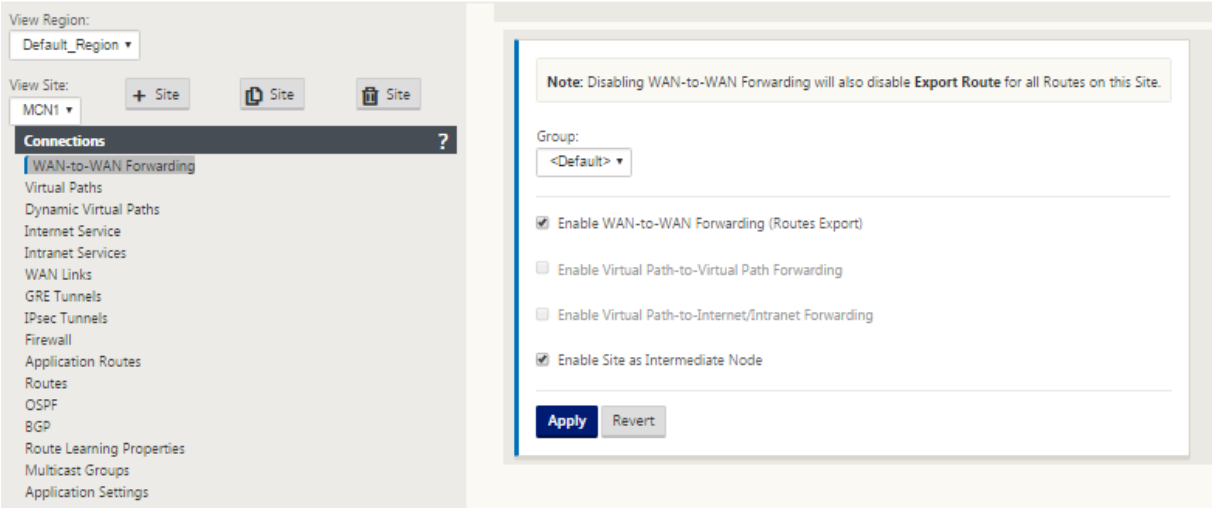
Dynamic Virtual Paths

Dynamic Virtual Paths can be allowed between two client nodes to build on-demand virtual paths for direct communication between the two sites. The advantage of a dynamic virtual path is that traffic can flow directly from one client node to the second without having to traverse the MCN or two virtual paths, which can 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.

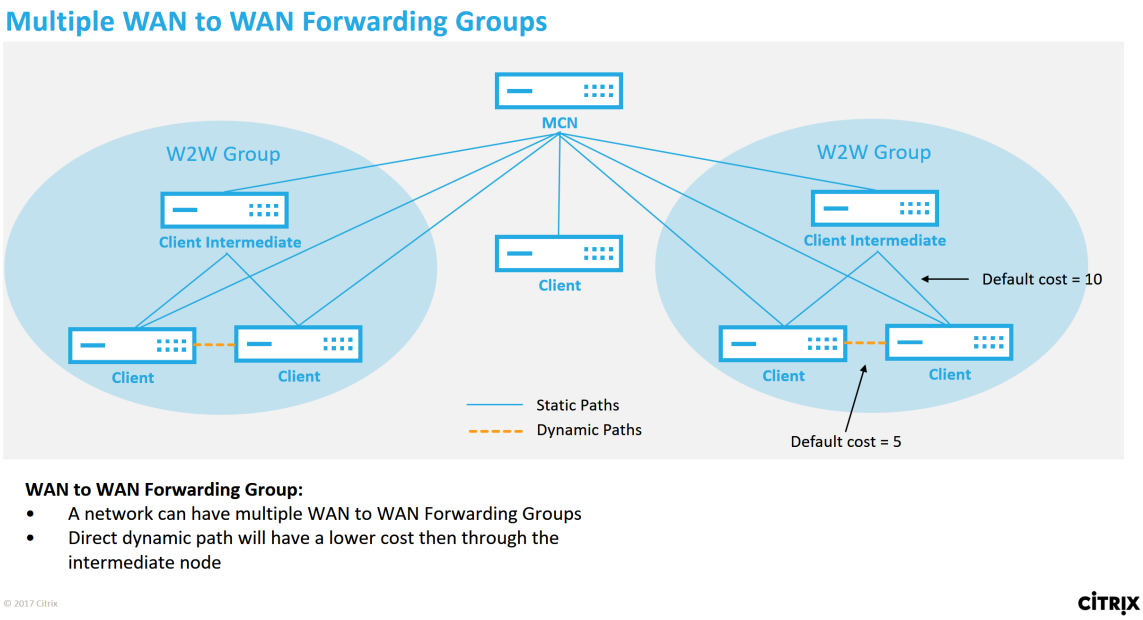
Once the thresholds for dynamic virtual paths are met, the client nodes dynamically create their virtualized path to one another using all available WAN paths between the sites and make full use of it in the following manner:

- 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
- If the user data falls below the configured thresholds for a user defined period, the dynamic virtual path is torn down

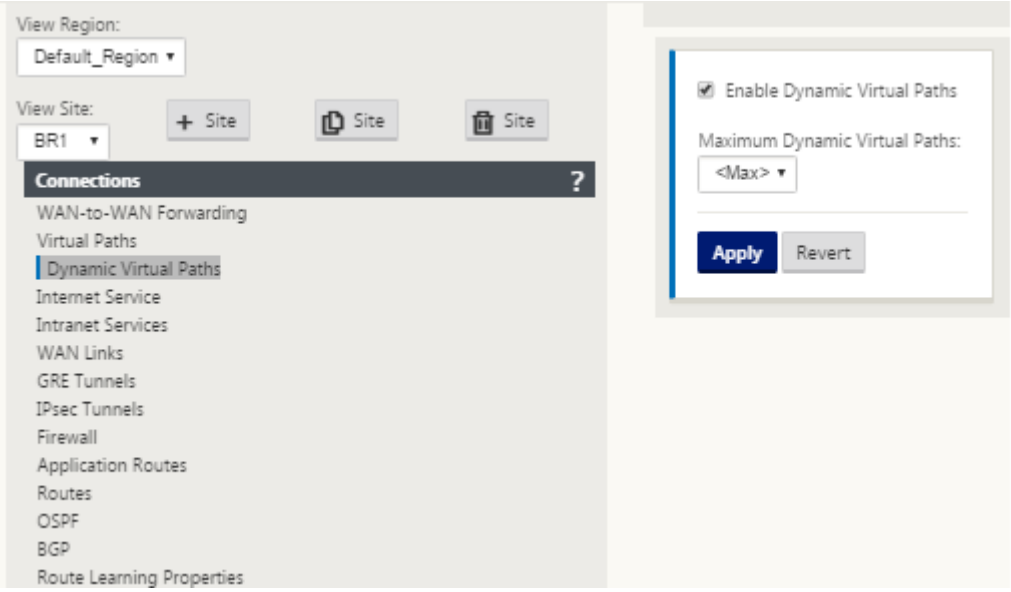
  Dynamic Virtual Paths have the concept of an Intermediate site. The intermediate site can be an MCN site or any other site in the network that has Static Virtual Path configured and connected to two or more other client nodes. Another design consideration requirement is to have WAN-to-WAN Forwarding 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** for this intermediate site to monitor client node communication and to dictate when the dynamic path must be established and torn down.



Multiple WAN-to-WAN Forwarding Groups can are allowed in the SD-WAN configuration, enabling full control to path establishment between certain client nodes and not others.



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 need **Enable Dynamic Virtual Path** option turned on for each client node.



Each SD-WAN device has 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 necessary
- 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

The following is an example SD-WAN site route table:

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

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

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.16.10.0/24	192.168.15.1	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	4	0	YES	N/A	N/A
1	192.168.100.0/24	*	Local	Default_LAN_Zone	YES	*	AWS	Static	-	-	5	0	YES	N/A	N/A
2	192.168.15.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
3	172.16.250.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
4	172.16.150.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
5	192.168.200.0/24	*	DC-AWS	Default_LAN_Zone	NO	*	Azure	Static	-	-	15	0	YES	N/A	N/A
6	192.168.10.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
7	172.16.200.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
8	172.16.100.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
9	172.16.30.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
10	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	1	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

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

Notice from the preceding SD-WAN route table that there are more elements not normally available 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 preceding table, we can see 14 defined routes. A description of the routes or groups of routes is described as follows:

- 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 the 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 are mapped to this service.
- Route 12 –Discard is the default route the system always adds to drop anything undefined.

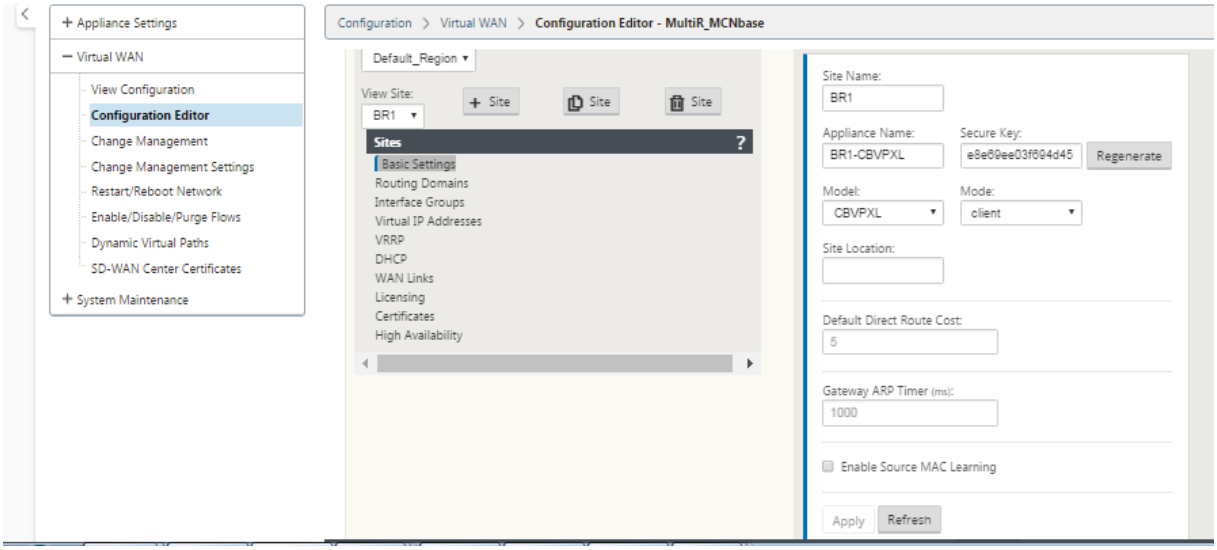
The Default Route Cost Values:

- 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

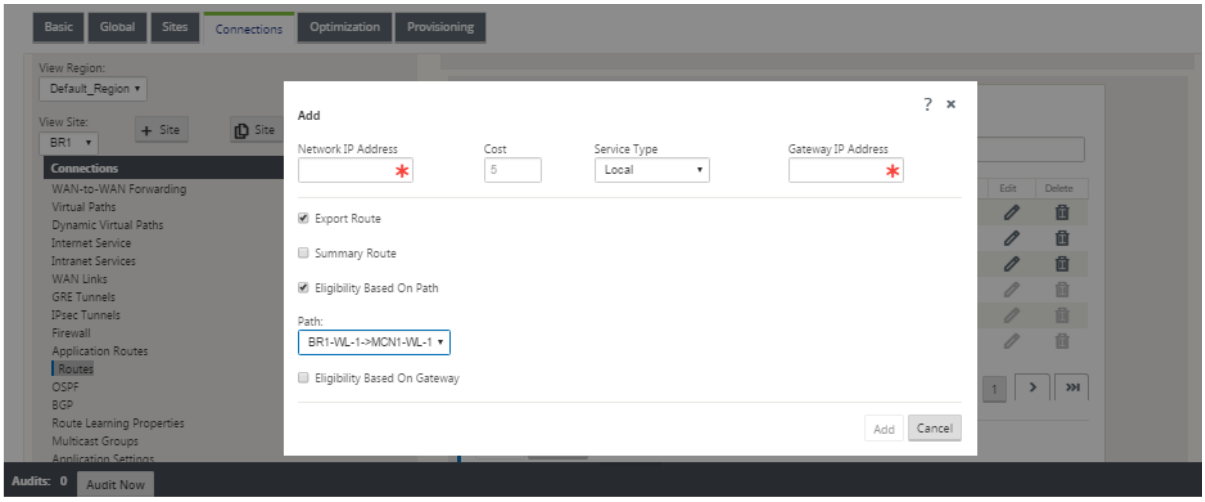
After defining these routes, it is important to understand how the traffic flows using the defined routes. These traffic flows are broken into the following flows:

- 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

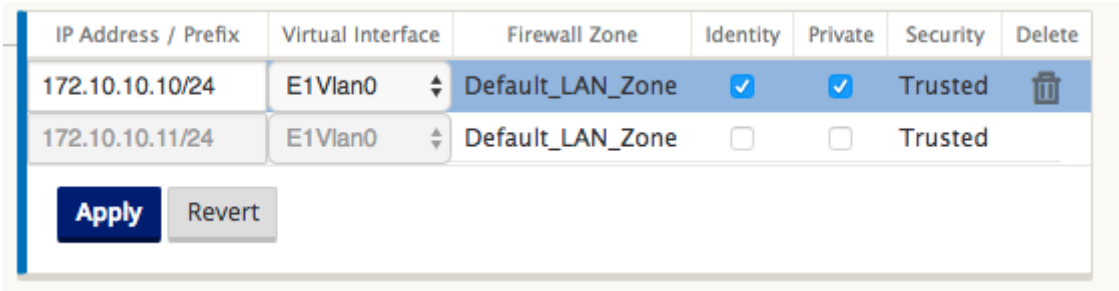
The default route cost can be altered on a per-site basis. The configuration can be found under **View Site** > **Basic Settings**:



Static routes can be defined per site under the **Connections** > **Site** > **Route**s node:



You 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 (that is, 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.



> **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 an SD-WAN WAN Link to support those types of services. It 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 is 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)
- 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 no assume that Passthrough works, it must be tested/verified, also test with Virtual Path down/disabled to verify desired behavior
- Route tables are static unless the route learning feature is enabled

  The maximum supported limit for multiple routing parameters is as follows:

- 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

Routing Domain

March 12, 2021

Citrix SD-WAN allows segmenting networks for more security and manageability by using the Routing Domain. 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.

Citrix 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 WAN Link or an Access Interface for each routing domain.

Following are the list of points to consider when configuring the Routing Domain functionality:

- By default, routing domains are enabled on an MCN.
- Routing domains are enabled on the Branch sites.
- Each enabled routing domain must 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.

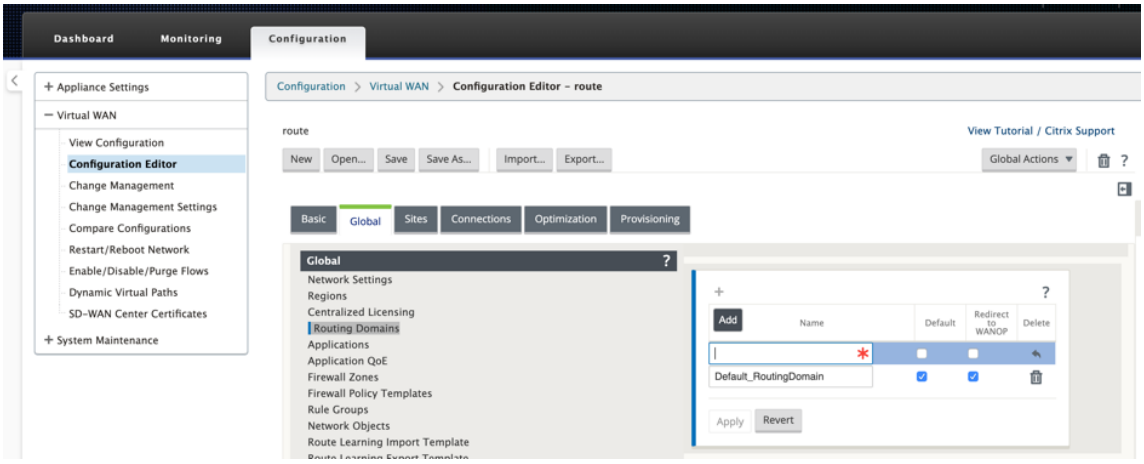
Configure Routing Domain

March 12, 2021

Citrix 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. You can configure up to 254 routing domains.

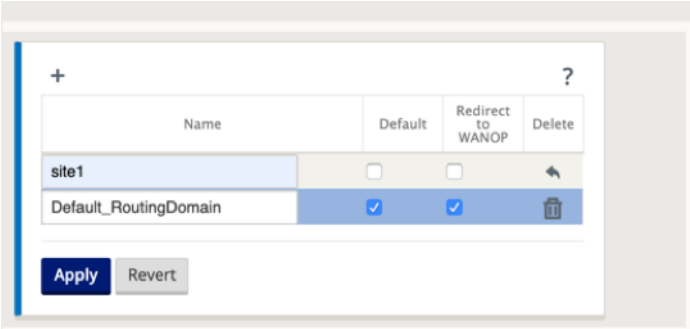
To configure routing domain:

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.

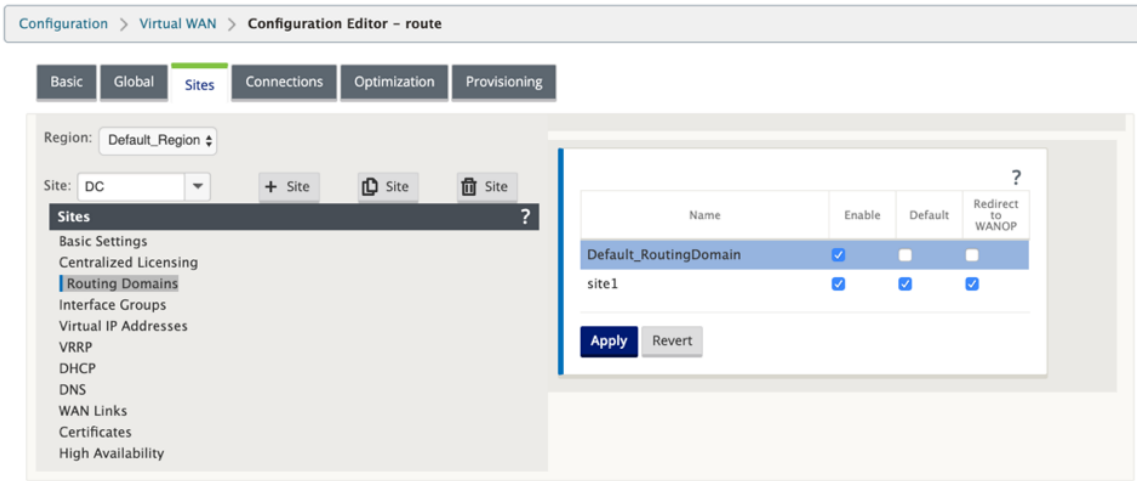


2. If you want to default to this Routing Domain, click the **Default** check box. Click **Apply** to save the changes. If you plan to implement a single Routing Domain, no explicit configuration is required.

   All new configurations are automatically populated with a default Routing Domain.



3. Navigate to **Sites** → **[Client Site Name]** > **Routing Domains**. Click the **Enable** check box to enable a configured Routing Domain for the Site.
4. Click the **Default** check box to make that Routing Domain the default for the Site. Click **Apply** to save the changes.



> **Note**
>
> Unchecking **Enable** for a Routing Domain makes it unavailable for use at the Site.

With 11.0.2 release, **Routing domains without routable Virtual IPs (VIPs)** is allowed with the following capabilities:

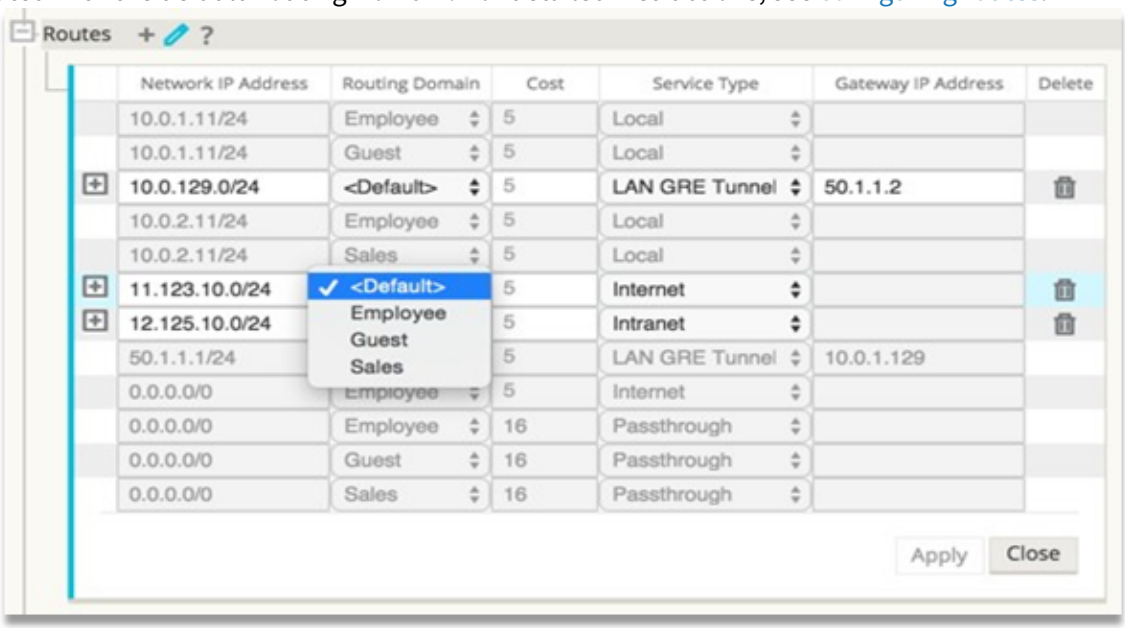
- Allow a device to have a Routing Domain for untrusted or no Interfaces.
- Allow branches to communicate among one another over a Routing Domain that has no physical presence at an intermediate site.

Configure Routes

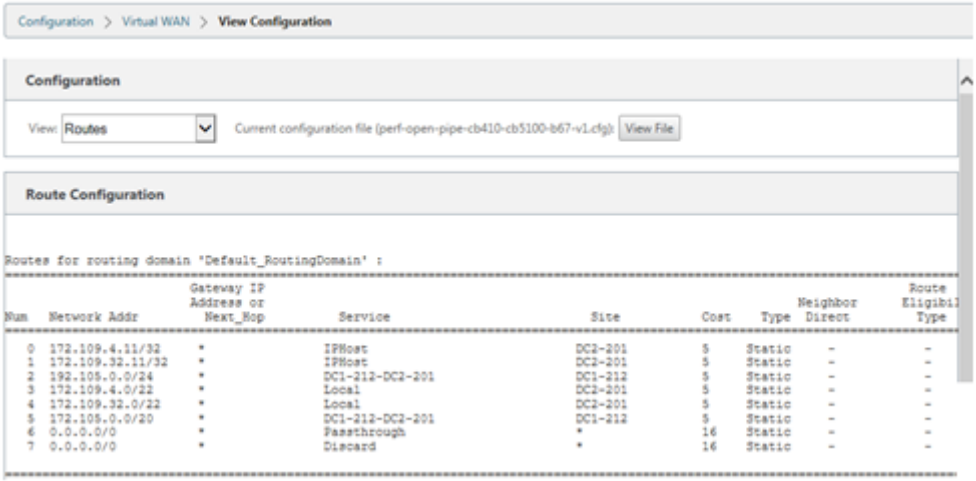
March 12, 2021

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 routes.



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

March 12, 2021

In Citrix 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?
<!--NeedCopy-->
```

Dynamic Routing

March 12, 2021

The following two dynamic routing protocols are supported by Citrix SD-WAN:

- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)

OSPF

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.

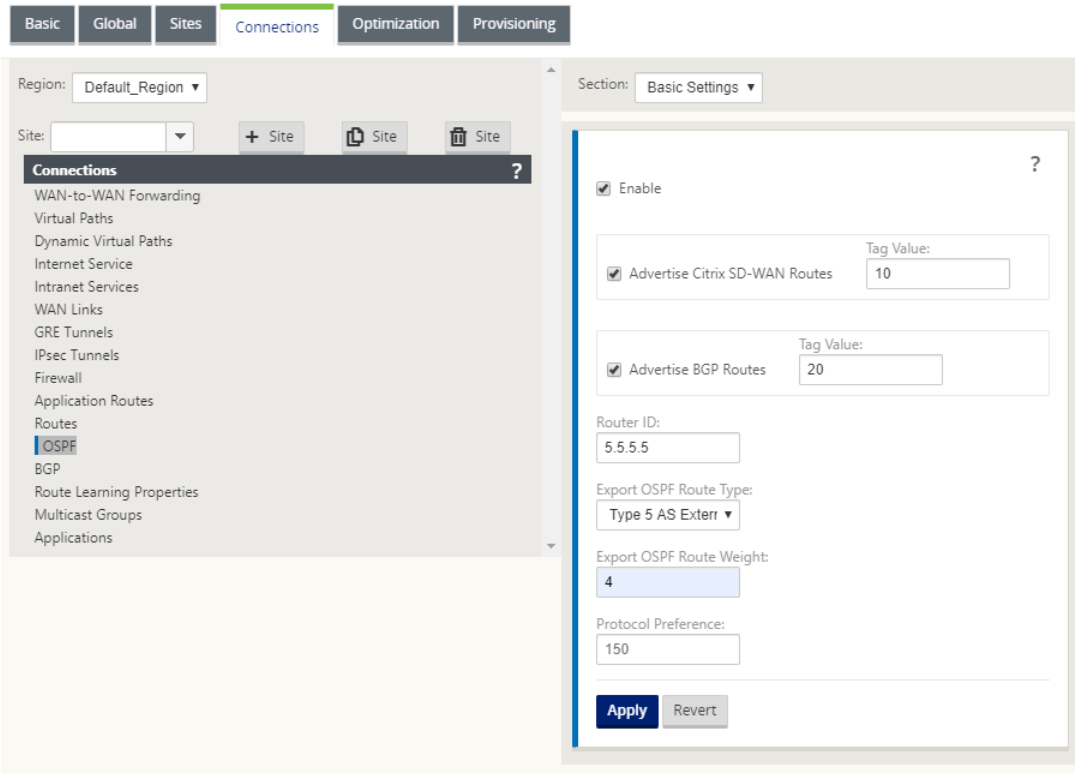
You can now configure Citrix SD-WAN appliances (Standard and Premium (Enterprise) Editions) to learn routes and advertise routes using OSPF.

> **Note**
>
> - Citrix 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."
> - Citrix SD-WAN appliance does not support summarization as an Area Border Router (ABR).

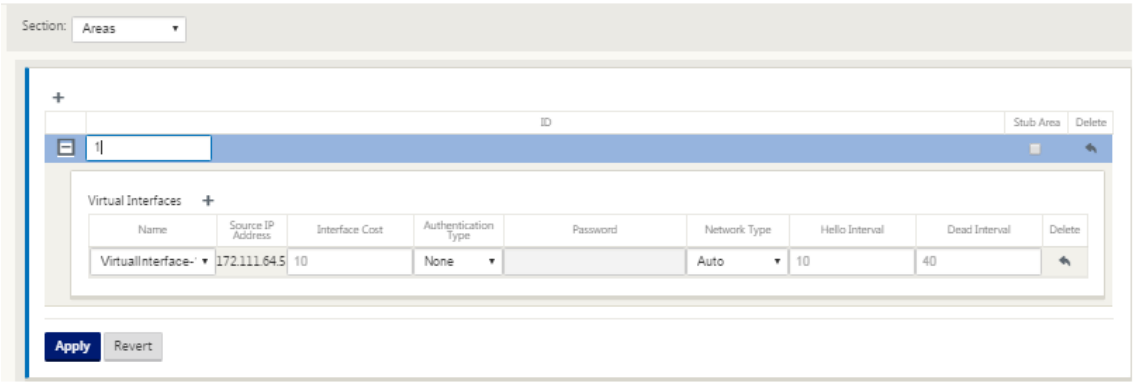
Configure OSPF

To configure OSPF:

1. In the **Configuration Editor**, navigate to **Connections > Region > Site > OSPF > Basic Settings**.
2. Click **Enable**, select, or enter values for the following parameters and click **Apply**.
   - **Advertise Citrix SD-WAN Routes**: Allow Citrix SD-WAN routes to be advertised via OSPF. You can also specify a tag for OSPF redistribution.
   - **Advertise BGP Routes**: Allow routes learned from BGP peers to be advertised via OSPF. You can also specify a tag for OSPF redistribution.
   - **Router ID**: The unique router identifier, the router is used for OSPF advertisements. If the Router ID is not specified, it is auto-selected as the lowest Virtual IP hosted in the SD-WAN network.
   - **Export OSPF Route Type**: Advertise the Citrix SD-WAN routes to OSPF peers as intra-area routes or external routes.
   - **Export OSPF Route Weight**: When exporting Citrix SD-WAN routes to OSPF, add this weight to each route's Citrix SD-WAN cost.
   - **Protocol Preference**: If prefixes are learned via multiple routing protocols, the protocol preference value determines routing protocol selection. For more information, see Protocol preference.



3. Expand **OSPF** -> **Area**, and click **Edit**.



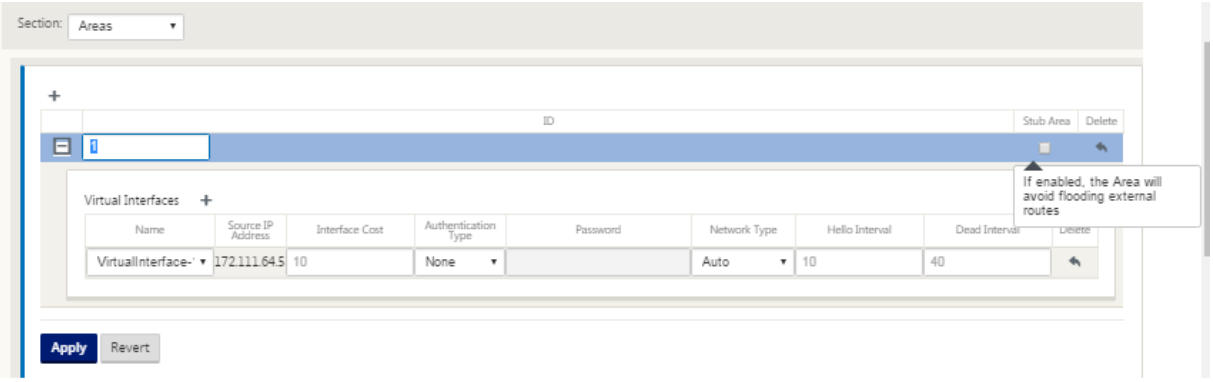
4. Enter an **area ID** to learn routes from and advertise to.
5. If Identity is not checked for a specific Virtual IP Address, the associated Virtual Interface is not available for IP services.
6. Choose one of the available Virtual Interfaces from the **Name** menu. The Virtual Interface determines the **Source IP Address**.
7. Enter the **Interface Cost** (10 is the default).
8. Choose an **Authentication Type** from the menu.
9. If you chose **Password** or **MD5** in step 8, enter the Password associated text field.

10. 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).
11. In the **Dead Interval** field, enter the interval to wait before marking a router as dead. The default dead interval is 40 seconds.
12. Click **Apply** to save your changes.

Stub area

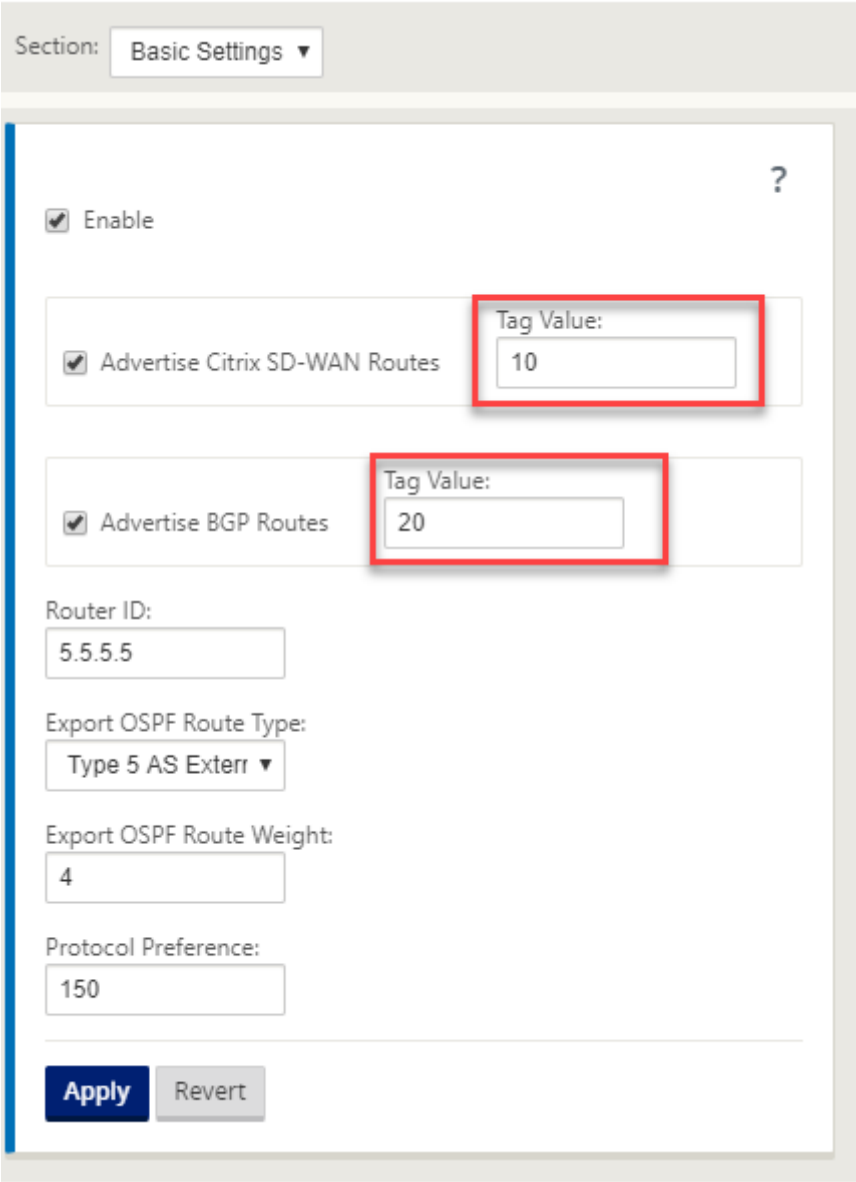
Stub areas are shielded from external routes and receive information about networks that belong to other areas of the same OSPF domain.

Enable the **Stub Area** check box.



OSPF redistribution tags

You can use OSPF tags to prevent routing loops during mutual redistributing between OSPF and other protocols. In the OSPF domain, if there are SD-WAN and BGP learned routes to the same subnet, the OSPF loop prevention mechanism identifies it as a loop and ignores the routes. Specifying different tags for SD-WAN and BGP learned routes allows these routes to be installed in the OSPF routing table. You can configure the OSPF redistribution tags for routes learned through SD-WAN and BGP in the OSPF, **Basic Settings** section.



BGP

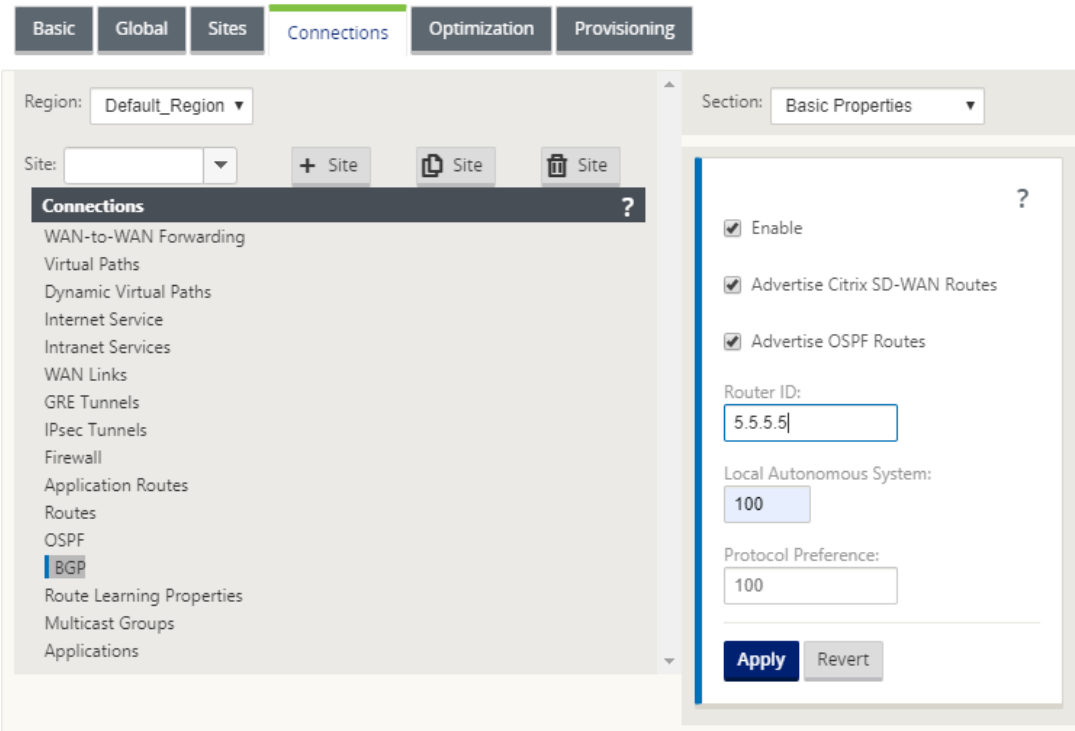
BGP is an inter-autonomous system routing protocol. An autonomous network or group of networks is managed under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between ISPs. Customer networks deploy Interior gateway protocols 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 Citrix SD-WAN appliances to learn routes and advertise routes using BGP.

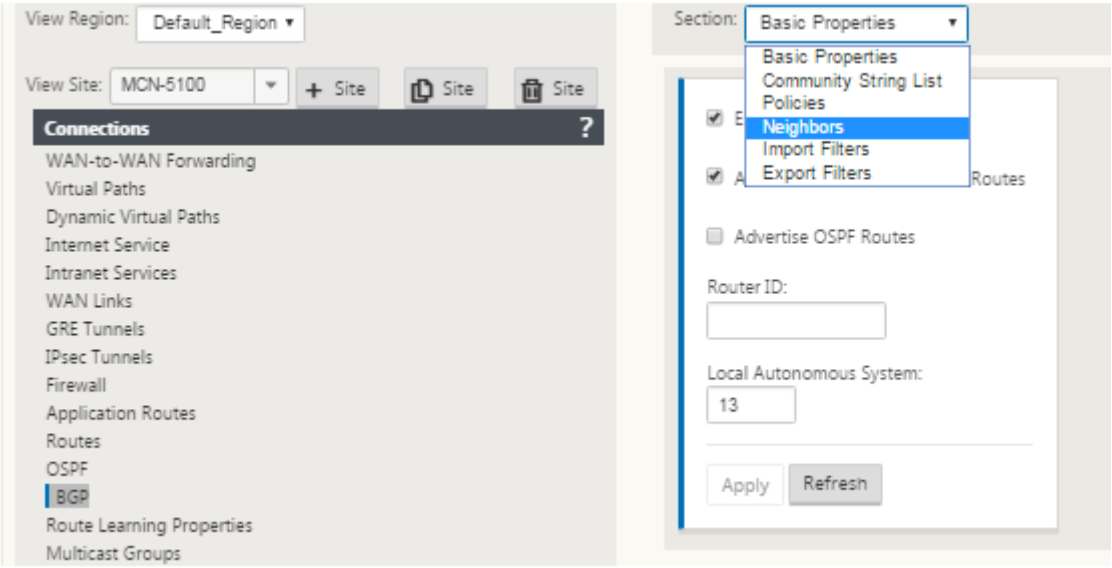
Configure BGP

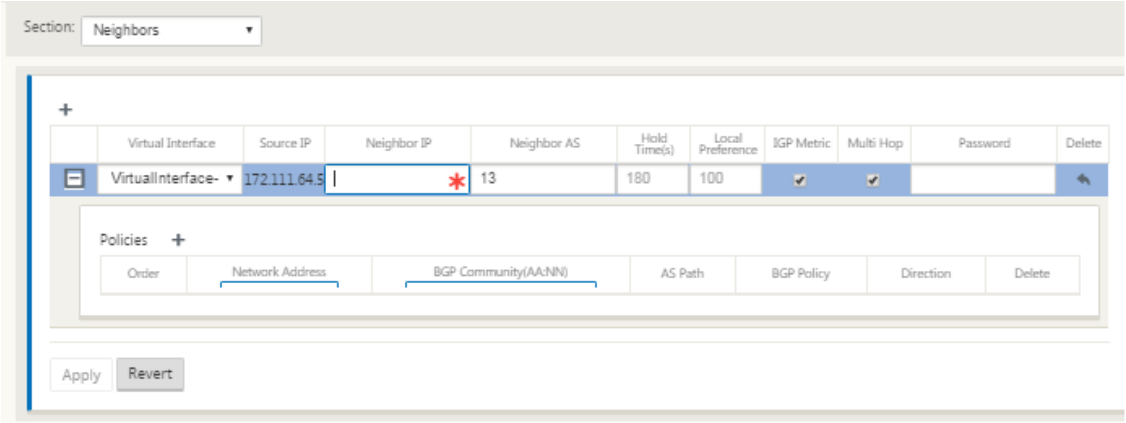
To configure BGP:

1. In the **Configuration Editor**, navigate to **Connections > Region > Site > BGP > Basic Settings.**
2. Click **Enable**, select, or enter values for the following parameters and click **Apply**.
    - **Advertise Citrix SD-WAN Routes**: Allow Citrix SD-WAN routes to be advertised via BGP.
    - **Advertise OSPF Routes**: Allow routes learned from OSPF peers to be advertised via BGP.
    - **Router ID**: The unique router identifier, the router is used for OSPF advertisements. If the Router ID is not specified, it is auto-selected as the lowest Virtual IP hosted in the SD-WAN network.
    - **Local Autonomous System**: The local autonomous system number from which the routes are learned and advertised to. The autonomous system number must match with one on the neighboring routers.
    - **Protocol Preference**: If prefixes are learned via multiple routing protocols, the protocol preference value determines routing protocol selection. For more information, see Protocol preference.



3. Expand **Basic Settings > Neighbors** and click the **Add (+)** icon.





For Sites with multiple Routing Domains choose a routing domain. Routing Domain determines which Virtual Interfaces are available.

4. Choose a **Virtual Interface** from the menu. The Virtual Interface determines the Source IP Address.
5. Enter the **IP Address** of the IBGP Neighbor router in the Neighbor IP field, and **Local Autonomous System** number in the Neighbor AS field.
6. In the **Hold Time (s)** field, enter the Hold Time, in seconds, to wait before declaring a neighbor down (the default is 180).
7. 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).
8. Click the **IGP Metric** check box to enable the comparison of internal distances to calculate the best route.
9. Click the **Multi-hop** check box to enable multiple hops for the route.
10. 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 SD-WAN network.

Exterior BGP (eBGP)

Citrix 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 replace the Routers. SD-WAN implements eBGP dynamic routing protocol to function as a dedicated routing device.

SD-WAN appliance establishes a neighborship 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, see the following use cases:

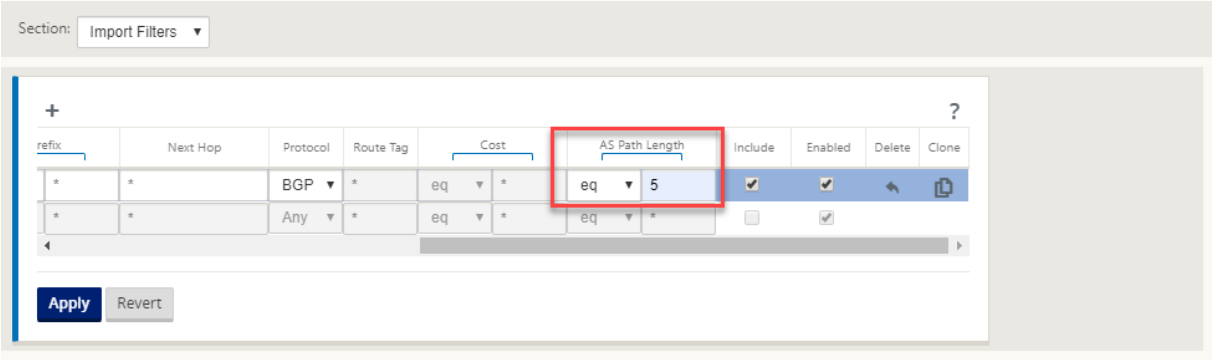
- SD-WAN site Communicating with non-SD-WAN site over eBGP
- Communication Between SD-WAN sites Using Virtual Path and eBGP
- Implementing OSPF in one-arm topology
- OSPF Type5 to Type1 deployment in MPLS Network
- SD-WAN and non-SD-WAN (third-party) appliance OSPF deployment
- Implementing OSPF using SD-WAN network with high-availability setup

AS path length

BGP protocol uses the **AS path length** attribute to determine the best route. The AS path length indicates the number of autonomous systems traversed in a route. Citrix SD-WAN uses the **BGP AS path length** attribute to filter and import routes.

Non-SD-WAN appliances can choose to route traffic to Primary DC or Secondary DC SD-WAN appliances by importing routes based on their AS path length. You can also dynamically steer traffic from a router to Secondary DC by simply increasing the AS path length of the Primary DC appliance on the router, making it unpreferable. Eliminating the need to change the route cost and perform a configuration update.

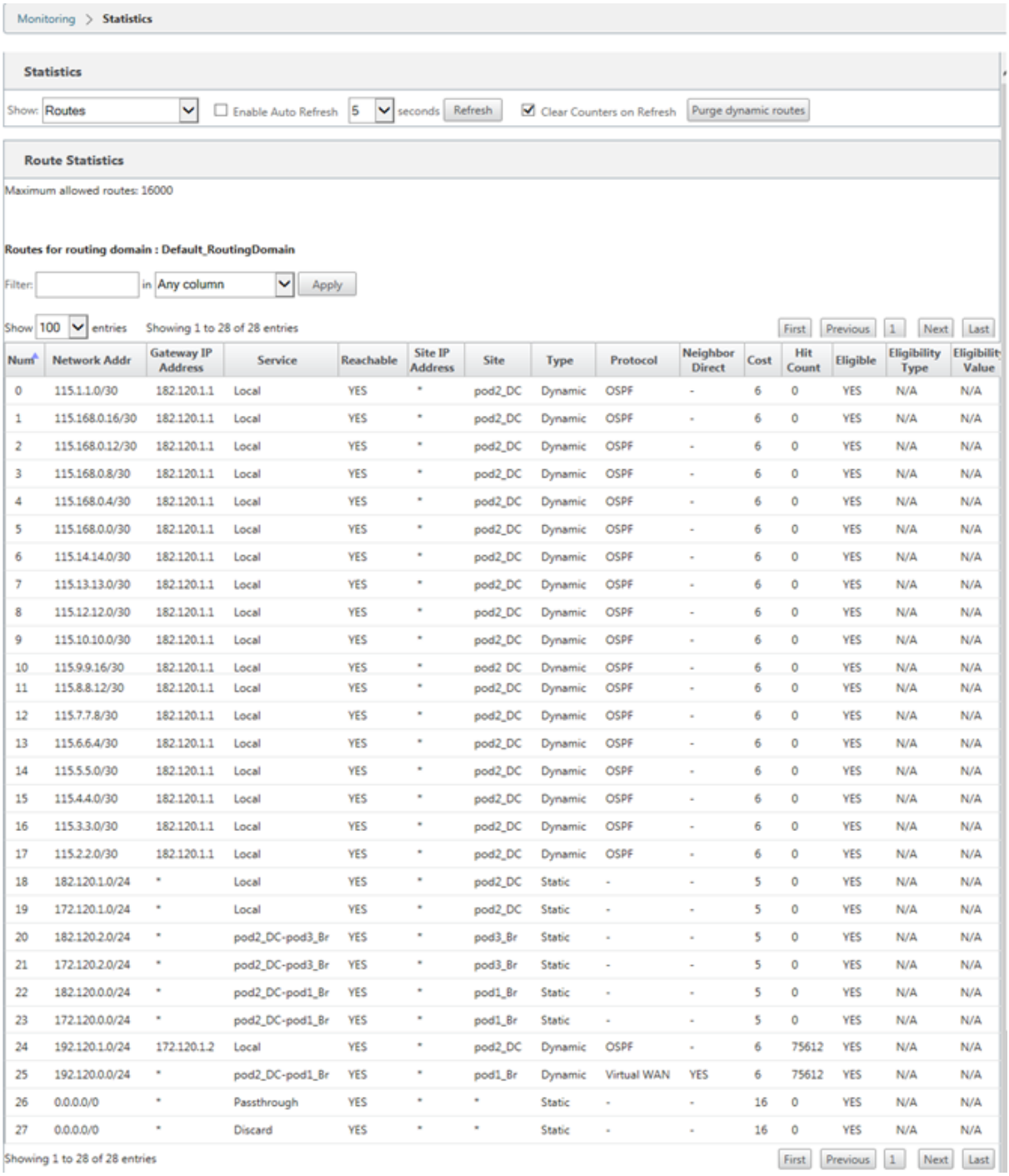
To configure AS path length in import filters, select BGP as the protocol, select a predicate, and enter the **AS path length**. For more information, see Route Filtering



Monitor route statistics

Navigate to **Monitor** > **Statistics**. Select **Routes** from the **Show** drop-down menu.

All functions for applicable Routes are supported in Citrix SD-WAN network regardless of whether a Route is Dynamic or Static.



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

OSPF

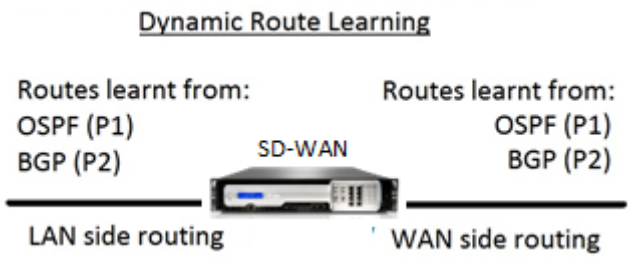
March 12, 2021

LAN Side: Dynamic Route Learning

OSPF running on the LAN port of Citrix SD-WAN appliance deployed in Gateway Mode:

Citrix 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 learned 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

Citrix SD-WAN appliance having an AREA defined as a STUB area by limiting the learning of Type 5 AS-external LSA.

Citrix 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 the SD-WAN appliance in a 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 the SD-WAN network. Additional PBR or WCCP configuration is not required any longer.

Prerequisites:

- SD-WAN Appliances at the DC and Branch sites must be running the latest release version.
- End-to-End IP connectivity must be configured and working fine.
- OSPF is enabled on all the sites.

To configure OSPF Type 1:

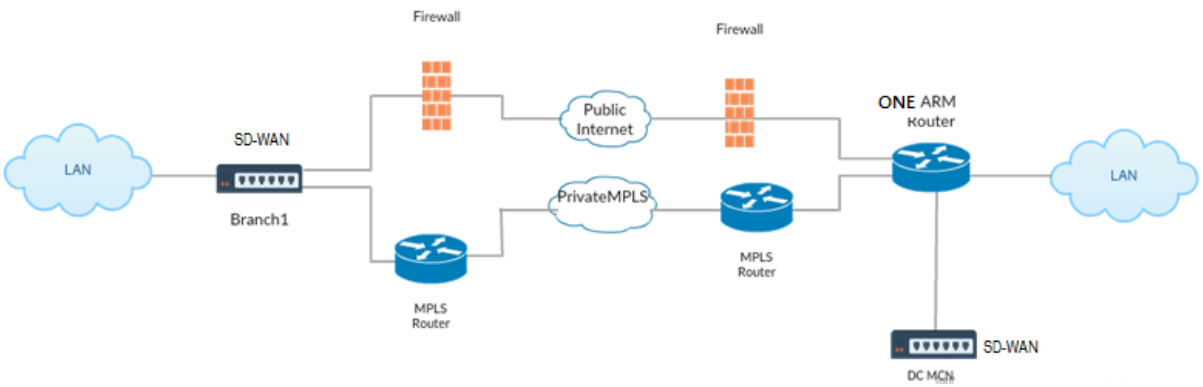
1. Configure **Virtual Interfaces** and **WAN links** on both the DC and Branch sites so that you can create the Virtual Path between them.
2. Under **Connections** > [**MCN**] > **Route Learning** > **OSPF**->**Basic Settings**, select **Export OSPF Route Type** to be **Type 1 Intra Area**.
3. Save the configuration, stage, and activate the configuration.

You must be able to see the following route types under
Export OSPF Route Type

- Type 5 AS External
- Type 1 Intra Area

You must be able to configure **Type 5 AS External** route.

After activation of the changed configuration, you must see the Route Type changes under **Configuration** > **Virtual WAN** > **View Configuration** > **Dynamic Routing**.



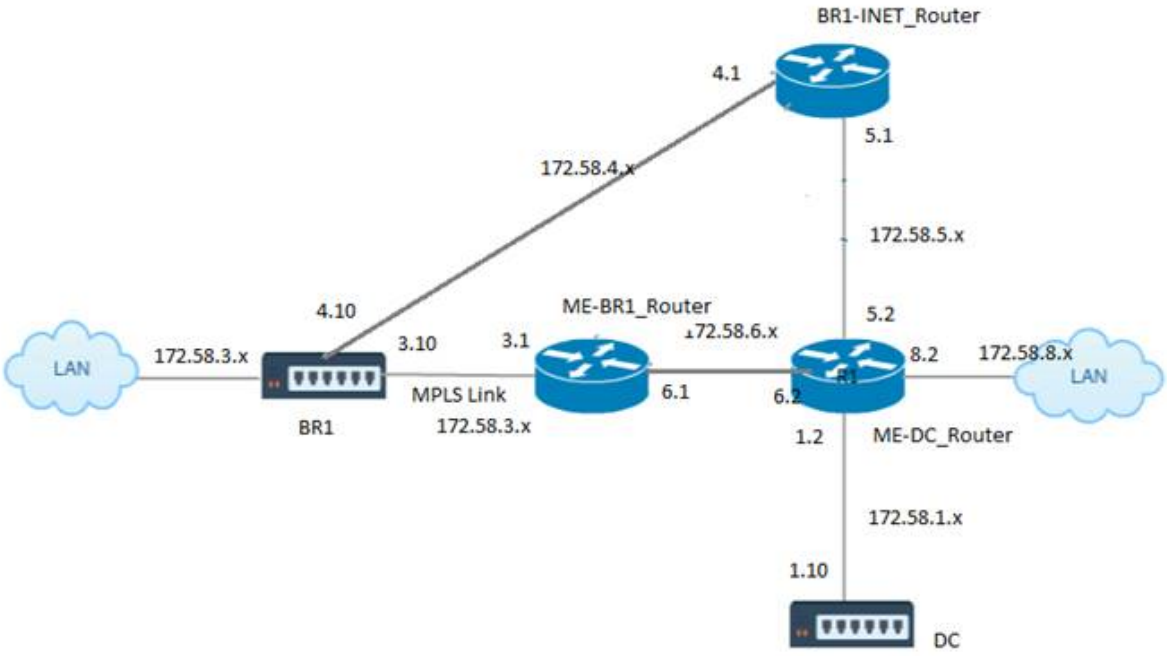
As shown in the illustration above, DC MCN is deployed in one-arm topology. When the DC site is up, the one-arm router forwards all traffic from the local LAN to other sites, such as the Branch's local

LAN whose destination IP address is within the same subnet to the SD-WAN first, then the 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, the 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:

1. Add, static route for 172.58.3.10/32(Virtual IP of BR1 for MPLS Link) through 172.58.6.1
2. 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 the 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 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 the 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 the 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.
- If this happens, MCN forwards the encapsulated packet destined to one the BR1 VIPs to the ME-DC Router and back from the 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)**.

- 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 the default SD-WAN cost of 5.
- 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 an 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 the SD-WAN appliance chosen as the preferred route initially, the interface cost of (172.58.3.1) must be manipulated to make it higher on the ME-BR1_Router so that the 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 ensures 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 the 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. You must be able to see the following two route types under **Export OSPF Route Type**:
   - Type 5 AS External
   - Type 1 Intra Area

After activation of the changed config, you can see the Route Type changes under **Configuration** > **Virtual WAN** > **View Configuration** > **Dynamic Routing**.

Routes must be advertised as Type5 External AS by the SD-WAN appliance. Routes learned through SD-WAN must 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 the 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**. The default route weight exported must be 0. Actual cost of the route must 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 the Virtual Path between them1. Under **Connections** > **[MCN]** > **Route Learning** > **OSPF** > **Export Filters** configure an export filter.

2. Expand the filter. Configure **Export OSPF Route Type** to **Type 1 Intra Area** route.
3. Save the configuration, stage, and activate the same. You must be able to see the following two route types under **Export OSPF Route Type**
   - Type 5 AS External
   - Type 1 Intra Area

After activation of the changed config, a user must be able to see the Route Type changes under **Configuration** > **Virtual WAN** > **View Configuration**. Route type must be displayed as Type 5 AS External.

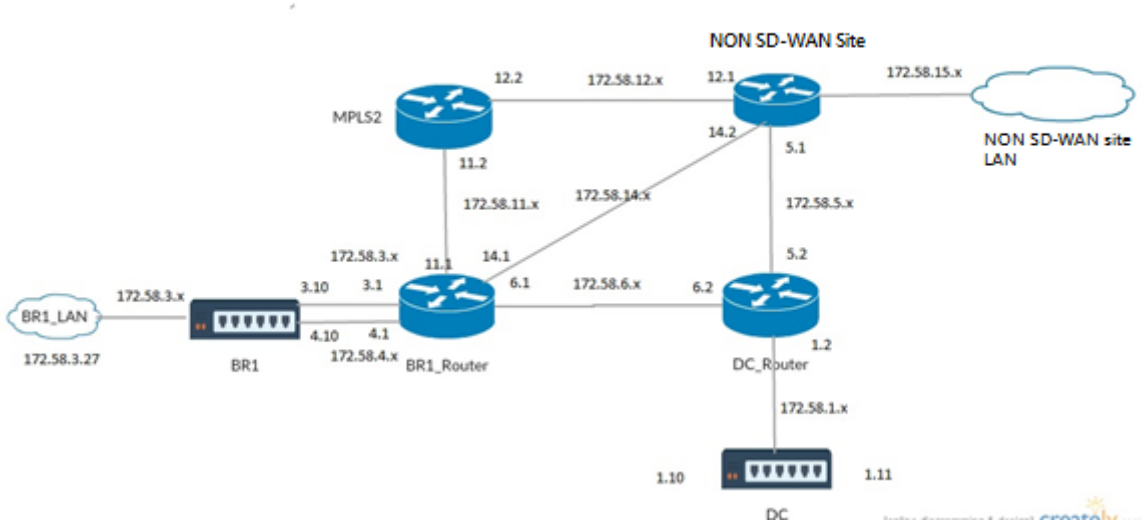
To configure OSPF exported route weight under Export Filter settings:

1. Configure Virtual Interfaces and WAN links on both DC and Branch so that we can create the 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.

After activation of the changed config, a user must be able to see the Route Type changes under **Configuration** > **Virtual WAN** > **View Configuration**.
Route Weight configured under Export Filter must override the Weight configured under **Basic OSPF Settings**.

SD-WAN and Third-Party (non-SD-WAN) Appliance Deployment

As shown in the illustration below, the third-party appliance site can get to Site B's LAN by sending traffic to Site B directly. If it cannot send traffic directly, the fallback route goes to Site A, then using the virtual path between DC to Branch sites to get to the Branch. If that fails, it uses MPLS2 to get to the Branch site.



Configuration Steps:

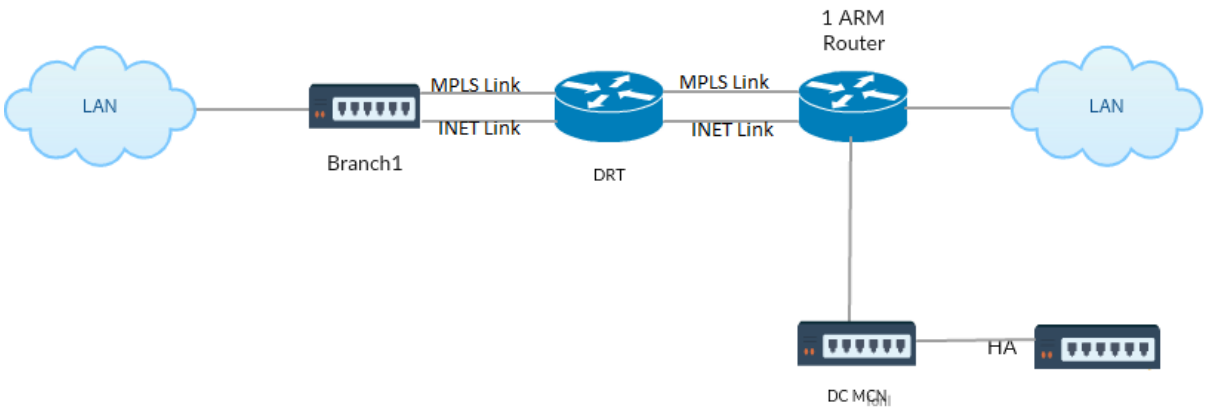
1. Configure **Virtual Interfaces** and **WAN links** on both DC and Branch so that a Virtual Path is created between the sites.
2. Configure **Export Route Type** as **Type1** and assign cost as **195** on the SD-WAN appliance.
3. Save, stage, and activate the configuration.
4. Send traffic between the end hosts on DC and Branch sites.
5. Shut down 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 the 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 the 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 must 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



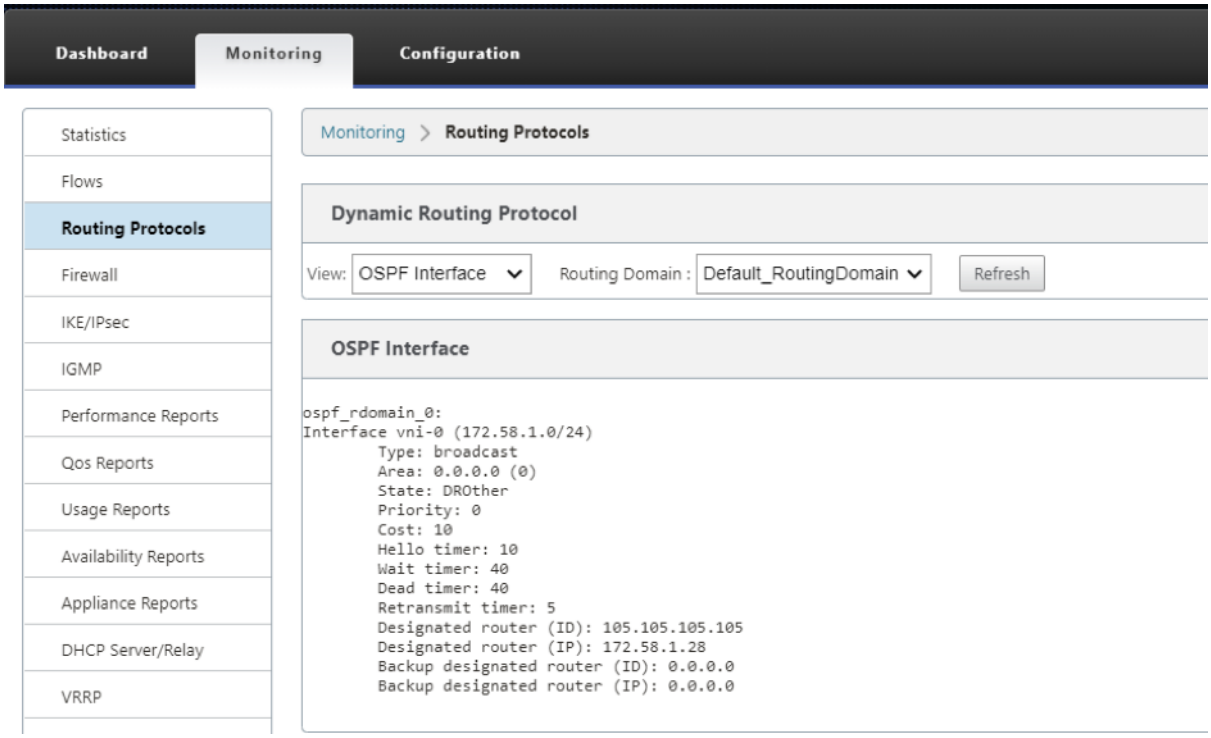
OSPF Type5 to Type1 with high-availability sites during failover to standby appliance and deployed in high-availablity setup:

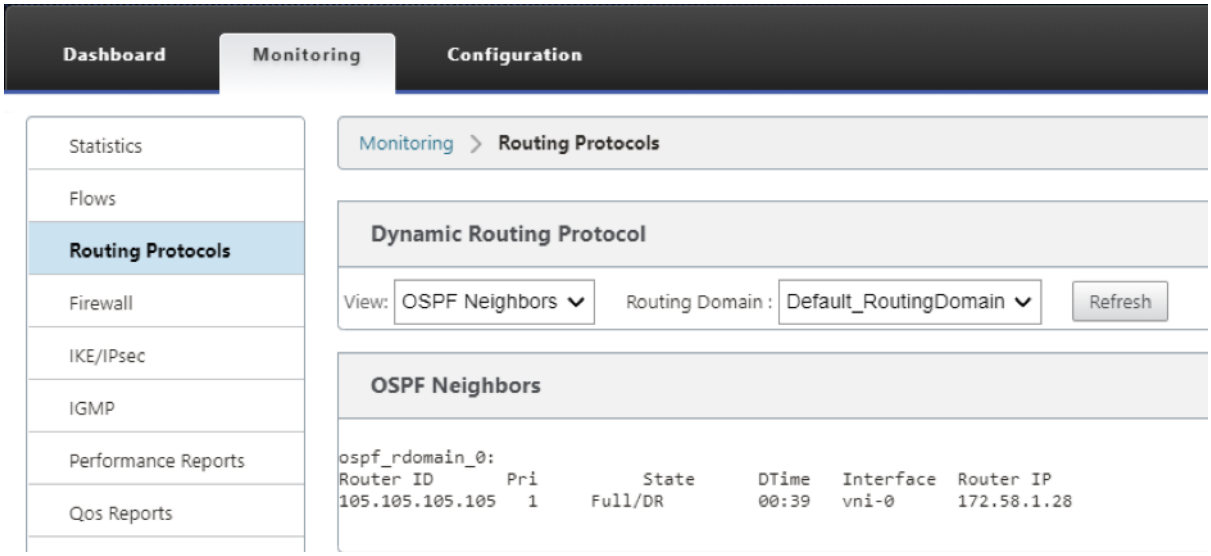
To configure OSPF in HA deployment:

1. Configure **Virtual Interfaces** and **WAN links** on both DC and Branch to create the Virtual Path between them.
2. Setup the High-Availaiblity.
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 the correct OSPF configuration for Local and Peer Appliance.
14. Verify that the hit count increases for OSPF routes with low cost under the view **Monitor** > **Statistics** > **Routes**.

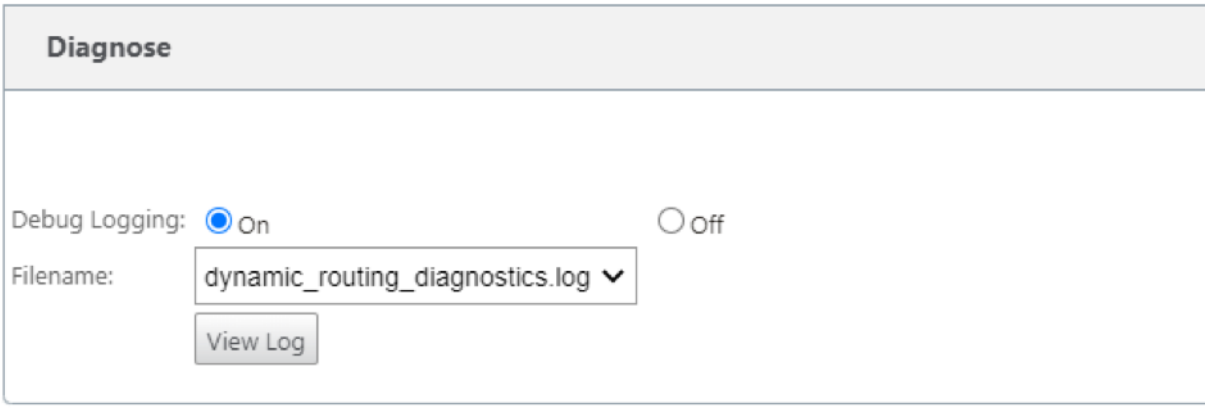
Troubleshooting

You can view the OSPF parameters under **Monitoring >Routing Protocols**.





You can also observe the Dynamic routing logs to see if there is any issue with OSPF Convergence.



BGP

March 12, 2021

The SD-WAN BGP routing functionality enables you to:

- Configure the autonomous system (AS) number of a neighbor or other peer router (iBGP or eBGP).
- Create BGP policies to be applied selectively to a set of networks on a per-neighbor 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**
>
> Only local preference and the IGP metric for path selection and manipulation is allowed.

Configuring Policies

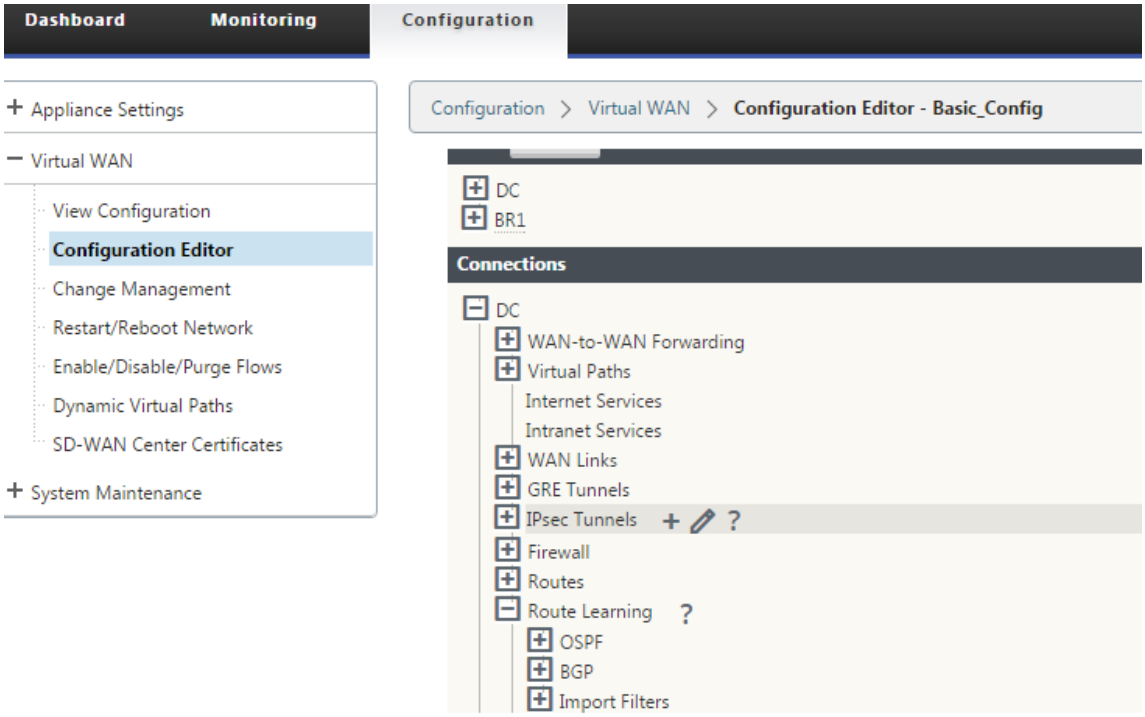
In the SD-WAN web management interface, the configuration editor has a new section, BGP policy, under **Route Learning** > **BGP**. In this section, users can add BGP attributes that constitute a policy. Adding community strings, prepending AS paths prepend, and configuring MED are supported.

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.

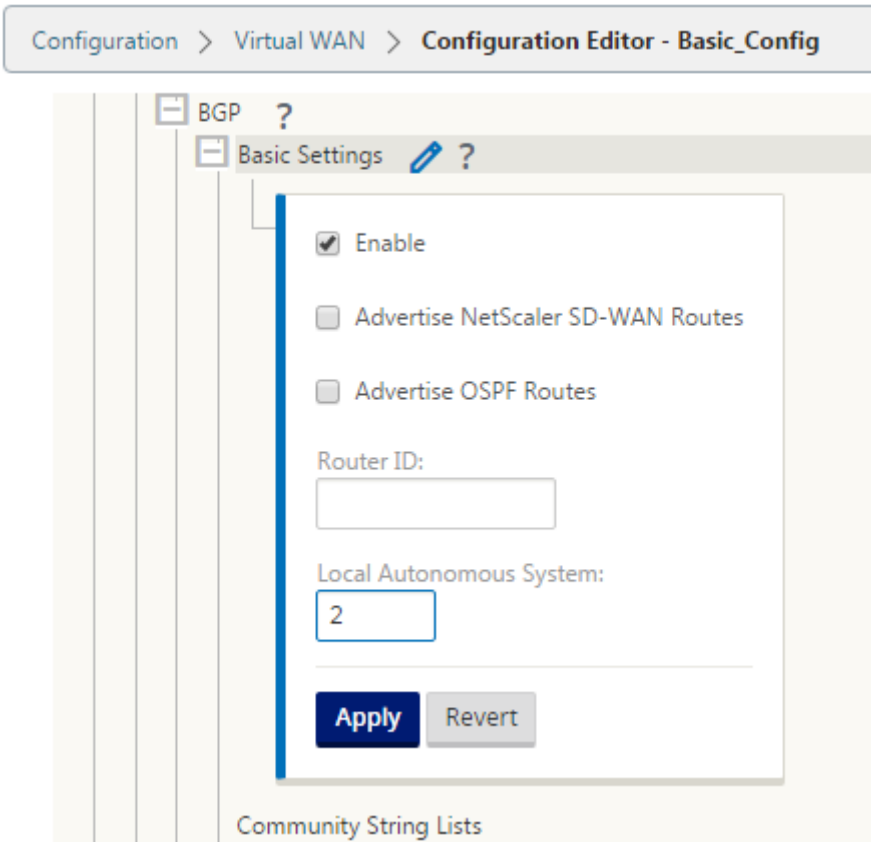
You can configure the number of times you want to prepend the local AS to the AS Path before advertising outside the local network. You can configure MED for matching routes.

To configure BGP policy:

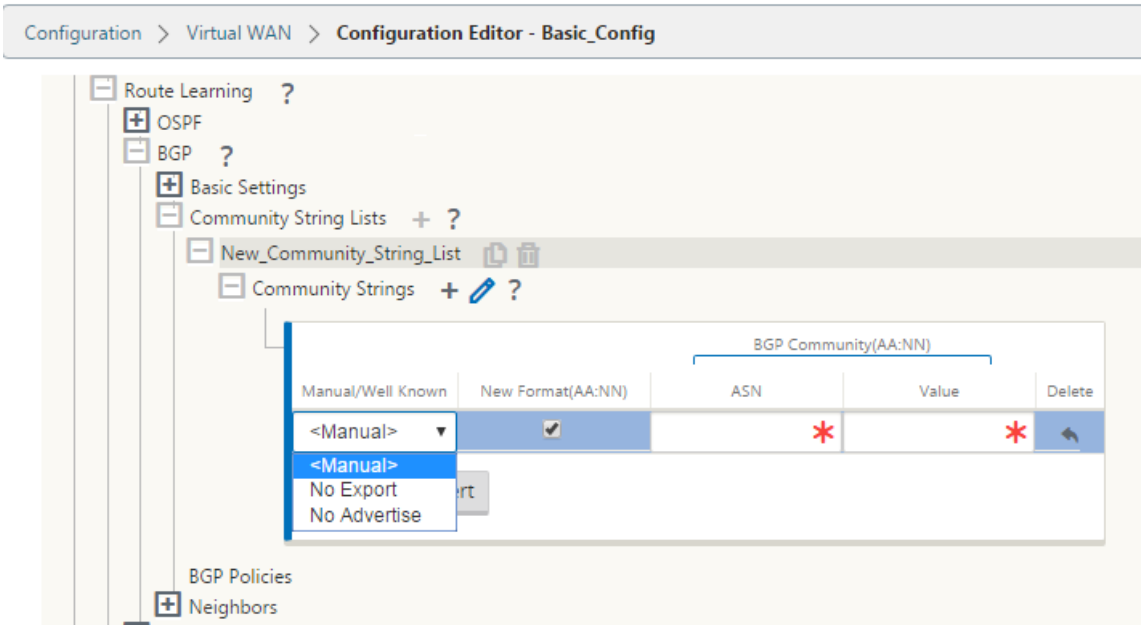
1. In the NetScaler SD-WAN web management interface, go to **Configuration** > **Virtual WAN** > **Configuration Editor**. Open an existing configuration package. Go to **Sites** > **DC** or **Branch** settings.



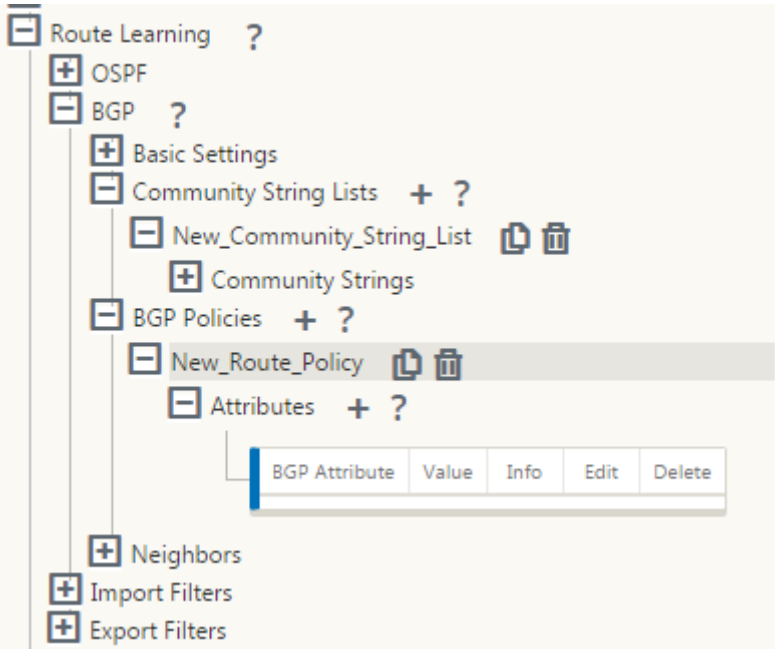
2. Expand **BGP** and click **Enable** under **Basic Settings**. Enter **Router ID** and **Local Autonomous System** value and click **Apply**.



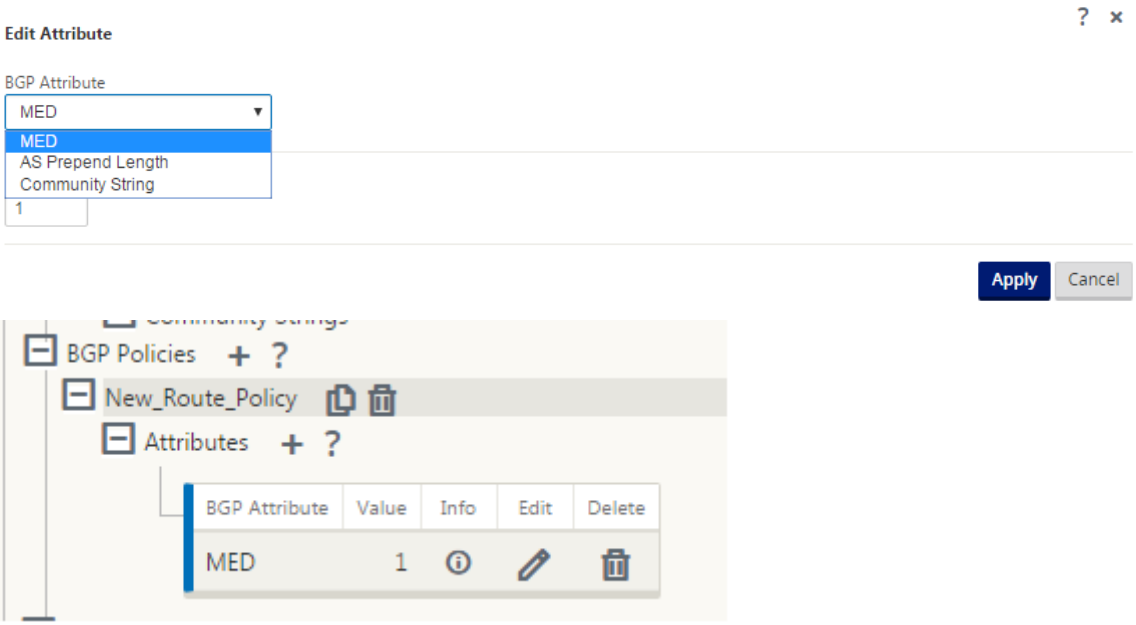
3. Click **+** sign next to the **Community String Lists**. Configure each community string manually or by selecting no advertise or no export community string from the drop-down menu. For manual configuration, you can enter an AS number and community. You can select **Insert/Remove** tag the routes 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 occurrences 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 extra column to the existing BGP neighbors section is added to configure the neighbor AS number. The existing configurations are pre-populated to this field with the local AS number when you import the 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.

Configuring Advanced Neighbors

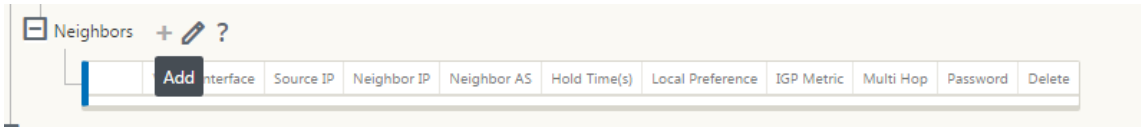
With this option, you can add network objects and add a configured BGP policy for that network object. This is similar to creating a route map and ACL to match certain routes and configuring BGP attributes for that neighbor. You can specify the direction to indicate if this policy is applied for incoming or outgoing routes.

The default policy is to <accept> all routes. Accept and reject policies are defaults and cannot be modified.

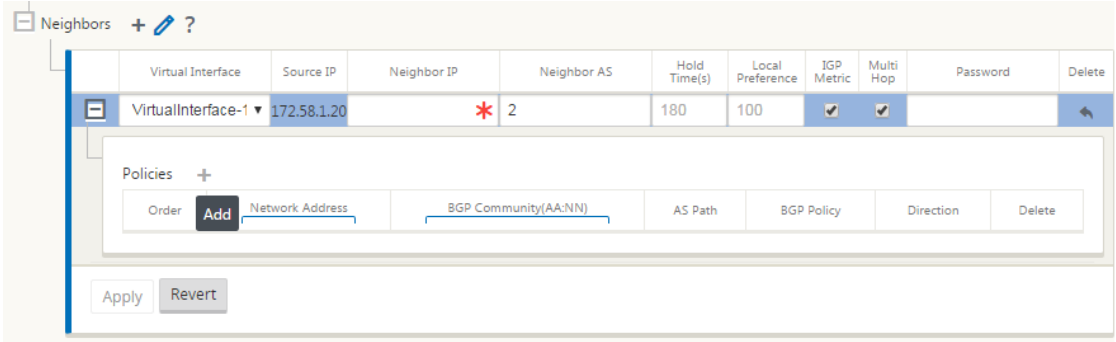
You have the ability to match routes based on Network address (destination address), AS Path, Community string and assign a policy and select direction for the policy to be applied.

To configure neighbors:

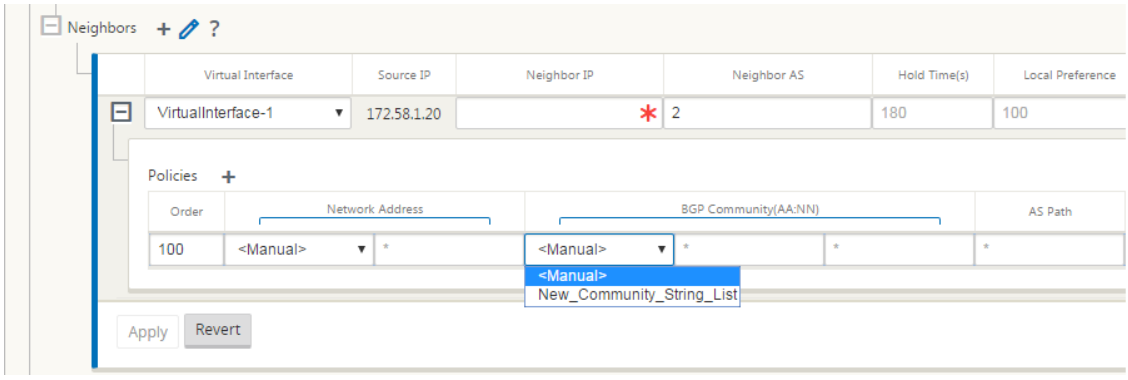
1. Configure neighbors by clicking **Add** as shown below.

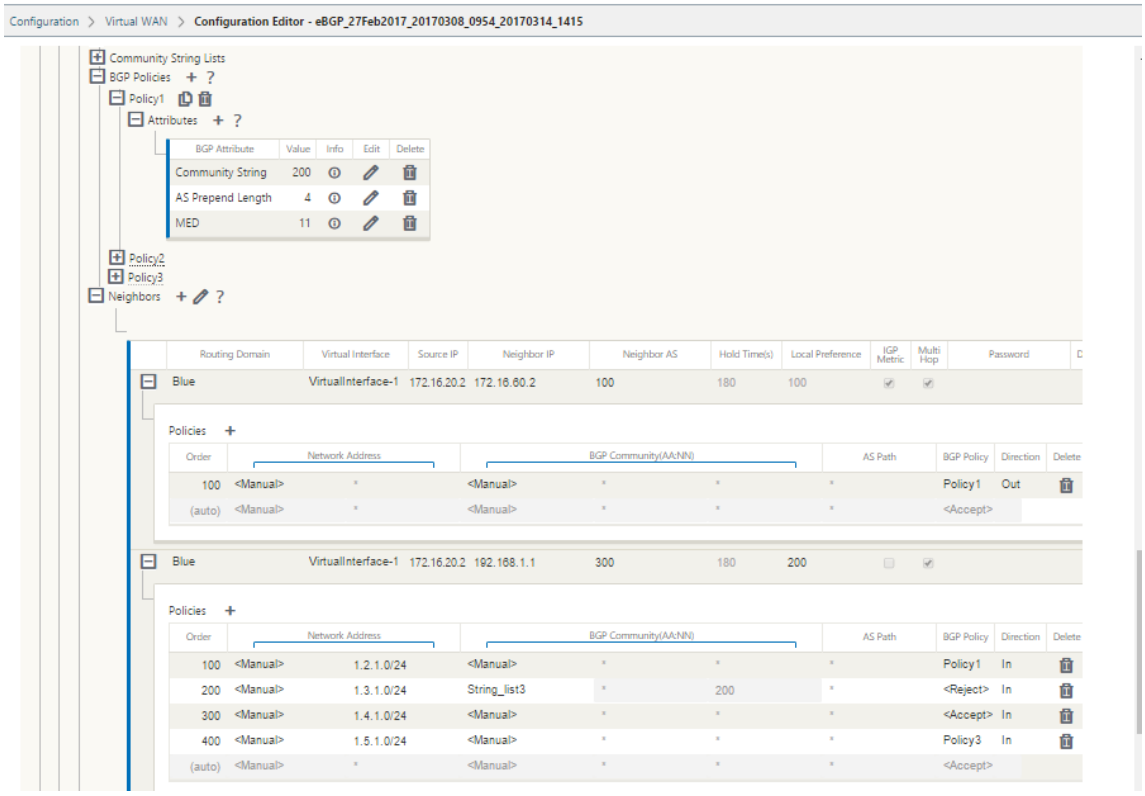


2. Click the **+** sign. Select a **Virtual Interface**. Enter the **Neighbor IP** address.



3. Add policies. Select **Network Address**, **BGP Community**, and **AS Path** details as desired. Click **Apply**.





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

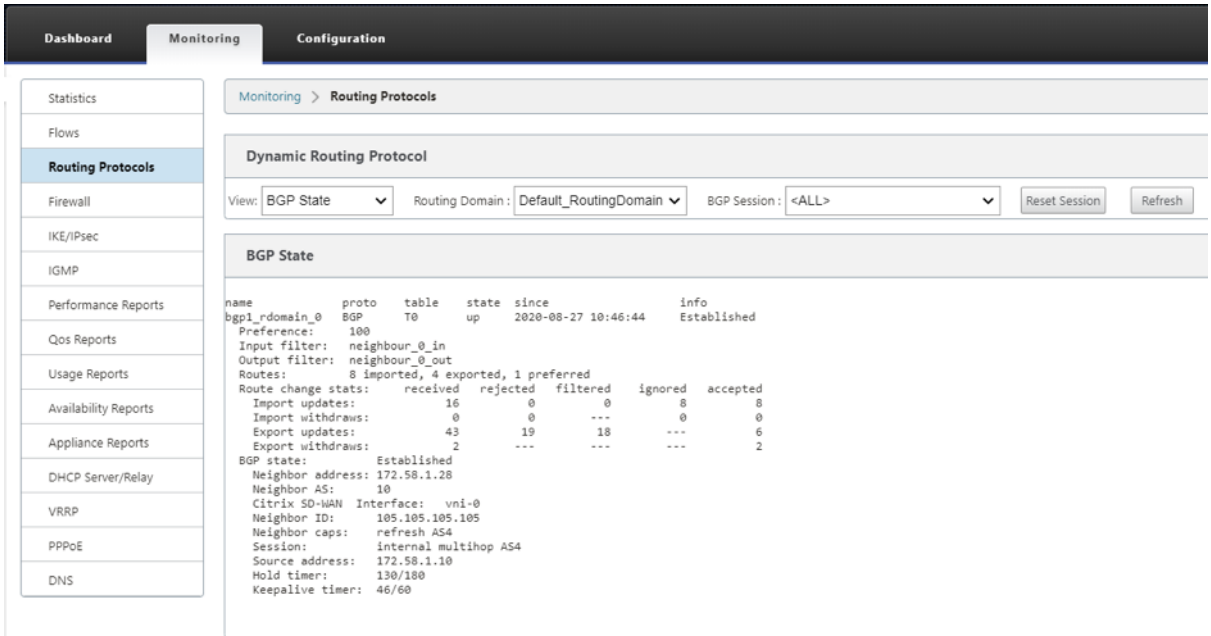
Routing policies for BGP peer include configurations such as route-map, distribute-list, prefix-list, and filter-list that might impact inbound or outbound routing table updates. When there is a change in the routing policy, the BGP session must be cleared, or reset, for the new policy to take effect.

Clearing a BGP session using a hard reset invalidates the cache and results in negative impact on the operation of the networks as the information in the cache becomes unavailable.

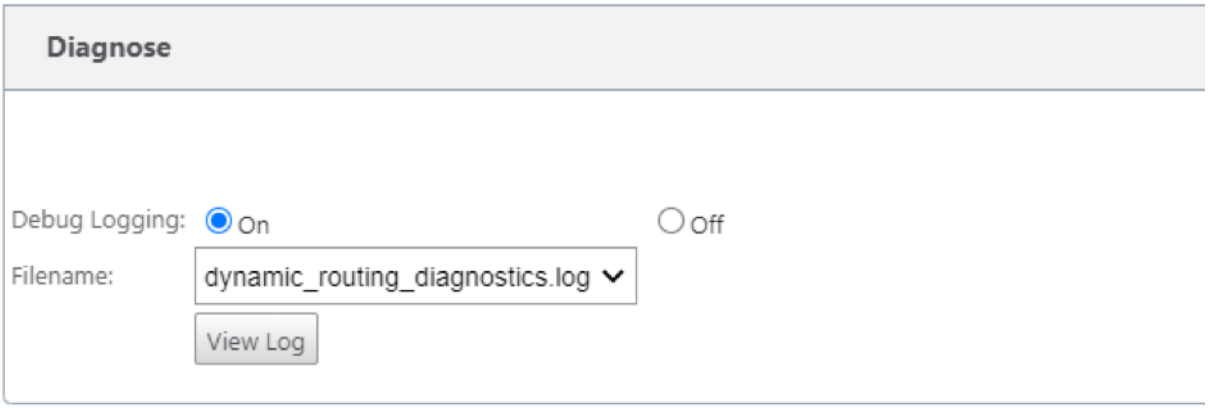
The BGP Soft Reset Enhancement feature provides automatic support for dynamic soft reset of inbound BGP routing table updates that are not dependent upon stored routing table update information.

Troubleshooting

To view the BGP parameters, navigate to **Monitoring > Routing Protocols** > select **BGP State** from the **View** field.



You can observe theDynamic routing logs to see if there is any issue with BGP Convergence.



iBGP

March 12, 2021

Citrix SD-WAN appliance with iBGP on the LAN side and eBGP on the WAN side:

Citrix 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 Citrix 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

March 12, 2021

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

March 12, 2021

In a typical enterprise network, the branch offices access applications on the on-premises 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.

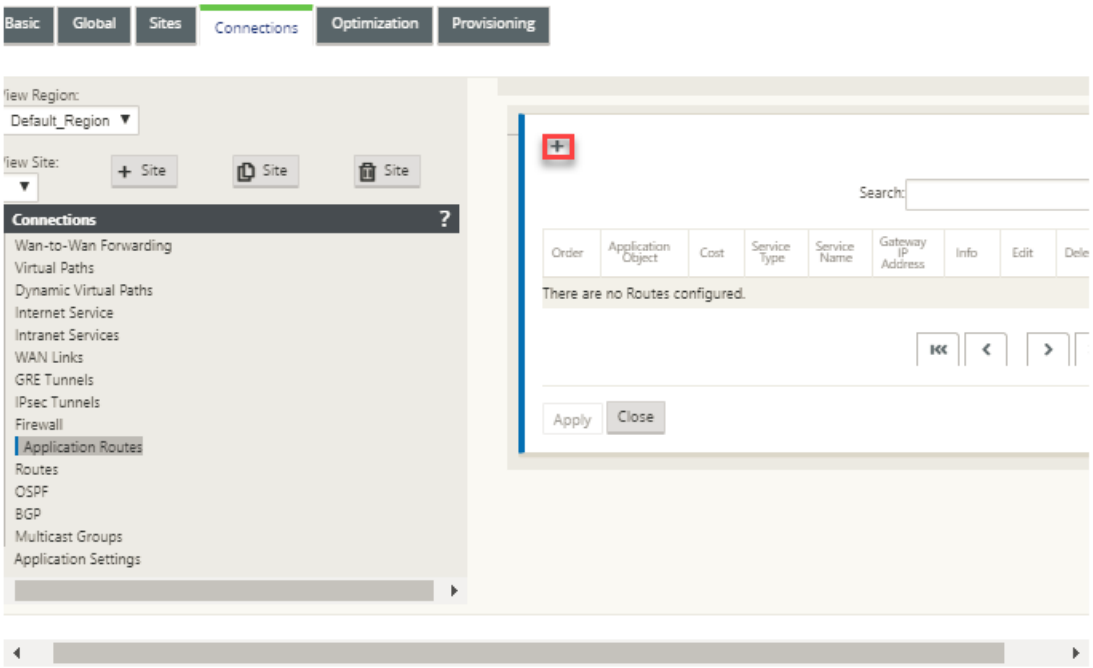
Citrix SD-WAN allows you to define the application routes for the following services:

- **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.

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.

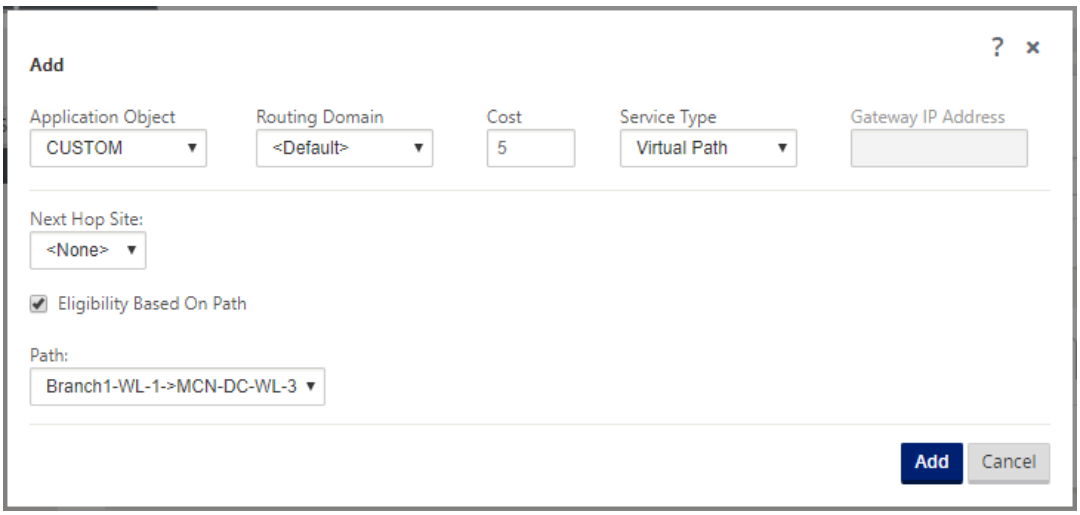
To configure application routing:

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 are directed.

  > **Note**
  >
  > Any flow hitting the Virtual Path Application Routes does 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 is ignored.

  > **Note**
  >
  > For local service type, once the DPI classification is completed the configured IP routes take the routing decision.

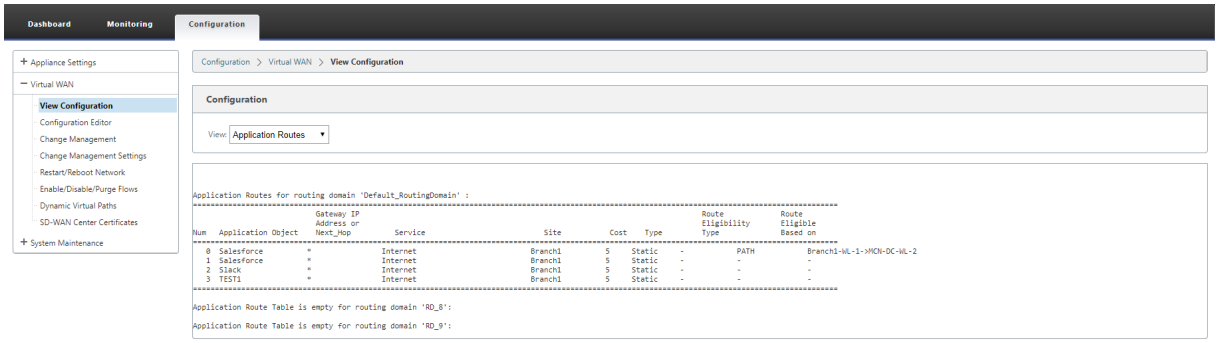
- **GRE Tunnel**: Identified the application traffic as destined for a GRE tunnel, and matches the LAN GRE tunnel configured at the site. In **the Gateway IP Address** field, enter the gateway IP Address that must be in the LAN GRE Tunnel's subnet. Select **Eligibility Based on Gateway** to enable the 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.

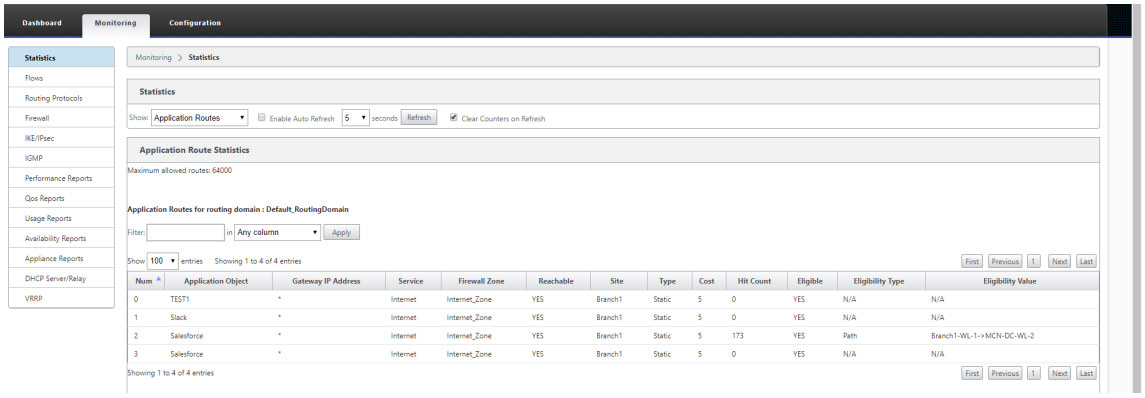
3. Click **Apply**.

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.

Troubleshooting

After creating the application route, you can confirm that the application is correctly routed to the intended service using the **Monitoring** section.

To view if the application is correctly routed to the intended service, navigate to the following pages:

- **Monitoring > Statistics > Application Routes**
- **Monitoring > Flows**
- **Monitoring > Firewall**

If there is any unexpected routing behavior, collect the STS diagnostics bundle while the issue is being observed, and share it with the Citrix Support team.

The STS bundle can be created and downloaded using **Configuration > System Maintenance > Diagnostics > Diagnostic Information**.

Route filtering

March 12, 2021

For networks with Route Learning enabled, Citrix SD-WAN provides more control over which SD-WAN routes are advertised to routing neighbors rather and which routes are received from routing neighbors, rather than advertising and accepting all or no routes.

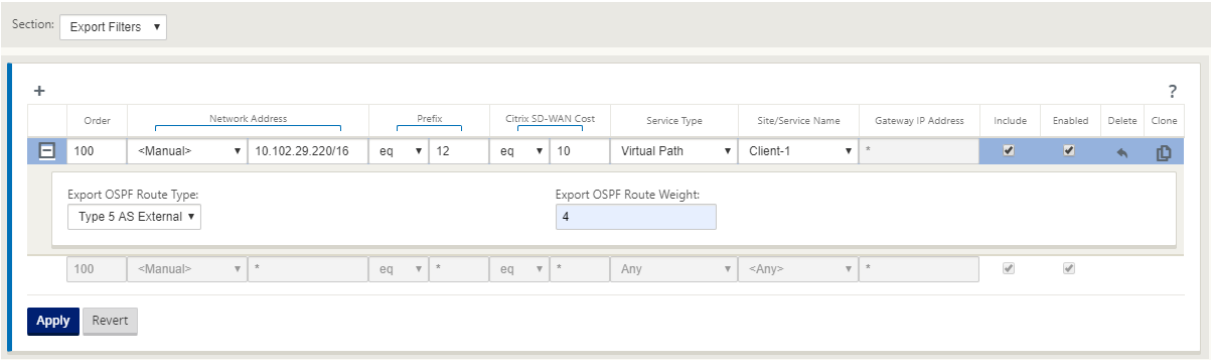
- Export Filters are used to include or exclude routes for advertisement using OSPF and BGP protocols based on specific match criteria. Export filter rules are the rules that have to be meet when advertising SD-WAN routes over dynamic routing protocols. All the routes are advertised to peers by default.
- Import Filters are used to accept or not accept routes which are received using OSPF and BGP neighbors based on specific match criteria. Import filter rules are the rules that have to be meet before importing dynamic routes into the SD-WAN route database. No routes are imported by default.

Route filtering is implemented on LAN routes and Virtual Path routes in an SD-WAN network (Data Center/Branch) and is advertised to a non-SD-WAN network through using BGP and OSPF.

You can configure up to 512 Export Filters and 512 Import Filters. This is the overall limit, not per routing domain limit.

Configure export filters

In the **Configuration Editor**, navigate to **Connections > Regions > Site > OSPF** or **BGP > Export Filters**.



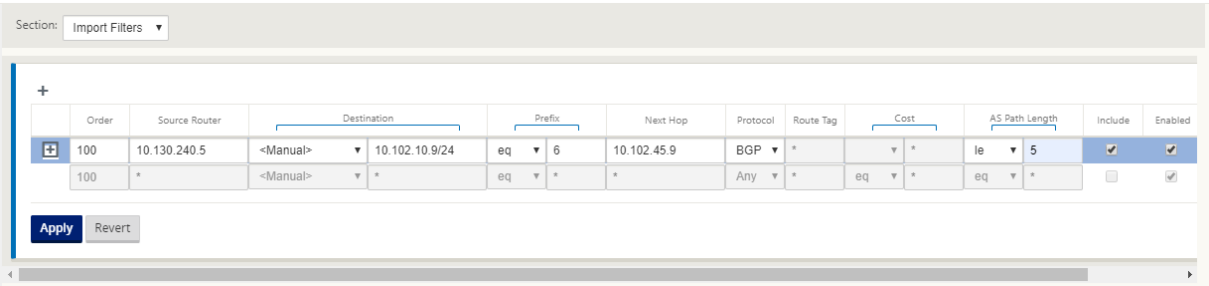
Use the following criteria to construct each Export Filter that you want to create.

Field Criteria	Description	Value
Order	The Order in which filters are prioritized. The first filter that a route matches are applied to that route	100, 200, 300, 400, 500, 600
Network Address	Enter the **IP address** and subnet mask of configured Network Object that describes the route's network	• IP address
Prefix	To match routes by prefix, choose a match predicate from the menu and enter a Route prefix in the adjacent field	• eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to
Citrix SD-WAN Cost	The method (predicate) and the SD-WAN Route Cost that are used to narrow the selection of routes exported	Numeric value

Field Criteria	Description	Value
Service Type	Select the Service types that are assigned to matching routes from a list of Citrix SD-WAN Services	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	Text string
Gateway IP Address	If you choose LAN GRE Tunnel as the Service Type, enter the gateway IP for the tunnel	IP address
Include	Select the check box to Include routes that match this filter. Otherwise matching routes are ignored	None
Enabled	Select the check box to Enable this filter. Otherwise the filter is ignored	None
Delete	Select the delete icon to delete this filter.	None
Clone	Click the clone icon to make a copy of an existing filter	None

Configure import filters

In the **Configuration Editor**, navigate to **Connections > Regions > Site > OSPF** or **BGP > Import Filters**.



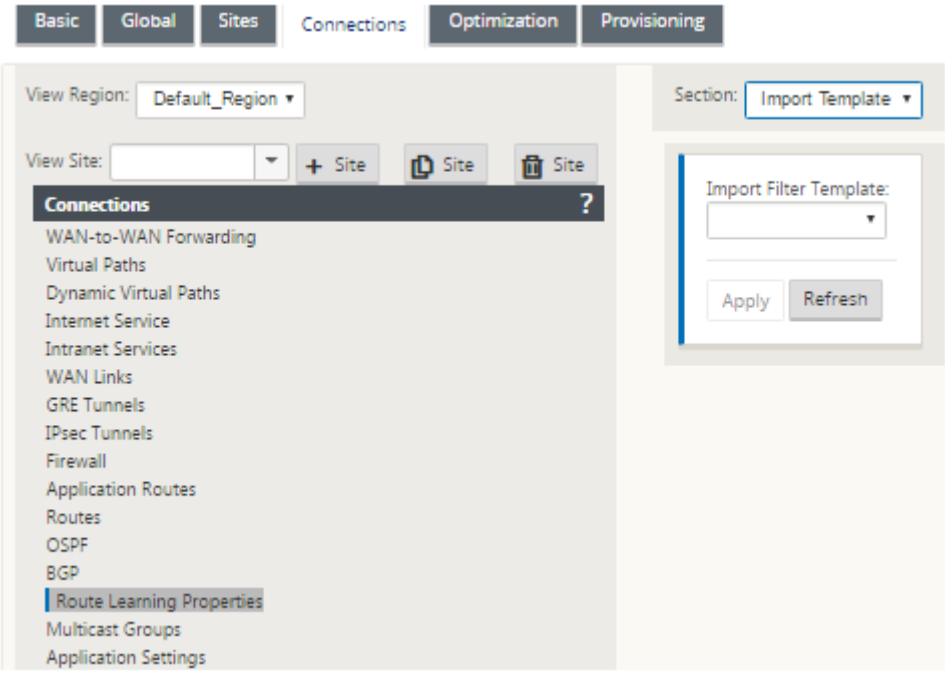
Use the following criteria to construct each Export Filter that you want to create.

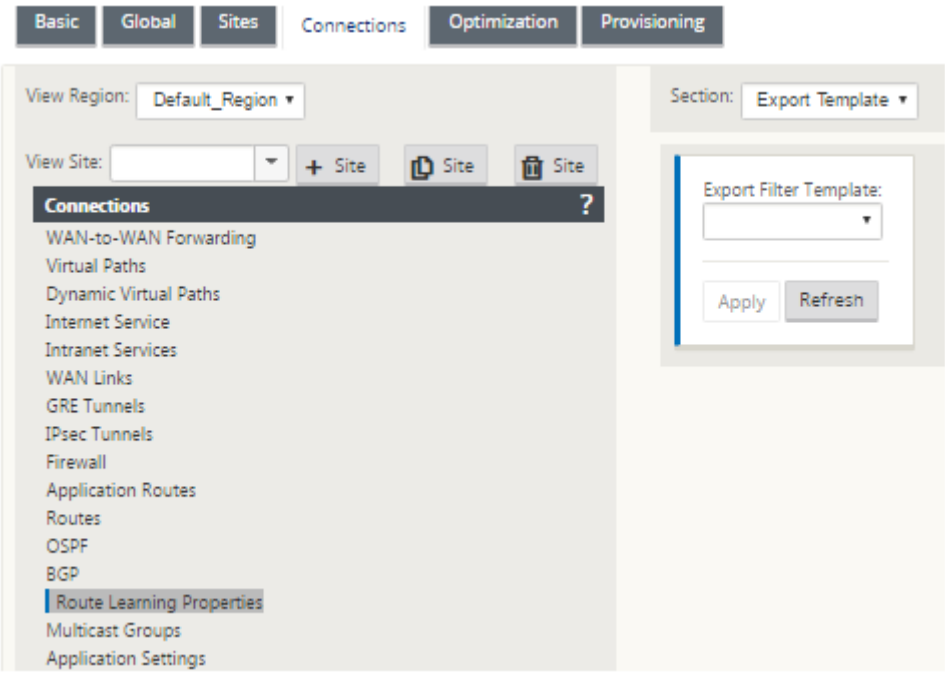
Field Criteria	Description	Value
Order	The Order in which filters are prioritized. The first filter that a route matches are applied to that route	100, 200, 300, 400, 500, 600
Source Router	The IP address of the source router, it is applicable for iBGP only	• IP address
Destination	The IP address and subnet mask of a route's destination	• IP address
Prefix	To match routes by prefix, choose a match predicate from the menu and enter a Route prefix in the adjacent field	• eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to
Next Hop	The IP address of the next hop	• IP address
Protocol	The routing protocol using which a route is learned	OSPF or BGP
Route Tag	The OSPF Route tag that the filter matches. OSPF route tags prevent routing loops during mutual redistributing between OSPF and other protocols	Numeric value
Cost	The route cost used to match OSPF routes for importing	Numeric value
AS Path Length	The AS path length used to match BGP routes for importing	Numeric value
Include	Select the check box to Include routes that match this filter. Otherwise matching routes are ignored	None
Enabled	Select the check box to Enable this filter. Otherwise the filter is ignored	None
Delete	Click the delete icon to delete this filter.	None
Clone	Click the clone icon to make a copy of an existing filter	None

Configure Route Policy Filter Templates

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.





Route Summarization

March 12, 2021

With the increase in the size of the enterprise networks, the routers need to maintain the 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.

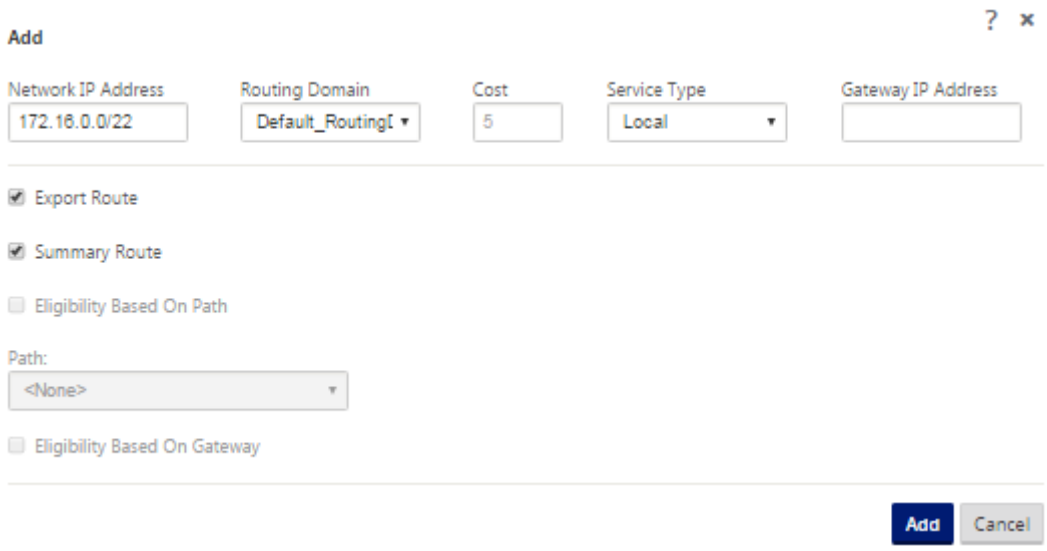
To configure a summary route for a local subnet:

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 and then click **Add**.

- **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 the 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.

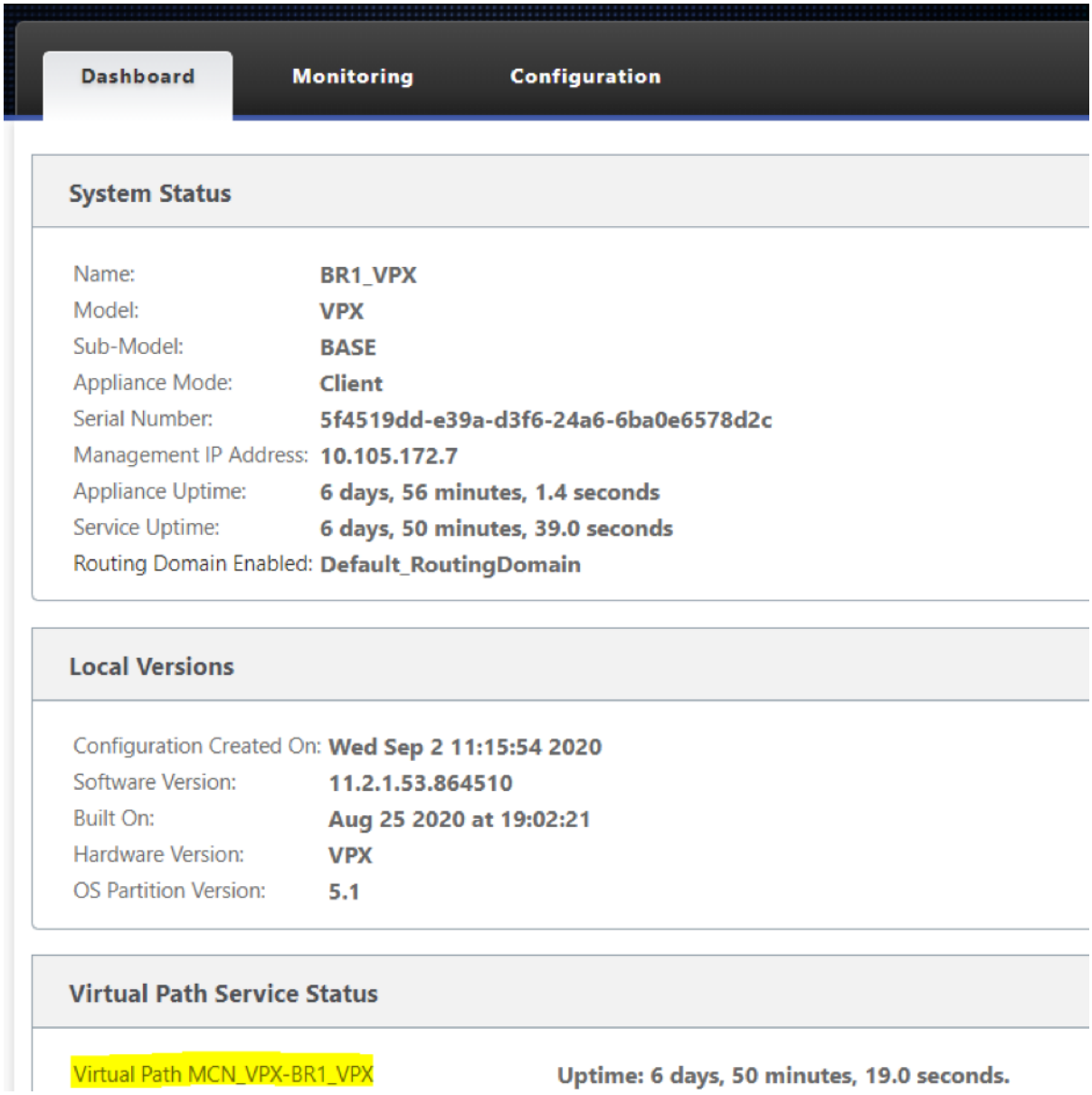
> **Note**
>
> You can select only **Local** and **Discard** service types for summary routes.

- **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.



Troubleshooting

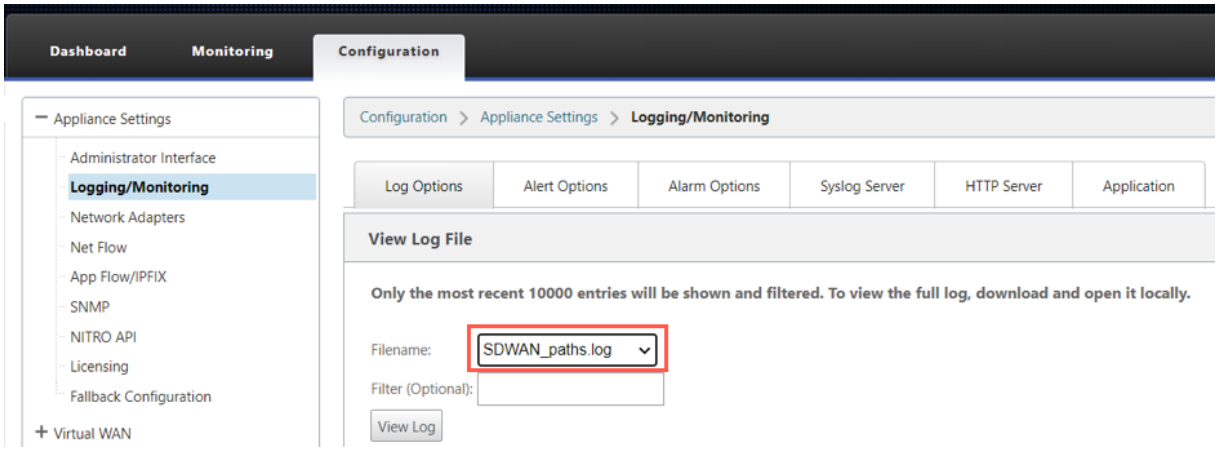
The summarized routes configured on the MCN are sent to the Branch over the virtual path. In case you do not see the virtual path details in the route table of the Branch, check the Branch dashboard. The dashboard displays the status of the virtual path between the MCN and Branch.



If the virtual path is down, check the reason for it under **Configuration > Logging/Monitoring**.

Select one of the following files from the **filename** drop-down list to verify:

- SDWAN_paths.log
- SDWAN_common.log



Protocol preference

March 12, 2021

Protocol preference is a Citrix SD-WAN specific feature, which is similar to router administrative distance.

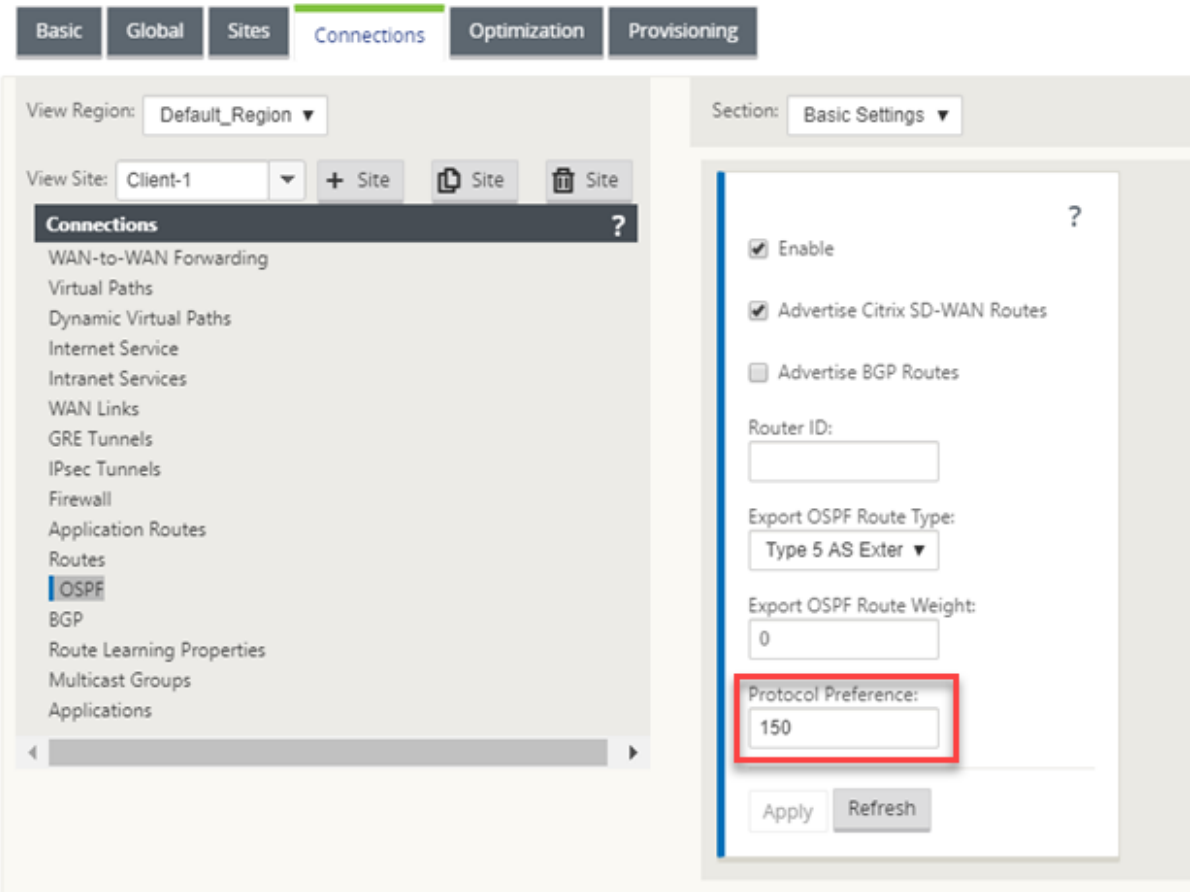
When Citrix SD-WAN learns a route prefix through virtual paths, OSPF protocol, or BGP protocol, at the same time, it follows the following default preference order.

- OSPF -150
- BGP - 100
- SD-WAN - 250

The protocol with the highest preference order is the most preferred. The route using the protocol with the highest protocol preference value

You can also choose to use the BGP protocol over the OSPF protocol by setting the protocol preference value, while configuring BGP or OSPF protocol. You can specify a preference in the range 100–200.

The protocol precedence information is local to the Citrix SD-WAN appliance and is not advertised to peer network elements.



Multicast routing

March 12, 2021

Multicast routing enables efficient distribution of one-to-many traffic. A multicast source, sends multicast traffic in a single stream to a multicast group. The multicast group contains receivers such as hosts and adjacent routers that use the IGMP protocol for multicast communication. Voice over IP, Video on demand, IP television, and Video conferencing are some of the common technologies that use multicast routing. When you enable multicast routing on the Citrix SD-WAN appliance, the appliance acts as a multicast router.

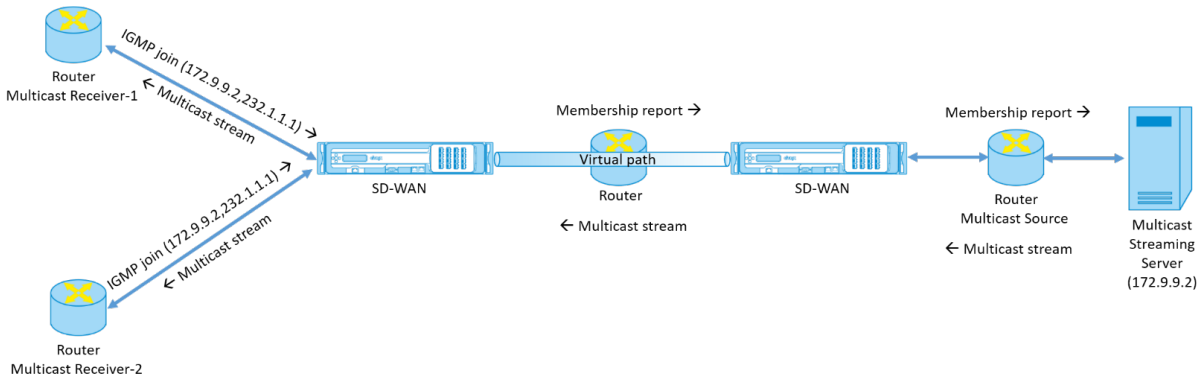
Source specific multicast

Multicast protocols typically allow multicast receivers to receive multicast traffic from any source. With source specific multicast (SSM), you can specify the source from which the receivers receive the multicast traffic. It ensures that the receivers are not open listeners to every source that is sending

multicast streams but rather listen to a particular multicast source. SSM reduces the cost of resources used in consuming traffic from every possible source and also provides a layer of security by ensuring that the receivers receive traffic from a known sender.

The following topology shows two multicast receivers at a branch site and a multicast server (172.9.9.2) at the Data Center. The multicast server streams traffic over a particular group (232.1.1.1), the receivers join the group. Any traffic streamed on the multicast group is relayed to all the receivers that joined the group.

> **Note**
>
> For SSM to work, the multicast group IP must fall within the range 232.0.0.0/8.



1. The multicast receivers send an IP IGMP join request indicating that the receivers want to join the multicast group and want to receive the multicast stream from the source. The IGMP join includes 2 attributes the multicast source and group (S, G). IGMP Version 3 is used for SSM on the multicast source and the receiver to relay some INCLUDE specific source addresses. SSM allows the receivers to explicitly receive streams from specific Multicast servers, whose source address is explicitly provided by the receivers as part of the JOIN request. In this example, an IGMP v3 join request is triggered with an explicit include source list, which contains the source 172.9.9.2, to be the address that sends the multicast stream over the group 232.1.1.1.
2. The Citrix SD-WAN at the branch listens to all the IGMP requests from these receivers and converts it into a membership report and sends it over the Virtual Path to the SD-WAN appliance at the data center.
3. The Citrix SD-WAN appliance at the data center receives the membership report over the Virtual Path and forwards it to the Multicast Source, establishing a control channel.
4. The Multicast source transmits the multicast stream over the Virtual path to the multicast receivers.

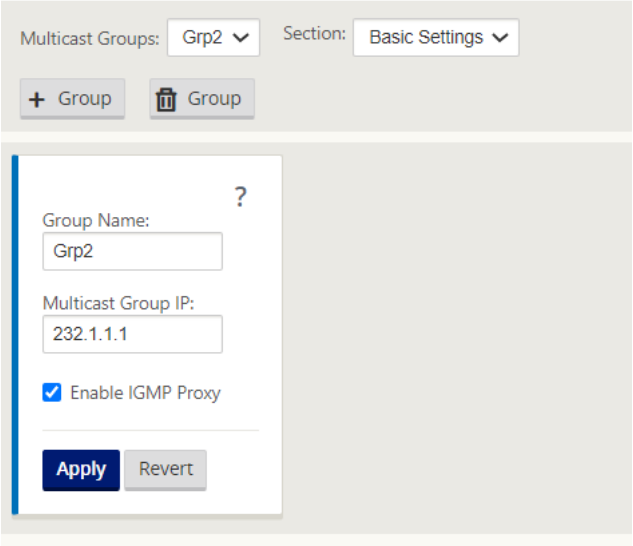
The control channel traffic and the multicast stream flow through the established virtual path between the branch and the data center. The Citrix SD-WAN overlay path insures and insulates multicast traffic from WAN degradation or link brownouts.

Configure multicast

To configure multicast, perform the following on the SD-WAN appliance at both the source and destination.

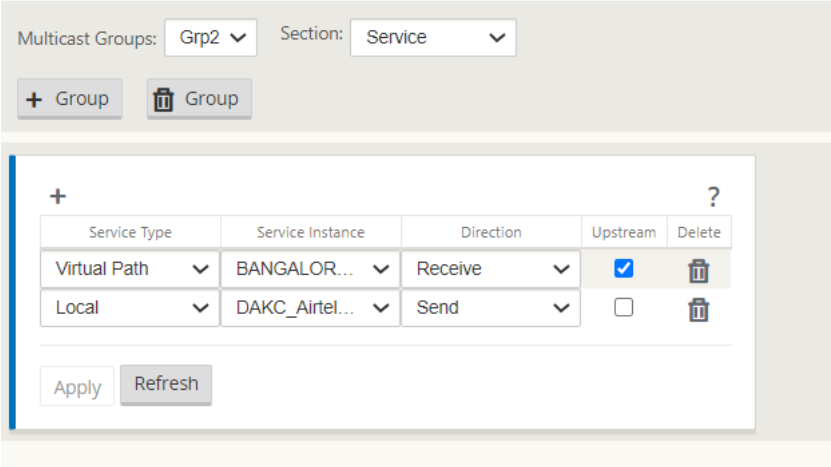
1. Create a multicast group - Provide a name and IP address for the multicast group. The multicast group IP must fall within the range 232.0.0.0/8 for source specific multicast.
2. Enable IGMP proxy –You can configure the Citrix SD-WAN appliance as an IGMP proxy to carry the IGMP control channel information for multicast routing. IGMP V3 is required for single source multicast.
3. Define the upstream and downstream services - An upstream interface enables the IGMP PROXY to connect to the SD-WAN appliance closer to the actual multicast source that streams the traffic. A downstream interface enables the IGMP Proxy to connect to the hosts that are farther away from the actual multicast source that streams the traffic.
   The upstream and downstream services are different for the appliance at the source and the appliance at the destination

To configure multicast on the Citrix SD-WAN appliance, navigate to **Connections** > **Multicast Groups**. Create a Multicast group by providing a name and IP address for the multicast group. Click **Enable IGMP Proxy**.

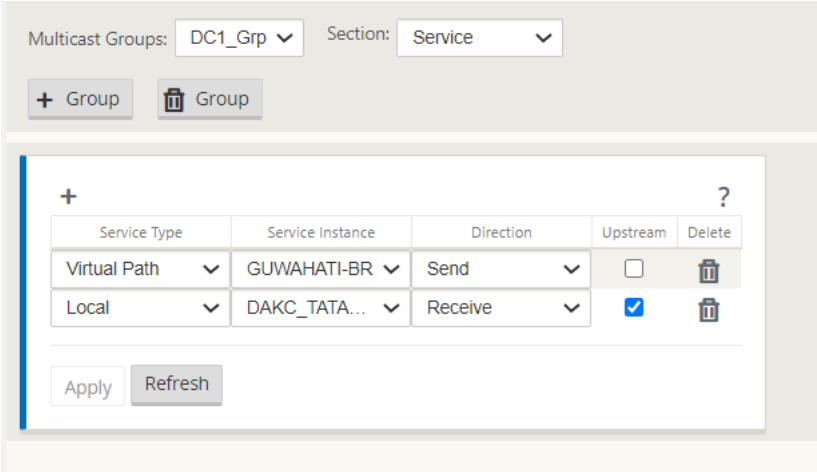


Configure the upstream and downstream paths for the Branch and data center appliances.

For the appliance closer to the multicast receiver (Branch), the appliance receives the multicast traffic on the Virtual Path Interface and sends the traffic on the Local Interface towards the receiver.



For the appliance closer to the multicast source (Data center), the appliance receives the multicast traffic on the Local Interface and sends the traffic on the Virtual Path Interface.

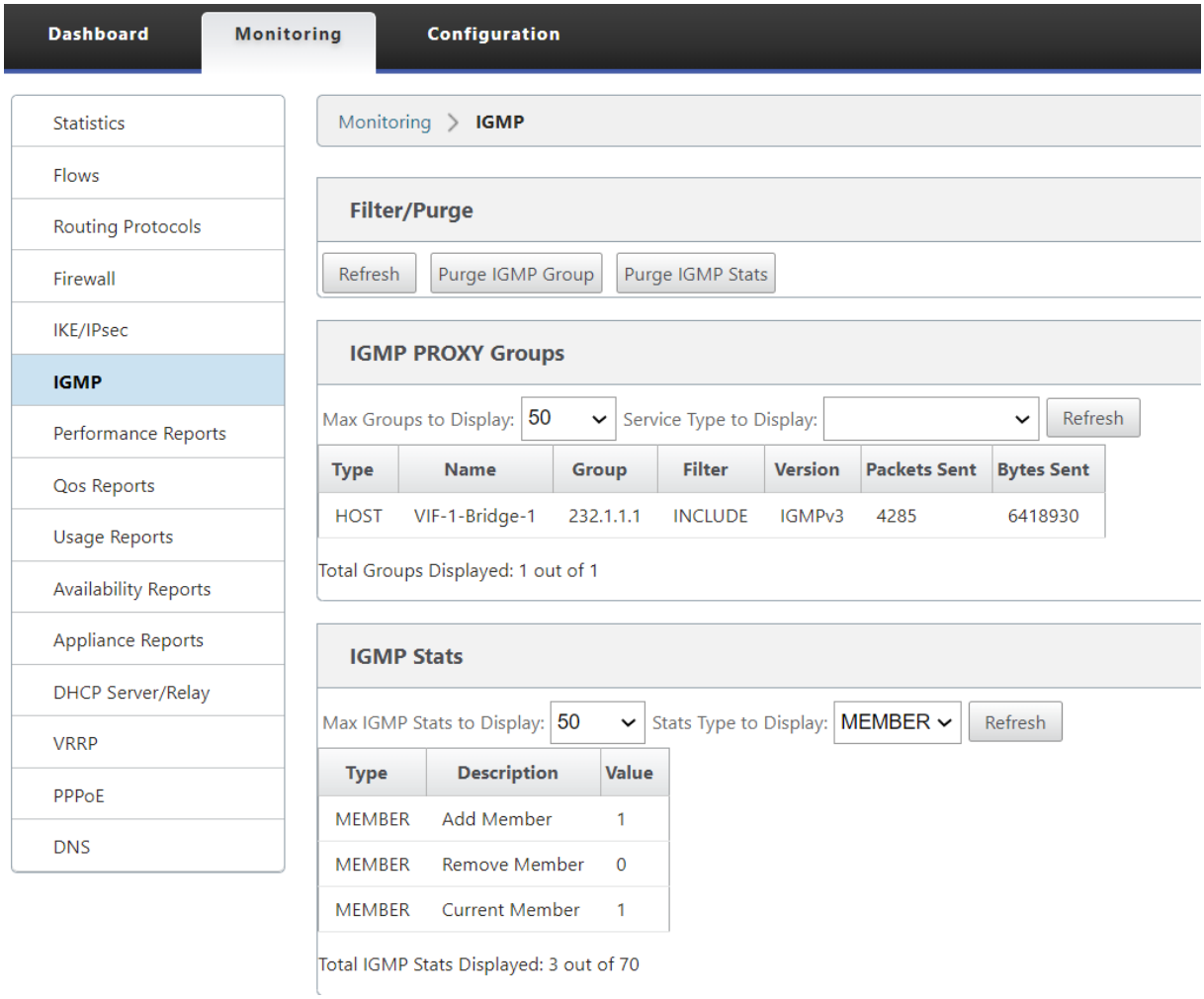


Monitoring

IGMP statistics

When the multicast receivers initiate a join group request, you can see the receiver details under **Monitoring** > **IGMP** on the appliance. You can see this information on the appliances at both the source and the destination.

The following image shows an IGMP Version 3 join is initiated and the filter type INCLUDE is used to include specific source addresses. You can also see the IGMP member statistics.



Configure Virtual Path Route Cost

March 12, 2021

Citrix SD-WAN supports the following routing enhancements related to data center administration.

For example, consider the 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 data center in North America and all sites in Europe to use the Europe data center. Previously, in SD-WAN 9.3 and earlier release versions, this functionality of data center administration was not supported. This is implemented with the introduction of Virtual Path Route cost.

- Virtual Path Route cost: You can configure the Virtual Path route cost for individual virtual paths that are added to the route cost when a route is learned from a remote site.

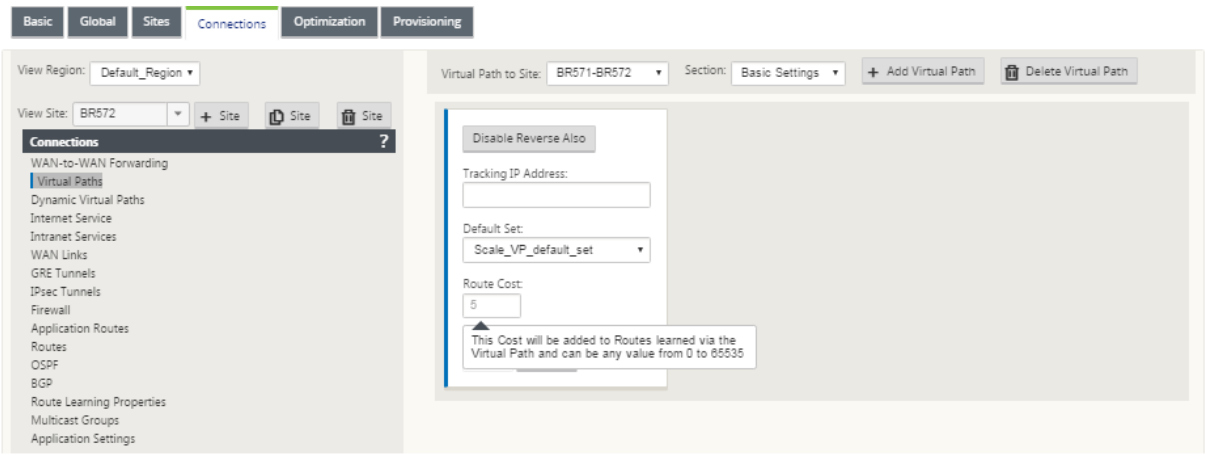
This feature invalidates or deletes the WAN to WAN forwarding Cost.

- OSPF Route Cost: You can now import OSPF route cost (type1 metric) by enabling **Copy OSPF Route Cost** in the 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 an appropriate virtual path route cost that is added if the route is learned from a remote site.
- BGP - VP cost to MED: You can now copy the 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.
- Any site can have multiple virtual paths to other sites. Sometimes, 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 can be an MCN and DC2 can be a Geo-MCN, and can be configured as another site with Static Virtual Path.
- 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.
- Allow cost to be configured within a small range of values (for example; 1–10) for each VP.
- Virtual path cost must be added to any route shared with neighbor sites to indicate routing preference, including routes learned via Dynamic Routing.
- No Static Virtual Path must 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 release version 10.0. The routing decisions based on WAN to WAN forwarding costs have to be reinfluenced 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 the SD-WAN GUI under **Connections** > **View Region** > **View site > Virtual Paths > Basic Settings**. All routes are installed with basic Citrix 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 data centers DC1 and DC2 that use both these subnets to transmit traffic to SD-WAN. With the default virtual path route cost, you cannot influence routing since it depends on which route got installed first it can 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 the default VP route cost of 5. This manipulation helps install routes with DC1 first and DC2 next for both.

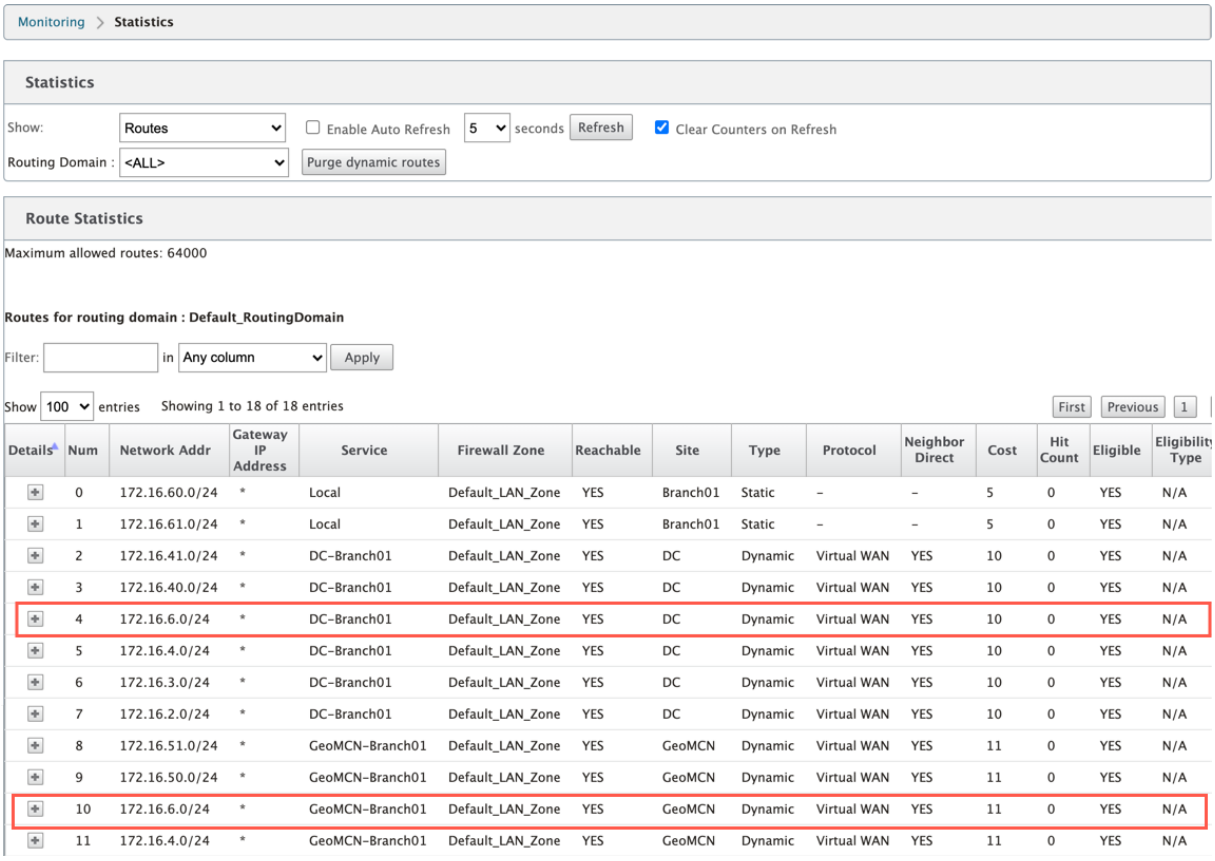
You can have four routes, two routes to 172.16.2.0/24; one via DC1 with lower cost and then via DC2 with higher cost, and 2 more for 172.16.3.0/24.

Monitoring and Troubleshooting

The routing table displays how the same subnets advertised by two sites connected to a branch site over the virtual path are installed with precedence of cost with Virtual Path route cost addition.

To verify the route cost and which routes are used in the routing table, navigate to **Monitoring > Statistics >** under **Show** field, select **Routes**. Route costs and hit counts can be verified in the same page.

The following figure 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.



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

Configure Virtual Router Redundancy Protocol

March 12, 2021

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.

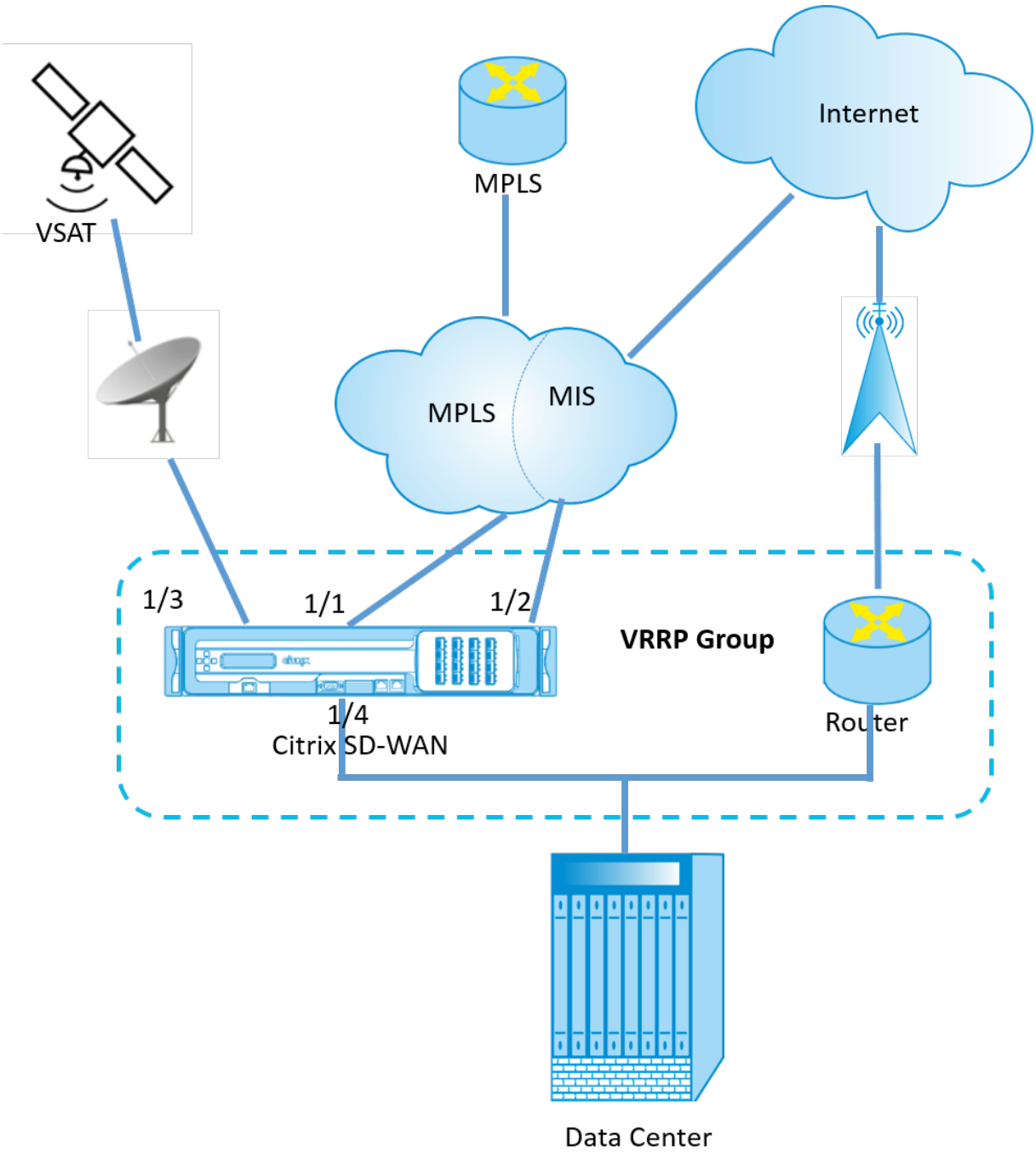
A back-up router automatically takes over if the primary / master router fails. In a VRRP set-up, the master router sends a VRRP packet known as an advertisement to the back-up routers. If the master router stops sending the advertisement, the back-up router sets the interval timer. If no advertisement 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 is the same among the routers, the router with the highest IP address becomes 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.

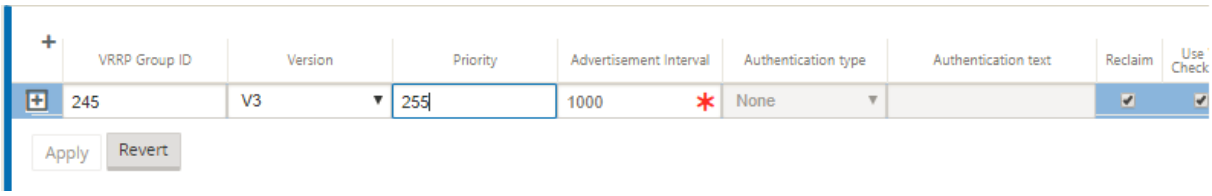
Citrix SD-WAN release version 10.1 supports VRRP version 2 and version 3 to inter-operate with any third party routers. The SD-WAN appliance acts as a master router and direct the traffic to use the Virtual Path Service between sites. You can configure the SD-WAN appliance as the VRRP master by configuring 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 Citrix 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 the VRRP instance:

1. In the Configuration Editor, navigate to **Sites > Site name > VRRP** and click **+**.



1. Configure a VRRP instance. Enter the values for the following fields:

- **VRRP group ID**: The VRRP group ID. The group ID must be a value range is 1–255. The same group ID must 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 Citrix 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 Interva**l: 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.

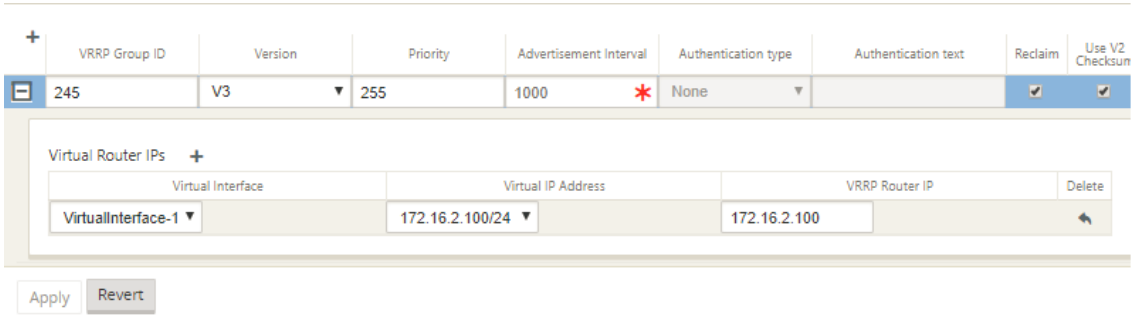
- **Reclaim:** enables preemption when the priority of the SD-WAN appliance is highest in the VRRP group. This is used in the VRRP election process.
- **Use V2 Checksum**: enables compatibility with third party network devices for VRRPv3. By default, VRRPv3 uses the v3 checksum computation method. Certain third party devices might only support VRRPv2 checksum computation. In such cases, enable this option.

Configure the VRRP IP address. Enter values for the following fields and click **Apply**.

- **Virtual Interface**: The virtual interface to be used for VRRP. Choose one of the configured virtual interfaces.

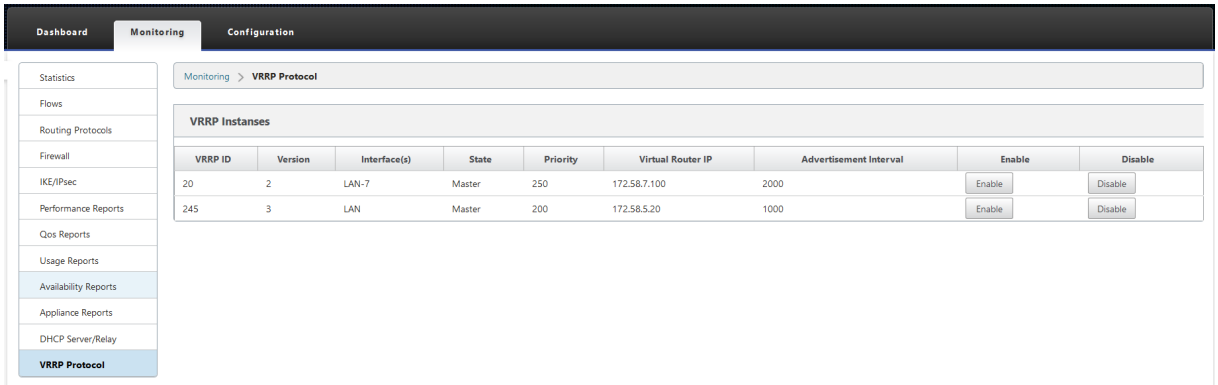
- **Virtual IP Address**: The virtual IP address assigned to the virtual interface. Choose one of the configured virtual IP addresses for the virtual interface.

- **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 Statistics

You can view the VRRP statistics under **Monitoring** > **VRRP Protocol**.



You can view the following statistics data:

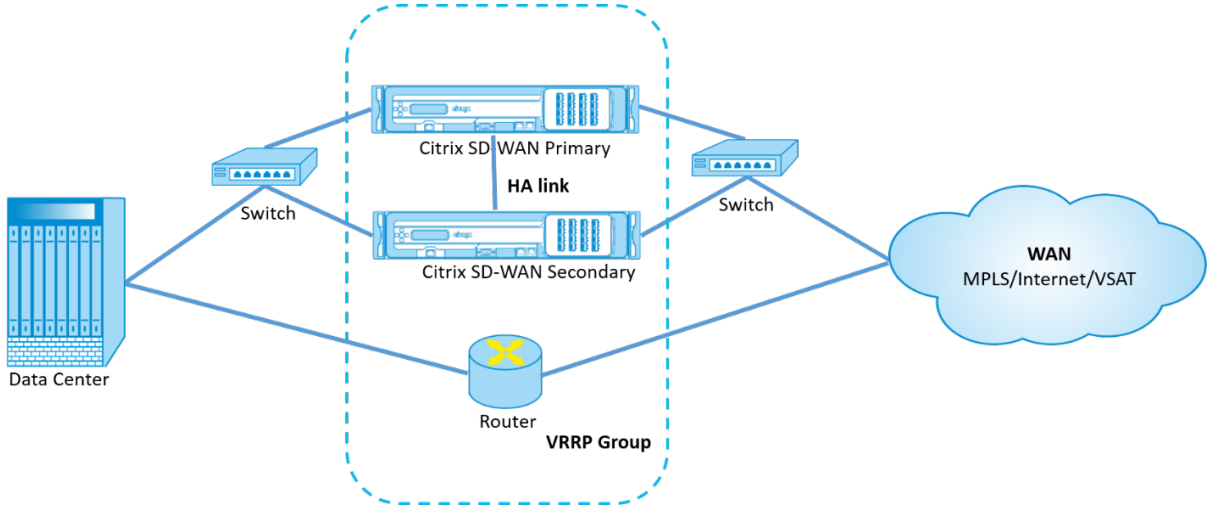
- **VRRP ID:** The VRRP group ID
- **Version:** The VRRP protocol version.
- **Interface:** The virtual interface used for VRRP.
- **State:** The VRRP state of the SD-WAN appliance. It indicates whether the appliance is a master or a backup.
- **Priority:** The priority of the SD-WAN appliance for a 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 SD-WAN appliance.
- **Disable:** Select this to disable the VRRP instance on the SD-WAN appliance.

Limitations

- VRRP is supported in Gateway Mode deployment only.
- You can configure up to four VRRP IDs (VRID).
- Up to 16 virtual network interfaces can participate in VRID.

High Availability and VRRP

You can significantly reduce network downtime and traffic disruption by leveraging both the high availability and VRRP features on your SD-WAN network. Deploy a pair of Citrix SD-WAN appliance in active/standby roles along with a standby router to form the VRRP group. This group appears as a single default gateway with one virtual IP address and one virtual MAC address.



The following are 2 cases with the above deployment:

1st case: High availability failover timer on SD-WAN equals the VRRP failover timer.

The expected behavior is high availability switchover to happen before the VRRP switchover, that is the traffic continues to flow through the new Active SD-WAN appliance. In this case SD-WAN continues with the VRRP Master role.

2nd case: High availability failover timer on SD-WAN greater than the VRRP failover timer.

The expected behavior is the VRRP switchover to the router happens, that is the router becomes VRRP Master and traffic might momentarily flow through the router, bypassing the SD-WAN appliance.

But once the high availability switchover happens, SD-WAN again becomes VRRP Master, that is the traffic now flows through the new active SD-WAN appliance.

For more information on high availability deployment modes, see High Availability.

Configure Network Objects

March 12, 2021

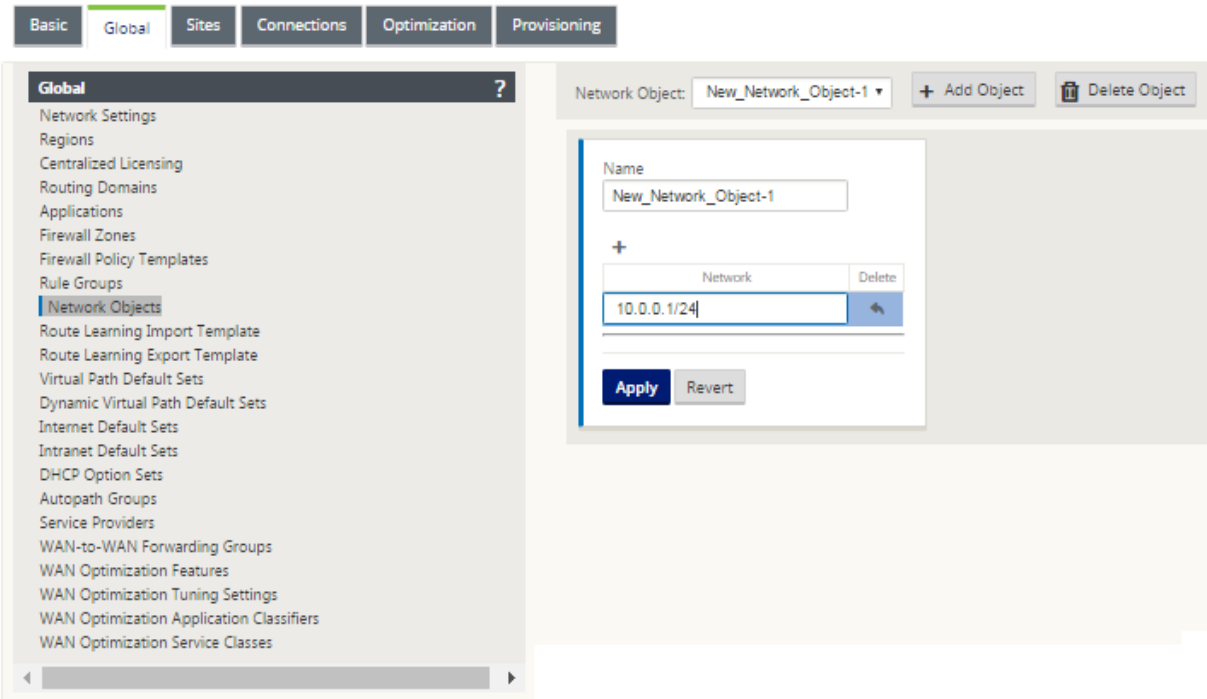
Citrix SD-WAN introduces the option of adding Network Objects under the **Global** panel in the Configuration Editor. You can group multiple subnets together and reference a single Network Object when

defining a Route Filter rather than creating a filter for each subnet.

To configure Network Objects:

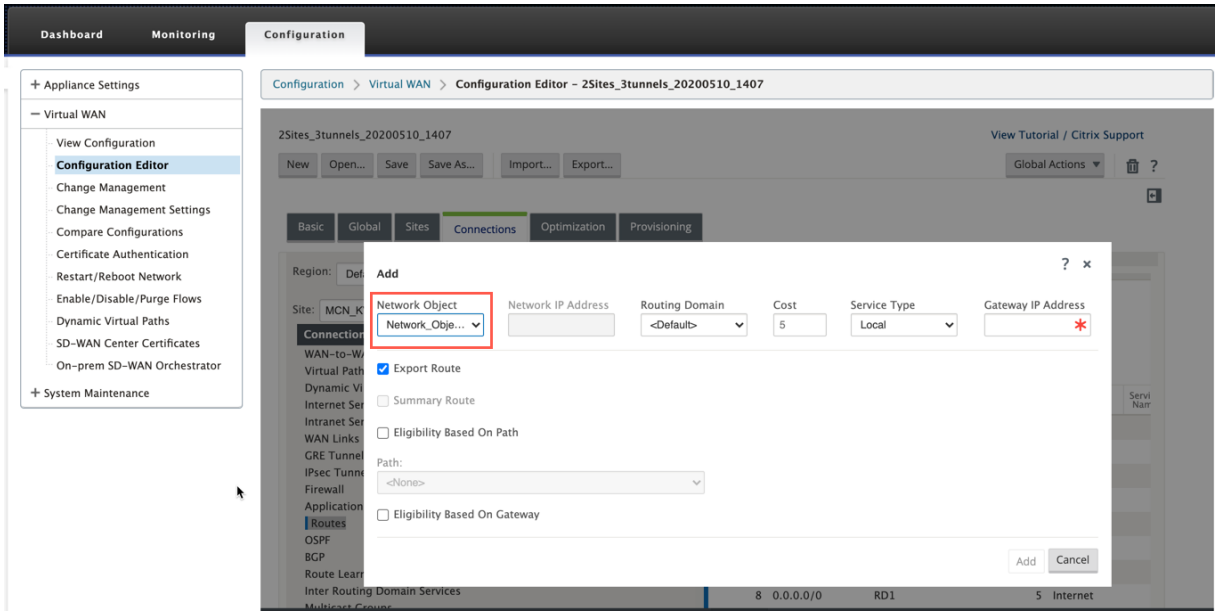
1. In the **Configuration Editor**, navigate to **Global** → **Network Objects**, click **Add (+)**.
2. Click **Add (+)** under Networks.
3. Enter the **IP Address** and **Subnet** of the new Network Object.
4. Click **Apply** to save the settings.

To edit the Network Object's name, click the name of the Network Object and enter a new name.

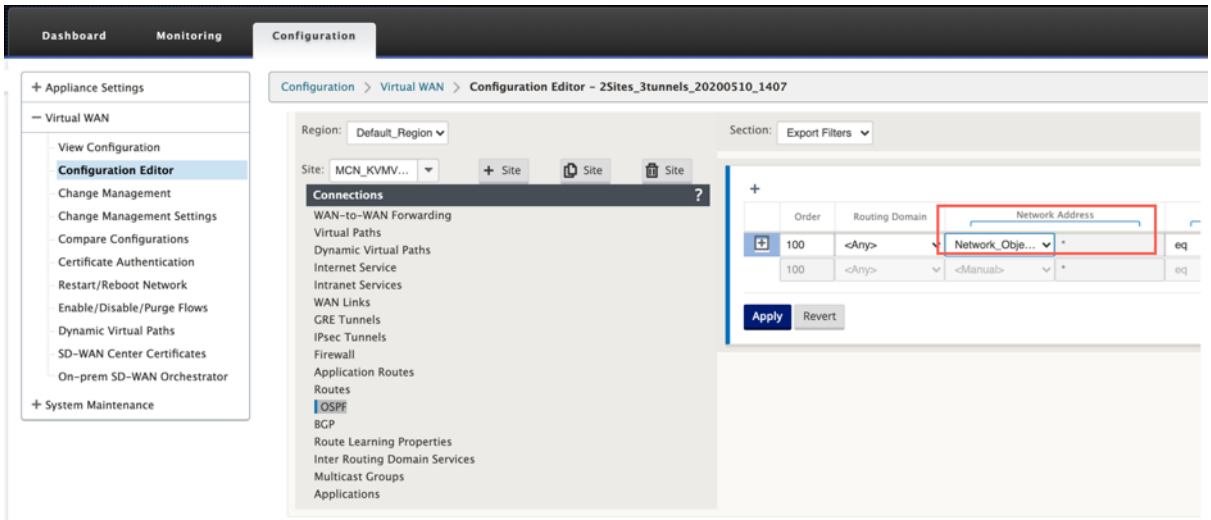


Following features are utilizing the network objects:

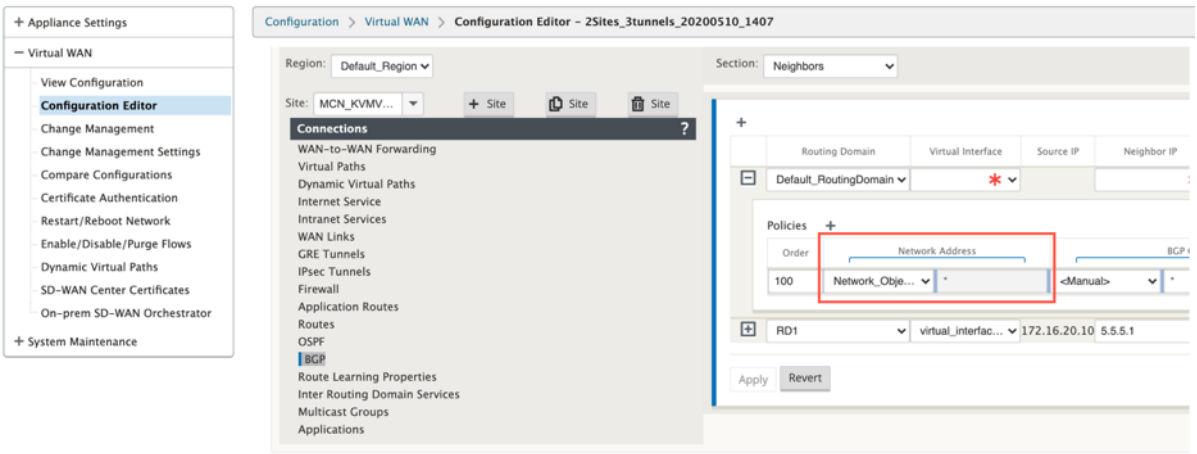
- Routes (**Configuration Editor > Connections > Routes >** Click **+** > **Network Object**)



- BGP and OSPF Import and Export Filters (**Configuration Editor > Connections > BGP/OSPF > Export/Import Filters >** click **+ > Network Address**)



- BGP Neighbor Policies (**Configuration Editor > Connections > BGP > Neighbours > Policies >** click **+ > Network Address**)



Routing Support for LAN Segmentation

March 12, 2021

The SD-WAN Standard and Premium (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 Premium (Enterprise) Edition appliance.

The above capability is implemented by using a Virtual Routing and Forwarding (VRF) table that is maintained in the SD-WAN Standard or Premium (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.

Inter-routing domain service

March 12, 2021

Citrix SD-WAN allows you to segment the network using Routing Domains, ensuring high security and easy management. With the use of the Routing Domain the traffic is isolated from each other in the overlay network. Each routing domain maintains its own routing table. For more information on Routing Domain, see Routing Domain.

However, sometimes we need to route the traffic between the Routing domains. For example if shared services such as printer, scanner, and mail server are provisioned as a separate Routing Domain. Inter-routing domain is required to enable users from different routing domains to access the shared services.

Citrix SD-WAN provides Static Inter-Routing Domain Service, enabling route leaking between Routing Domains within a site or between different sites. This eliminates the need for an edge router to handle route leaking. The Inter-routing domain service can further be used to set up routes, firewall policies, and NAT rules.

A new Firewall Zone, **Inter_Routing_Domain_Zone** is created by default and serves as the firewall zone for the Inter-Routing Domain Services for routing and filtering.

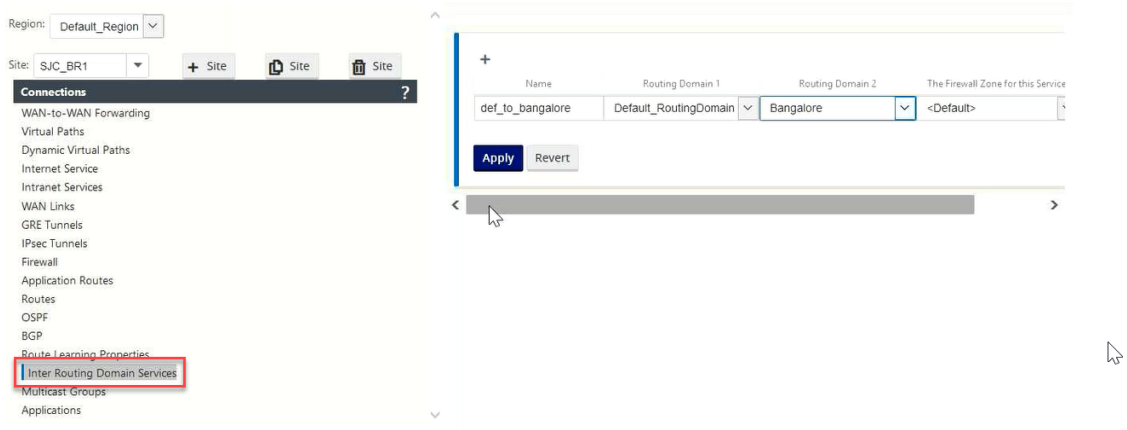
> **Note**
>
> Citrix SD-WAN PE appliances do not perform WAN optimization functionality on Inter-Routing Domain packets.

To configure Inter-routing Domain Service between two routing domains.

Consider an SD-WAN network with an MCN and 2 or more branches with at least two Routing Domains configured globally. By default, all the routing domains are enabled on the MCN. Selectively enable the required routing domains on the other sites. For information on configuring Routing Domain see, Configure Routing Domain.

1. In the SD-WAN Configuration Editor, navigate to **Connections** > Select Site > **Inter-Routing Domain Service**.
2. Click **+** and enter values for the following parameters:

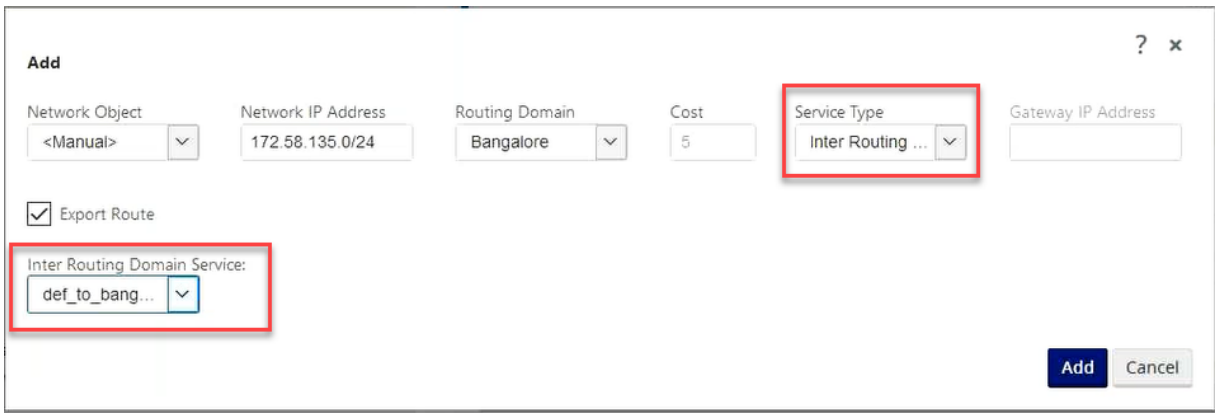
- **Name**: The name of the Inter-Routing Domain Service.
- **Routing Domain 1**: The first Routing Domain of the pair.
- **Routing Domain 2**: The second Routing Domain of the pair.
- **Firewall Zone**: The Firewall Zone of the Service.
  - Default: The Inter_Routing_Domain_Zone firewall zone is assigned.
  - None: No zone is selected and the original zone of the packet is retained.
  - All Zones configured in the network might be selected.



1. Click **Apply** to create the Inter-routing domain service. The created service can be used to create routes, firewall policies, and NAT policies.

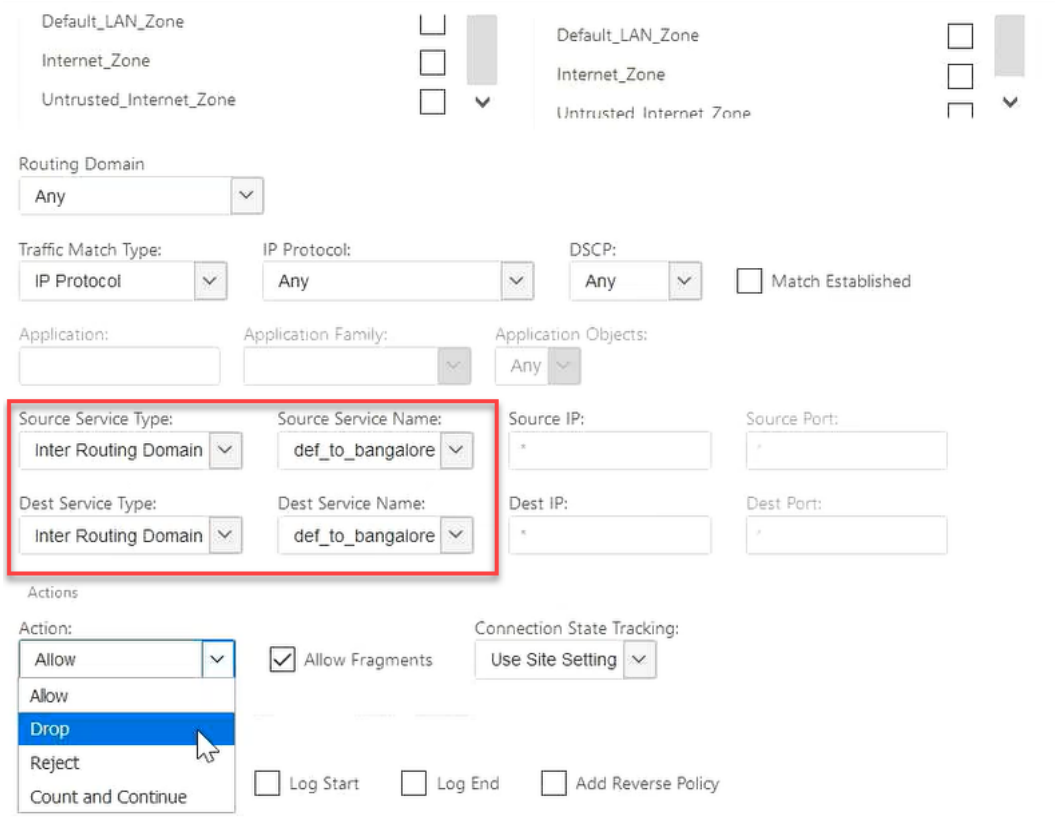
> **Note**
>
> You cannot configure an Inter-routing domain service, using routing domains that are not enabled on a site.

To create routes using the Inter-routing domain service, create a route with the **Service type** as **Inter-Routing Domain Service** and select the inter-routing domain service. For more information on configuring Routes, see How to Configure Routes.

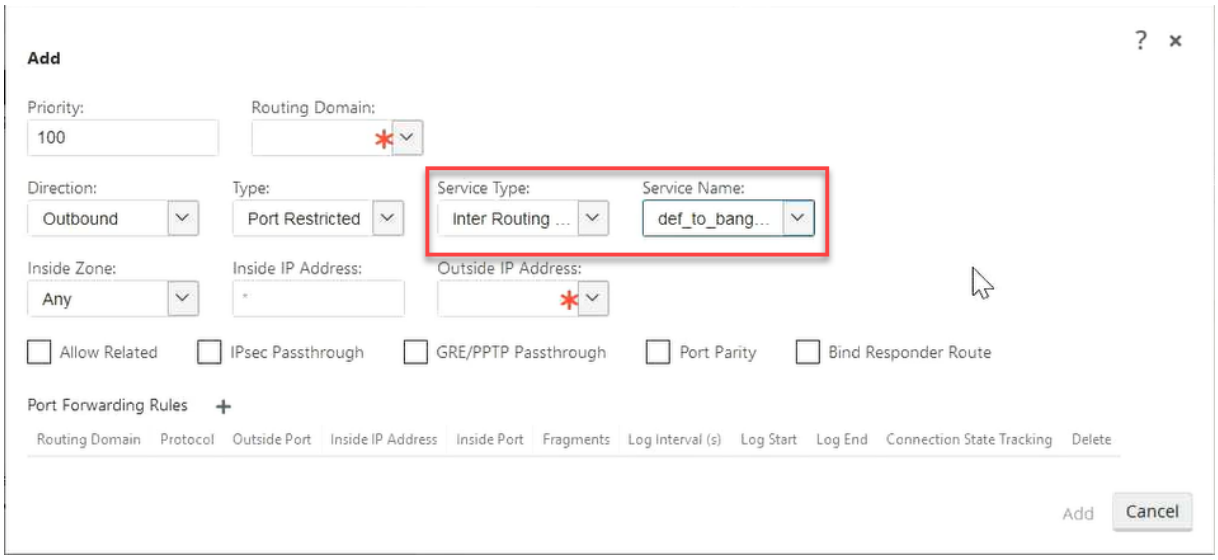


Also add a route from the other Routing Domain pair, to establish connection to and fro between the two routing domains.

You can also configure firewall policies to control the flow of traffic between routing domains. In the firewall policies, select Inter-Routing domain service for the source and destination services and select the required firewall action. For information on configuring Firewall Policies, see Policies.

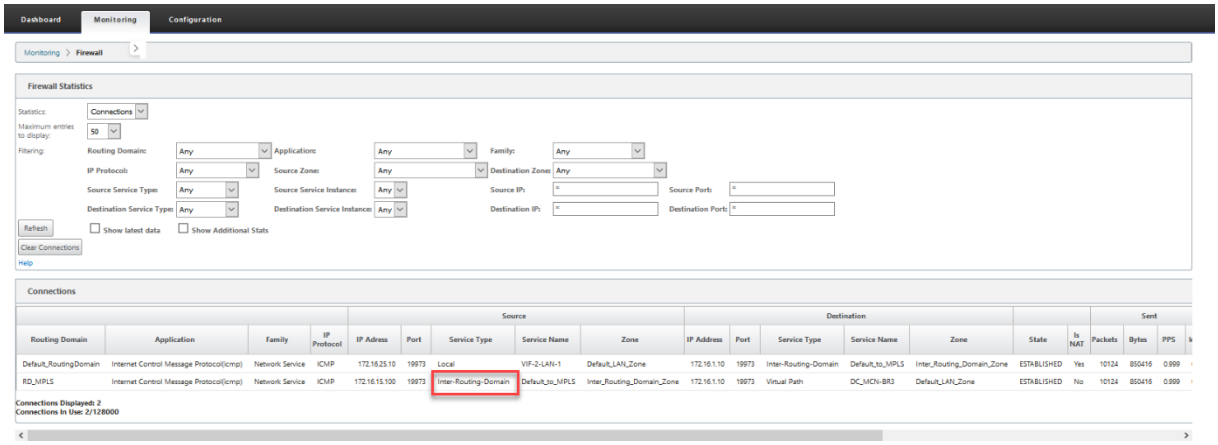


You can also choose Intranet service type to configure Static and Dynamic NAT policies. For more information on configuring NAT policies, see Network Address Translation.



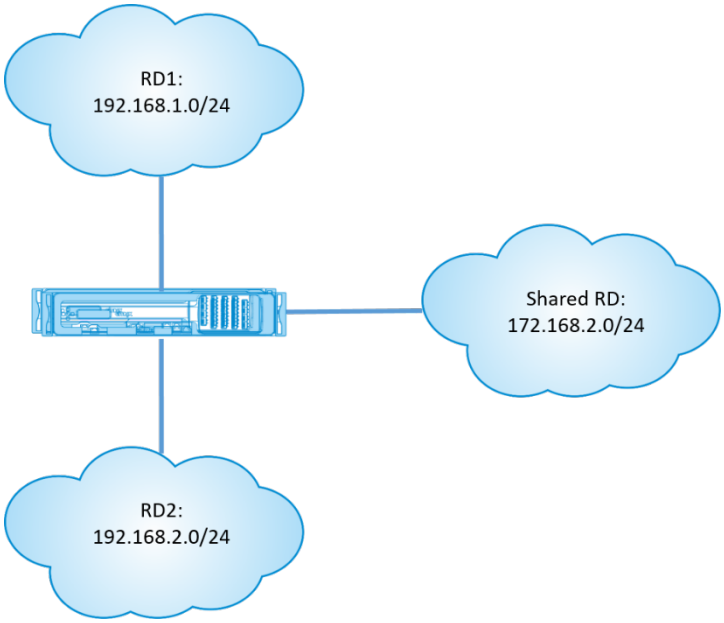
Monitoring

You can view monitoring statistics for connections that use inter-routing-domain services under **Monitoring** > **Firewall Statistics** > **Connections**.



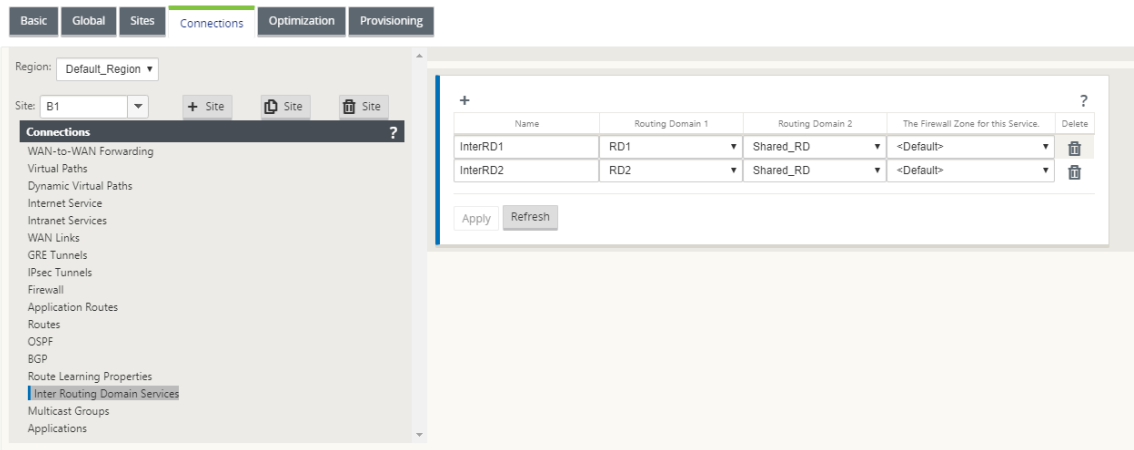
Use Case: Sharing resources across Routing Domains

Let us consider a scenario, in which users in different routing domains need to access common assets, such a printer or network storage. There are 3 routing domains at a branch RD1, RD2, and Shared RD as shown in the figure.

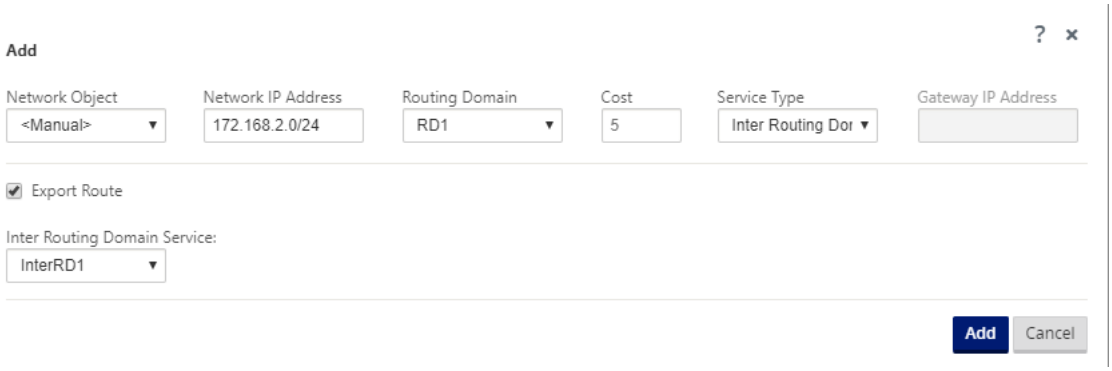


To enable users in RD1 and RD2 to access resources in Shared RD:

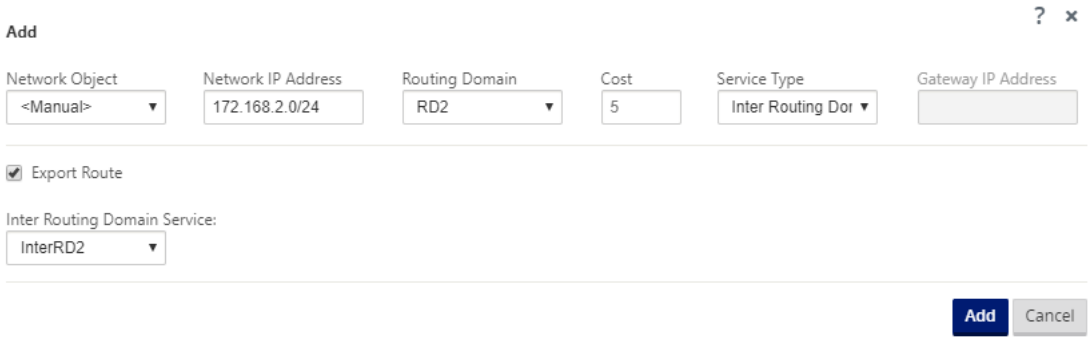
1. Create an Inter-Routing Domain service between RD1 and Shared RD, for example **Inter RD1**.
2. Create an Inter-Routing Domain service between RD2 and Shared RD, for example **Inter RD2**.



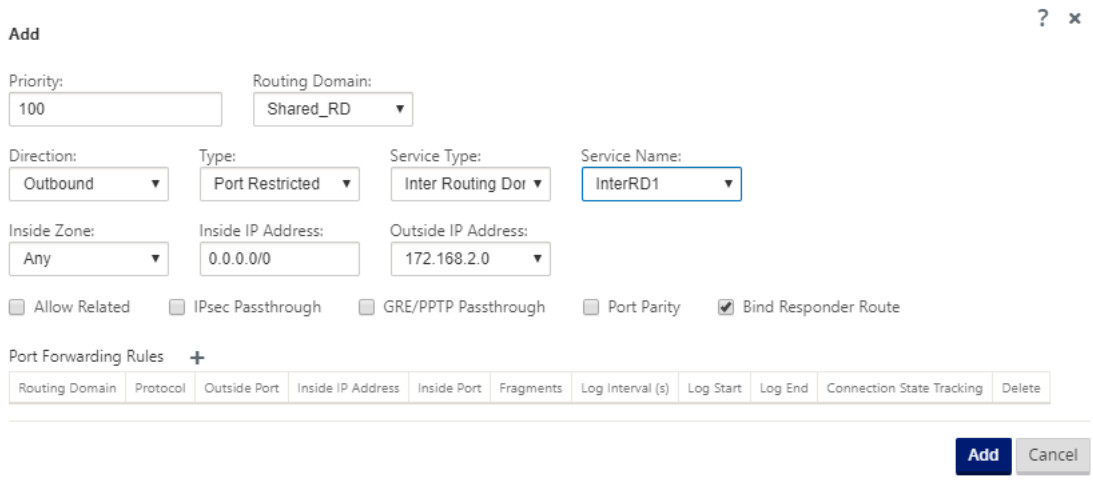
3. Configure a static route to Shared RD from RD1 and RD2. In RD1, add a route 172.168.2.0/24 to InterRD1.



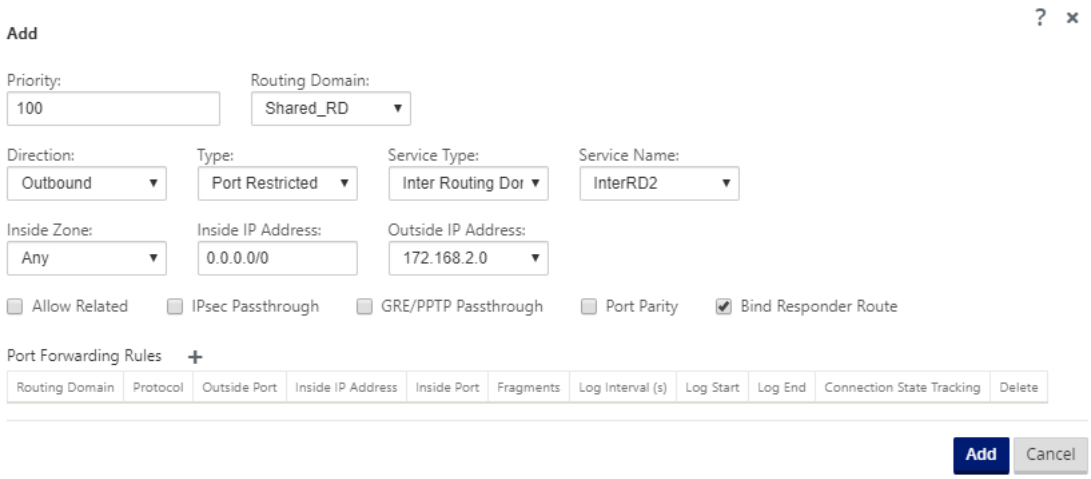
4. In RD2, add a route 172.168.2.0/24 to InterRD2.



5. Add a Dynamic NAT rule to InterRD1 using a VIP in shared RD. Enable **Bind Responder Route** to ensure that the reverse route uses the same service type.



6. Add a Dynamic NAT rule to InterRD2 using a VIP in shared RD, for example 10.0.0.11. Enable Bind Responder Route to ensure that the reverse route uses the same service type.



7. Use filters to limit what resources in Shared RD are allowed to be accessed by users in RD1/RD2.

Secure peering

March 12, 2021

Premium (Enterprise) Edition appliance can be installed at the data center and can 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 use 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:

To perform auto secure peering to a PE appliance from a standalone WANOP / SDWAN SE/WANOP on the DC site.

Steps to initiate this deployment:

- WANOP DC appliance is in LISTEN ON mode (2312/Any non-standard port) and Branch PE is in CONNECT-TO mode.
- WANOP DC initiates automatic secure peering to a PE appliance which installs the Private CA Certs and CERT KEY Pairs and configure CONNECT-TO on the PE appliance with WANOPs LISTEN-ON IP.

To perform Auto-secure peering initiated from PE appliance at DC site and Branch site PE appliance.

Steps to initiate this deployment:

- PE DC appliance is in LISTEN ON mode (on port 443). Branch PE is in CONNECT-TO mode.
- PE DC appliance initiates automatic secure peering to a PE Branch appliance which installs the Private CA Certs and CERT KEY Pairs and configures CONNECT-TO on the PE Branch appliance with DC PE's LISTEN-ON IP.
- LISTEN-ON IP for PE is in the interface IP associated to the routing domain for which "Redirect to WANOP"is enabled.

Auto Secure Peering initiated from PE Appliance at DC site and Branch with WANOP/ SDWAN SE appliance.

Steps to initiate this deployment:

- PE DC appliance is in LISTEN ON mode (on port 443). Branch WANOP / SD-WAN SE is in CONNECT-TO mode.
- PE DC appliance initiates automatic secure peering to Branch WANOP / SD-WAN SE appliance which installs the Private CA Certs and CERT KEY Pairs and configures CONNECT-TO on the PE appliance with DC PE's LISTEN-ON IP.

Manual Secure Peering deployments:

Manual Secure Peering initiated from PE appliance at DC site to Branch PE Appliance.

Steps to initiate this deployment:

- PE DC appliance is in LISTEN ON mode (on port 443). Branch PE is in CONNECT-TO mode.
- LISTEN-ON IP for PE 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.

Manual Secure Peering initiated from PE appliance at DC site to Branch WANOP/SDWAN-SE Appliance.

Steps to initiate this deployment:

- PE DC appliance is in LISTEN ON mode (on port 443). Branch WANOP / SD-WAN SE is in CONNECT-TO mode.
- LISTEN-ON IP for PE 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.

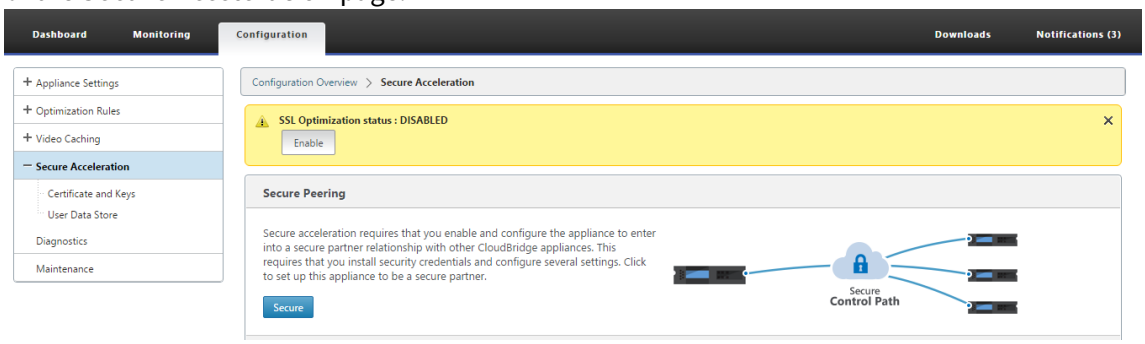
Auto Secure Peering to a PE appliance from a Standalone SD-WAN SE and WANOP Appliance on the DC site

March 12, 2021

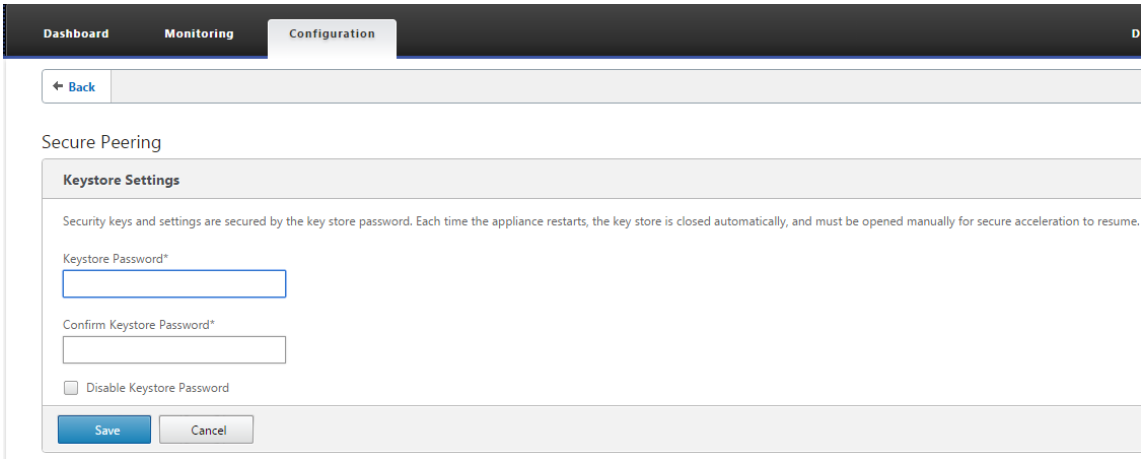
To perform auto secure peering on a PE appliance from a standalone SD-WAN SE and WANOP appliance on the DC Side:

- WANOP DC appliance is in LISTEN ON mode (2312/Any non-standard port).
- Branch PE appliance is in CONNECT-TO mode.
- WANOP DC initiates automatic secure peering to a PE appliance which installs the Private CA Certs and CERT KEY Pairs and configure CONNECT-TO on the PE appliance with WANOPs LISTEN-ON IP.

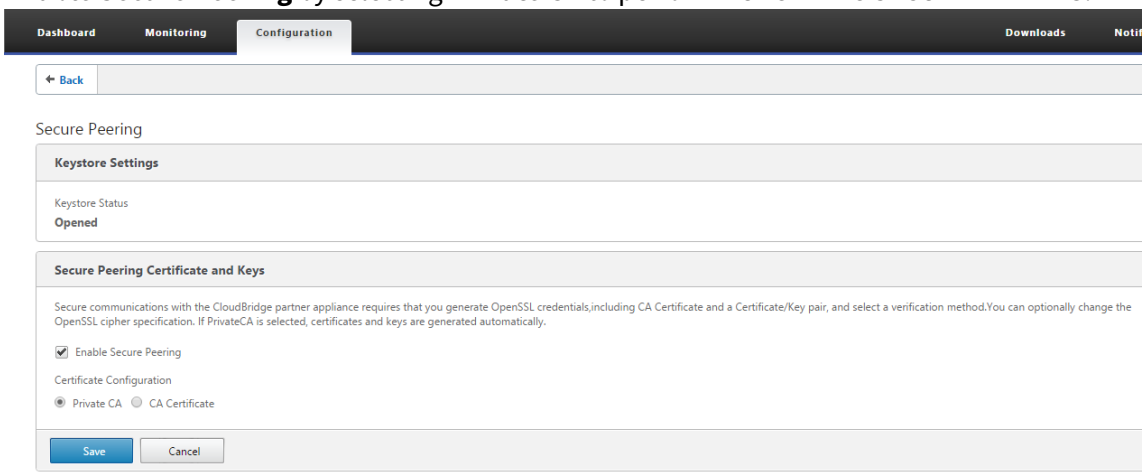
1. On a standalone WANOP appliance at the data center, click **Secure** in the **Secure Peering** pane of the **Secure Acceleration** page.



2. Configure the keystore settings by providing the **keystore password** or by disabling the keystore.

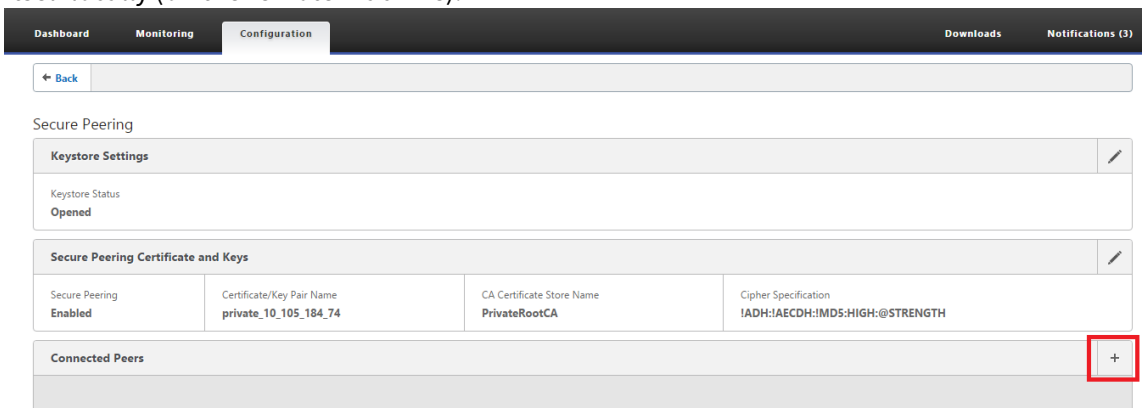


3. **Enable Secure Peering** by selecting **Private CA** to perform AUTOMATIC SECURE PEERING.



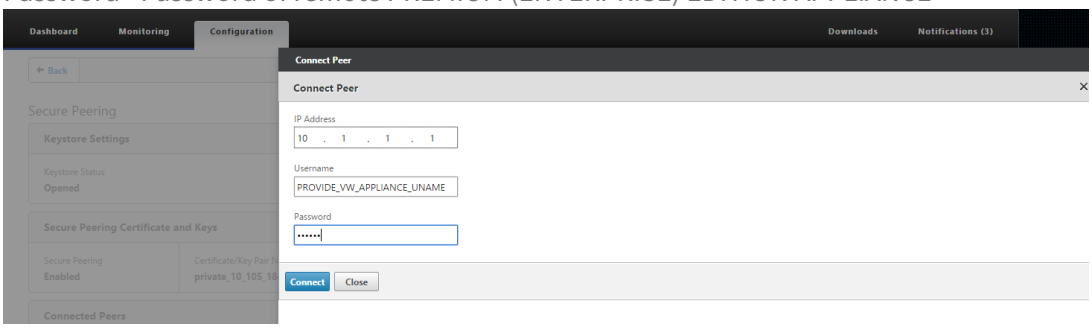
4. The appliance level CA certificate and private Certificate and Key is generated on the local WANOP and a table to add a REMOTE PEER TO Perform AUTO secure peering with is displayed.

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).

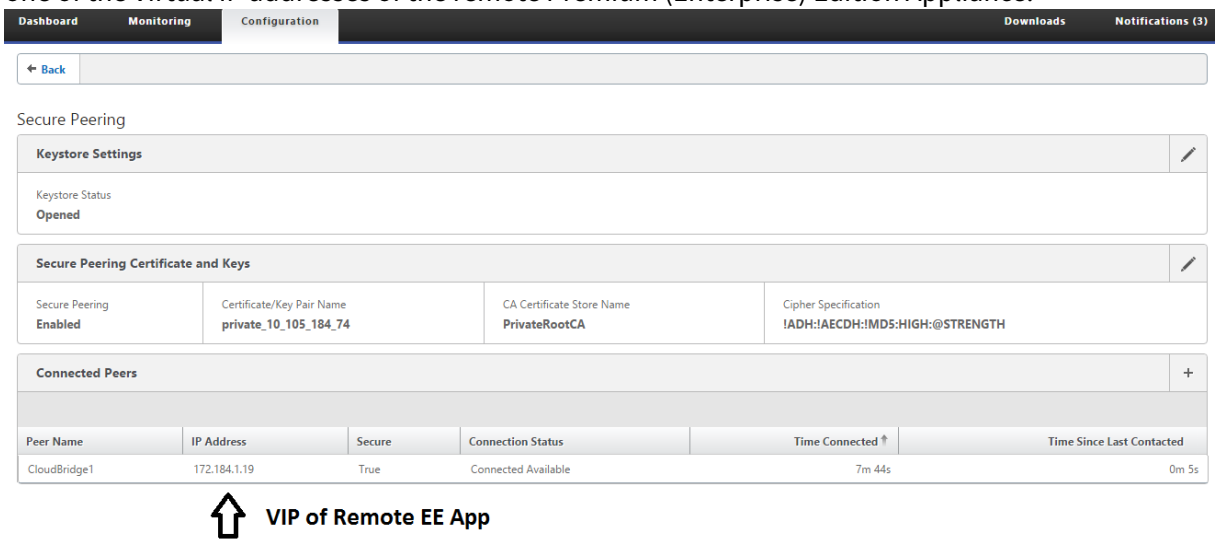


Note

- IP Address –IP Address of remote PREMIUM (ENTERPRISE) EDITION APPLIANCE MANAGEMENT IP
- Username –Username of remote PREMIUM (ENTERPRISE) EDITION APPLIANCE
- Password –Password of remote PREMIUM (ENTERPRISE) EDITION APPLIANCE



After Successful Authentication, you will see Secure Peering as TRUE and the partner IP address as one of the Virtual IP addresses of the remote Premium (Enterprise) Edition Appliance.

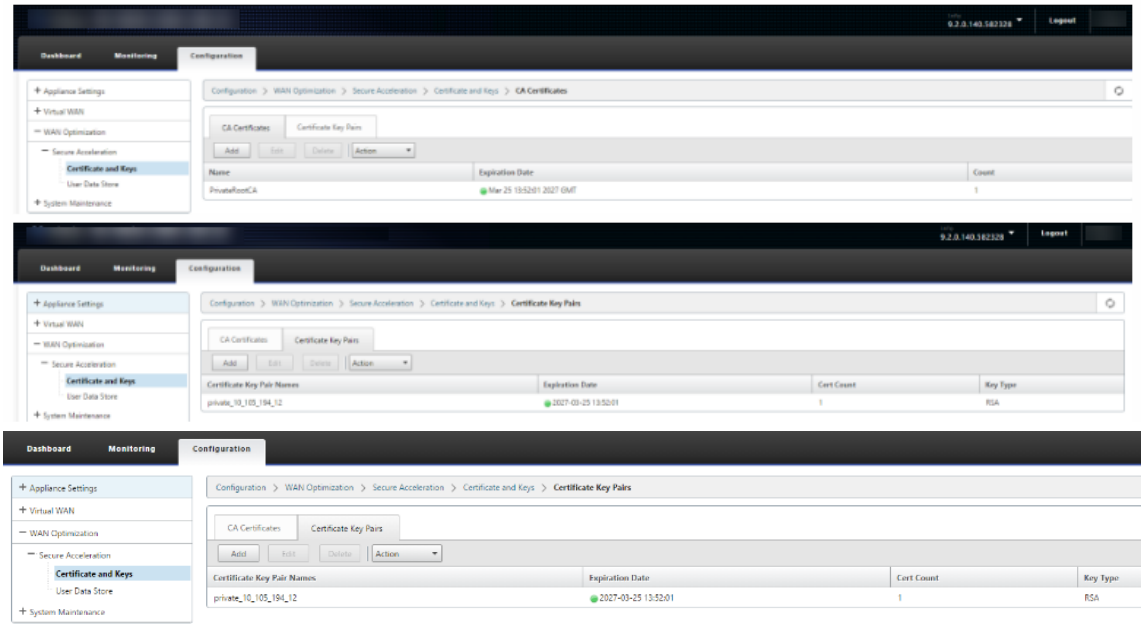


Monitoring

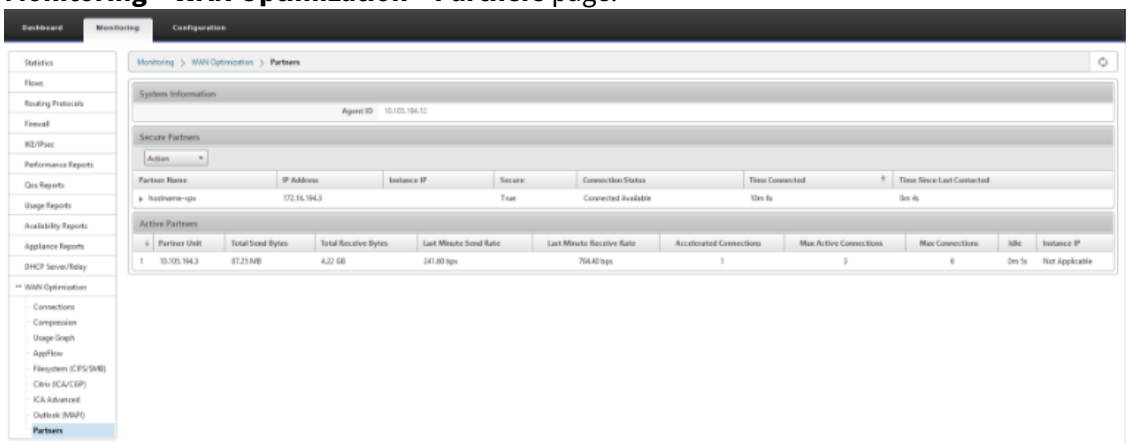
View Secure Partner Information on the Premium (Enterprise) Edition appliance under **WANOPTIMIZATION** > **Partners** in the **Monitoring** page.

1. Data Store Encryption can be performed on the Premium (Enterprise) Edition appliance through feature enablement from the MCN under Optimization node for a Premium (Enterprise) Edition appliance.
2. For a Premium (Enterprise) Edition appliance, secure peering is always enabled.

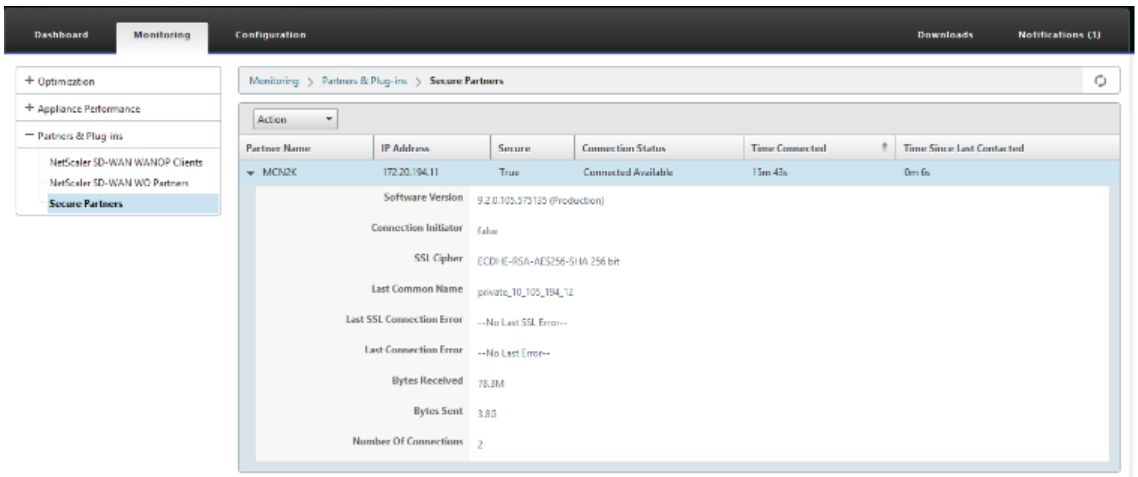
3. To validate if the **Private CA** and **Private Certificate Key** pair is generated successfully, review the information below:



4. View **Secure Partner Information** on the Premium (Enterprise) Edition appliance under **Monitoring** > **WAN Optimization** > **Partners** page.

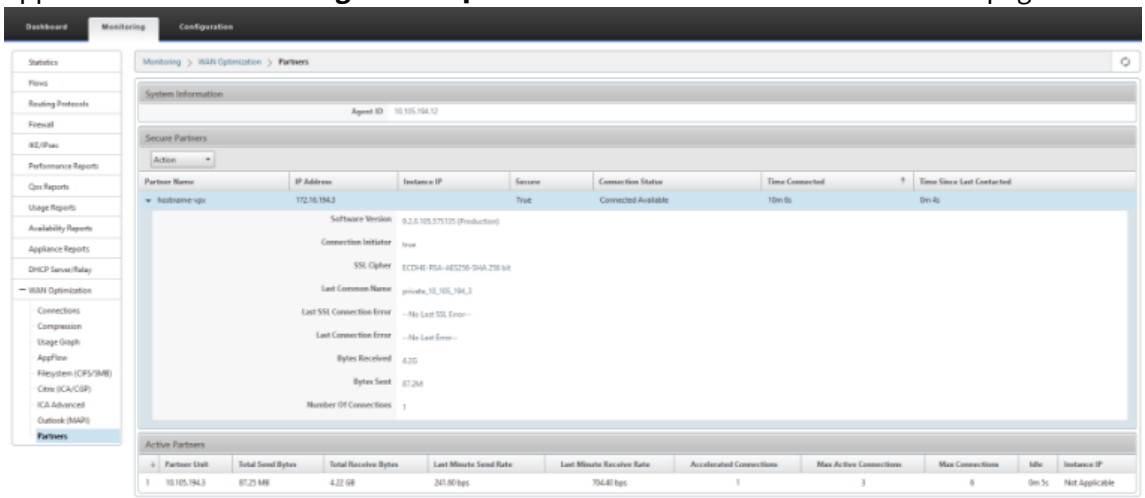


5. On partner appliance, **View Secure Partner Information** of the Premium (Enterprise) Edition appliance under **Monitoring** > **Partners & Plug-ins** > **Secure Partner**s page.

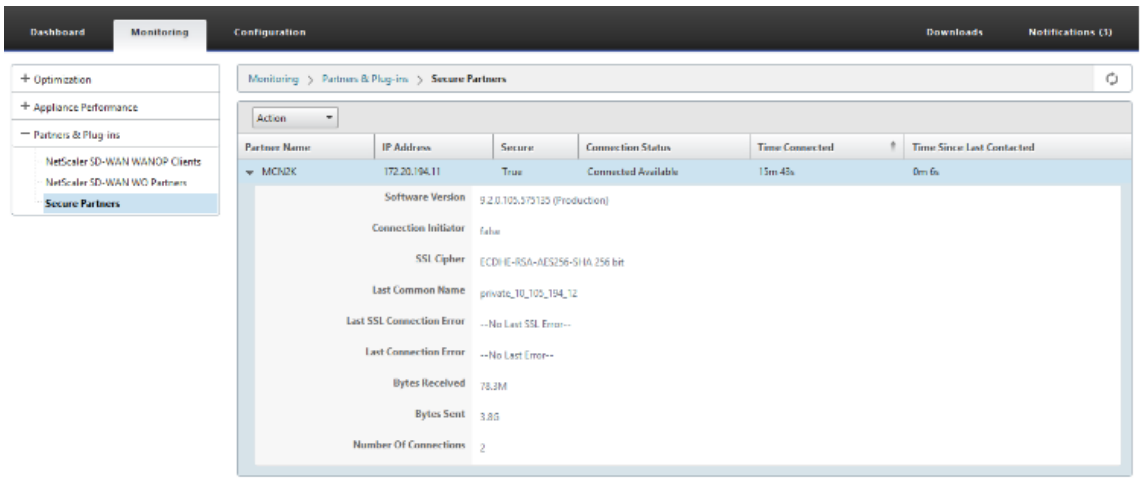


Troubleshooting

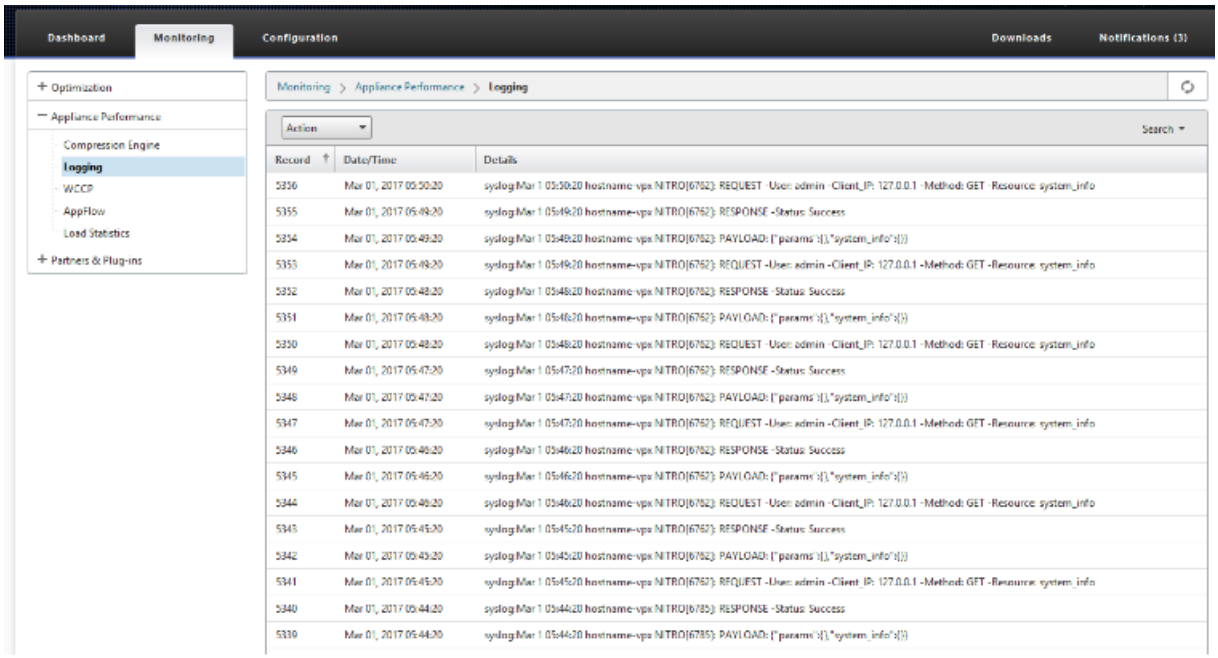
1. View **Secure Partner Success** / **Failure Information** on the Premium (Enterprise) Edition appliance under **Monitoring** > **WAN Optimization** > **Partners** > **Secure Partners** page.



2. On partner appliance, view Secure Partner Information on the Premium (Enterprise) Edition appliance under **Monitoring** > **Partners & Plug-ins** > **Secure Partners** page.



3. On partner appliance, view Secure Partner Information on the Premium (Enterprise) Edition appliance under **Monitoring** > **Appliance Performance** > **Logging** page.



Auto Secure Peering initiated from PE appliance at DC site and branch site PE appliance

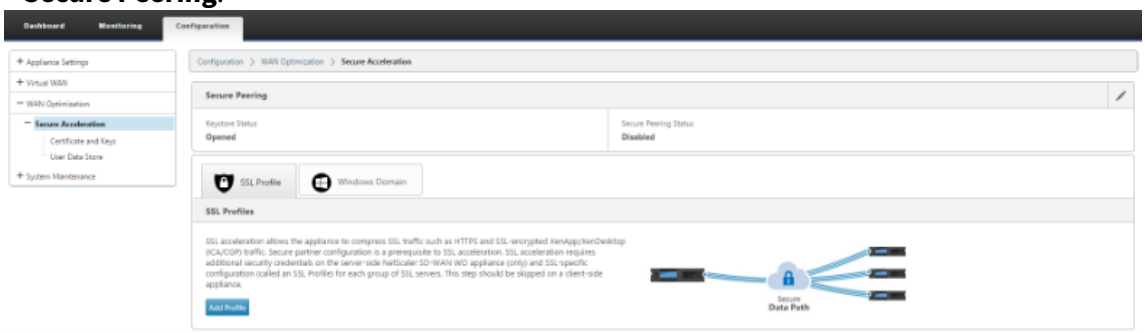
March 12, 2021

Configuration

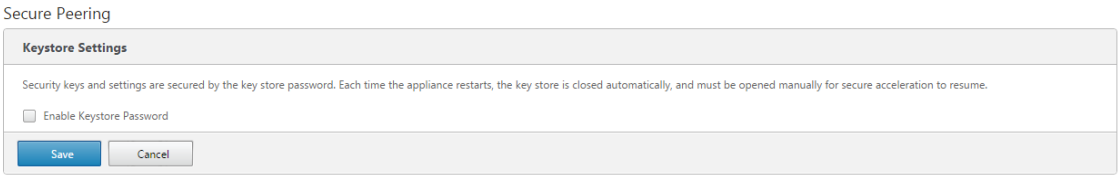
To configure auto secure peering on a new Premium (Enterprise) Edition appliance at DC:

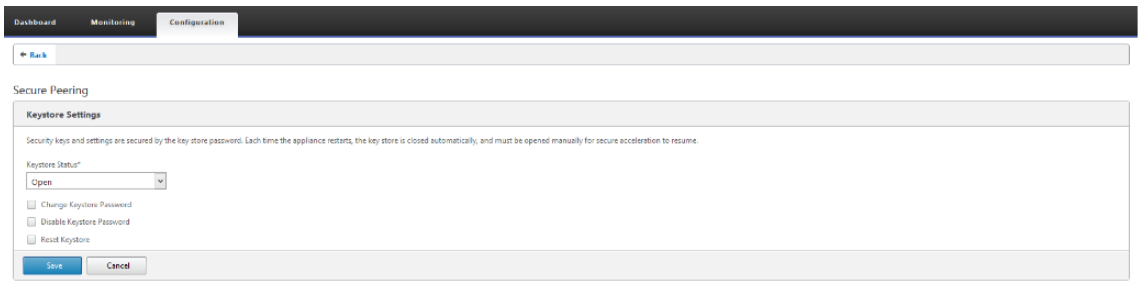
- PE DC appliance is in LISTEN ON mode (on port 443). Branch PE appliance is in CONNECT-TO mode.
- PE DC appliance initiates automatic secure peering to a PE Branch appliance which installs the Private CA Certs and CERT KEY Pairs and configures CONNECT-TO on the PE Branch appliance with DC EE's LISTEN-ON IP.
- LISTEN-ON IP for PE appliance is in the interface IP associated to the routing domain for which "Redirect to WANOP"is enabled.

1. In the SD-WAN web GUI, navigate to **Configuration** > **WAN Optimization** > **Secure Acceleration** > **Secure Peering**.

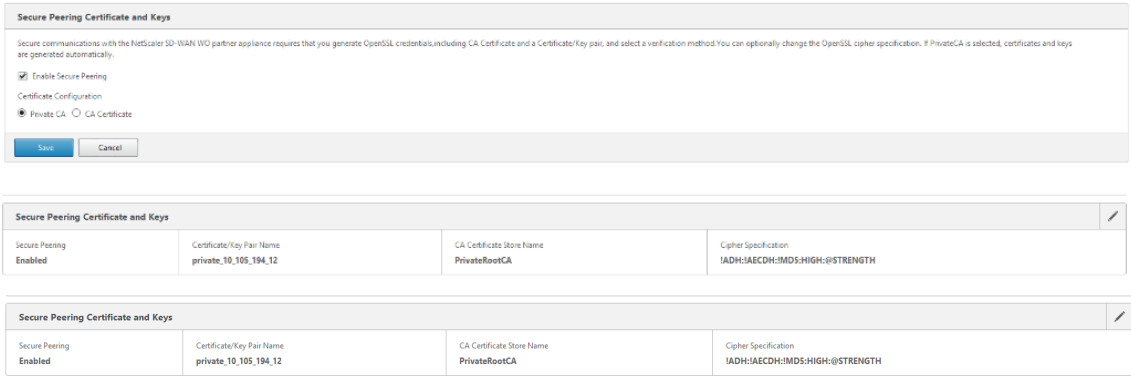


2. Configure keystore by providing the keystore password or by disabling keystore.



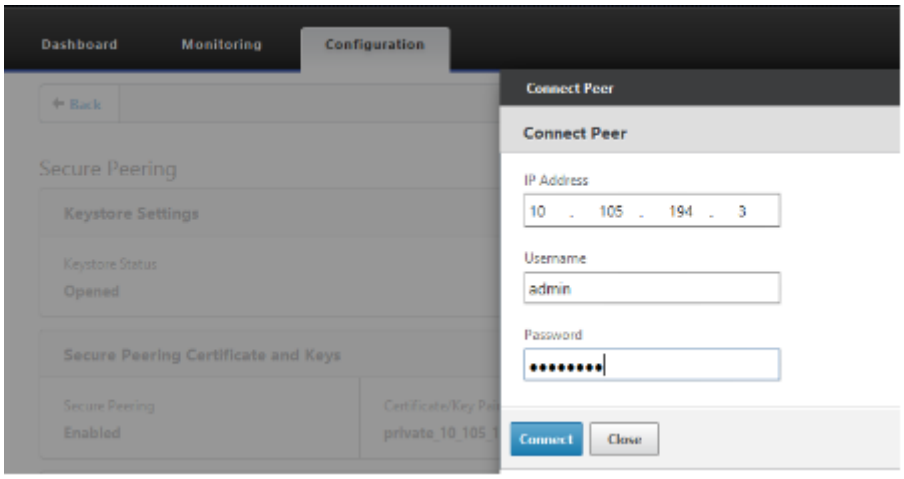


3. Enable **Secure Peering** by selecting **Private CA** to perform AUTOMATIC SECURE PEERING.



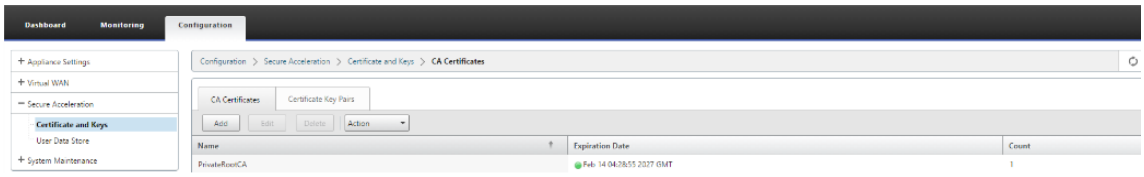
4. Click the '+'icon and to add IP with username and password. After successful authentication with the remote IP and credentials provided, a request is sent to the remote machine that will install CA Certificate and the Private cert and key for itself locally on the remote machine.

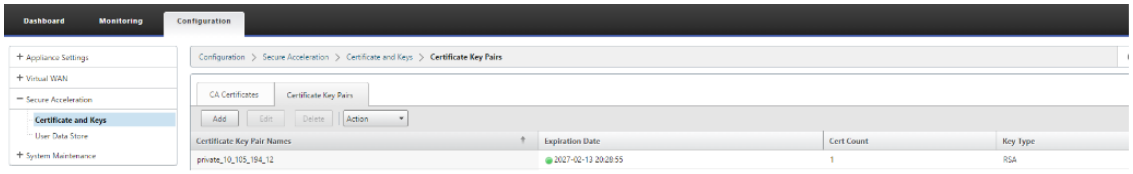
> **Note**
>
> IP Address –IP Address of remote EE Appliance MANAGEMENT IP
>
> Username –Username of remote EE Appliance
>
> Password –Password of remote EE Appliance



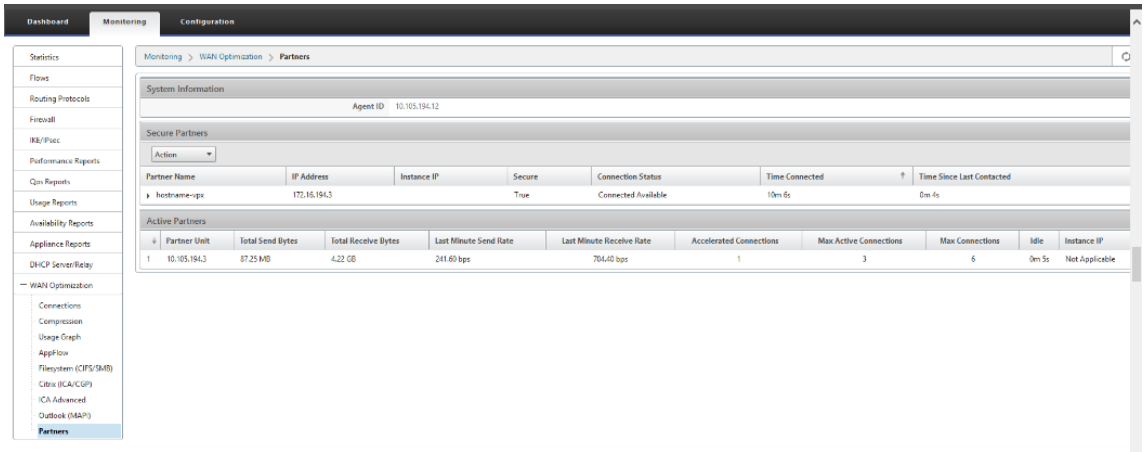
Monitoring

1. To validate if the Private CA and Private Certificate Key pair is generated successfully, review the information displayed below.

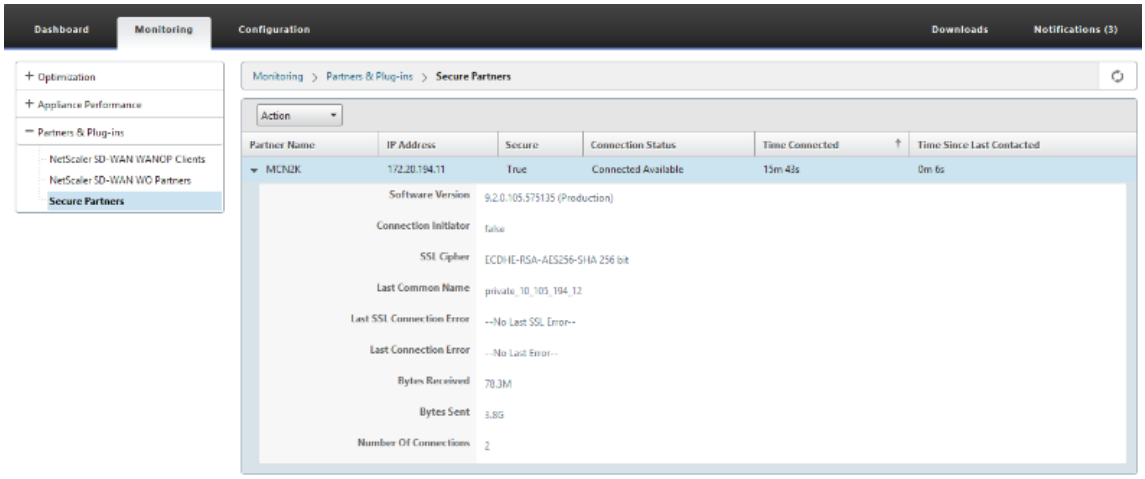




2. View **Secure Partner Information** on the Premium (Enterprise) Edition appliance under **Monitoring** > **WAN Optimization** > **Partners** page.

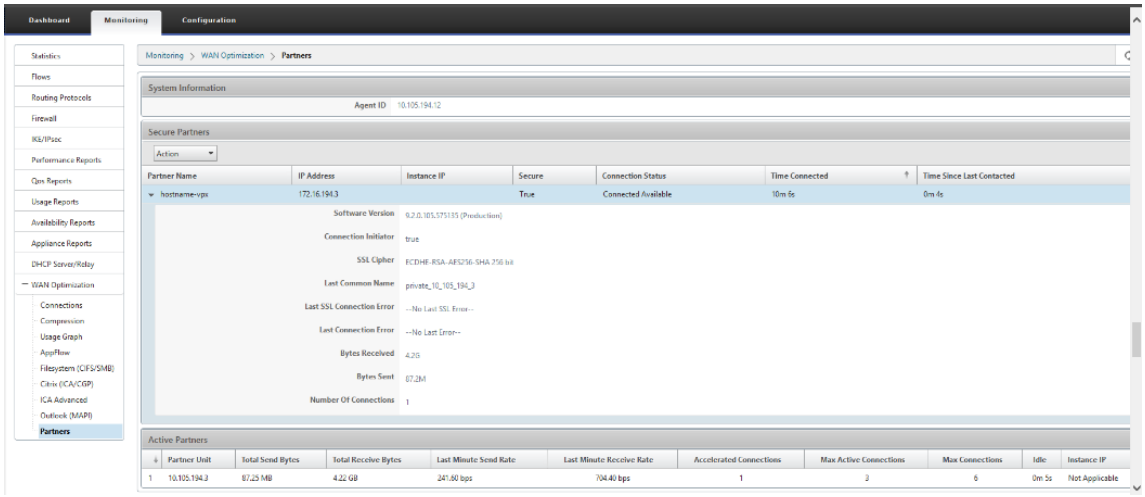


3. On partner appliance, view Secure Partner Information on the Premium (Enterprise) Edition Appliance under **Monitoring** > **Partners & Plug-ins** > **Secure Partners** page.

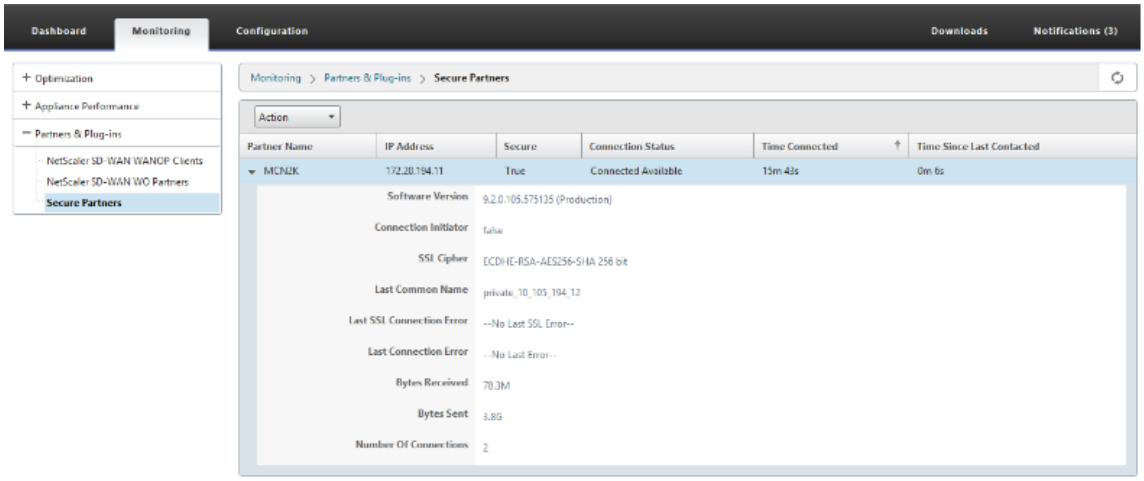


Troubleshooting

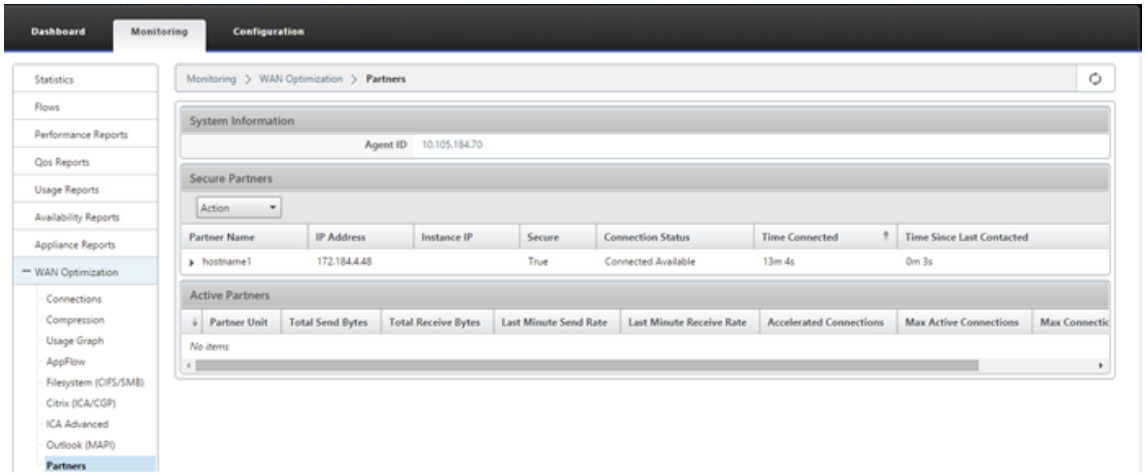
1. View Secure Partner Success / Failure Information on the Premium (Enterprise) Edition Appliance under **Monitoring** > **WAN Optimization** > **Partners** > **Secure Partners** page.

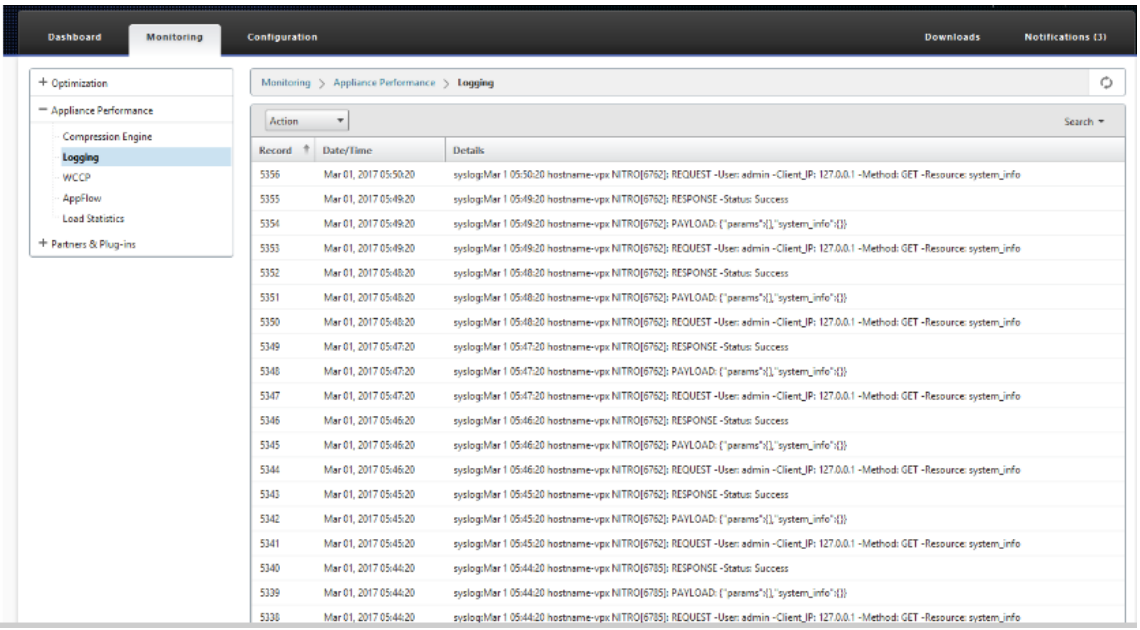


2. On partner appliance, view Secure Partner Information on the Premium (Enterprise) Edition Appliance under **Monitoring** > **Partners & Plug-ins** > **Secure Partners** page.



3. On partner Appliance, view Secure Partner Information on the Premium (Enterprise) Edition Appliance under **Monitoring** > **Appliance Performance** > **Logging** page.





Auto Secure Peering initiated from PE appliance at DC site and branch with standalone SD-WAN SE and WANOP appliance

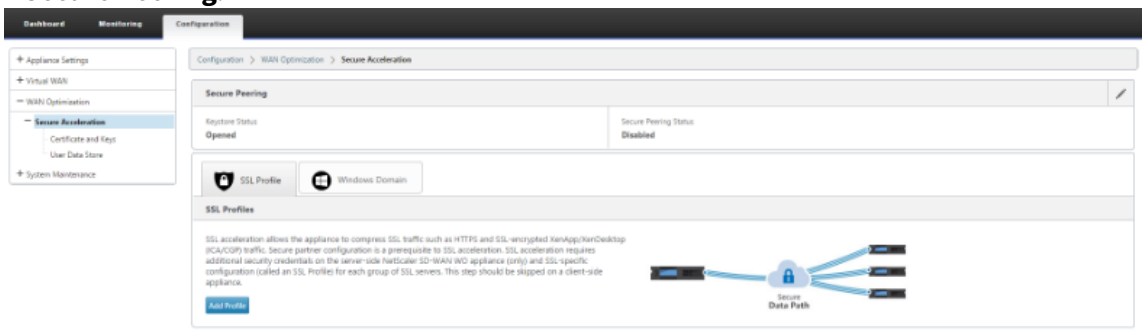
March 12, 2021

Configuration

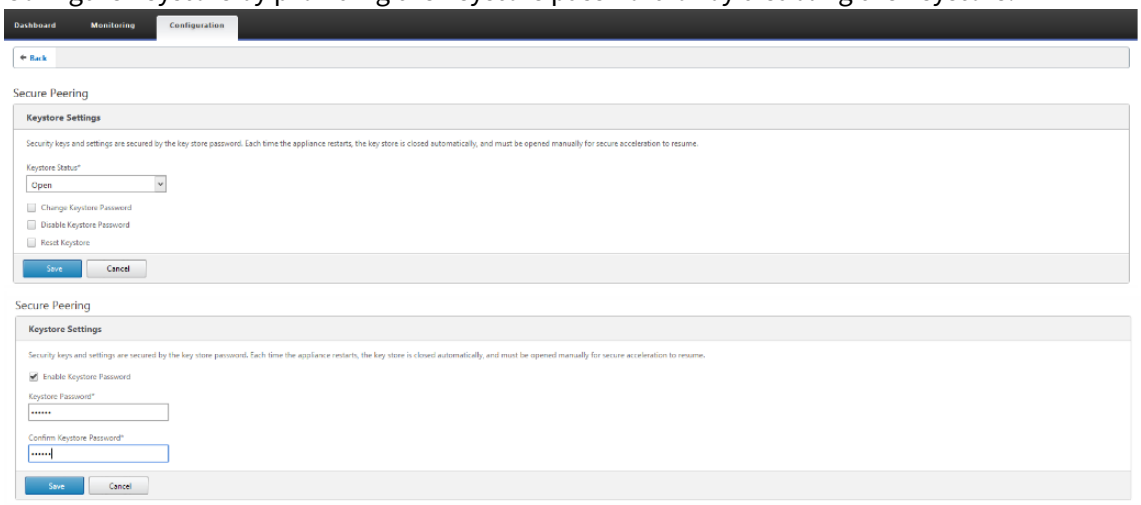
To configure a new Premium (Enterprise) Edition appliance with auto secure peering at the DC site and Branch with Standalone SD-WAN and WANOP appliance:

- PE DC appliance is in LISTEN ON mode (on port 443).
- Branch standalone SD-WAN SE and WANOP is in CONNECT-TO mode.
- PE DC appliance initiates automatic secure peering to Branch standalone SD-WAN SE and WANOP appliance which installs the Private CA Certs and CERT KEY Pairs and configures CONNECT-TO on the PE appliance with DC EE's LISTEN-ON IP.

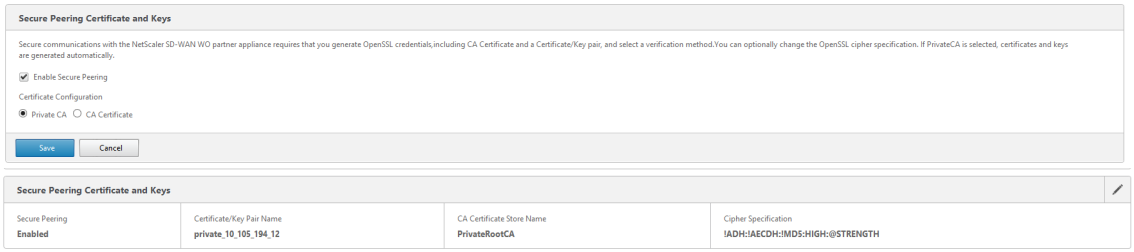
1. In the SD-WAN web GUI, navigate to **Configuration** > **WAN Optimization** > **Secure Acceleration** > **Secure Peering**.



2. Configure keystore by providing the keystore password or by disabling the keystore.

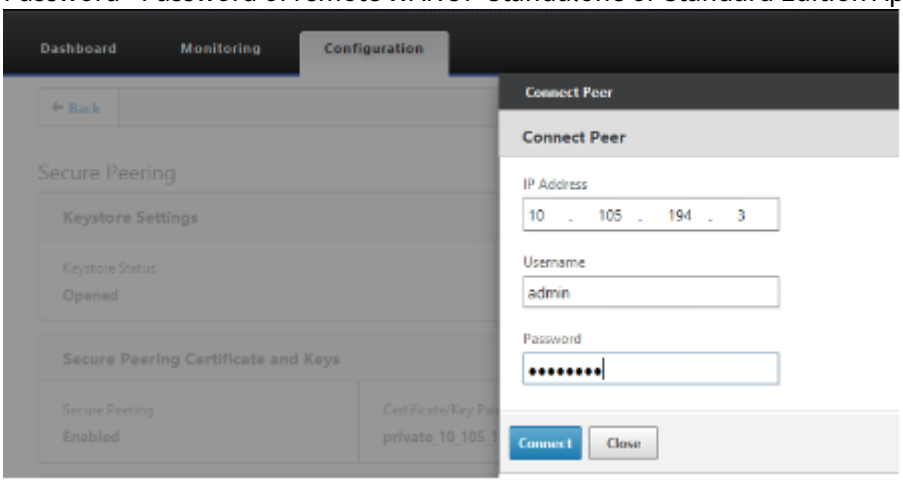


3. Enable **Secure Peering** by selecting **Private CA** to perform AUTOMATIC SECURE PEERING.

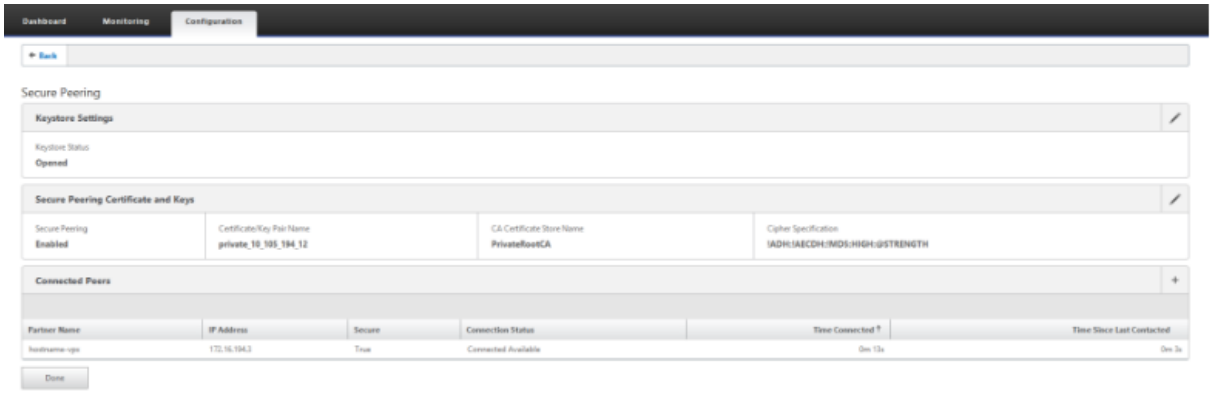


4. Click the '+'icon and to add IP with username and password. After successful authentication with the remote IP and credentials provided, a request is sent to the remote machine that will install CA Certificate and the Private cert and key for itself locally on the remote machine.

- 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.

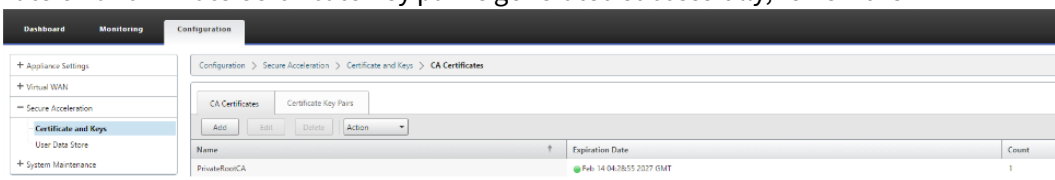


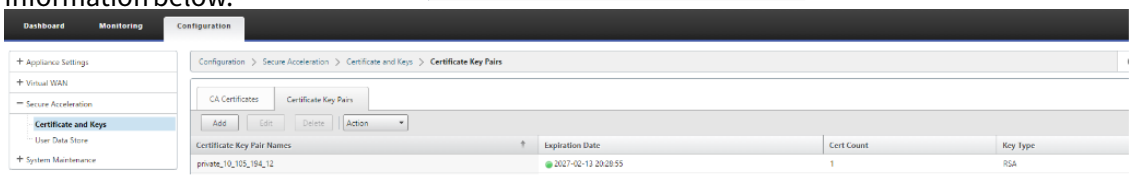
After Successful Authentication, you can view Secure Peering as TRUE and the partner IP as one of the Virtual IP of the remote WANOP Standalone appliance.



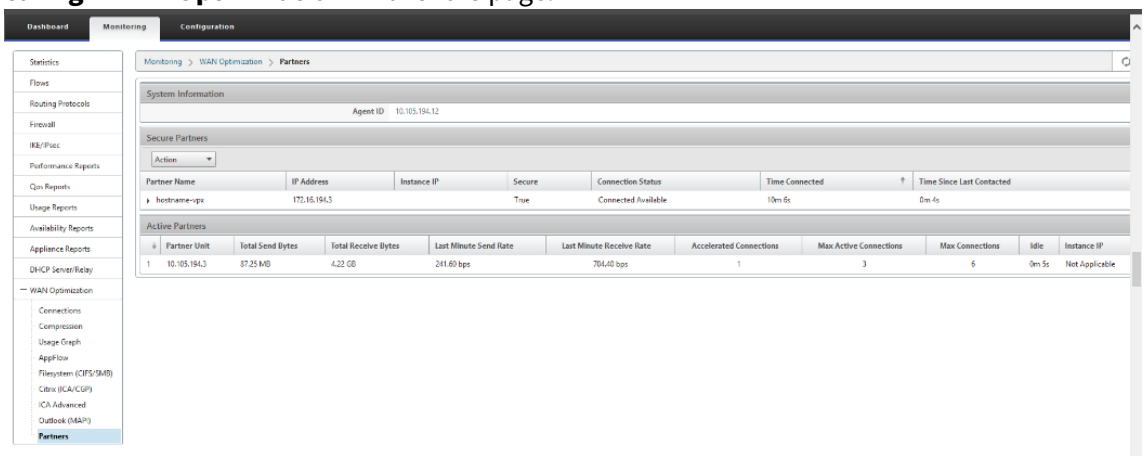
Monitoring

1. To validate if the Private CA and Private Certificate Key pair is generated successfully, review the information below.

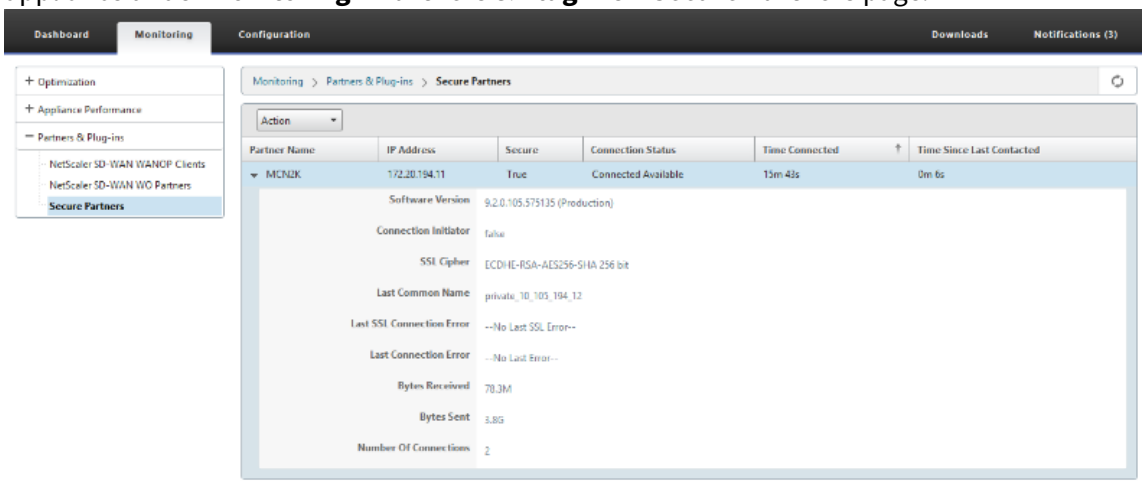




2. View Secure Partner Information on the Premium (Enterprise) Edition appliance under **Monitoring** > **WAN Optimization** > **Partners** page.

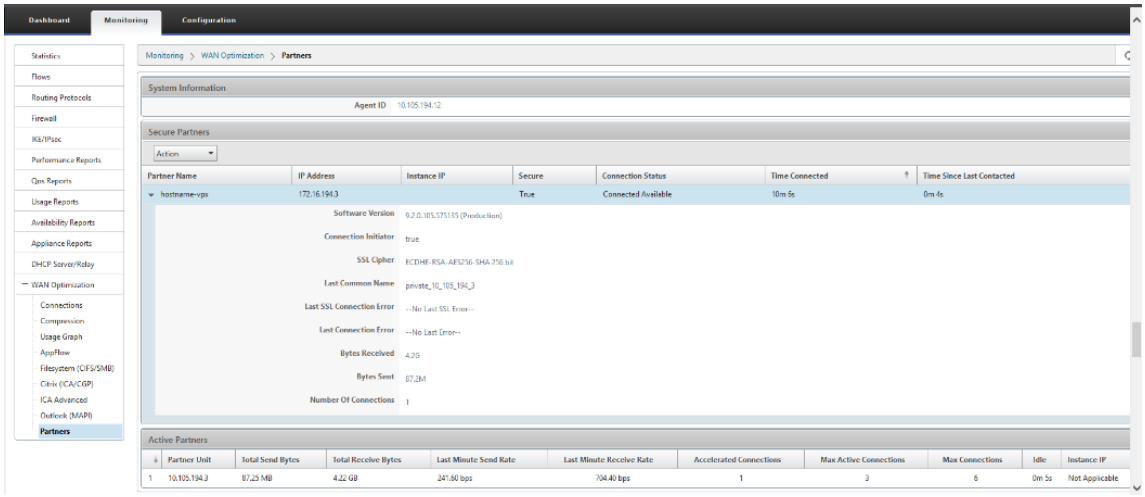


3. On partner appliance, View Secure Partner Information on the Premium (Enterprise) Edition appliance under **Monitoring** > **Partners & Plug-ins** > **Secure Partners** page.

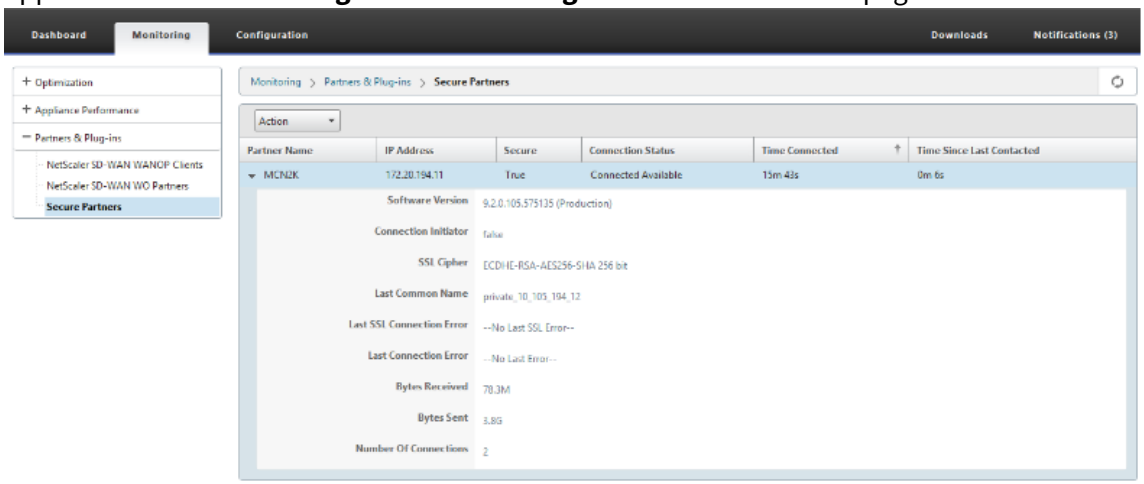


Troubleshooting

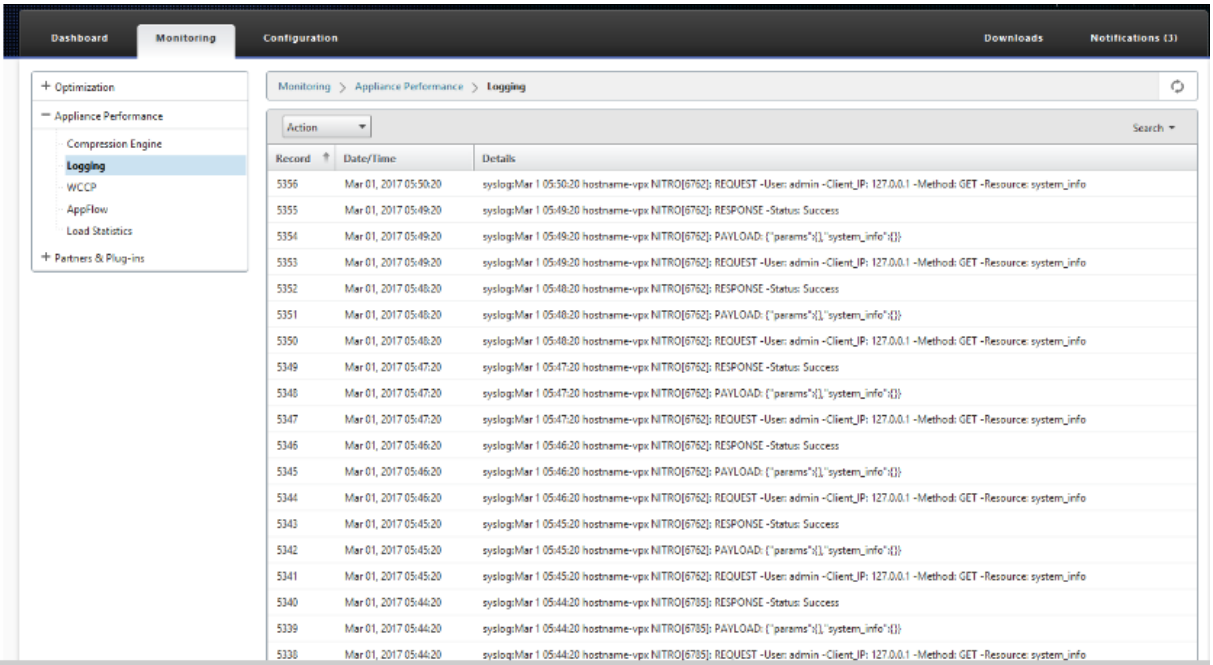
1. View Secure Partner Success / Failure Information on the Premium (Enterprise) Edition appliance under **Monitoring** > **WAN Optimization** > **Partners** > **Secure Partners** page.



2. On partner appliance, view **Secure Partner Information** on the Premium (Enterprise) Edition appliance under **Monitoring** > **Partners & Plug-ins** > **Secure Partners** page.



3. On partner appliance, view **Secure Partner Information** on the Premium (Enterprise) Edition appliance under **Monitoring** > **Appliance Performance** > **Logging** page.



Manual Secure Peering initiated from PE appliance at DC site and Branch PE appliance

March 12, 2021

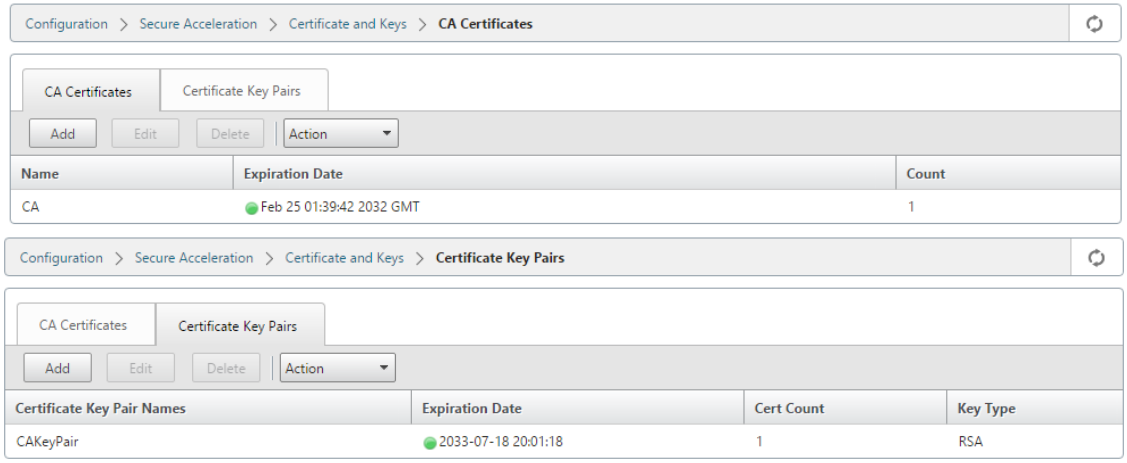
This deployment configures DC site PE appliance in LISTEN ON mode and Branch site PE appliance in CONNECT TO mode.

- PE DC appliance is in LISTEN ON mode (on port 443).
- Branch PE appliance is in CONNECT-TO mode.
- LISTEN-ON IP for PE 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.

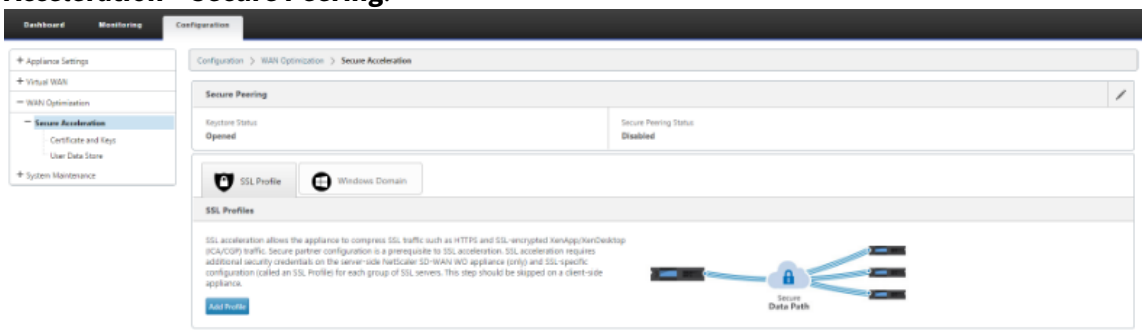
Configuration

To configure auto secure peering initiated from an PE appliance at DC site and PE appliance at branch site:

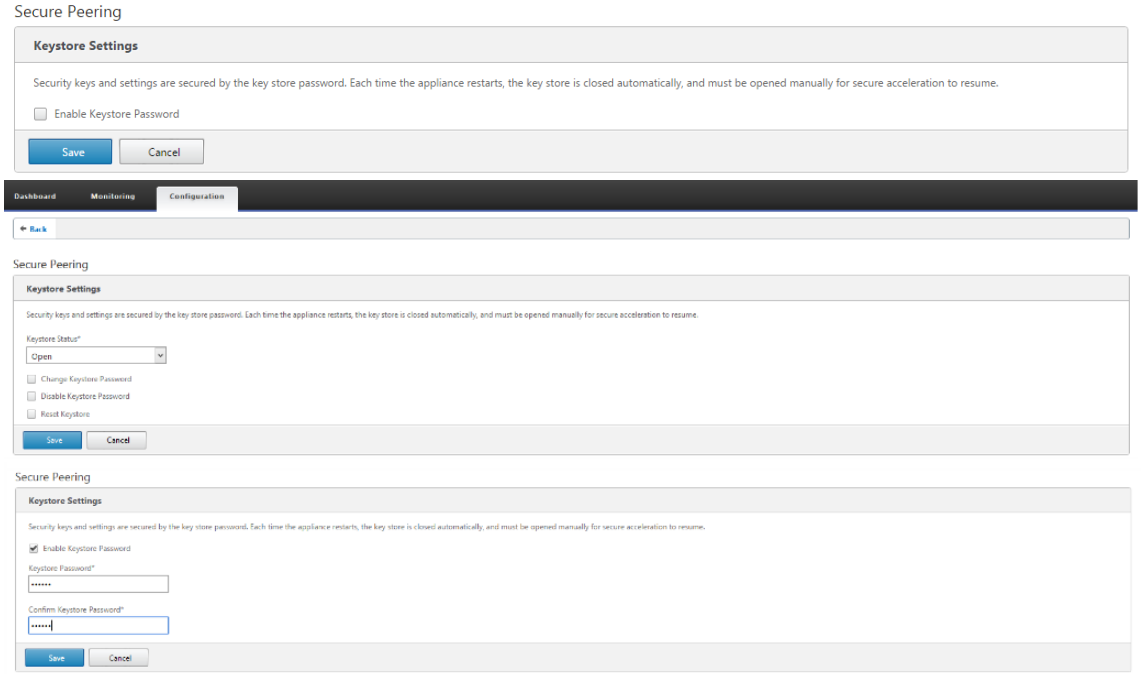
1. Upload **CA Certificate** and **CA Key Certificate** obtained from authentic certificate and provide to SD-WAN as shown below.



2. On a new PE appliance at the DC site, in the SD-WAN web GUI, go to **Configuration** > **Secure Acceleration** > **Secure Peering**.

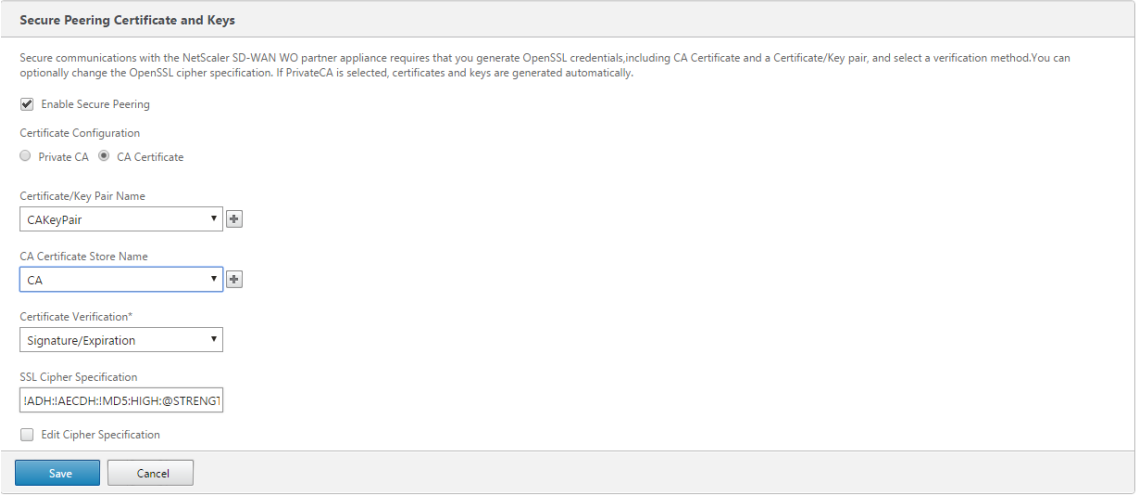


3. Configure keystore by providing the keystore password or by disabling the keystore.

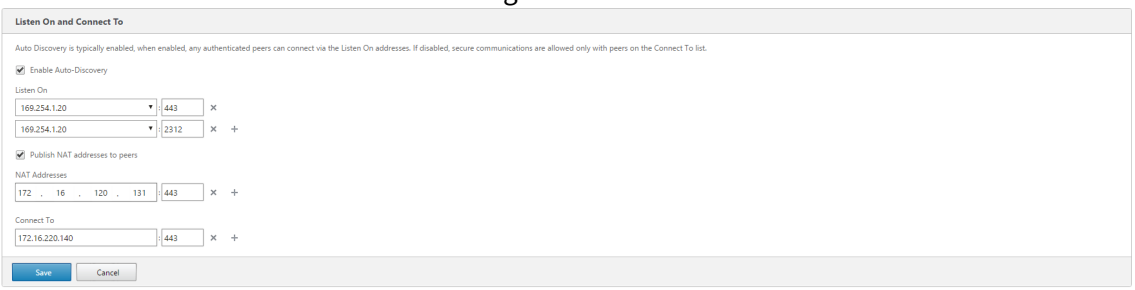


4. Enable secure peering by selecting **CA Certificate** radio button and providing uploaded CA and

CA Key pair certificates appropriately as shown below.

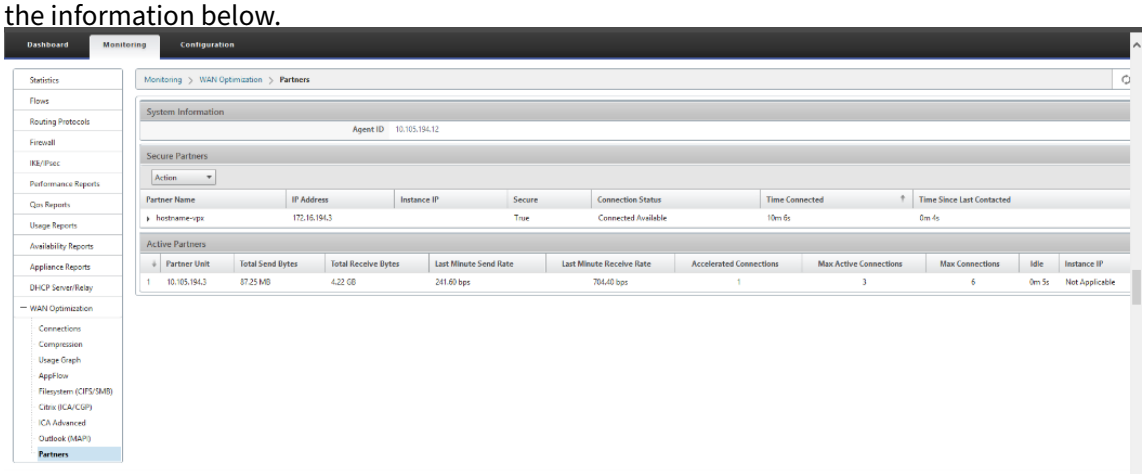


5. Provide Remote machine's Virtual IP along with Port 443 as shown below.

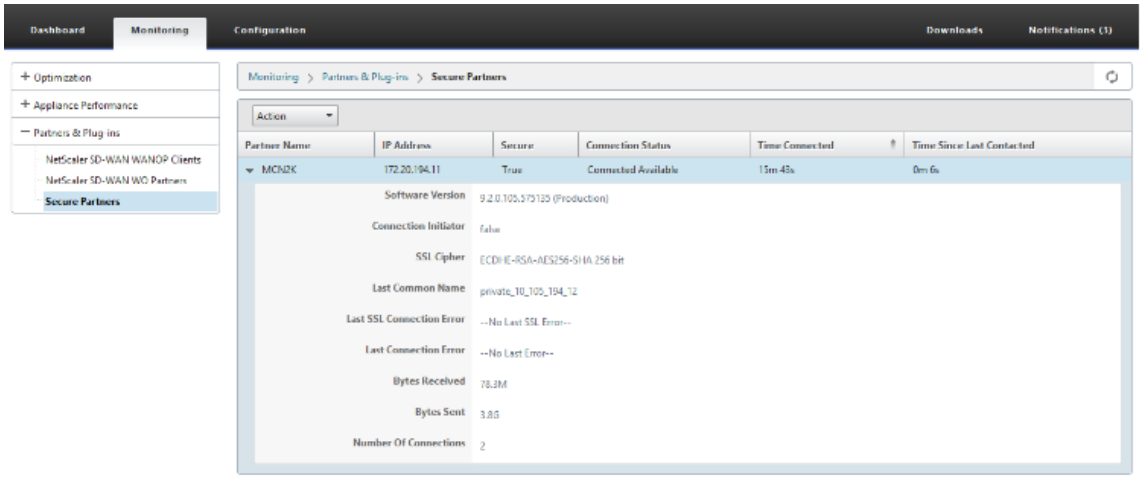


Monitoring

1. To validate if the **Private CA** and **Private Certificate Key** pair is generated successfully, review the information below.

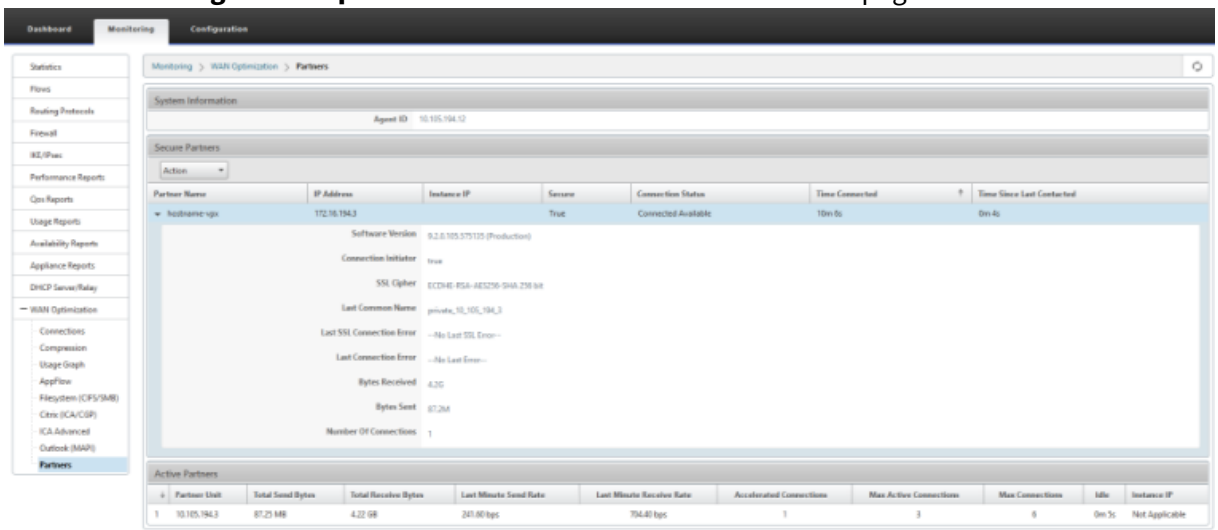


2. On partner appliance, **View Secure Partner Information** on the Premium (Enterprise) Edition appliance under **Monitoring** > **Partners** > **Secure Partners** page.



Troubleshooting

View **Secure Partner Success / Failure** Information on the Premium (Enterprise) Edition Appliance under **Monitoring** > **WAN Optimization** > **Partners** > **Secure Partners** page.



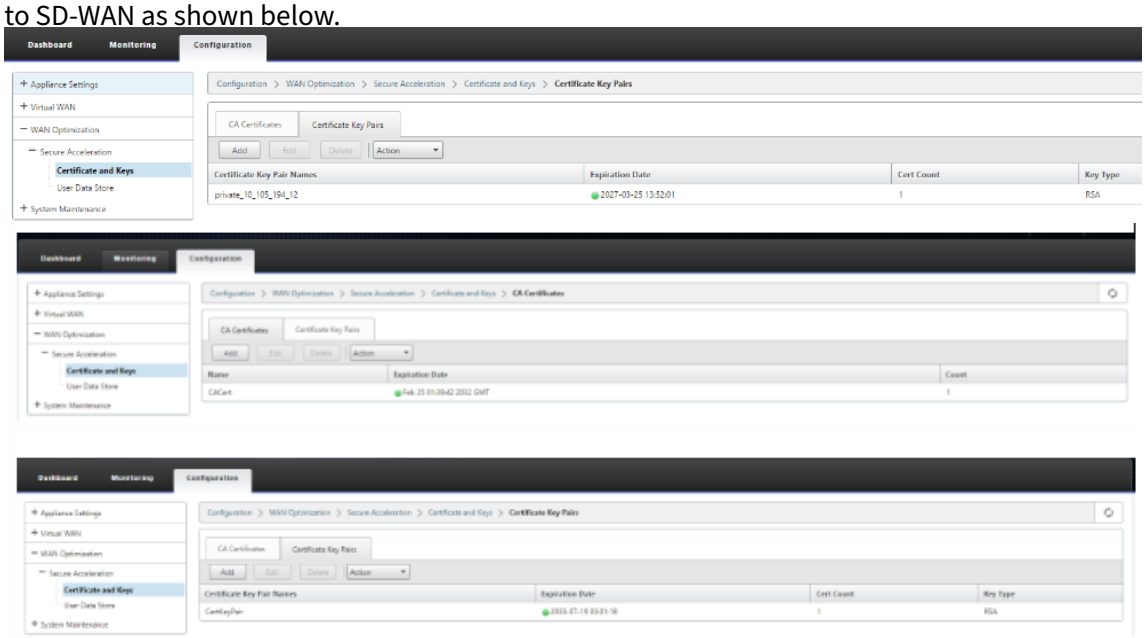
Manual Secure Peering initiated from PE appliance at DC site to Branch Standalone SD-WAN SE and WANOP Appliance

March 12, 2021

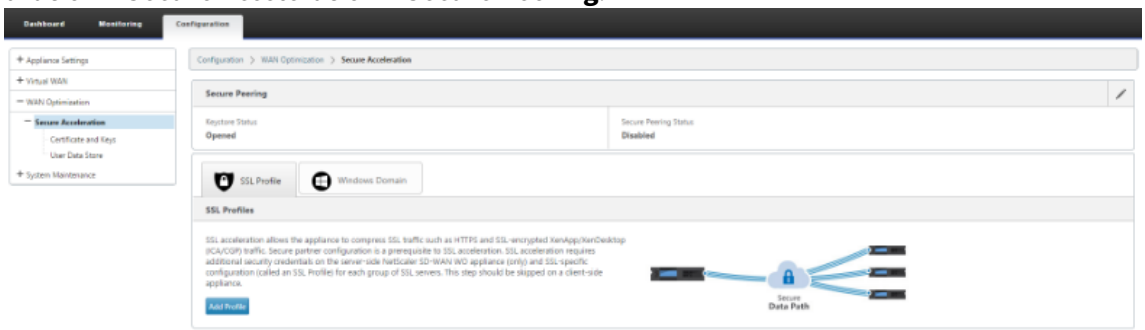
- PE DC appliance is in LISTEN ON mode (on port 443).
- Branch PE appliance is in CONNECT-TO mode.

- LISTEN-ON IP for PE 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.

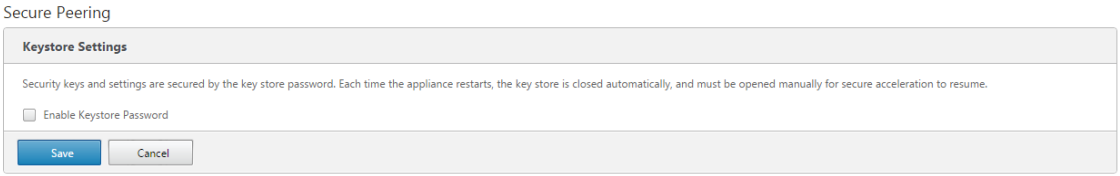
1. Upload **CA Certificate** and **CA Key Certificate** obtained from authentic certificate and provide to SD-WAN as shown below.

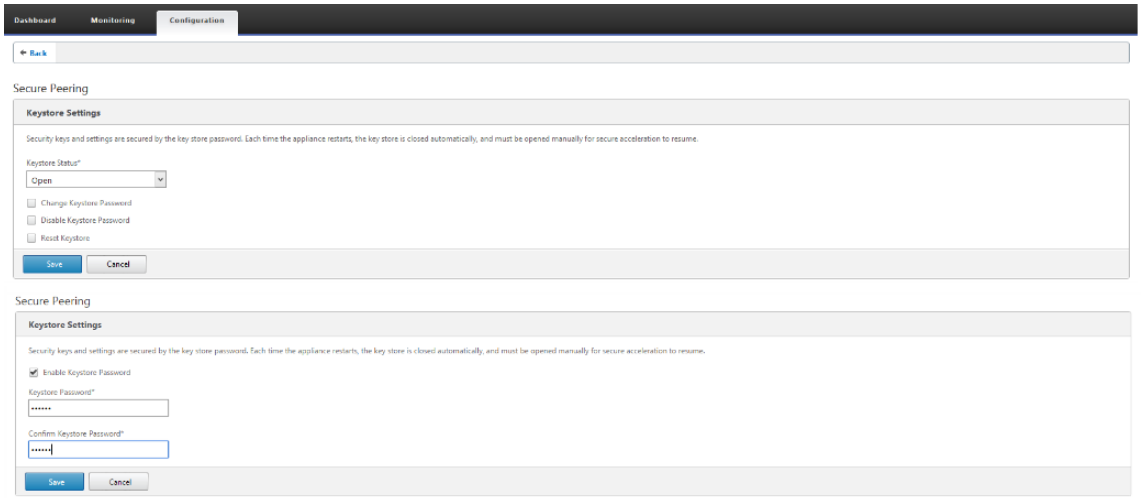


2. On a new PE (Premium Edition) appliance at the DC site, in the SD-WAN web GUI, go to **Configuration** > **Secure Acceleration** > **Secure Peering**.

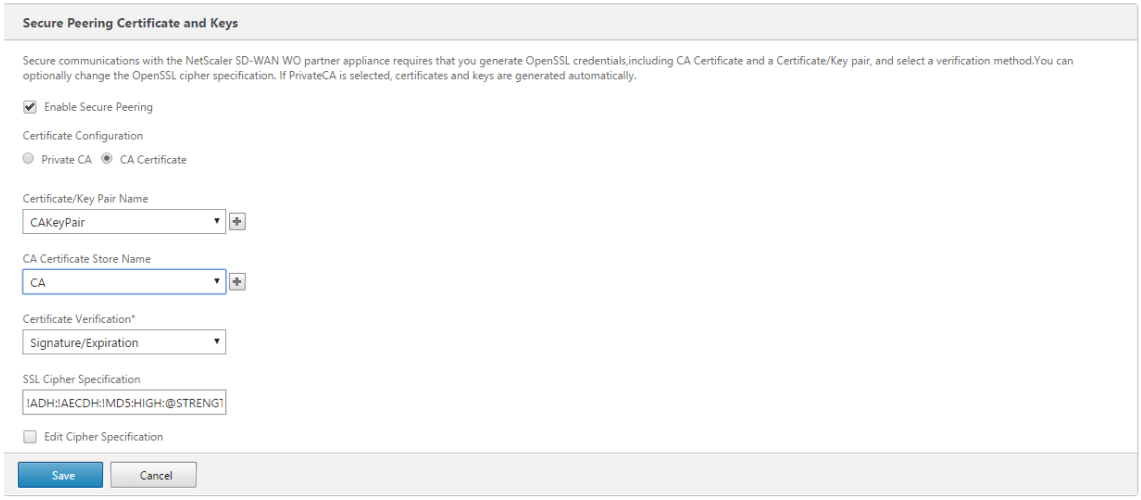


3. Enable the keystore by providing the **keystore password** or disable the keystore.

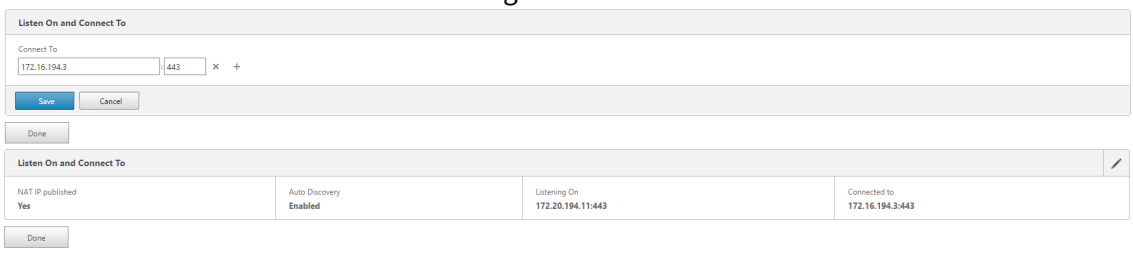




4. Enable secure peering by selecting **CA Certificate** radio button and providing uploaded CA and CA Key pair certificates appropriately as shown below.

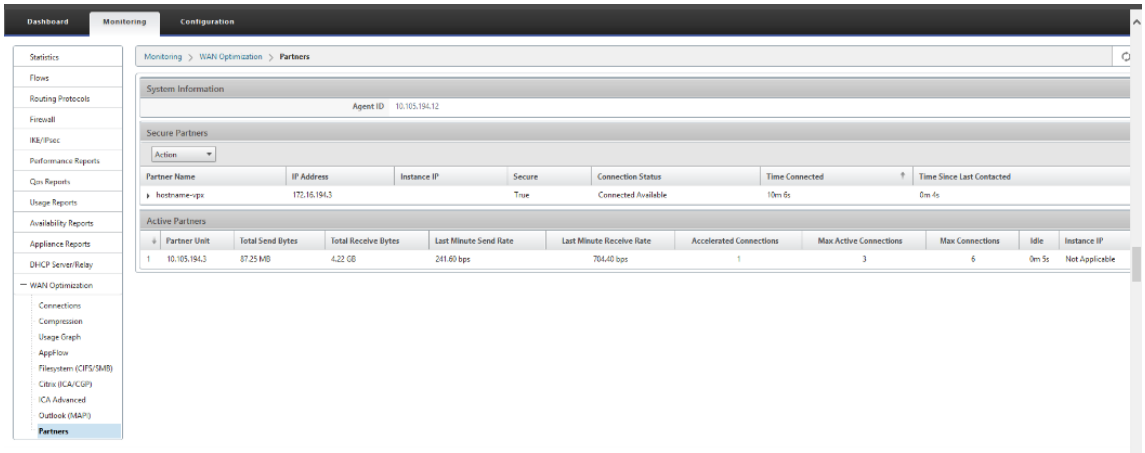


5. Provide Remote machine's Virtual IP along with Port 443 as shown below.

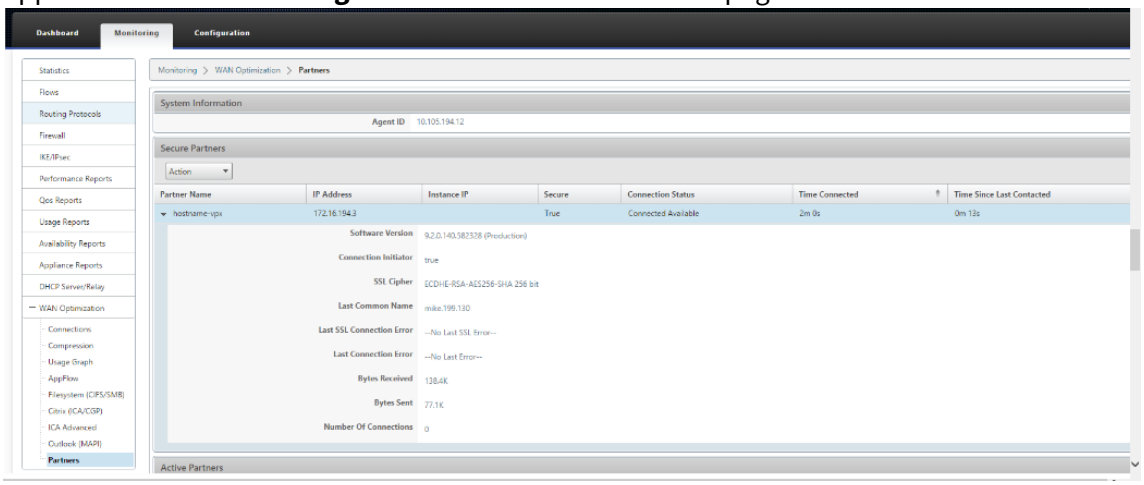


Monitoring

1. View Secure Partner Information on the Premium (Enterprise) Edition appliance under **Monitoring** > **WAN Optimization** > **Partners** page.

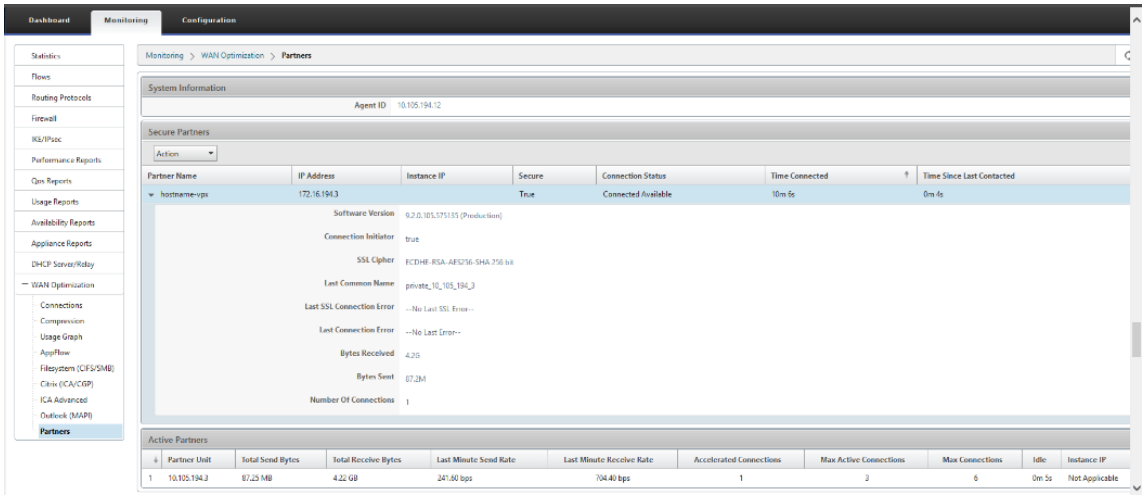


2. On partner appliance, View Secure Partner Information on the Premium (Enterprise) Edition appliance under **Monitoring** > **Partners** > **Secure Partners** page.

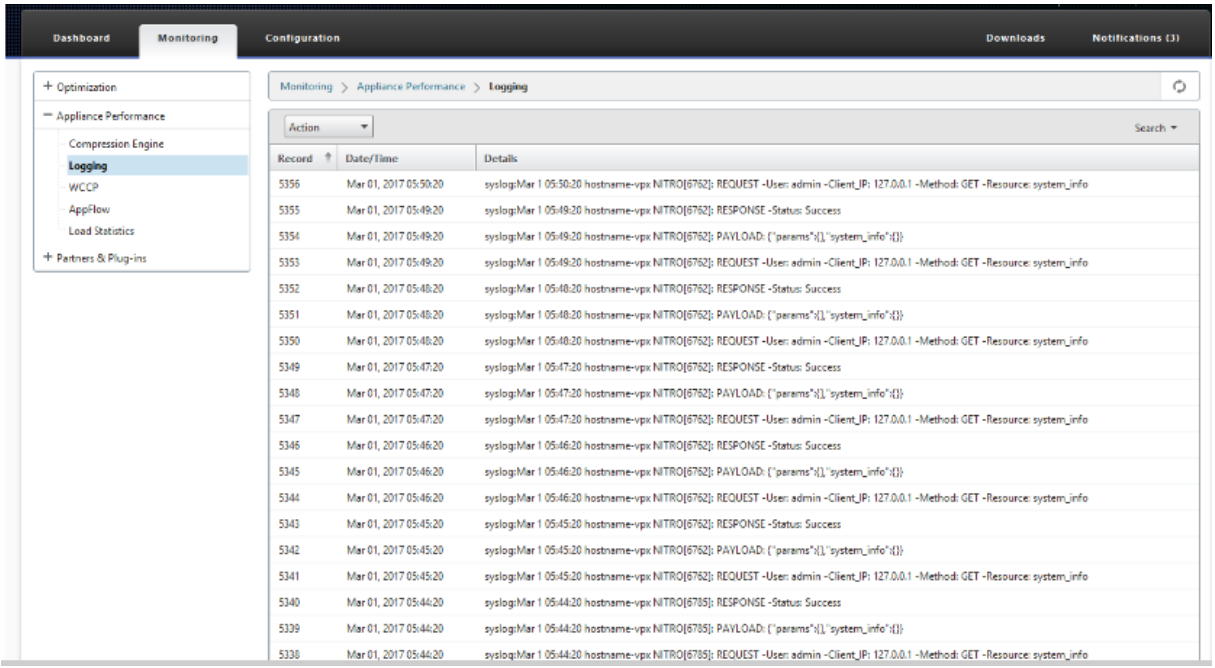


Troubleshooting

1. View **Secure Partner Success** / **Failure Information** on the Premium (Enterprise) Edition Appliance under **Monitoring** > **WAN Optimization** > **Partners** > **Secure Partners** page.



2. On partner appliance, view **Secure Partner Information** on the Premium (Enterprise) Edition appliance under **Monitoring** > **Appliance Performance** > **Logging** page.

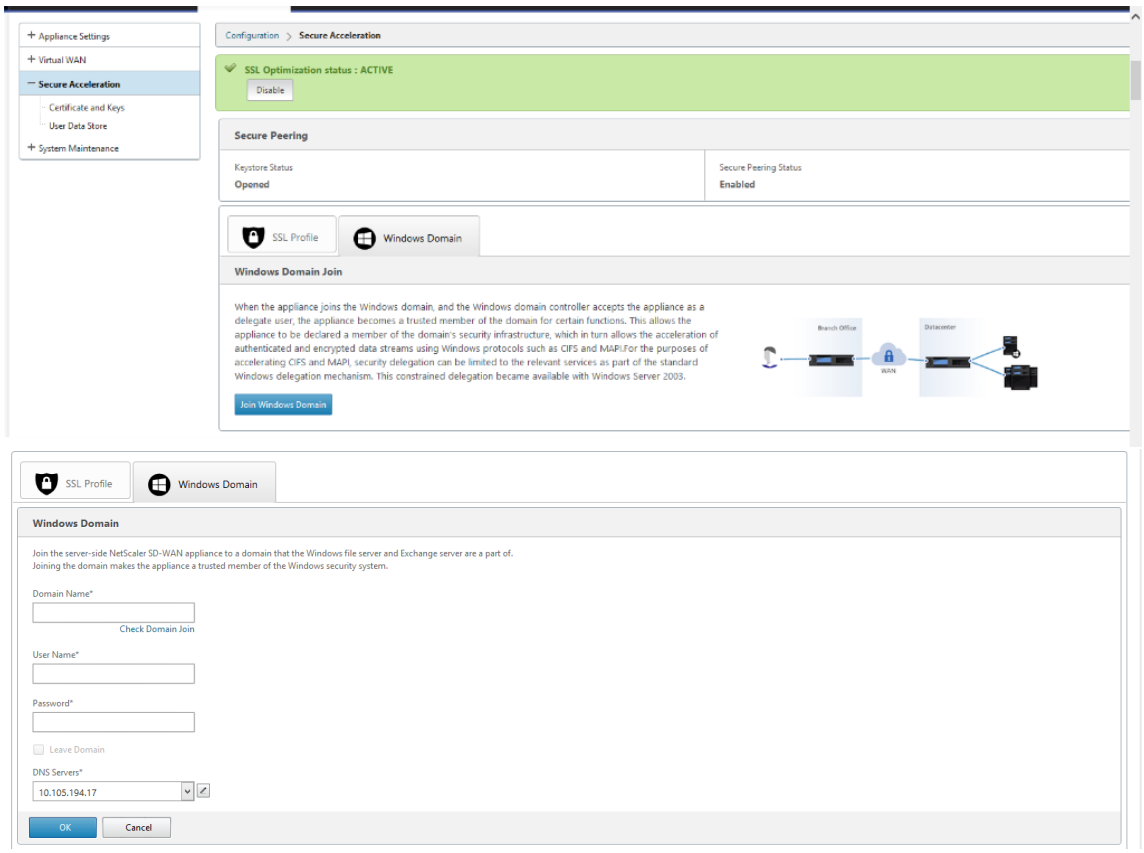


Domain join and delegate user creation

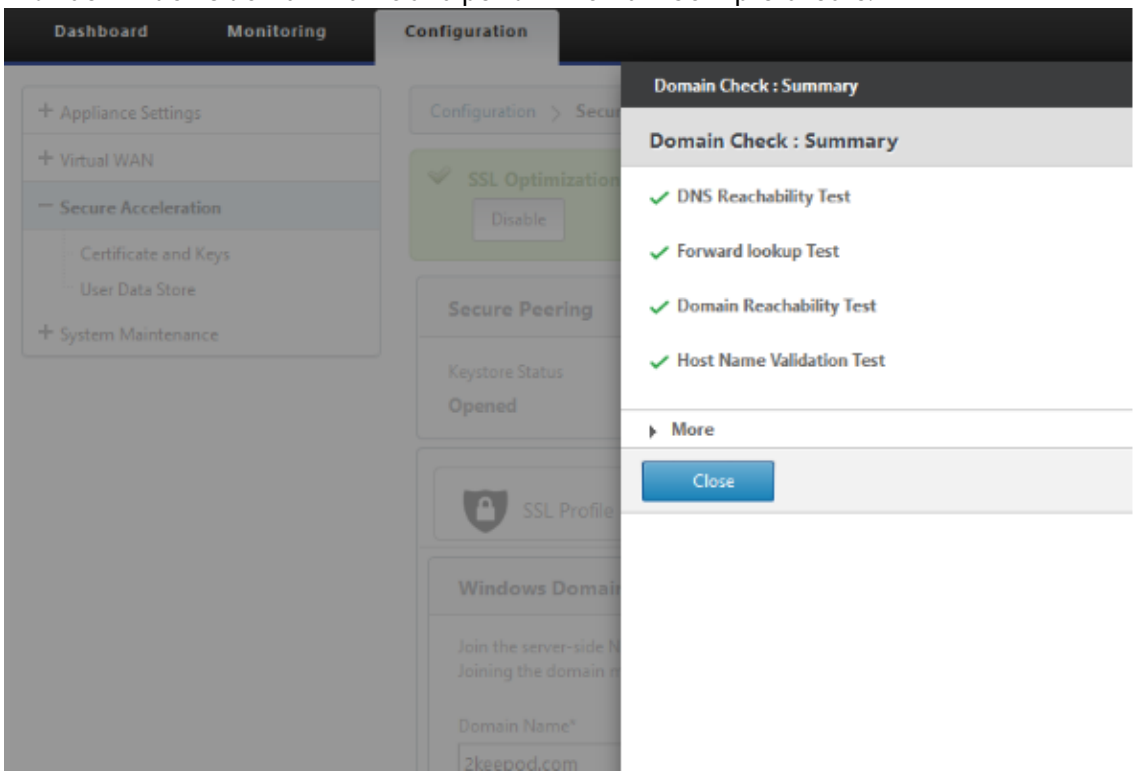
March 12, 2021

To configure new Premium (Enterprise) Edition (PE) appliance at the DC to windows domain:

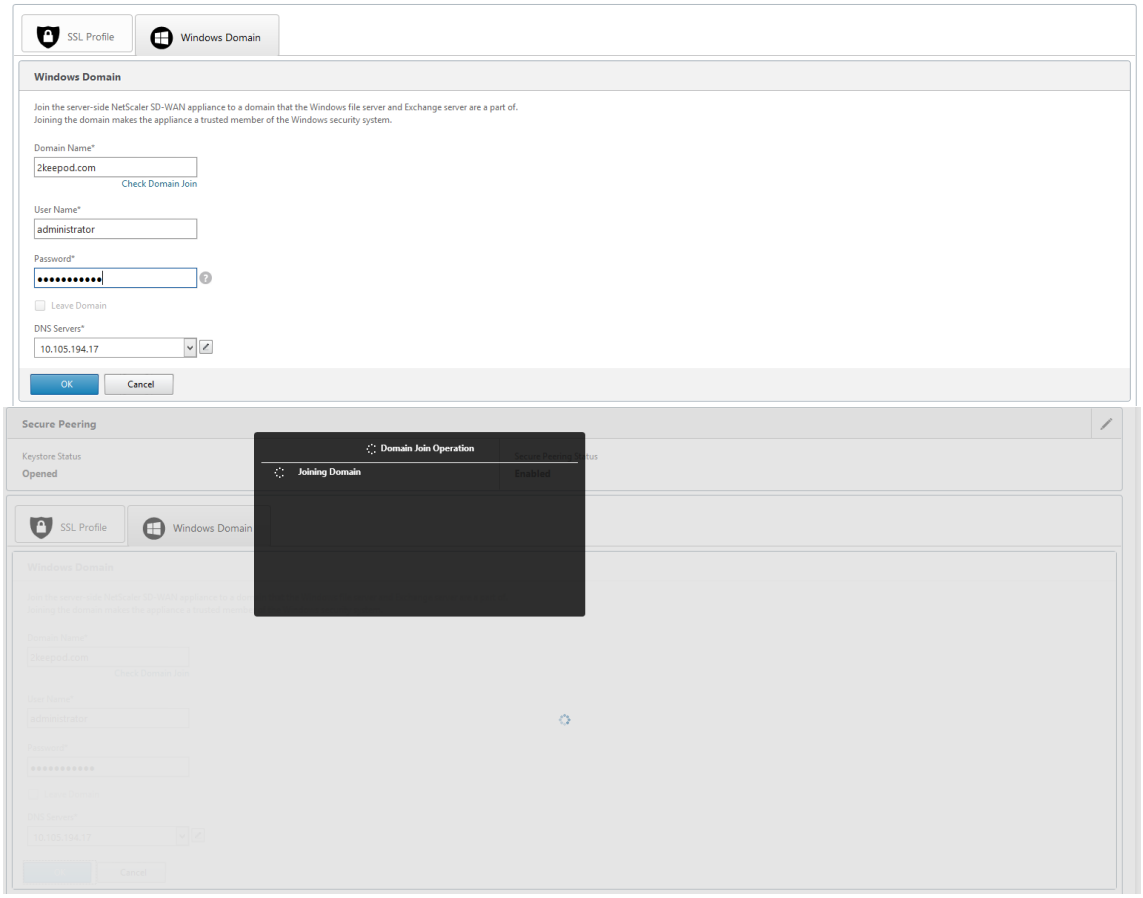
1. Go to Windows Domain in SD-WAN web GUI, navigate to **Configuration** > **Secure Acceleration** > and click **Join Windows Domain**.



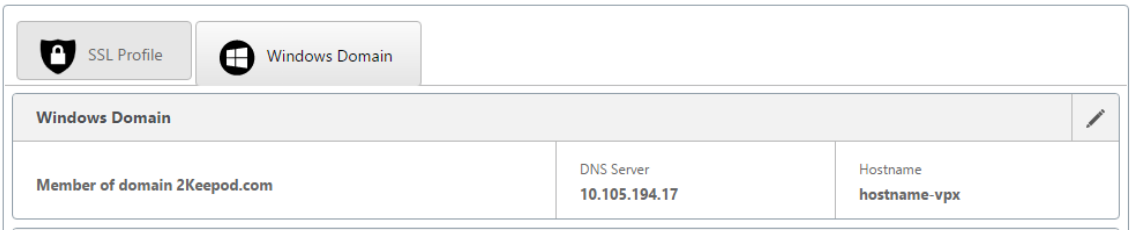
2. Provide **Windows domain name** and perform **Domain Join** pre-checks.



3. After pre-check summary shows as successful, enter domain controller's credentials.



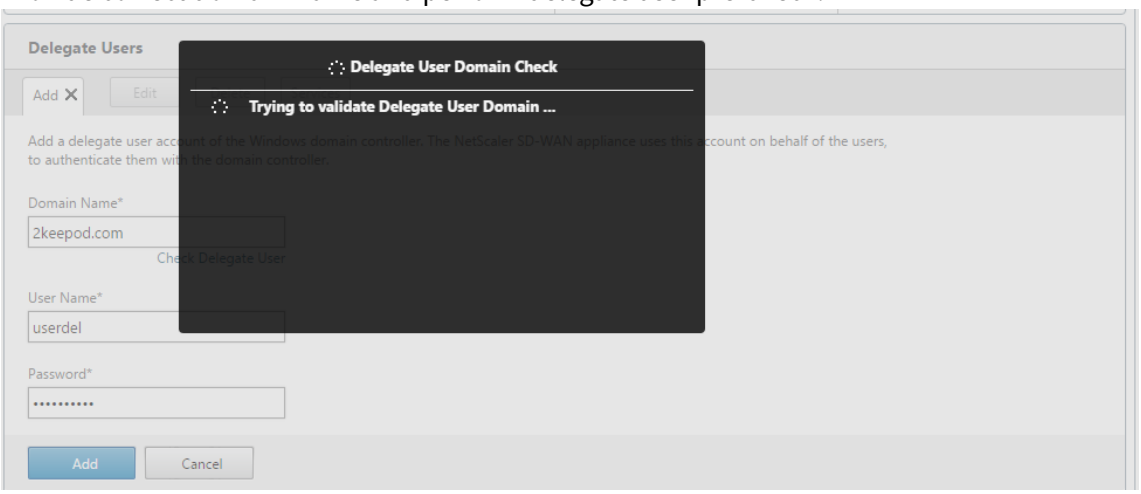
4. On successful domain join, you get the following output.

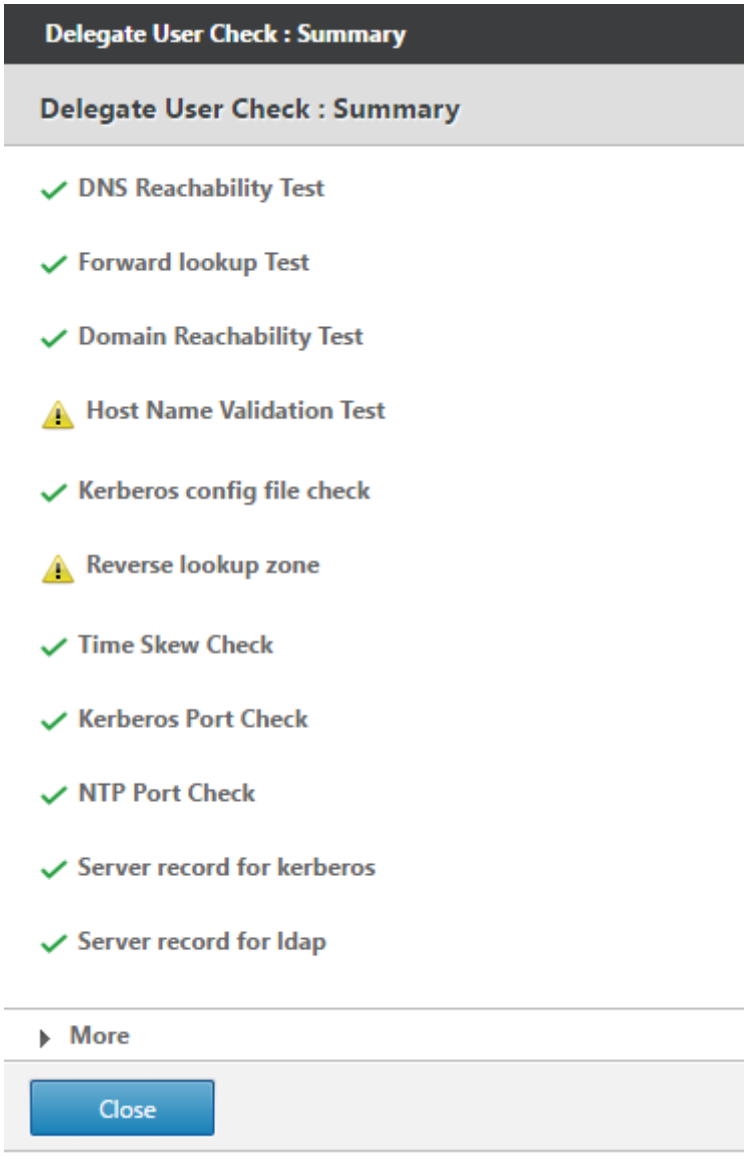


Delegate user

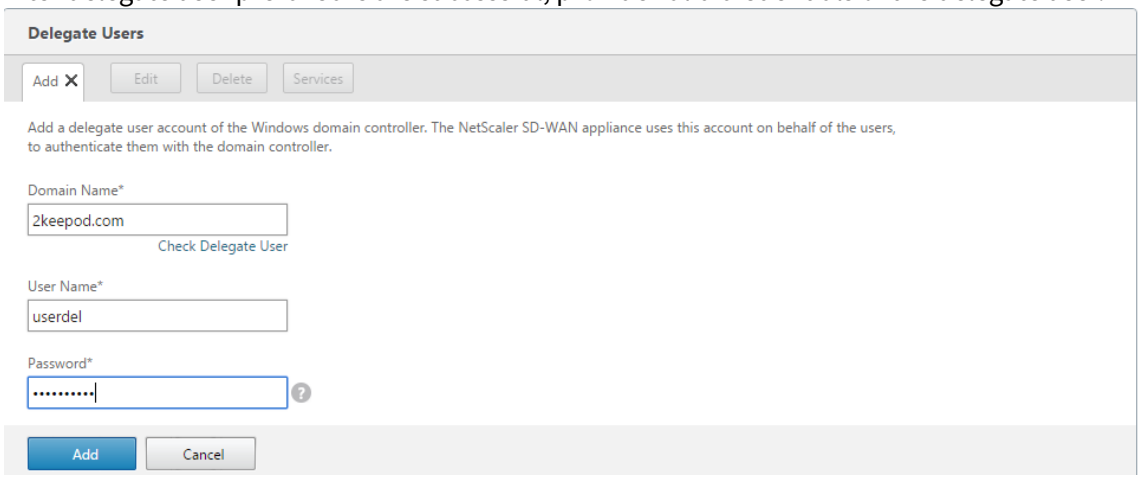
1. Add delegate user to delegate the services as shown below.

2. Provide correct domain Name and perform delegate user pre-check.

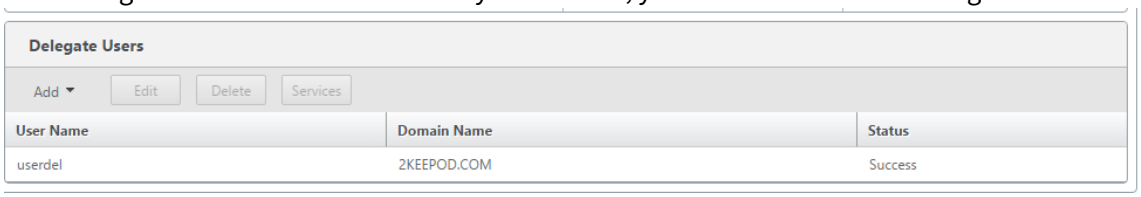




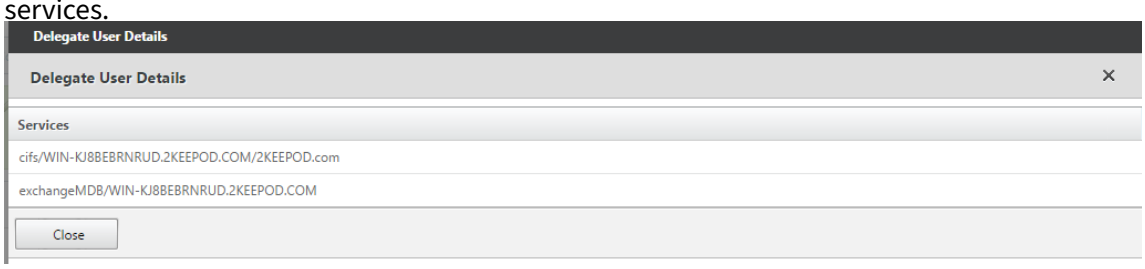
3. After delegate user pre-checks are successful, provide valid credentials of the delegate user.



4. After delegate user is added successfully to SD-WAN, you notice a success message.



5. To check what all services are delegated by the delegate user, point to the user and select services.



Security

March 12, 2021

The topics in this section provide general security guidance for Citrix SD-WAN deployments.

Citrix 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:

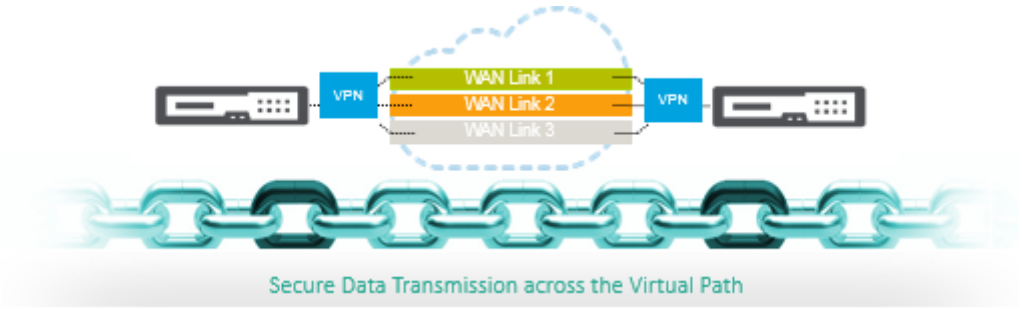
- IPsec tunnels
- Firewall

IPSec Tunnel Termination

March 12, 2021

Citrix SD-WAN supports IPsec virtual paths, enabling third-party devices to terminate IPsec VPN Tunnels on the LAN or WAN side of a Citrix 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 cryptographicbinary.

Citrix SD-WAN also supports resilient IPsec tunneling using a differentiated virtual path tunneling mechanism.



Citrix SD-WAN integration with AWS Transit Gateway

March 12, 2021

Amazon Web Service (AWS) Transit Gateway service enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. As the number of workloads running on AWS grows, you can scale your networks across multiple accounts and Amazon VPCs to keep up with the growth.

You can now connect pairs of Amazon VPCs using peering. However, managing point-to-point connectivity across many Amazon VPCs, without the ability to centrally manage the connectivity policies, can be operationally costly and cumbersome. For on-premises connectivity, you need to attach your AWS VPN to each individual Amazon VPC. This solution can be time consuming to build and hard to manage when the number of VPCs grows into the hundreds.

With **AWS Transit Gateway**, you only have to create and manage a single connection from the central gateway into each Amazon VPC, on-premises data center, or remote office across your network. The Transit Gateway acts as a hub that controls how traffic is routed among all the connected networks which act like spokes. This hub and spoke model significantly simplifies management and reduces operational costs because each network only has to connect to the Transit Gateway and not to every

other network. Any new VPC is connected to the Transit Gateway and automatically available to every other network that is connected to the Transit Gateway. This ease of connectivity makes it easy to scale your network as you grow.

As enterprises migrate an increasing number of applications, services, and infrastructure to the cloud, they are rapidly deploying SD-WAN to realize the benefits of broadband connectivity and to directly connect branch site users to cloud resources. There are many challenges with the complexities of building and managing global private networks using internet transport services to connect geographically distributed locations and users with proximity-based cloud resources. The **AWS Transit Gateway Network Manager** changes this paradigm. Now, Citrix SD-WAN customers who use AWS can use Citrix SD-WAN with AWS transit gateway by integrating Citrix SD-WAN branch appliance AWS Transit Gateway to deliver the highest quality of experience for users with the ability to reach out to all VPCs connected to the Transit Gateway.

The following are the steps to integrate Citrix SD-WAN with AWS Transit Gateway:

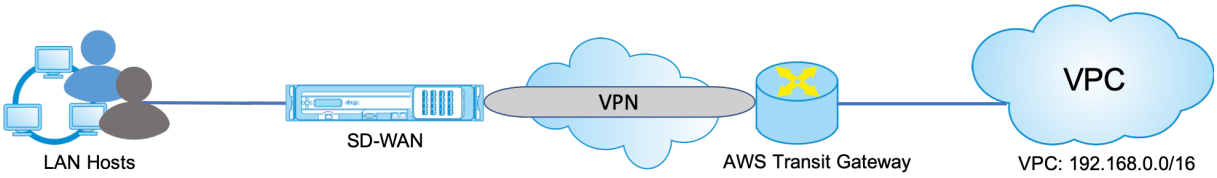
1. Create the AWS Transit Gateway.
2. Attach a VPN to the Transit Gateway (either existing VPN or a new one).
3. Attach VPN to the configured Transit Gateway where the VPN is with SD-WAN site located On-prem or in any cloud (AWS, Azure, or GCP).
4. Establish the Border Gateway Protocol (BGP) peering over the IPsec Tunnel with the AWS Transit Gateway from Citrix SD-WAN to learn the networks (VPCs) attached to Transit Gateway.

Use case

The use case is to reach out to resources deployed within AWS (in any VPC) from the branch environment. Using AWS Transit Gateway allows the traffic to reach to all VPCs connected to the Transit Gateway without dealing with BGP routes. To achieve this, perform the following methods:

- Establish the IPsec to AWS Transit Gateway from the branch Citrix SD-WAN appliance. In this deployment method you will not get full SD-WAN benefits as the traffic will go over IPsec.
- Deploy a Citrix SD-WAN appliance within AWS and connect it to your On-prem Citrix SD-WAN appliance via virtual path.

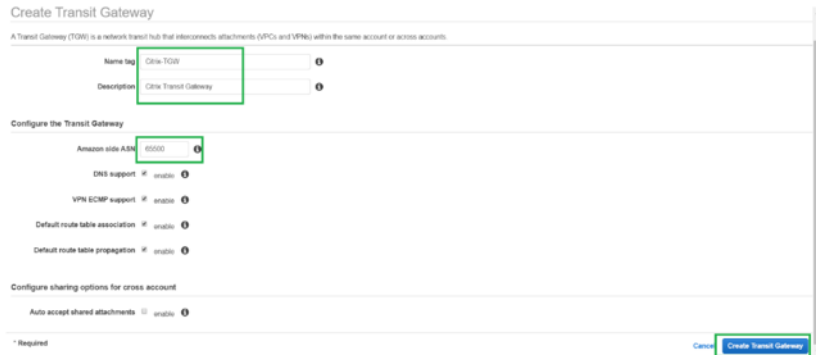
Regardless of which method is chosen, the traffic reaches to the VPCs connected to the Transit Gateway without manually manage the routing within AWS infra.



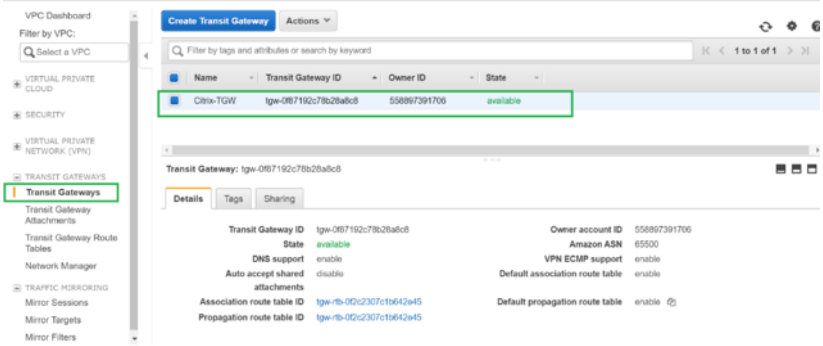
AWS Transit Gateway configuration

To create the **AWS Transit Gateway**, navigate to VPC dashboard and go to **Transit Gateway** section.

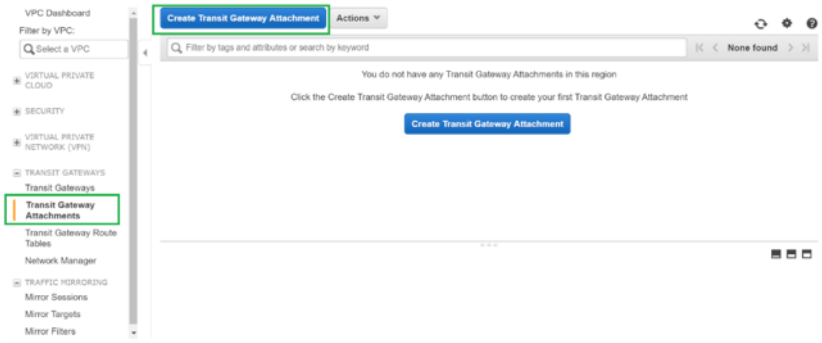
1. Provide the Transit Gateway Name, Description, and Amazon ASN number as highlighted in the following screenshot and click **Create Transit Gateway**.



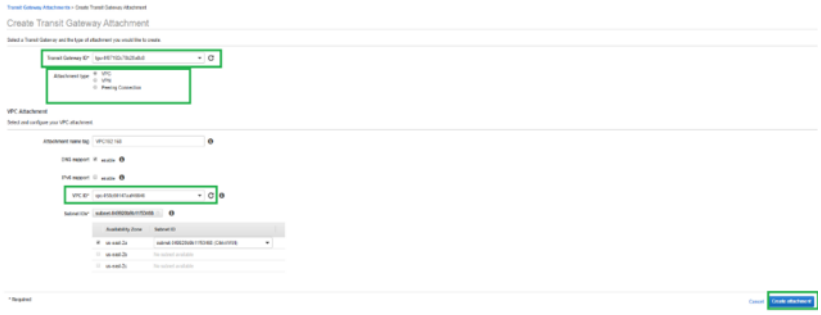
Once the Transit Gateway creation is completed, you can see the status as **Available**.



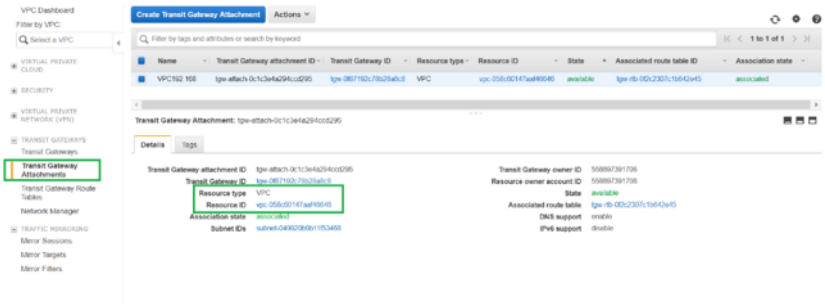
2. To create the **Transit Gateway Attachments**, navigate to **Transit Gateways > Transit Gateway Attachments** and click **Create Transit Gateway Attachment**.



3. Select the Transit Gateway created from the drop-down list and select attachment type as **VPC**. Provide the attachment name tag and select the VPC ID that you want to attach to the Transit Gateway created. One of the subnets from the selected VPC will be auto selected. Click **Create Attachment** to attach VPC to the Transit Gateway.

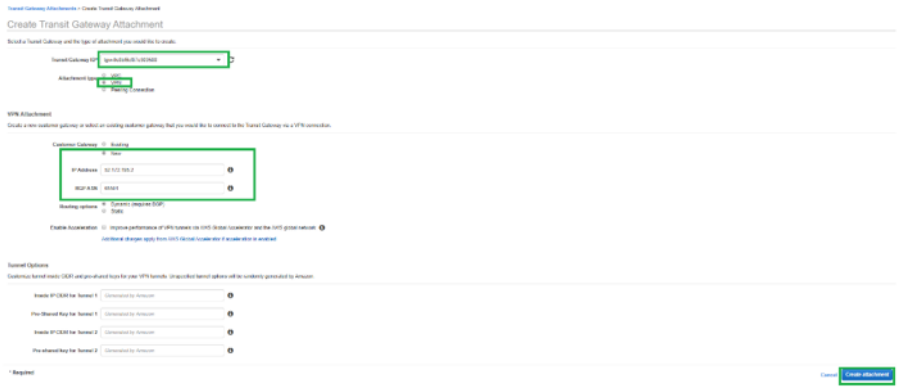


4. After attaching the VPC to the transit gateway, you can see that the **Resource type VPC** got associated to the Transit Gateway.

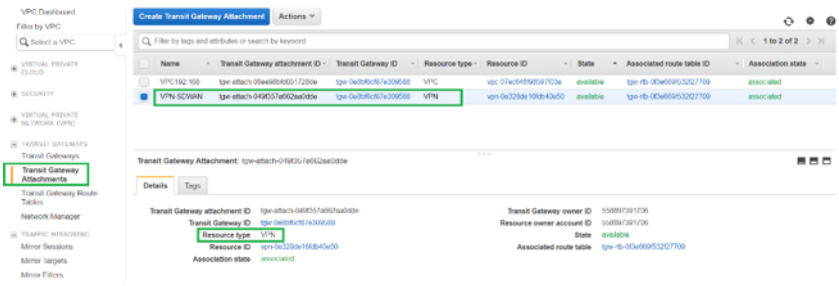


5. To attach SD-WAN to the Transit Gateway using VPN, select the **Transit Gateway ID** from the drop-down list and select **Attachment type** as **VPN**. Ensure that you select the correct Transit Gateway ID.

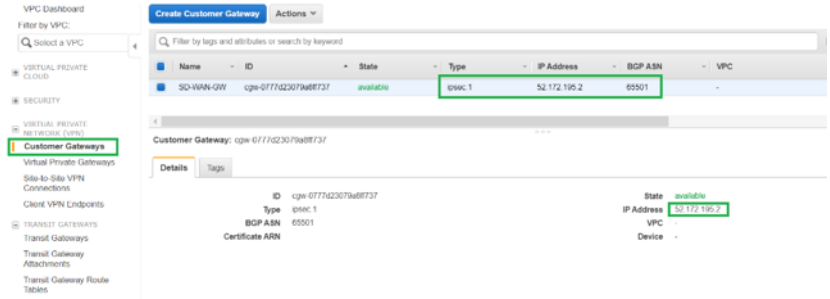
   Attach a new VPN Customer Gateway by providing the SD-WAN WAN link Public IP address and its BGP ASN Number. Click **Create Attachment** to attach VPN with Transit Gateway.



6. Once the VPN Attached to the Transit Gateway, you can view the details as shown in the following screenshot:

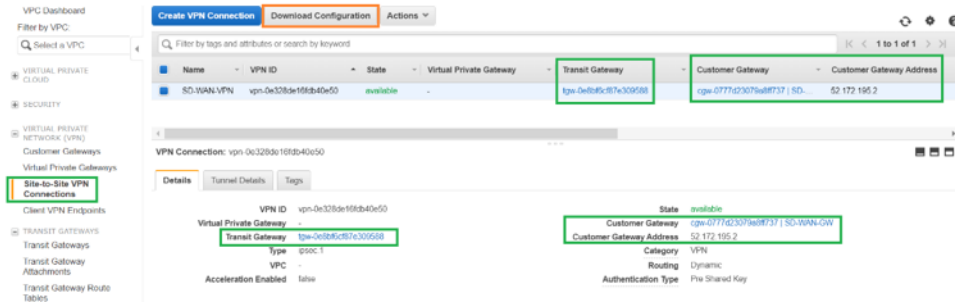


7. Under **Customer Gateways**, SD-WAN Customer Gateway and Site-to-Site VPN Connection is created as part of VPN Attachment to Transit Gateway. You can see that the SD-WAN Customer Gateway is created along with the IP address of this Customer Gateway that represents the WAN link Public IP address of SD-WAN.

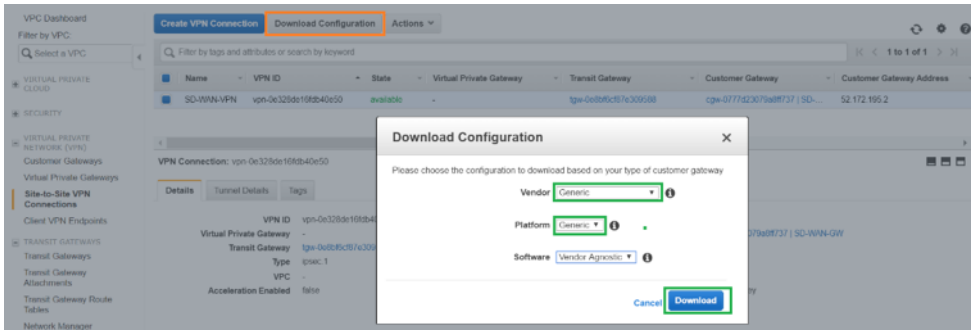


8. Navigate to **Site-to-Site VPN Connections** to download **SD-WAN Customer Gateway VPN Configuration**. This configuration file has two IPsec Tunnel details along with the BGP peer information. Two tunnels are created from SD-WAN to Transit Gateway for redundancy.

   You can see that SD-WAN WAN link Public IP address was configured as the Customer Gateway Address.



9. Click **Download Configuration** and download the VPN configuration file. Select the **Vendor**, **Platform** as **Generic**, and **Software** as **Vendor Agnostic**.



The downloaded configuration file contains the following information:

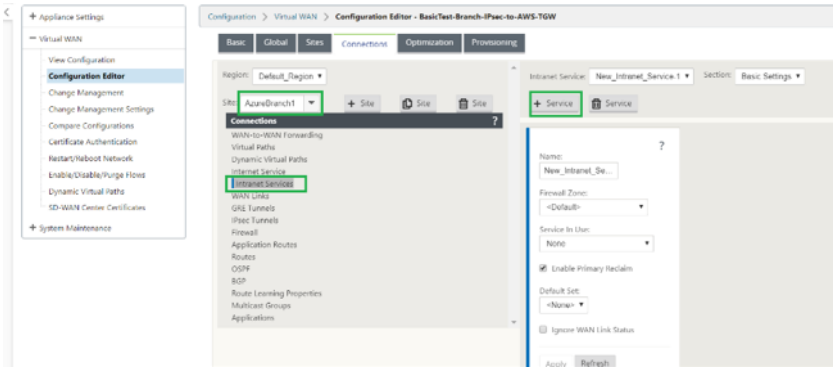
- IKE config
- IPsec configuration for AWS Transit Gateway
- Tunnel interface configuration
- BGP configuration

This information is available for two IPsec tunnels for High Availability (HA). Ensure that you configure both the tunnel end points while configuring this in SD-WAN. See the following screenshot for reference:

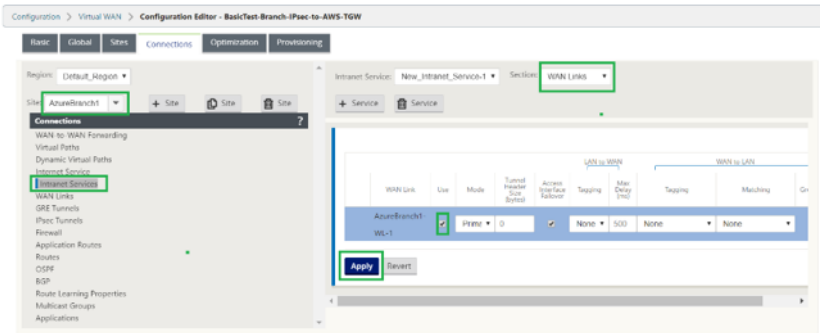
```
#3: Tunnel Interface Configuration

Your Customer Gateway must be configured with a tunnel interface that is
associated with the IPSec tunnel. All traffic transmitted to the tunnel
interface is encrypted and transmitted to the Virtual Private Gateway.


The Customer Gateway and Virtual Private Gateway each have two addresses that relate
to this IPSec tunnel. Each contains an outside address, upon which encrypted
traffic is exchanged. Each also contain an inside address associated with
the tunnel interface.

The Customer Gateway outside IP address was provided when the Customer Gateway
was created. Changing the IP address requires the creation of a new
Customer Gateway.

The Customer Gateway inside IP address should be configured on your tunnel
interface.

Outside IP Addresses:
  - Customer Gateway                  : 52.172.195.2
  - Virtual Private Gateway           : 3.133.37.22

Inside IP Addresses
  - Customer Gateway                  : 169.254.216.178/30
  - Virtual Private Gateway           : 169.254.216.177/30

Configure your tunnel to fragment at the optimal size:
  - Tunnel interface MTU     : 1436 bytes
```

Configure Intranet service on SD-WAN

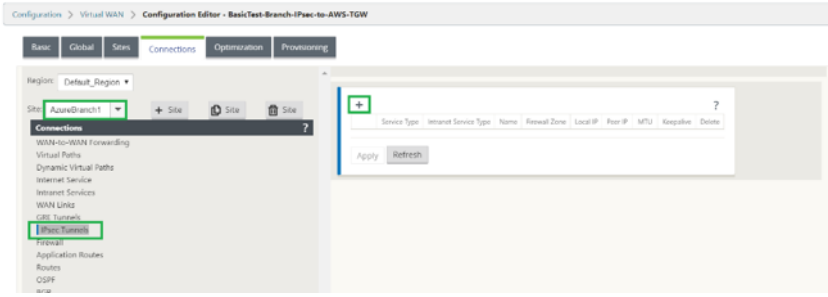
1. To configure the Intranet service that is used in the IPsec tunnel configuration on SD-WAN, navigate to **Configuration Editor > Connections >**, select the site from the drop-down list, and select **Intranet Service**. Click **+ Service** to add a new Intranet service.



2. After addition of Intranet service, select the WAN link (Using which you are going to establish the Tunnel towards Transit Gateway) that is used for this service.

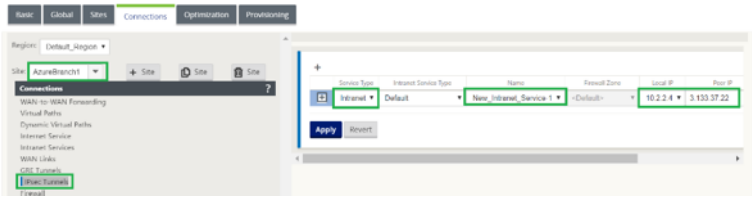


3. To configure IPsec tunnel towards AWS Transit Gateway, navigate to **Configuration Editor > Connections >** select the Site from the drop-down list and click **IPsec Tunnels**. Click **+** option to add IPsec Tunnel.

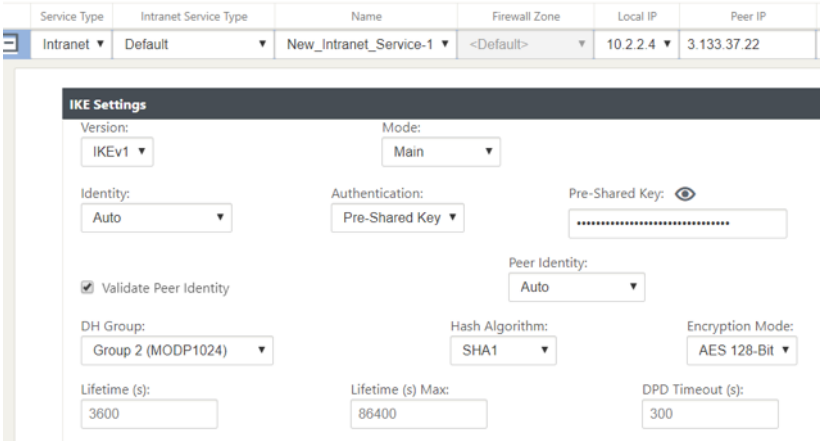


4. Select the **Service Type** as **Intranet** and select the **Intranet service Name** that you have added. Select the **Local IP** address as the WAN Link IP Address and **Peer** address as Transit Gateway Virtual Private Gateway IP address.

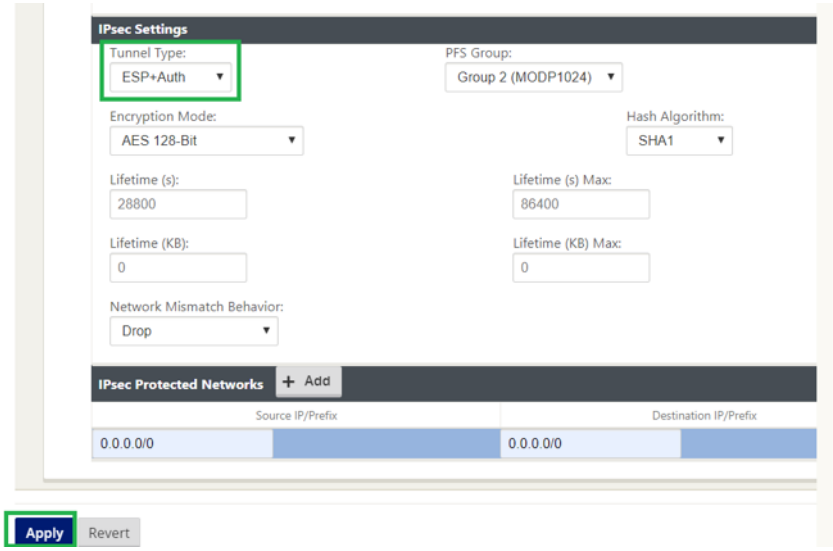
   Click **Keepalive** check box to have the tunnel initiated by SD-WAN immediately after config activation.



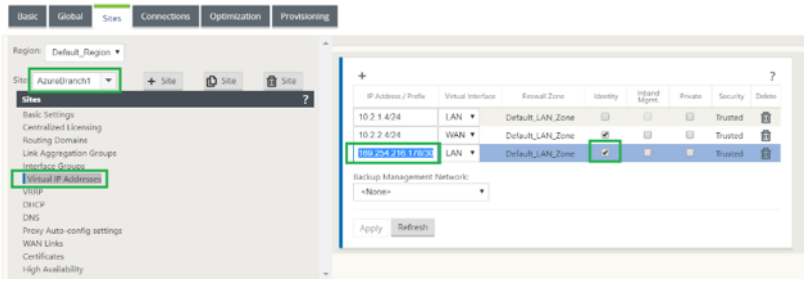
5. Configure IKE Parameters based on the VPN configuration file that you have downloaded from AWS.



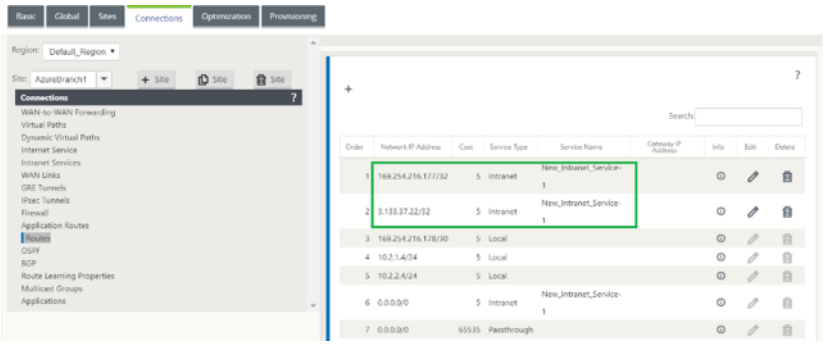
6. Configure IPsec parameters based on the VPN configuration file that you have downloaded from AWS. Also configure **IPsec Protected Networks** based on the network that you want to send through the tunnel. You can see that it's configured to allow any traffic through IPsec Tunnel.



7. Configure the **Customer Gateway inside IP address** as one of the Virtual IP addresses on SD-WAN. From the VPN Configuration File downloaded, locate the customer gateway inside IP Address related to Tunnel-1. Configure this customer gateway inside IP Address as one of the Virtual IP addresses on SD-WAN and enable the **Identity** check box.

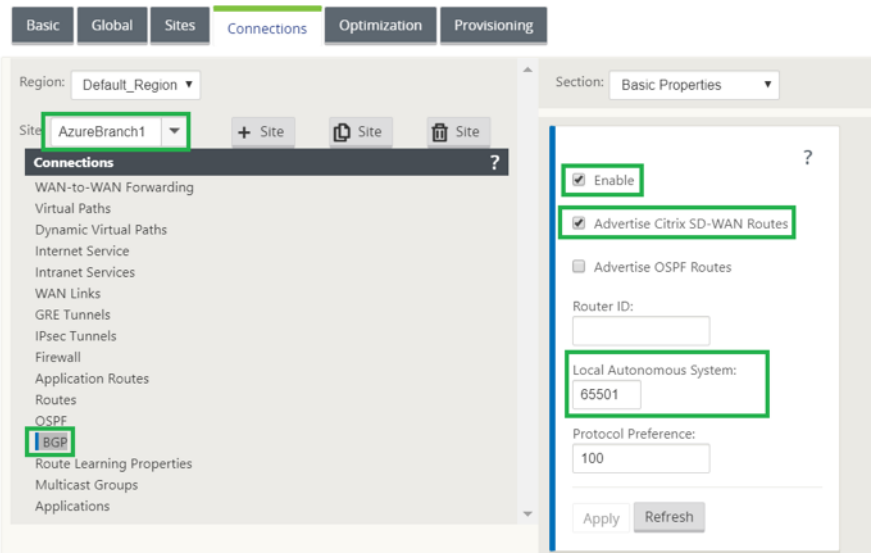


8. Add **Routes** on SD-WAN to reach **Virtual Private Gateway** of Transit Gateway. From the VPN Configuration File downloaded, locate inside and outside IP address of Virtual Private Gateway related to Tunnel-1. Add routes to inside and outside IP address of Virtual Private Gateway with **Service Type** as **Intranet** and select the Intranet service created in the above steps.



9. Configure **BGP** on SD-WAN. Enable BGP with appropriate ASN Number. From the VPN Configuration File downloaded, locate BGP configuration options related to Tunnel-1. Use these details to add BGP neighbor on SD-WAN.

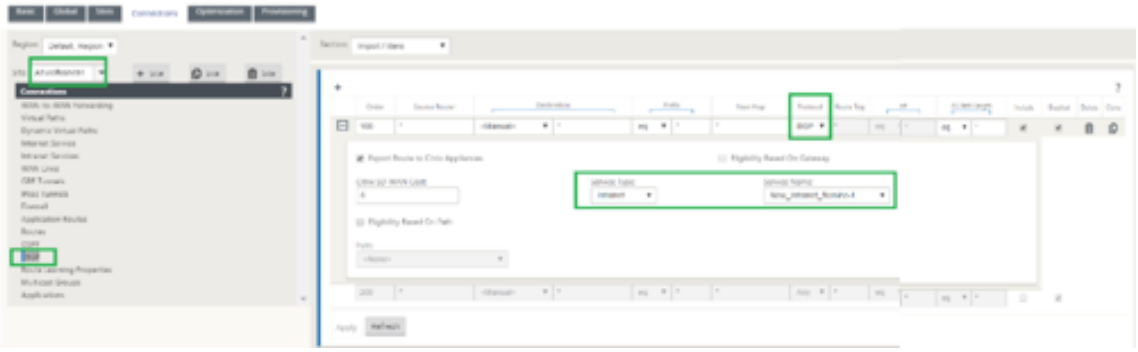
   To enable BGP on SD-WAN, navigate to **Connections** select the site from the drop-down list, then select **BGP**. Click **Enable** check box to enable BGP. Click **Advertise Citrix SD-WAN Routes** check box to advertise SD-WAN routes towards Transit Gateway. Use the **Customer Gateway ASN** from the BGP configuration options and configure that as **Local Autonomous System**.



10. To add BGP **Neighbors** on SD-WAN, navigate to **Connections >** select the site from the drop-down list, then select **BGP**. Click **Neighbors** section and click **+** option.

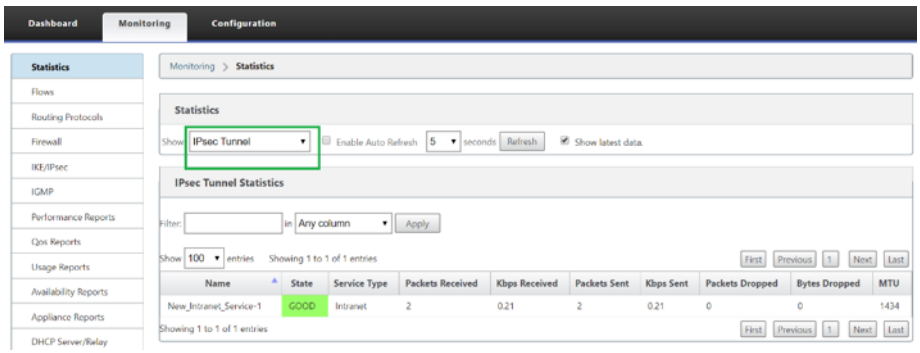
    Use **Neighbor IP Address** and **Virtual Private Gateway ASN** from the BGP configuration options while adding neighbor. The **Source IP** must match **Customer Gateway** inside IP address(Configured as Virtual IP Address on SD-WAN) from the downloaded configuration file from AWS. Add BGP Neighbor with **Multi Hop** enabled on SD-WAN.

11. To add **Import Filters** to import BGP routes onto SD-WAN, navigate to **Connections**, select the site from the drop-down list, then select **BGP** and click **Import Filters** section. Click **+** option to add an Import filter. Select the **Protocol** as **BGP** and match any to import all BGP routes. Select the **Service type** as **Intranet** and select the created Intranet service. This is to import BGP routes with service type as Intranet.

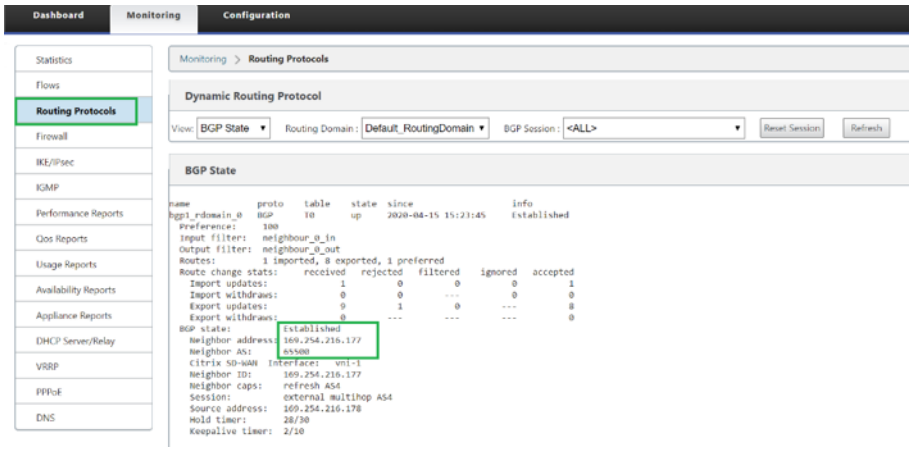


Monitoring and Troubleshooting on SD-WAN

1. To verify the IPsec Tunnel establishment status on SD-WAN, navigate to **Monitoring > Statistics > IPsec Tunnel**. In the following screenshot, you can see that the IPsec Tunnel is established from SD-WAN towards AWS Transit Gateway and the state is **GOOD**.
   Also, you can monitor the amount of traffic sent and received over this IPsec Tunnel.

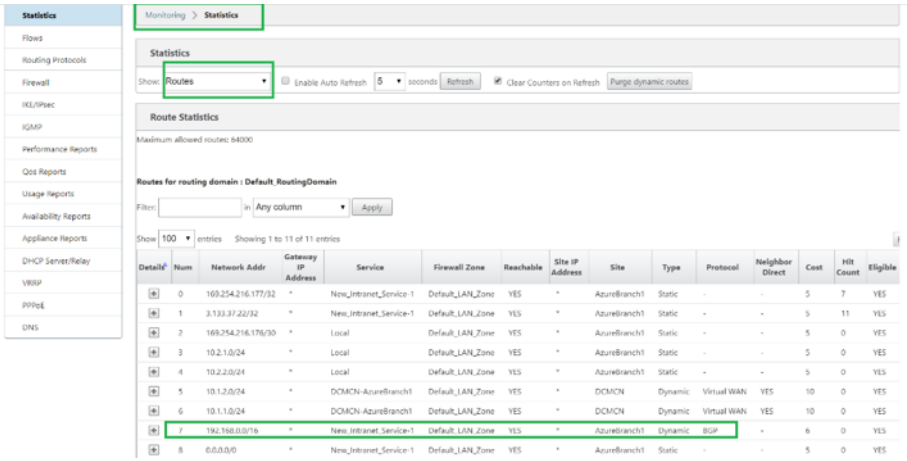


2. To verify the **BGP Peering** status on SD-WAN, navigate to **Monitoring > Routing Protocols** and select **BGP State**. You can see that the BGP state was reported as **Established** and the **Neighbor IP address** and **Neighbor ASN** are matching AWS BGP neighbor details. With this you can ensure that the BGP peering got established from SD-WAN to AWS transit Gateway through IPsec tunnel.



   A VPC (192.168.0.0) is attached to AWS Transit Gateway. SD-WAN has learned this VPC network(192.168.0.0) from AWS Transit Gateway through BGP
   And this route was installed on SD-WAN with service type as Intranet as per the import filter created in above steps.

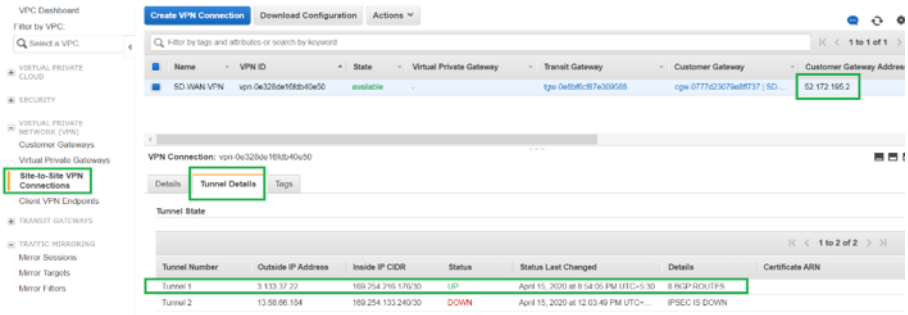
3. To verify the BGP route installation on SD-WAN, navigate to **Monitoring > Statistics > Routes** and check for the network 192.168.0.0/16 that got installed as BGP route with service type as Intranet. This means you can learn the networks attached to AWS Transit Gateway and can communicate to those networks through IPsec Tunnel established.



Monitoring and Troubleshooting on AWS

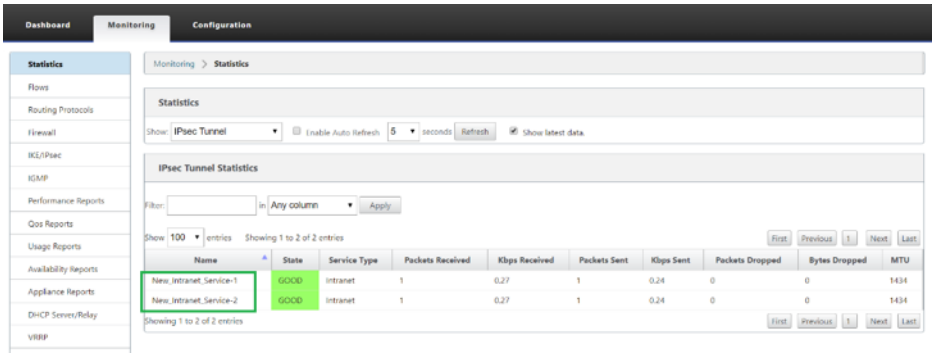
1. To verify the IPsec Tunnel establishment status on AWS, Navigate to **VIRTUAL PRIVATE NETWORK(VPN) > Site-to-Site VPN Connections**. In the following screenshot, you can observe that the Customer Gateway Address represents SD-WAN Link Public IP address using which you have established tunnel.

   The Tunnel status is shown as **UP**. Also it can be observed that AWS has learned **8 BGP ROUTES** from SD-WAN. This means SD-WAN is able to establish Tunnel with AWS Transit Gateway and also able to exchange routes over BGP.

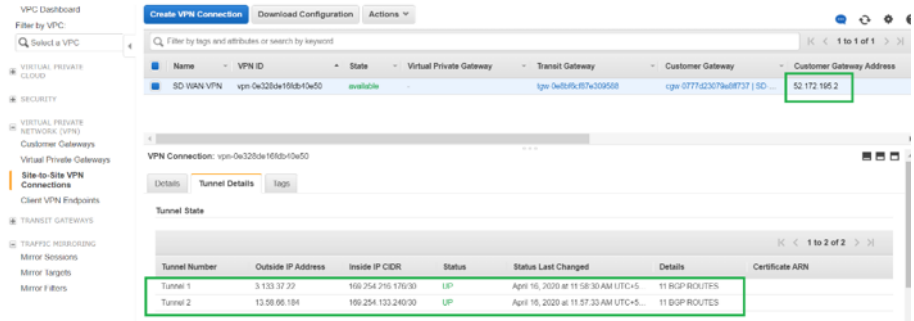


2. Configure IPsec and BGP details related to the second tunnel based on the downloaded configuration file on SD-WAN.

   Status related to both the tunnels can be Monitored on SD-WAN as follows:



3. Status related to both the tunnels can be Monitored on AWS as follows:

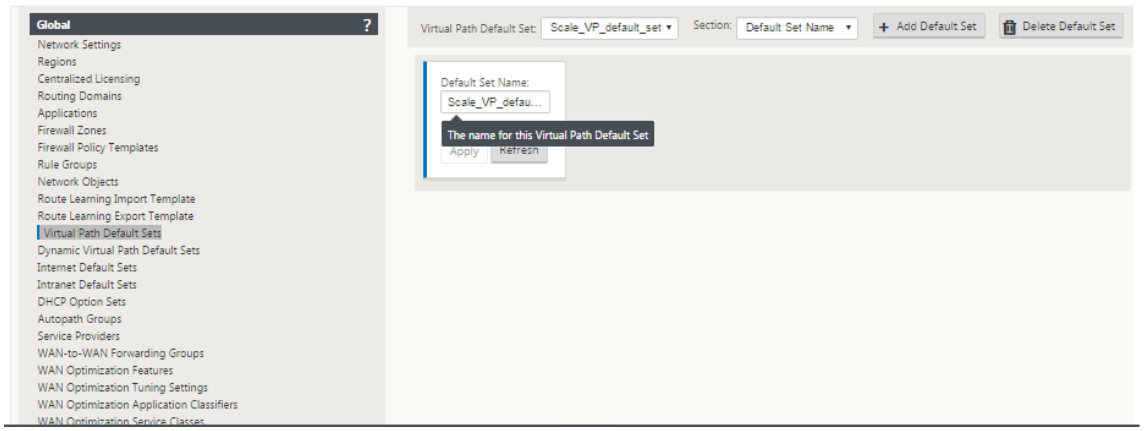


How to configure IPsec tunnels for virtual and dynamic paths

March 12, 2021

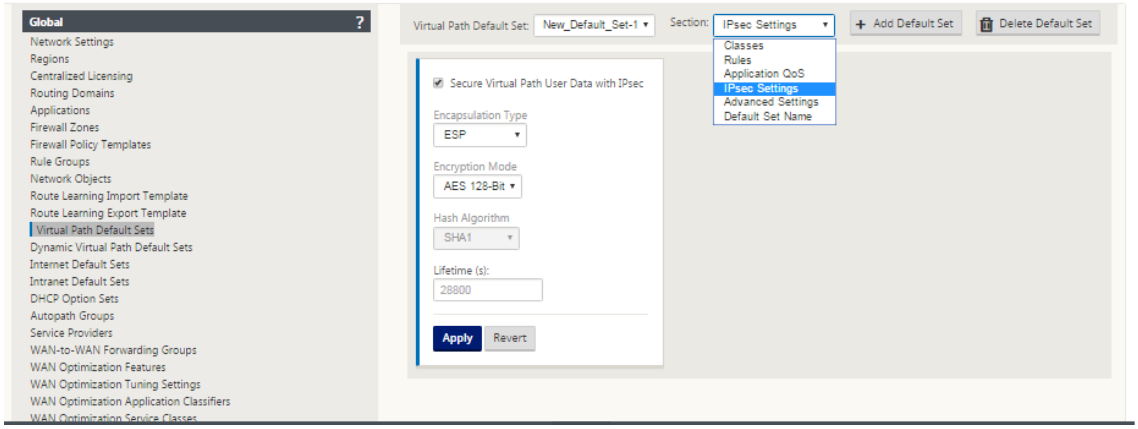
To configure IPsec tunnels for virtual and dynamic virtual paths between Citrix SD-WAN branch sites:

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-CBC, 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.

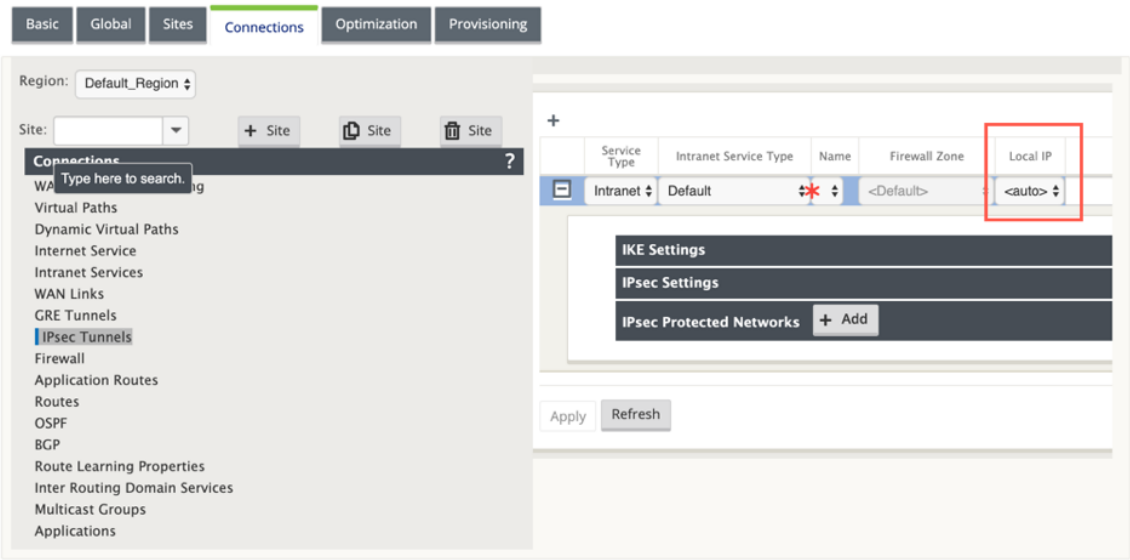


How to configure IPsec tunnel between SD-WAN and third-party devices

March 12, 2021

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 determines which Local IP addresses are available.



Citrix SD-WAN can now establish IPsec tunnels when a WAN link is directly terminated on the appliance and a dynamic IP is being assigned to the WAN link.

With 11.1.0 release, Intranet IPsec tunnels must be configurable when the local tunnel IP address is not or cannot be known. This helps in creating IPsec tunnels on the interfaces whose address is assigned through DHCP.

While configuring the interface for IPsec tunnel, a local tunnel IP must be mentioned. This interface is modified to allow an empty IP to be selected when the tunnel type is **Intranet**.

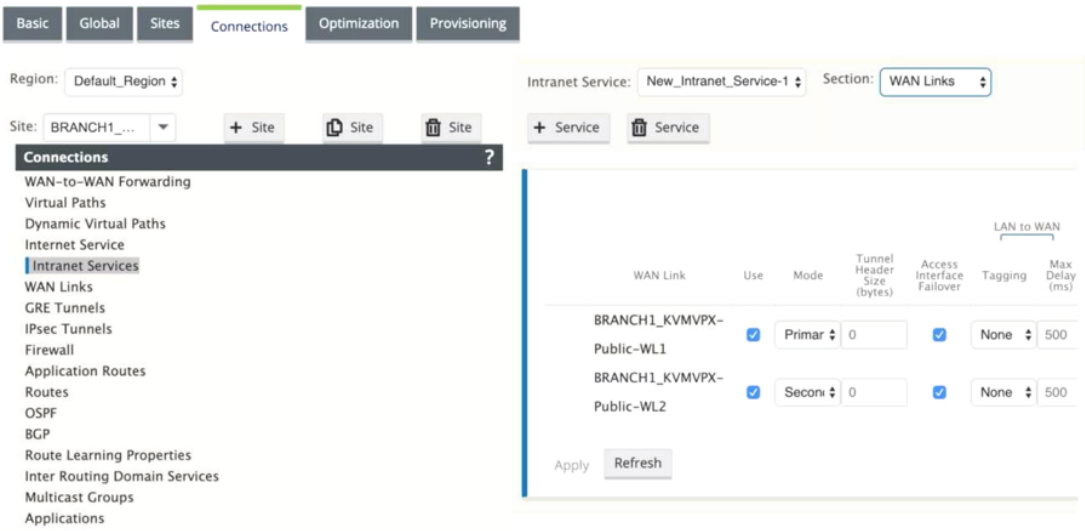
Also, the label for an unset address is changed to **Auto** when the tunnel type is **Intranet**.

If the Local IP is set as **Auto**, it has the ability of taking the IP address that is incorporated for the access interface on that WAN link. That WAN link access interface might get the IP either statically configured or from DHCP. IPsec tunnel is established using the primary WAN link access interface by default.

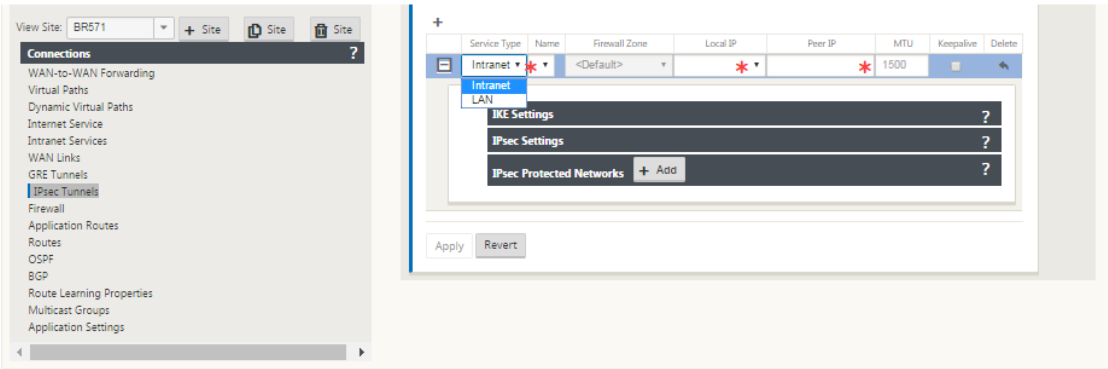
Earlier, you can establish IPsec tunnels over a single WAN link. This exposes the branch environment to service loss during periods of outright link failures and when packet loss on a link is inadvertently high to allow for reliable connectivity.

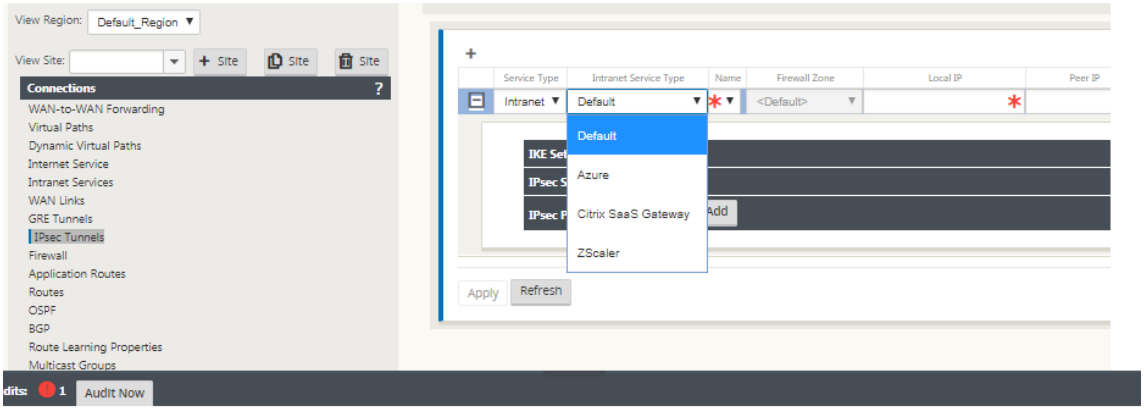
From 11.1.0 release onwards, you can use two WAN links for establishing IPsec tunnels to guard branch environments against periods of service disruption. If the primary link goes down, the secondary link turns active/up within milliseconds.

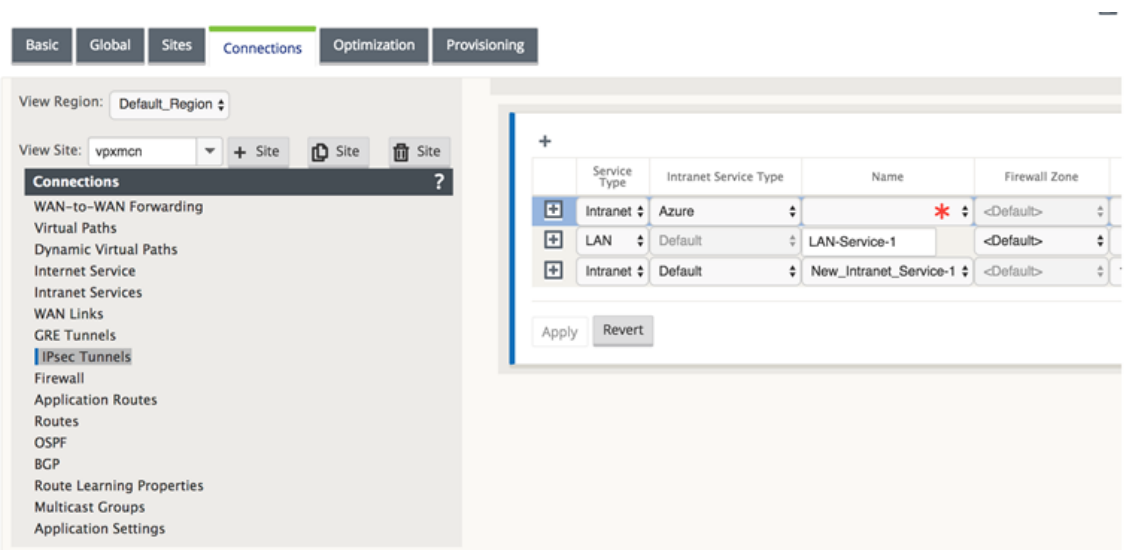
> **Note**
>
> When the <**Auto**> option is selected, the IPsec tunnel is established using the primary WAN link access interface. If the primary wan link goes down IPsec tunnel is established using the secondary WAN link access interface.



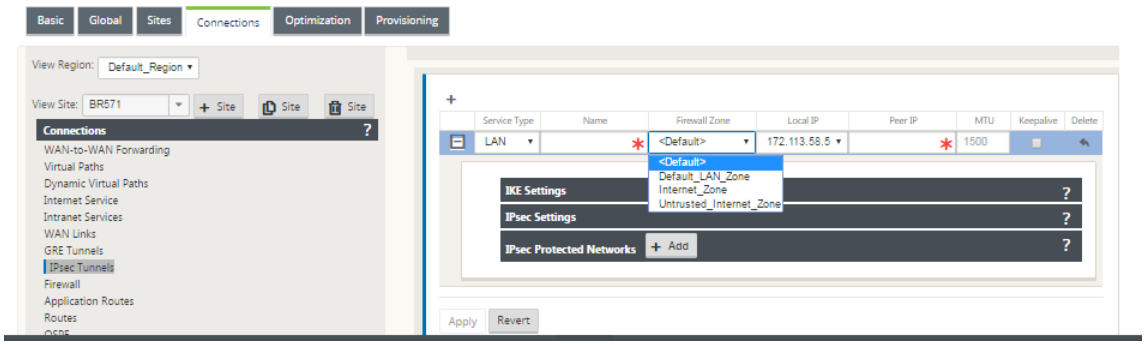
3. Select the available **Local IP** address and enter the **Peer IP** address of the IPsec tunnel.







> **Note**
>
> If the Service Type is Intranet, the IP address is pre-determined by the chosen Intranet Service.



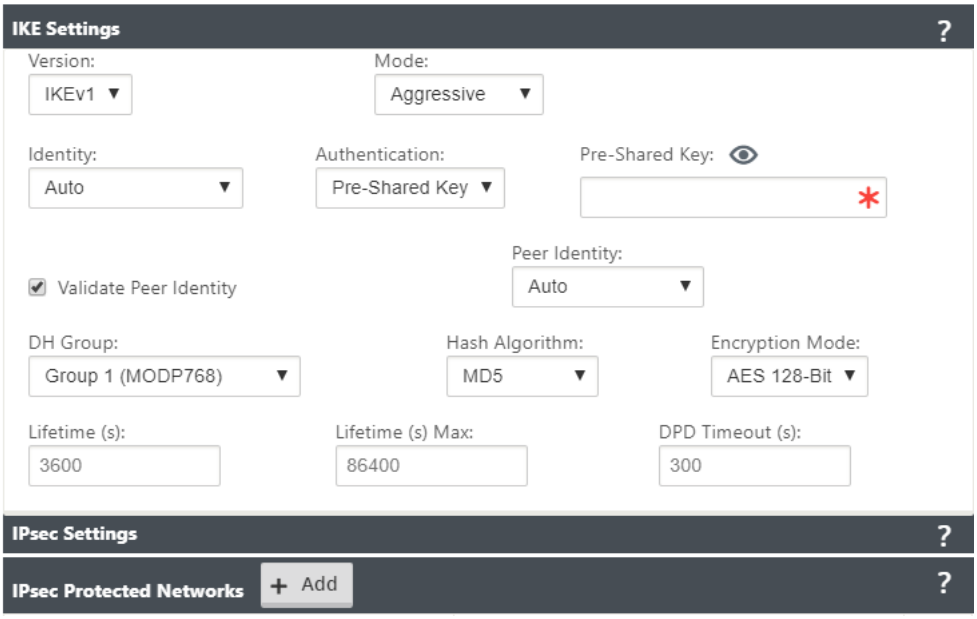
4. Configure IPsec settings by applying the criteria described in the following tables. When finished, click **Apply** to save your settings.

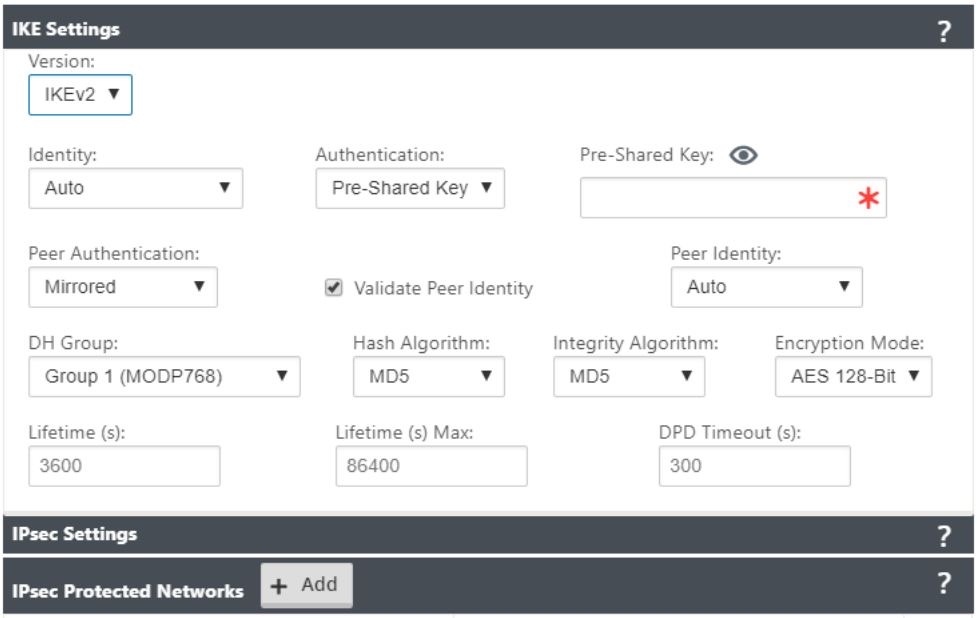
Field	Description	Value
Service Type	Choose a service type from the drop-down menu	Intranet, LAN
Name	If the service type is Intranet, choose from the list of configured intranet services in the drop-down menu. If the service type is LAN, enter a unique name	Text string

Field	Description	Value
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	IP address
Peer IP	Enter the peer IP address of the IPsec Tunnel	IP address
MTU	Enter the **MTU** for fragmenting IKE and IPsec fragments	Default: 1500
IKE Settings	Version: Choose an IKE version from the drop-down menu	IKEv1 IKEv2
Mode	Choose a mode from the drop-down menu	FIPS compliant: Main, Non-FIPS compliant: Aggressive
Identity	Choose an Identity from the drop-down menu	Auto IP Address Manual IP Address User FQDN
Authentication	Choose the authentication type from the drop-down menu	Pre-Shared Key: If you are using a pre-shared key, copy and paste it into this field. Click the Eyeball () icon to view the Pre-Shared Key. Certificate: If you are using an identity certificate, choose it from the drop-down menu.
Validate Peer Identity	Select this check box to validate the IKE's peer. If the peer's ID type is not supported, do not enable this feature	None
DH Group	Choose Diffie-Hellman group to use for IKE key generation from the drop-down menu	Non-FIPS compliant: Group 1, FIPS-compliant: Group 2 Group 5 Group 14 Group 15 Group 16 Group 19 Group 20 Group 21
Hash Algorithm	Choose an algorithm from the drop-down menu to authenticate IKE messages	Non-FIPS compliant: MD5 FIPS compliant: SHA1 SHA-256

Field	Description	Value
Encryption Mode	Choose the **Encryption Mode** for IKE messages from the drop-down menu	AES 128-bit AES 192-bit AES 256-bit
Lifetime (s)	Enter the preferred duration, in seconds, for an IKE security association to exist	3600 seconds (default)
Lifetime (s) Max	Enter the maximum preferred duration, in seconds, to allow an IKE security association to exist	86400 seconds (default)
DPD Timeout (s)	Enter the **Dead Peer Detection timeout**, in seconds, for VPN connections	300 seconds (default)
IKEv2	Peer Authentication: Choose **Peer Authentication** from the drop-down menu	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	Text string
Integrity Algorithm	Choose an algorithm as the hashing algorithm to use for HMAC verification from the drop-down menu	Non-FIPS compliant: MD5 FIPS compliant: SHA1 SHA-256

> **Note:**
>
> If the terminating IPsec router includes Hash-based Message Authentication Code (HMAC) in the config, change the IPsec mode to **EXP+Auth** with a hashing algorithm as **SHA1**.



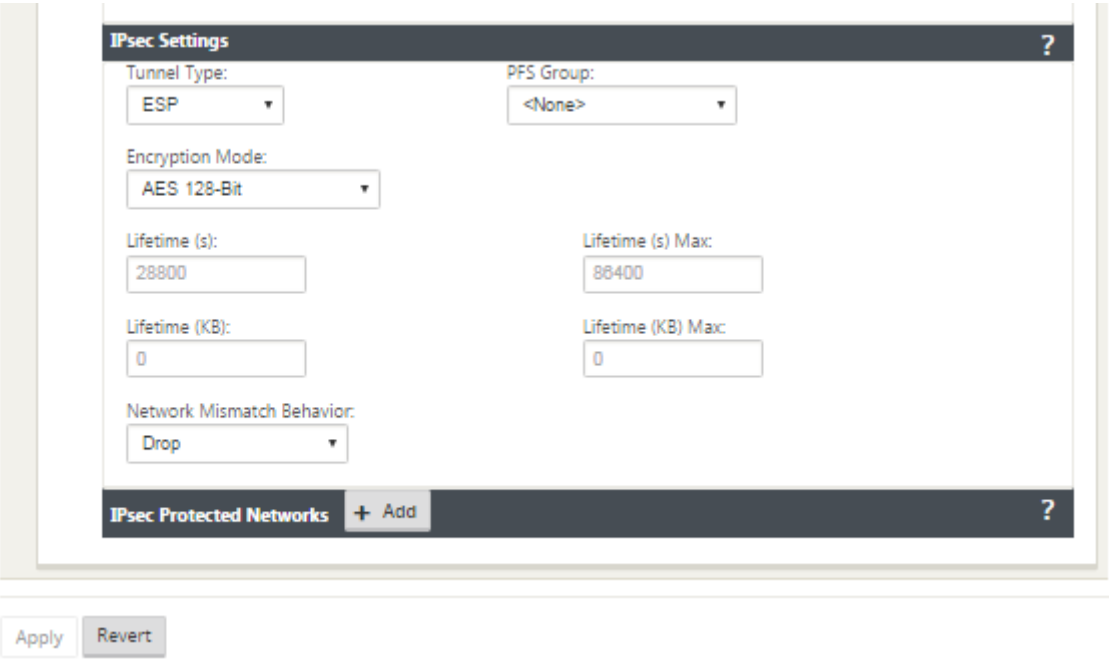


IPsec and IPsec Protected Network Settings:

Field	Description	Value (s)
Tunnel Type	Choose the **Tunnel Type** from the drop-down menu	ESP ESP+Auth ESP+NULL AH
PFS Group	Choose Diffie-Hellman group to use for perfect forward secrecy key generation from the drop-down menu	None Group 1 Group 2 Group 5 Group 14 Group 15 Group 16 Group 19 Group 20 Group 21

Field	Description	Value (s)
Encryption Mode	Choose the **Encryption Mode** for IPsec messages from the drop-down menu	If you chose ESP or ESP+ Auth, select either one of the following, AES 128-Bit, AES 192-Bit, AES 256-Bit, AES 128-Bit GCM 64-Bit, AES 192-Bit GCM 64-Bit, AES 256-Bit GCM 64-Bit, AES 128-Bit GCM 96-Bit, AES 192-Bit GCM 96-Bit, AES 256-Bit GCM 96-Bit, AES 128-Bit GCM 128-Bit, AES 192-Bit GCM 128-Bit, AES 256-Bit GCM 128-Bit. AES 128/192/256-Bit are CBC supported.
Lifetime (s)	Enter the amount of time, in seconds to allow an IPsec security association to exist	28800 seconds (default)
Lifetime Max (s)	Enter the maximum amount of time, in seconds to allow an IPsec security association to exist	86400 seconds (default)
Lifetime (KB)	Enter the amount of data, in kilobytes, for an IPsec security association to exist	Kilobytes
Lifetime (KB) Max	Enter the maximum amount of data, in kilobytes, to allow an IPsec security association to exist	Kilobytes
Network Mismatch Behavior	Choose the action to take if a packet does not match the IPsec Tunnel's Protected Networks from the drop-down menu	Drop, Send Unencrypted, Use Non-IPsec Route
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	IP address

Field	Description	Value (s)
IPsec Protected Networks	**Destination IP/Prefix**: Enter the **Destination IP** and Prefix of the network traffic the IPsec Tunnel will protect	IP address



Monitor IPsec Tunnels

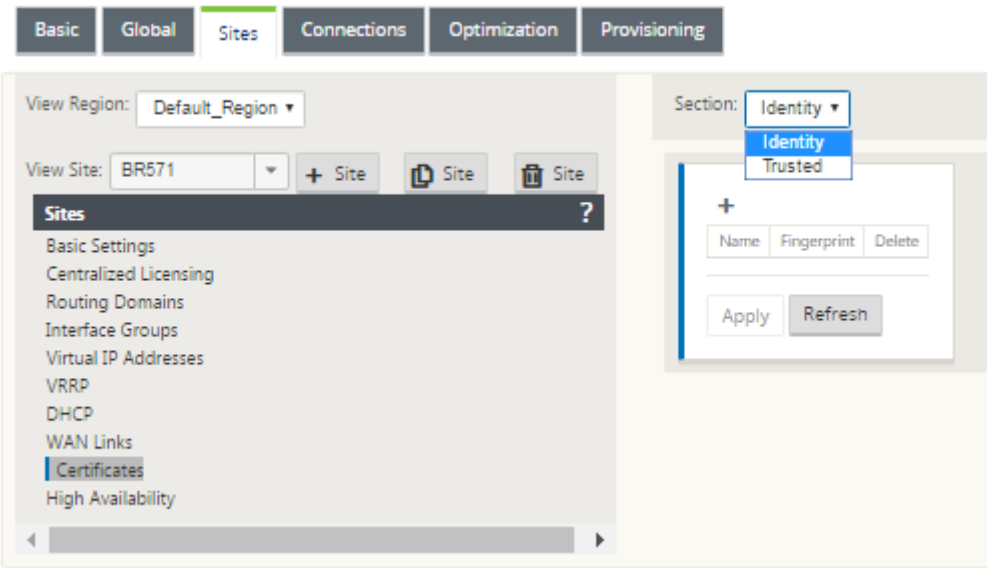
Navigate to **Monitoring>IKE/IPsec** in the SD-WAN appliance GUI to view and monitor IPsec tunnel configuration.

How to add IKE certificates

March 12, 2021

To implement certificates for IKE negotiation:

1. Navigate to **Sites** > **Certificates** and add any necessary certificates.

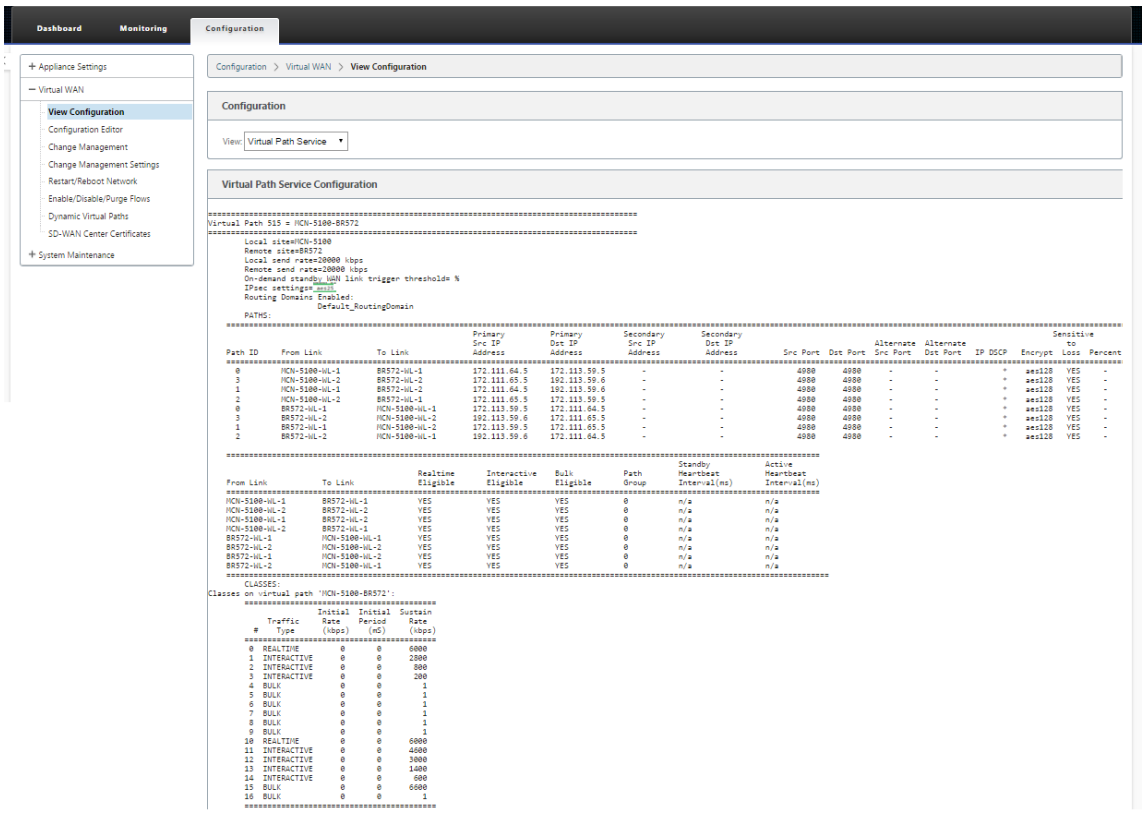


How to view ipsec tunnel configuration

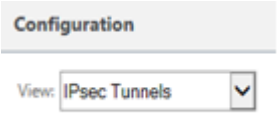
March 12, 2021

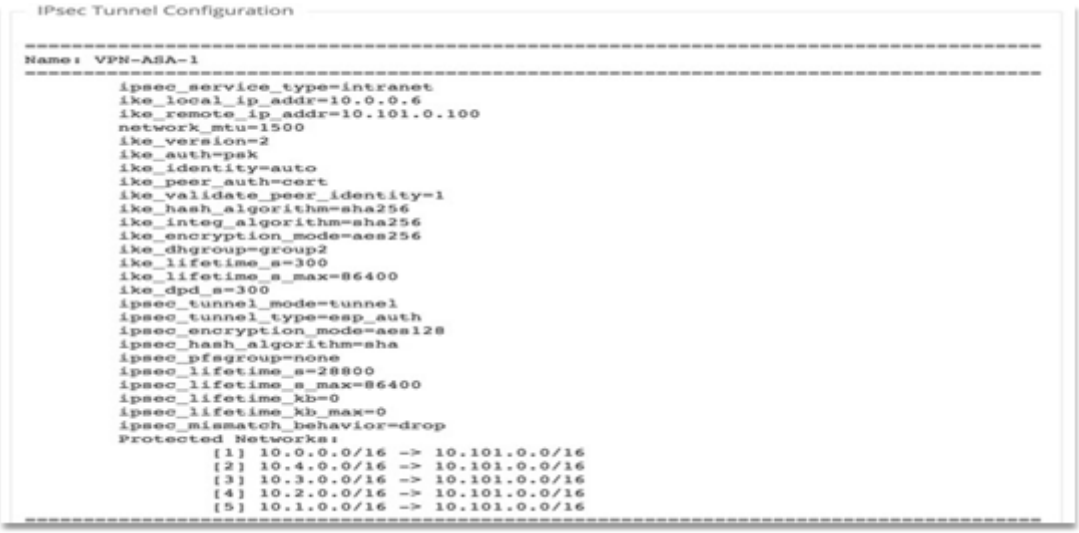
To view ipsec tunnel configuration:

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.

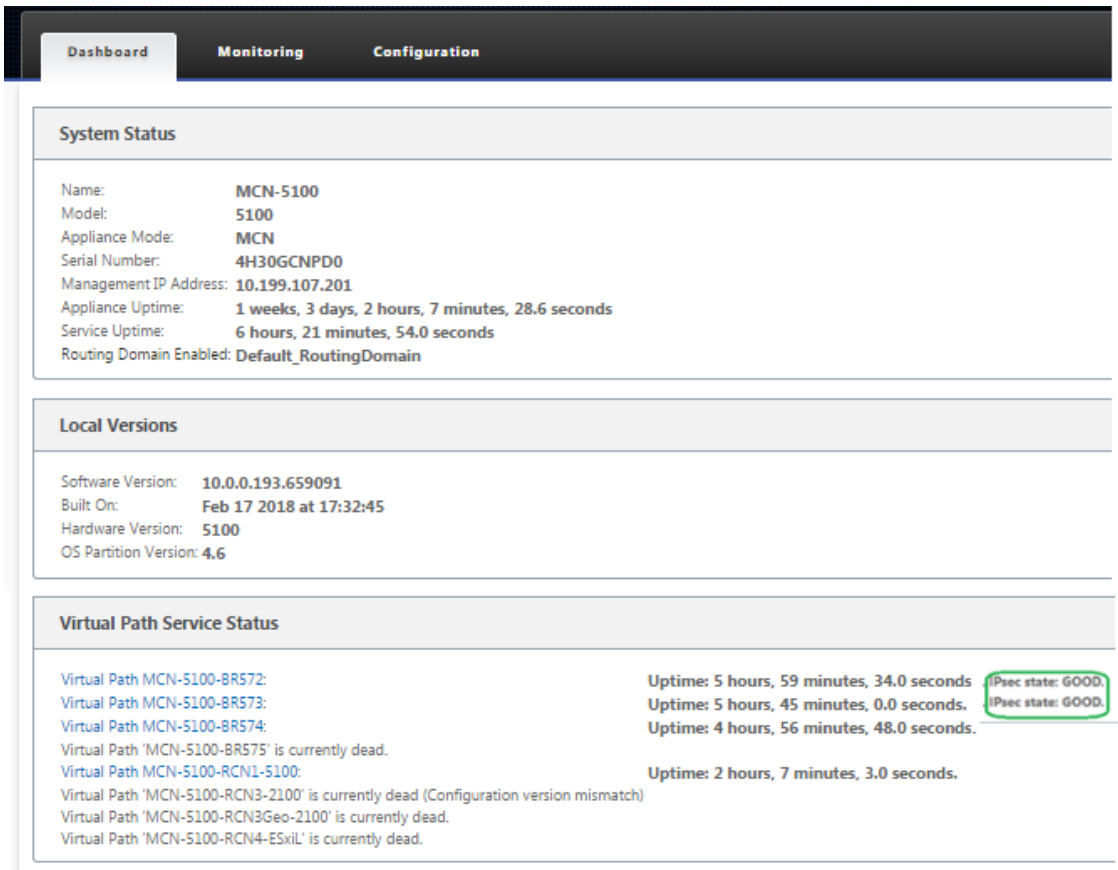


3. Select **IPsec Tunnels** from the drop-down menu to view the IPsec Tunnel configuration.





4. Each virtual path will show its own IPsec tunnel status as shown below.

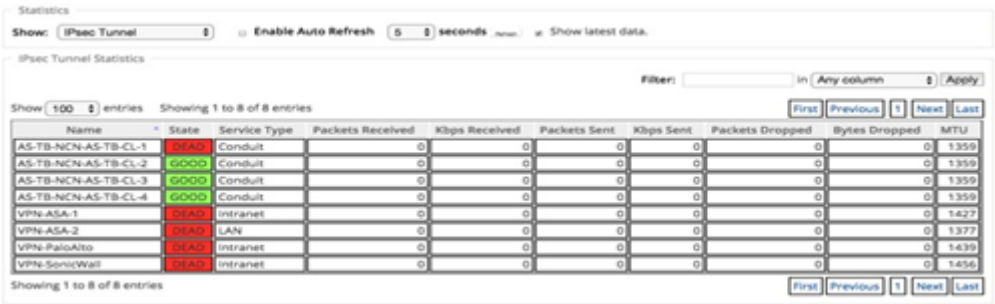


IPSec monitoring and logging

March 12, 2021

To monitor ipsec tunnel statistics:

1. Navigate to **Monitor > Statistics**. Choose **IPsec Tunnel** from the **Show** drop-down menu as shown below:

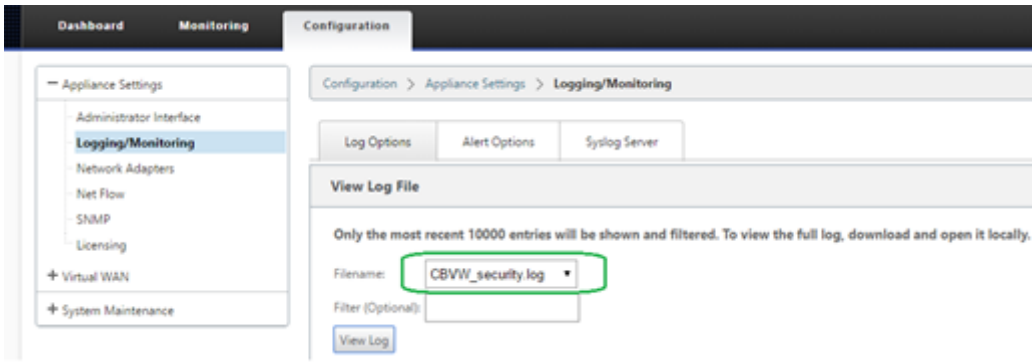


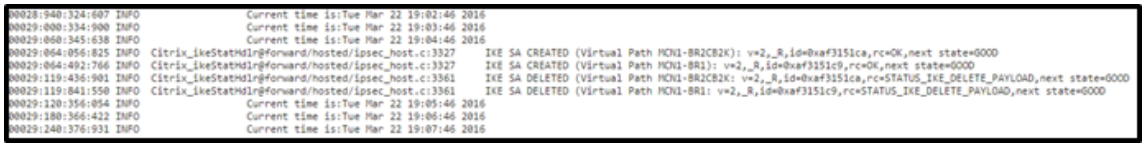
2. Navigate to **Monitor** > **IKE/IPsec**. Observe the configured IPsec tunnels, the IKE and IPsec service associations between two or mode VPN endpoints configured within the SD-WAN network.

How to monitor ipec logs

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

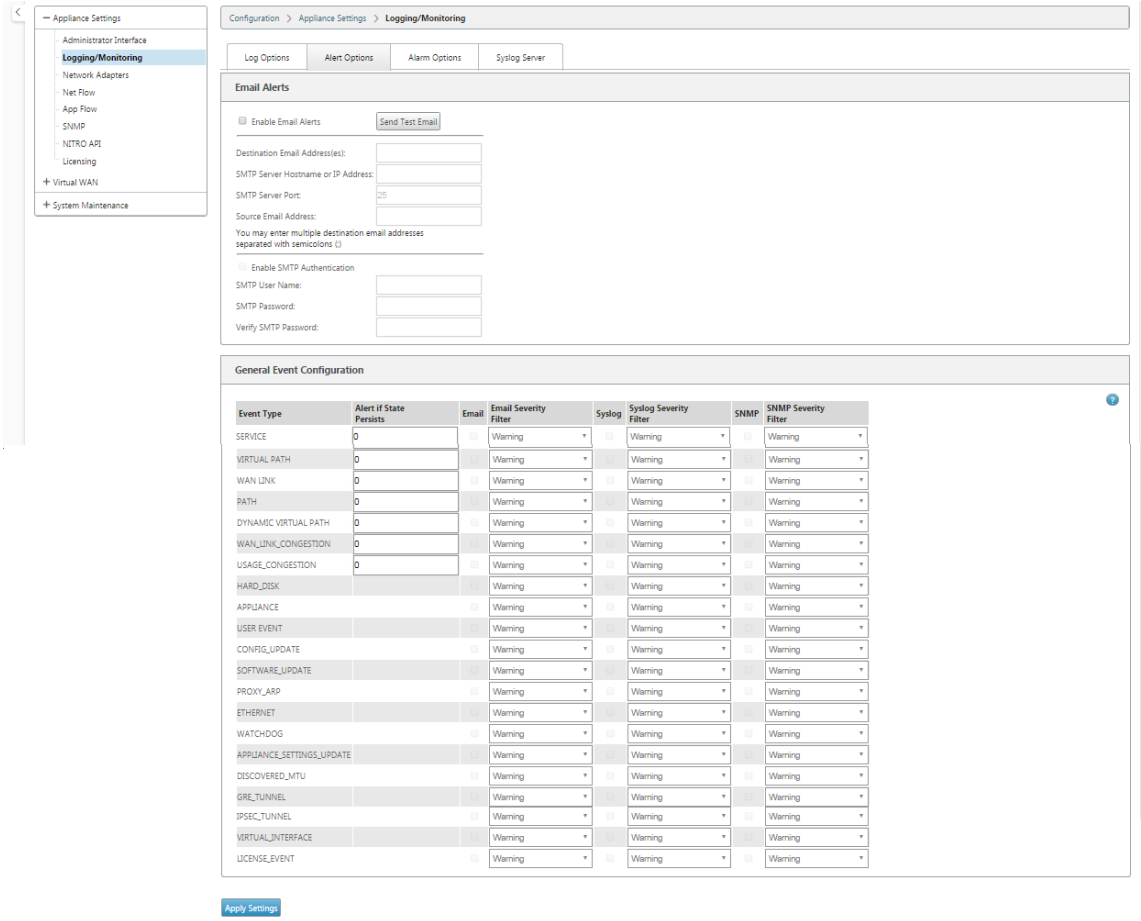




How to view ipsec tunnel alerts

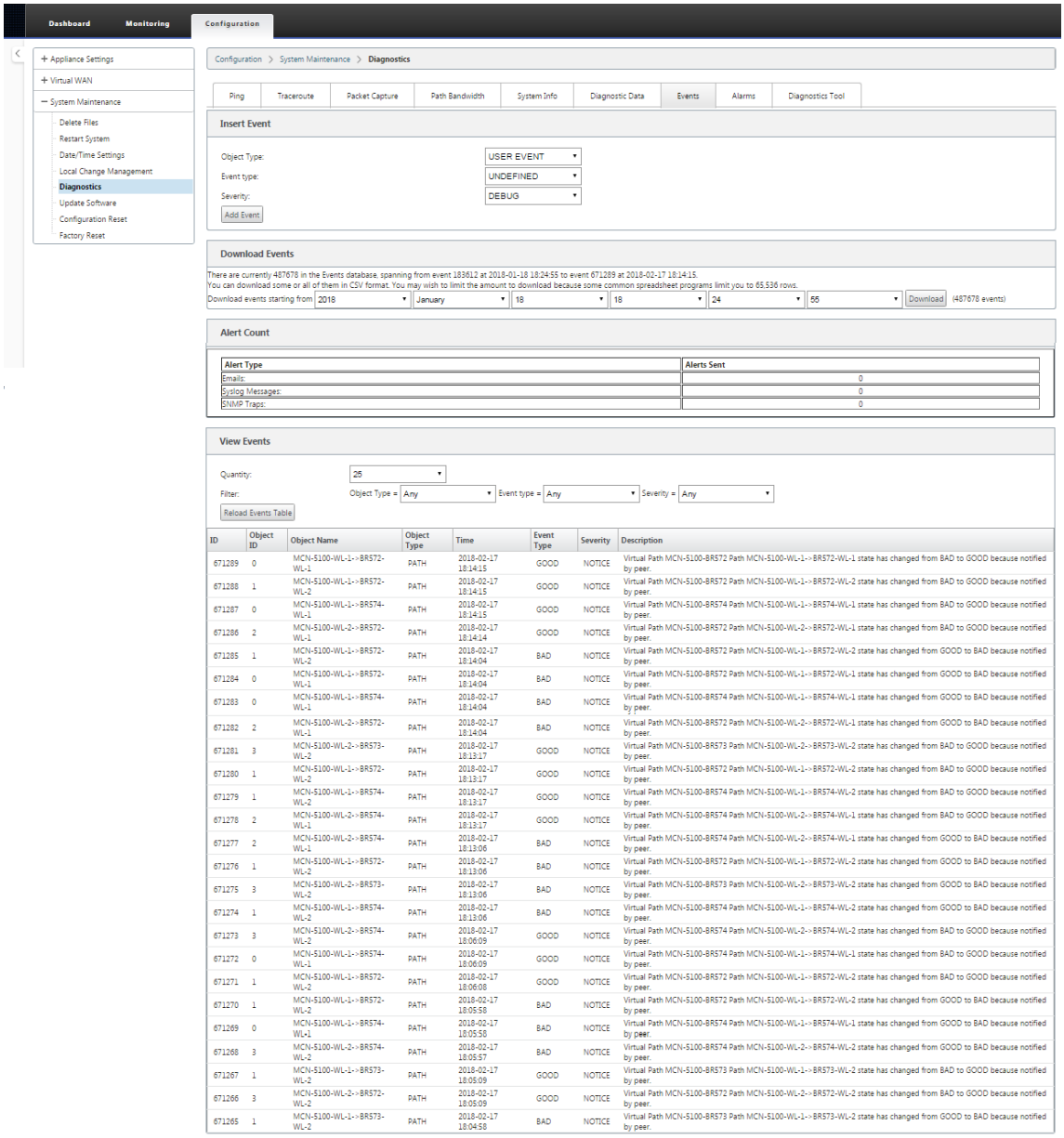
1. Navigate to **Configuration** > **Appliance Settings > Logging/Monitoring** > **Alert Options**.
2. Create Email and Syslog alerts for IPsec tunnel state reporting.

    - Supports IPSEC_TUNNEL as one of the Event types which allows you to configure Email and Syslog Severity Filters.



How to monitor ipsec tunnel events

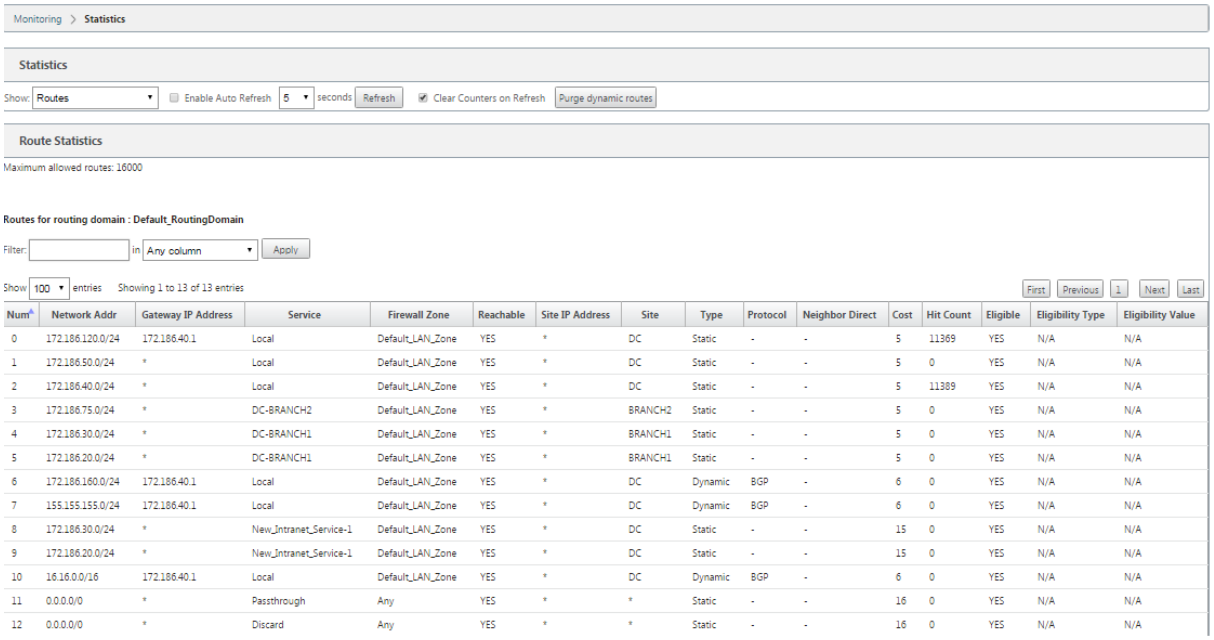
1. Navigate to **Configuration > System Maintenance** > **Diagnostics** > **Events**.
2. Add events based on the **IPSEC_TUNNEL** object type. Create filters for all IPsec related events.



Eligibility for ipsec non-virtual path routes

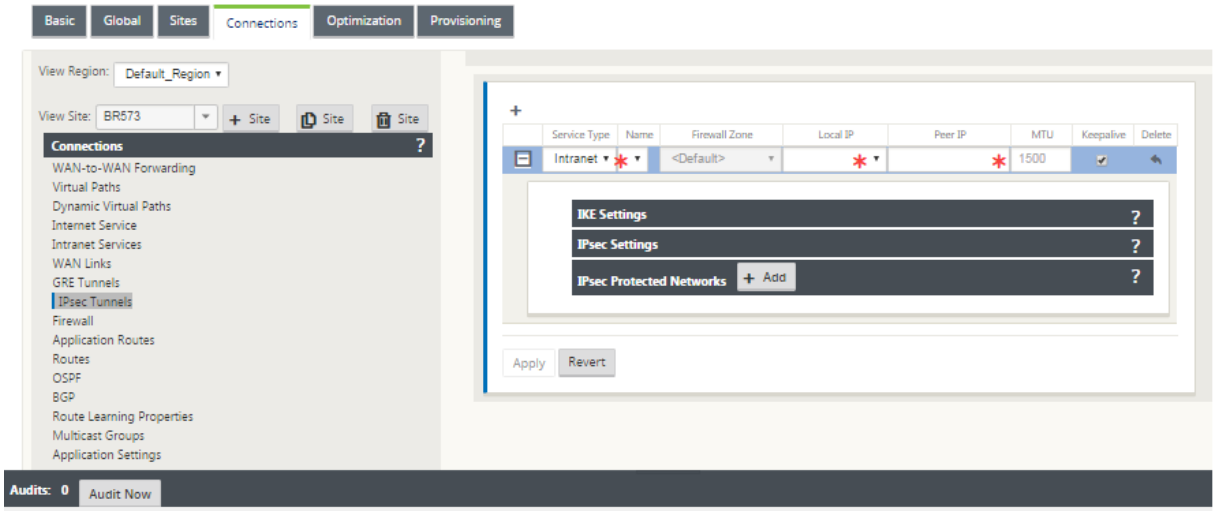
March 12, 2021

In previous releases, ipsec tunnel routes would remain in the route table, even if the tunnel became unavailable.



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.



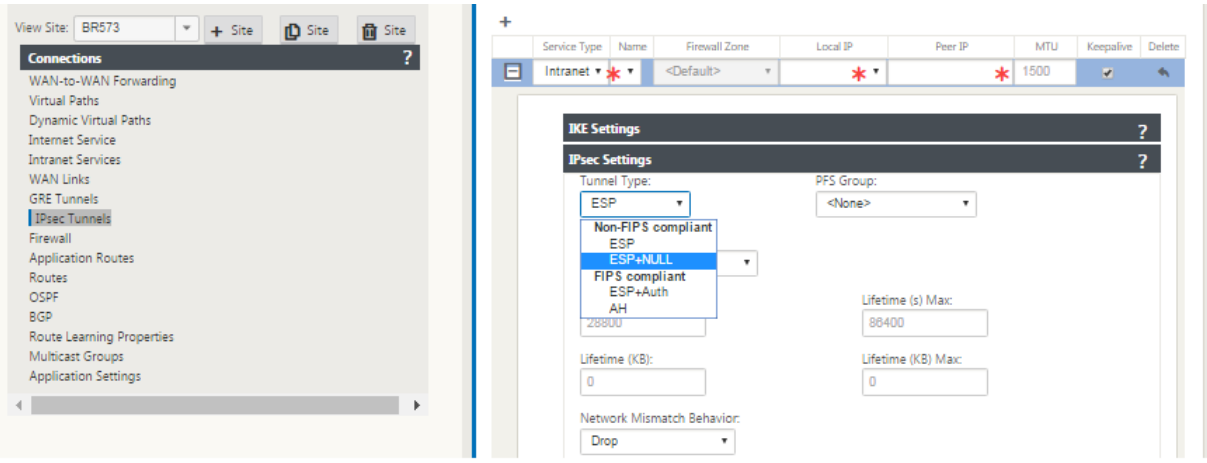
IPsec null encryption

March 12, 2021

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.



FIPS Compliance

March 12, 2021

In Citrix 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
- IKE Hash and (IKEv2) Integrity mode, IPsec auth mode.
- Performs audit errors for FIPS based Lifetime Settings

To enable FIPS compliance by using the Citrix 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 are prompted through audit-errors and warnings to configure IPsec.

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 accepted by FIPS, but SHA256 is highly recommended.
- IPsec lifetime should be configured for no more than 8 hours (28,800 seconds).

The Virtual WAN uses IKE version 2 with pre-shared-keys to negotiate IPsec tunnels through the Virtual Path using the following settings:

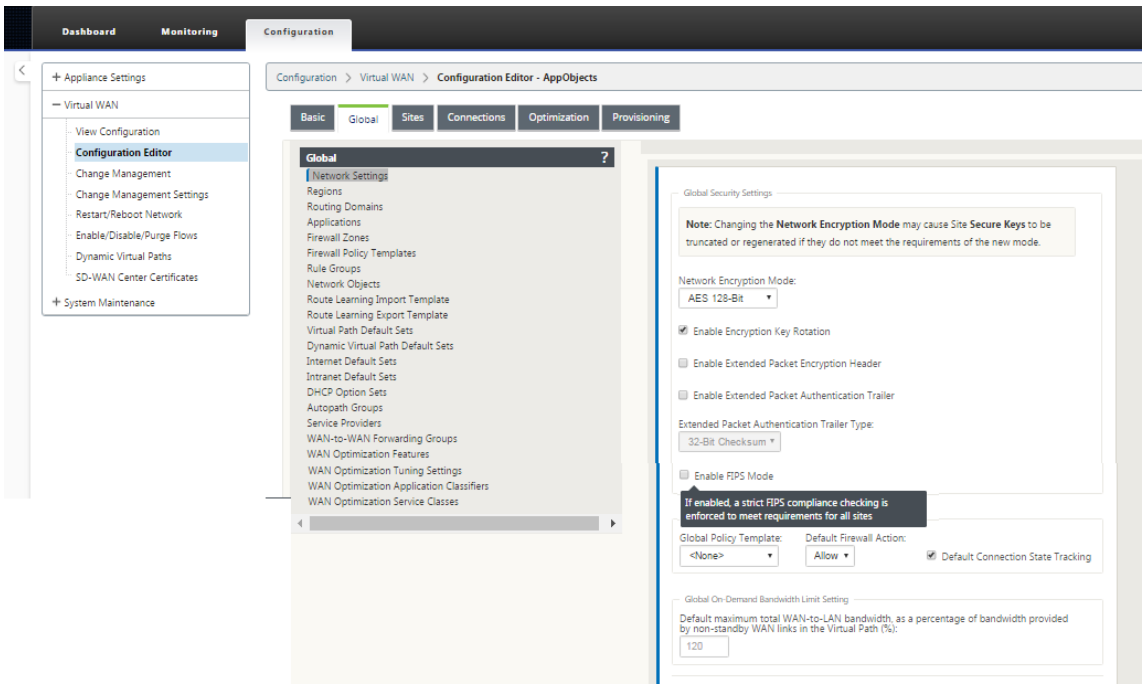
- DH Group 19: ECP256 (256-bit Elliptic Curve) for key negotiation
- 256-bit AES-CBC Encryption
- SHA256 hashing for message authentication
- SHA256 hashing for message integrity
- DH Group 2: MODP-1024 for Perfect Forward Secrecy

To configure IPsec Tunnel for a third party, use the following settings:

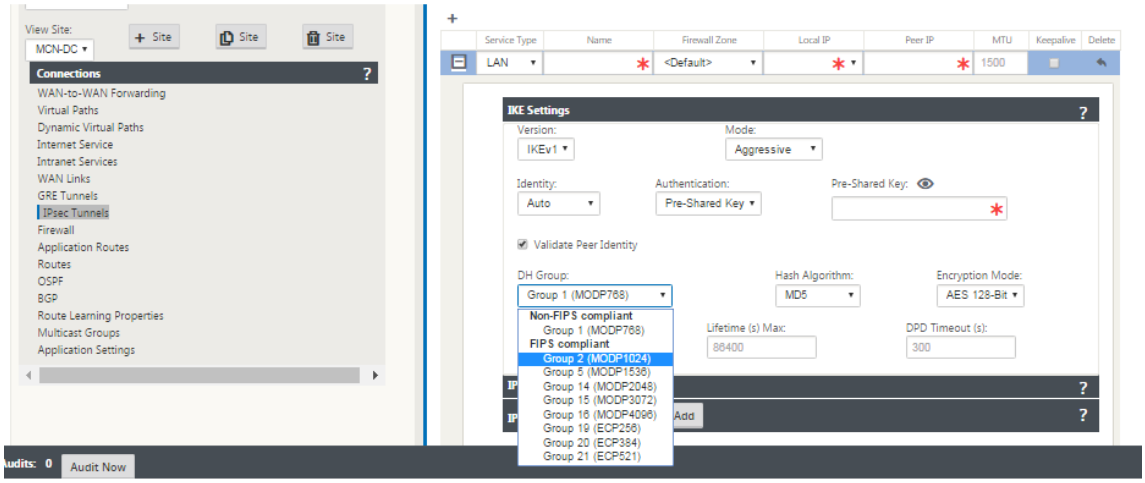
1. Configure FIPS approved DH Group. Groups 2 and 5 are permissible under FIPS, however groups 14 and above are highly recommended.
2. Configure FIPS approved hash function. SHA1 is accepted by FIPS, however SHA256 is highly recommended.
3. If using IKEv2, configure a FIPS approved integrity function. SHA1 is accepted by FIPS, however SHA256 is highly recommended.
4. Configure an IKE lifetime, and max lifetime, of no more than 24 hours (86,400 seconds).
5. Configure IPsec message authentication by changing the IPsec Mode to AH or ESP+Auth and use a FIPS approved hashing function. SHA1 is accepted by FIPS, but SHA256 is highly recommended.
6. Configure an IPsec lifetime, and max lifetime, of no more than eight hours (28,800 seconds).

To configure IPSec tunnels:

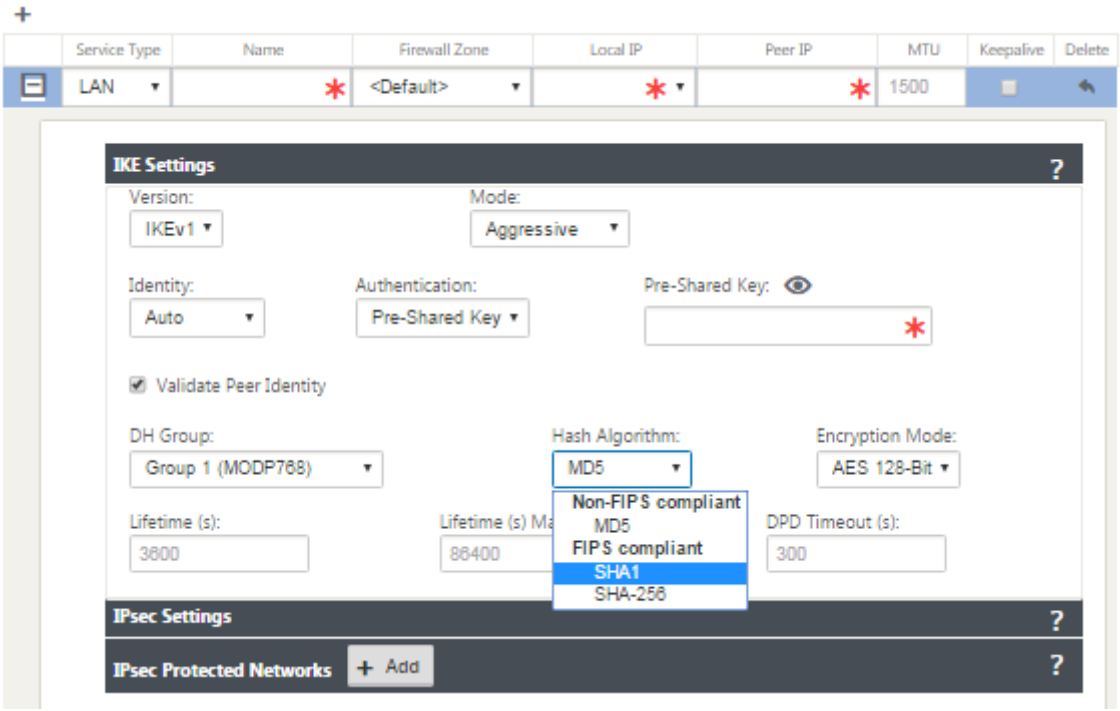
1. On the MCN appliance, go to **Configuration** > **Virtual WAN** > **Configuration Editor**. Open an existing configuration package. Go to **Connections** > **IPSec Tunnels**.



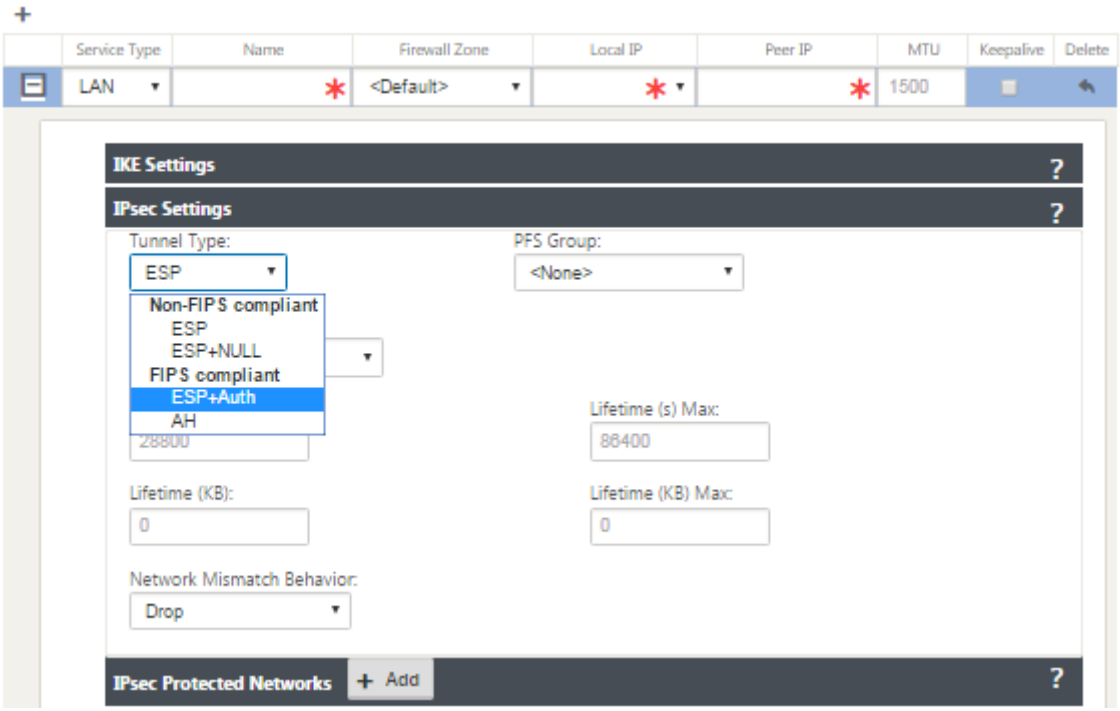
2. Go to **Connections** > **IPsec Tunnels**. With **LAN** or **Intranet Tunnel** selected, the screen distinguishes the FIPS-compliant groups in the IKE settings from those that are not compliant, so that you can easily configure FIPS compliance.



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 are also enabled, and incorrect lifetime value is entered.

Citrix SD-WAN secure web gateway

March 12, 2021

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 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 many 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 SD-WAN appliance to the Zscaler Cloud Security Platform. You can then use a central Zscaler console to create granular security policies for 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 more 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 addresses 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 Citrix SD-WAN appliance, configure FIPS mode.

Forcepoint:

By using Citrix 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.

Zscaler Integration by using GRE tunnels and IPsec tunnels

June 9, 2021

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.

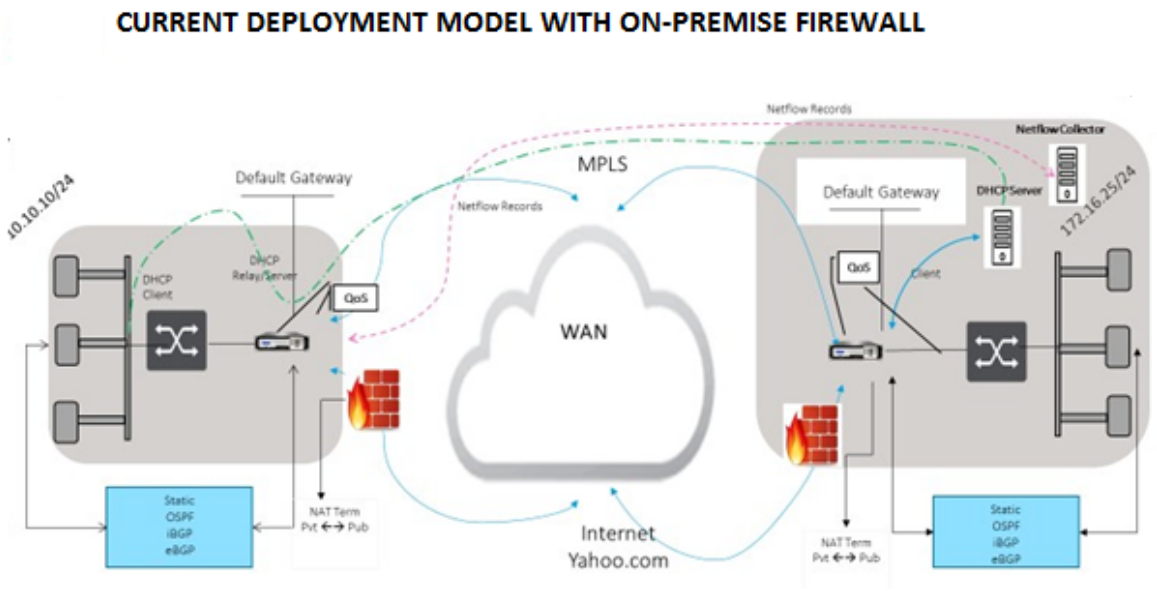
Citrix SD-WAN appliances can connect to a Zscaler cloud network through GRE tunnels at the customer's site. A Zscaler deployment using SD-WAN appliances supports the following functionality:

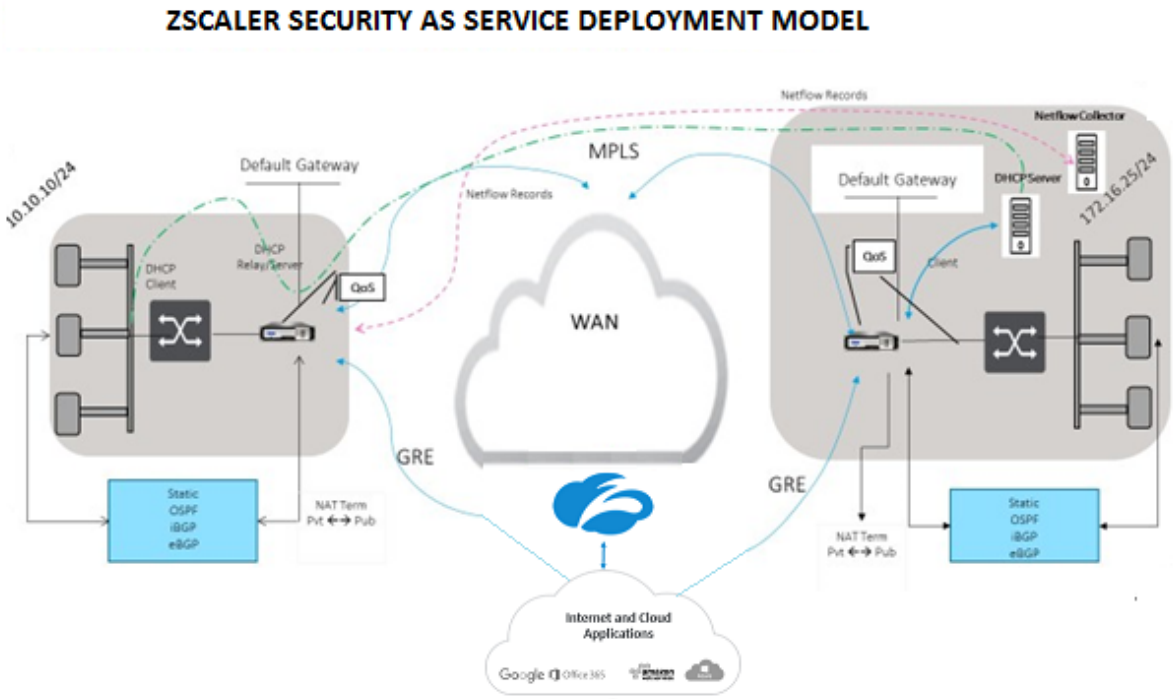
- Forwarding all GRE traffic to Zscaler, thereby enabling direct Internet breakout.
- Direct internet access (DIA) using Zscaler on a per customer site basis.
  - On some sites, you might want to provide DIA with on-premises security equipment and not use Zscaler.
  - On some sites, you might choose 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.

Topology





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

Configuring an Internet Service

To configure an internet service:

1. Navigate to **Connections**- **Internet Services**. Configure internet service.
2. Select **+ Service** and enable the settings (Basic settings, WAN Links, and Rules) as required.
3. Select **Apply**.

For more information about enabling Internet service for a site, see Direct Internet Breakout at Branch with Integrated Firewall.

You can configure the following settings on an Internet Service:

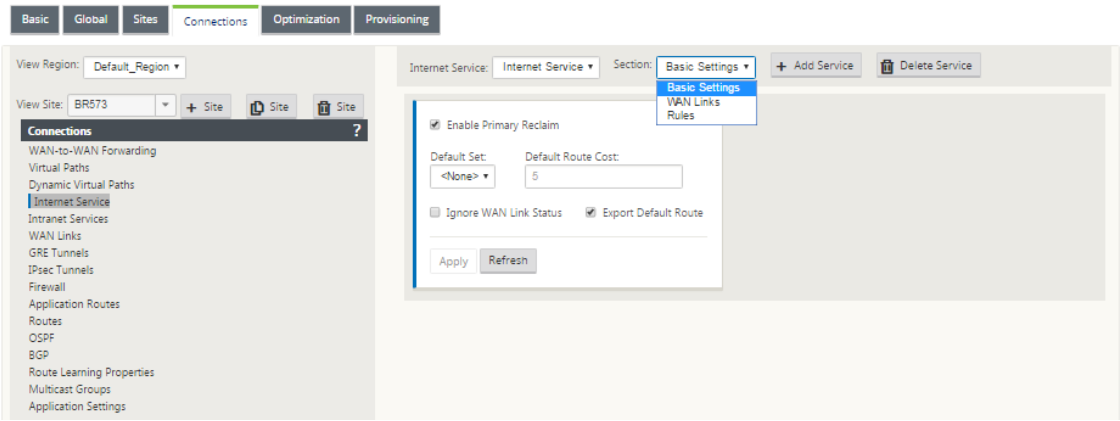
- Basic settings
- WAN links
- Rules

Basic settings

A Firewall zone setting is not configurable for an Internet Service. If the Internet Service is trusted, it is assigned to **Internet_Zone**. If the Internet Service is untrusted, it is assigned to **Untrusted_Internet_Zone**.

The basic settings that are configurable are described below:

- **Enable Primary Reclaim**: If enabled, the (use = primary) usage associated with this service on a WAN Link forcefully reclaims status as the active service on that WAN link.
- **Default Set**: Name of the Internet default set that populates rules for the Internet service on the Site.
- **Default Route Cost**: Route cost associated with the default (0.0.0.0/0) internet route.
- **Ignore WAN Link Status**: If enabled, packets destined for this service still choose this service even if all WAN links for this service are unavailable.
- **Export Default Route**: If enabled, the default route for the Internet Service, 0.0.0.0/0, is exported to other Sites if WAN-to-WAN forwarding is enabled.



WAN links

The WAN link settings that are configurable are described below:

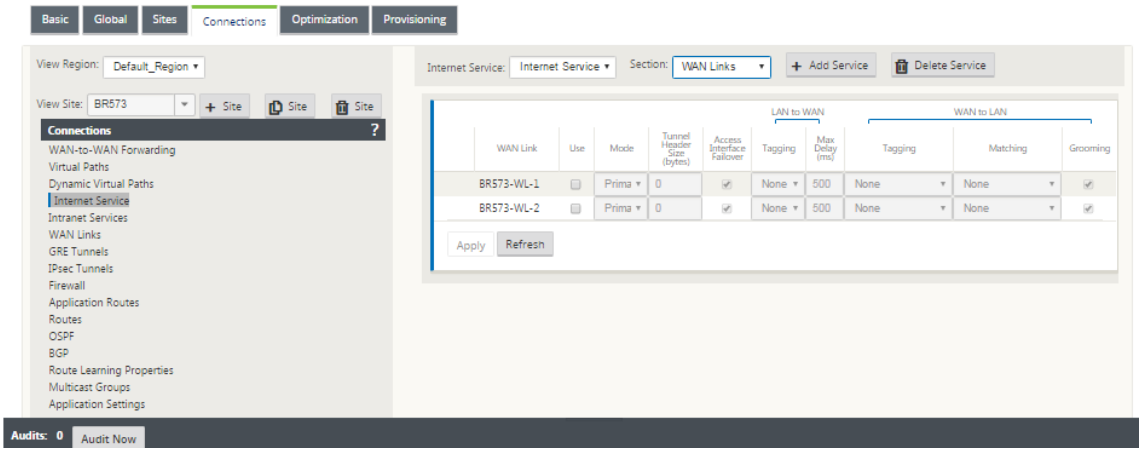
- **Use**: Allow the Service to use this WAN Link. When Use is disabled, all the other options are unavailable.
- **Mode**: The mode of Service –Primary, Secondary, or Balance, for traffic redundancy or load balancing.
- **Tunnel Header Size (bytes)**: The size of the tunnel header, in bytes, if applicable.
- **Access Interface Failover**: If enabled, the Internet or Intranet packets with mismatched VLANs can still use the service.

LAN to WAN

- **Tagging**: The DSCP tag to apply to LAN to WAN packets on the Service.
- **Max Delay (ms)**: The maximum time, in milliseconds, to buffer packets when the WAN Links bandwidth is exceeded.

WAN to LAN

- **Tagging**: The DSCP tag to apply to WAN to LAN packets on the service.
- **Matching**: Internet WAN to LAN packets matching this tag are assigned to the service.
- **Grooming**: If enabled, packets are randomly dropped to prevent WAN to LAN traffic from exceeding the provisioned bandwidth of the service.



Rules

Internet traffic is identified based on the rules defined. A rule definition is used to match a specific traffic flow. Once matched, you must define the action to apply for the traffic flow.

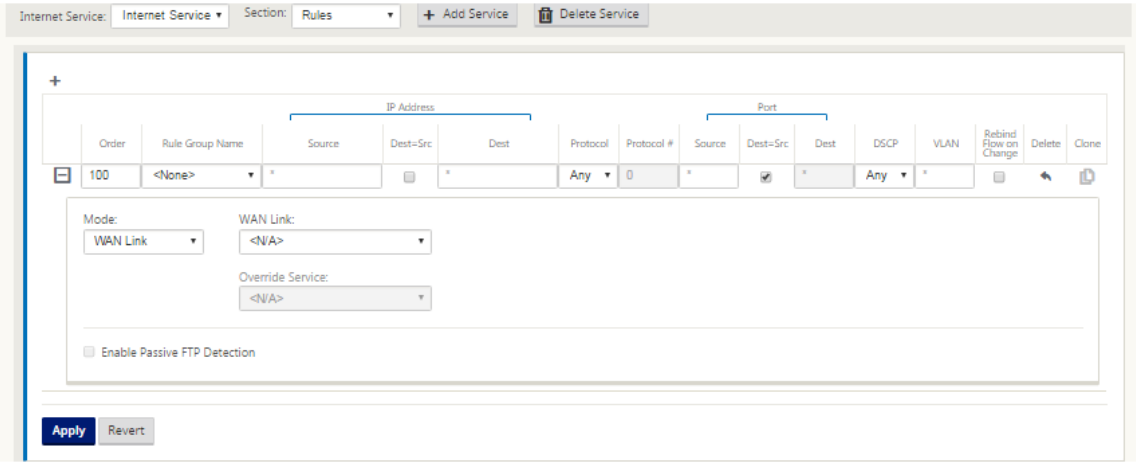
The list of available rules is described below:

- **Order**: The sequence in which rules are applied and automatically redistributed.
- **Rule group Name**: Name given to a rule that allows rule statistics to be summed in groups when they are displayed. All the statistics for rules with the same rule group name can be viewed together.
- **Source**: The source IP address and subnet mask that matches with the rule.
- **Dest-Src**: If enabled, the source IP address is also used as the destination IP address.
- **Dest**: The destination IP address and subnet mask that matches with the rule.
- **Protocol**: The protocol name that matches with the filter.
- **Protocol #**: The protocol number that matches with the filter.
- **DSCP**: The DSCP tag in the IP header that matches with the rule.

The list of available actions is described below:

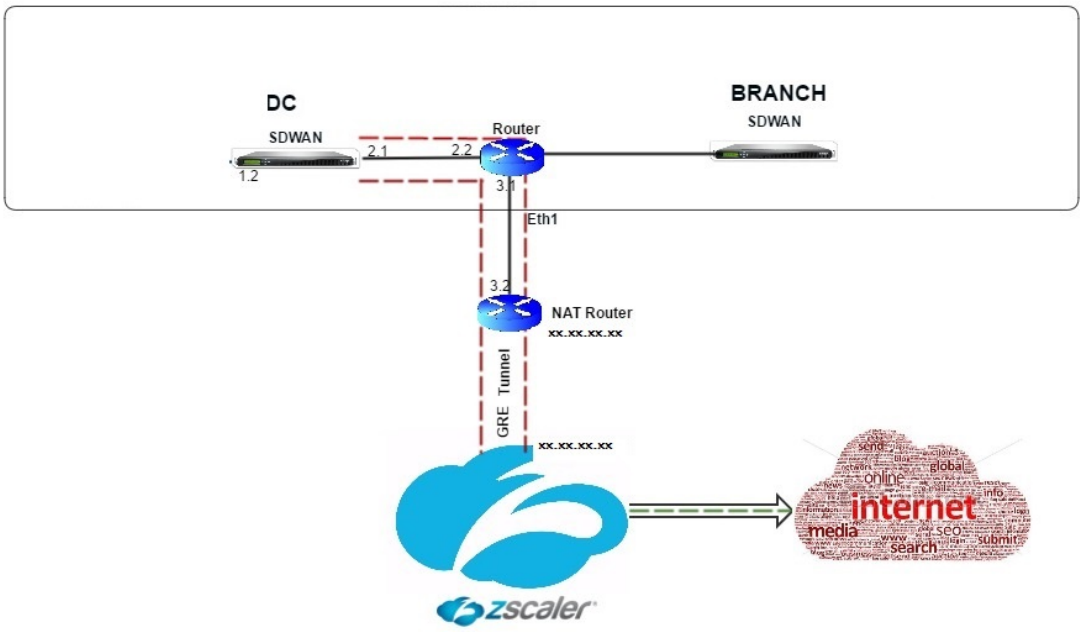
- **WAN Link**: The WAN link to be used by flows matching the rule when Internet load balancing is enabled.
- **Override Service**: The destination service for flows matching the rule.

- **Discard**: Drop the traffic.
- **Passthrough**: Map the flow to pass-through and allow the traffic to flow through the appliance unchanged.



Configure GRE Tunnel

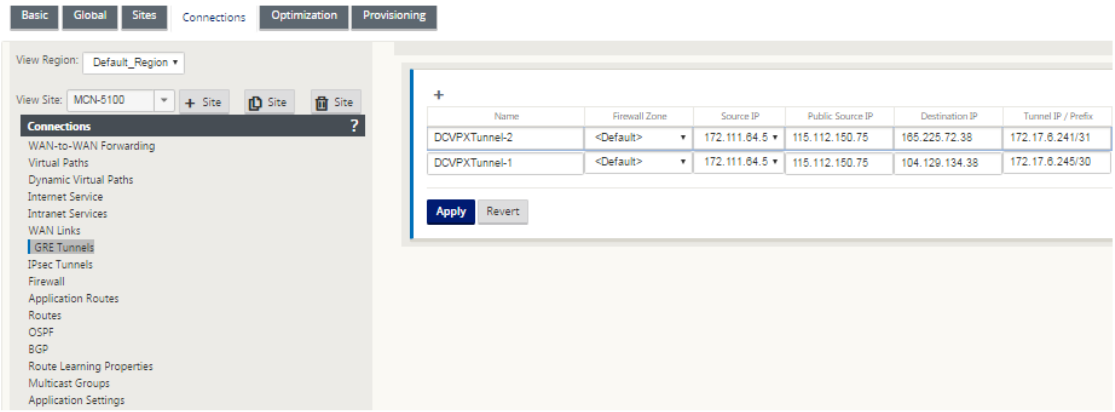
1. Source IP address is the Tunnel Source IP address. If the Tunnel Source IP address is NATted, the Public Source IP address is the public Tunnel Source IP address, even if it is NATted on a different intermediate device.
2. Destination IP address is the ZEN IP address that Zscaler provides.
3. The Source IP address and the Destination IP address are the router GRE headers when the original payload is encapsulated.
4. 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 trafic 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 for GRE tunnels

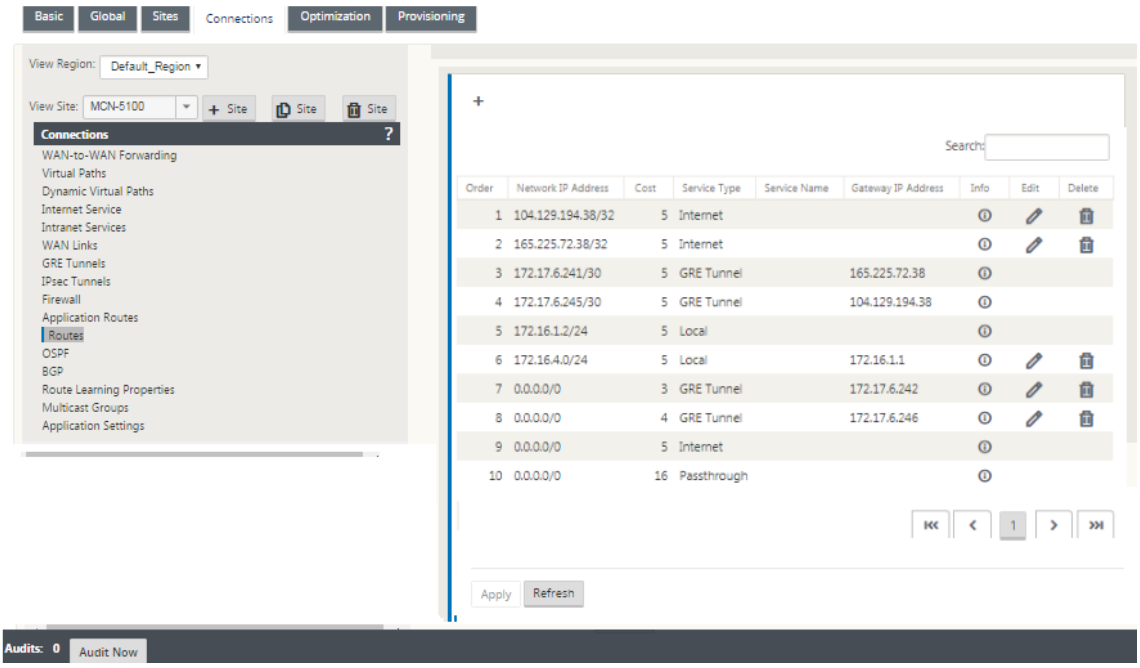
Configure routes to forward internet prefix services to the Zscaler GRE Tunnels.

- 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 matches 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:

1. Navigate to **Connections** > **Site** > **Routes**, and follow the procedures described in Configuring Routes for instructions about creating routes.



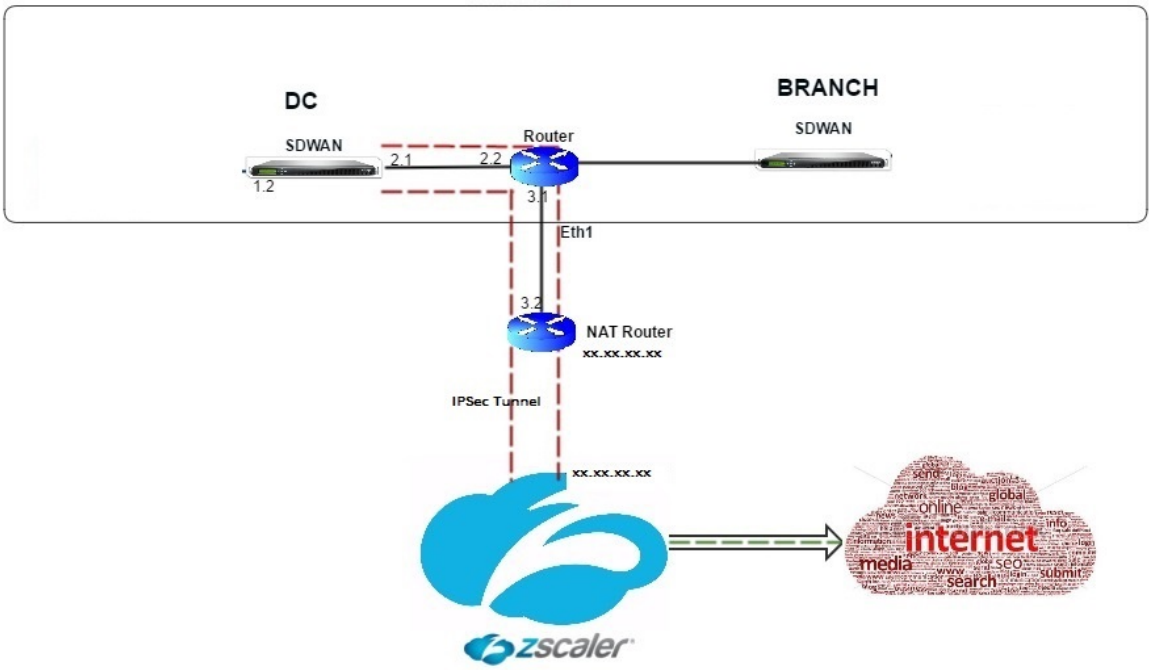
> **Note**
>
> If you do not have specific routes for the Zscaler IP address, configure the route prefix 0.0.0.0/0 to match the ZEN IP address and route it through a GRE tunnel encapsulation loop. This configuration uses the tunnels in an active-backup mode. With the values shown in the above figure, 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 Citrix SD-WAN GUI interface (in the case when SD-WAN appliance Tunnel Source is NATted by an intermediate device). The Citrix SD-WAN GUI includes a field called Public Source IP, which provides the NAT address

> of the GRE Source address when the Citrix SD-WAN appliance's Tunnel Source is NATted by an intermediate device.

Limitations

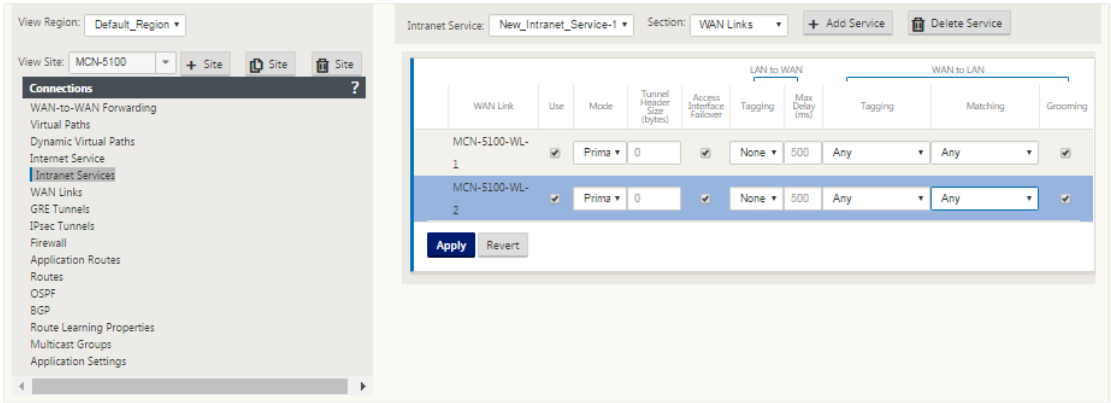
- Multiple VRF deployments are not supported.
- Primary backup GRE tunnels are supported for a high-availability design mode only.

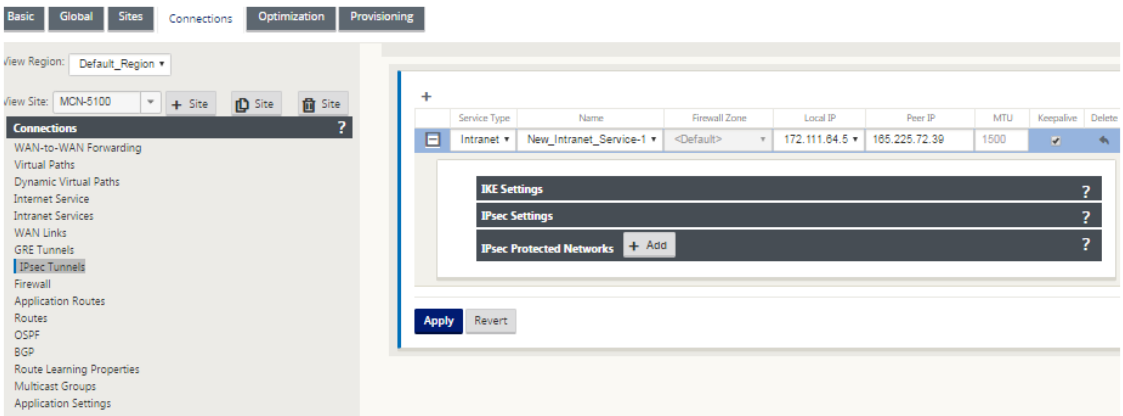
Configure IPsec Tunnels



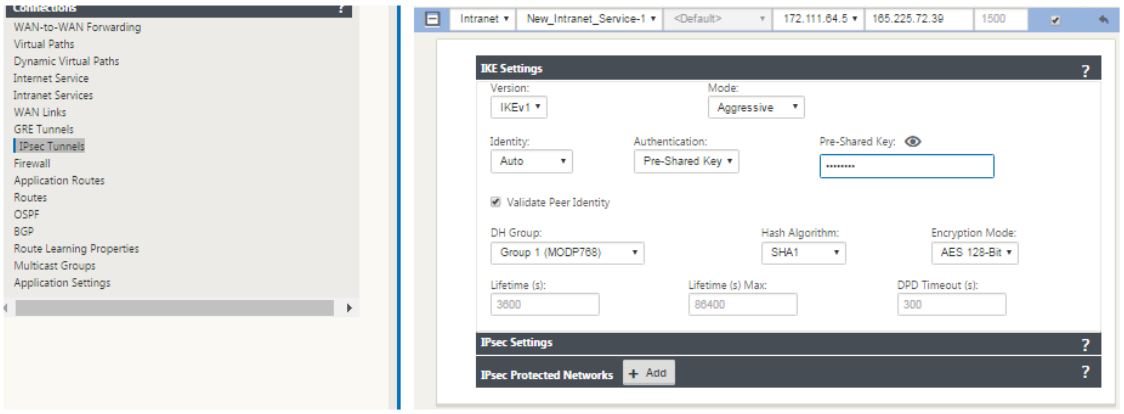
To configure IPsec Tunnels for intranet or LAN services in the Citrix SD-WAN appliance GUI:

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.



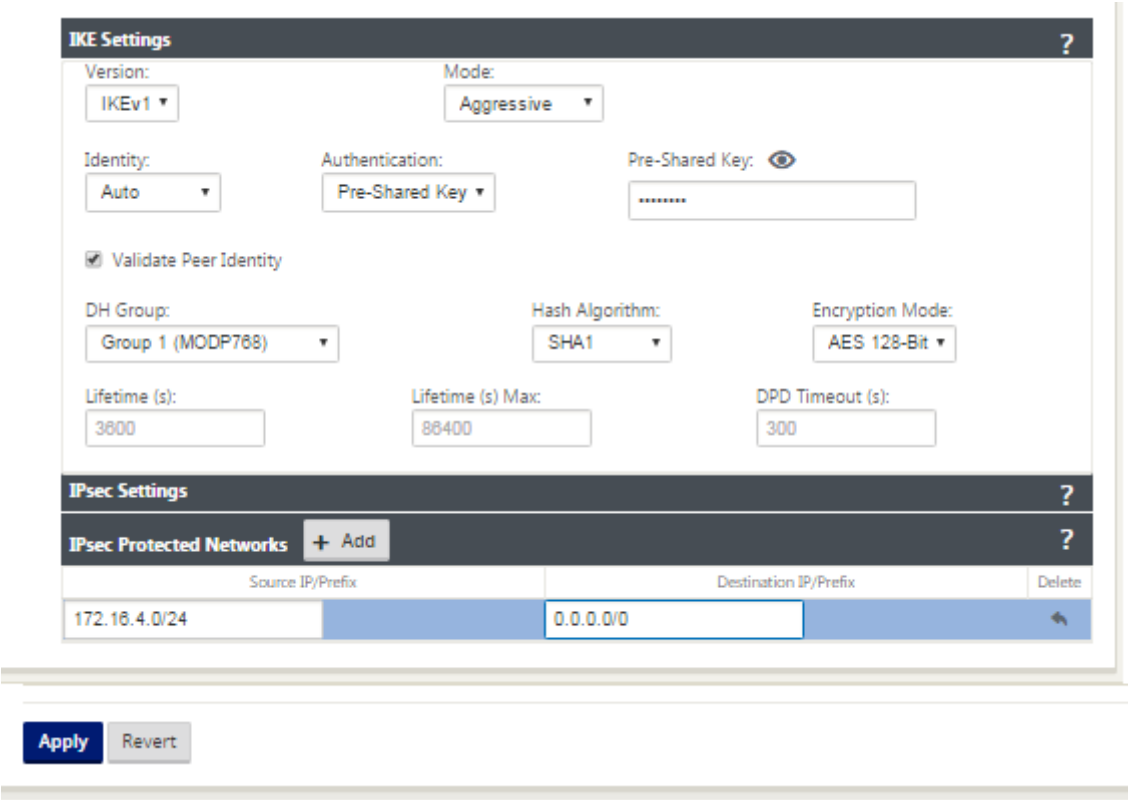


4. Select **IKEv1** for **IKE Settings**. Zscaler supports only IKEv1.



5. Under IPsec Settings, select **ESP-NULL** for **Tunnel type**, to redirect traffic to Zscaler through the IPSec tunnel. The IPSec tunnel does not encrypt the traffic.

6. Because internet traffic is redirected, the destination IP/Prefix can be any IP address.

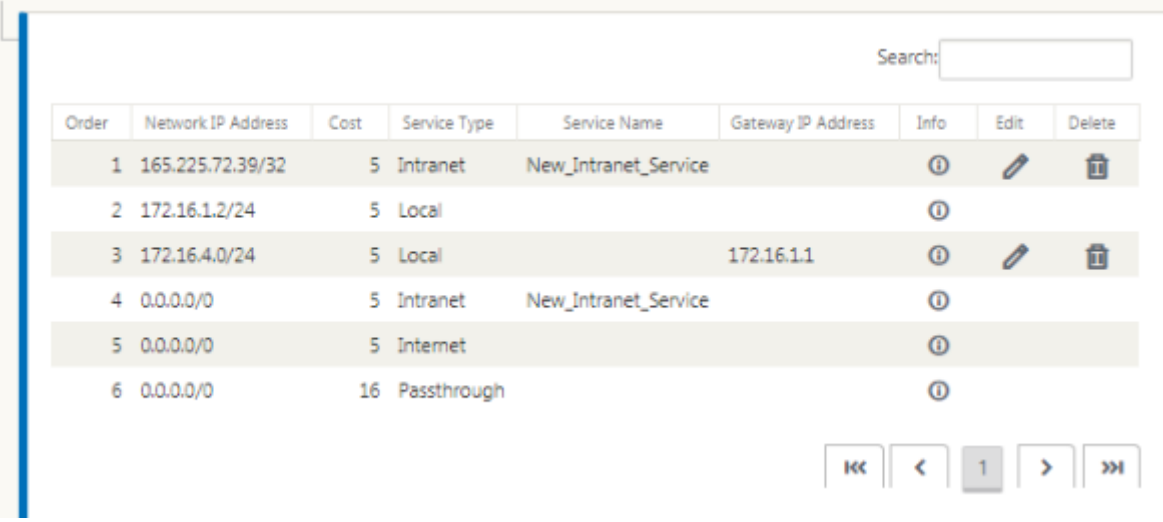


For more information about configuring IPSec Tunnels by using the Citrix SD-WAN web interface, see; the IPsec Tunnels topic.

Configure routes for IPsec tunnels

To configure IPsec routes:

1. Navigate to **Connections** > **DC** > **Routes** and follow the procedures described in Configuring Routes for instructions about creating routes.



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.

Firewall Traffic Redirection Support by Using Forcepoint in Citrix SD-WAN

March 12, 2021

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[1]s IP range - partnership/development
- Firewall redirect (transparent proxy by Destination NAT)

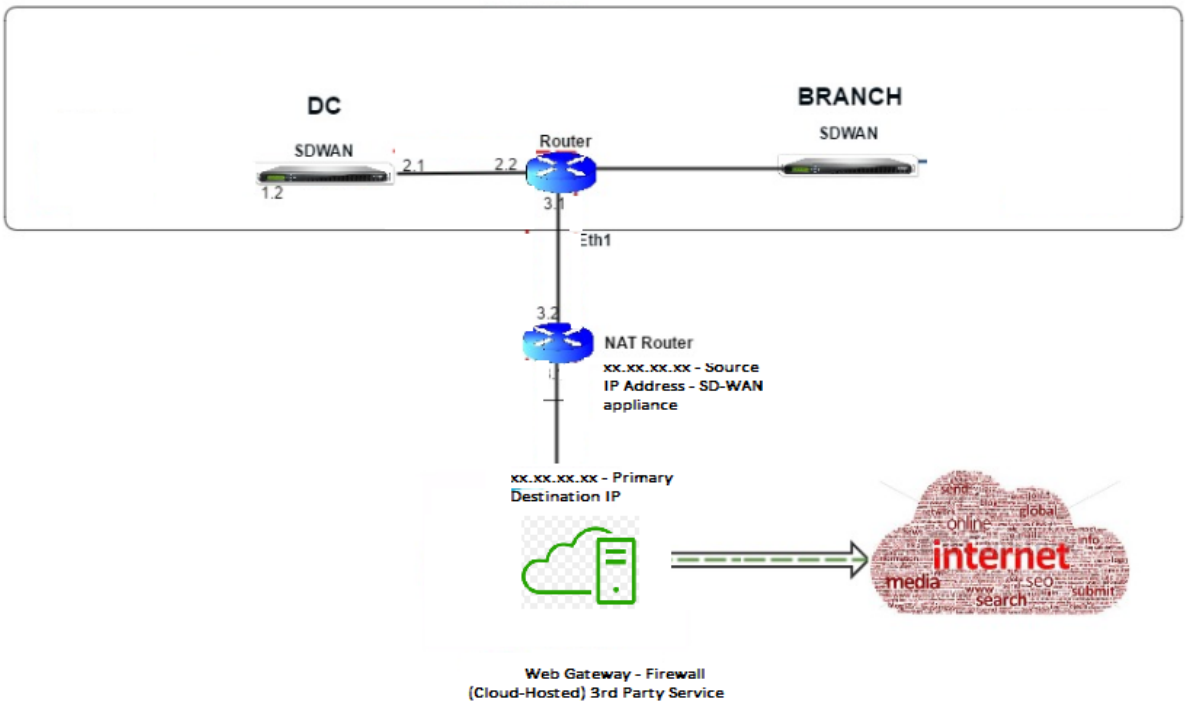
The Destination NAT policy enables enterprises to route internet traffic through cloud-hosted security service using ForcePoint.

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. Log in 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 an 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 Citrix SD-WAN, see the following topic, Configure NAT



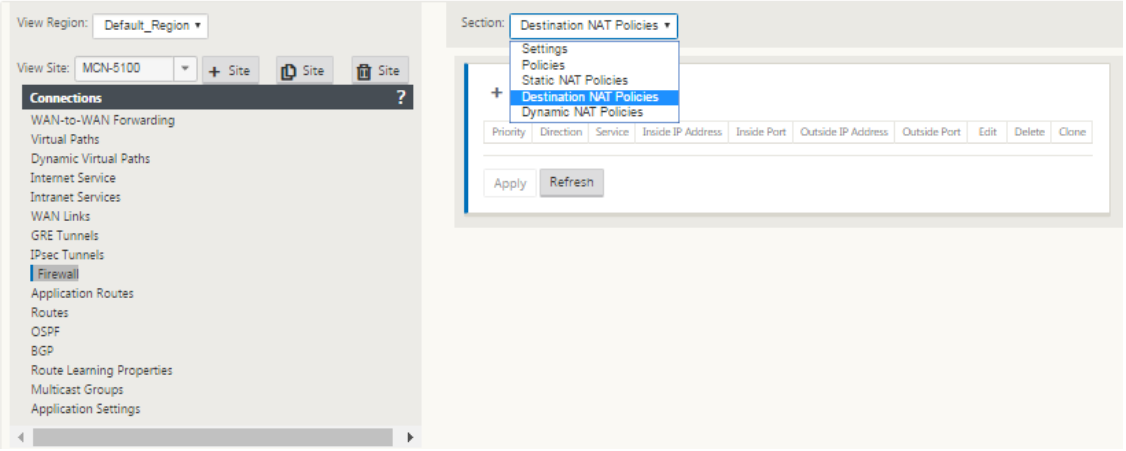
Configuring Destination NAT (DNAT)

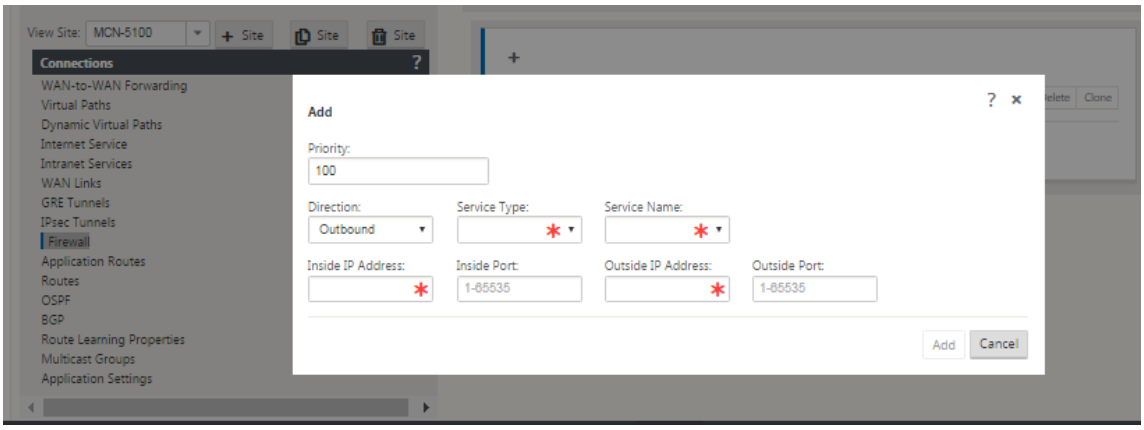
Use the Citrix SD-WAN GUI to configure Destination NAT (DNAT). In the configuration, add one or more DNAT policies that redirect traffic matching a specific destination IP address and port.

To configure Destination NAT:

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 DNAT rules while building the network configuration.

1. At the DC (MCN), configure Internet Service. Go to **Connections** -> **Firewall**.
2. Click **+ Add** to add a DNAT policy.
3. 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





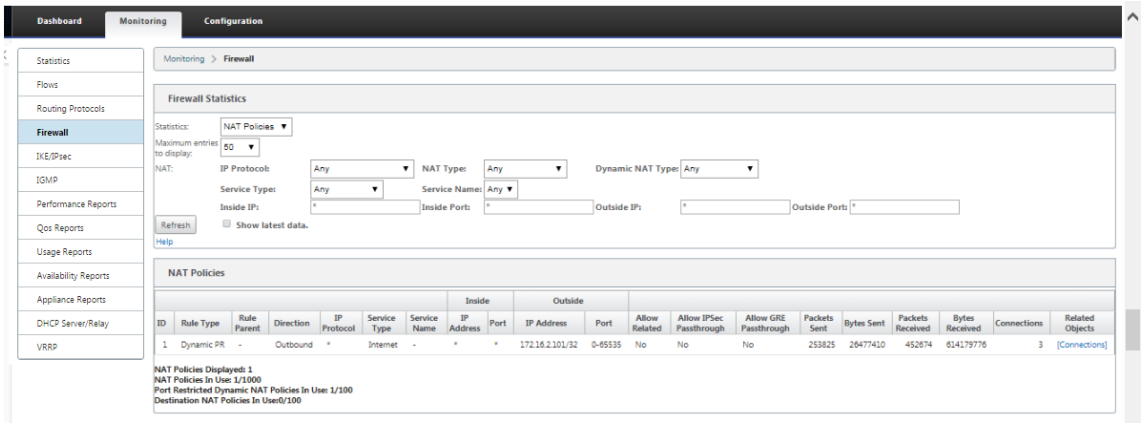
4. Provision Destination NAT rules for Firewall traffic redirect, similar to static NAT.
5. Enter the matching criteria and the Destination IP/port to be NATed.
6. Perform connection matching of the DNAT rule with statistics.
7. Remove or Update DNAT rules during configuration update.

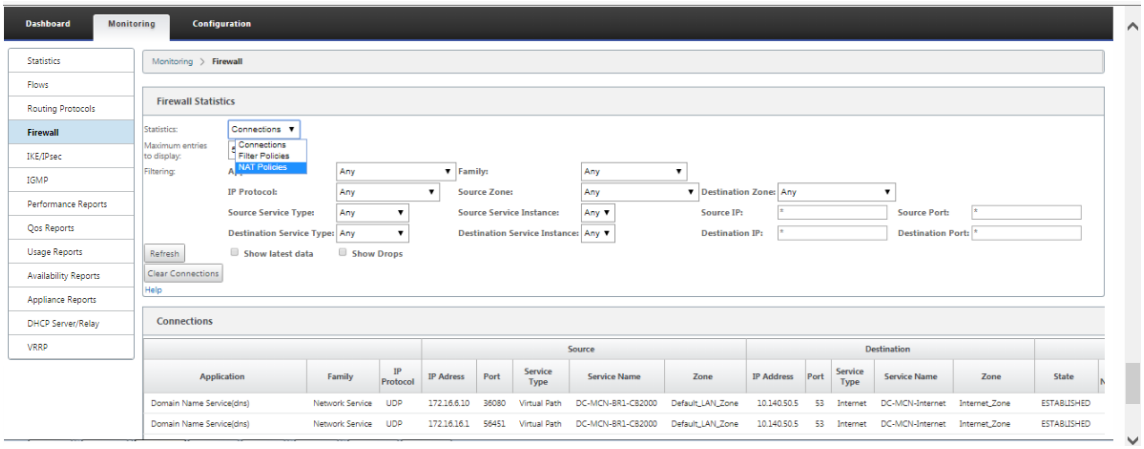
Monitoring a Destination NAT Policy (Firewall)

You can also use the Citrix SD-WAN GUI to monitor the current DNAT policy configuration.

To monitor the current Destination NAT policy configuration:

1. In the Citrix SD-WAN GUI, navigate to **Monitoring** > **Firewall** > **NAT Policies**.
2. Select the tab that includes the statistics you want to monitor.





Palo Alto integration using IPsec tunnels

March 12, 2021

Palo Alto networks deliver cloud-based security infrastructure for protecting remote networks. It provides security by allowing organizations to set up regional, cloud-based firewalls that protect the SD-WAN fabric.

Prisma Access service for remote networks allows you to onboard remote network locations and deliver security for users. It removes the complexity in configuring and managing devices at every remote location. The service provides an efficient way to easily add new remote network locations and minimize the operational challenges with ensuring that users at these locations are always connected and secure, and it allows you to manage policy centrally from Panorama for consistent and streamlined security for your remote network locations.

To connect your remote network locations to the Prisma Access service, you can use the Palo Alto Networks next-generation firewall or a third-party, IPSec-compliant device including SD-WAN, which can establish an IPsec tunnel to the service.

- Plan the Prisma Access Service for Remote Networks
- Configure the Prisma Access Service for Remote Networks
- Onboard Remote Networks with Configuration Import

The Citrix SD-WAN solution already provided the ability to break out Internet traffic from the branch. This is critical to delivering a more reliable, low-latency user experience, while avoiding the introduction of an expensive security stack at each branch. Citrix SD-WAN and Palo Alto Networks now offer distributed enterprises a more reliable and secure way to connect users in branches to applications in the cloud.

Citrix SD-WAN appliances can connect to the Palo Alto cloud service (Prisma Access Service) network through IPsec tunnels from SD-WAN appliances locations with minimal configuration. You can configure Palo Alto network in Citrix SD-WAN Center.

Before you begin to configure the Prisma Access Service for Remote Networks, make sure you have the following configuration ready to ensure that you are able to successfully enable the service and enforce policy for users in your remote network locations:

1. **Service Connection**—If your remote network locations require access to infrastructure in your corporate headquarters to authenticate users or to enable access to critical network assets, you must set up Access to Your Corporate Network so that headquarters and the remote network locations are connected.

If the remote network location is autonomous and does not need to access to infrastructure at other locations, you do not need to set up the service connection (unless your mobile users need access).

1. **Template**—The Prisma Access service automatically creates a template stack (Remote_Network_Template_ and a top-level template (Remote_Network_Template) for the Prisma Access service for remote networks. To Configure the Prisma Access Service for Remote Networks, you configure the top-level template from scratch or leverage your existing configuration, if you are already running a Palo Alto networks firewall on premise.

   The template requires the settings to establish the IPsec tunnel and Internet Key Exchange (IKE) configuration for protocol negotiation between your remote network location and the Prisma Access service for remote networks, zones that you can reference in security policy, and a log forwarding profile so that you can forward logs from the Prisma Access service for remote networks to the Logging Service.

2. **Parent Device Group**—The Prisma Access service for remote networks requires you to specify a parent device group that includes your security policy, security profiles, and other policy objects (such as application groups and objects, and address groups), as well as authentication policy so that the Prisma Access service for remote networks can consistently enforce policy for traffic that is routed through the IPsec tunnel to the Prisma Access service for remote networks. You

need to either define policy rules and objects on Panorama or use an existing device group to secure users in the remote network location.

> **Note:**
>
> If you use an existing device group that references zones, make sure to add the corresponding template that defines the zones to the Remote_Network_Template_Stack.

This allows you to complete the zone mapping when you configure the Prisma Access Service for Remote Networks.

3. **IP Subnets**—In order for the Prisma Access service to route traffic to your remote networks, you must provide routing information for the subnetworks that you want to secure using the Prisma Access service. You can either define a static route to each subnetwork at the remote network location, or configure BGP between your service connection locations and the Prisma Access service, or use a combination of both methods.

   If you configure both static routes and enable BGP, the static routes take precedence. While it might be convenient to use static routes if you have just a few subnetworks at your remote network locations, in a large deployment with many remote networks with overlapping subnets, BGP will enable you to scale more easily.

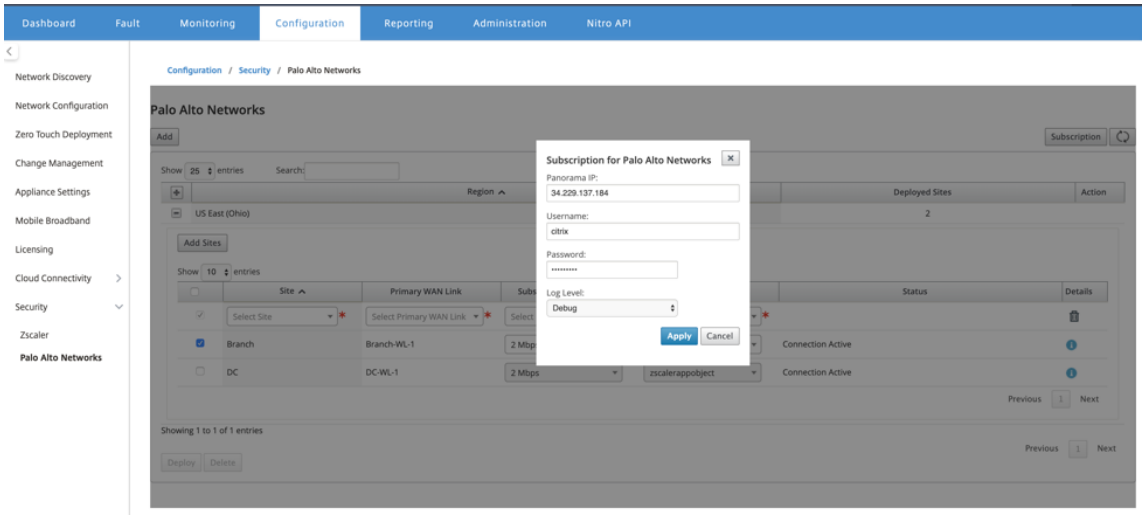
Palo Alto network in SD-WAN Center

Ensure that the following prerequisites are met:

- Obtain panorama IP address from PRISMA ACCESS service.
- Obtain user name and password user in the PRISMA ACCESS service.
- Configure IPsec tunnels in the SD-WAN appliance GUI.
- Make sure the site is not onboarded to a Region, which already has a different site configured with ike/ipsec profiles other than Citrix-IKE-Crypto-Default/Citrix-IPSec-Crypto-Default.
- Make sure that Prisma Access configuration is not changed manually when config is updated by SD-WAN Center.

In the Citrix SD-WAN Center GUI, provide Palo Alto subscription information.

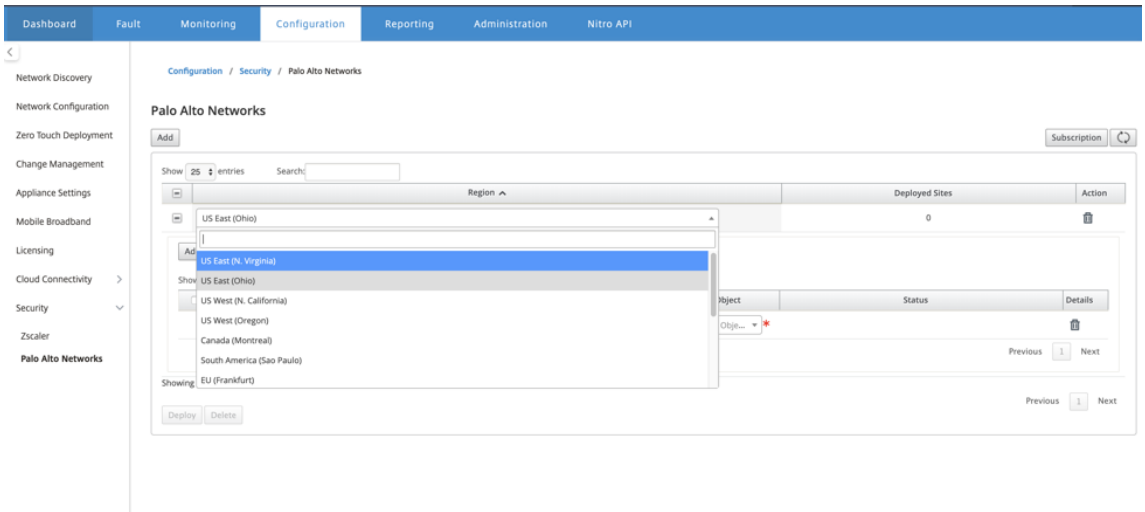
- Configure panorama IP address. You can obtain this IP address from Palo Alto (PRISMA ACCESS service).
- Configure user name and password used in the PRISMA ACCESS service.

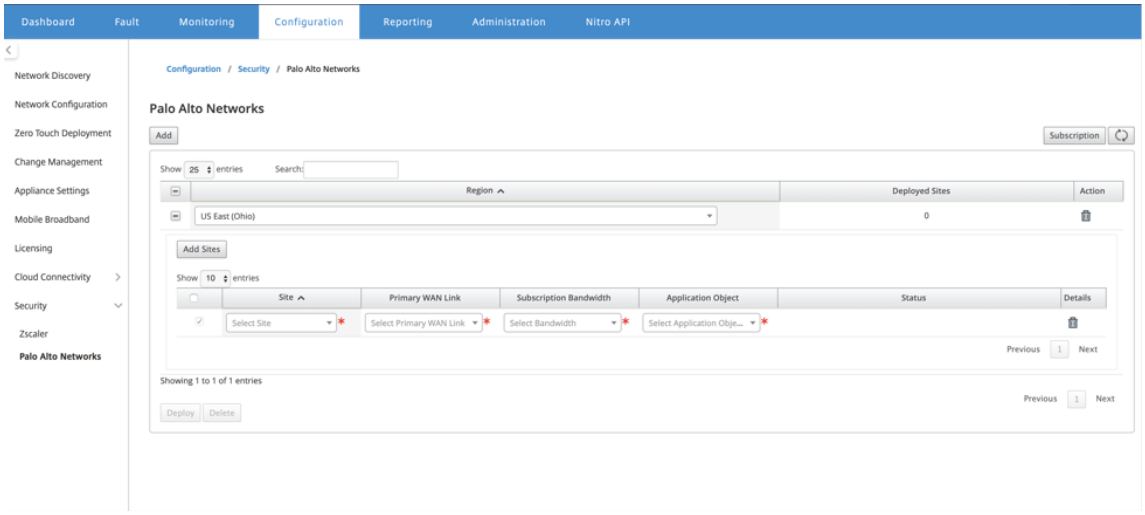


Add and deploy sites

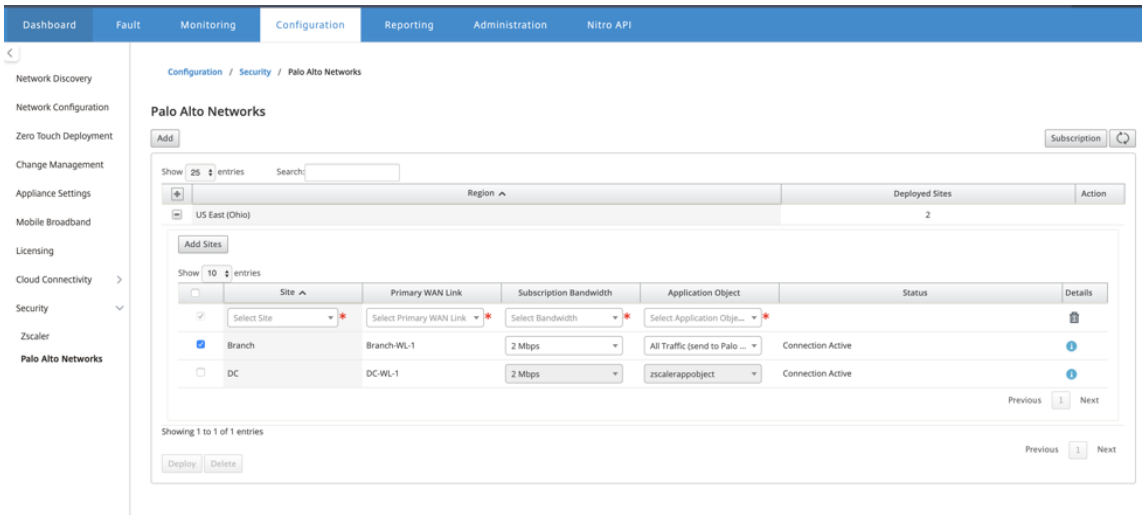
1. To deploy the sites, choose the PRISMA ACCESS network region and the SD-WAN site to be configured for the Prisma Access region, and then select the site WAN link, bandwidth, and application object for traffic selection.

> **Note:**
>
> Traffic flow is impacted if the selected bandwidth exceeds available bandwidth range.
>
> You can choose to redirect all internet bound traffic to the PRISMA ACCESS service by selecting the **All traffic** option under the Application object selection.

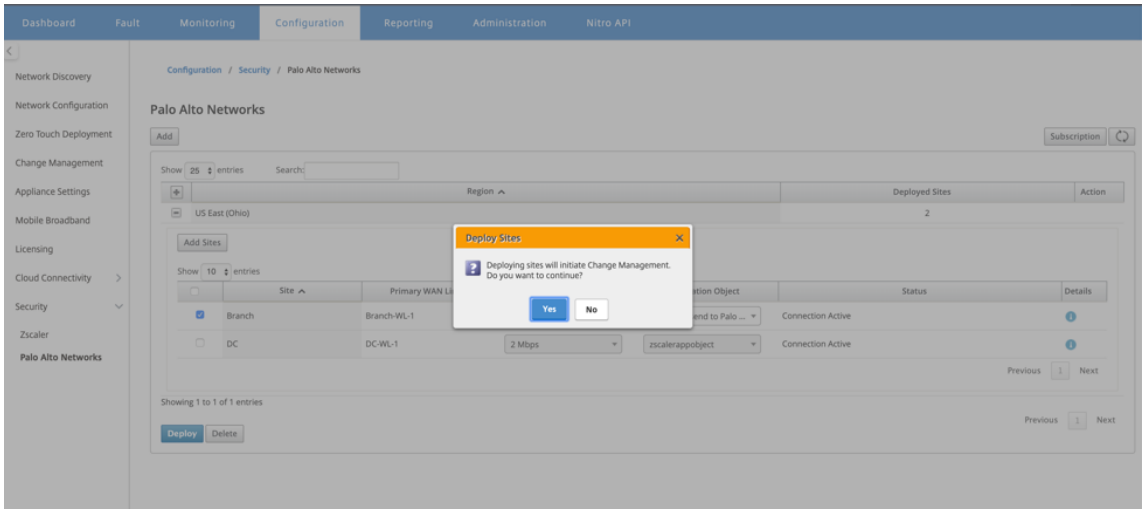




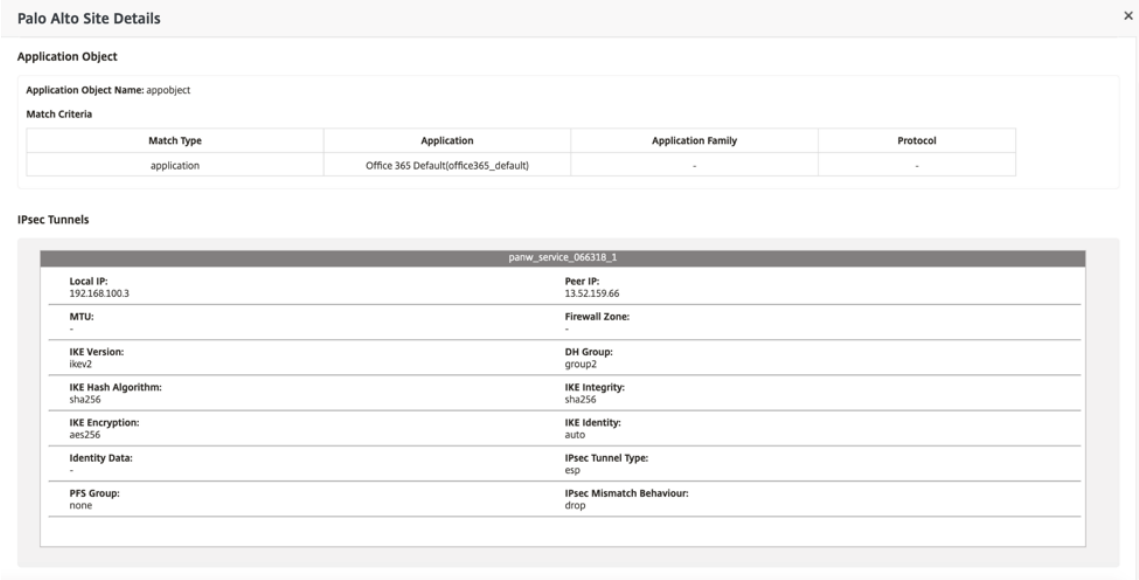
2. You can continue to add more SD-WAN branch sites as required.



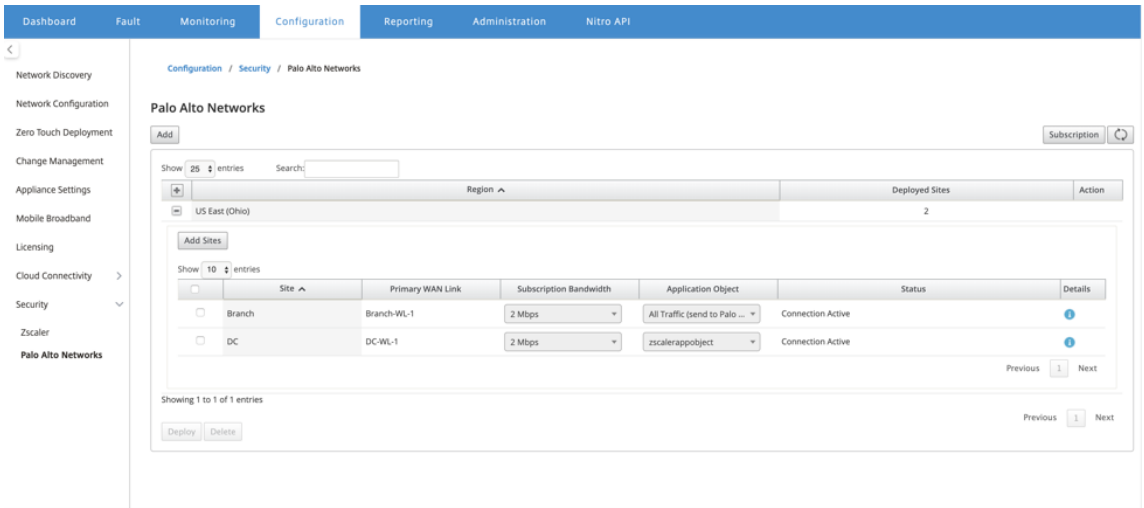
3. Click **Deploy**. The change management process is initiated. Click **Yes** to continue.



After deployment, the IPsec Tunnel configuration used to establish the tunnels is as follows.



The landing page shows the list of all sites configured and grouped under different SD-WAN regions.



Verify end-to-end traffic connection:

- From LAN subnet of branch, access internet resources.
- Verify that traffic goes through Citrix SD-WAN IPsec tunnel to the Palo Alto Prisma Access.
- Verify that Palo Alto security policy is applied on traffic under the Monitoring tab.
- Verify response from internet to host in a branch comes through.

Stateful Firewall and NAT Support

March 12, 2021

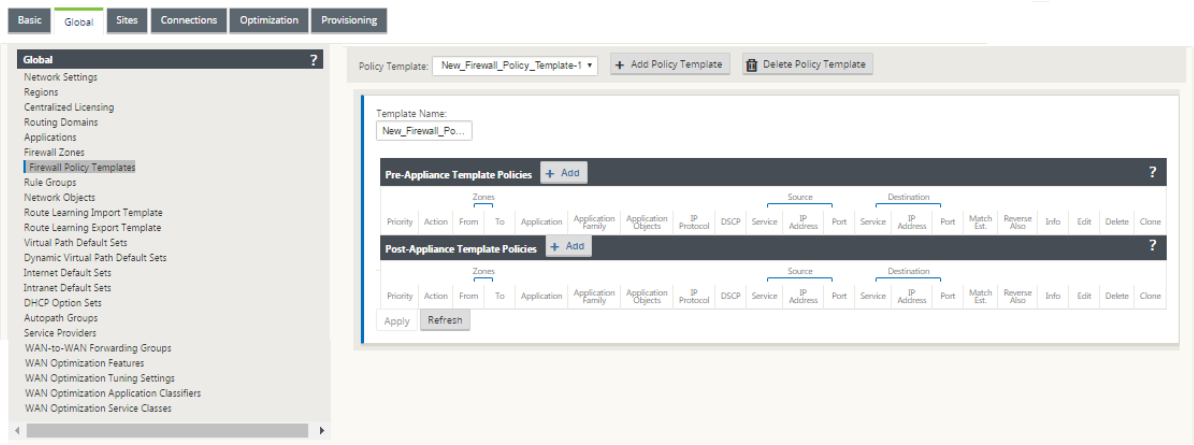
This feature provides a firewall built into the SD-WAN application. The firewall allows policies between services and zones, and supports Static NAT, Dynamic NAT (PAT), and Dynamic NAT with Port Forwarding. More firewall capabilities include:

- 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

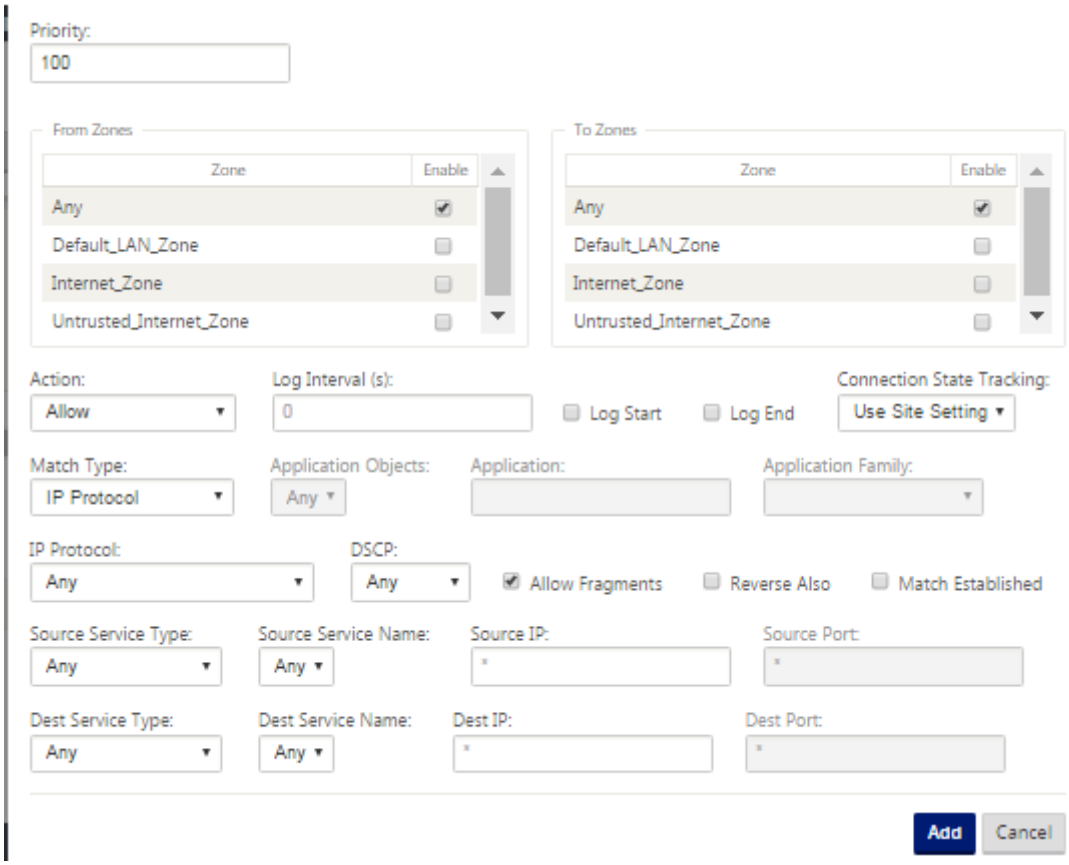
To simplify the configuration process, firewall Policies are created at the Global Configuration level. This Global configuration consists of Pre-Appliance and Post-Appliance site Policy Templates that can be applied to all sites within the SD-WAN network.

> **Note**
>
> It is not recommended to use firewall in Fail-to-Wire inline mode due to security reasons.

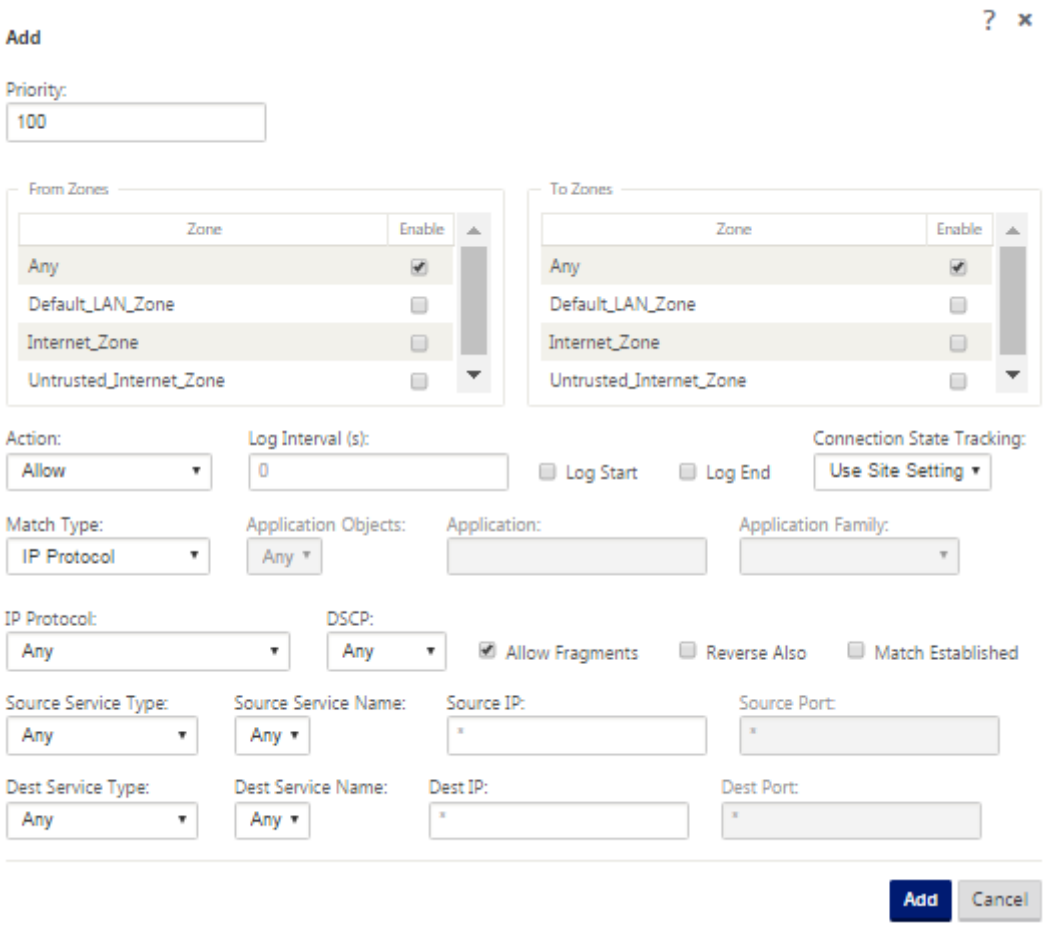
Global-policy templates



Pre-policy template



Post-policy template



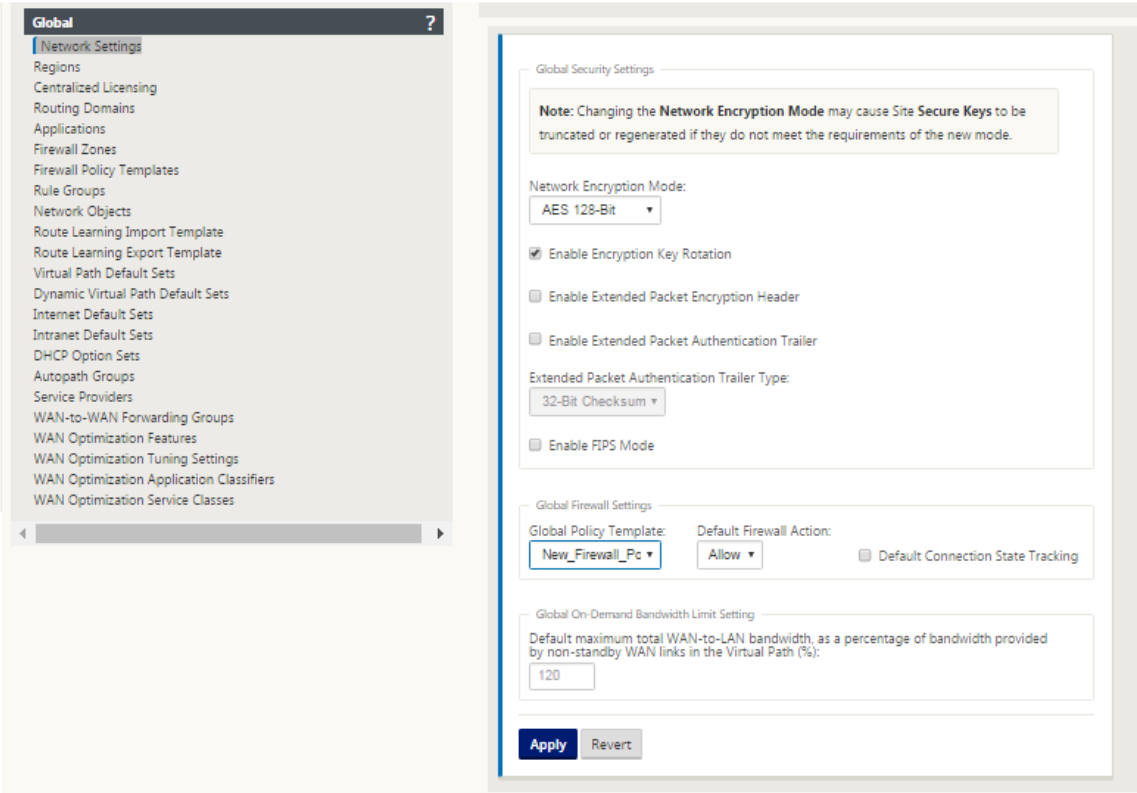
Global firewall settings

March 12, 2021

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.
3. Click **Apply**.

> **Note**
>
> You can also configure these settings at the site level, this will override the global setting.

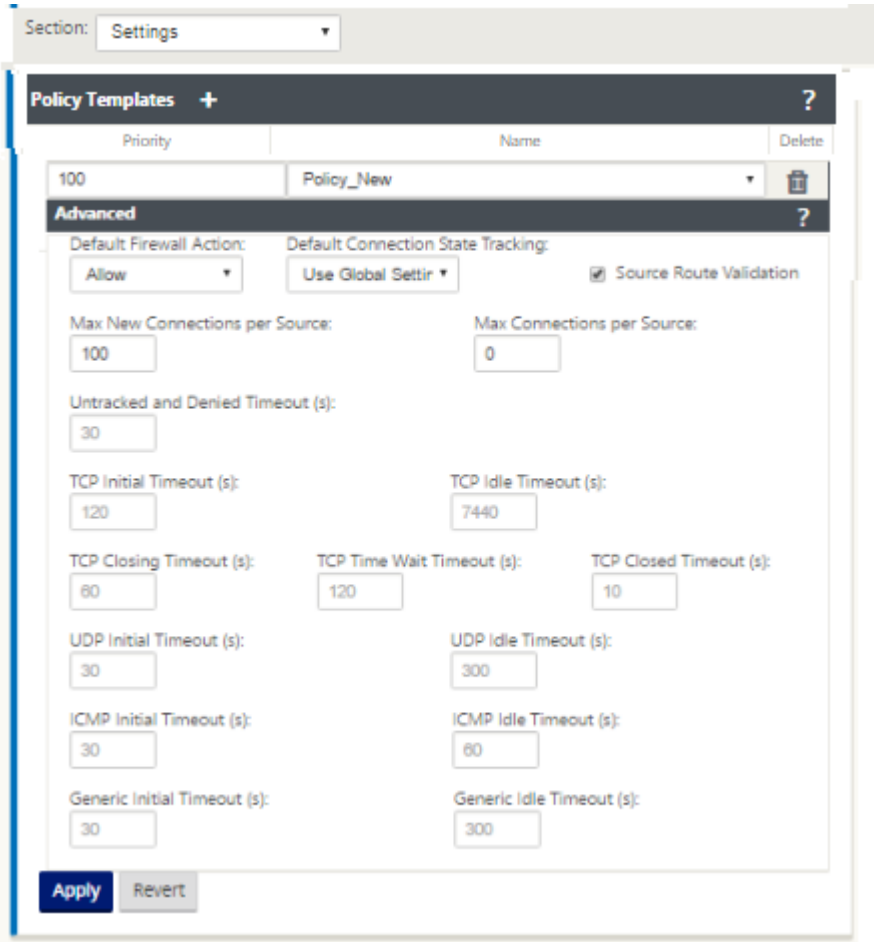
Advanced firewall settings

March 12, 2021

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**.



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

March 12, 2021

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:

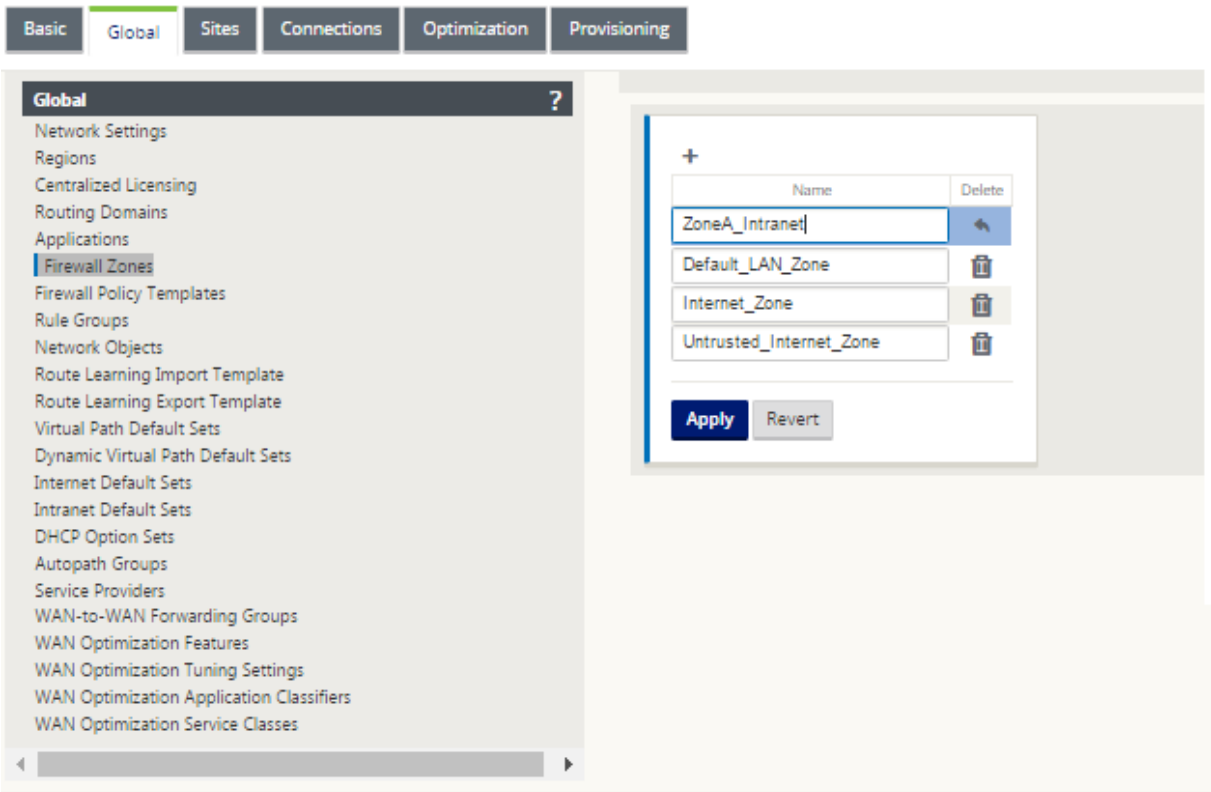
- Internet_Zone
  - Applies to traffic to or from an Internet service using a Trusted interface.
- Untrusted_Internet_Zone
  - Applies to traffic to or from an Internet service using an Untrusted interface.
- Default_LAN_Zone
  - Applies to traffic to or from an object with a configurable zone, where 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

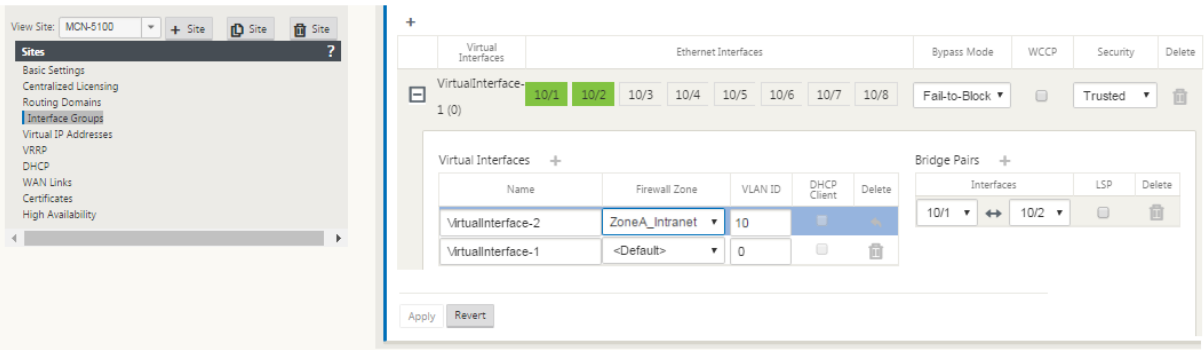
- LAN IPsec Tunnels

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 polices 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".

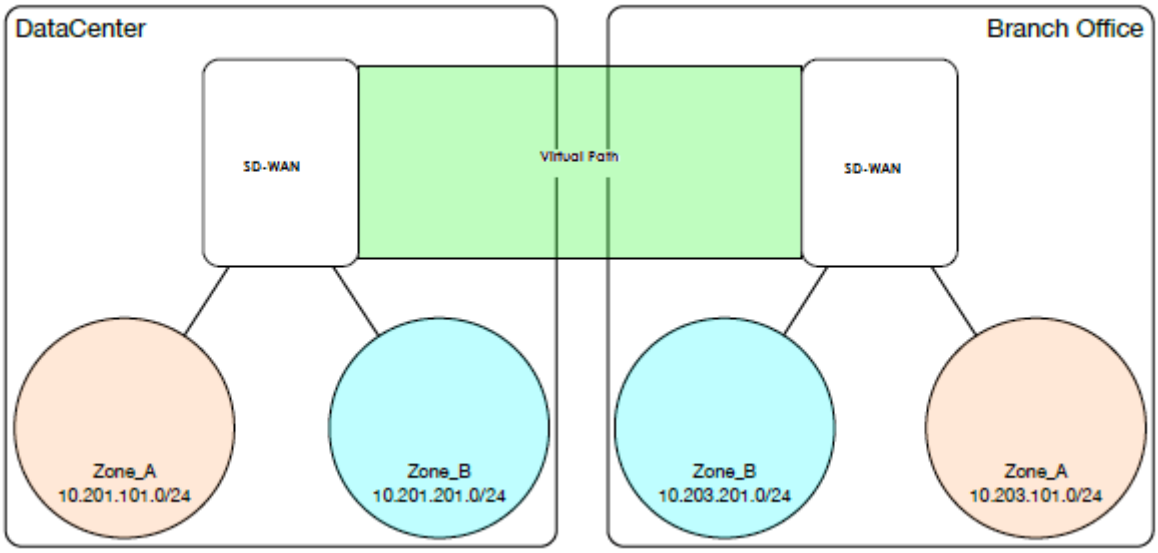


The destination zone of a packet is determined based on the destination route match. When a SD-WAN appliance looks up the destination subnet in the route table, the packet will match a route, which has a zone assigned to it.

- 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.



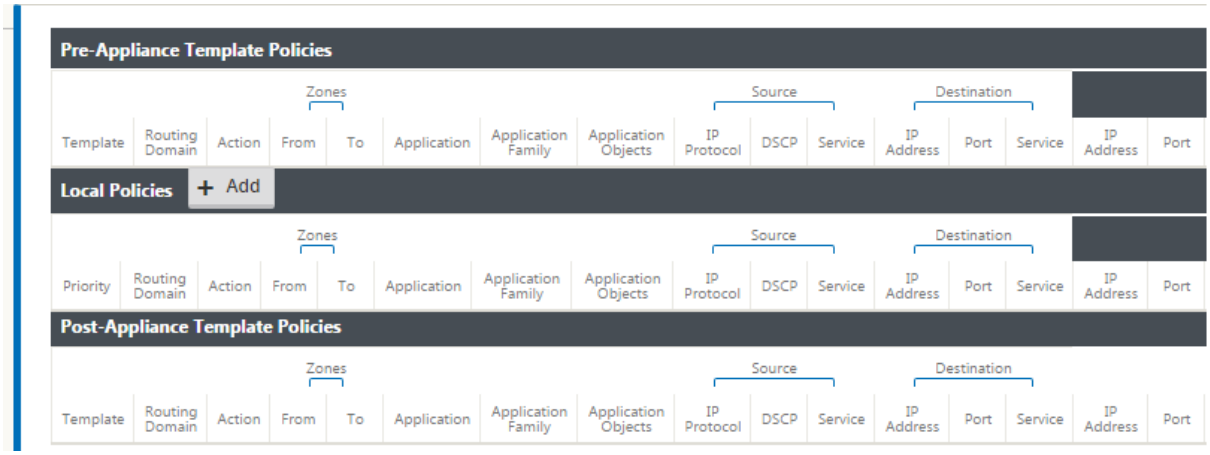
Screenshot below displays the inheritance of zone for a Virtual IP (VIP) from its assigned Virtual Network Interface (VNI).

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
172.16.187.11/24	VirtualInterface-1	Default_LAN_Zone	✓		Trusted	
172.16.187.12/24	VirtualInterface-1	Default_LAN_Zone			Trusted	

Policies

March 12, 2021

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.



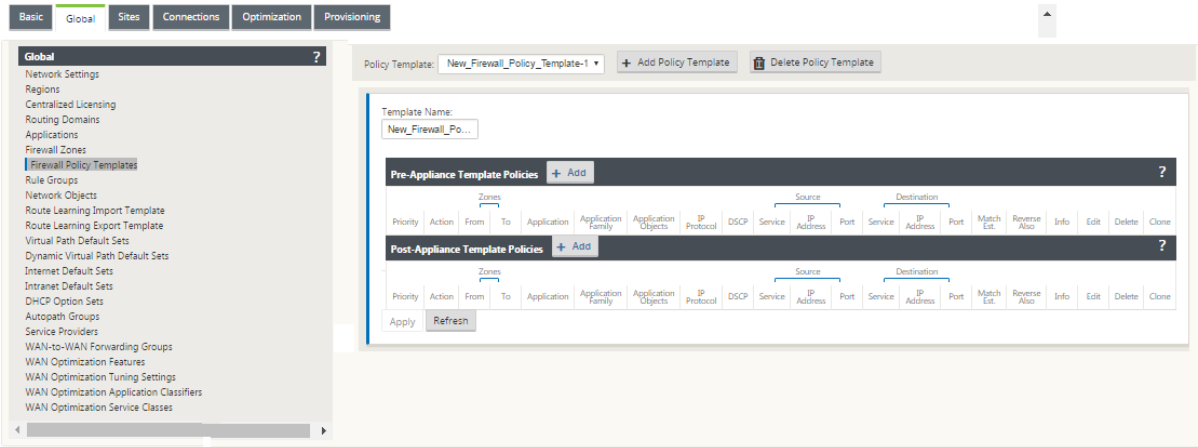
Pre-Appliance Template Policies are applied before any local site policies. Local site policies are applied next, followed by Post-Appliance Template Policies. The goal is to simplify the configuration process by allowing you to apply global policies while still maintaining the flexibility to apply site-specific policies.

Filter policy evaluation order

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.

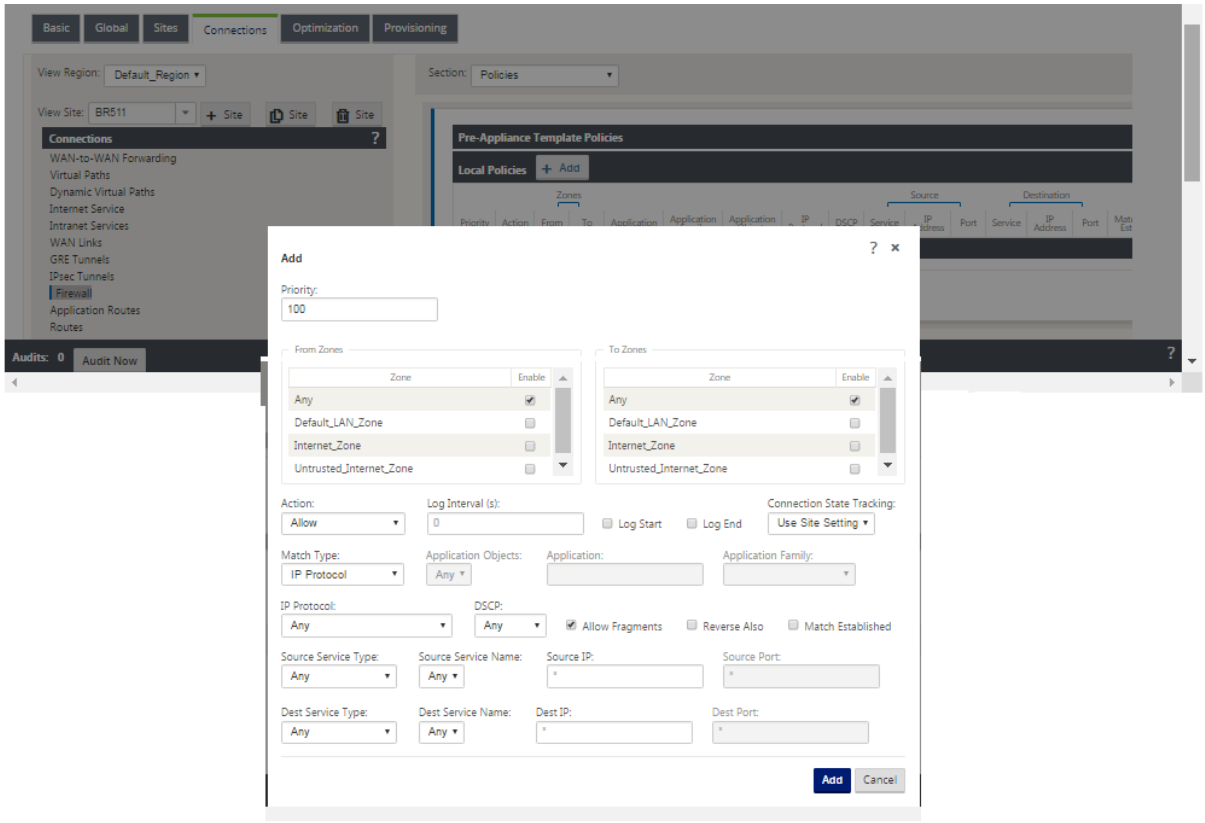
Policy definitions - Global and Local (site)

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.



Policy attributes

- **Priority** –order in which the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority polices.
- **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.

State table for the track option

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)

March 12, 2021

Network Address Translation (NAT) performs IP address conservation to preserve the limited number of registered IPv4 addresses. It enables private IP networks that use unregistered IP addresses to connect to the Internet. The NAT feature on Citrix SD-WAN connects your private SD-WAN network with the public internet. It translates the private addresses in the internal network into a legal public address. NAT also ensures extra security by advertising only one address for the entire network to the internet, hiding the entire internal network. Citrix SD-WAN supports the following NAT types:

- Static one-to-one NAT
- Dynamic NAT (PAT- Port Address Translation)
- Dynamic NAT with Port Forwarding rules

> **Note**
>
> 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.

Static NAT

March 12, 2021

Static NAT is a one-to-one mapping of a private IP address or subnet inside the SD-WAN network to a public IP address or subnet outside the SD-WAN network. Configure Static NAT by manually entering the inside IP address and the outside IP address to which it has to translate. You can configure Static NAT for the Local, Virtual Paths, Internet, Intranet, and Inter-routing domain services.

Inbound and Outbound NAT

The direction for a connection can either be inside to outside or outside to inside. When a NAT rule is created, it is applied to both the directions depending on the direction match type.

- Inbound: The source address is translated for packets received on the service. The destination address is translated for packets transmitted on the service. For example, Internet service to LAN service –For packets received (Internet to LAN), the source IP address is translated. For packets transmitted (LAN to Internet), the destination IP address is translated.
- Outbound: The destination address is translated for packets received on the service. The source address is translated for packets transmitted on the service. For example, LAN service to Internet service –for packets transmitted (LAN to Internet) the source IP address is translated. For packets received (Internet to LAN) the destination IP address is translated.

Zone Derivation

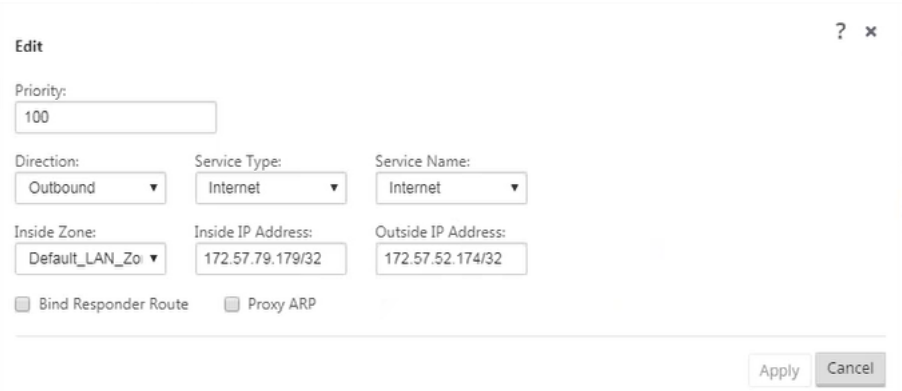
The source and destination firewall zones for the inbound or outbound traffic should not be the same. If both the source and destination firewall zones are the same, NAT is not performed on the traffic.

For outbound NAT, the outside zone is automatically derived from the service. Every service on SD-WAN is associated to a zone by default. For example, Internet service on a trusted internet link is associated with the trusted internet zone. Similarly, for an inbound NAT, the inside zone is derived from the service.

For a Virtual path service NAT zone derivation does not happen automatically, you have to manually enter the inside and outside zone. NAT is performed on traffic belonging to these zones only. Zones cannot be derived for virtual paths because there might be multiple zones within the Virtual path subnets.

Configure Static NAT Policies

To configure Static NAT policies, in the Configuration Editor, navigate to **Connections** > **Firewall** > **Static NAT Policies**.

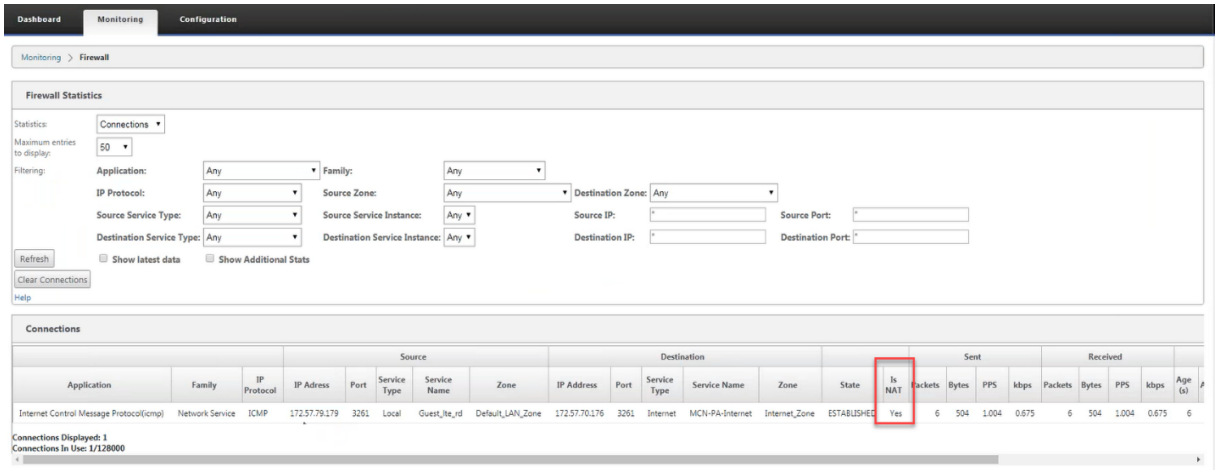


- **Priority**: The order in which the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority policies.
- **Direction**: The direction in which the traffic is flowing, from the perspective of the virtual interface or service. It can either be inbound or outbound traffic.
- **Service Type**: The SD-WAN service types on which the NAT policy is applied. For static NAT, the service types supported are Local, Virtual Paths, Internet, Intranet, and Inter-routing domain services
- **Service Name**: Select a configured service name that corresponds to the Service Type.
- **Inside Zone**: The Inside firewall zone match-type that the packet must be from to allow translation.
- **Outside Zone**: The outside firewall zone match-type that the packet must be from to allow translation.

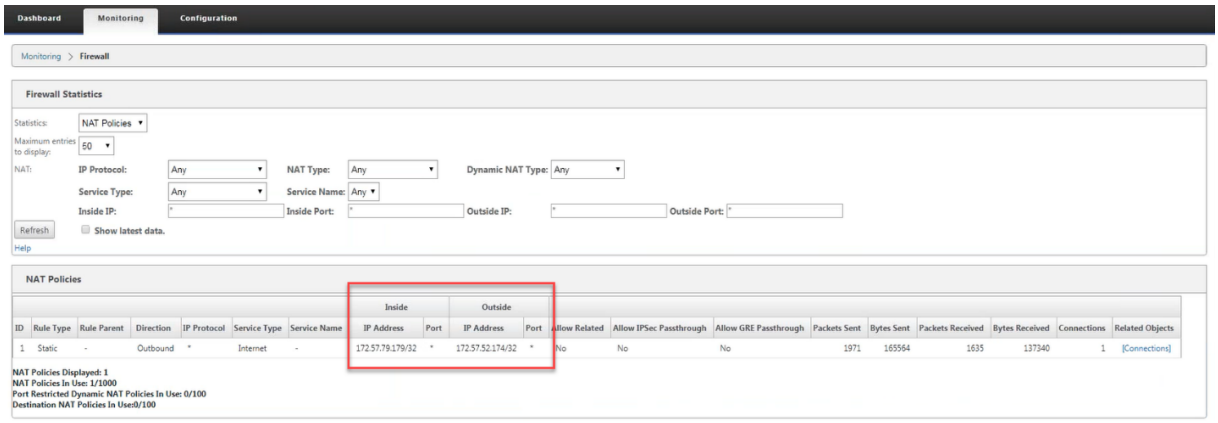
- **Inside IP address**: The inside IP address and prefix that has to be translated to if the match criteria is met.
- **Outside IP address**: The outside IP address and prefix that the inside IP address is translated to if the match criteria is met.
- **Bind Responder Route**: Ensures that the response traffic is sent over the same service that it is received on, to avoid asymmetric routing.
- **Proxy ARP**: Ensures that the appliance responds to local ARP requests for the outside IP address.

Monitoring

To monitor NAT, navigate to **Monitoring** > **Firewall Statistics** > **Connections**. For a connection you can see if NAT is done or not.

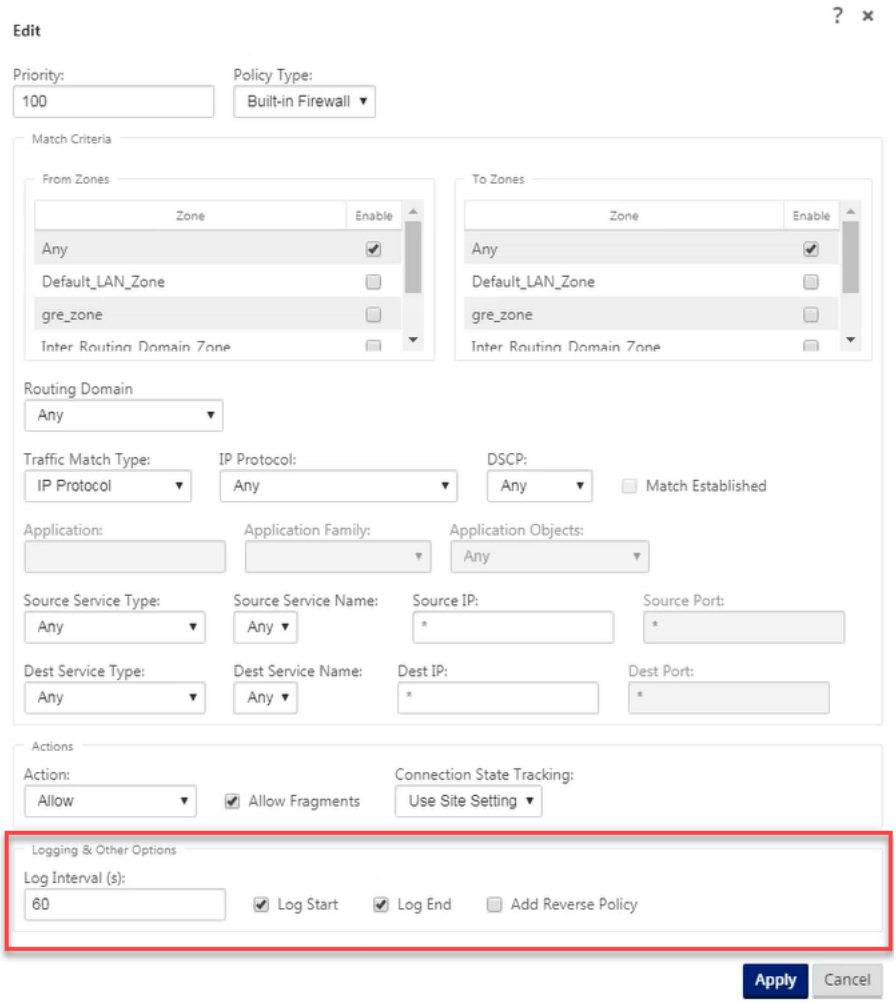


To further see the inside IP address to outside IP address mapping, click **Post-Route NAT** under **Related Objects** or navigate to **Monitoring** > **Firewall Statistics** > **NAT policies**.

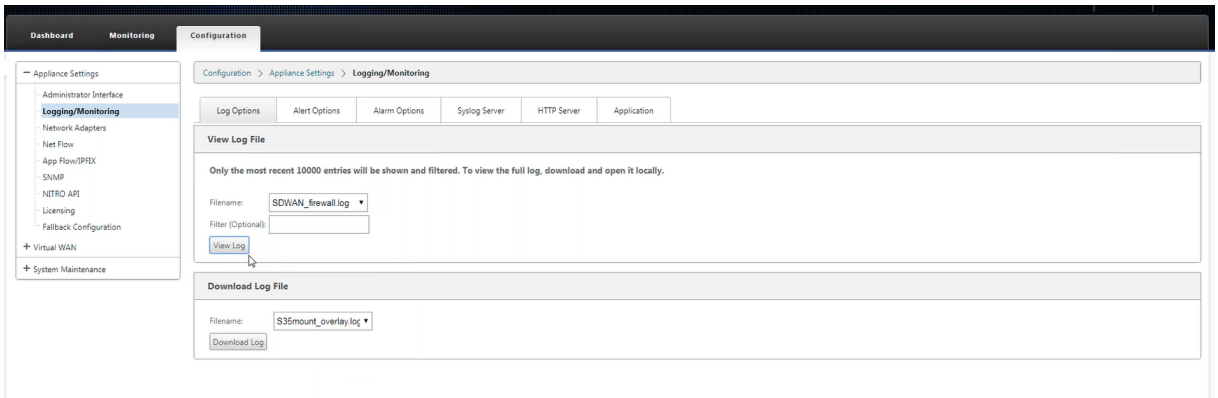


Logs

You can view logs related to NAT in firewall logs. To view logs for NAT, create a firewall policy that matches your NAT policy and ensure that logging is enabled on the firewall filter.



Navigate to **Logging/Monitoring** > **Log Options**, select **SDWAN_firewal.log**, and click **View Log**.



The NAT connection details are displayed in the log file.


```
2020-05-11T10:14:19.861597+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO    conn_clear_all@forward/firewall/connection.c:8704:      Removed 1 Connections
2020-05-11T10:15:44.750109+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:16.981504+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:20.108292+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:16:21.299055+0000 INFO    t2_firewall_monitor.pl   NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112650+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:21.353441+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:20:22.374898+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.598370+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 50 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.846123+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
```

Dynamic NAT

March 12, 2021

Dynamic NAT is a many-to-one mapping of a private IP address or subnets inside the SD-WAN network to a public IP address or subnet outside the SD-WAN network. The traffic from different zones and subnets over trusted (inside) IP addresses in the LAN segment is sent over a single public (outside) IP address.

Dynamic NAT types

Dynamic NAT does Port Address Translation (PAT) along with IP address translation. Port numbers are used to distinguish which traffic belongs to which IP address. A single public IP address is used for all internal private IP addresses, but a different port number is assigned to each private IP address. PAT is a cost effective way to allow multiple hosts to connect to the Internet using a single Public IP address.

- **Port Restricted**: Port Restricted NAT uses the same outside port for all translations related to an Inside IP Address and Port pair. This mode is typically used to allow Internet P2P applications.
- **Symmetric**: Symmetric NAT uses the same outside port for all translations related to an Inside IP Address, Inside Port, Outside IP Address, and Outside Port tuple. This mode is typically used to enhance security or expand the maximum number of NAT sessions.

Inbound and Outbound NAT

The direction for a connection can either be inside to outside or outside to inside. When a NAT rule is created, it is applied to both the directions depending on the direction match type.

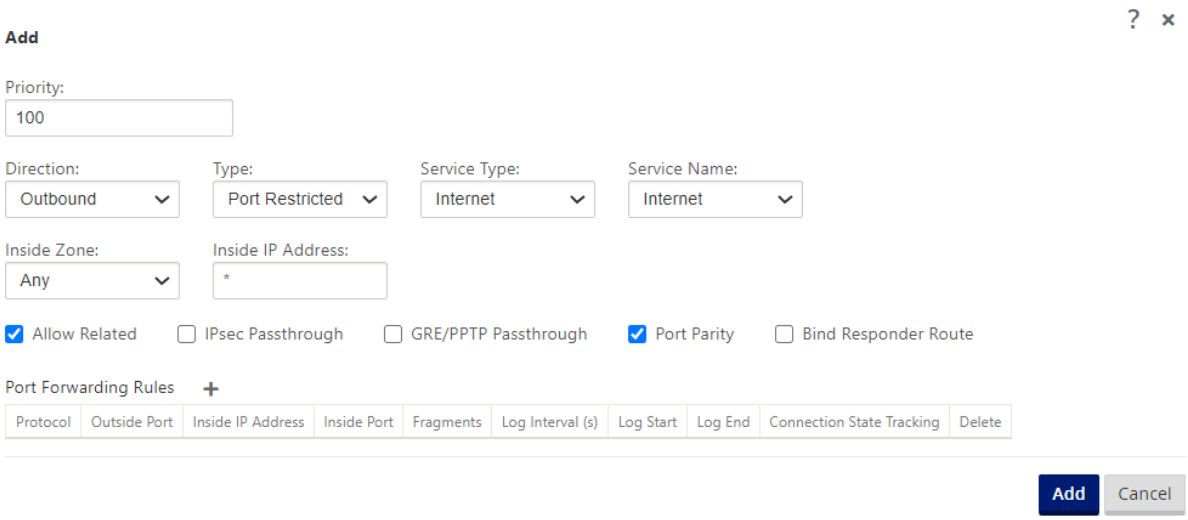
- **Outbound**: The destination address is translated for packets received on the service. The source address is translated for packets transmitted on the service. Outbound dynamic NAT

is supported on Local, Internet, Intranet, and Inter-routing domain services. For WAN services such as Internet and Intranet services, the configured WAN link IP address is dynamically chosen as the outside IP address. For Local and Inter-routing domain services, provide an outside IP address. The Outside zone is derived from the selected service. A typical use case of outbound dynamic NAT is to simultaneously allow multiple users in your LAN to securely access the internet using a single Public IP address.

- **Inbound**: The source address is translated for packets received on the service. The destination address is translated for packets transmitted on the service. Inbound dynamic NAT is not supported on WAN services such as Internet and Intranet. There is an explicit audit error to indicate the same. Inbound dynamic NAT is supported on Local and Inter-routing domain services only. Provide an outside zone and outside IP address to be translated to. A typical use case for inbound dynamic NAT is to allow external users access email or web servers hosted in your private network.

Configure Dynamic NAT Policies

To configure Dynamic NAT policies, in the Configuration Editor, navigate to **Connections** > **Firewall** > **Dynamic NAT Policies**.

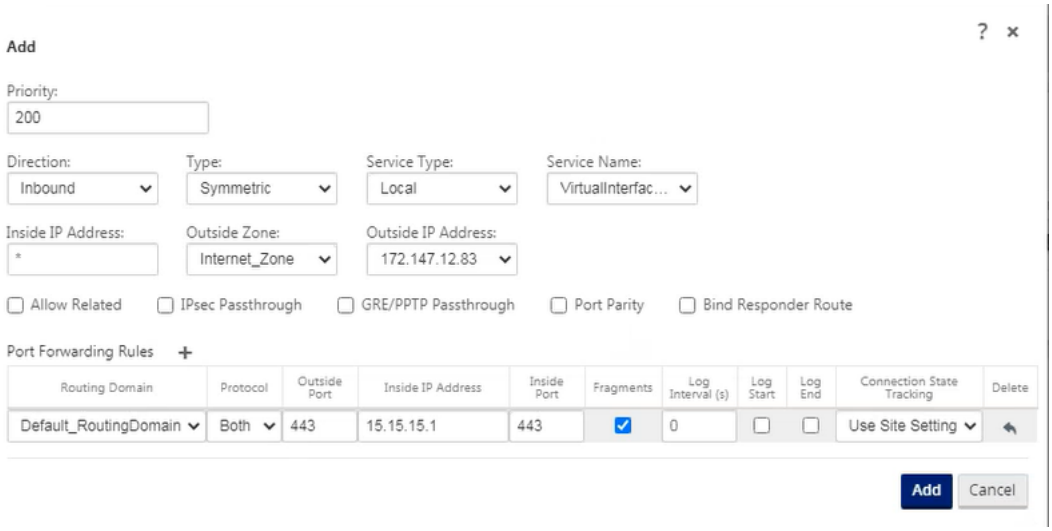


- **Priority**: The order the policy is applied within all the defined policies. Lower priority policies are applied before higher priority policies.
- **Direction**: The direction in which the traffic is flowing, from the perspective of the virtual interface or service. It can either be inbound or outbound traffic.
- **Type**: The type of dynamic NAT to perform, Port-restricted, or Symmetric.
- **Service Type**: The SD-WAN service types on which the dynamic NAT policy is applied. Inbound dynamic NAT is supported on Local and Inter-routing domain services. Outbound dynamic NAT is supported on Local, Internet, Intranet, and Inter-routing domain services

- **Service Name**: Select a configured service name that corresponds to the Service Type.
- **Inside Zone**: The Inside firewall zone match-type that the packet must be from to allow translation.
- **Outside Zone**: For inbound traffic, specify the outside firewall zone match-type that the packet must be from to allow translation.
- **Inside IP address**: The inside IP address and prefix that has to be translated to if the match criteria is met. Enter '*'to indicate any inside IP address.
- **Outside IP address**: The outside IP address and prefix that the inside IP address is translated to if the match criteria is met. For outbound traffic using Internet and Intranet services, the configured WAN link IP address is dynamically chosen as the outside IP address.
- **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 Pass through**: Allow an IPsec (AH/ESP) session to be translated.
- **GRE/PPTP Pass through**: Allow a GRE/PPTP session to be translated.
- **Port Parity**: If enabled, outside ports for NAT connections maintain parity (even if inside port is even, odd if outside port is odd).
- **Bind Responder Route**: Ensures that the response traffic is sent over the same service that it is received on, to avoid asymmetric routing.

Port Forwarding

Dynamic NAT with port forwarding allows you 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 you can define the port forwarding policies. Configure dynamic NAT for IP address translation and define the port forwarding policy to map an outside port to an inside port. Dynamic NAT port forwarding is typically used to allow remote hosts to connect to a host or server on your private network. For a more detailed use case see, Citrix SD-WAN Dynamic NAT explained.



- **Protocol**: TCP, UDP, or both.
- **Outside Port**: The Outside port that is port forward into the inside port.
- **Inside IP address**: The inside address to forward matching packets.
- **Inside Port**: The Inside port that the outside port will be port forwarded into.
- **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**: Bidirectional connection state tracking is performed on TCP, UDP, and ICMP packets matching the Rule. This feature blocks flows which appear illegitimate, due to asymmetric routing or failure of checksum, protocol specific validation. The state details are displayed under **Monitoring** > **Firewall** > **Connections**.
- **No Tracking**: Bidirectional connection state tracking is not performed on packets matching the Rule.

Every port forwarding rule has a parent NAT rule. The outside IP address is taken from the parent NAT rule.

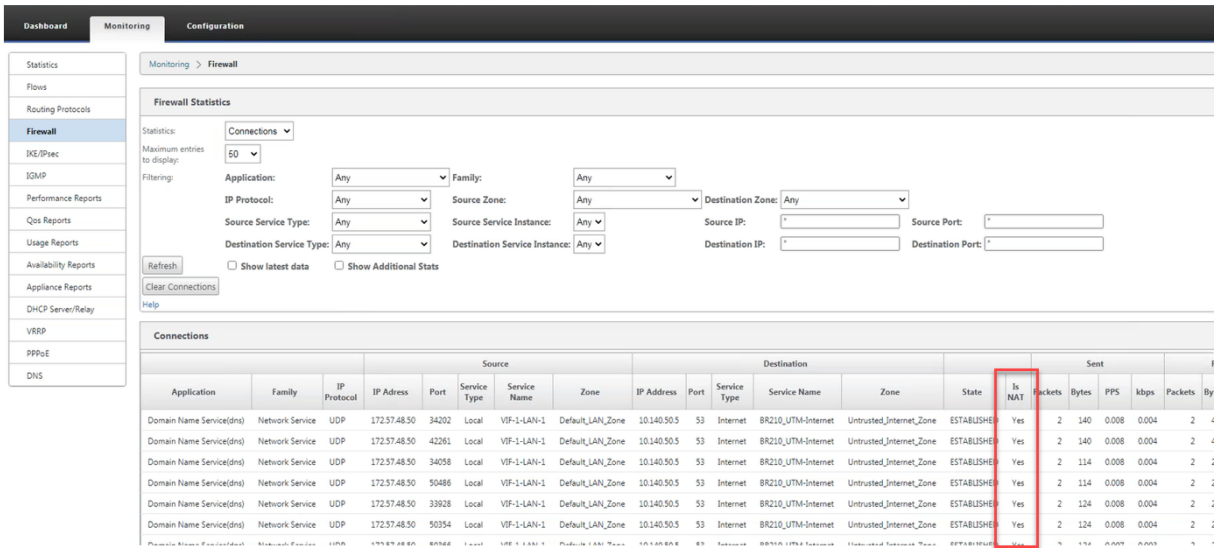
Auto-created Dynamic NAT policies

Dynamic NAT policies for the Internet service are auto created in the following cases:

- Configuring internet service on an untrusted interface (WAN link).
- Enabling internet access for all routing domains on a single WAN link. For more details, see Configure firewall segmentation.
- Configuring DNS forwarders or DNS proxy on SD-WAN. For more details, see Domain name system.

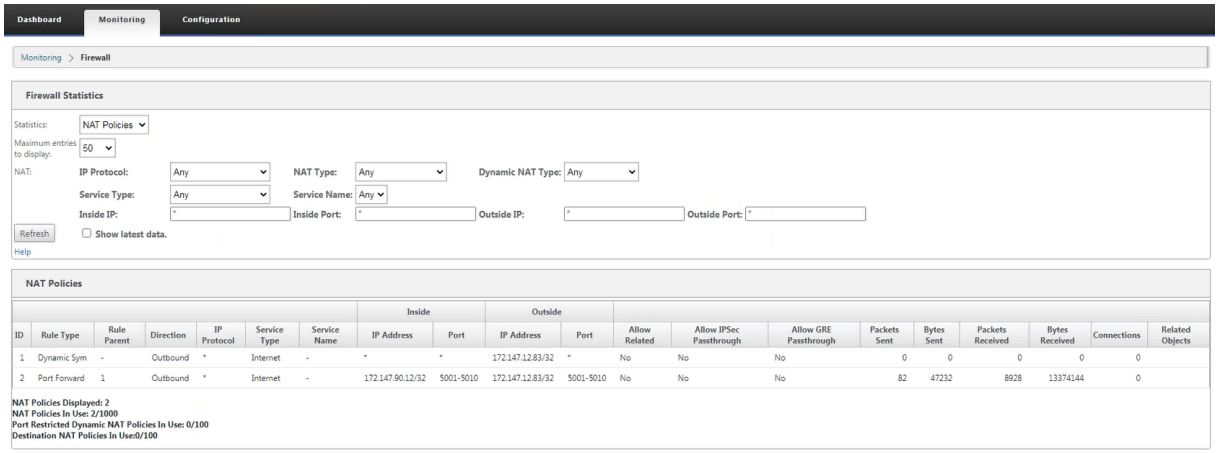
Monitoring

To monitor dynamic NAT, navigate to **Monitoring** > **Firewall Statistics** > **Connections**. For a connection you can see if NAT is done or not.

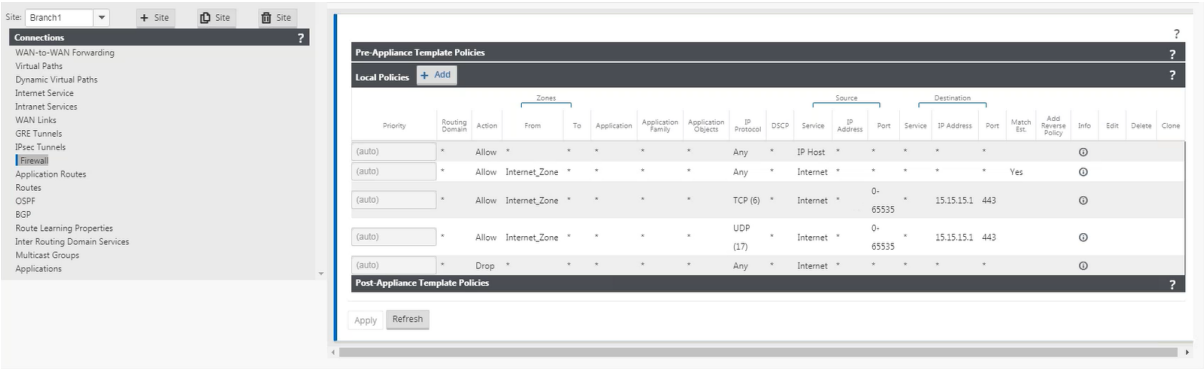


To further see the inside IP address to outside IP address mapping, click **Pre-Route NAT** or **Post-route NAT** under **Related Objects** or navigate to **Monitoring** > **Firewall Statistics** > **NAT policies**.

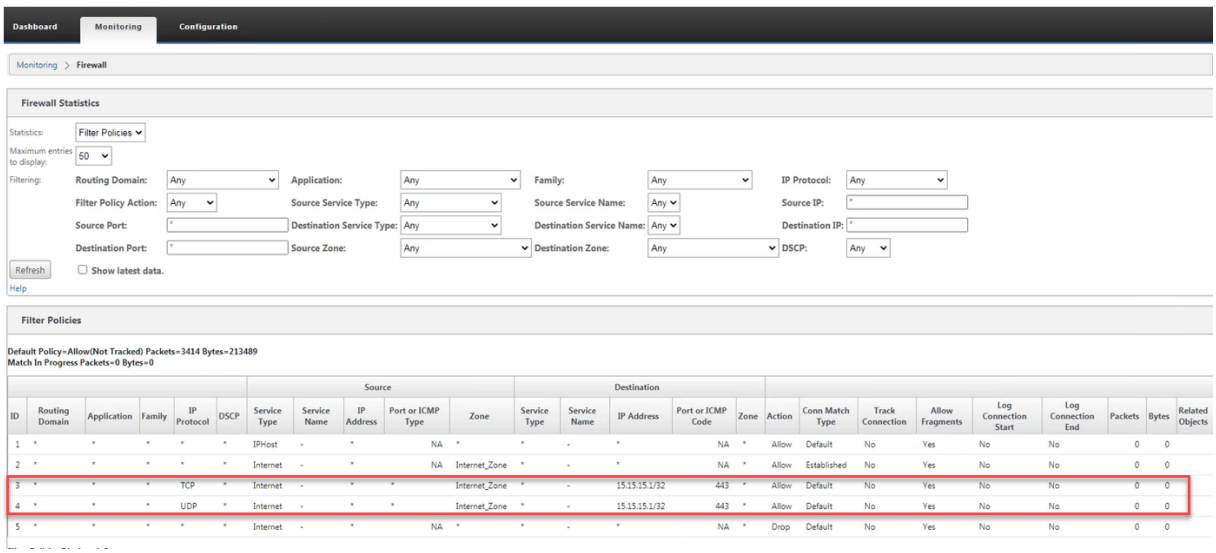
The following screenshot shows the statistics for the Dynamic NAT rule of type symmetric and its corresponding port forwarding rule.



When a port forwarding rule is created a corresponding firewall rule is also created.

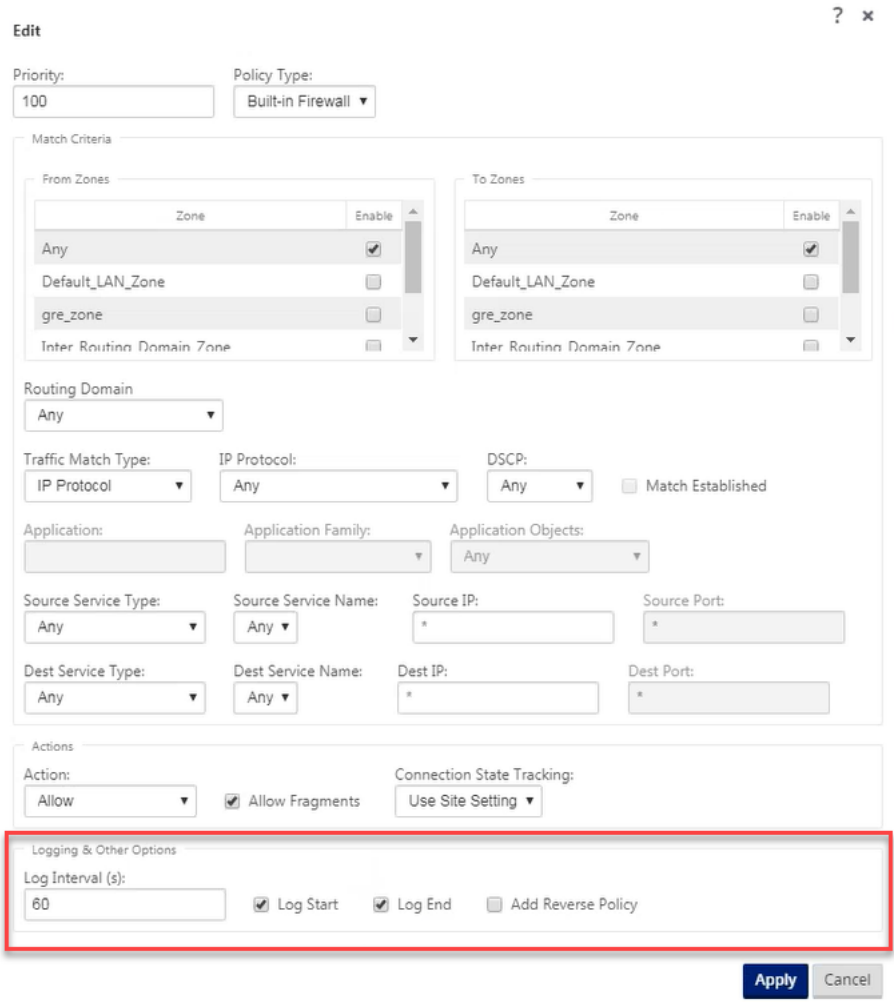


You can see the filter policy statistics by navigating to **Monitoring** > **Firewall Statistics** > **Filter Policies**.

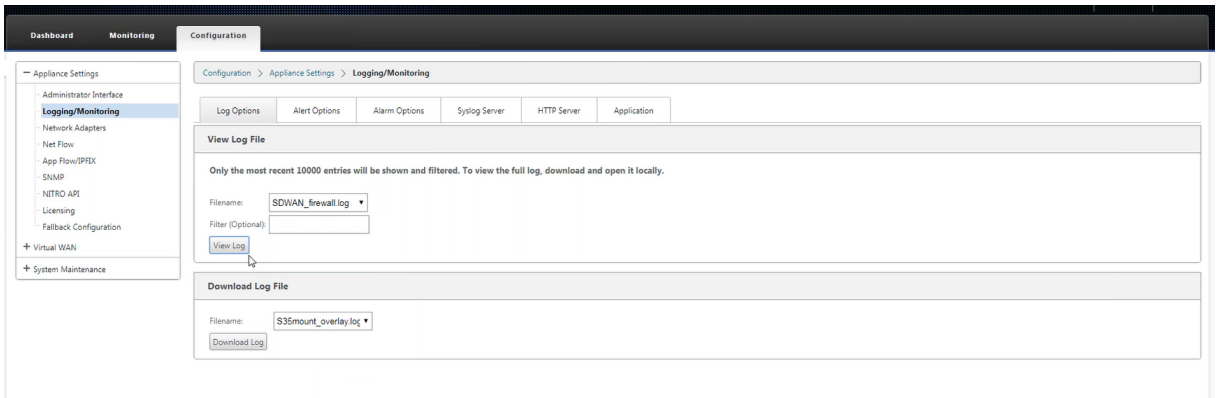


Logs

You can view logs related to NAT in firewall logs. To view logs for NAT, create a firewall policy that matches your NAT policy and ensure that logging is enabled on the firewall filter.



Navigate to **Logging/Monitoring** > **Log Options**, select **SDWAN_firewal.log**, and click **View Log**.



The NAT connection details are displayed in the log file.


```
2020-05-11T10:14:19.861597+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO    conn_clear_all@forward/firewall/connection.c:8704:      Removed 1 Connections
2020-05-11T10:15:44.750109+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:16.981504+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:20.108292+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:16:21.299055+0000 INFO    t2_firewall_monitor.pl   NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112650+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:21.353441+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:20:22.374898+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.598370+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 50 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.846123+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
```

Configure Virtual WAN Service

March 12, 2021

The Citrix SD-WAN configuration describes and defines the topology of your Citrix SD-WAN network. Before you can deploy an SD-WAN network, you must define the Virtual WAN configuration. To do this, use Configuration Editor in the Citrix 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 bit 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 with 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 with that combined key.

Enabling virtual WAN service

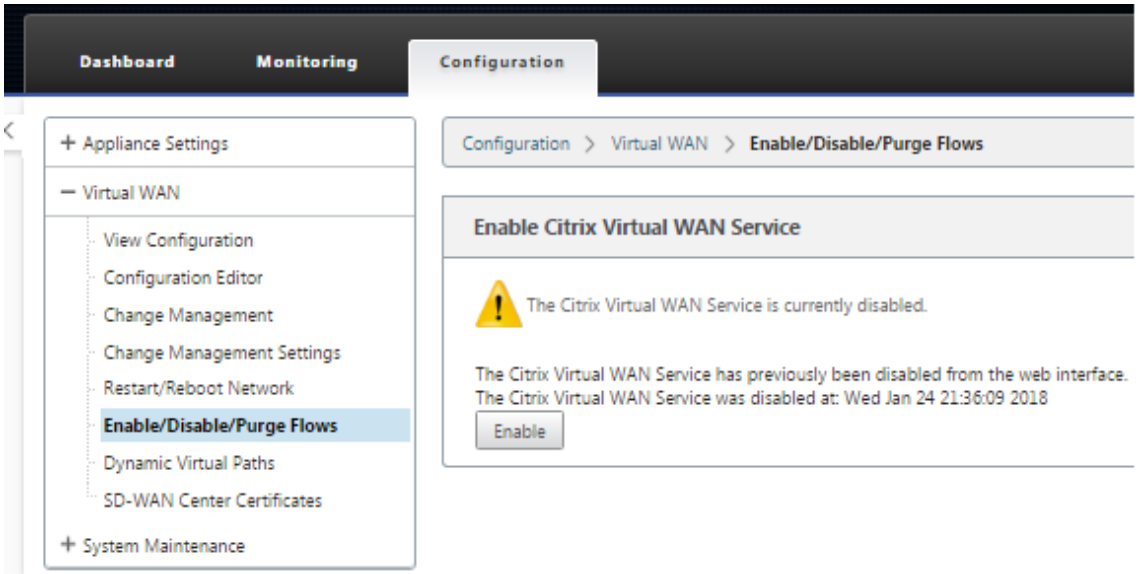
If this is an initial installation and configuration, as a final step you need to manually enable the Virtual WAN Service on each SD-WAN appliance in your network. Enabling the service enables and starts the Virtual WAN daemon.

> **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.

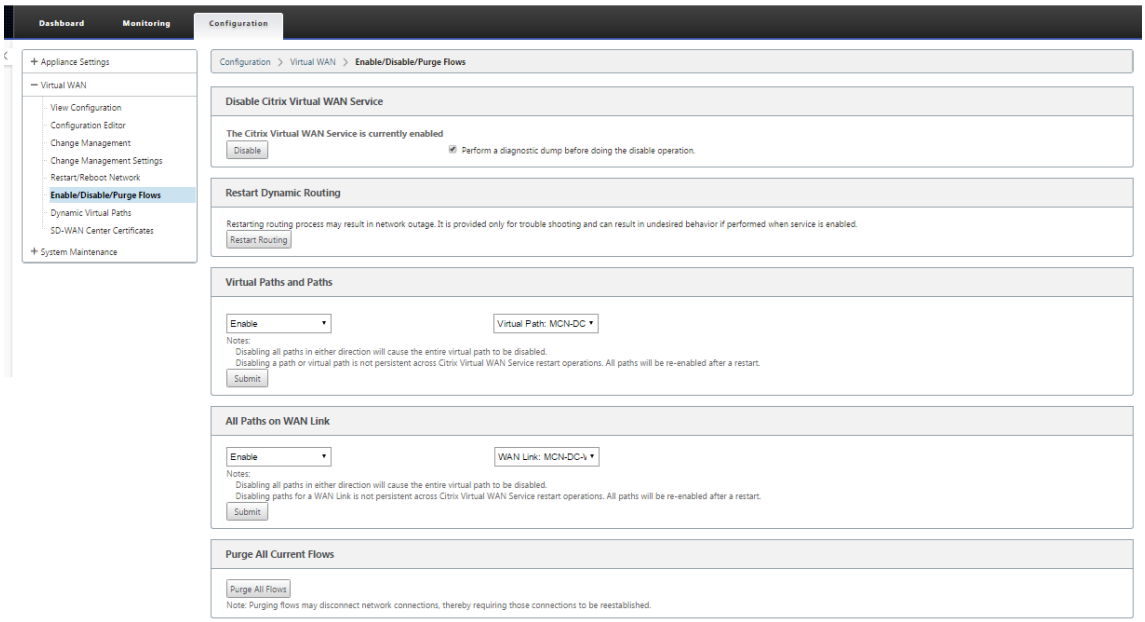
To manually enable the Virtual WAN Service on an appliance, do the following:

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 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

March 12, 2021

Virtual Route Forwarding (VRF) firewall segmentation provides multiple routing domains accesses 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.

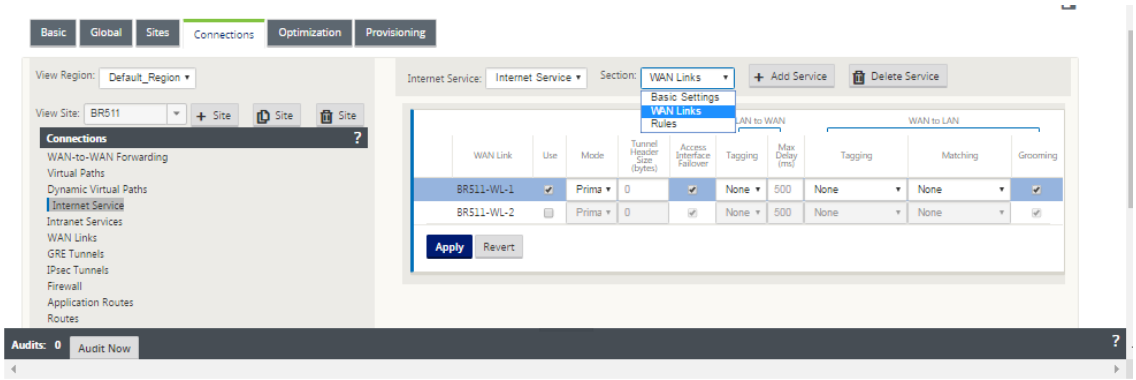
- When enabled, this feature applies to all routing domains.

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.

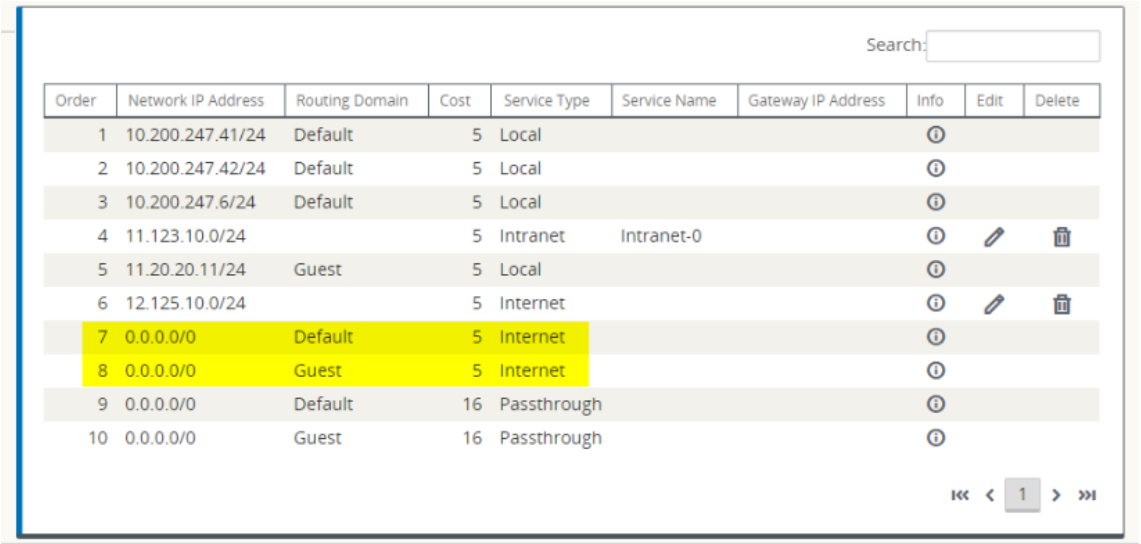
> **Note**
>
> For more information, see how to configure VRFs.

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.



> **Note**
>
> You should see that 0.0.0.0/0 routes added, one per routing domain, under **Connections** > **View Region** > **View Site** > [Site Name] > **Routes**.

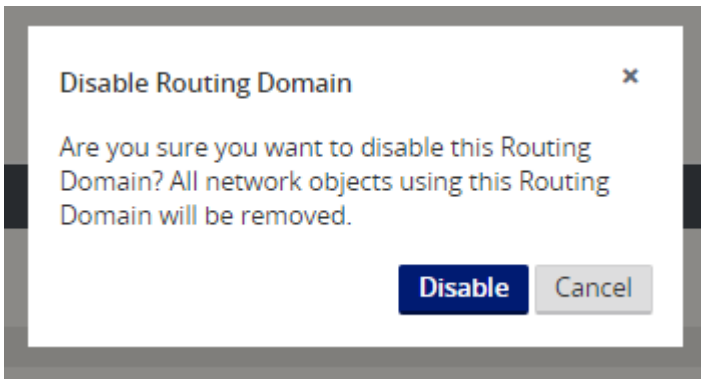


Search:

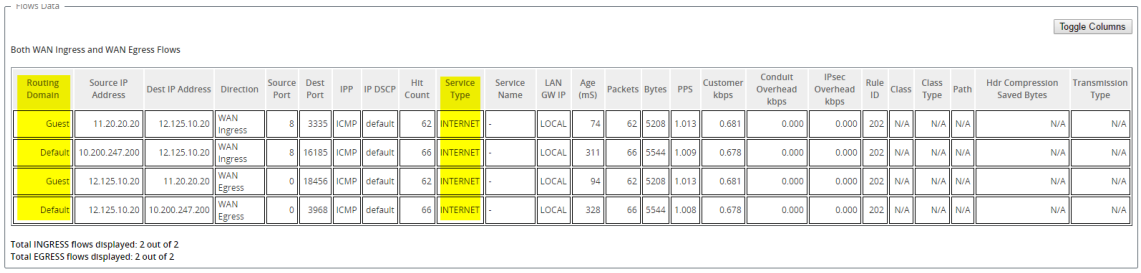
Order	Network IP Address	Routing Domain	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.200.247.41/24	Default	5	Local					
2	10.200.247.42/24	Default	5	Local					
3	10.200.247.6/24	Default	5	Local					
4	11.123.10.0/24		5	Intranet	Intranet-0				
5	11.20.20.11/24	Guest	5	Local					
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					

It is no longer required to have all routing domains enabled at the MCN.

2. If you disable routing domains at the MCN, the following message appears if the domains are in use at a branch site:



3. 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

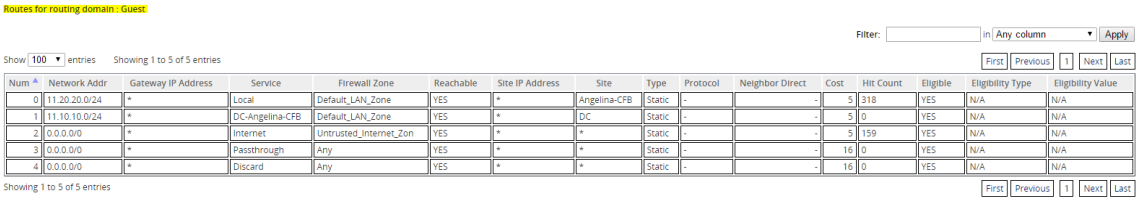
Toggle Columns

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	N/A
Default	10.200.247.200	12.125.10.20	WAN Ingress	8	16185	ICMP	default	66	INTERNET	-	LOCAL	311	66	5544	1.009	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Guest	12.125.10.20	11.20.20.20	WAN Egress	0	18456	ICMP	default	62	INTERNET	-	LOCAL	94	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	12.125.10.20	10.200.247.200	WAN Egress	0	3968	ICMP	default	66	INTERNET	-	LOCAL	328	66	5544	1.008	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A

Total INGRESS flows displayed: 2 out of 2
Total EGRESS flows displayed: 2 out of 2

4. You can also check the routing table for each routing domain under **Monitor** > **Statistics** > **Routes**.



Routes for routing domain : Guest

Filter: in Any column Apply

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

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	11.20.20.0/24	*	Local	Default_LAN_Zone	YES	*	Angelina-CFB	Static	-	-	5	318	YES	N/A	N/A
1	11.10.10.0/24	*	DC-Angelina-CFB	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	159	YES	N/A	N/A
3	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
4	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

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

Use Cases

In previous Citrix 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

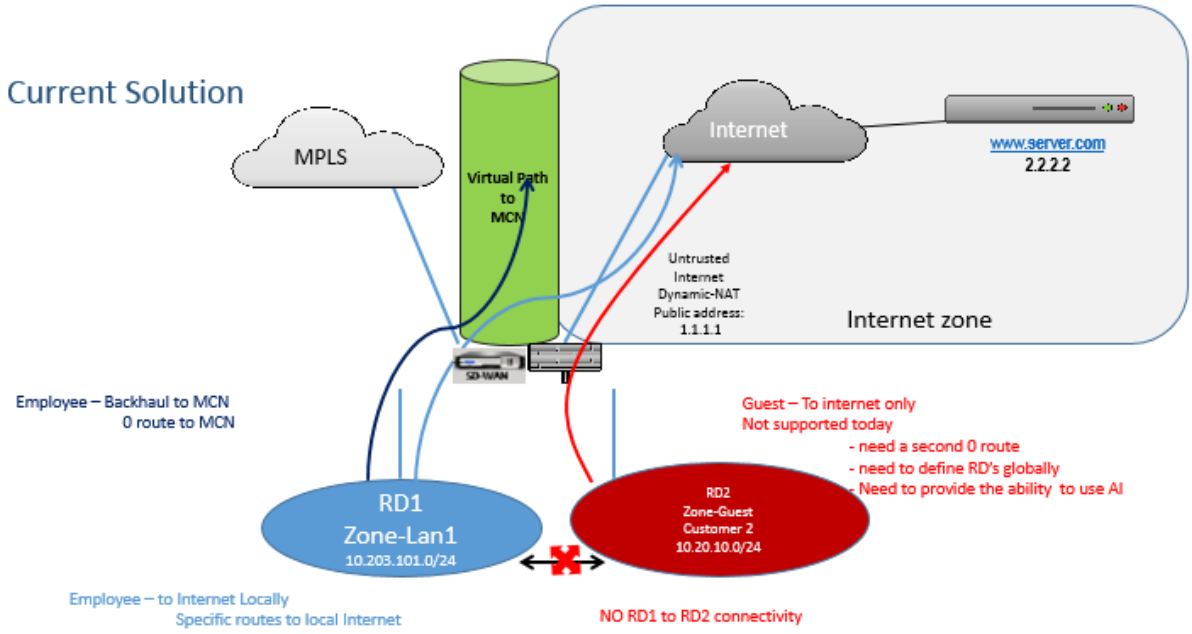
With the Virtual Forwarding and Routing Firewall segmentation enhancements, you can:

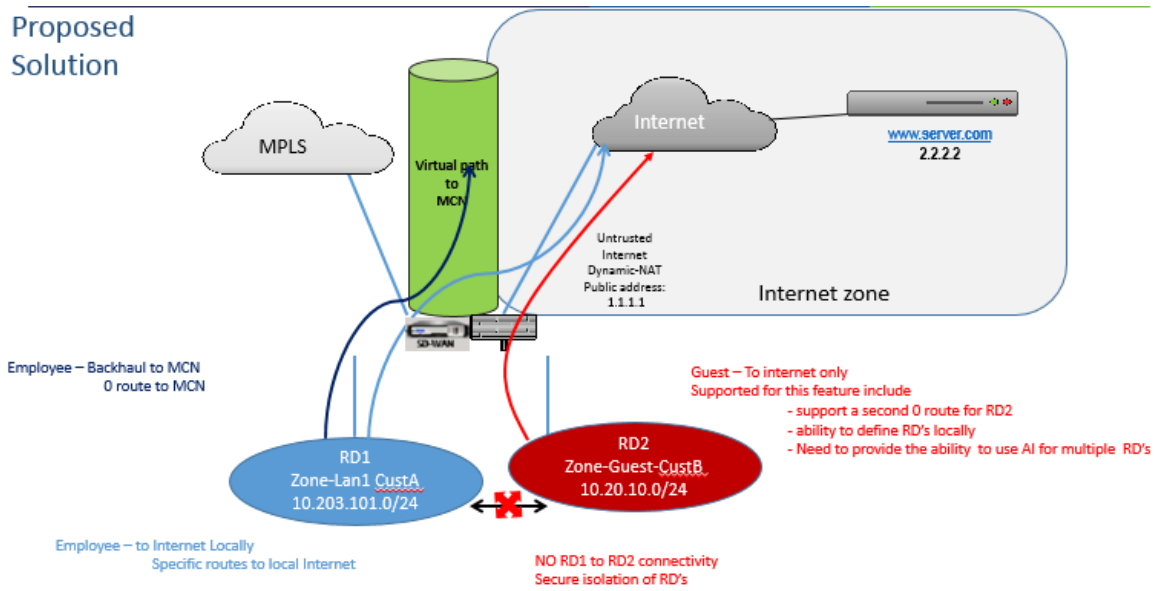
- Provide an infrastructure, at the branch site, that supports secure connectivity for at least two user groups, such as employees and guests. The infrastructure can support up to 16 routing domains.
- Isolate each routing domain's traffic from the traffic of any other routing domain.
- Provide internet 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 necessary
- 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 is assigned a 0.0.0.0 route
- Allows specific routes to be added for an 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**, ensure 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





Limitations

- 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.

Certificate authentication

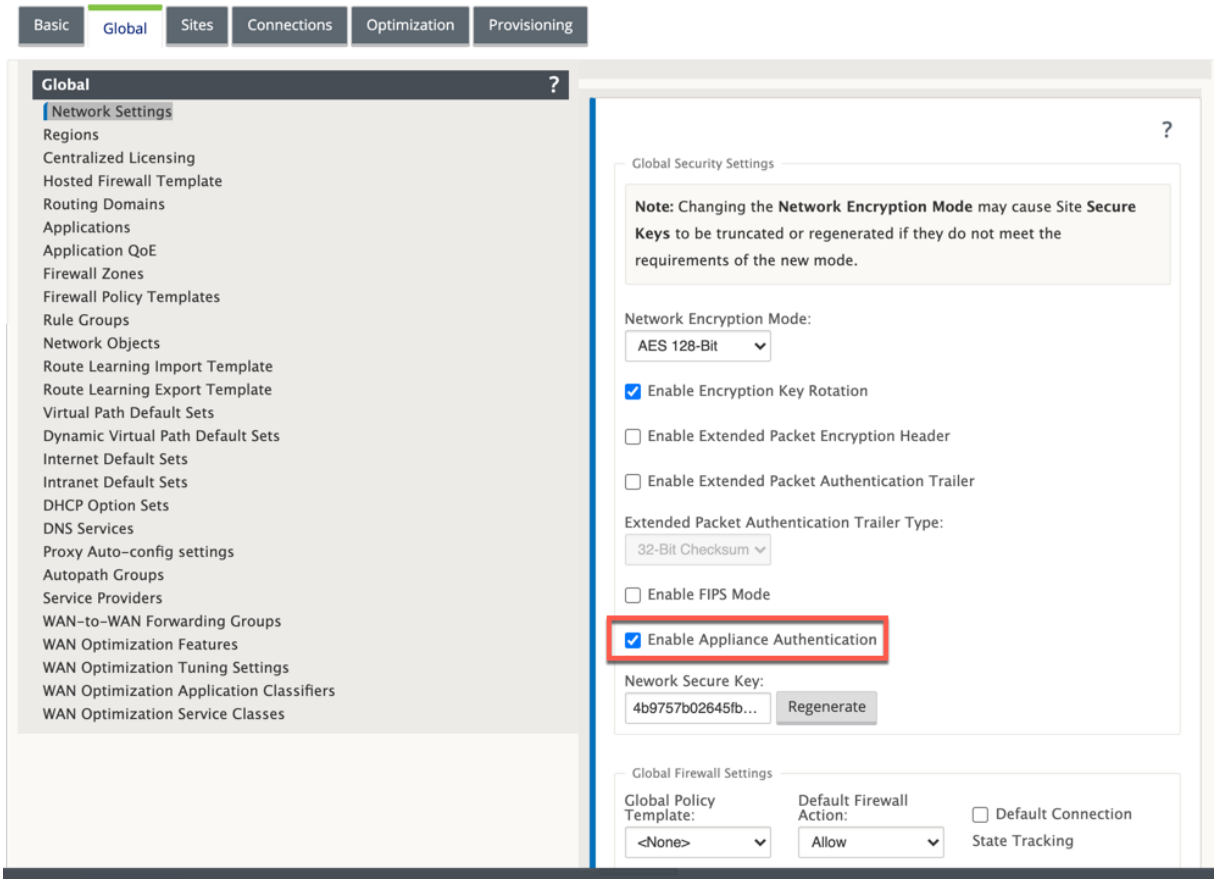
March 12, 2021

Citrix SD-WAN ensures secure paths are established between appliances in the SD-WAN network by using security techniques such as network encryption and virtual path IPsec tunnels. In addition to the existing security measures, certificate based authentication is introduced in Citrix SD-WAN 11.0.2.

Certificate authentication, allows organizations to use certificates issued by their private Certificate Authority (CA) to authenticate appliances. The appliances are authenticated before establishing the virtual paths. For example, if a branch appliance tries to connect to the data center and the certificate from the branch does not match with the certificate that the data center expects, the virtual path is not established.

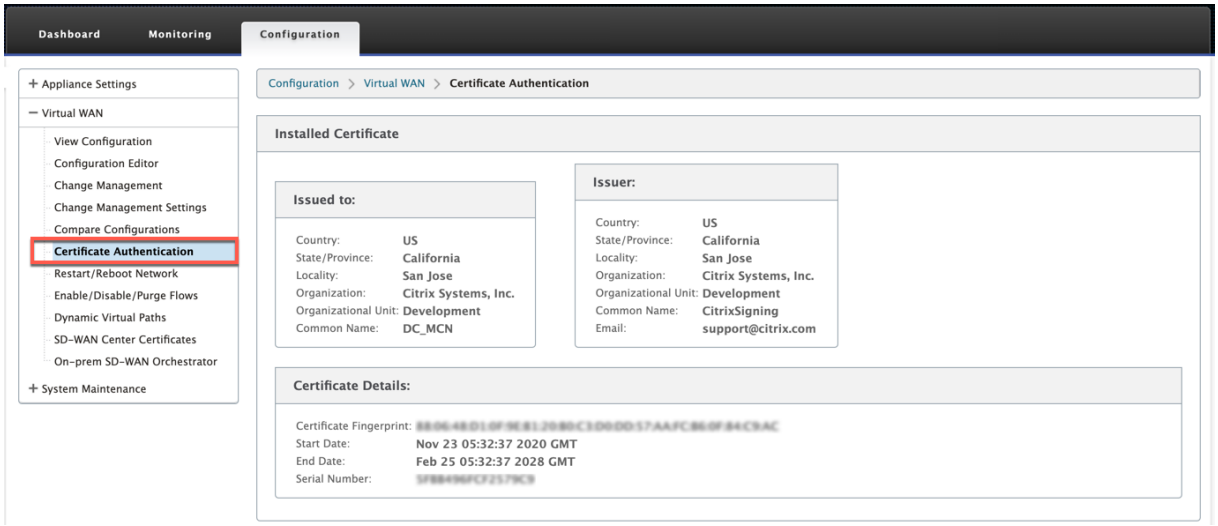
The certificate issued by the CA binds a public key to the name of the appliance. The public key works with the corresponding private key possessed by the appliance identified by the certificate.

To enable appliance authentication, in the configuration editor, navigate to **Global** > **Network Settings** and select **Enable Appliance Authentication**.



After the configuration is staged and applied, a new **Certificate Authentication** option is listed under **Configuration** > **Virtual WAN**.

You can manage all the certificates used for virtual path authentication from the **Certificate Authentication** page.

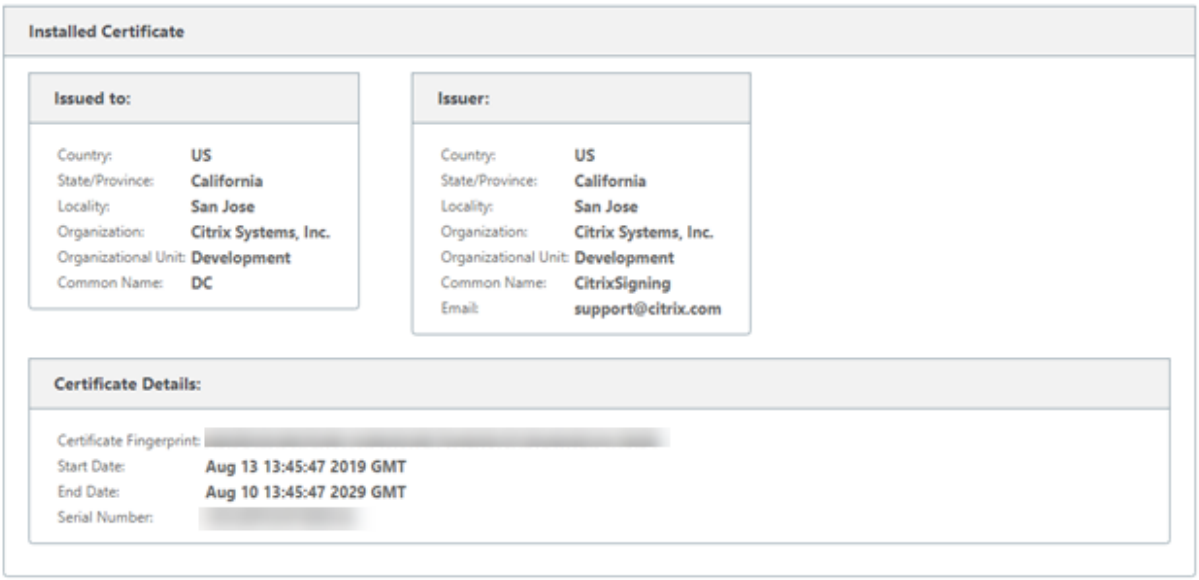


> **Note**
>
> If you are upgrading the appliance software from SD-WAN version 11.0 to version 11.1 or higher, uncheck the **Enable Appliance Authentication** option and perform the software upgrade. Once the upgrade process is completed, select the **Enable Appliance Authentication** option.

Installed certificate

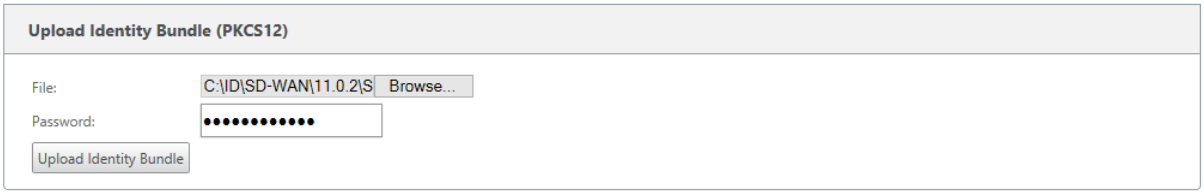
The **Installed Certificate** section provides a summary of the certificate that is installed on the appliance. The appliance uses this certificate to identify itself in the network.

The **Issued to** section provides details about who the certificate was issues to. The **Common Name** in the certificate matches with the name of the appliance, since the certificate is bound to the appliance name. The **Issuer** section provides the details of the certificate signing authority, who signed the certificate. The Certificate details include the fingerprint of the certificate, serial number, and the validity period for the certificate.



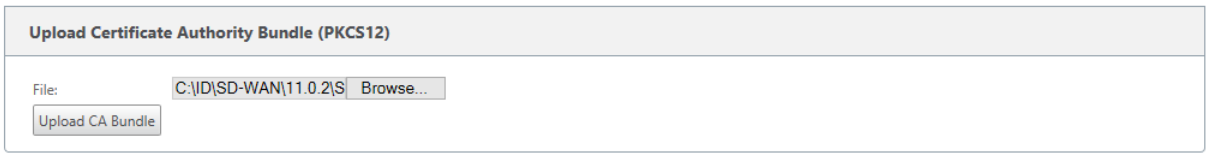
Upload identity bundle

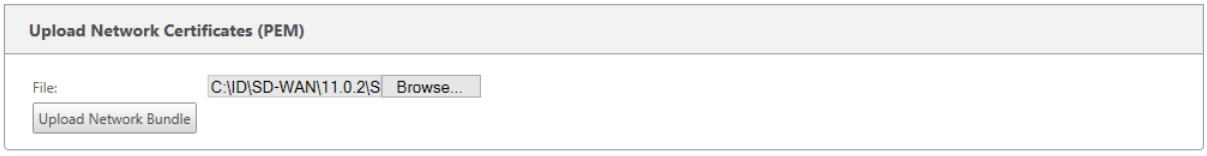
The Identity bundle includes a private key and the certificate associated with the private key. You can upload the appliance certificate issued by the CA into the appliance. The certificate bundle is a PKCS 12 file, with .p12 extension. You can choose to protect it with a password. If you leave the password field blank it is treated as no password protection.



Upload certificate authority bundle

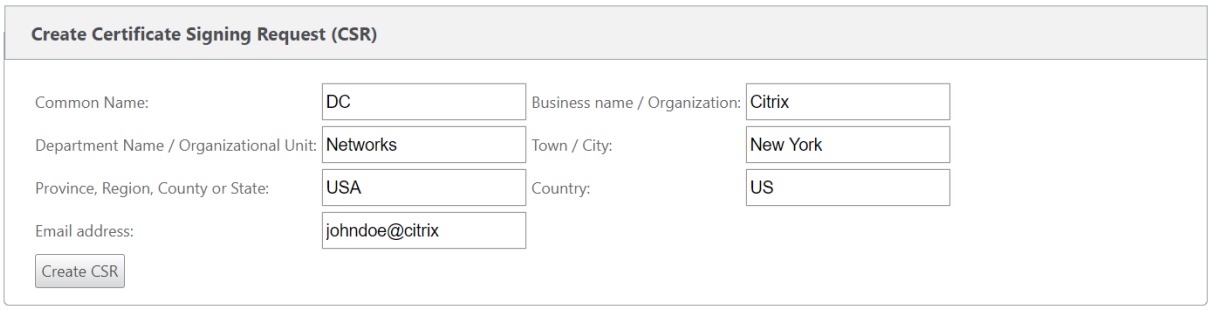
Upload the PKCS 12 bundle that corresponds to the certificate signing authority. The certificate authority bundle includes the complete chain of signatures, the root and all the intermediate signatory authority.





Create certification signing request

The appliance can generate an unsigned certificated and create a Certificate Signing Request (CSR). The CA can then download the CSR from the appliance, sign it and upload it back to the appliance in PEM or DER formats. This is used as an Identity certificate for the appliance. To create a CSR for an appliance, provide the appliance common name, organization details, and address.

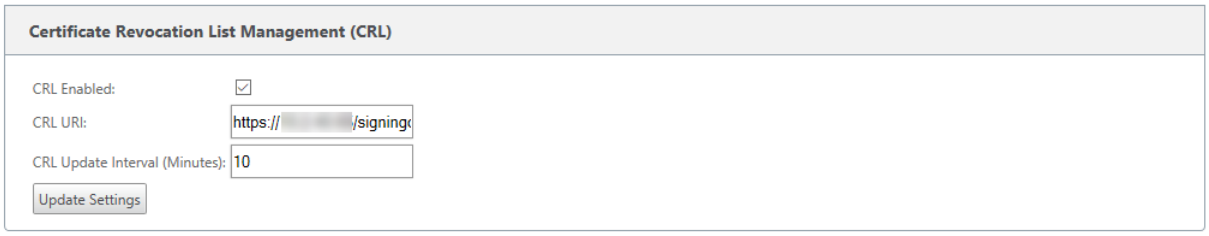


Certificate revocation list manager

A Certificate Revocation List (CRL) is a published list of certificate serial numbers that are no longer valid in the network. The CRL file is periodically downloaded and stored locally on all the appliance.

When a certificate is being authenticated the responder examines the CRL to see if the initiators certificate was revoked already.Citrix SD-WAN currently supports version 1 CRLs in PEM and DER format.

To enable CRL, select the CRL enabled option. Provide the location where the CRL file is maintained. HTTP, HTTPS, and FTP locations are supported. Specify the time interval to check and download the CRL file, the range is 1–1440 minutes.



> **Note**
>
> The reauthentication period for a virtua1 path can be between 10–15 minutes, if the CRL update interval is set to a shorter duration, the updated CRL list may include a currently active serial number. Making an actively revoked certificate available in your network for a short duration.

AppFlow and IPFIX

March 12, 2021

AppFlow and IPFIX are flow export standards used to identify and collect application and transaction data in the network infrastructure. This data gives better visibility into application traffic utilization and performance.

The collected data, called flow records are transmitted to one or more IPv4 collectors. The collectors aggregate the flow records and generate real-time or historical reports.

AppFlow

AppFlow exports flow level data for HDX / ICA connections only. You can enable either the TCP only for HDX dataset template or the HDX dataset template. The TCP only for HDX dataset provides multi-hop data. The HDX dataset provides HDX insight data.

> **Note**
>
> HDX template is available for Citrix SD-WAN PE edition and Two-box appliances only. It should be enabled on the Data Center appliance.

AppFlow Collectors like Splunk and Citrix ADM have dashboards to interpret and present these templates.

IPFIX

IPFIX is a collector export protocol used for exporting flow level data for all connections. For any connection, you can view information such as packet count, byte count, type of service, flow direction, routing domain, application name and so on. IPFIX flows are transmitted through the management interface. Most collectors can receive IPFIX flow records, but may need to build a custom dashboard to interpret IPFIX template.

The IPFIX template defines the order in which the data stream is to be interpreted. The collector receives a template record, followed by the data records. Citrix SD-WAN uses templates 611, 612 and 613 to export IPFIX flow data.

You can choose **Application Flow Info (IPFIX)** to export data sets as per templates 611 and 612. If there are issues exporting the flow data, choose **Basic Properties (IPFIX)** which exports data sets as per template 613.

The following tables provide the detailed list of flow data associated with each IPFIX template.

Application Flow Info (IPFIX) - V10 templates

Template ID - 611

Info Element (IE)	IE name & ID	Type and len	Description
Observation point ID	observationPointId, 138	Unsigned32, 4	
Export process ID	exportingProcessId, 144	Unsigned32, 4	
Flow ID	flowId, 148	Unsigned64, 8	
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
Ipv4 DST IP	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	ipVersion, 60	Unsigned8, 1	
IP protocol number	protocoldentifier,4	Unsigned8, 1	
Padding	N/A	Unsigned16, 2	
SRC Port	sourceTransportPort, 7	Unsigned16, 2	

Info Element (IE)	IE name & ID	Type and len	Description
DST Port	destinationTransportPort, 11	Unsigned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Time for first pkt in microseconds	flowStartMicroseconds, 154	dateTimeMicroseconds, 8	
Time for lastpkt in microseconds	flowEndMicroseconds, 155	dateTimeMicroseconds, 8	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Flags	tcpControlBits, 6	Unsigned8, 2	Currently set to 0.
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Output Interface	egressInterface, 14	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Input Vlan ID	vlanId, 58	Unsigned16, 2	
Output Vlan ID	postVlanId, 59	Unsigned16, 2	
VRF ID	ingressVRFID, 234	Unsigned32, 4	
Flow Key Indicator	flowKeyIndicator, 173	Unsigned64, 8	Set to 0x1E037F.

Info Element (IE)	IE name & ID	Type and len	Description
Application ID	applicationId, 95	octetArray, variable	The Application ID is same as the ID of the applications classified by the DPI engine. The application IDs remain constant. The application IDs for Custom domain name based applications change with every configuration update.

Template 612

Info Element (IE)	IE name & ID	Type	Comment
Application ID	applicationId, 95	octetArray	The Application ID is same as the ID of the applications classified by the DPI engine. The application IDs remain constant. The application IDs for Custom domain name based applications change with every configuration update.
Application Name	applicationName, 96	string	Specifies the name of the Citrix SDWAN specific proprietary application.
Application Description	applicationDescription, 94	string	Specifies the description of the application.

Basic Properties (IPFIX) –V9 compliant template - Template 613

Info Element (IE)	IE name & ID	Type and len	Comment
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
Ipv4 DST IP	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	ipVersion, 60	Unsigned8, 1	
IP protocol number	protocoldentifier,4	Unsigned8, 1	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN
SRC Port	sourceTransportPort, 7	Unsigned16, 2	
DST Port	destinationTransportPort, 11	Unsigned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Output Interface	egressInterface, 14	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Input Vlan ID	vlanId, 58	Unsigned16, 2	
Output Vlan ID	postVlanId, 59	Unsigned16, 2	

Limitations

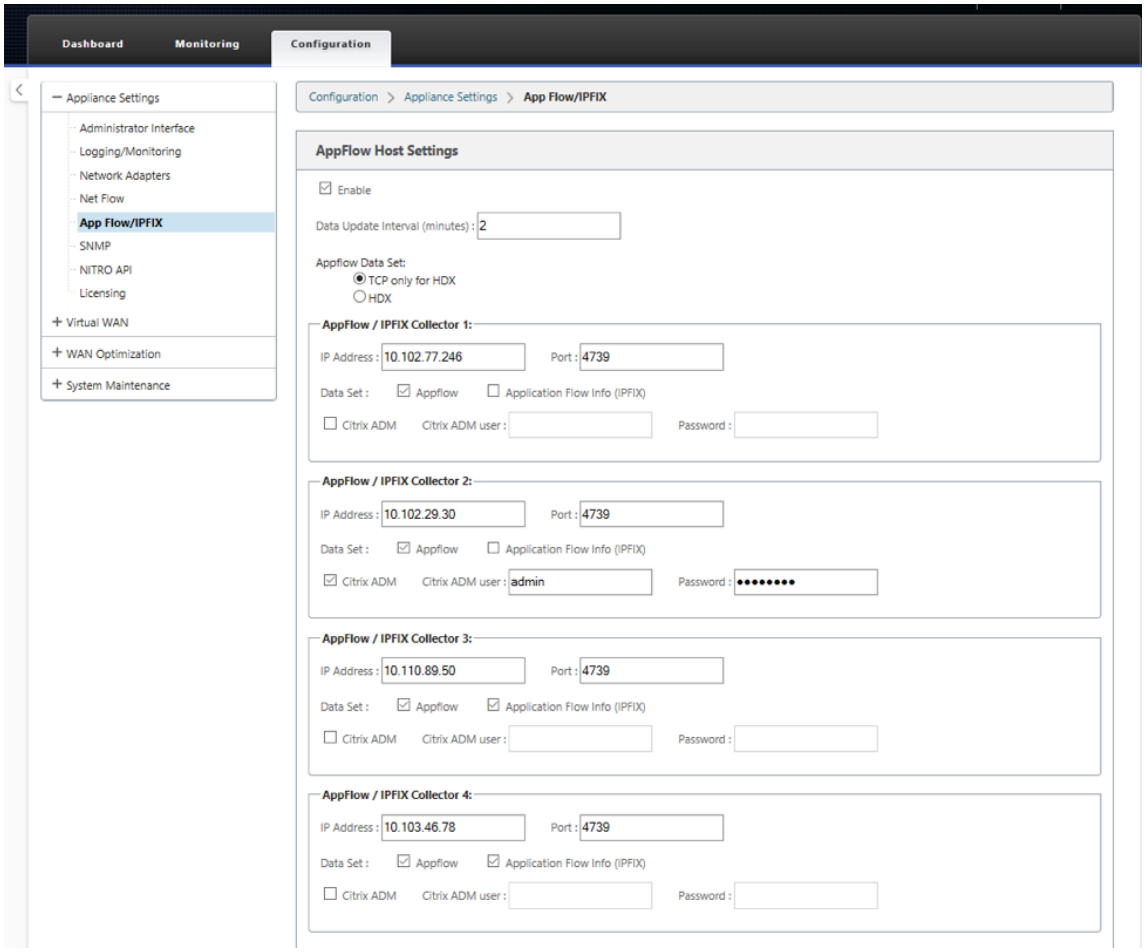
- The export interval for Net Flow is increased from 15 seconds to 60 seconds.
- AppFlow/IPFIX flows are transmitted over UDP, on connection loss not all data is retransmitted. If the export interval is set to X minutes, the appliance stores X minutes of data only. Which is retransmitted after X minutes of connection loss.
- In Citrix SD-WAN, release 10 version 2 the **AppFlow** settings are made local to every appliance, while in the previous releases it was a global setting. If the SD-WAN software release is downgraded to any of the previous releases and if AppFlow is configured on any one of the appliances, it will be applied globally to all alliances.

Configuring AppFlow/IPFIX

You can configure AppFlow / IPFIX on individual SD-WAN appliances or configure it on SD-WAN Center and push the configuration to a group of appliances.

To configure AppFlow / IPFIX on SD-WAN appliances:

1. In Citrix SD-WAN SE/PE web interface, navigate to **Configuration > AppFlow/IPFIX**.
2. Click **Enable**.



3. In the **Data Update Interval** field, specify the time interval, in minutes, at which the flow reports are exported to AppFlow/IPFIX collector. The maximum interval is 10 minutes.
4. Select the **AppFlow dataset** template, you can choose either one of the following dataset templates:
   - **TCP only for HDX (AppFlow)**: The AppFlow dataset template to collect and send multi-hop data of ICA connections to the AppFlow collector.
   - **HDX (AppFlow)**: The AppFlow dataset template to collect and send HDX insight data of ICA connections to AppFlow collector.

   > **Note**
   >
   > **HDX** template is available for Citrix SD-WAN PE and Two Box appliances only.

5. You can configure up to four AppFlow / IPFIX collectors. For each collector specify the following parameters:
   - **IP Address**: The IP Address of the external AppFlow / IPFIX collector system.

- **Port**: The port number on which the external AppFlow / IPFIX collector system listens. The default value is 4739. You can change the port number depending on the collector used.
- **Application Flow Info (IPFIX)**: Sends flow records, as per IPFIX templates 611 and 612, to IPFIX collectors.
- **Basic Properties (IPFIX)**: Sends flow records, as per IPFIX template 613, to IPFIX collectors.
- **Citrix ADM**: Select this to use Citrix ADM as the AppFlow collector.

> **Note**
>
> Citrix ADM currently does not support IPFIX collection.

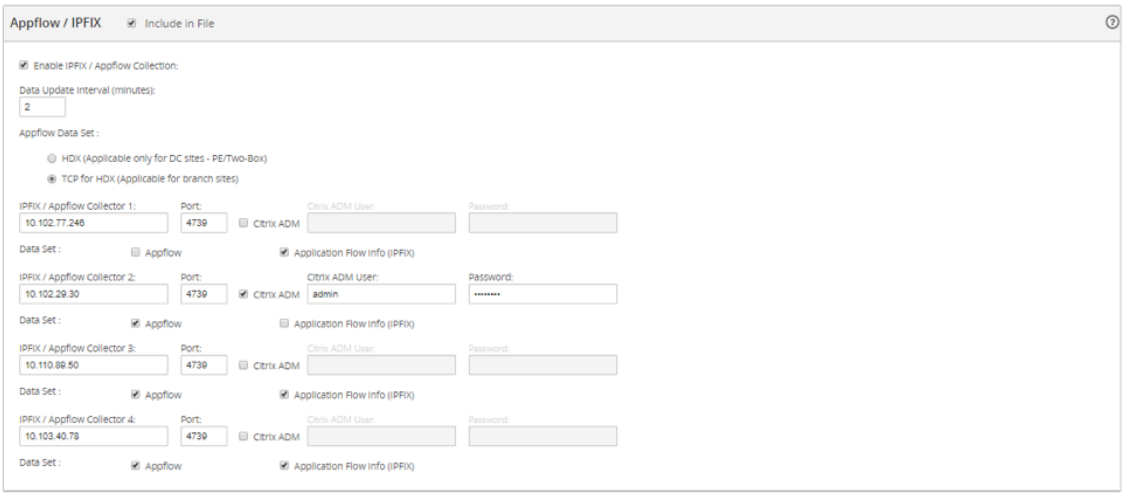
- **Citrix ADM User**: User name of the Citrix ADM collector
- **Password**: Citrix ADM collector password.

The user name and password are used to seamlessly log in into Citrix ADM and store flow data.

6. Click **Apply Settings**.

To configure **AppFlow / IPFIX** collector using Citrix SD-WAN Center:

1. In Citrix SD-WAN Center management UI, navigate to **Configuration > Appliance Settings**.
2. Navigate to the **AppFlow / IPFIX** section and choose **Include in File**.
3. Select **Enable IPFIX / AppFlow Collection**.



4. In the **Data Update Interval** field, specify the time interval, in minutes, at which the AppFlow reports are exported to the AppFlow / IPFIX collector.
5. Select the **AppFlow dataset** template, you can choose either one of the following dataset templates:

- **TCP only for HDX**: The AppFlow dataset template to collect and send multi-hop data of ICA connections to the AppFlow collector.
- **HDX**: The AppFlow dataset template to collect and send HDX insight data of ICA connections to AppFlow collector.

> **Note**
>
> **HDX** template is available for Citrix SD-WAN PE and Two Box appliances only.

6. You can configure up to four AppFlow / IPFIX collectors. For each collector specify the following parameters:

   - **IPFIX / AppFlow Collector**: The IP Address of the external AppFlow / IPFIX collector system.
   - **Port**: The port number on which the external AppFlow / IPFIX collector system listens. The default value is 4739. You can change the port number depending on the collector used.
   - **Application Flow Info**: Sends flow records, as per IPFIX templates 611 and 612, to IPFIX collectors.
   - **Basic Properties (IPFIX)**: Sends flow records, as per IPFIX template 613, to IPFIX collectors.
   - **Citrix ADM**: Select this to use Citrix ADM as the AppFlow collector.

     > **Note**
     >
     > Citrix ADM currently does not support IPFIX collection.

   - **Citrix ADM User**: User name of the Citrix ADM collector.
   - **Password**: Citrix ADM collector password.

     The user name and password are used to seamlessly log in into Citrix ADM and store flow data.

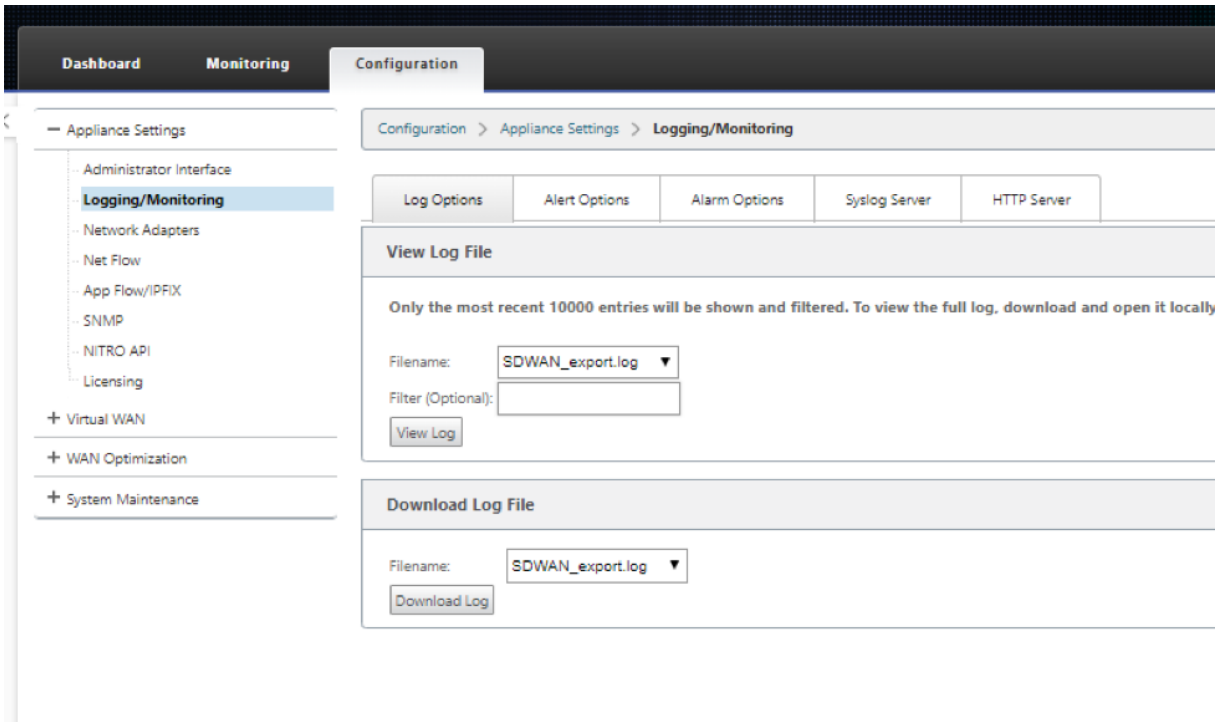
7. **Save** and **Export** the configuration to the managed appliances.

> **Note**
>
> If SD-WAN Center version is lower than 10.2 and SD-WAN appliances version is 10.2 and above then you can observe the following conditions.
>
> - If local collectors are enabled on the appliances, the AppFlow / IPFIX configuration pushed from SD-WAN center does not affect the existing configuration.
> - If local collectors are not enabled on the appliances, the AppFlow/IPFIX configuration pushed from SD-WAN center will be applied to the appliance.

> - If the global AppFlow/IPFIX configuration is enabled in SD-WAN Center configuration, all the local collectors are enabled on the appliances.

Log files

For troubleshooting issues related to AppFlow / IPFIX export protocols, you can view and download the SDWAN_export.log files. Navigate to **Configuration > Logging / Monitoring** and select the **SD-WAN_export.log** files.



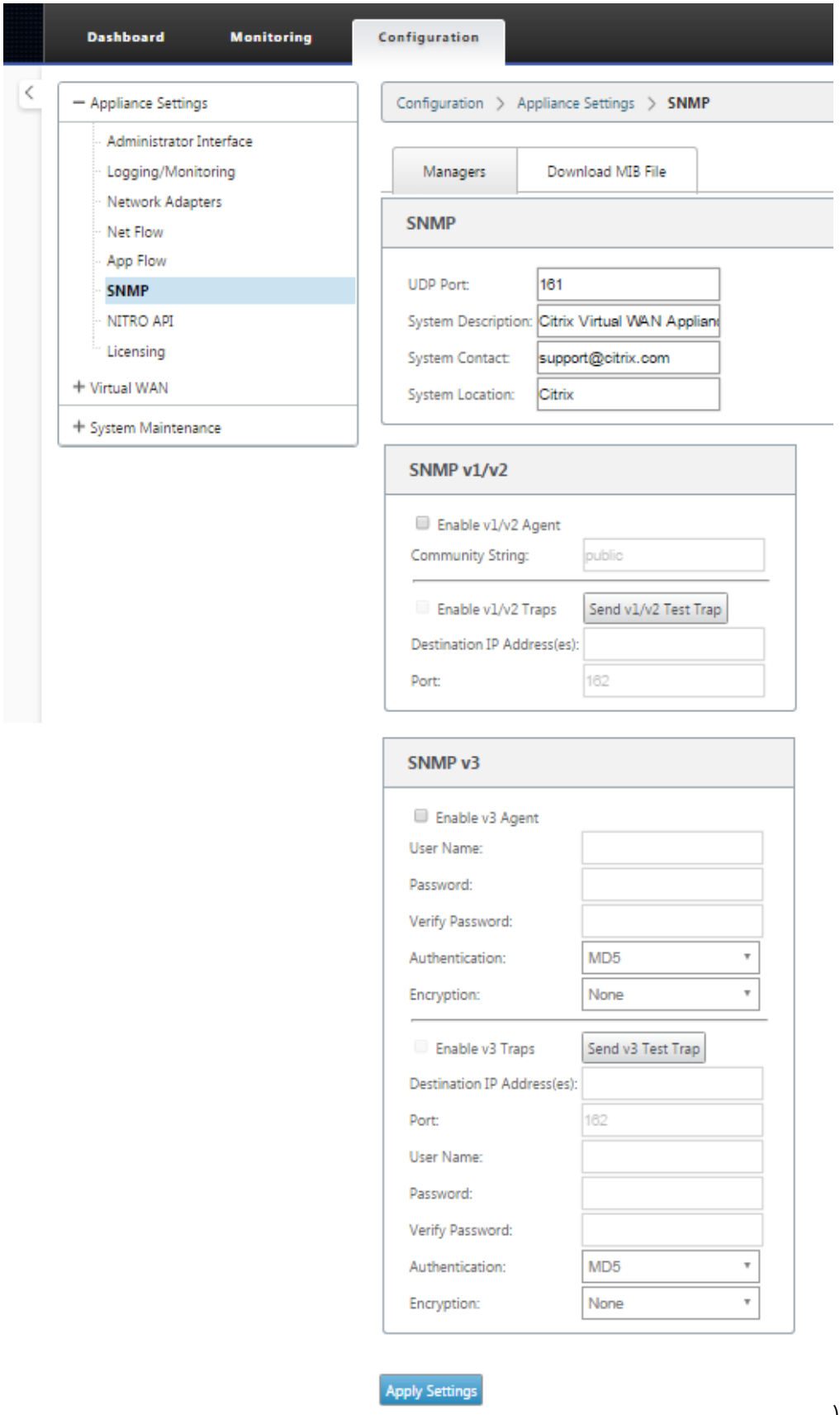
SNMP

March 12, 2021

Citrix 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.



)

Standard MIB Support

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.mib
RFC1213-MIB	https://www.ietf.org/rfc/rfc1213.txt
SNMPv2-MIB	https://www.ietf.org/rfc/rfc3418.txt
TCP-MIB	https://www.ietf.org/rfc/rfc4022.txt
P-BRIDGE-MIB.txt	http://www.icir.org/fenner/mibs/extracted/P-BRIDGE-MIB-rfc2674.txt
RMON2-MIB.txt	https://www.ietf.org/rfc/rfc3273.txt
TOKEN-RING-RMON-MIB.txt	http://www.icir.org/fenner/mibs/extracted/TOKEN-RING-RMON-MIB-rmonmib-01.txt

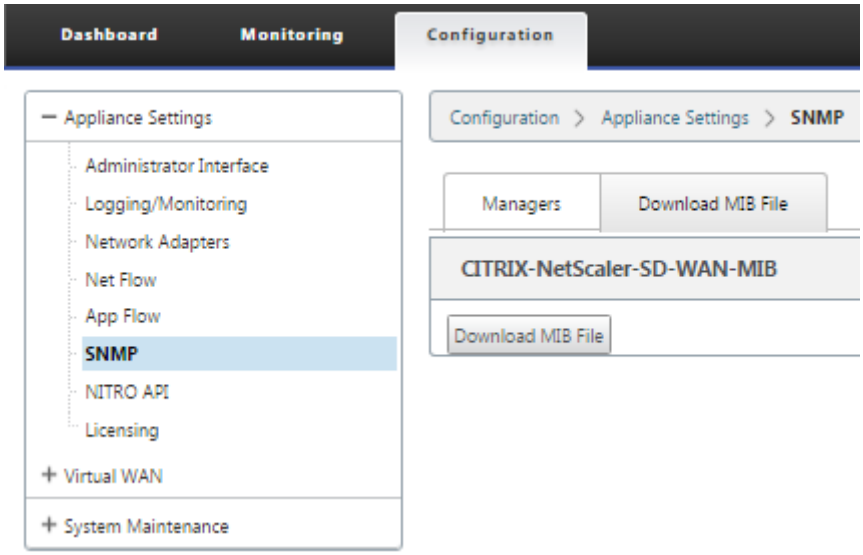
You must download the following SNMP files before you can start monitoring a Citrix SD-WAN appliance:

- 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 provide 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 must 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: CloudBridge

WAN optimization

March 12, 2021

The Citrix SD-WAN WANOP appliance optimizes WAN links, ensuring maximum responsiveness and throughput. The Citrix 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 Citrix SD-WAN WANOP:

- Compression
- TCP Protocol Acceleration
- Traffic Management
- Application Acceleration
- Citrix XenApp/XenDesktop (HDX) Acceleration
- Integration
- Monitoring and Management

For information about Citrix SD-WAN WANOP 10.2 installation, deployment, and feature configuration, please refer to the Citrix SD-WAN WANOP documentation. The features and procedures for the Citrix SD-WAN WANOP 10.2 are similar to the procedures documented in the Citrix SD-WAN WANOP release.

You can enable and configure WAN optimization feature on your Citrix SD-WAN Premium Edition. For more information, see Citrix SD-WAN Premium 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.

Citrix SD-WAN premium edition

March 12, 2021

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

> **Note**
>
> You must have an SD-WAN Premium (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 (premium edition) and 2000-EE (premium edition) 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 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.

Enable optimization and configure the default feature settings

March 12, 2021

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:

   a) If necessary, log back into the Management Web Interface, and open the **Configuration Editor.**

      To open the **Configuration Editor**, do the following:

      i. Select the **Configuration** tab at the top of the page to open the **Configuration** navigation tree (left pane).

      ii. In the navigation tree, click **+** to the left of the **Virtual WAN** branch to open that branch.

      iii. In the **Virtual WAN** branch, select **Configuration Editor.**

   b) 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 is available in the **Configuration Editor**.

      > **Note**
      >
      > If the **Optimization** section is not available, check that you have installed an SD-WAN

> Premium (Enterprise) Edition license in your Virtual WAN. SD-WAN Standard Edition does not support WAN Optimization features.

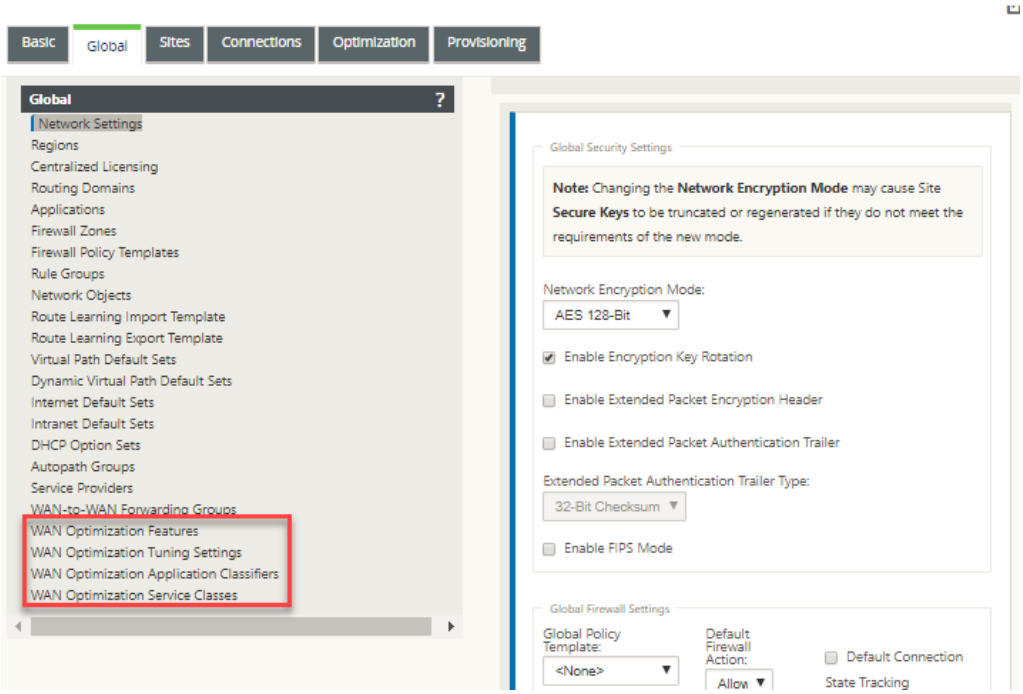
For details and instructions, see the following sections:

- The SD-WAN Editions
- Licensing

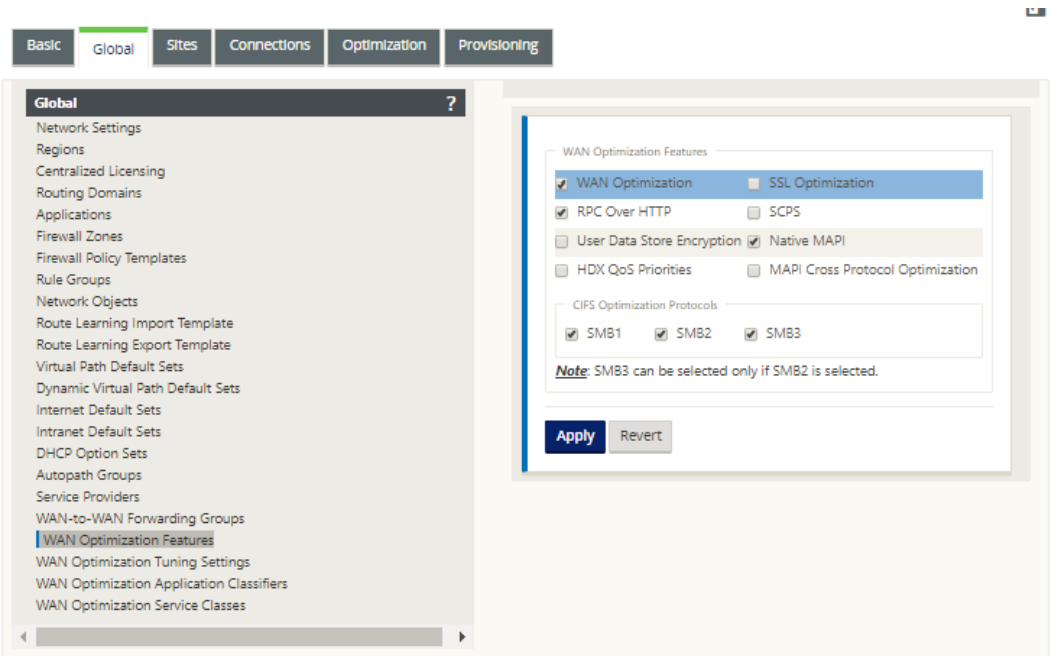
c) Click the **Global** tab.

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



d) Click **WAN Optimization Features**.



e) Select the **WAN Optimization** check box.

The **WAN Optimization** check box 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.

f) Configure the **Features** settings.

Click a check box to select or deselect an option. You can accept the default settings preselected 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 the check box 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 the check box to enable TCP Protocol optimization for Satellite Links.
- **HDX QoS Priorities** –Select the check box to enable optimization of ICA traffic based on prioritization of HDX subchannels.
- **MAPI Cross Protocol Optimization** –Select the check box to enable cross-protocol optimization of Microsoft Outlook (MAPI) traffic.
- **SSL Optimization** –Select the check box to enable optimization for traffic streams with SSL encryption.
- **RPC Over HTTP** – Select the check box to enable optimization of Microsoft Exchange traffic that uses RPC over HTTP.
- **User Data Store Encryption** – Select the check box to enable enhanced security of data through the encryption of WAN Optimization compression history.
- **Native MAPI** –Select the check box to enable optimization of Microsoft Exchange traffic.

  The **CIFS Optimization Protocols** options are as follows:

  - **SMB1** –Select the check box to enable Optimization of Windows File Sharing (SMB1)
  - **SMB2** –Select the check box to enable Optimization of Windows File Sharing (SMB2)
  - **SMB3** –Select the check box to enable Optimization of Windows File Sharing (SMB3). You must first select the **SMB2** option before you can select **SMB3**.

g) Click **Apply** to enable and add the selected **Default Features** to the configuration package.

The next step is to configure the **Optimization** default **Tuning Settings**.

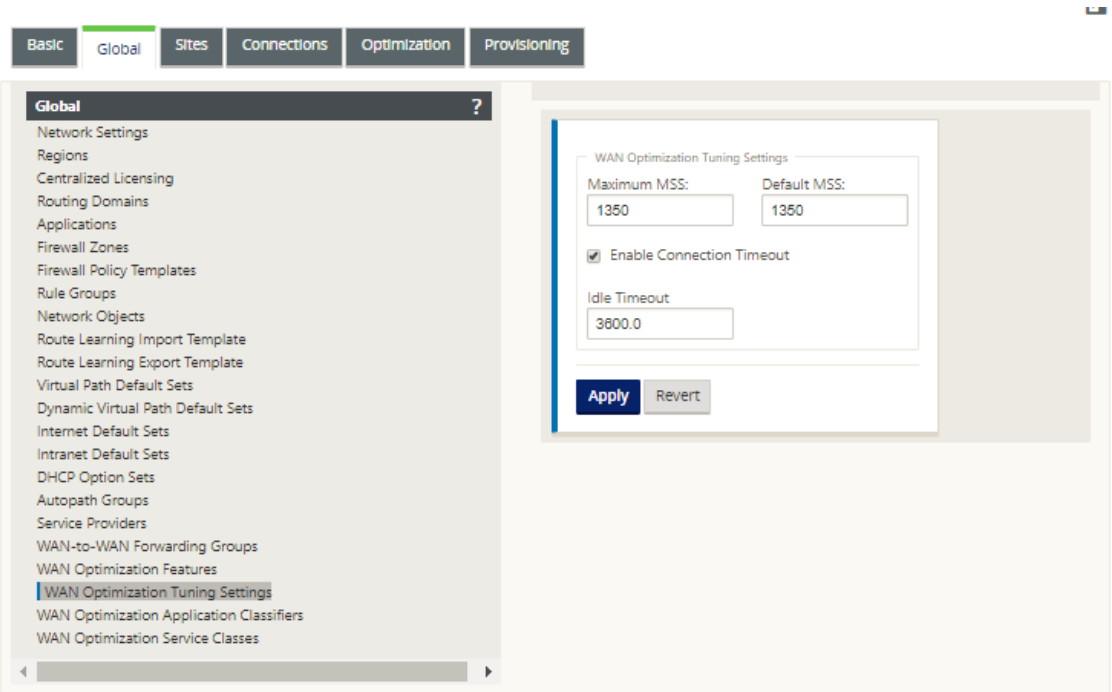
Configure optimization default tuning settings

March 12, 2021

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.

Configure optimization default application classifiers

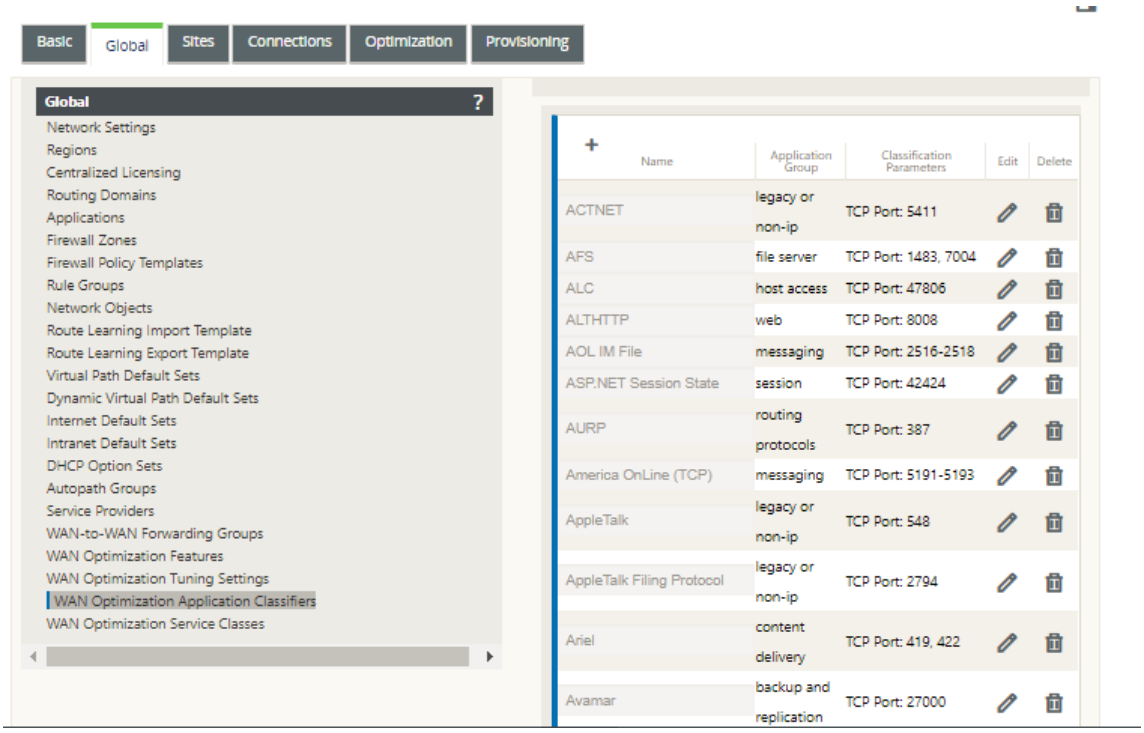
March 12, 2021

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.



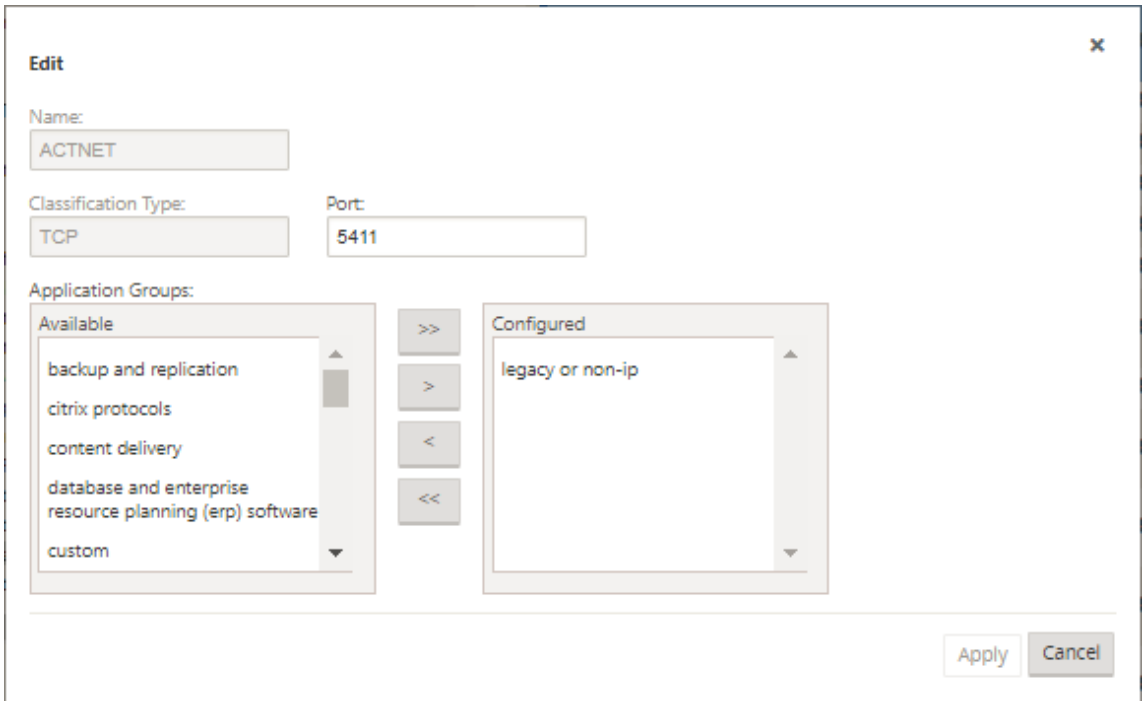
   This table is also a configuration form. You can use this form to configure (edit), delete, and add Application Classifiers to create a customized default set. The modified default **Application**

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.

Configure optimization default service classes

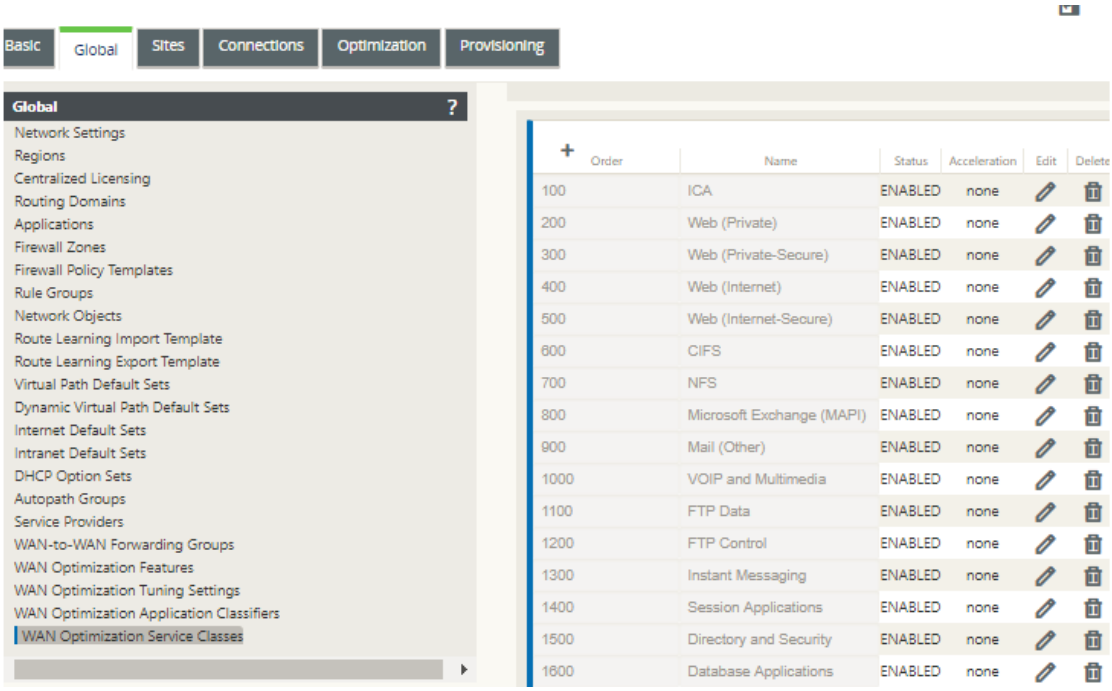
March 12, 2021

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.

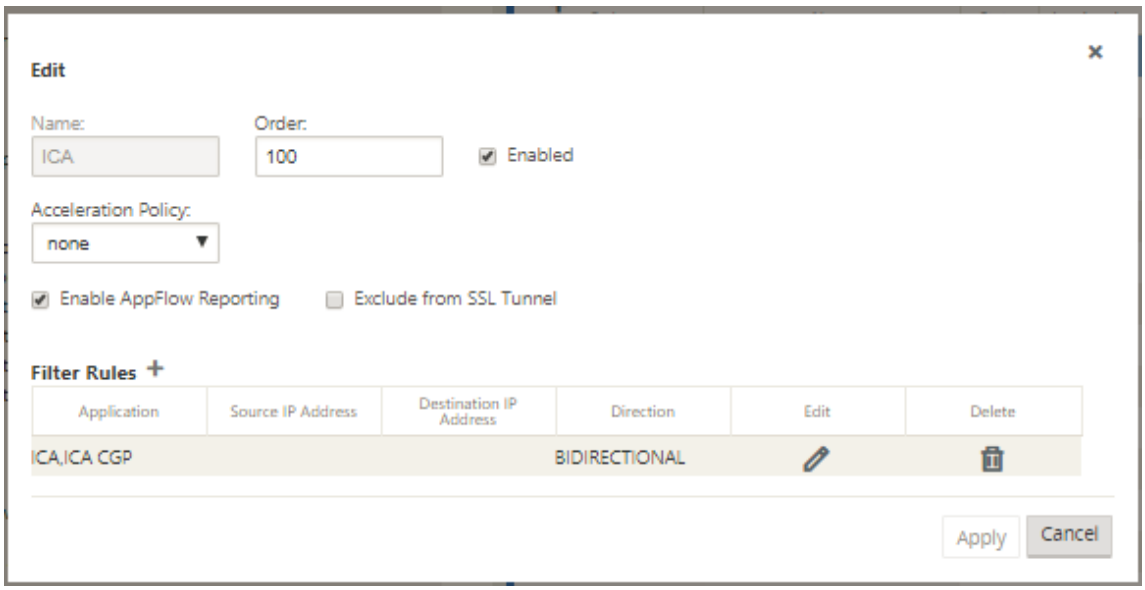


   This table is also a configuration form. You can use this form to configure (edit), delete, and add Service Classes to create a customized default set. The modified default **Service Classes** set and individual Service Class settings you configure are automatically applied as the defaults to any branch 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



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.

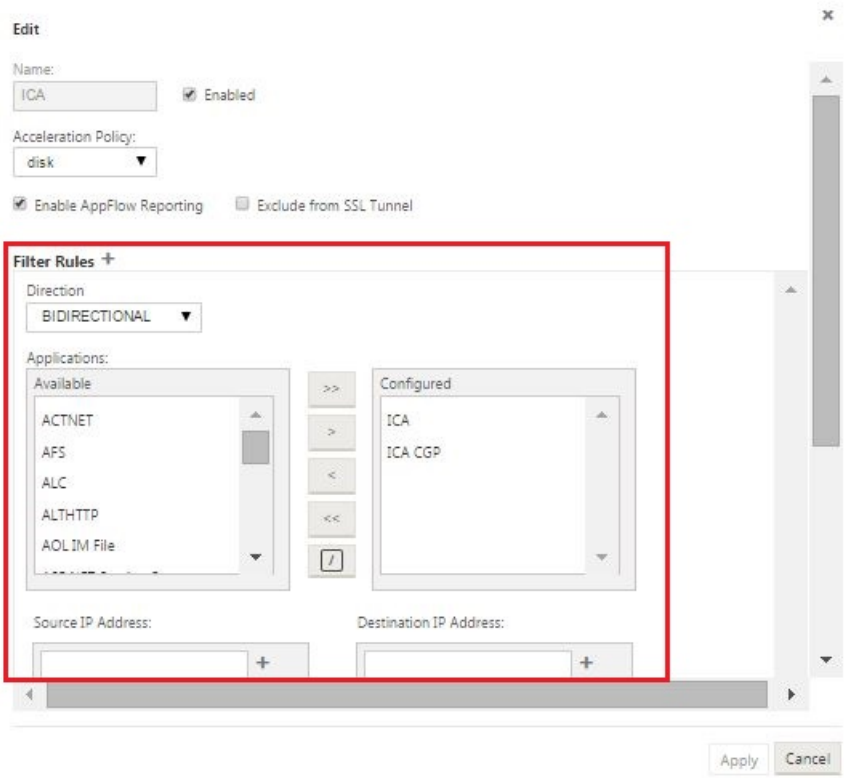
- **Exclude from the SSL Tunnel** –Select this to exclude traffic associated with the Service Class from SSL Tunneling.

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.



   b) Select the filter direction from the Direction drop-down menu.

      Select one of the following options:

      - **BIDIRECTIONAL**

- **UNIDIRECTIONAL**

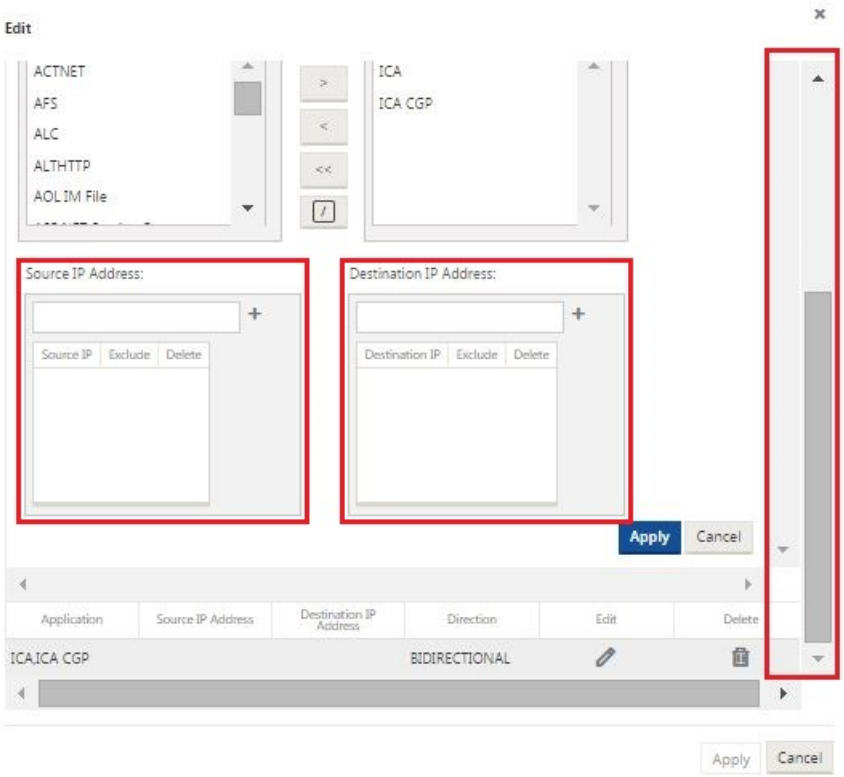
c) Add or remove Applications in the **Configured** list.

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.

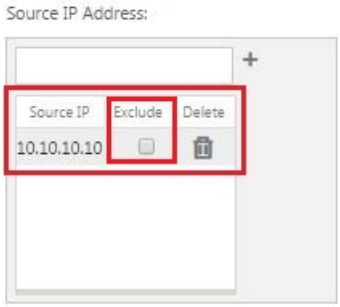
The **Filter Rules** settings section is somewhat long, so you will need to use the scroll bars to reveal the truncated portion of the form.



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.



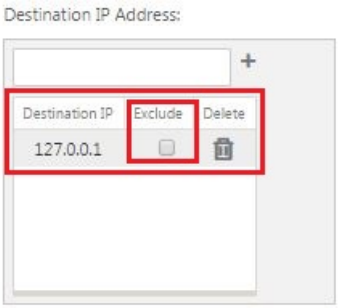
g) Specify whether to include or exclude the Source IP Address for this Filter Rule.

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.

Configure optimization for a Branch Site

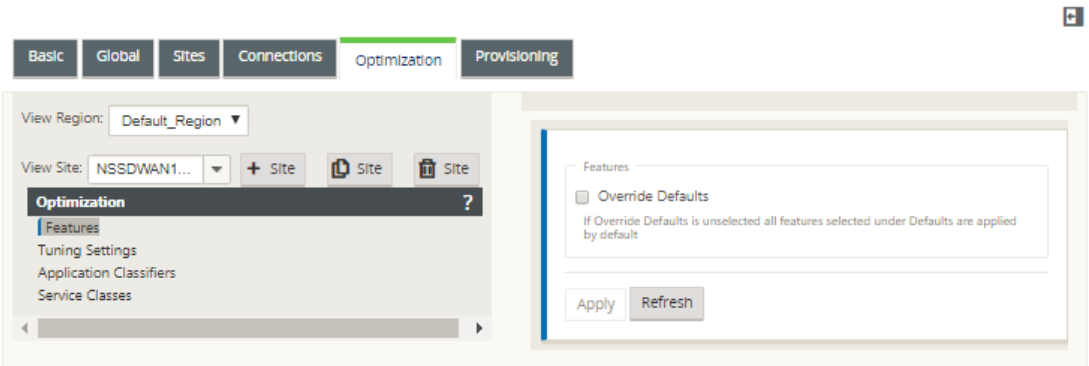
March 12, 2021

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:

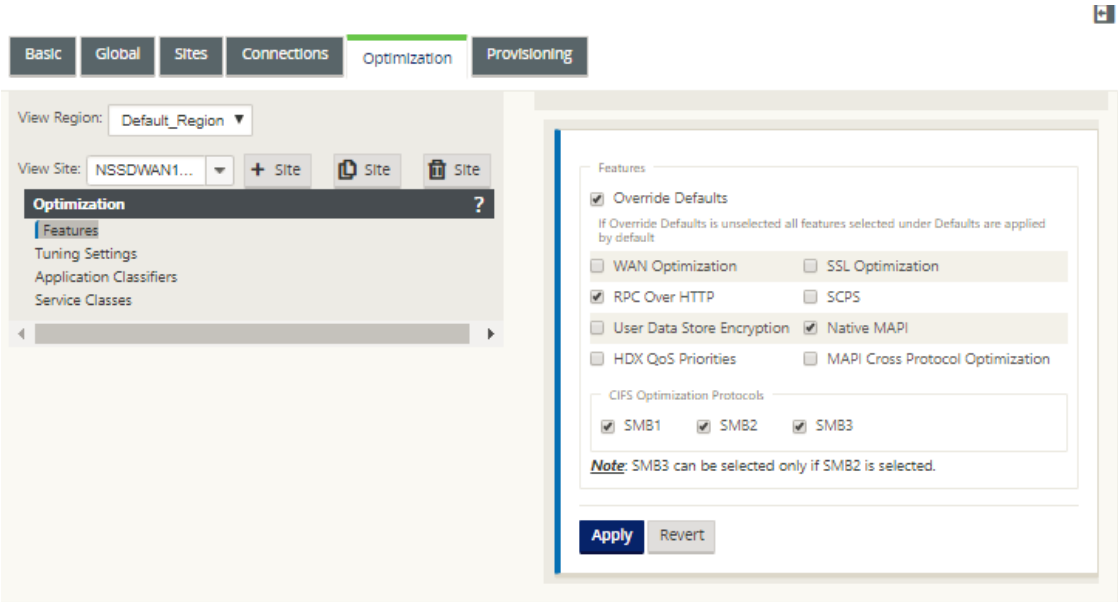
1. Click **Optimization** tab, in the View Site field, select a site.



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.

4. (Optional, recommended) **Save** the configuration package.

   You have now completed configuring the **Optimization** section sets and settings for your Virtual WAN.

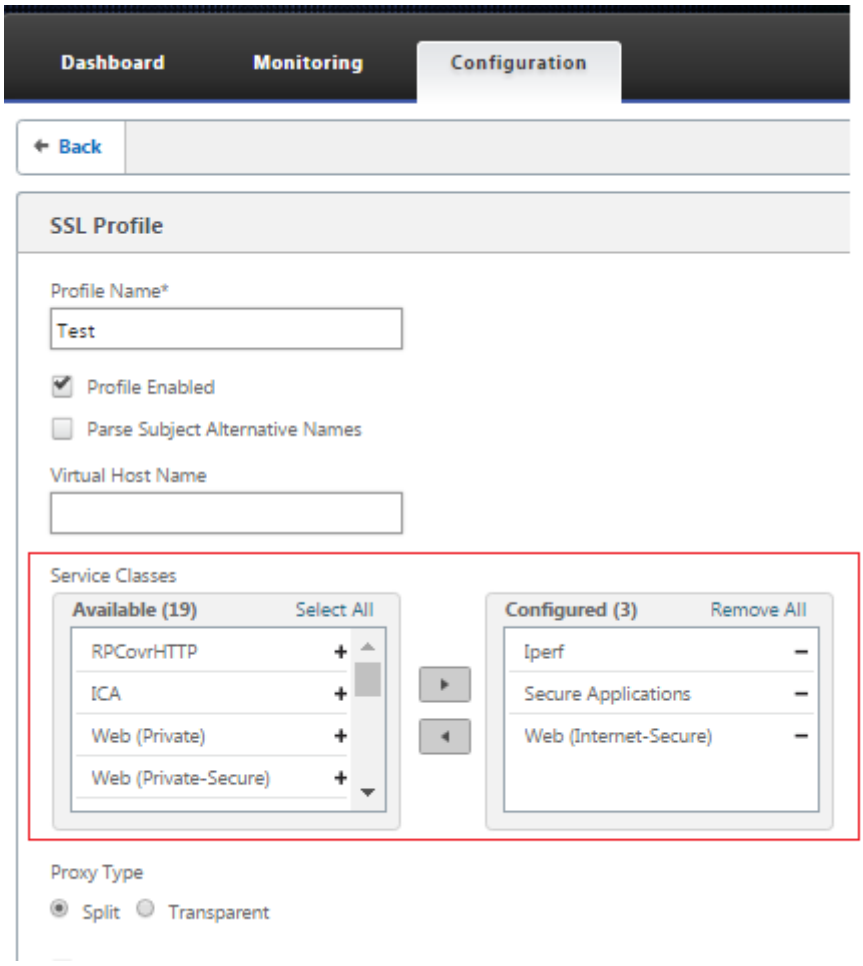
Configure SSL profiles

March 12, 2021

All SSL related configuration is available through the new configuration editor of the appliance for security and usability. On the SD-WAN Premium (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.

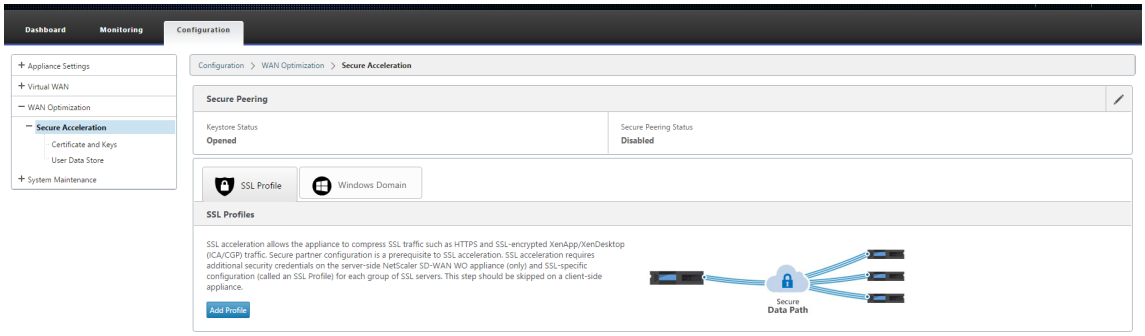
One of the limitations is that the SSL profile will get attached to all rules in a service class. If you need to attach the SSL profile selectively to a particular rule, the service class configuration is split into detailed rules for further selection.

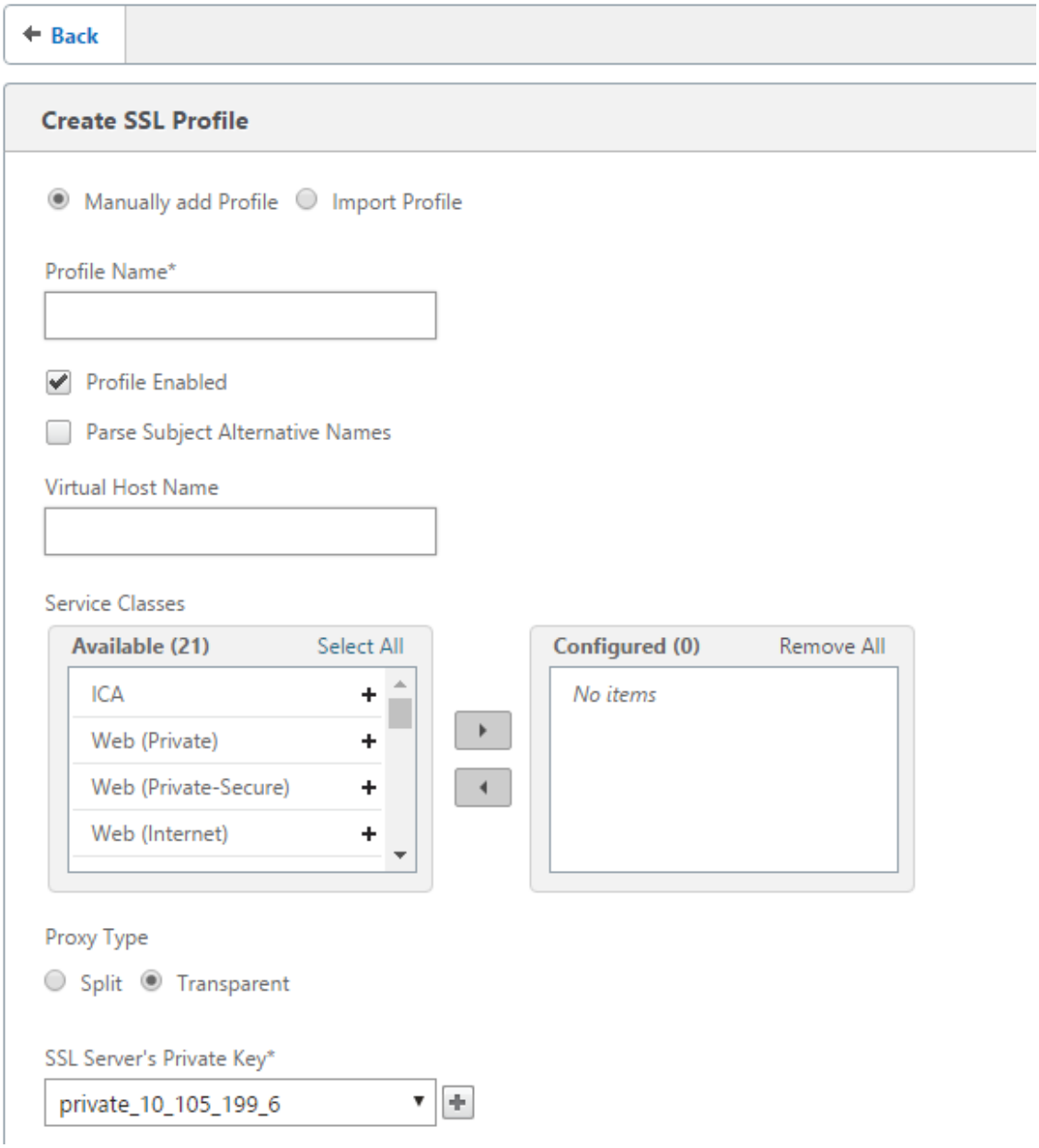
> **Note**
>
> Only the service classes that have their filter rules direction set to unidirectional can be associated with SSL profiles.



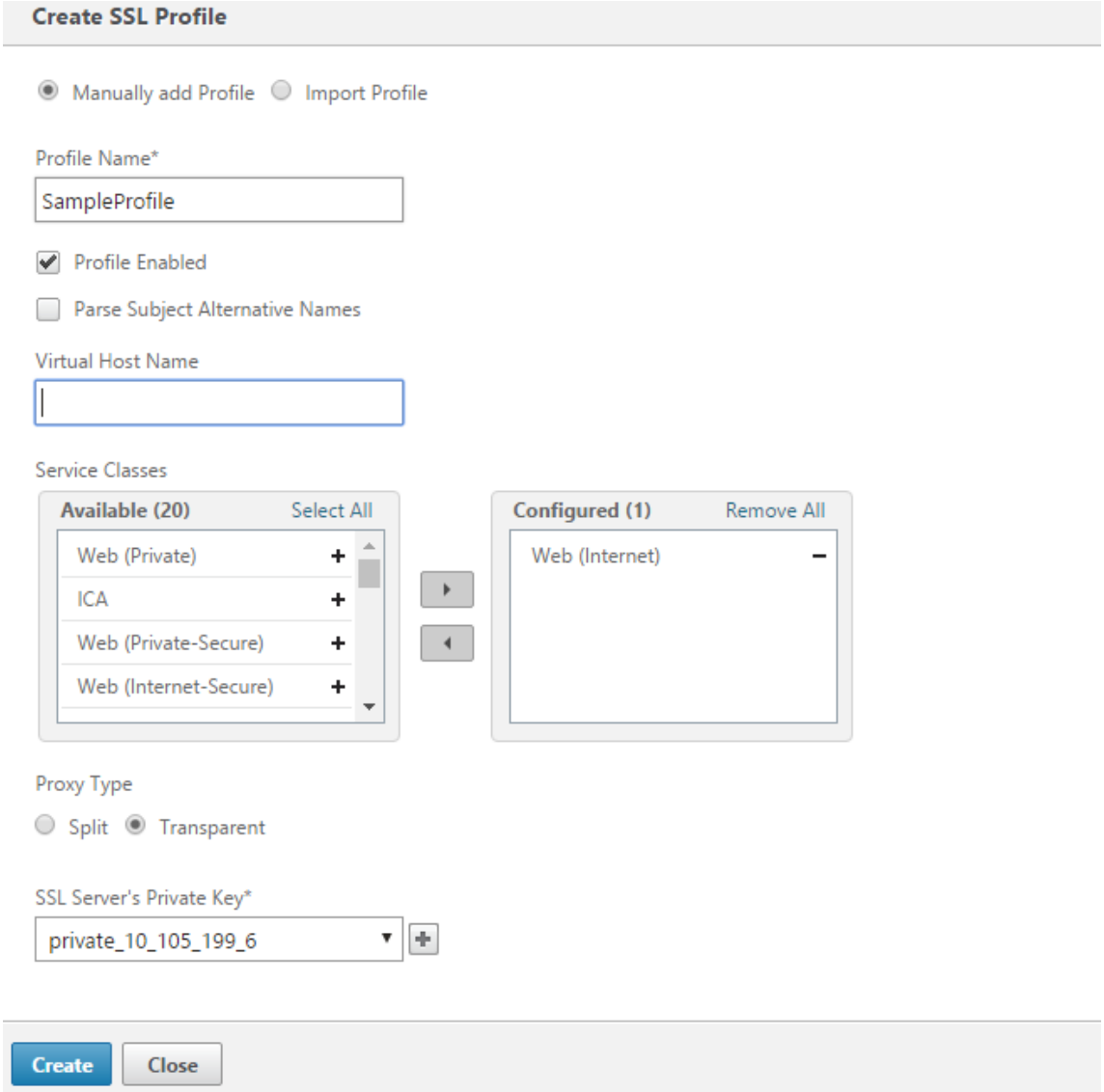
To create SSL profile on new Premium (Enterprise) Edition appliance at the data center:

1. In the SD-WAN web GUI, go to the **Configuration** > **Secure Acceleration** page. Click **Add Profile**. Create the **SSL Profile**.

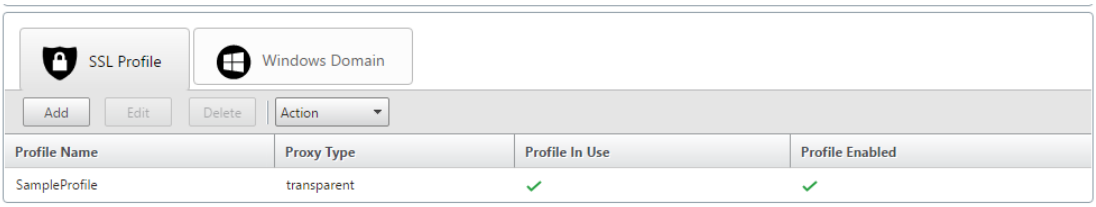




2. In the **Create SSL Profile** page, provide a profile name and select **Service Classes** that will be associated to this profile. Choose **Proxy Type** and provide relevant data and click **Create**.



3. After SSL Profile is created successfully and service class is associated, view the SSL profile information as shown below.



Citrix WAN optimization client plug-in

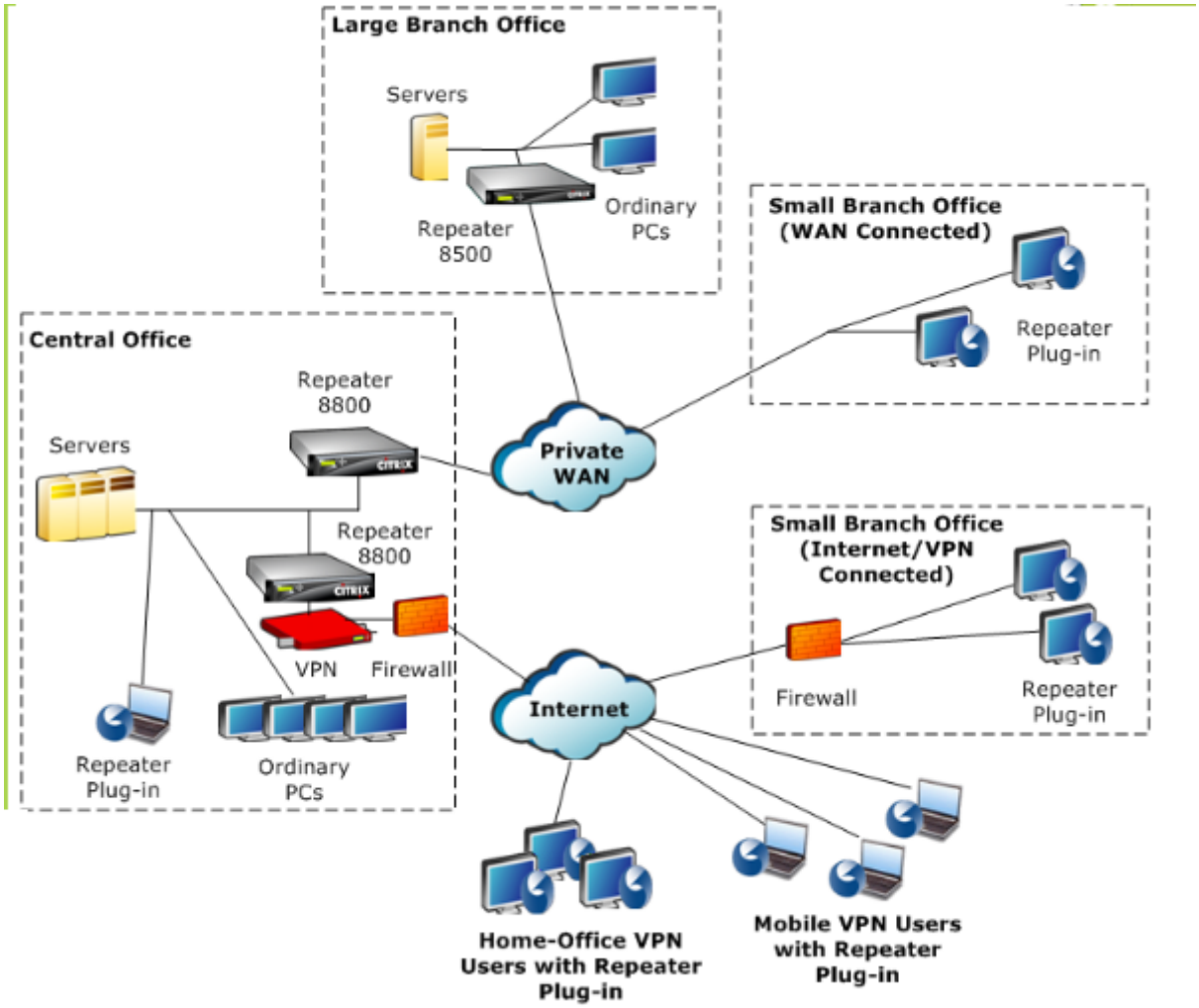
March 12, 2021

The Citrix 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

March 12, 2021

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 Premium (Enterprise) Edition)
- Windows 10 (32-bit and 64-bit versions of Premium (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

March 12, 2021

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).

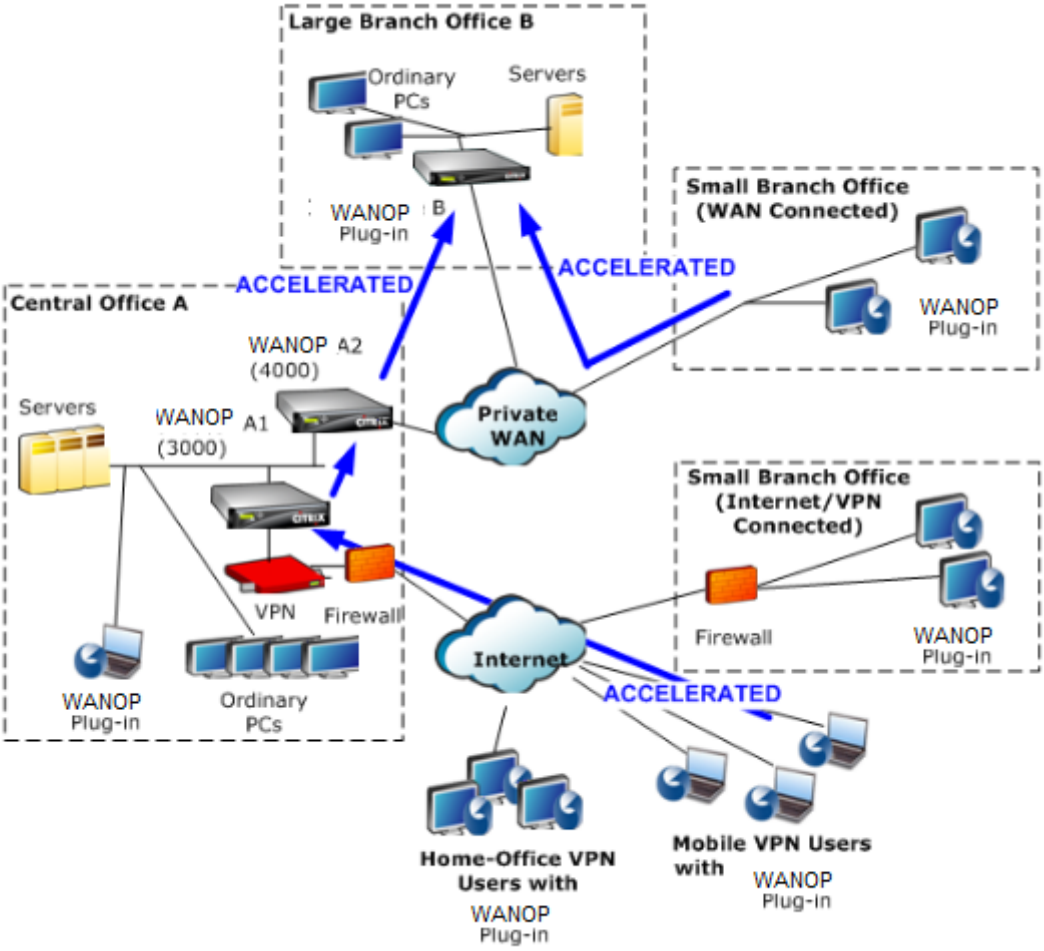
  Best Practice: Use transparent mode when you can, and redirector mode when you must.

Transparent mode

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.

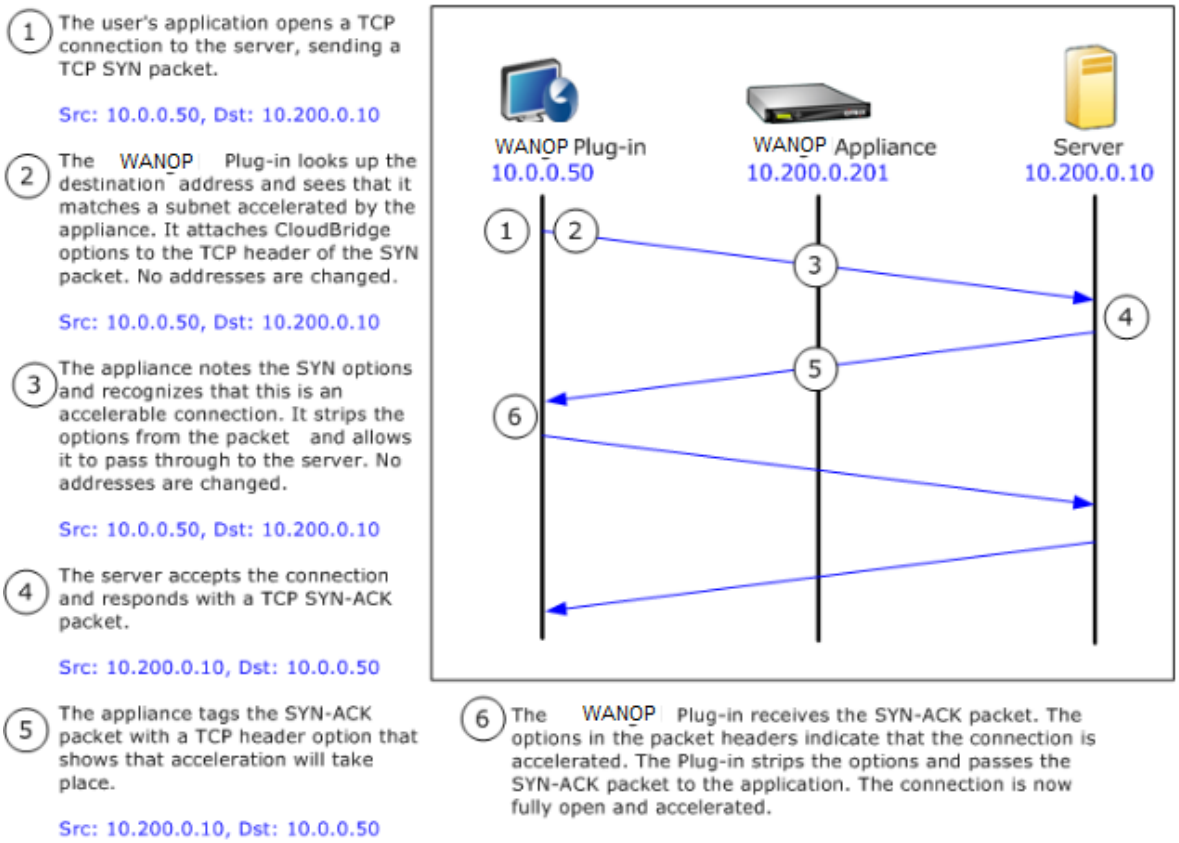
Transparent mode resembles appliance-to-appliance acceleration but is not identical to it. The differences are:

- 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



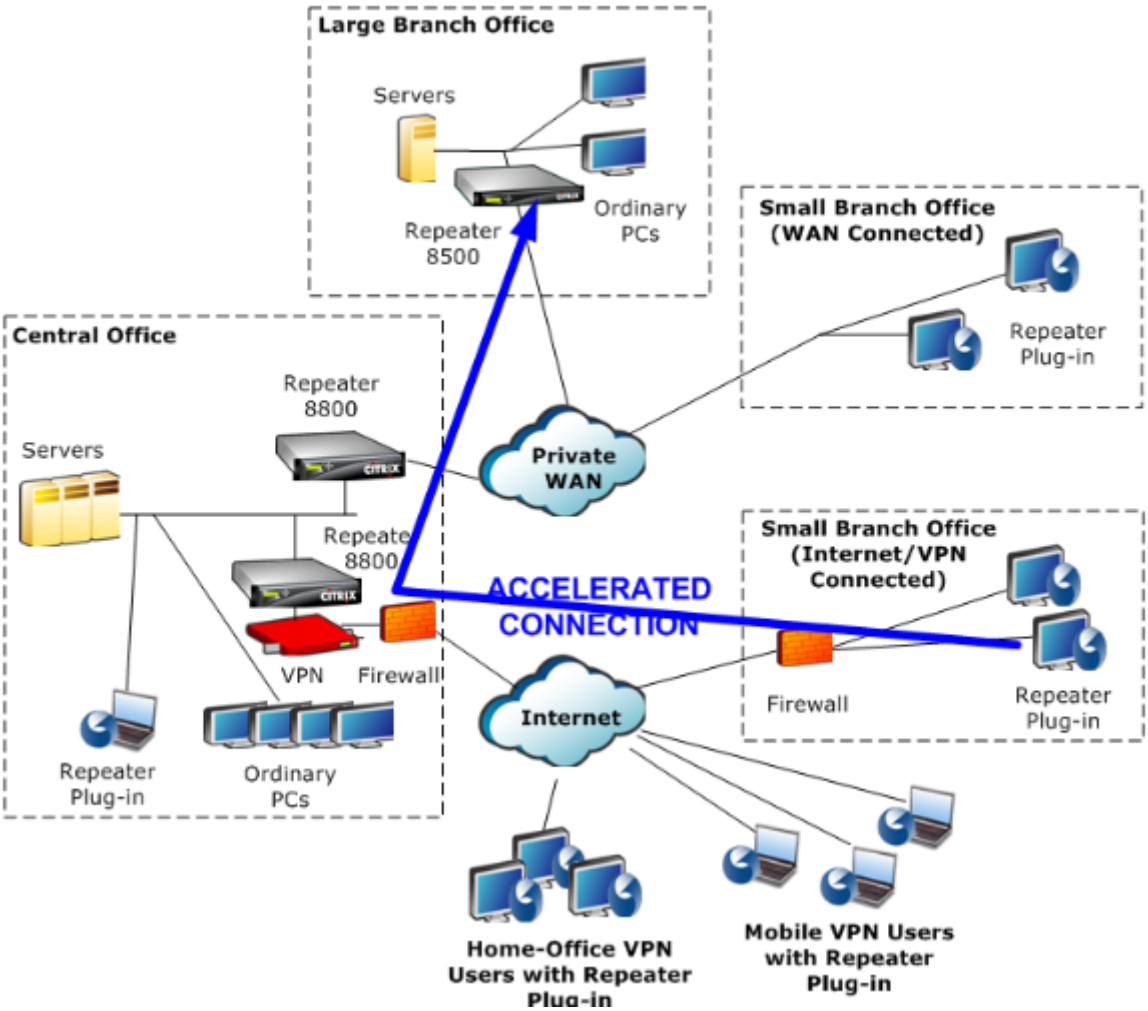
Redirector mode

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

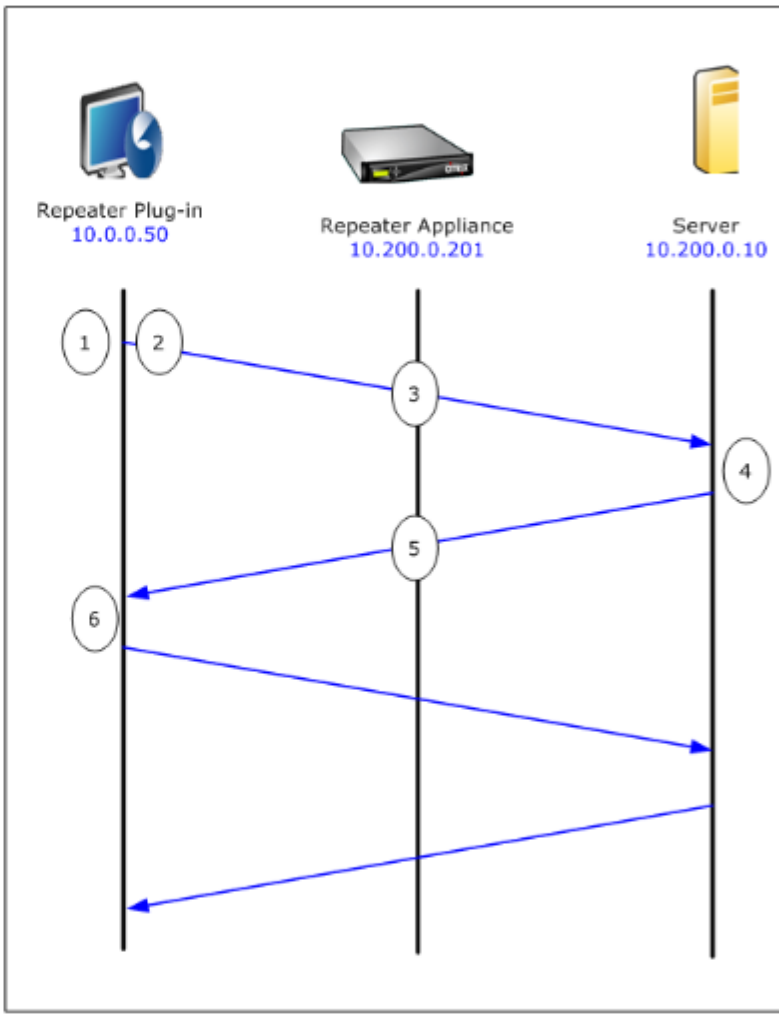
5. The appliance rewrites the addresses and forwards the packet to the Plug-in (placing the server address in an option field).

   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.



How the plug-in selects an appliance

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.

Deploy appliances for Use with plug-ins

March 12, 2021

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.

Use a dedicated appliance when possible

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.

Use inline mode when possible

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.

Place the appliances in a secure part of your network

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.

Avoid NAT problems

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.

Select softboost mode

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.

Define plug-in acceleration rules

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.

Define 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

Signaling Channel Configuration | **Acceleration Rules** | General Configuration

Repeater Plug-In: Acceleration Rules

Apply | Cancel | Add | Delete | Up | Down

Rule	Rule Type	Destination IP/Mask	Port
1	Exclude	10.200.33.102	All
2	Exclude	10.200.33.100	All
3	Exclude	10.200.33.104	All
4	Exclude	10.200.33.105	All
5	Accelerate	10.0.0.0/8	All
Default	Exclude	All	All

1. 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.

IP port usage

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 commu-

nication 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.

TCP option usage and firewalls

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.

Customize the plug-in MSI file

March 12, 2021

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 it 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.

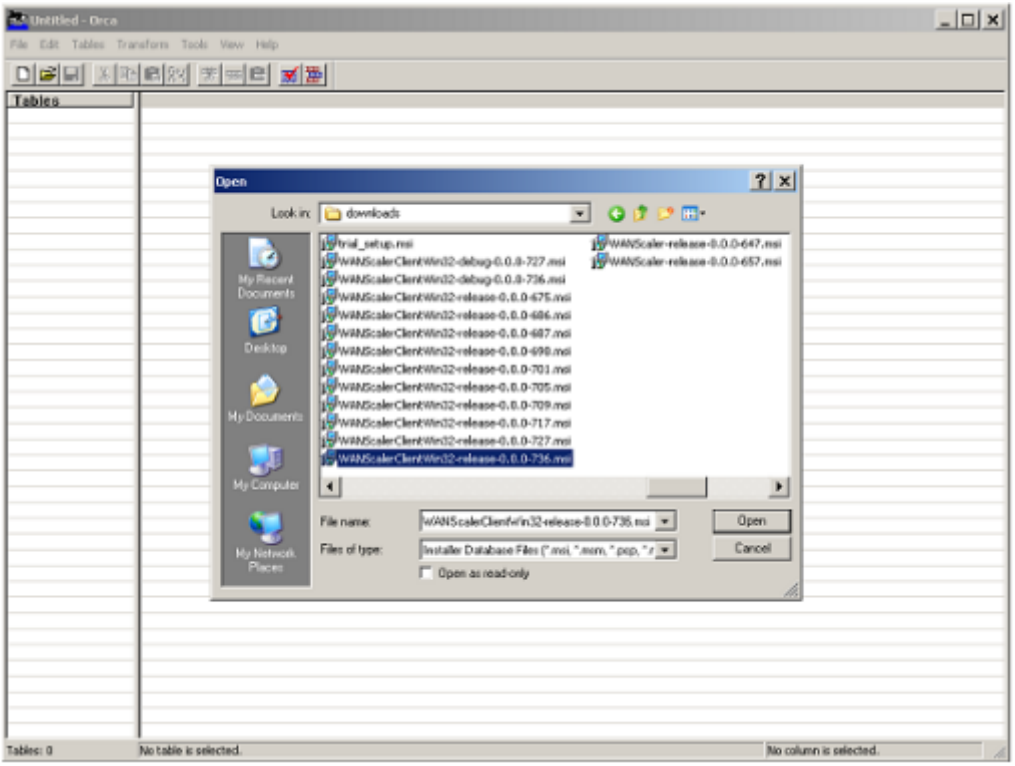
Install the Orca MSI Editor:

There are many MSI editors such as 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 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 .
DBCMINSIZE	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 DBCMINSIZE.

Parameter	Description	Default	Comments
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 the plug-in. 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 ——)

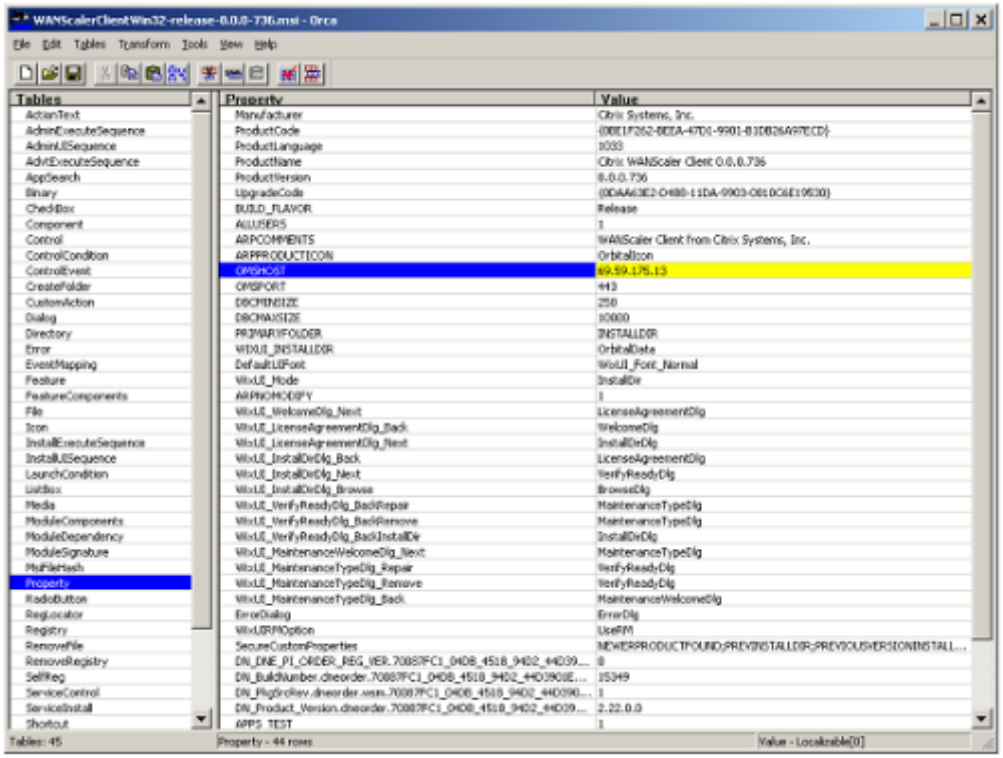
6. On the Tables menu, click Property. A list of all the editable properties of the .MSI file appears. Edit the parameters shown in the following table. To edit a parameter, double-click on its value, type the new value, and press **Enter**.

Parameter	Description	Default	Comments
WSAPPLIANCES	List of appliances	None	Enter the IP or DNS addresses of your WANOP Client Plug-in 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* .
DBCMINSIZE	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 DBCMINSIZE.
PRIVATEKEYPEM	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——)

Parameter	Description	Default	Comments
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 the plug-in. 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 ——)

7. 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:



8. 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.

Deploy plug-ins on windows systems

March 12, 2021

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.

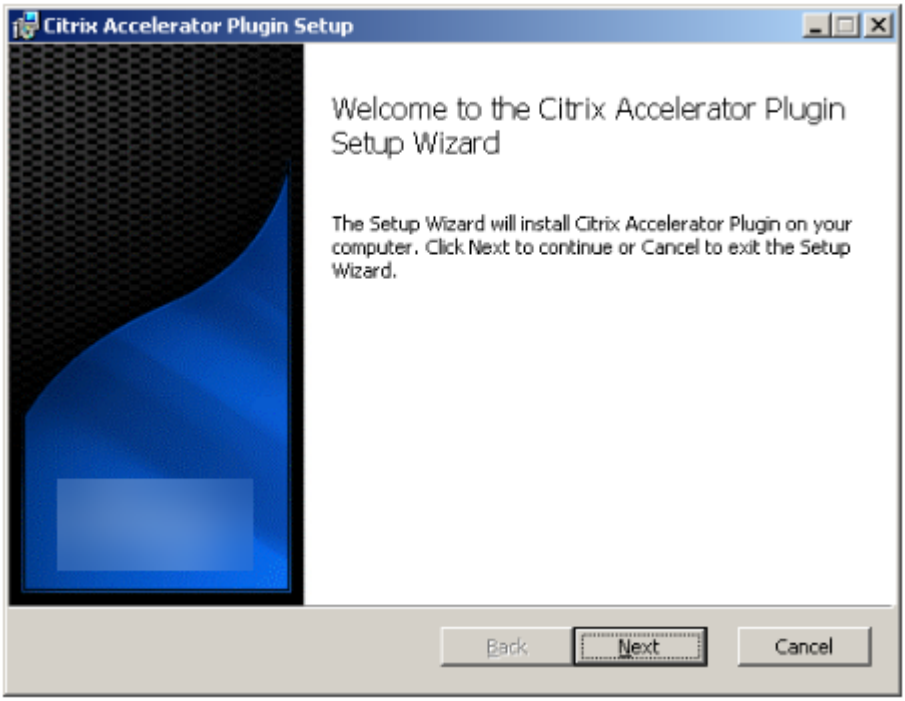
Installation

> **Prerequisites:**
>
> Windows 10 requires all drivers to have a valid digital signature to perform the installation without any error.

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:

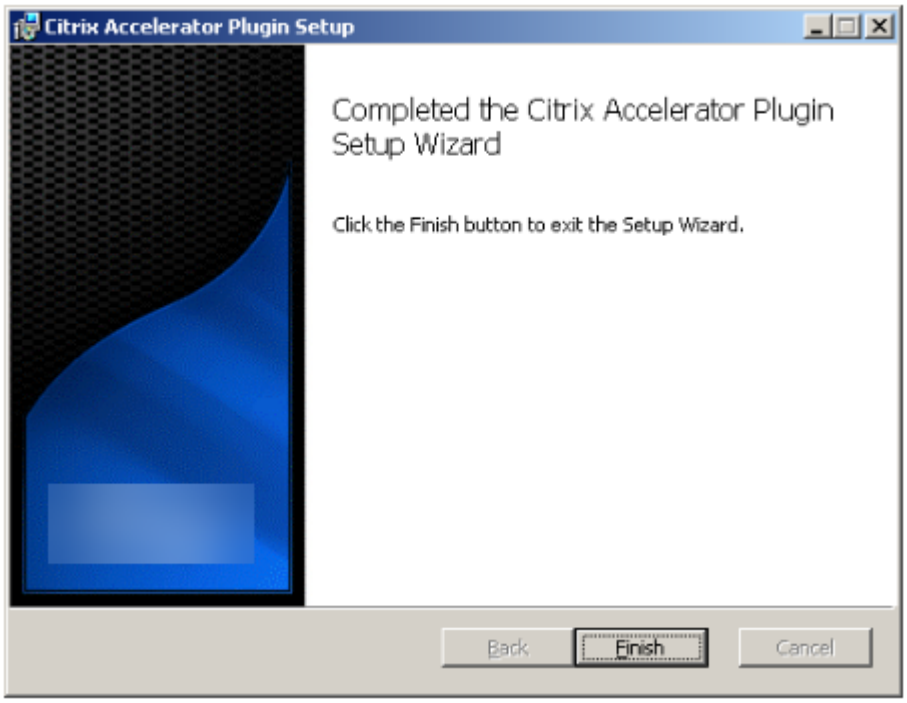
   The steps below are for an interactive installation. A silent installation can be performed with the command:

"**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.

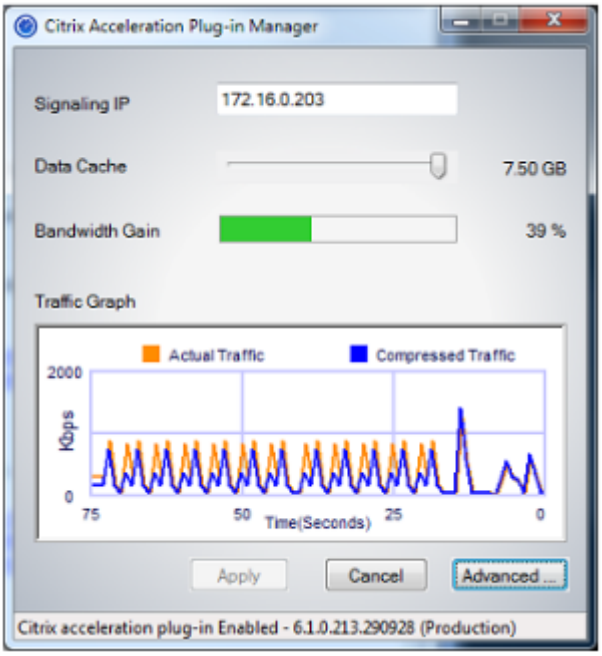
3. When the installer finishes, it might ask you to restart the system. After a restart, the WANOP Client Plug-in Plug-in starts automatically.

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.

Troubleshoot plug-ins

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.

Deterministic network enhancer locking error

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.

Other installation problems

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

March 12, 2021

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.

Basic display

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.

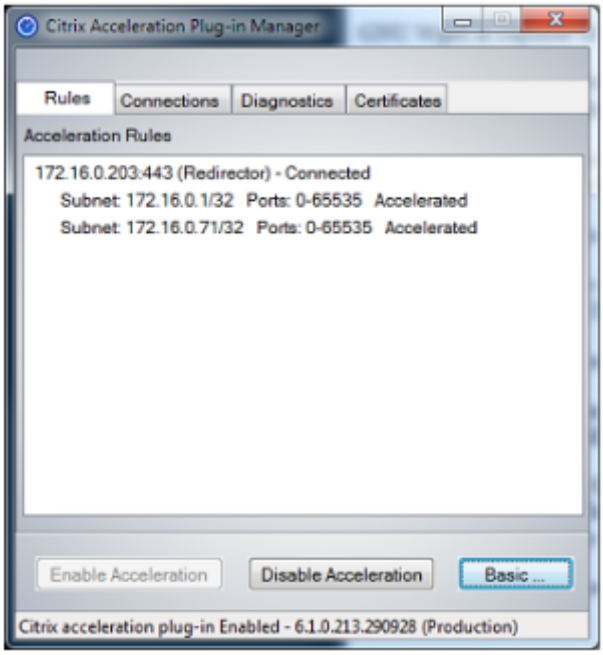
  Examples: 10.200.33.200, ws.mycompany.com, ws2.mycompany.com

- 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.

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.

Rules tab

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.

Connections tab

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 sys-

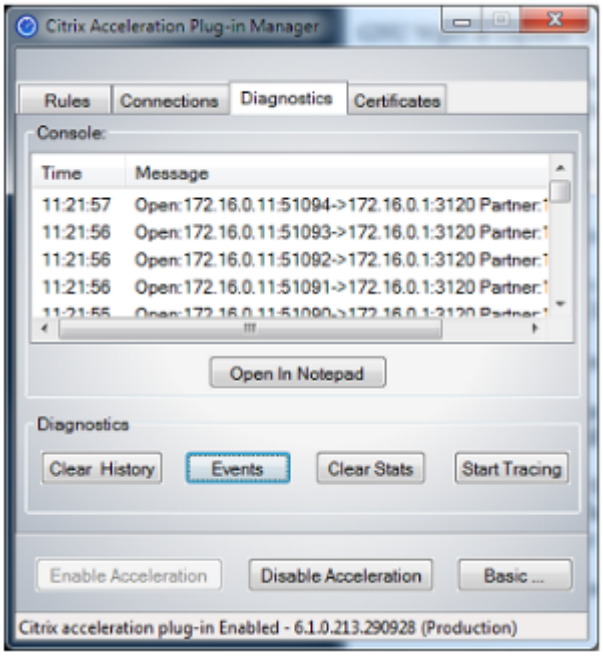
tems. Clicking More displays the same information as with accelerated connections, plus a status field that reports Active if the CIFS connection is running with WANOP Client Plug-in's special CIFS optimizations.

- **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.

Diagnostics tab

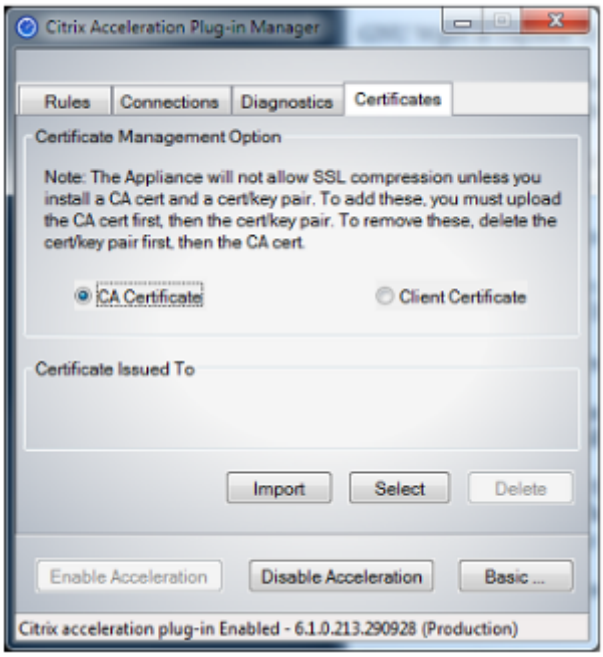
The Diagnostics page reports the number of connections in different categories, and other useful information.

- **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.



Certificates tab

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.

Update the WANOP plug-in

March 12, 2021

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.

Uninstall the WANOP client 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.

Troubleshoot WANOP plug-in

March 12, 2021

- **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.

SMB 3.1.1 connection

March 12, 2021

The Server Message Block (SMB) Protocol is a network file sharing protocol. The message packets that defines a particular version of the protocol is called a dialect. The Common Internet File System (CIFS) Protocol is a dialect of SMB.

In Citrix SD-WAN release 10 version 1, the SMB 3.1.1 protocol is introduced on the Citrix SD-WAN WANOP and Premium Edition platforms.

The Citrix SD-WAN WANOP supports SMB 3.1.1 connections. The SMB 3.1.1 connections are applicable when the client is Windows 10 and the server is Windows Server 2016.

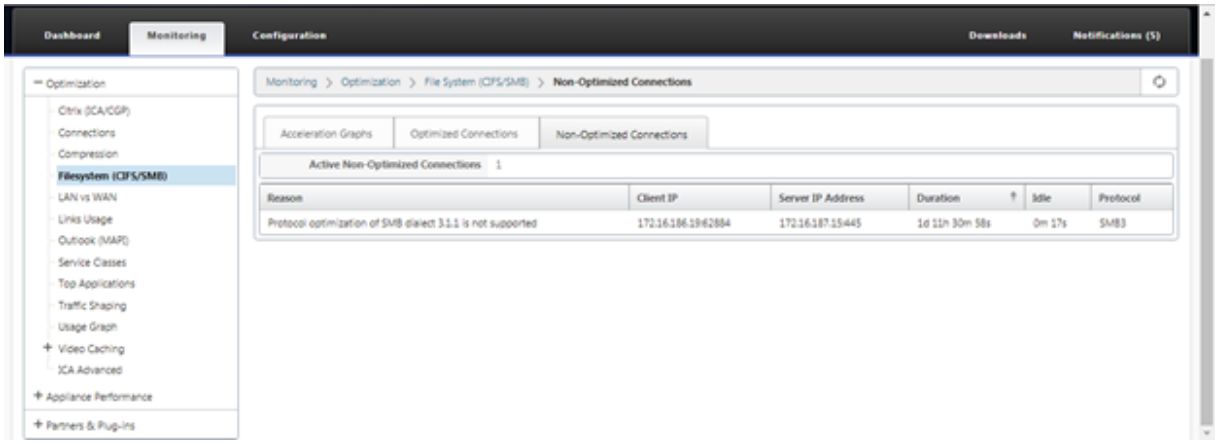
When SMB 3.1.1 traffic passes through the WANOP module:

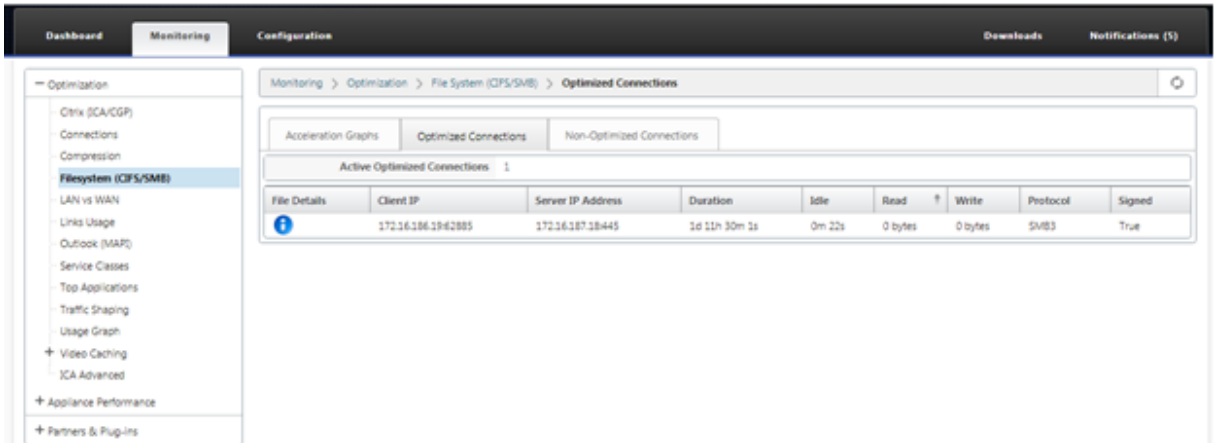
- It is counted/visible as part of SMB 3.1 CIFS un-optimized connections
- The following trace message is displayed, “Pass Through this connection as SMB 3.1.1 is not supported”.

Client	Server	SMB version
Windows 10	Win 2016, 2012R2	SMB 3.1.1, 3.0.2
Windows 8.1	SMB 3.0	SMB 3.0
Windows 7	SMB 3.0	SMB 3.0

For non-optimized connections, the Citrix SD-WAN WANOP appliance GUI displays a message for SMB 3.1.1.

In the Citrix SD-WAN WANOP appliance GUI, navigate to **Monitoring** > **Filesystem (CIFS/SMB)**. Click the **Non Optimized Connections** tab, the following message is displayed, *Protocol optimization of SMB dialect 3.1.1 is not supported*. There are no log entries available, and there is no new configuration required in SD-WAN WANOP to support this.





How-to-articles

March 12, 2021

The “How-to-articles”describe the procedure to configure supported features by Citrix 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
- Secure Peering and Manual Secure Peering
- Zero touch Deployment
- Two Box mode Deployment

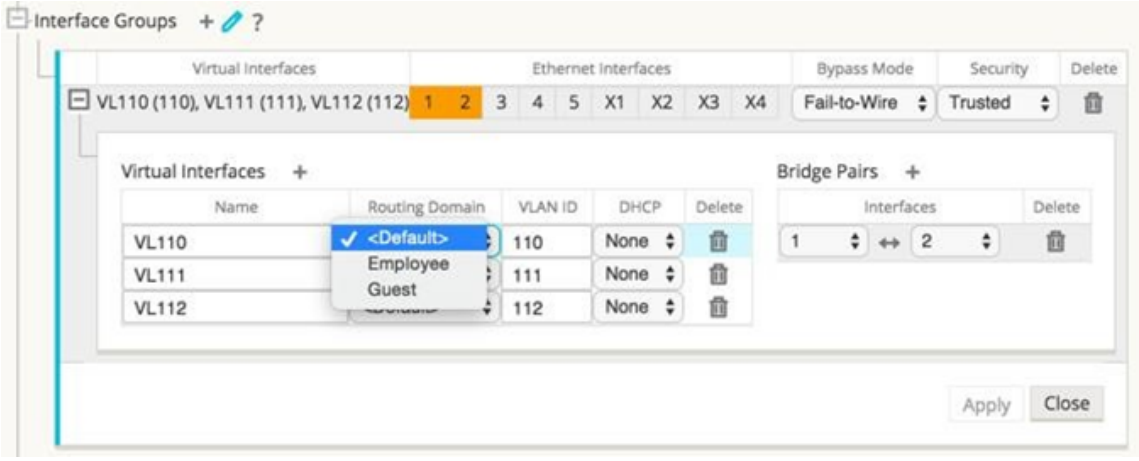
Interface Groups

March 12, 2021

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.



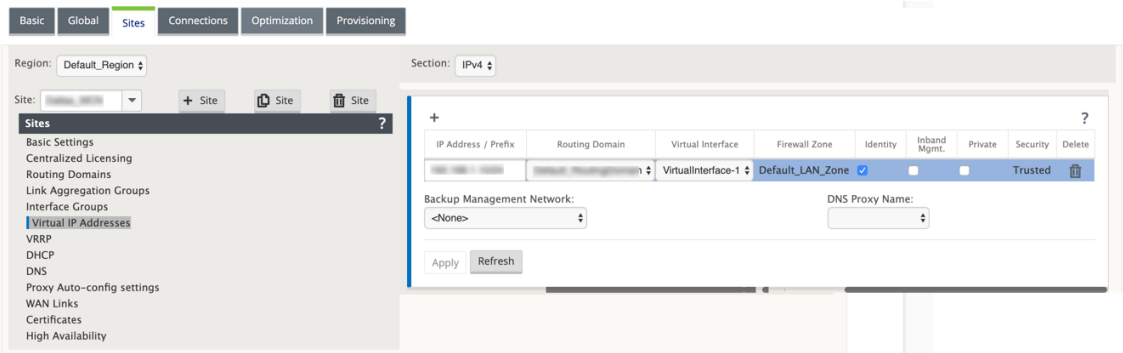
Configure Virtual IP Address Identity

March 12, 2021

Virtual network interface can host multiple IP addresses in same or different Subnets. But, you can select only one virtual IP with identity set to true which can be used for dynamic routing protocols like BGP/OSPF, DHCP server/relay, and In-band management.

To configure Virtual IP Address identity:

1. In the **Configuration Editor**, navigate to **Sites** > **[Site Name]** > **Virtual IP Addresses**.
2. Click the **Identity** check box for a Virtual IP Address to use it for IP services.



Configure access interface

March 12, 2021

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 **How to configure access interface** section in Configure MCN topic.

Configure Virtual IP addresses

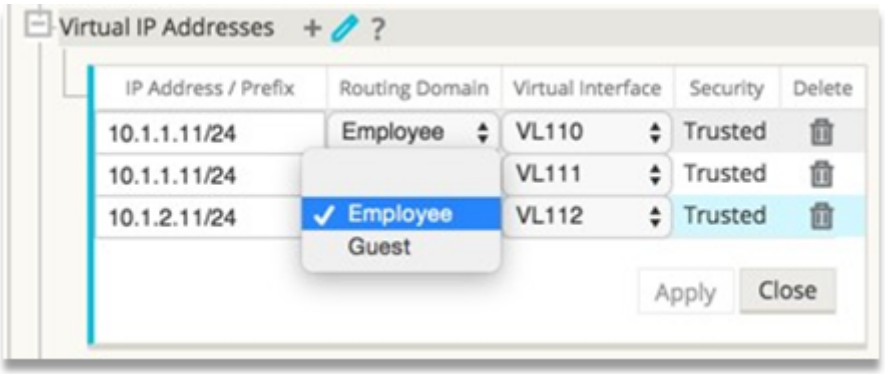
March 12, 2021

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.



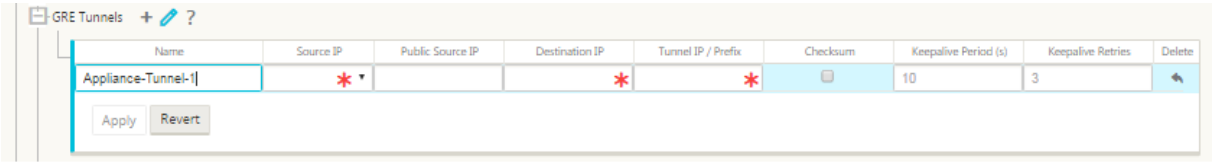
Configure GRE Tunnels

March 12, 2021

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.



For more information about securing web gateway using GRE tunnels, see; Secure Web Gateway

Setup dynamic paths for branch to branch communication

March 12, 2021

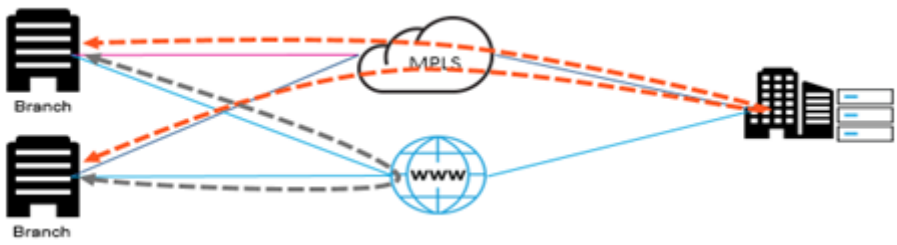
With demand for VoIP and video conferencing, the traffic is increasingly moving between offices. It is inefficient to set up full mesh connections through datacenters which can be time consuming.

With Citrix 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.

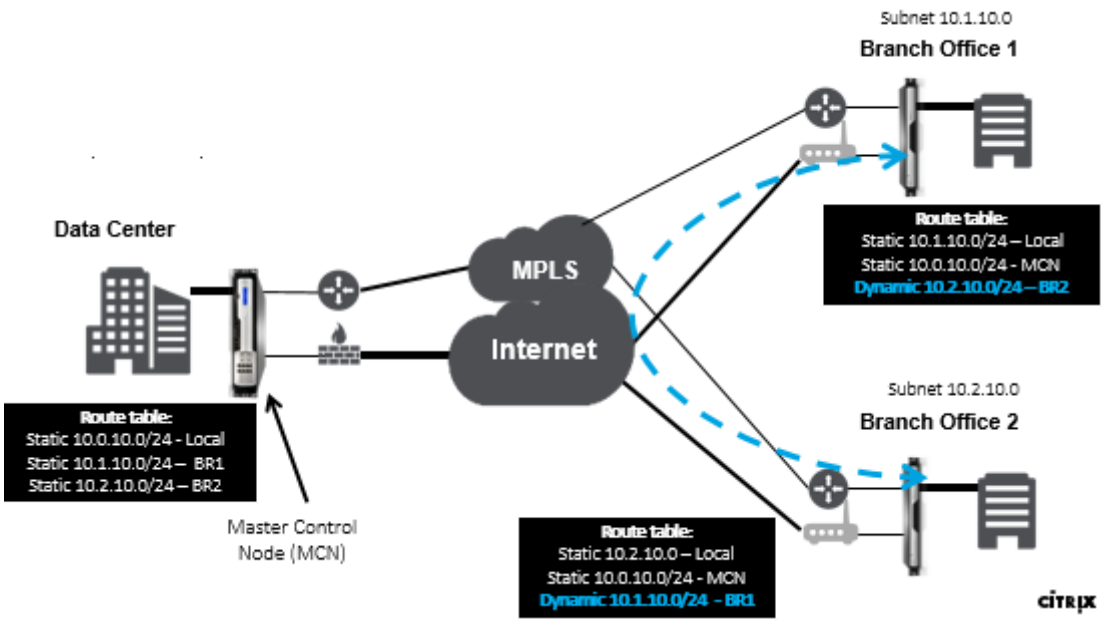
Additional benefits of SD-WAN network include:

- 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 virtual paths:



SD-WAN network with dynamic path:

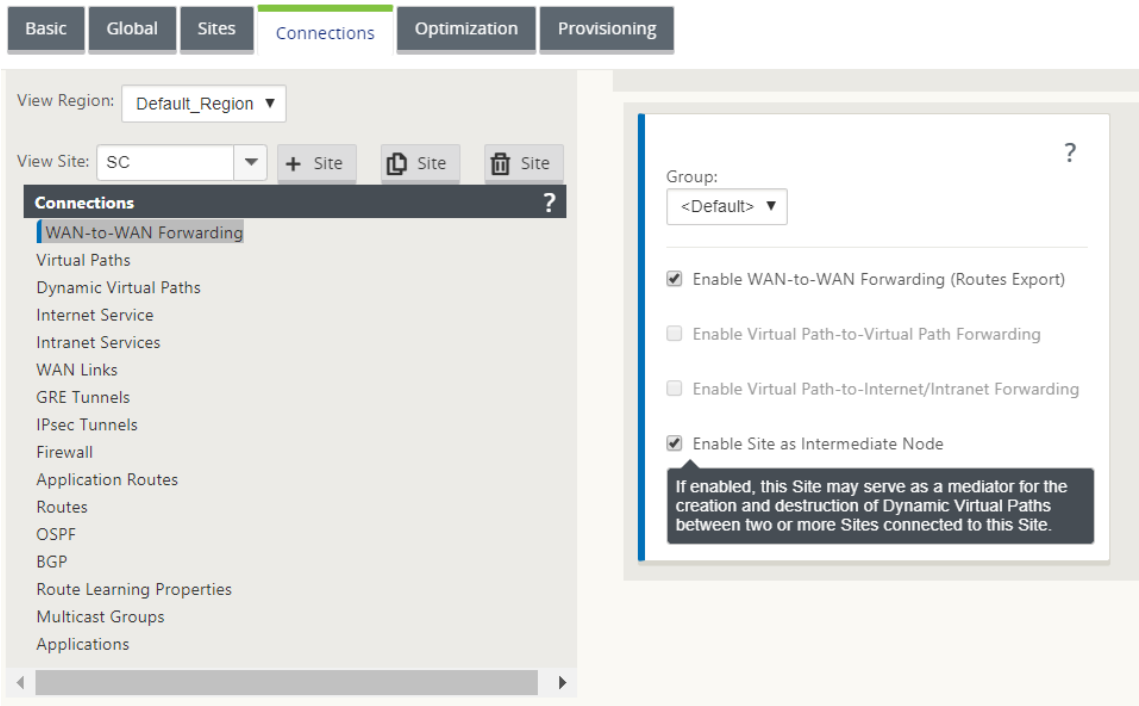


- Dynamic virtual paths are used for large scale deployments, such as Enterprises
- Smaller deployments use Static virtual paths and any-to-any virtual paths
- Always use Static virtual paths between two Data Centers (DC to DC)
- Not all WAN paths need to be configured for using Dynamic virtual path
- 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.

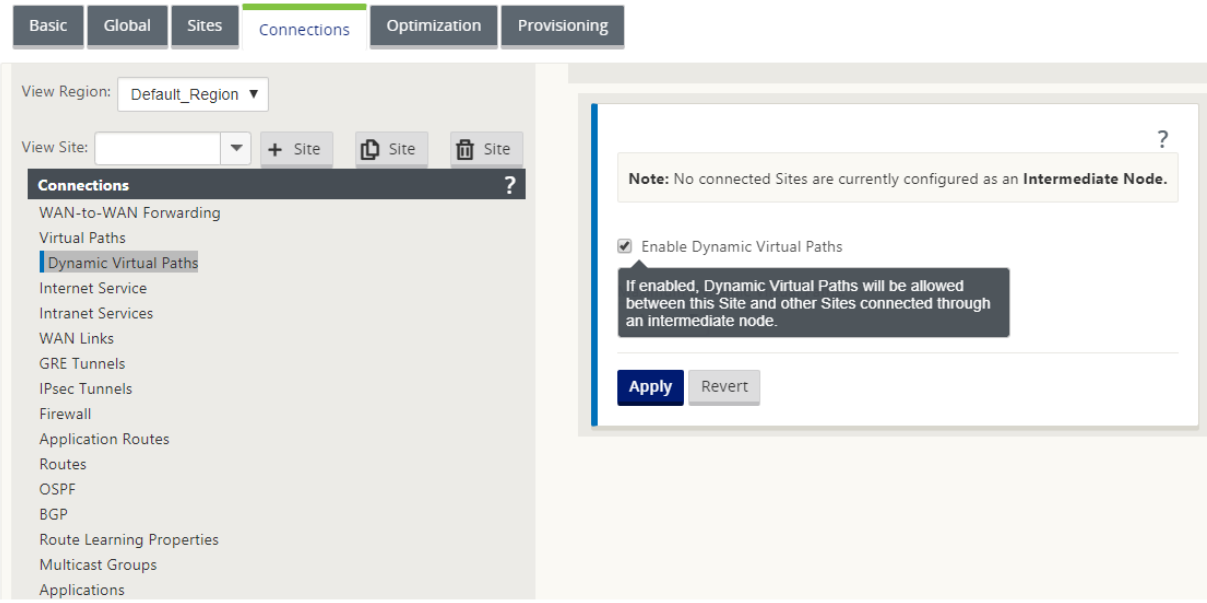
How to enable dynamic virtual path in the SD-WAN GUI

To enable dynamic virtual paths:

1. In the Citrix 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**.
3. Enable **WAN to WAN Forwarding** to enable the site to serve as a proxy for multi-hop site to site.
4. Enable **Site as Intermediate Node**
5. Navigate to **Connections > Remote Site > WAN to WAN Forwarding**.
6. Enable WAN to WAN Forwarding to enable the site to serve as a proxy for multi-hop site to site.

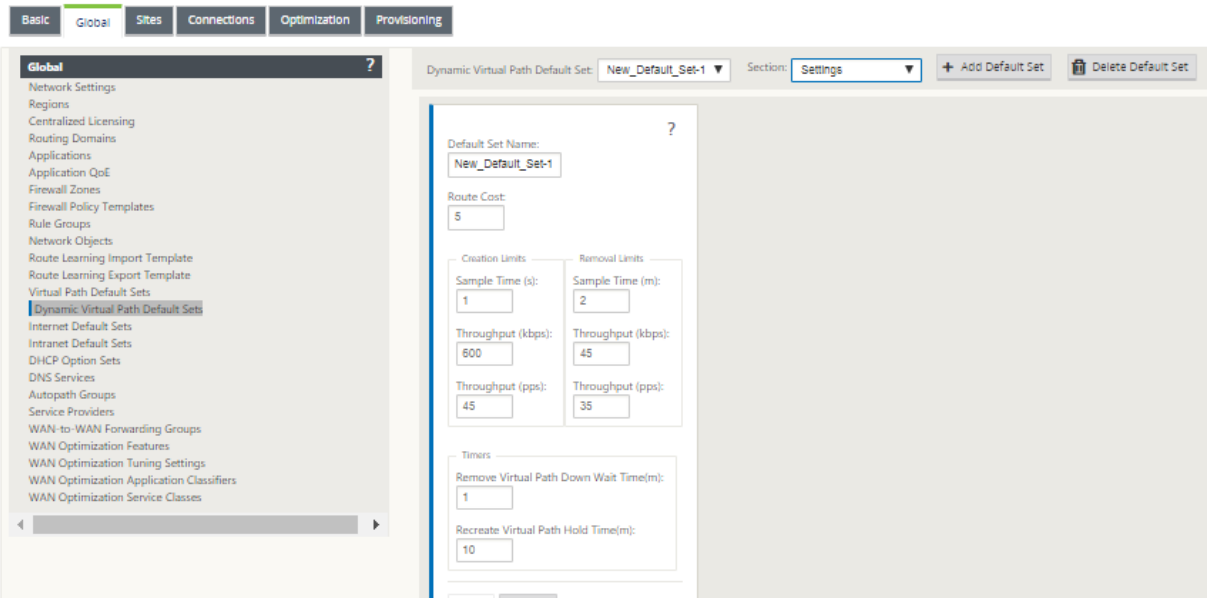


7. Navigate to **Connections > Remote Site > Virtual Path > Dynamic Virtual Path**.
8. Enable **Dynamic Virtual Paths**.
9. Set the maximum number of dynamic paths.



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.



WAN-to-WAN forwarding

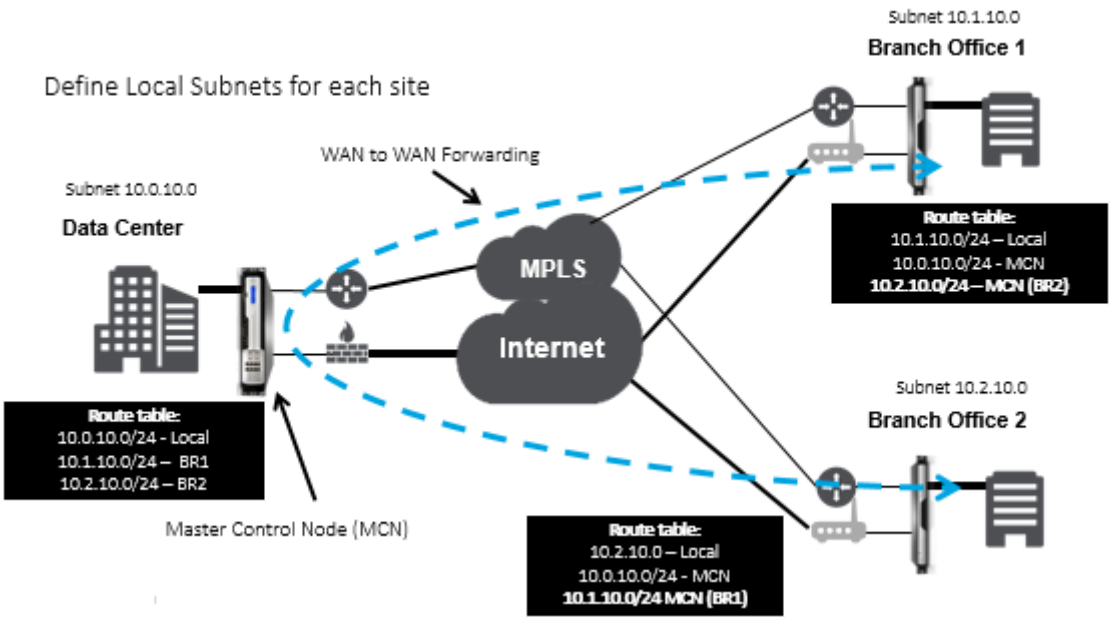
March 12, 2021

Enabling WAN-to-WAN forwarding on the MCN, allows the MCN to advertise remote site routes.

- Clients are aware of MCN local routes and 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.

Appliances running in client mode are unaware of other branches subnets until WAN-to-WAN forwarding is enabled on the MCN. Enabling this option makes the branch SD-WAN nodes aware of other branch subnets. The traffic destined to other branches is forwarded to MCN. MCN routes it to the correct destination.



Monitoring and Troubleshooting

March 12, 2021

You can use the Citrix SD-WAN appliance web management interface to monitor and troubleshoot supported features. Below are the links to Monitoring and Troubleshooting topics applicable for Citrix SD-WAN appliances.

Monitoring Virtual WAN

March 12, 2021

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.

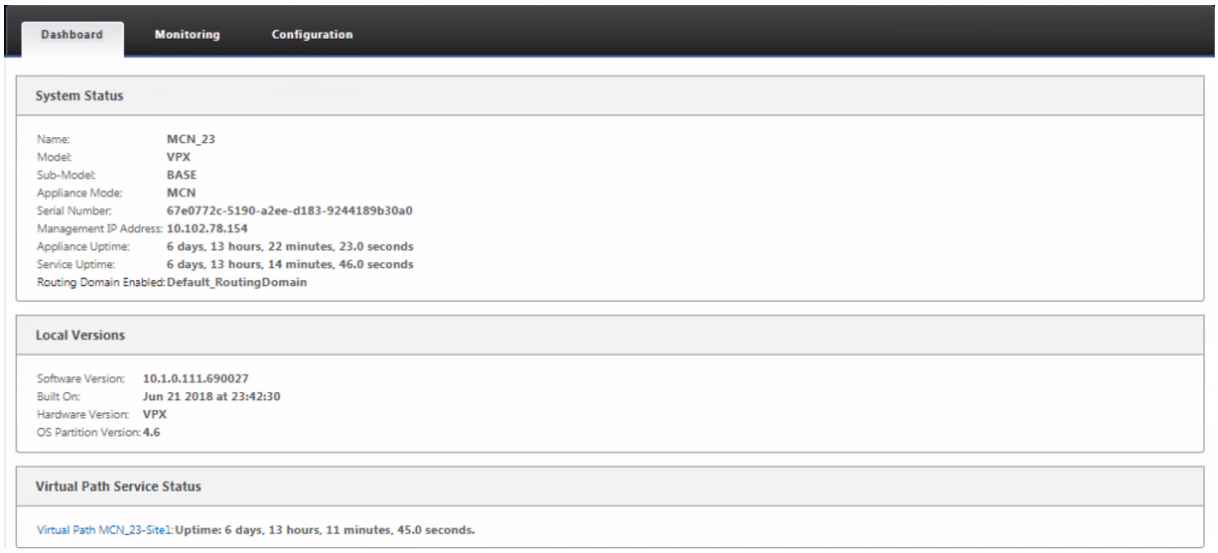
Virtual Path Service Status:

Virtual Path [site name] –This displays the 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.



Viewing Statistical Information

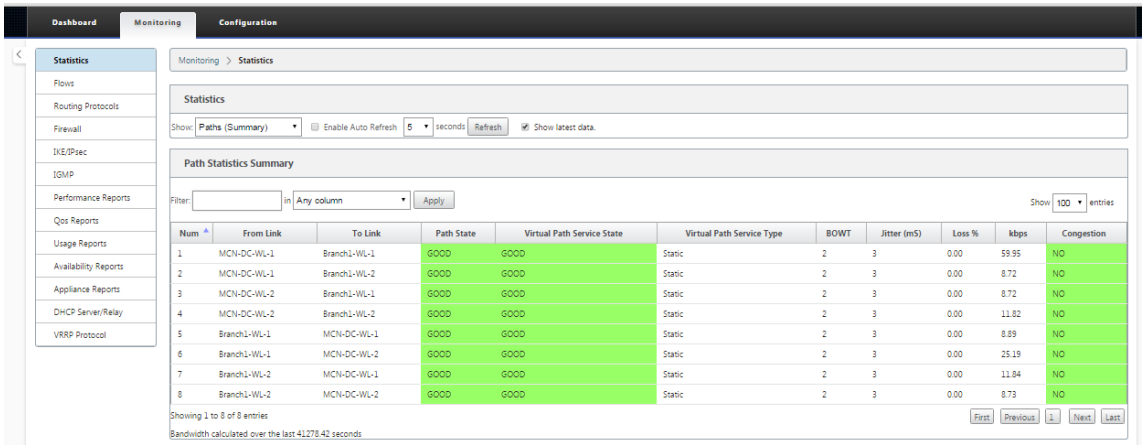
March 12, 2021

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.

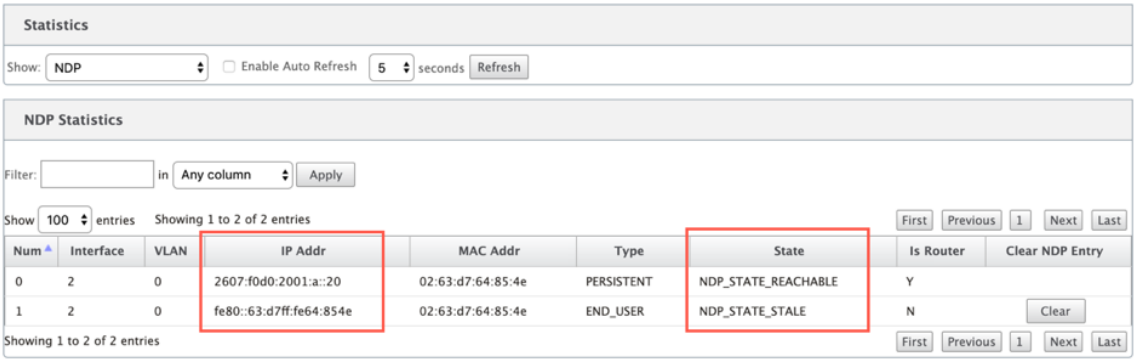
   This opens the **Monitoring** navigation tree in the left pane. By default, this also displays the **Statistics** page with **Paths** preselected in the **Show** field. This contains a detailed table of path statistics.

> **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).

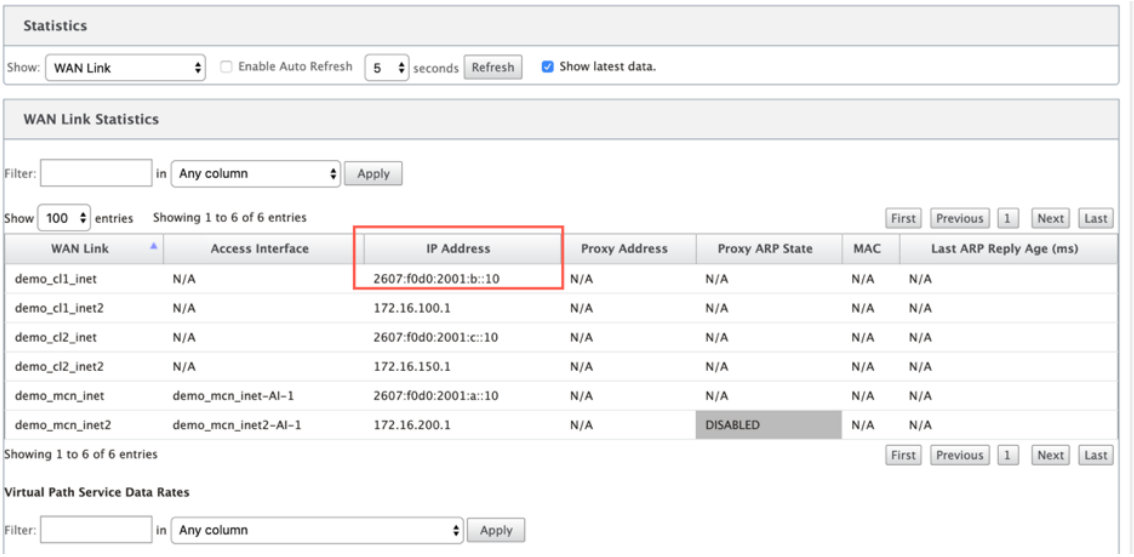


With 11.1.0 release, Neighbor Discovery Protocol (NDP) option is added for debugging neighbor discovery issues.

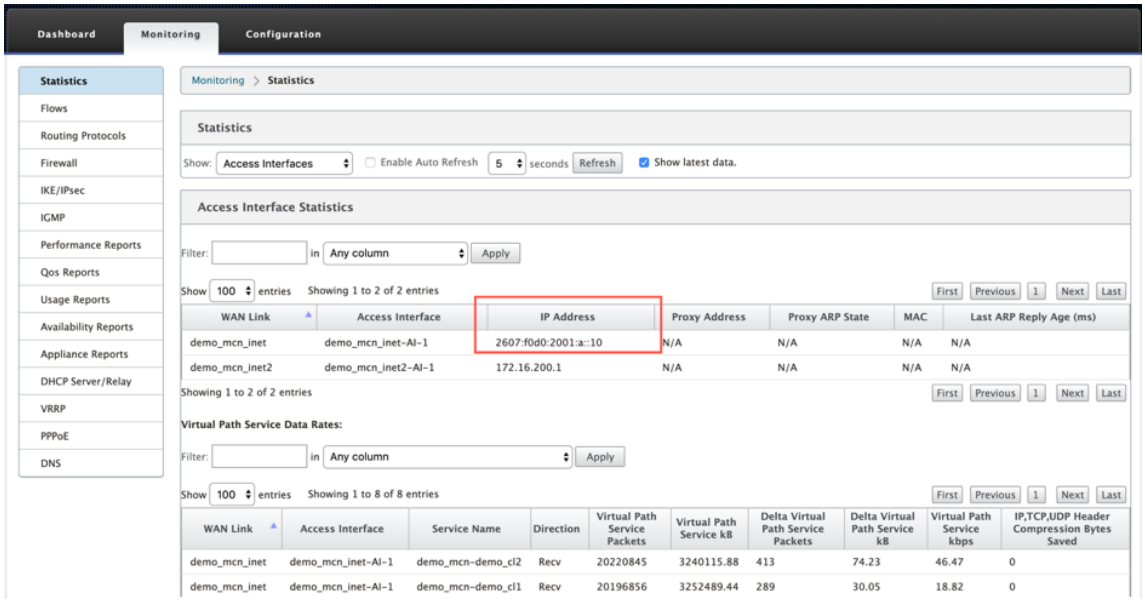
1. Select the NDP option from the Show drop-down menu and you can view the state of NDP along with the IPv6 addresses.



2. Select WAN Link from the drop-down menu. You can view the IPv6 address as well if you configured under IP Address tab.

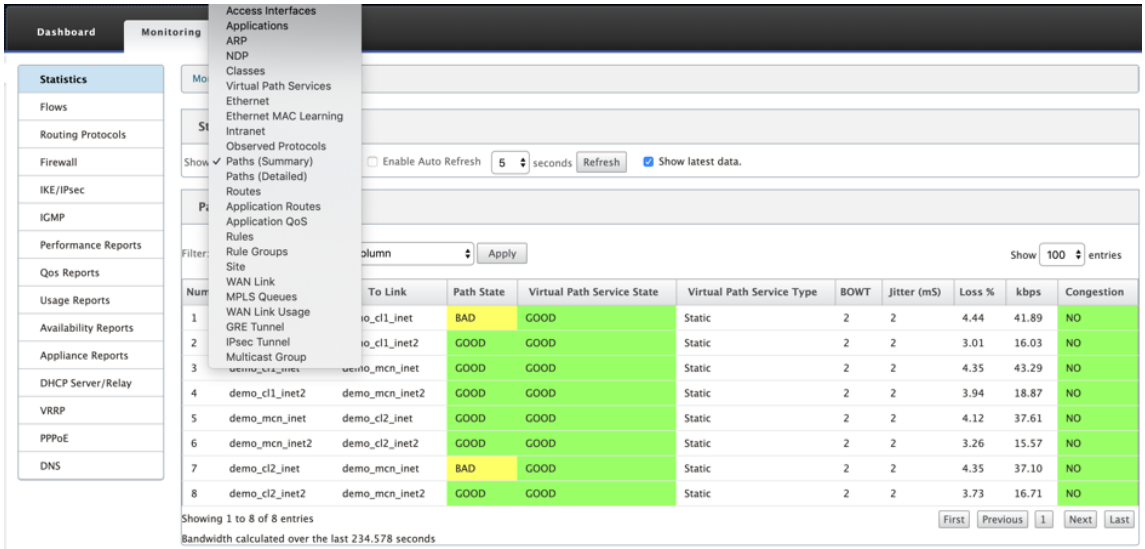


3. You can also view the Access Interface statistics.



4. Open the **Show** drop-down menu.

   In addition to the **Paths, NDP, Access Interface,** and **WAN Links statistics**, the **Show** menu also offers several more options for filtering and viewing statistical information.



Select a filter from the **Show** menu to view a table of statistical information for that topic.

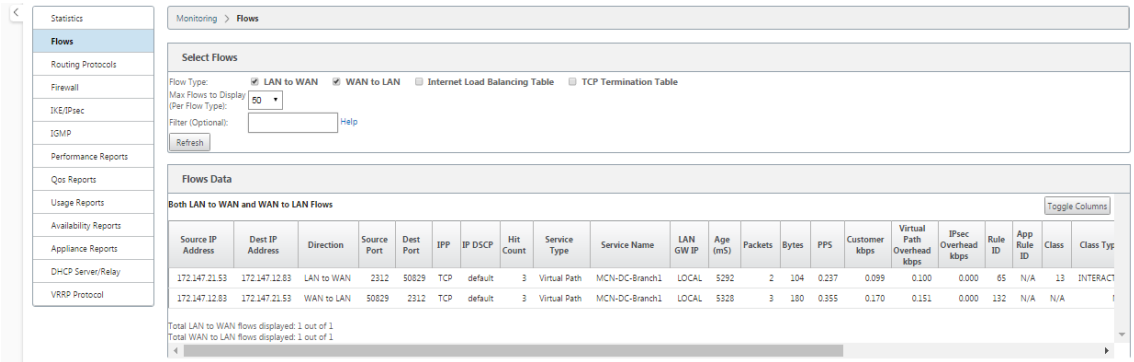
Viewing Flow Information

March 12, 2021

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. It opens the **Monitoring** navigation tree in the left pane.
2. Select the **Flows** branch in the navigation tree. It displays the **Flows** page with **LAN** to **WAN** preselected in the **Flow Type** field.



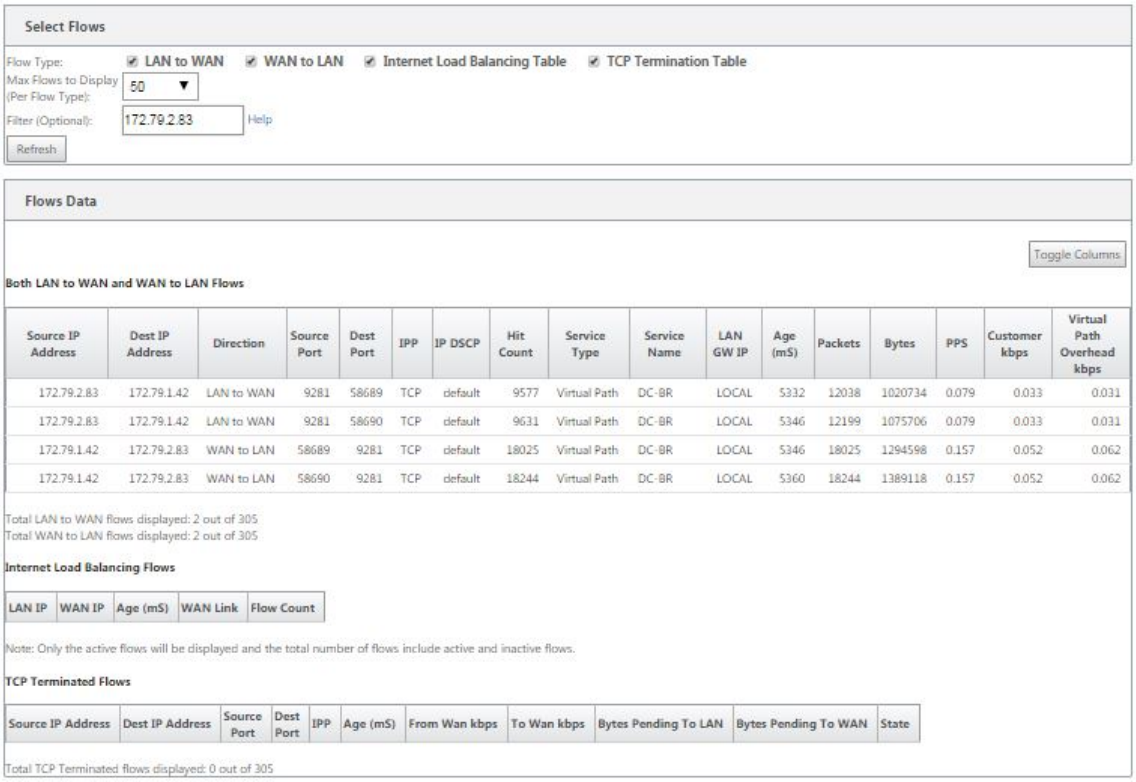
3. Select the **Flow Type**. The **Flow Type** field is located in the **Select Flows** section at the top of the **Flows** page. Next to the **Flow Type** field is a row of check box options for selecting the flow

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.
5. It determines the number of entries to display in the **Flows** table. The options are: **50**, **100**, **1000**.
6. (Optional) Enter search text in the **Filter** field. It filters the table results so that only entries containing the search text display in the table.

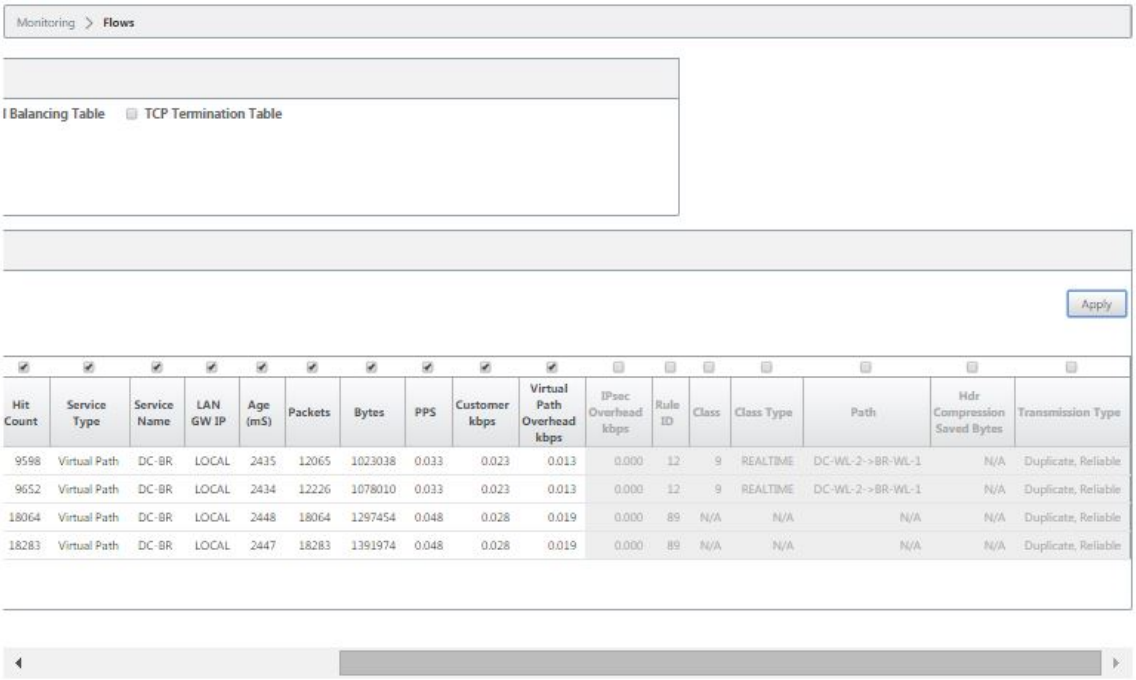
> **Tip**
>
> To see detailed instructions for using filters to refine **Flow** table results, click **Help** to the right of the **Filter** field. To close the help display, click **Refresh** in the bottom left corner of the **Select Flows** section.

7. Click **Refresh** to display the filter results. The figure shows a sample **Flows** page filtered display with all flow types selected.



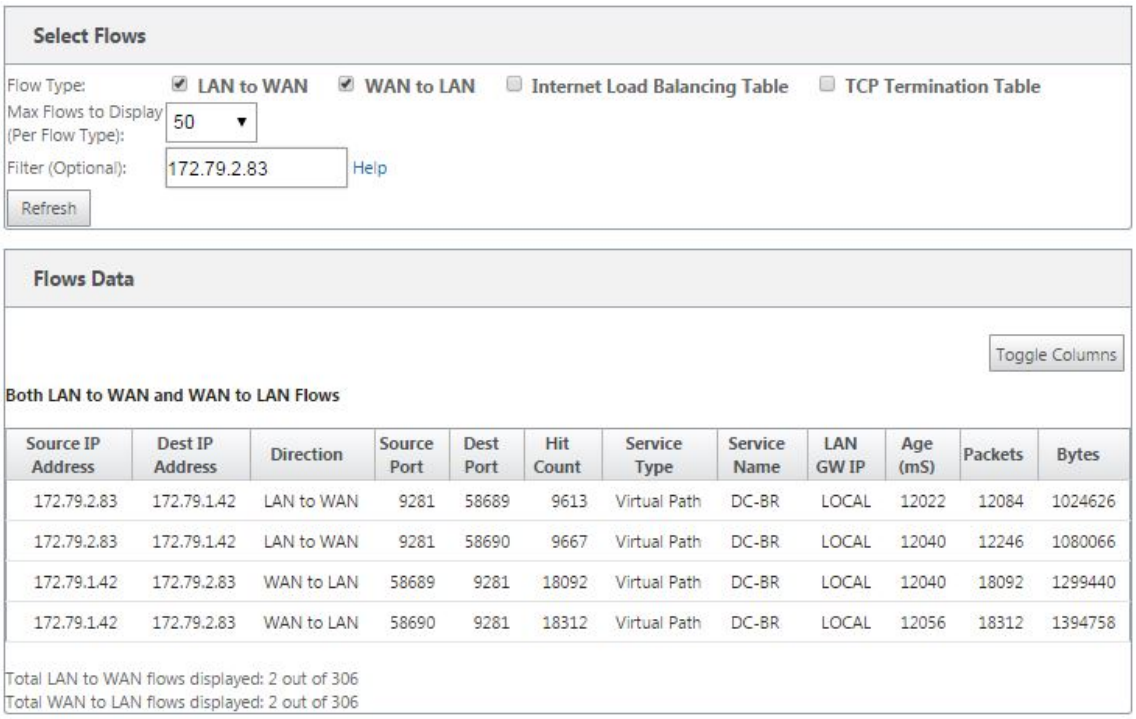
8. (Optional) Select the columns to include in the table. Do the following:
9. Click **Toggle** Columns. The **Toggle Columns** button is just above the top right corner of the **Flows** table. It reveals any deselected columns, and opens a check box above each column for selecting or deselecting that column. Deselected columns display grayed out, as shown in the figure.

> **Note**
>
> By default, all 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.



Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
9598	Virtual Path	DC-BR	LOCAL	2435	12065	1023038	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
9652	Virtual Path	DC-BR	LOCAL	2434	12226	1078010	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
18064	Virtual Path	DC-BR	LOCAL	2448	18064	1297454	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable
18283	Virtual Path	DC-BR	LOCAL	2447	18283	1391974	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable

10. Click a check box to select or deselect a column.
11. Click **Apply** (above the top right corner of the table). It dismisses the selection options, and refreshes the table to include only the selected columns.



Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes
172.79.2.83	172.79.1.42	LAN to WAN	9281	58689	9613	Virtual Path	DC-BR	LOCAL	12022	12084	1024626
172.79.2.83	172.79.1.42	LAN to WAN	9281	58690	9667	Virtual Path	DC-BR	LOCAL	12040	12246	1080066
172.79.1.42	172.79.2.83	WAN to LAN	58689	9281	18092	Virtual Path	DC-BR	LOCAL	12040	18092	1299440
172.79.1.42	172.79.2.83	WAN to LAN	58690	9281	18312	Virtual Path	DC-BR	LOCAL	12056	18312	1394758

DPI Applications in SD-WAN Center

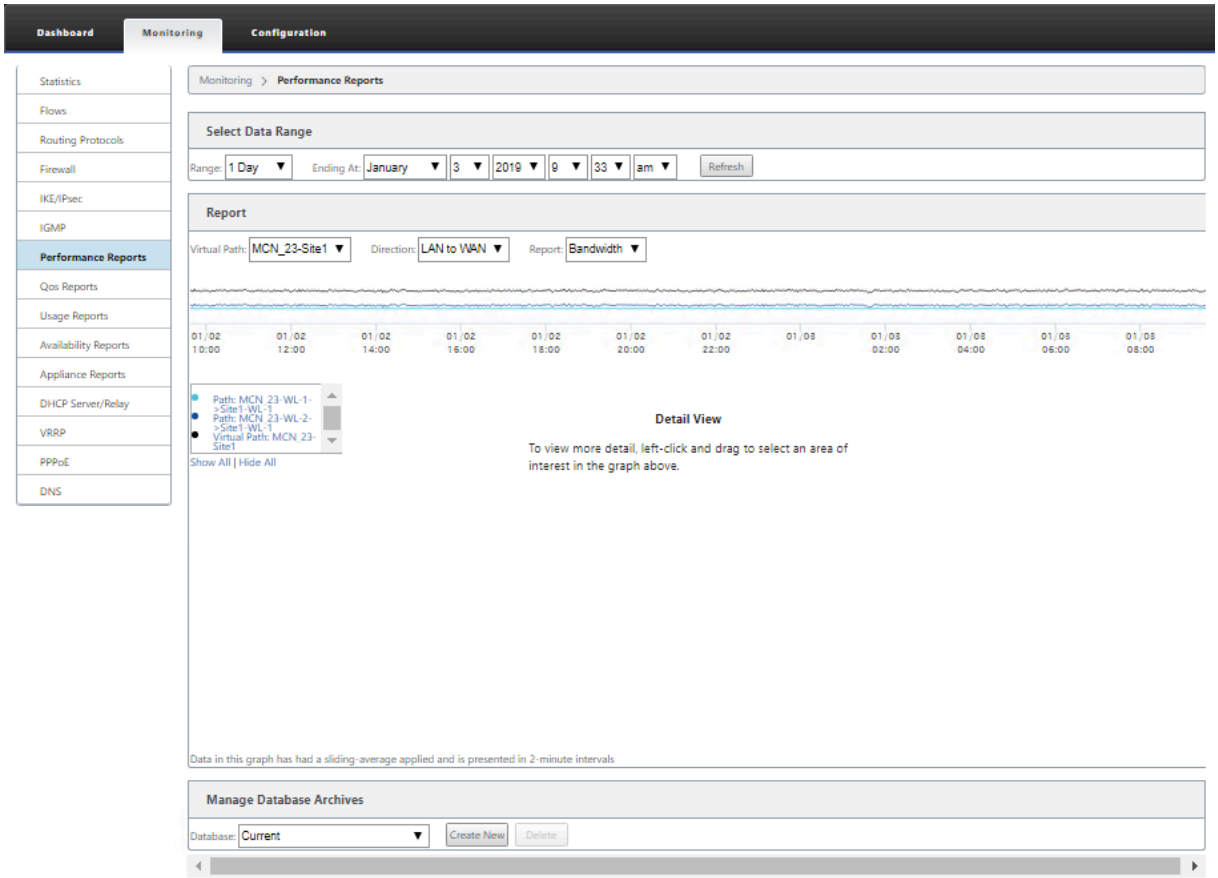
In earlier releases, around 4,000 applications and configured with 800 services (550 Virtual Paths, 256 Intranet Services) can be identified. Storing this data would impact overall system performance (CPU cycles and disk space needed to store the data). It also has an impact, if reporting on data per Usage or Path is supported.

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, it 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.

Viewing Reports

March 12, 2021

This section provides basic instructions for generating and viewing Virtual WAN reports about the local appliance using the Management Web Interface. An appliance can maintain up to 30 archives and purge the oldest archives which are more than 30 entries.



> **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.

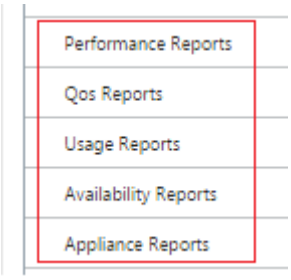
To generate and view Virtual WAN reports, do the following:

1. Log on to 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.

   The available report types are as follows:

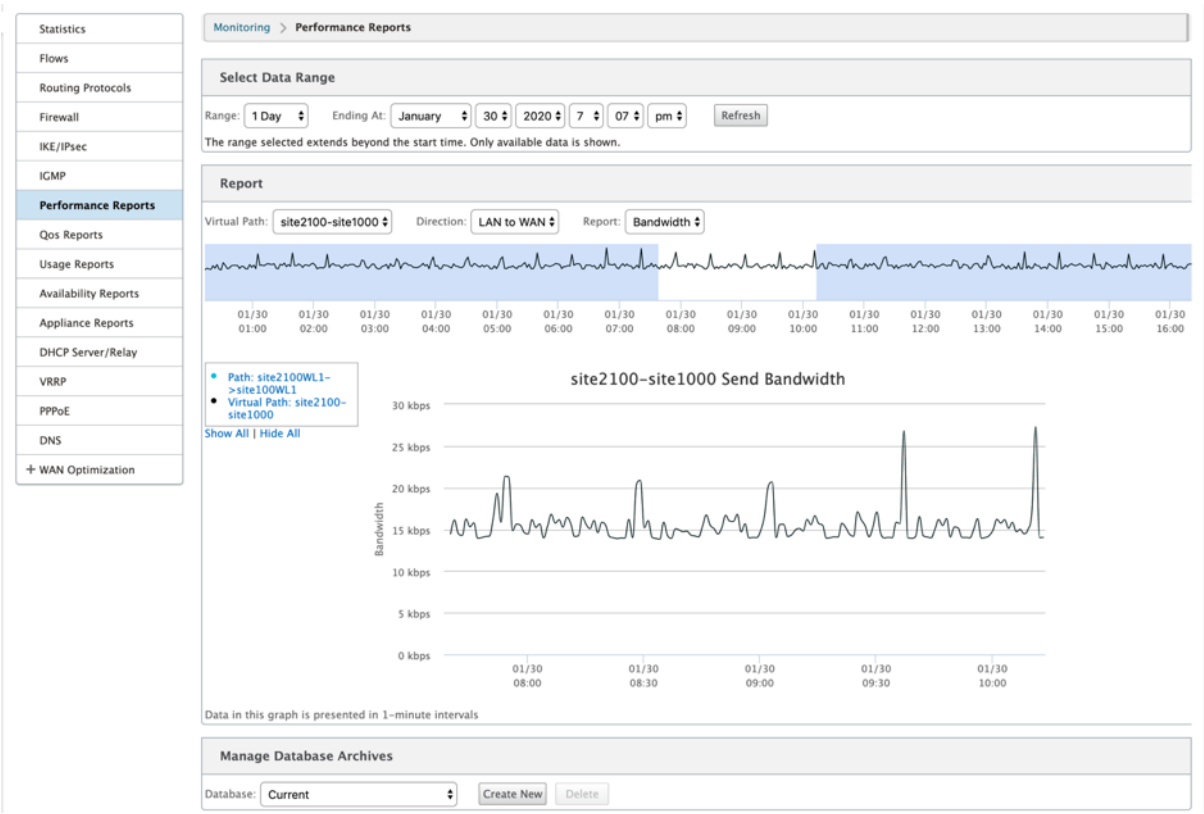
- **Performance Reports**
- **QoS Reports**
- **Usage Reports**
- **Availability Reports**
- **Appliance Reports**

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.

Performance reports

Citrix SD-WAN can show performance statistics at the site, virtual path, or Direction (LAN to WAN and WAN to LAN) level. With Citrix SD-WAN, you can collect metrics that show the efficiency of each link in milliseconds. To view more detail, left-click and select a specific area of path or time frame in the graph line.



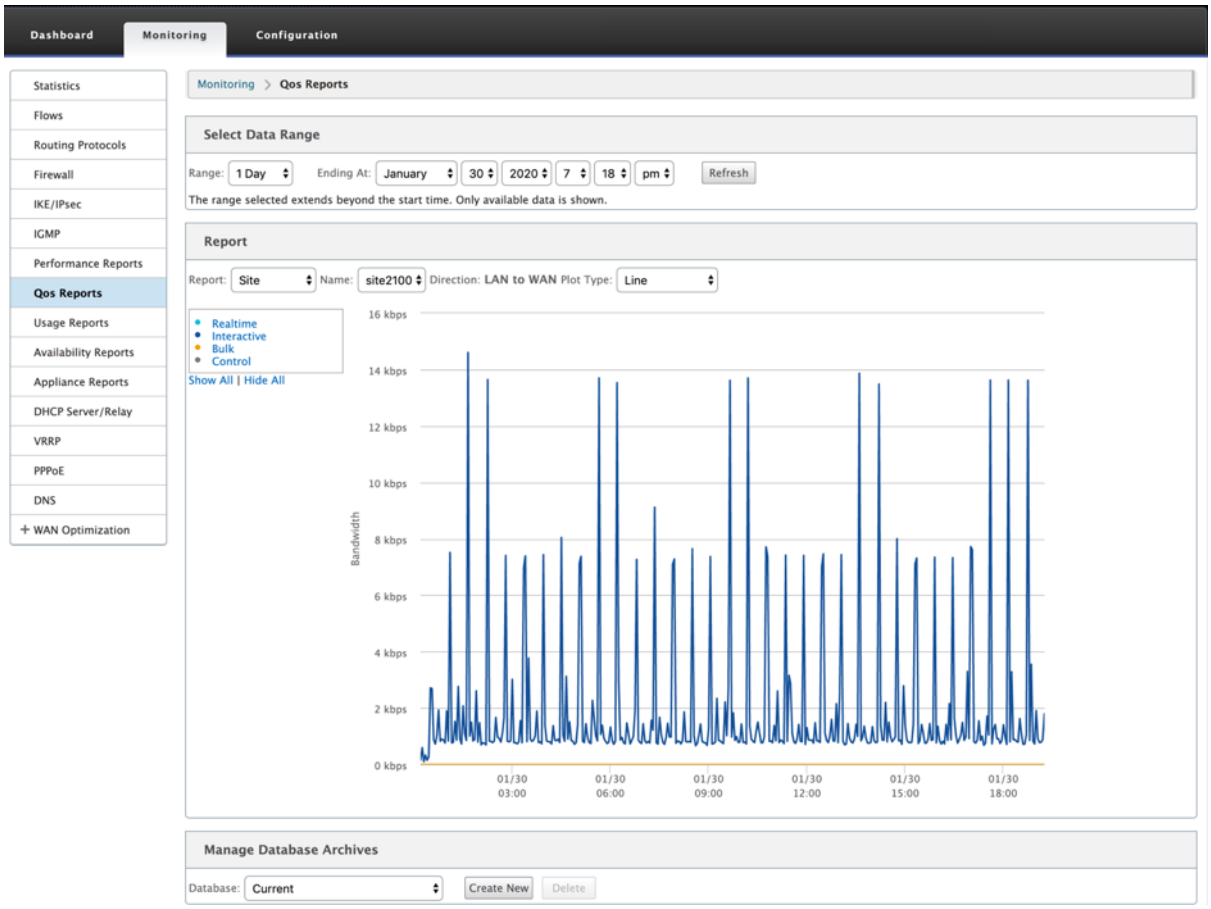
You can select the data range as needed with the following fields to view the performance report:

- **Virtual Path:** Select the Virtual Path from the drop-down list.

- **Direction:** Select the Direction as required (LAN to WAN or WAN to LAN).
- **Report:** Select the following network parameters to view the report:
  - Bandwidth
  - Latency
  - Jitter
  - Loss
  - Quality

QoS reports

You can monitor the application QoS report such as the number of packets or bytes uploaded, downloaded, or dropped at each Site, WAN Link, Virtual Path, and Path level.



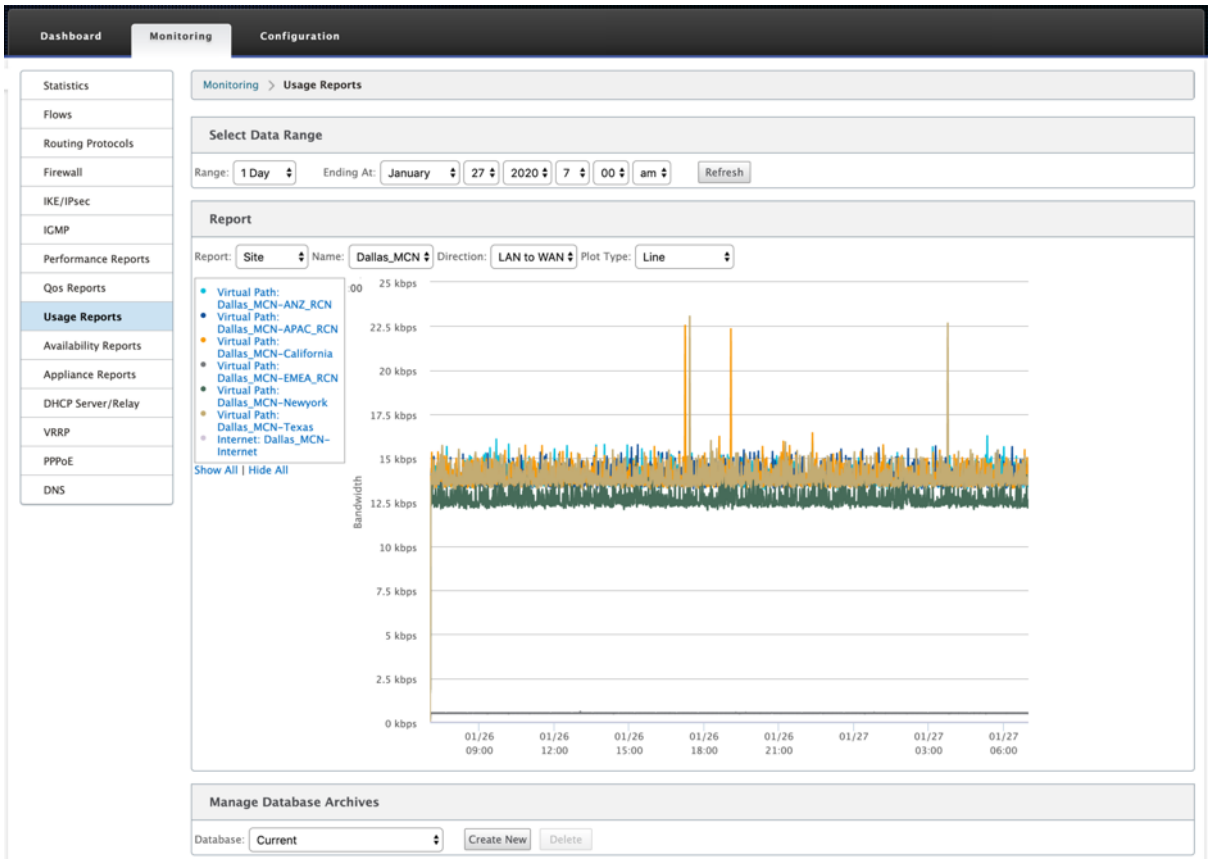
You can view the following metrics:

- **Real-time:** Bandwidth consumed by applications that belong to the real-time class type in the Citrix SD-WAN configuration. The performance of such applications depends on a great extent upon network latency. A delayed packet is worse than a lost packet (for example, VoIP, Skype for Business).

- **Interactive:** Bandwidth consumed by applications that belong to the interactive class type in the Citrix SD-WAN configuration. The performance of such applications depends on a great extent upon network latency, and packet loss (for example, XenDesktop, XenApp).
- **Bulk:** Bandwidth consumed by applications that belong to the bulk class type in the Citrix SD-WAN configuration. These applications involve little human intervention and are mostly handled by the systems themselves (for example, FTP, backup operations).
- **Control:** Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.

Usage reports

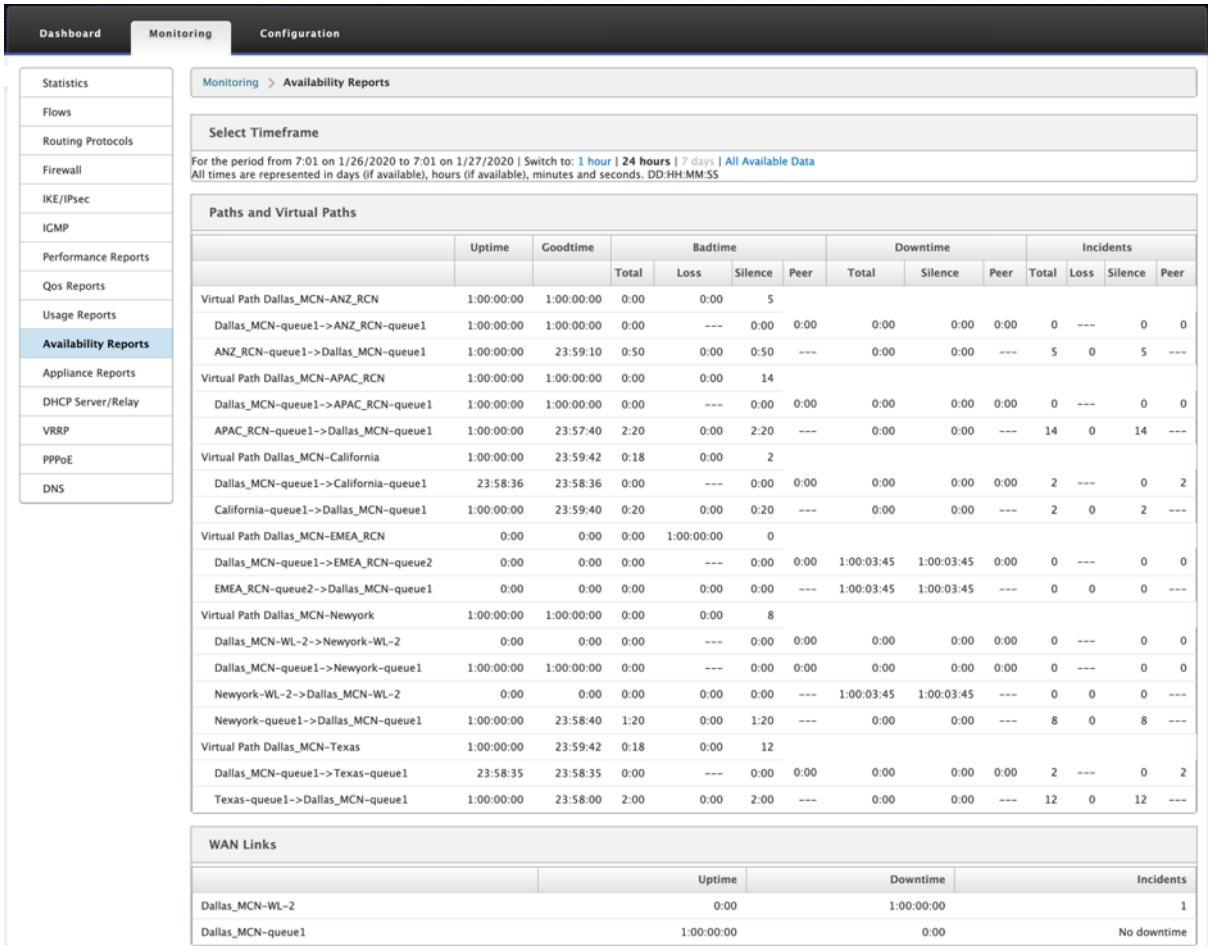
The Usage reports deliver the Virtual paths usage information.



- **Report:** Select **Site** or **WAN Link** from the drop-down list to view the report.
- **Name:** Select the name of the site or WAN link from the drop-down list.
- **Direction:** Select the direction as required (LAN to WAN or WAN to LAN).
- **Plot Type:** Select the Plot type from the drop-down list (Line or Area).

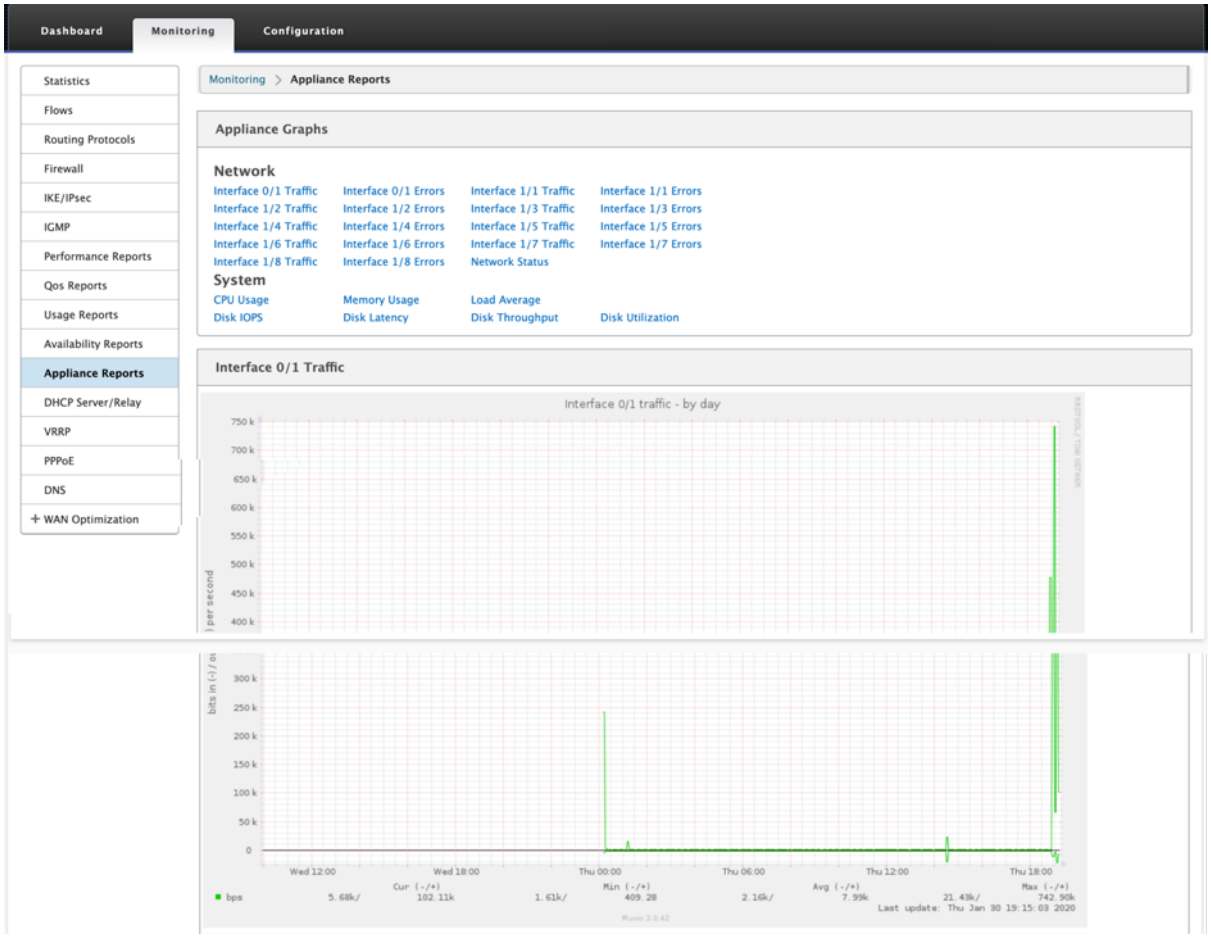
Availability reports

In this report, you can view the availability data of WAN Links, Paths, and Virtual Paths. You can also switch to or choose a specific time frame, such as 1 hour, 24 hours, and 7 days to see the available data. The Paths and Virtual Paths data are represented in a **DD:HH:MM:SS** format.



Appliance reports

Appliance report delivers Network traffic and System usage reports. Click each link to view or monitor the appliance graph by day, weekly, monthly, and yearly.



Viewing Firewall Statistics

March 12, 2021

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.

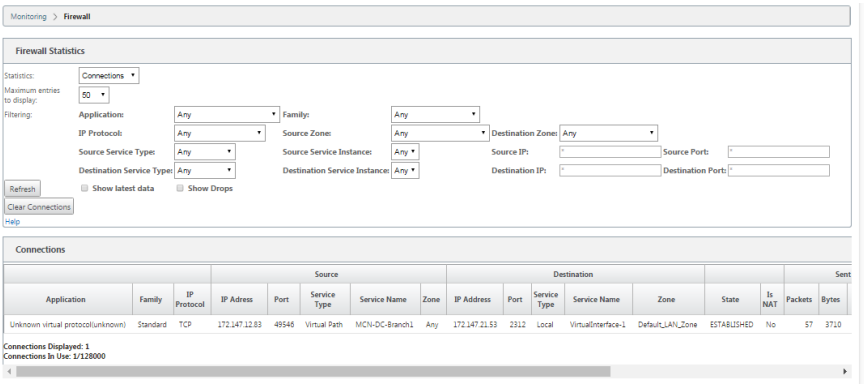
NAT Policies

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.



4. Click **Refresh**.

Diagnostics

November 18, 2021

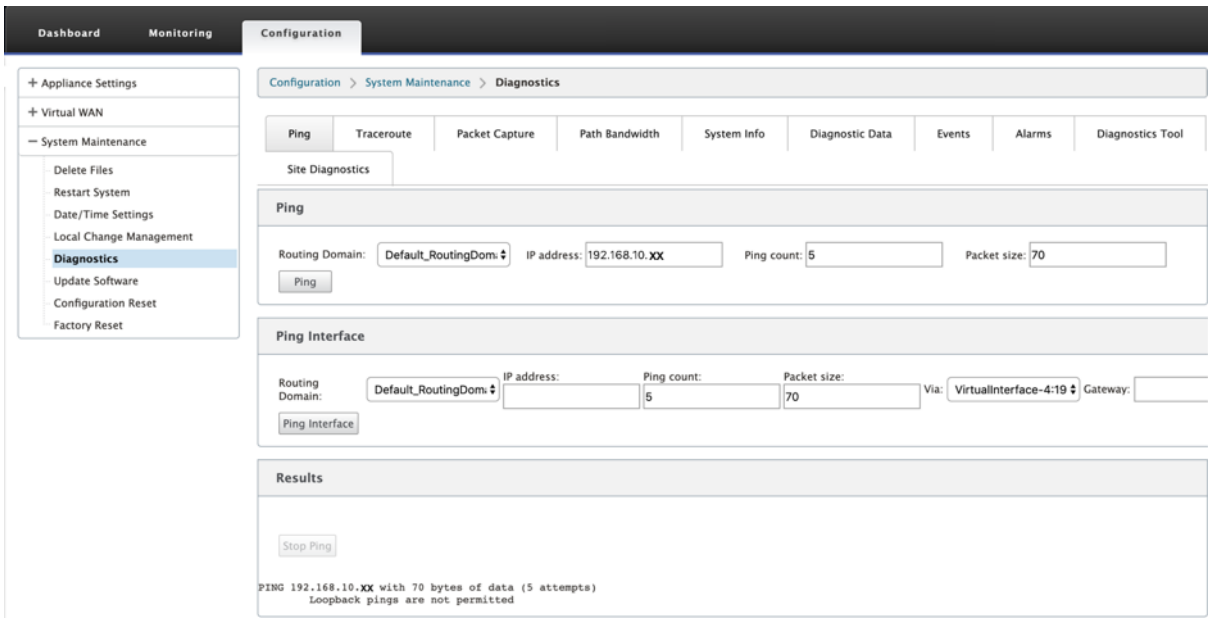
Citrix SD-WAN Diagnostics utilities provide the following options to test and investigate connectivity issues:

- Ping
- Traceroute
- Packet Capture
- Path Bandwidth
- System Info
- Diagnostics Data
- Events
- Alarms
- Diagnostics Tool
- Site Diagnostics

The diagnostic options in the **Citrix SD-WAN Dashboard** control data collection.

Ping

To use the **Ping** option, navigate to **Configuration > Diagnostics** and select **Ping**. You can use Ping to check host reachability and network connectivity.

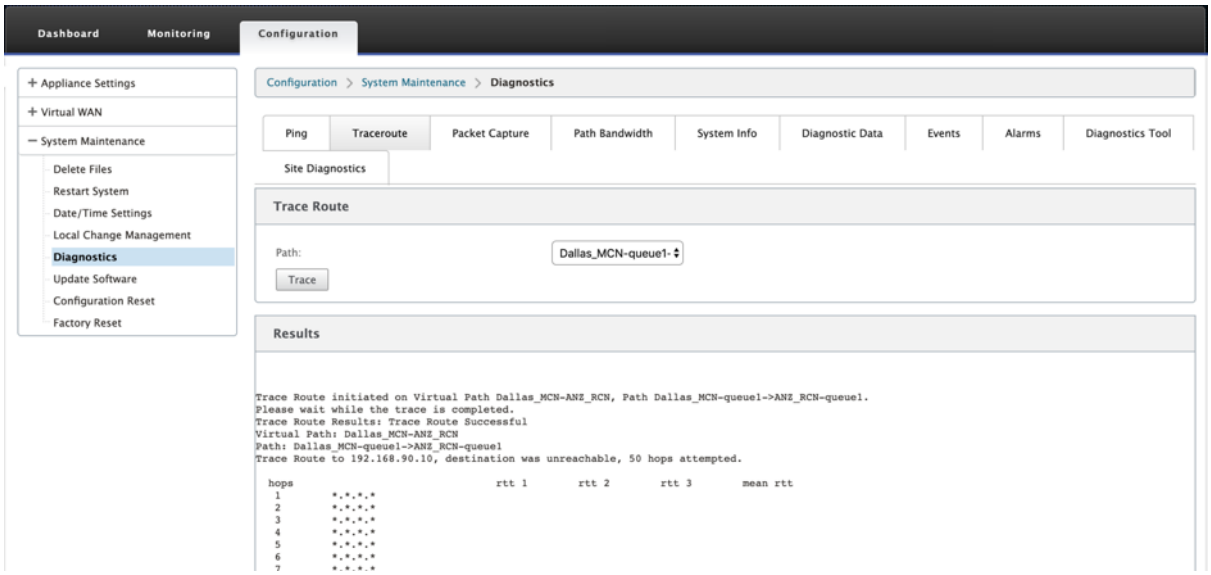


Select the routing domain. Provide a valid IP address, number of ping counts (number of times to send the ping request), and packet size (number of data bytes). Click **Stop Ping** to stop an ongoing ping search.

You can ping through a specific interface. Select the routing domain and specify the IP address with ping count, packet size, and select the virtual interface from the drop-down list.

Traceroute

To use **Traceroute** option, navigate to **Configuration > expand System Maintenance > Diagnostics** and select **Traceroute**.

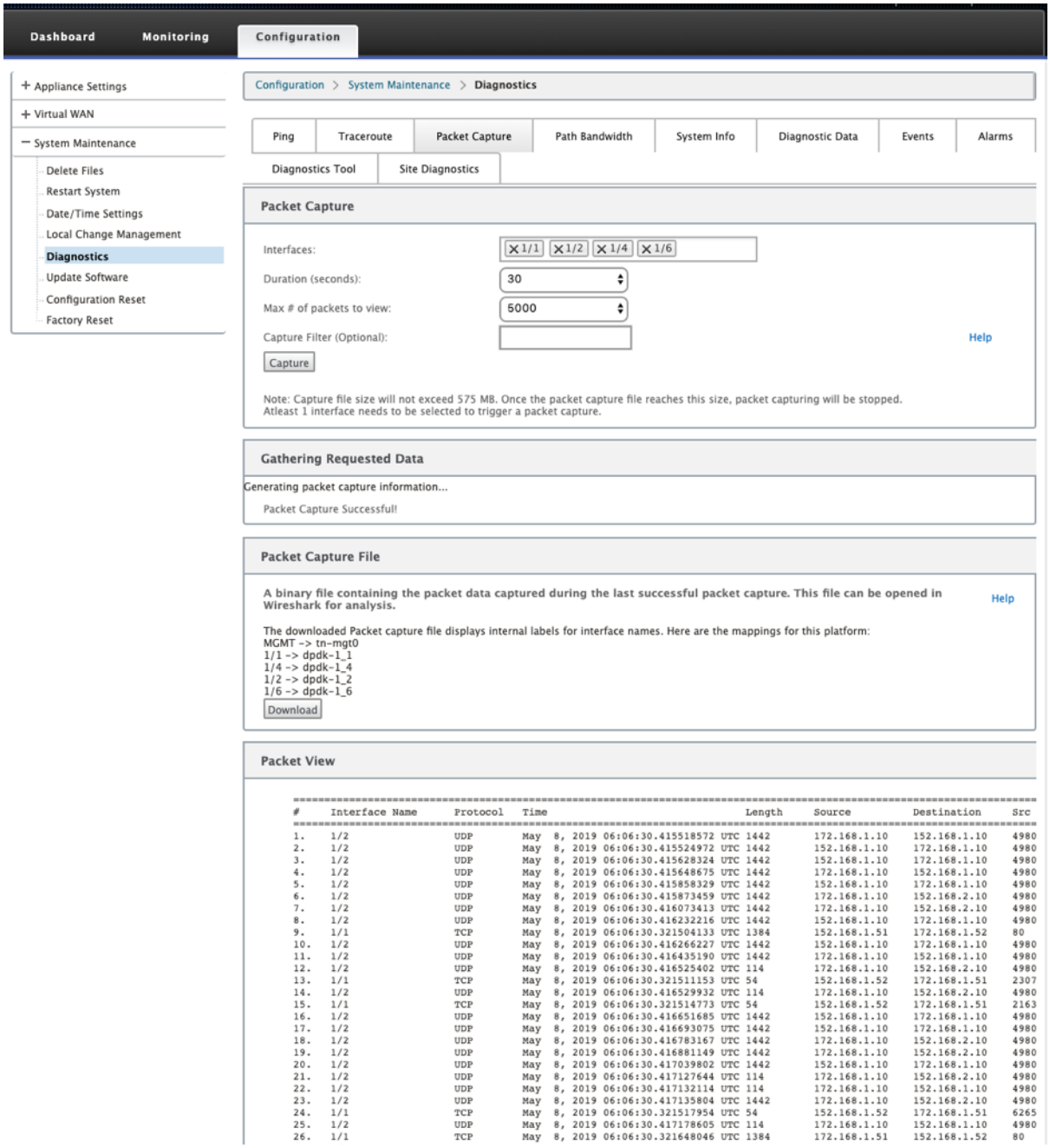


Traceroute helps to discover and show the path or route to a remote server. Use the **Traceroute** option as a debugging tool to detect the points of failure in a network.

Select a path from the drop-down list and click **Trace**. You can view the details under **Results** section.

Packet capture

You can use the **Packet Capture** option to intercept the real-time data packet that is traversing over the selected active interface present in the selected site. Packet capture helps you to analyze and troubleshoot the network issues.



Provide the following inputs for packet capture operation:

- **Interfaces** - Active interfaces are available for packet capture for the SD-WAN appliance. Select an interface or add interfaces from the drop-down list. At least one interface must be selected to trigger a packet capture.

> **Note:**
>
> The ability to run packet capture across all the interfaces at once helps to speed up the troubleshooting task.

- **Duration(seconds**) –Duration (in seconds) for how long the data have to be captured.
- **Max # of packets to view** - Maximum limit of packets to view in the packet capture result.
- **Capture Filter (Optional)** - The optional Capture Filter field accepts a filter string that is used to determine which packets are captured. Packets are compared to the filter string and if the comparison result is true, then the packet is captured. If the filter is empty, then all packets are captured. For more information, see Capture Filters.

Following are some examples of this capture filter:

- **Ether proto\ARP** - Captures only ARP packets
- **Ether proto\IP** - Captures only IPv4 packets
- **VLAN 100** - Captures only packets with a VLAN of 100
- **Host 10.40.10.20** - Captures only IPv4 packets to or from the host with the address 10.40.10.20
- **Net 10.40.10.0 Mask 255.255.255.0** - Captures only IPv4 packets in the 10.40.10.0/24 subnet
- **IP proto \ TCP** - Captures only IPv4/TCP packets
- **Port 80** - Captures only IP packets to or from port 80
- **Port range 20–30** - Captures only IP packets to or from ports 20 through 30

> **Note**
>
> The maximum capture file size limit is up to 575 MB. Once the packet capture file reaches this size, packet capturing is stopped.

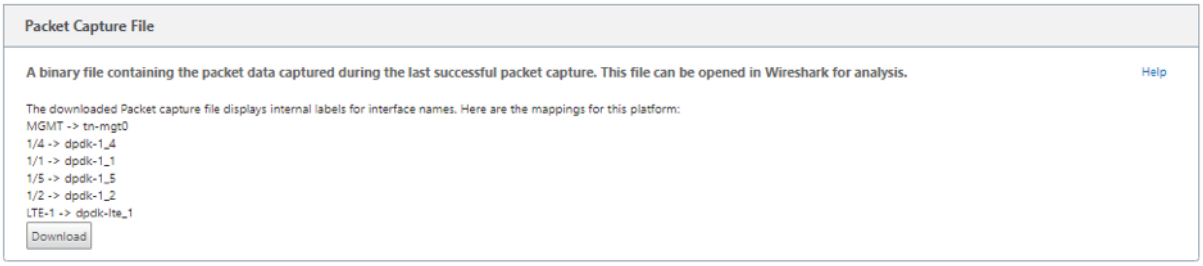
Click **Capture** to view the packet capture result. You can also download a binary file containing the packet data captured during the last successful packet capture.

Gathering requested data

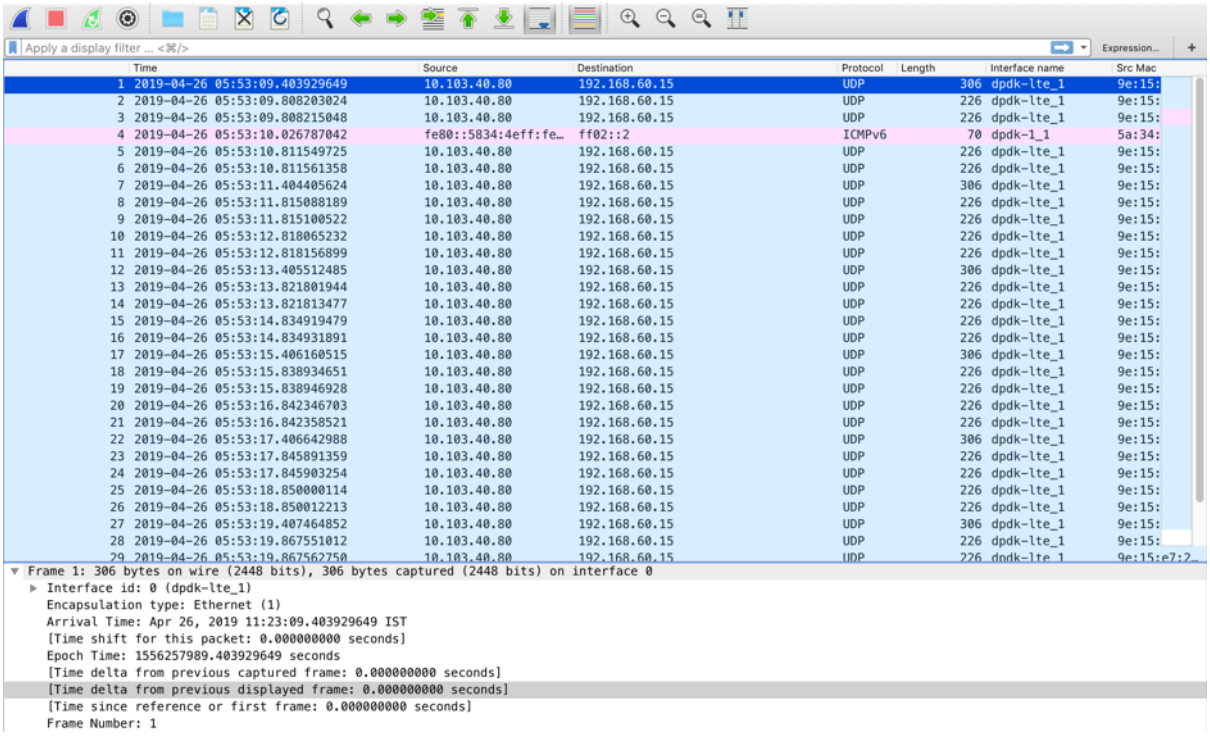
You can see the status of generating packet capture information (whether packet capture is successful or no packet capture) in this table.

Packet capture file

Packets are captured as a binary data during the last successful packet capture. You can download the binary file to analyze the packet information offline. The interfaces name is different in the downloaded file as compared to the GUI interface. To view the internal interface mapping, click the Help option.



You need **Wireshark** software 2.4.13 version or higher to open and read the binary file.

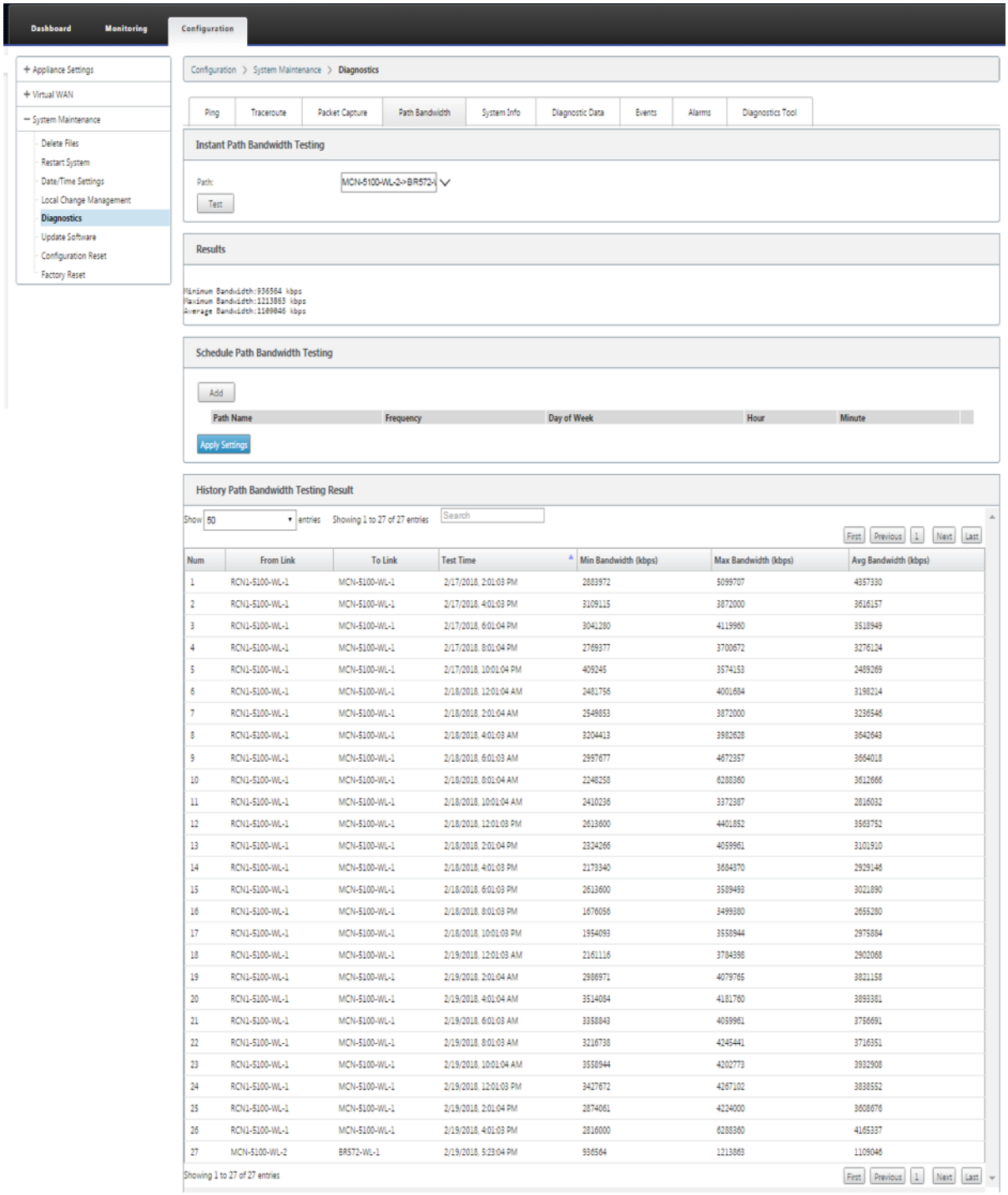


Packet view

If the packet capture file size is more, it takes more time to complete the rendering process for the packet view. In this case, it is recommended to download the file and use **Wireshark** for analysis instead of relying on the **Packet View** result.

Path bandwidth

To use the **Path Bandwidth** feature, navigate to **Configuration > expand System Maintenance > Diagnostics** and select **Path Bandwidth**.



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.

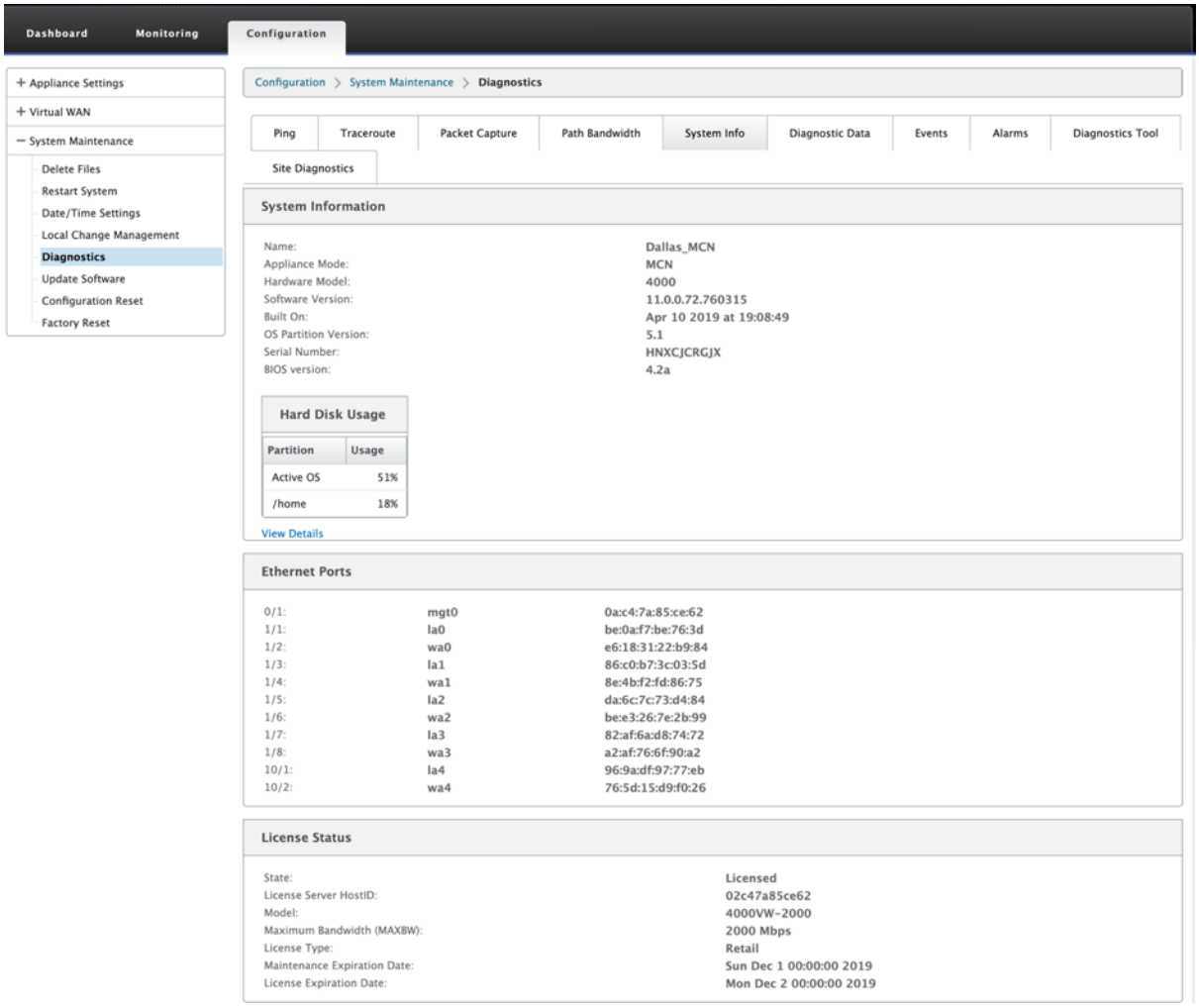
The **Path Bandwidth** feature is useful for demonstrating how much bandwidth is available between two locations during new and existing installations. Also for testing paths to determine the outcome of

setting and confirmation changes, such as adjusting DSCP tag settings or bandwidth Permitted Rates. For more information, see Active Bandwidth Testing.

System info

The **System Info** page provides the system information, ethernet ports detail, and license status.

To view the System Info, navigate to **Configuration > expand System Maintenance > Diagnostics** and select **System Info**.

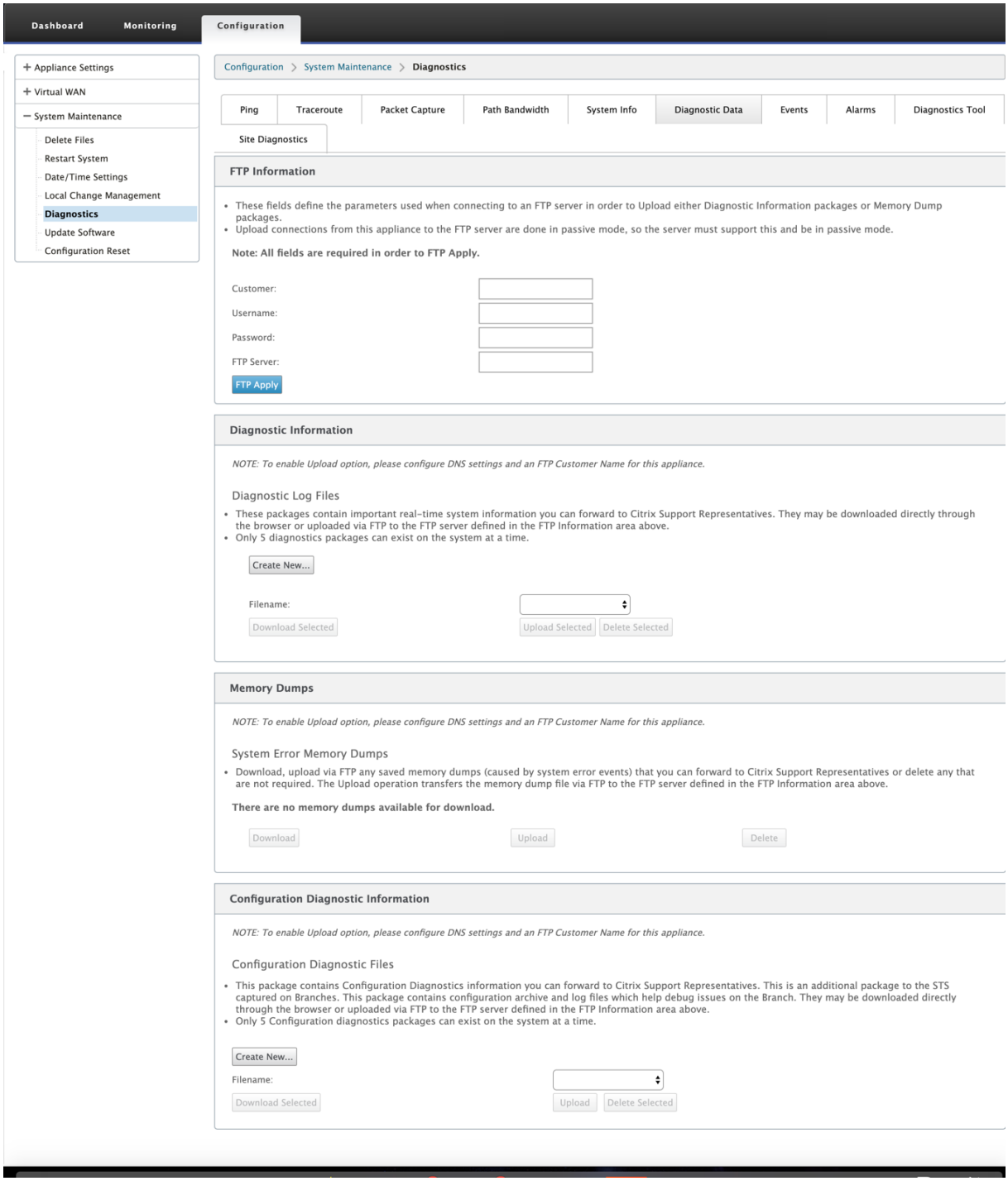


The **System Info** lists all the parameters that are not set to their defaults. This information is read-only. It is used by Support when some kind of misconfiguration is suspected. When you report a problem, you might be asked to check one or more values on this page.

Diagnostic data

Diagnostic Data allows you to generate the diagnostic data package for analysis by the Citrix Support team. You can download the **Diagnostics Log Files** package and share it with the Citrix Support team.

To view the **Diagnostic Data**, navigate to **Configuration > expand System Maintenance > Diagnostics** and select **Diagnostic Data**.



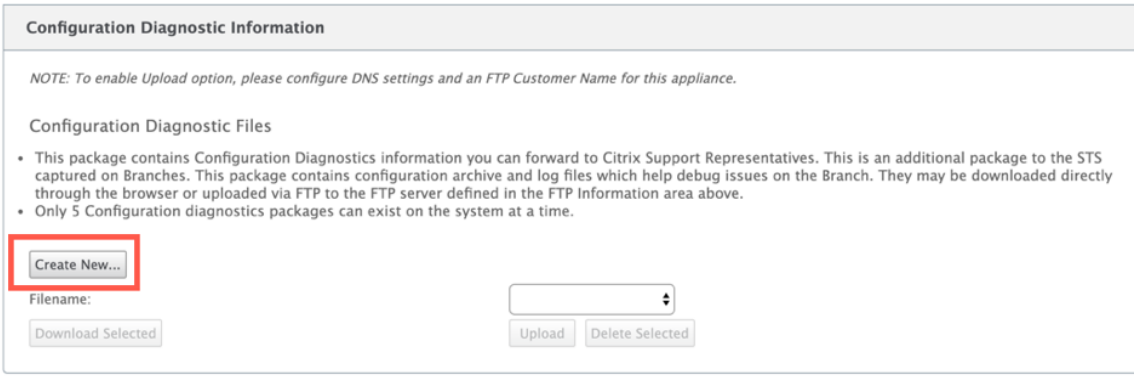
The **Diagnostics Data** includes:

- **FTP Information** –Provide the FTP parameters detail and click **FTP Apply**. The FTP information required to connect an FTP server to upload diagnostic information package.
- **Diagnostics Information** –The diagnostics log file package contains real-time system information that can be downloaded through the browser or uploaded via FTP to the FTP server.

> **Note:**
>
> Only five diagnostics packages can exist on the system at a time.

- **Configuration Diagnostic Information** - In the Citrix SD-WAN 11.0 release, Network configuration file will not be available in the Diagnostic information collected for the branch. For any support case, provide the diagnostic information of the branch and Configuration diagnostic information from the control node the branch is connected to.

  To collect configuration diagnostic information from the Control Node GUI, navigate to **Configuration > System Maintenance > Diagnostics > Diagnostic Data** > under **Configuration Diagnostic Information**, click **Create New**.



  On completion of the **Configuration Diagnostic Information** creation, click **Download Selected** file and provide this file to Citrix Support OR use the FTP apply operation available in the same page to FTP this file.

- **Memory Dumps** –You can download or upload the system error memory dumps file and share with the Citrix Support team. You can also delete the files if not required.

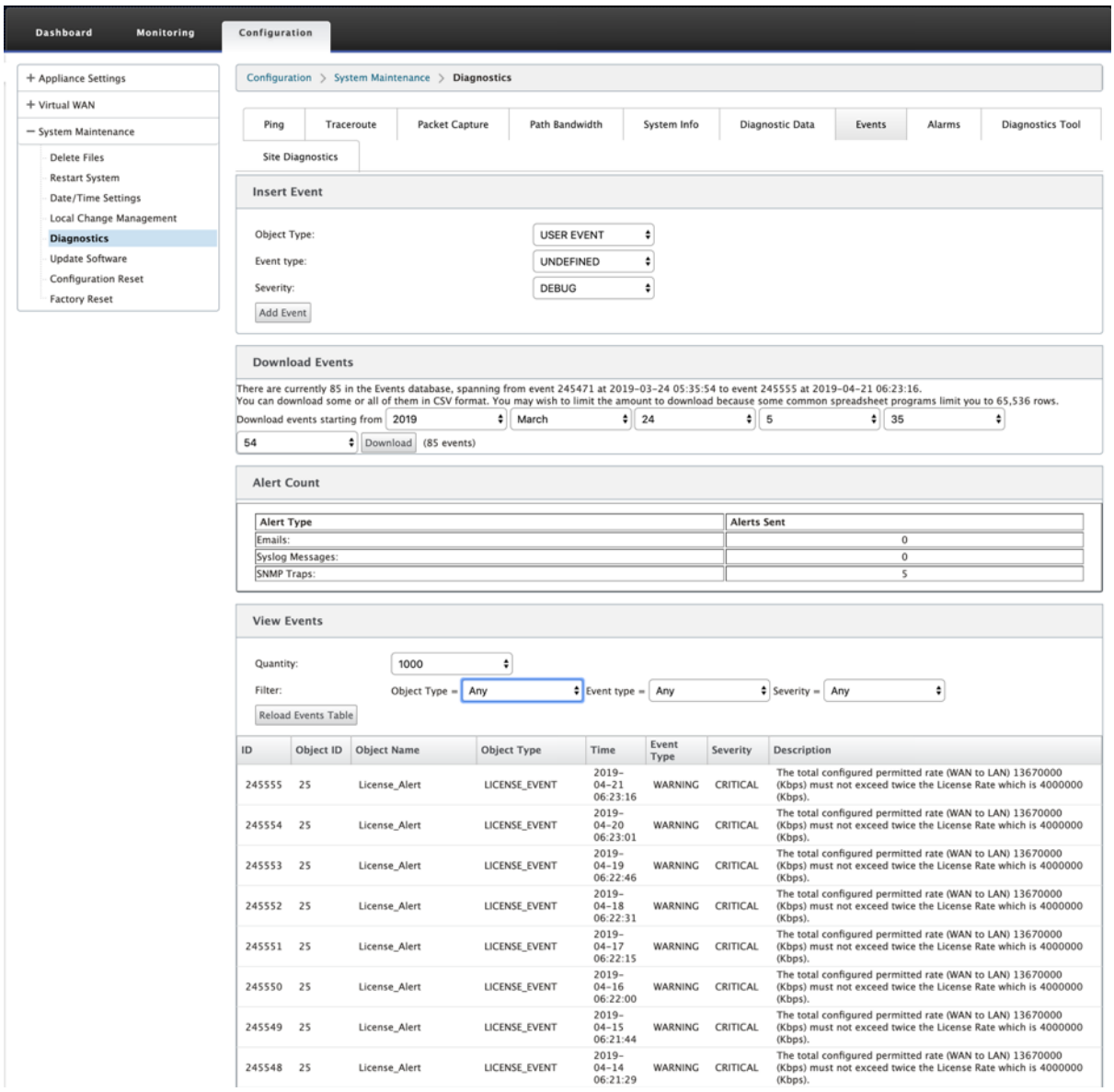
> **NOTE:**
>
> By default the **Upload** option is in disabled mode. To enable it, configure **DNS** settings and an **FTP Customer Name** for this appliance.

Events

Use the **Events** feature to add, monitor, and manage the events generated. It helps to identify events in real-time, that helps you address issues immediately and keep the Citrix SD-WAN appliance running effectively. You can download events in CSV format.

To add an event, select object type, event type, and severity from the drop-down list and click **Add Event**.

To view **Events**, navigate to **Configuration >** expand **System Maintenance > Diagnostics** and select **Events**.



You can configure Citrix SD-WAN to send event notifications for different event types as **Emails, SNMP Traps,** or **Syslog Messages**.

Once the email, SNMP, and syslog notification settings are configured, you can select the severity for different event types and select the mode (email, SNMP, syslog) to send event notifications.

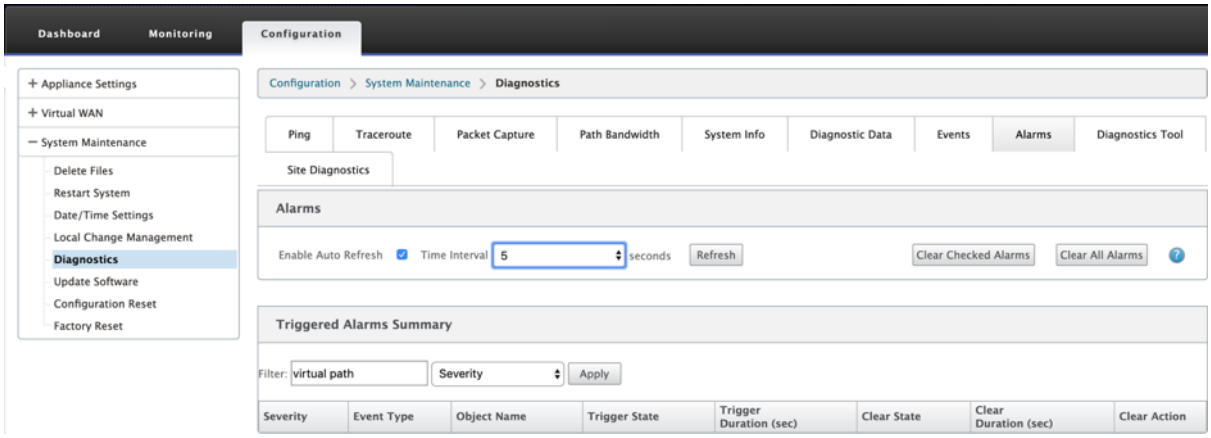
Notifications are generated for events equal to or above the specified severity level for the event type.

You can view the events detail under **View Events** table. The event details include the following information.

- **ID** –Event ID.
- **Object ID** - The ID of the object generating the event.
- **Object Name** - The name of the object generating the event.
- **Object Type** –The type of the object generating the event.
- **Time** –The time the event was generated.
- **Event Type** –The state of the object at the time of the event.
- **Severity** –The severity level of the event.
- **Description** –A text description of the event.

Alarms

You can view and clear the triggered alarm. To view **Alarms**, navigate to **Configuration > expand System Maintenance > Diagnostics** and select **Alarms**.



Select the alarms that you want to clear and click **Clear Checked Alarms** or click **Clear All Alarms** to clear all the alarms.

You can view the following summary of all the triggered alarms:

- **Severity** –The severity is displayed in the alerts sent when the alarm is triggered or cleared and in the triggered alarm summary.
- **Event Type** –The SD-WAN appliance can trigger alarms for particular subsystems or objects in the network. These alarms are called event types.
- **Object Name** –The name of the object generating the event.
- **Trigger State** –The event state that triggers an alarm for an Event Type.
- **Trigger Duration (sec)** –The duration in seconds determines how quickly the appliance triggers an alarm.
- **Clear State** –The event state that clears an alarm for an Event Type after the alarm is triggered.
- **Clear Duration (sec)** –The duration in seconds determines how long to wait before clearing an alarm.
- **Clear Action** –The action that is taken while clearing alarms.

Diagnostics tool

The **Diagnostic tool** is used to generate test traffic which allows you to troubleshoot network issues that might results 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 and 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.

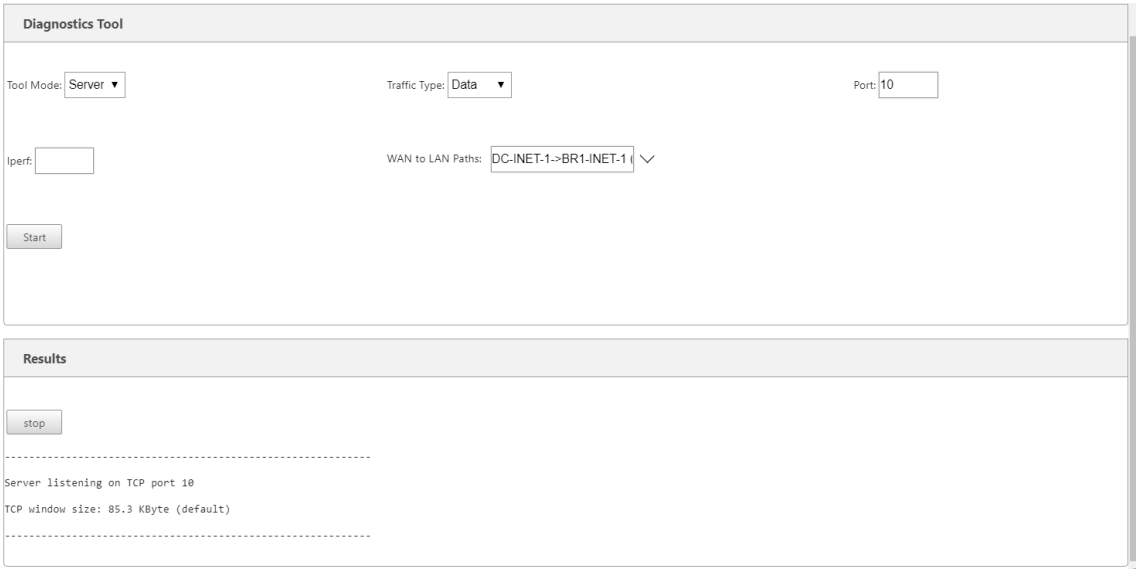
The diagnostic tool allows to generate the following two types of traffic:

- **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 then. Traffic is 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**.

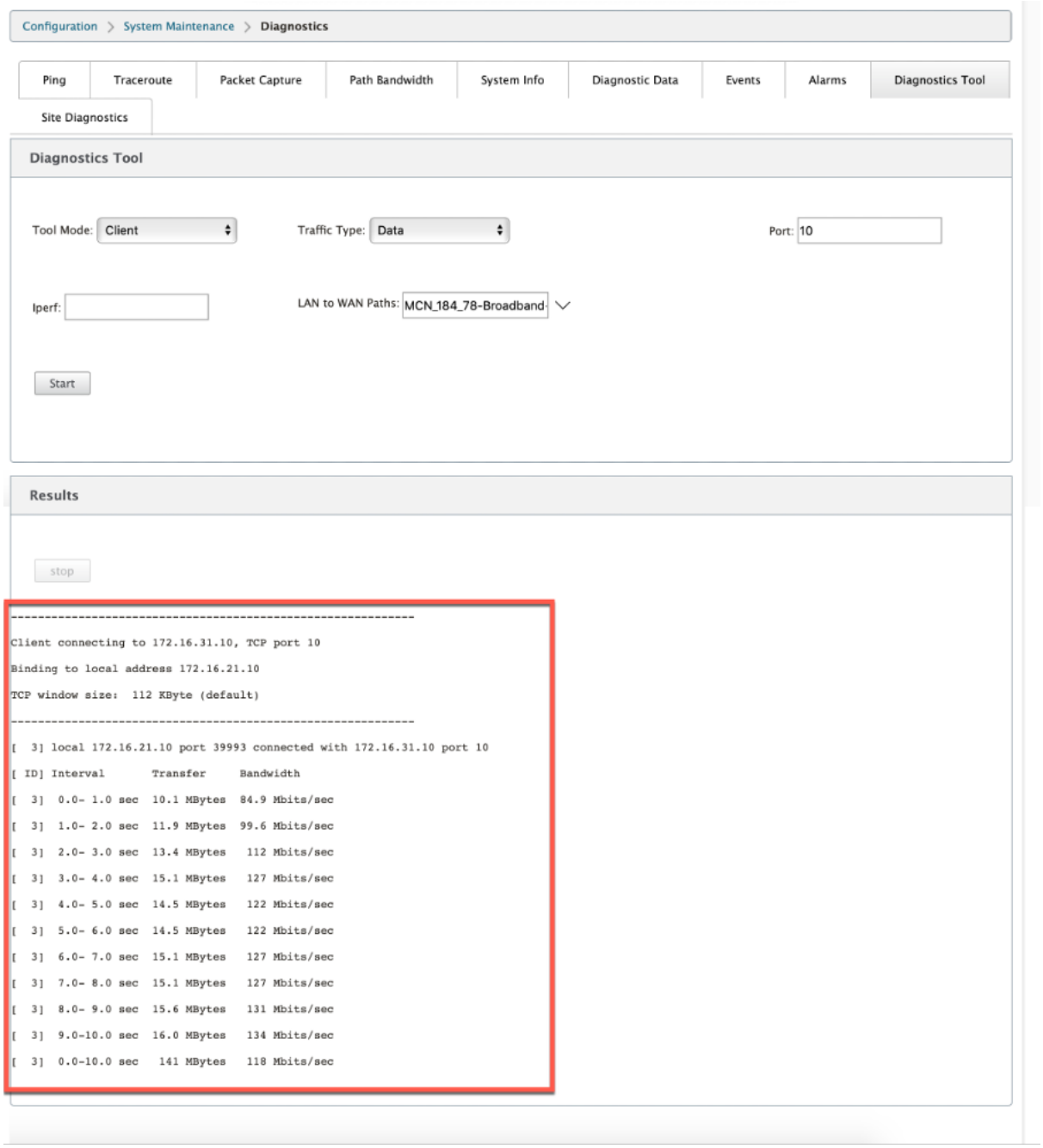


2. In the **Tool Mode** field, select **Server** on one appliance and select **Client** on the appliance residing on the remote end of the selected path.
3. In the **Traffic Type** field, select the type of diagnostic traffic, either **Control** or **Data**. Select the same traffic type on both the appliances.
4. In the **Port** field, specify the **TCP / UDP** port number on which the diagnostic traffic is 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.
   > - -i: Output interval in seconds.
   > - -t: Total duration of the test in seconds.

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.

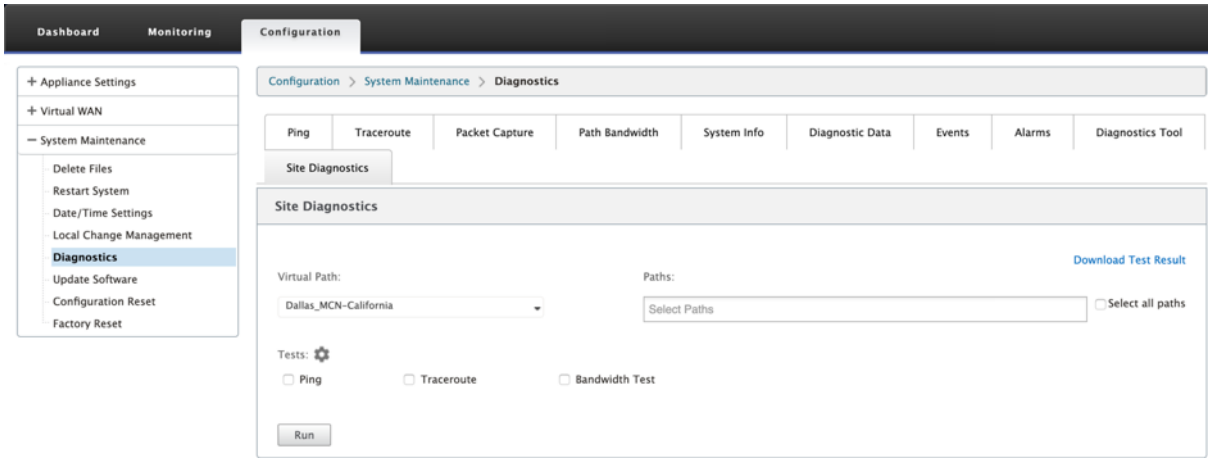
The result displays the mode (client or server) of the selected appliance and the TCP or UDP port on which the test is run. It periodically displays the data transferred and bandwidth utilized for the interval specified until the total duration of the test is reached.



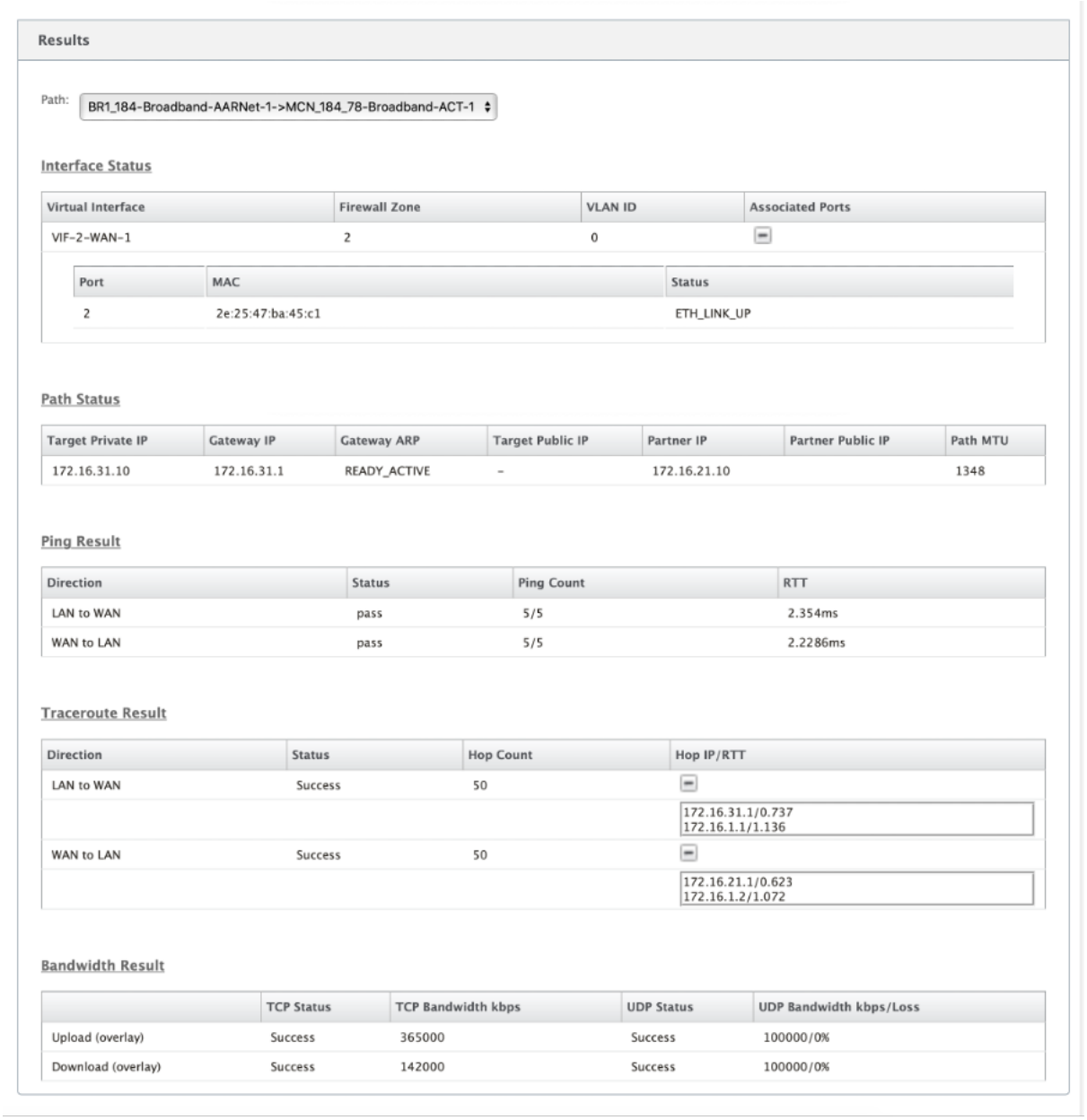
Site diagnostics

You can test the bandwidth usage, ping, and perform traceroute for the WAN links configured at different sites in the Citrix SD-WAN network. It provides information which helps in troubleshooting issues in the existing configuration.

To use **Site Diagnostics**, navigate to **Configuration >** expand **System Maintenance > Diagnostics** and select **Diagnostics Tool**.



- **Interface Status**: Provides the name of the interface, number of firewall zones associated with the interface, VLAN ID, and its associated ports.
- **Path Status**: Provides the details of target private IP, Gateway IP, Target Public IP, Partner IP, Partner Public IP addresses. It also displays the status of Gateway ARP and path MTU.
- **Ping Result**: Provides the direction, status, count (including the number of attempts and failures), and RTT of the ping.
- **Traceroute Result**: Provides the direction, status, number of hops, and IP address or RTT of the hops.
- **Bandwidth Result**: Provides the status of TCP and UDP along with the bandwidth used (in kbps) for the overlay and underlay network. Compared to UDP, the bandwidth used by TCP is more, because UDP is bandwidth based and therefore uses only the configured bandwidth. TCP is a ramp up protocol; based on underlying network configuration, usage might report higher bandwidth compared to configured bandwidth.



Results

Path: BR1_184-Broadband-AARNet-1->MCN_184_78-Broadband-ACT-1

Interface Status

Virtual Interface	Firewall Zone	VLAN ID	Associated Ports
VIF-2-WAN-1	2	0	

Port	MAC	Status
2	2e:25:47:ba:45:c1	ETH_LINK_UP

Path Status

Target Private IP	Gateway IP	Gateway ARP	Target Public IP	Partner IP	Partner Public IP	Path MTU
172.16.31.10	172.16.31.1	READY_ACTIVE	-	172.16.21.10		1348

Ping Result

Direction	Status	Ping Count	RTT
LAN to WAN	pass	5/5	2.354ms
WAN to LAN	pass	5/5	2.2286ms

Traceroute Result

Direction	Status	Hop Count	Hop IP/RTT
LAN to WAN	Success	50	
			172.16.31.1/0.737 172.16.1.1/1.136
WAN to LAN	Success	50	
			172.16.21.1/0.623 172.16.1.2/1.072

Bandwidth Result

	TCP Status	TCP Bandwidth kbps	UDP Status	UDP Bandwidth kbps/Loss
Upload (overlay)	Success	365000	Success	100000/0%
Download (overlay)	Success	142000	Success	100000/0%

Improved Path Mapping and Bandwidth Usage

March 12, 2021

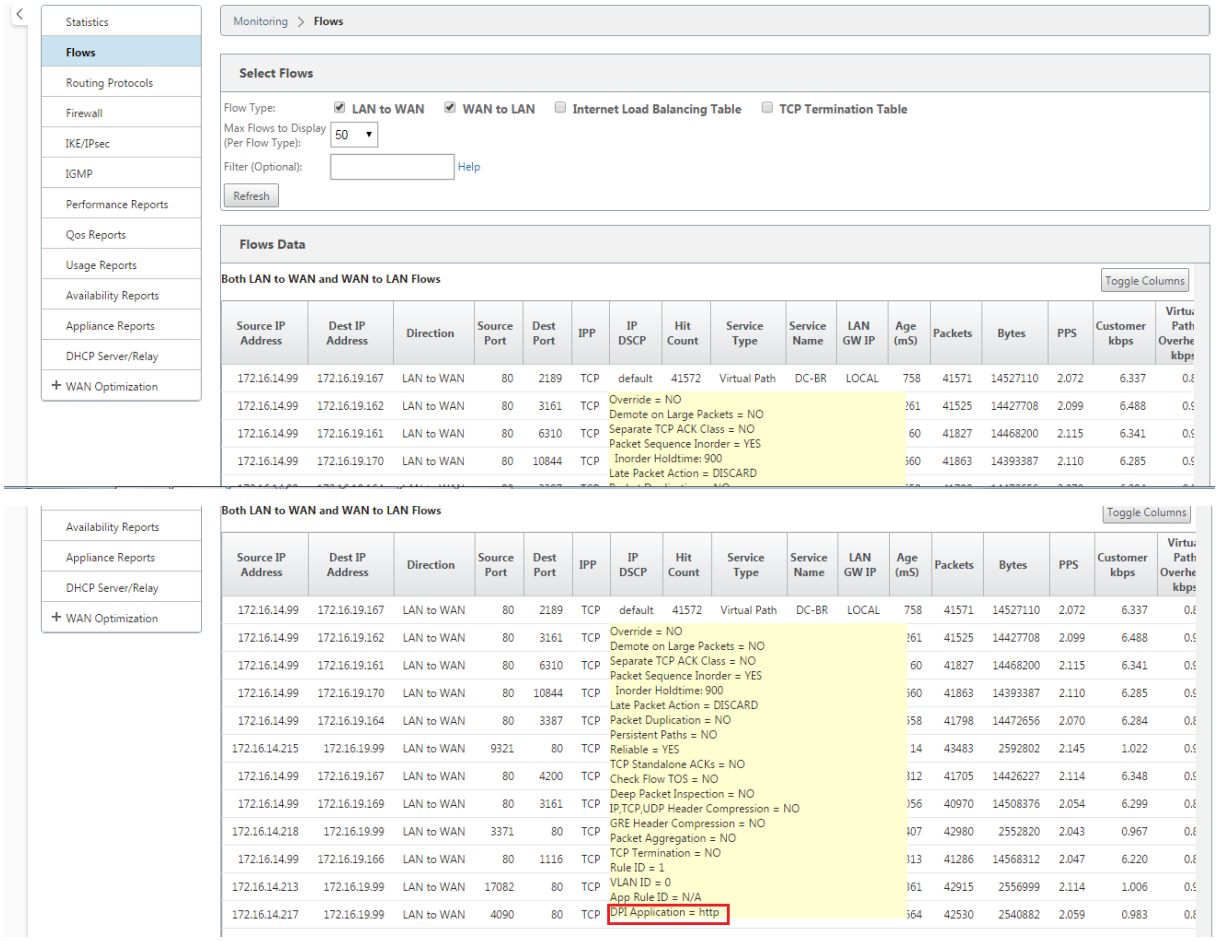
Path mapping and bandwidth usage enhancements are implemented in the Monitoring tab to show traffic flows. For instance, when only one virtual path is serving a network connection, and if that virtual path becomes inactive, a new best path is chosen and the initial path becomes the last best path. This 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 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.



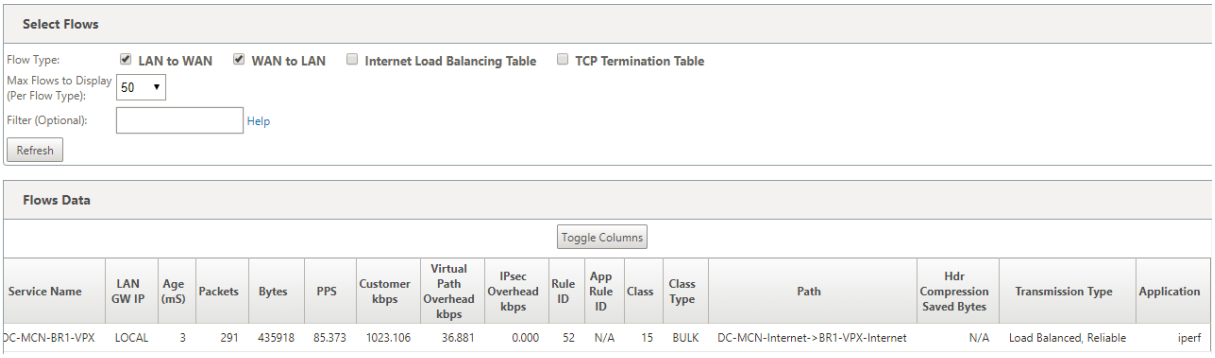
Monitoring Path information for traffic flow in SD-WAN GUI

It is possible that based on the incoming traffic rate demanding bandwidth, one or more paths are required to process the traffic.

For determining how path mapping is performed, review the following scenarios:

Load Balanced Transmission mode:

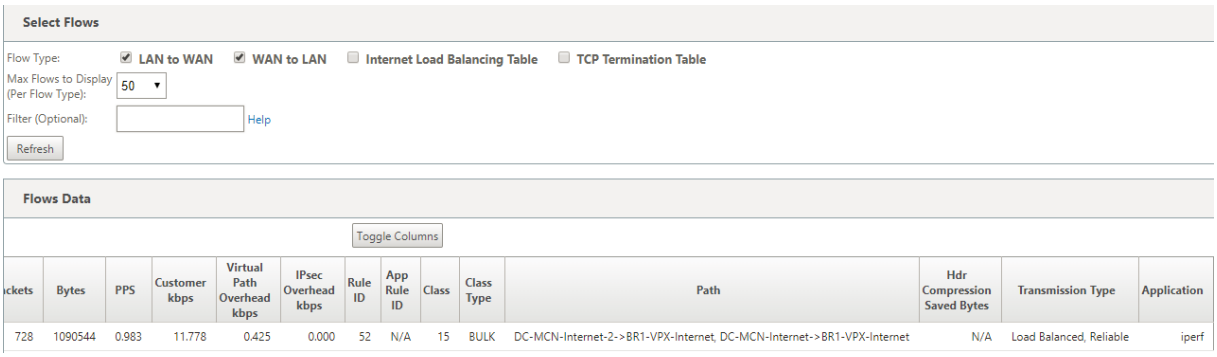
The following figure illustrates the scenario when traffic is initiated and all paths are good, one best path is chosen as bandwidth demand is enough to be served by one path. You notice that only one path **DC-MCN-Internet** -> **BR1-VPX-Internet** is chosen and the type of transmission type is displayed as **Load Balanced.**



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 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.

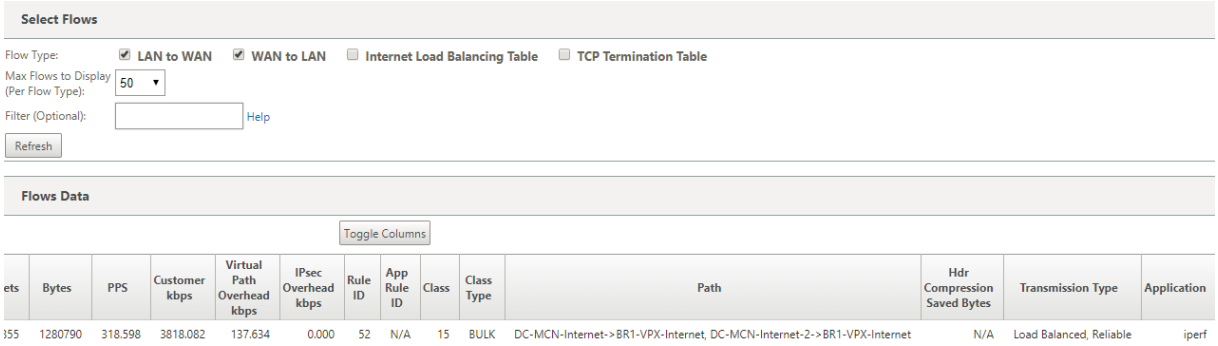


ckets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
728	1090544	0.983	11.778	0.425	0.000	52	N/A	15	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

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 when 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.

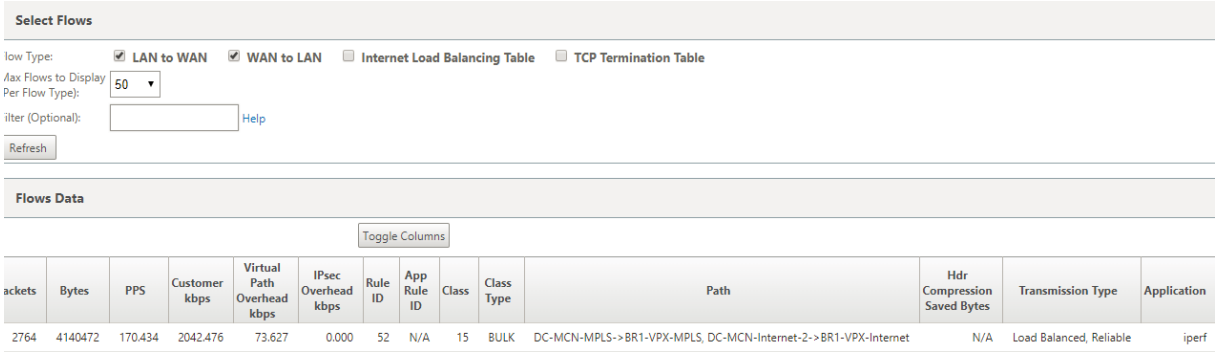
Observe **DC-MCN-Internet->BR1-VPX-Internet**, **DC-MCN-Internet2->BR1-VPX-Internet** being the two paths shown in the **Flows Data** table.

> **Note**
>
> As indicated, only max two paths in the flows table are displayed.



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 is 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.



Duplicate Transmit Mode

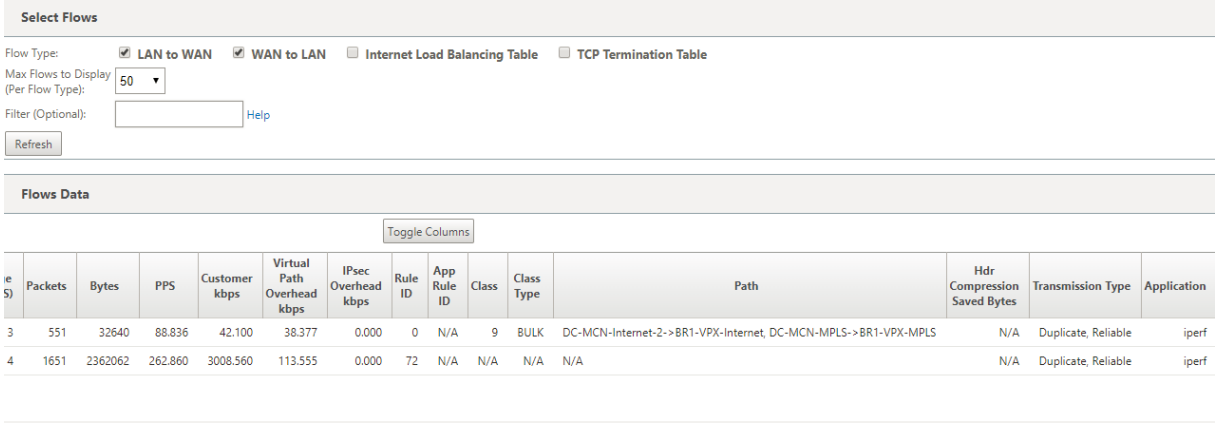
General packet duplication mode ensures that two paths are initially taken for processing packets of the same connection to ensure reliable delivery by duplicating packets across two separate paths.

For Path Mapping, you 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 wen 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

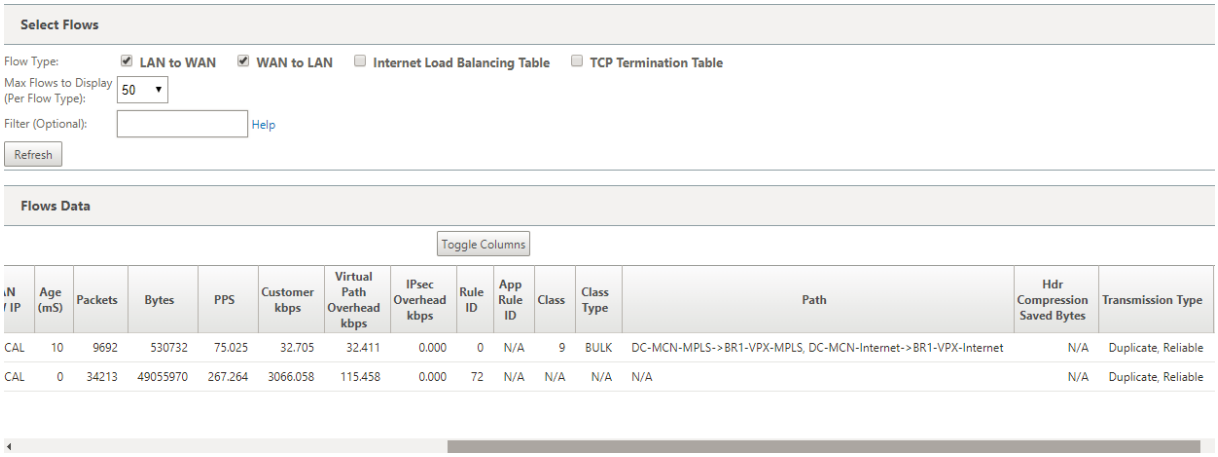
be provided by just one path, this mode will always duplicate traffic across two paths for reliable application delivery.

You 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**.



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
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
1651	2362062	262.860	3008.560	113.555	0.000	72	N/A	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 paths becomes inactive, another path is chosen and there still be two paths as part of the path section in the **Flows Data** table.



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
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
0	34213	49055970	267.264	3066.058	115.458	0.000	72	N/A	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 serves it all. Currently there is only one best path which is **DC-MCN-Internet->BR1-VPX-Internet.**

Flows Data

Toggle Columns

rvice 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
ual Path	DC-MCN-BR1-VPX	LOCAL	662	3	4494	1.127	13.511	0.487	0.000	4	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

The following figure illustrates that if the path **DC-MCN-Internet->BR1-VPX-Internet** becomes latency prone or is disabled, you 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 shows **DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet**.

Flows Data

Toggle Columns

AN / 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
OCAL	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 displays 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 stay persistent as long as there is no path latency impedance crossing (50 ms). 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 makes 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

Troubleshooting Management IP

March 12, 2021

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 Premium (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 servers 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 servers 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 reinitiate DHCP discovery protocol, if current DHCP server is not reachable.
  - Appliances 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 Citrix SD-WAN appliances (physical/virtual). This allows appliances to have predictable management IP address.

Session-based HTTP Notifications

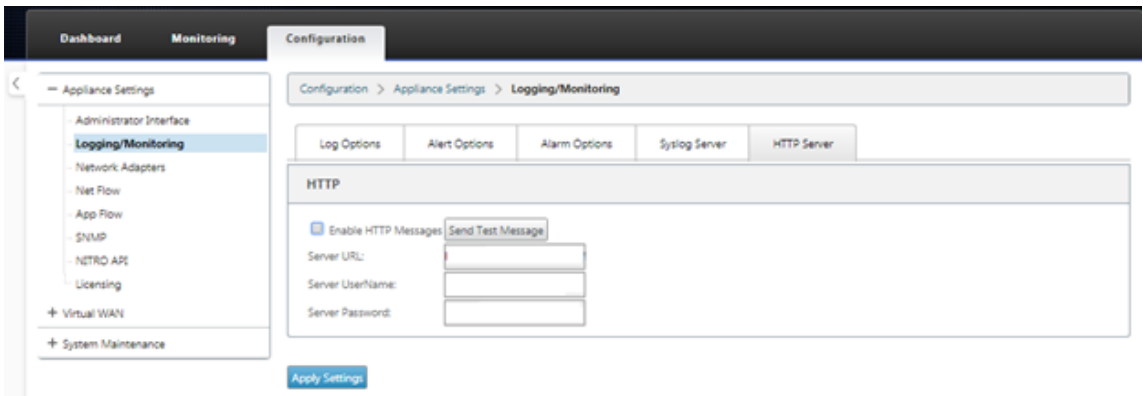
March 12, 2021

You can now configure event and alarm reporting for generic HTTP POST API service requests in the Citrix SD-WAN appliance GUI. The HTTP alarm and event notification configuration are similar to the email and SNMP events for events and alarms supported in SD-WAN.

The session based HTTP Post notification is sent to an external service; such as Service Now. The event notifications for HTTP server can be configured in the Citrix SD-WAN appliance GUI and Citrix SD-WAN Center.

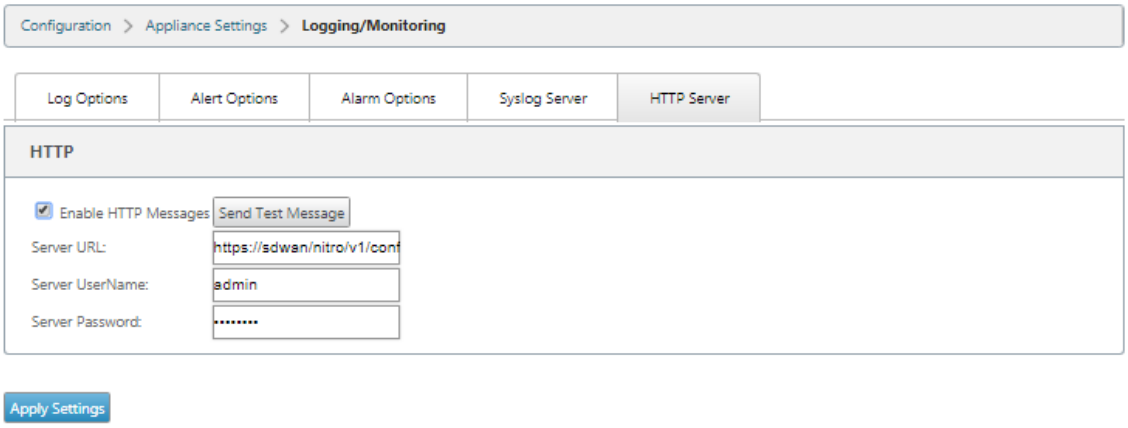
To configure HTTP POST notifications in the Citrix SD-WAN appliance GUI:

1. Navigate to **Configuration** > **Logging/Monitoring** > **HTTP Server**.



2. Click **Enable HTTP Messages**.

3. Enter **Server URL** of the HTTP server for which you want to receive notifications from. Enter the **Server UserName** and **Server Password**.

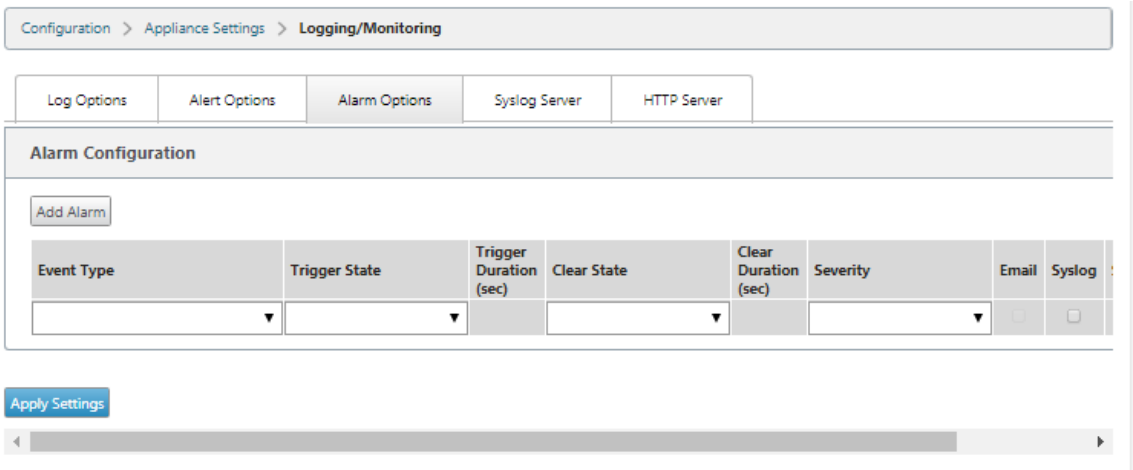


4. Click **Apply Settings**. The page refreshes after the HTTP server notifications settings are applied.

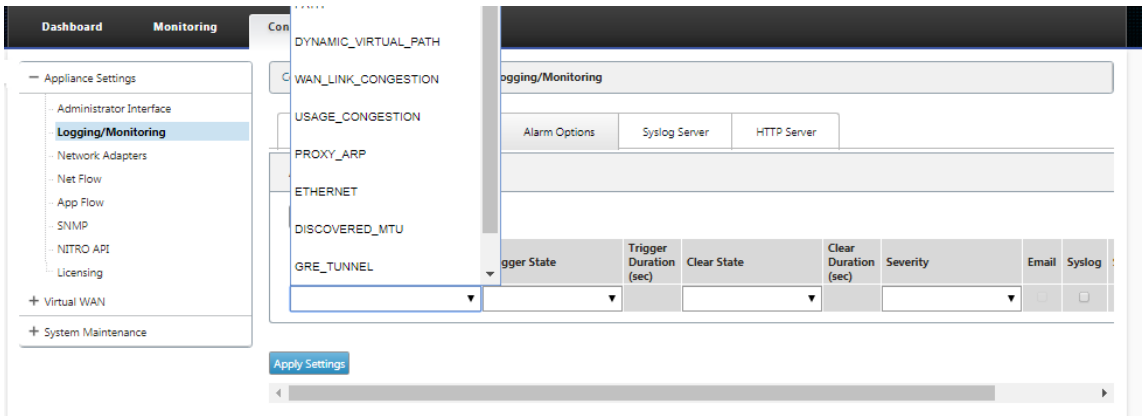
> **Note**
>
> Use the **Send Test Message** option to verify that the HTTP server connection is successful.

To add Alarm notification for HTTP server session:

1. In the **Logging/Monitoring** page, go to the **Alarm Options** tab page.
2. Click **Add Alarm**.

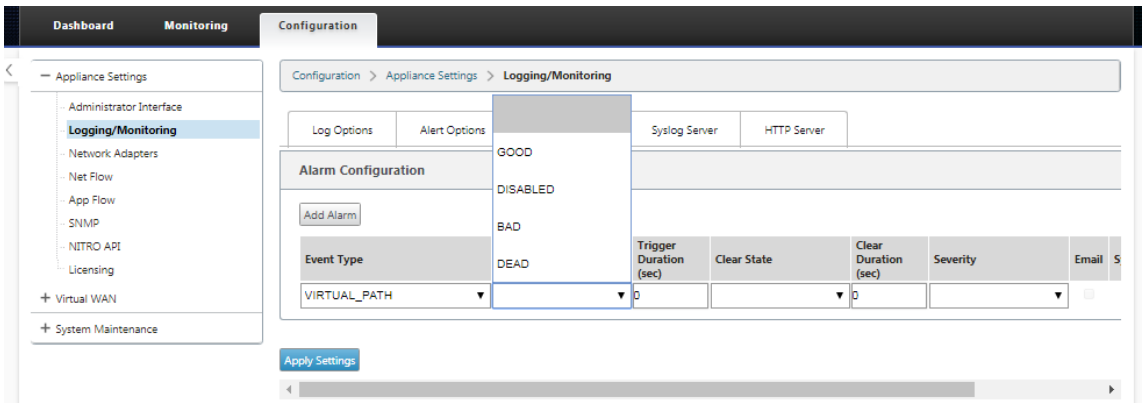


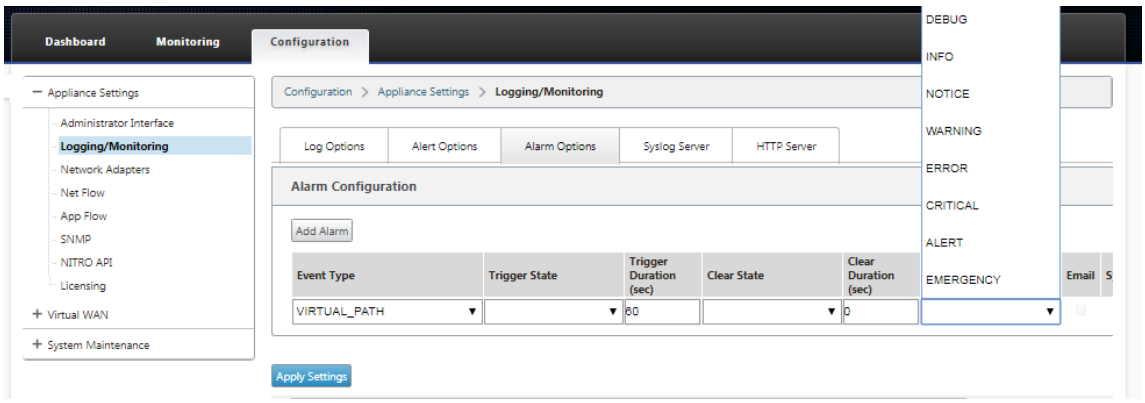
3. Select an **Event Type** from the drop-down list.



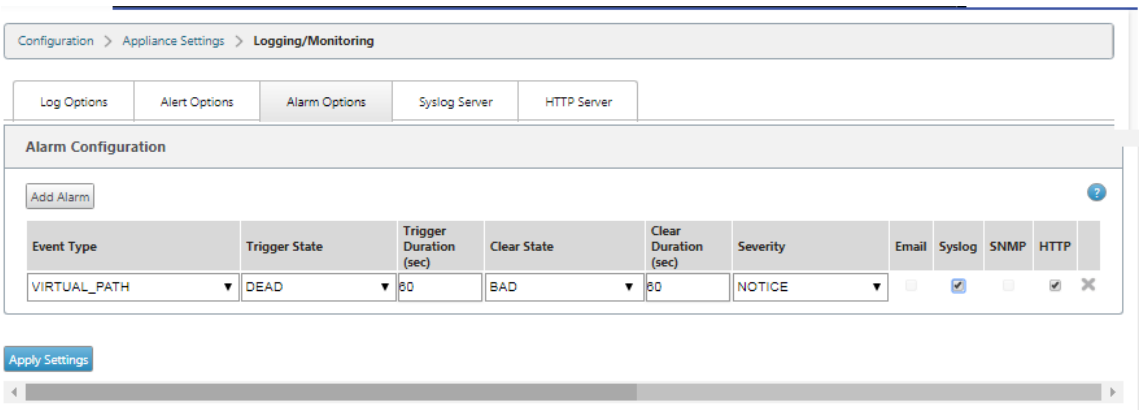
4. Select following alarm notification states for the chosen **Event Type**. The trigger state and clear state change according to the selected Event Type.

   - Trigger State –GOOD, DISABLED, BAD, DEAD
   - Trigger Duration –time in seconds
   - Clear State - GOOD, DISABLED, BAD, DEAD
   - Clear Duration –time in seconds
   - Severity –DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, EVENT, EMERGENCY





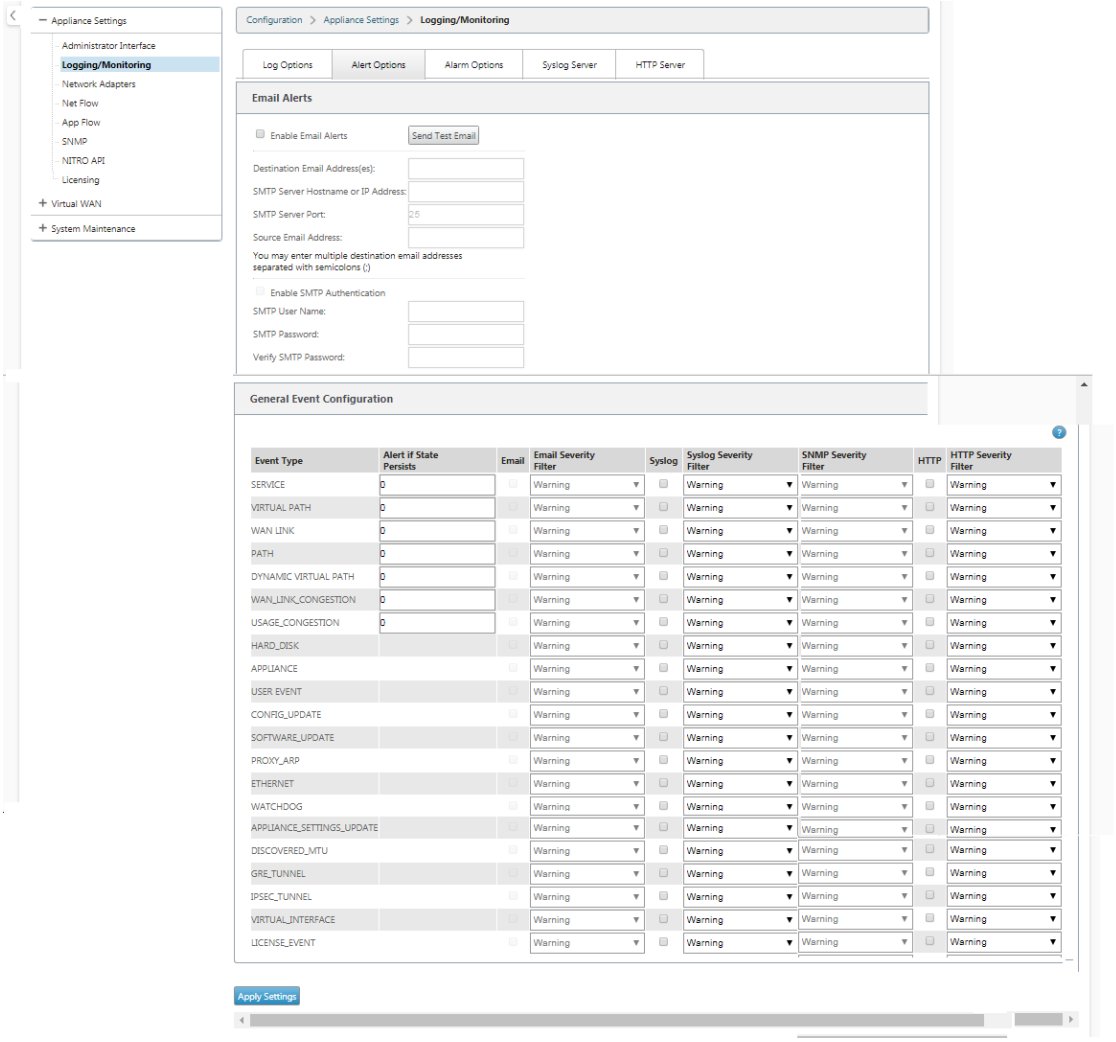
5. Select the **Syslog** and **HTTP** checkboxes to receive notifications specific to the Syslog and HTTP server events. Click **Apply Settings**.



To configure event options:

Go to the **Alert Options** tab page. Under **General Event Configuration** page; select the HTTP server notification filter for an **Event Type** and click **Apply Settings**.

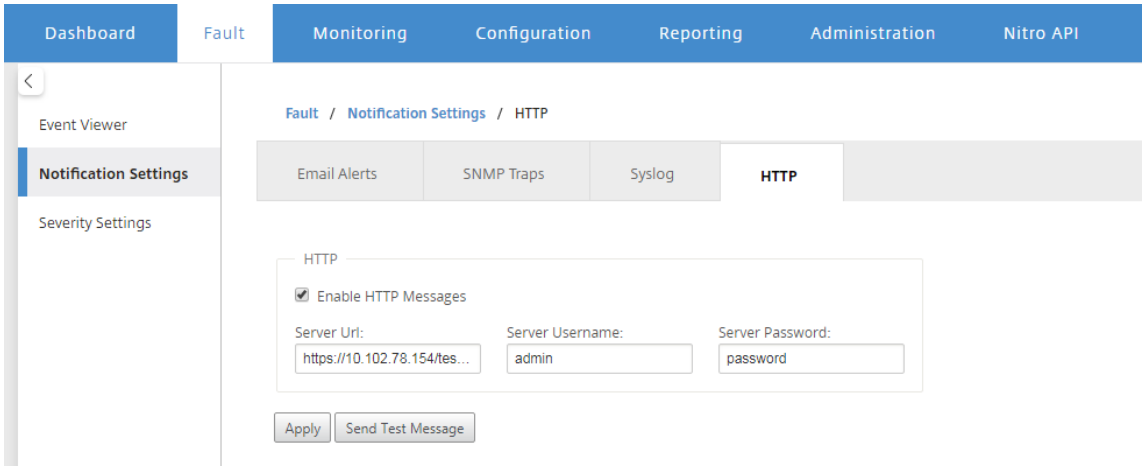
- HTTP
- HTTP Severity Filter



Configure HTTP Notifications in Citrix SD-WAN Center

To configure HTTP notifications:

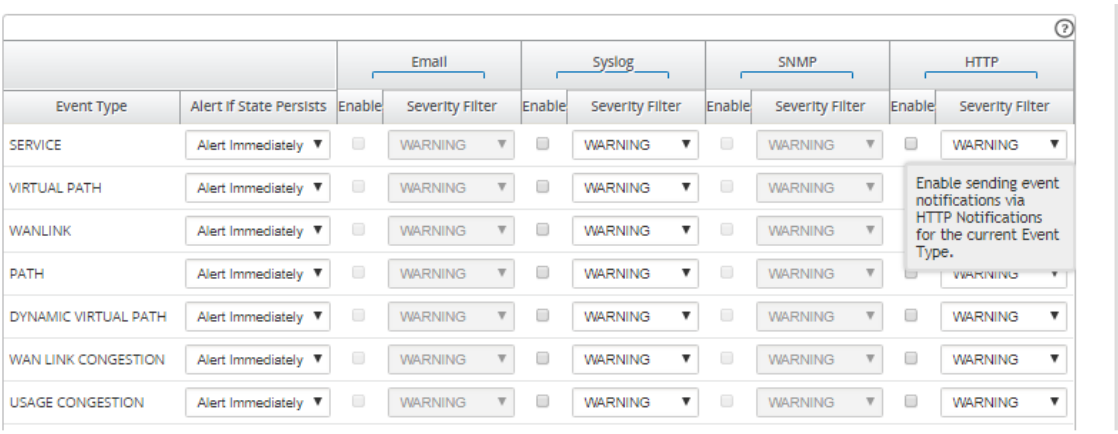
1. Navigate to **Fault** > **Notification Settings** > **HTTP**.



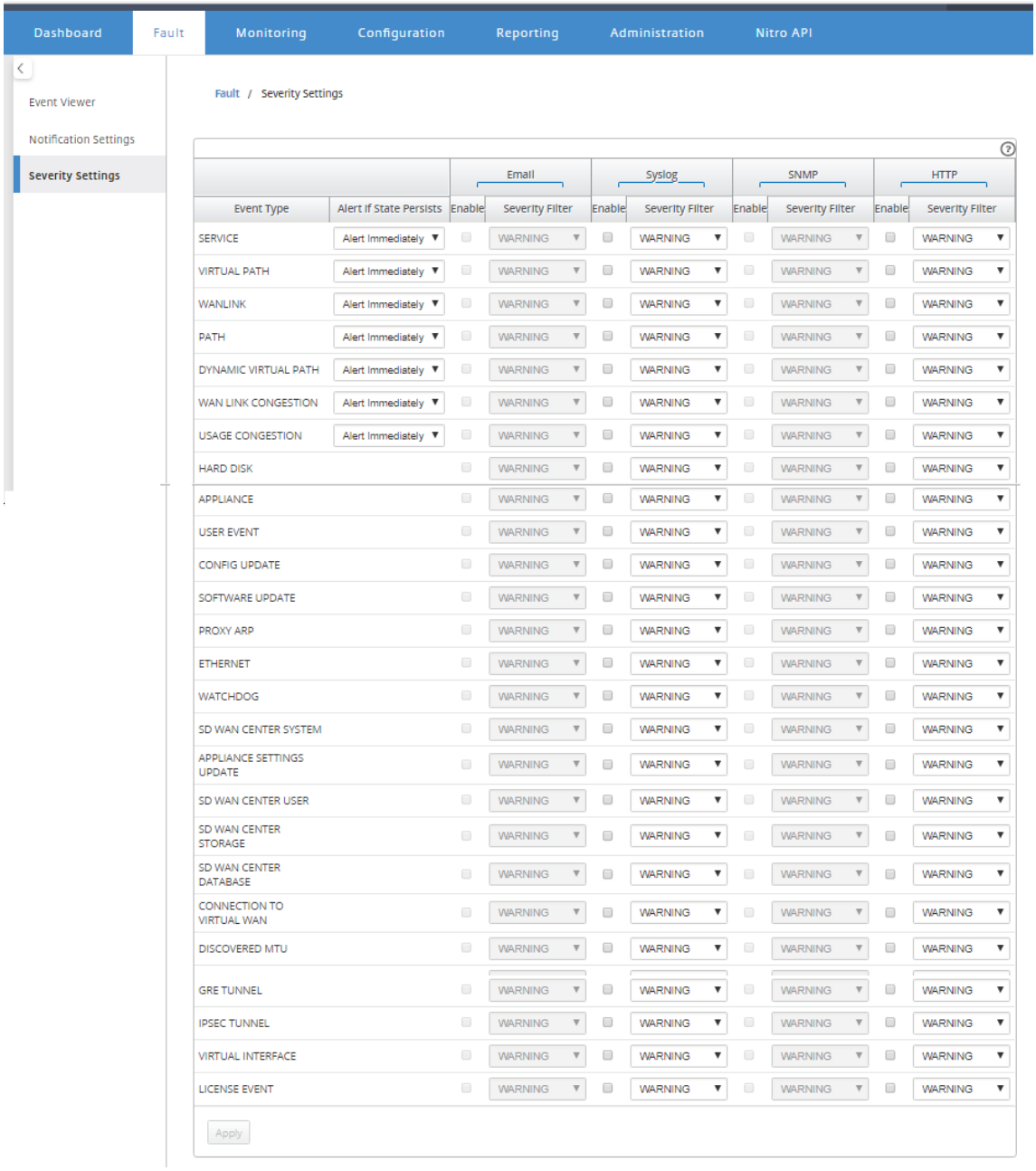
2. Enter the **Server URL**, **Server UserName**, and **Server Password** for the HTTP server.
3. Click **Apply**

To configure severity settings:

1. Go to the **Severity Settings** page. Click **Enable** to start monitoring HTTP notifications for a chosen Event Type.



2. You can choose to monitor Email, Syslog, SNMP, and HTTP event notifications for the following Event Types. Click **Apply**.



Active bandwidth testing

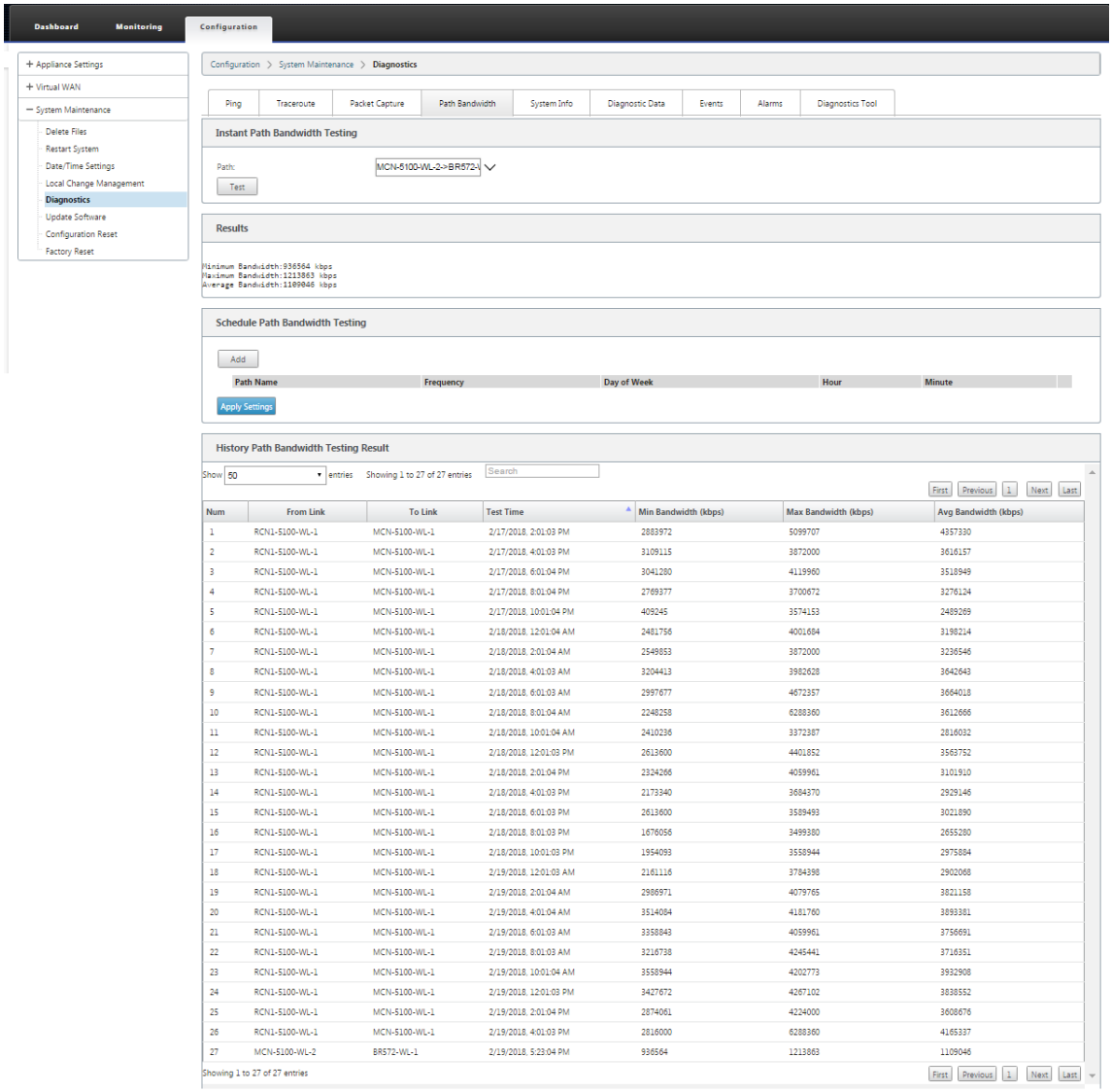
March 12, 2021

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.

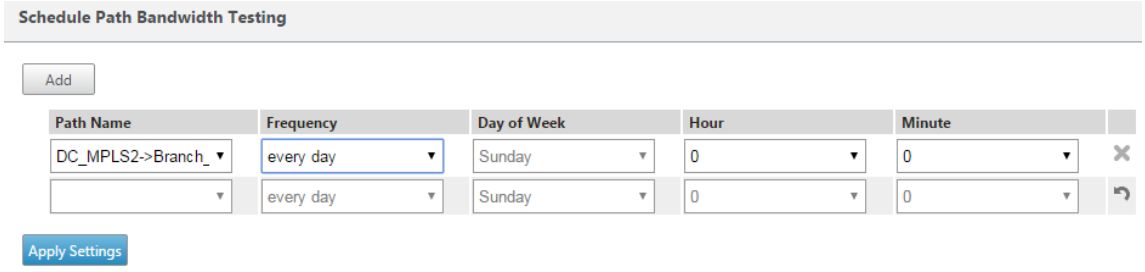
To use the active bandwidth testing feature:

1. Navigate to **System Maintenance** > **Diagnostics** > **Path Bandwidth**.
2. Select the desired **Path** and click **Test**.

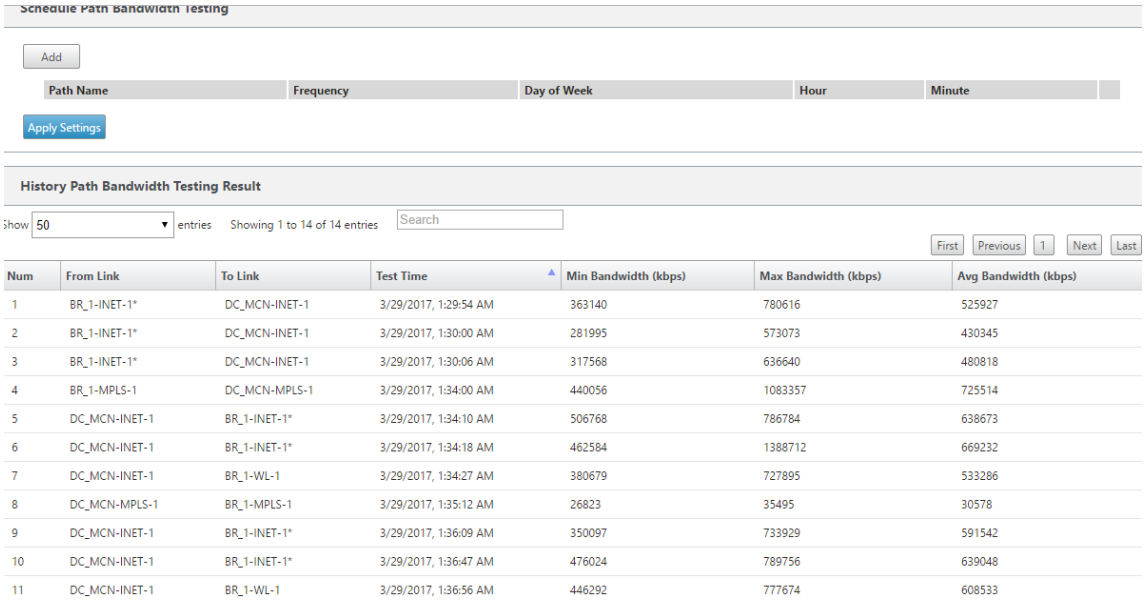


The output displays average bandwidth used as value to set as the permitted rate for the WAN Link minimum and maximum bandwidth results of the test. Along with the ability to test the bandwidth, you can now change the configuration file to use the learned bandwidth. This is accomplished through the Auto Learn option is under **Site** > [Site Name] > **WAN Links**> [WAN Link Name] > **Settings** and if enabled, the system uses the learned bandwidth.

You can also schedule recurring tests of path bandwidth in weekly, daily, or hourly intervals.



> **Note**
>
> A history of the path bandwidth testing results is displayed at the bottom of this page and results are archived every seven days.



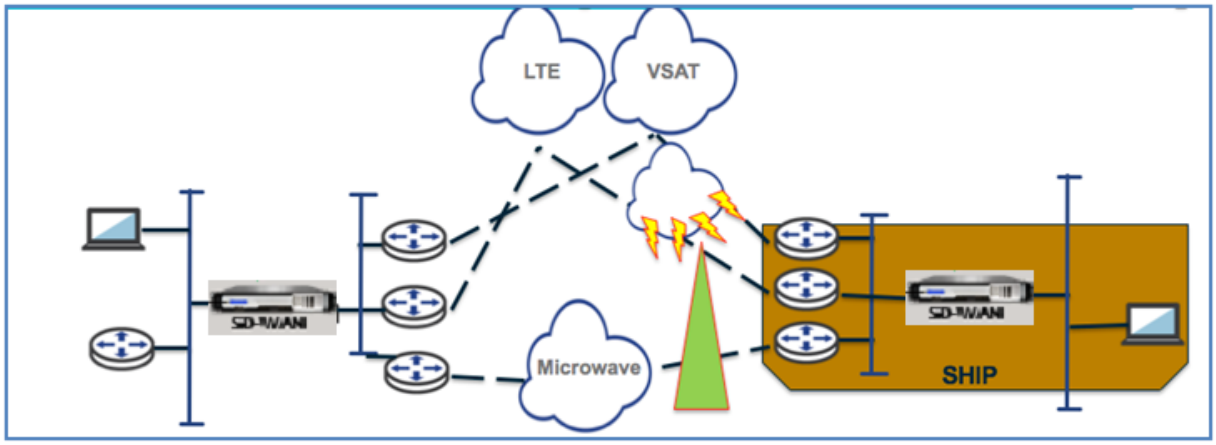
Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:29:54 AM	363140	780616	525927
2	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:00 AM	281995	573073	430345
3	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:06 AM	317568	636640	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

March 12, 2021

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 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.

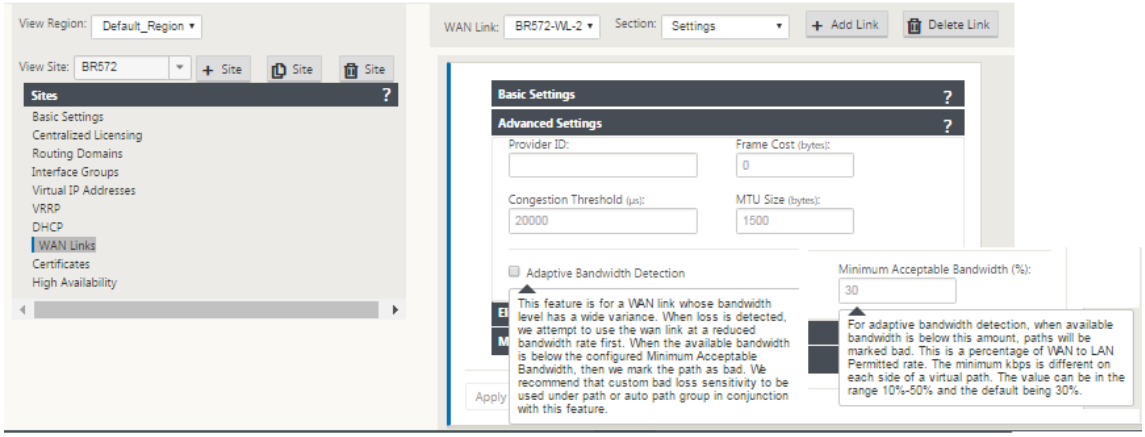
- Greater bandwidth reliability (Over VSAT, Microwave, 3G/4G, and LTE)
- Greater predictability of adaptive bandwidth over user configured settings



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**.



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 Apply

Show 100 entries Showing 1 to 4 of 4 entries First Previous 1 Next Last

WAN Link	Service	Direction	Packets	Packets KB	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Recv	5437658	3467411.62	0	0	0	25	NO
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Send	7598365	559484464	118	8.39	12.69	5905	N/A
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Recv	58537274	41745181.34	6562	5203.86	7872.71	8105	NO
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Send	20640095	1497892080	229	17.25	26.1	5880	N/A

Showing 1 to 4 of 4 entries First Previous 1 Next Last

Best practices

March 12, 2021

The following topics provide the best practices to be followed when the Citrix SD-WAN solution is being designed, planned, and executed in your network.

Security

Routing

QoS

WAN links

Security

March 12, 2021

This article outlines security best practices for the Citrix SD-WAN solution. It provides general security guidance for Citrix SD-WAN deployments.

Citrix 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 Citrix SD-WAN Appliances in a Secure Server Room - The appliance or server on which Citrix 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 is monitored by CCTV that continuously records all activity for auditing purposes. If 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 uninterruptible power supply (UPS).

Appliance security

For appliance security, secure the operating system of any server hosting a Citrix SD-WAN virtual appliance (VPX), perform remote software updates, and following secure lifecycle management practices:

- Secure the Operating System of Server Hosting a Citrix SD-WAN VPX Appliance - A Citrix 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. Also, 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-reminisce 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 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.

Citrix 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. Go to, **Configuration> Appliance Settings> Administrator Interface** in the SD-WAN appliance GUI.

User accounts:

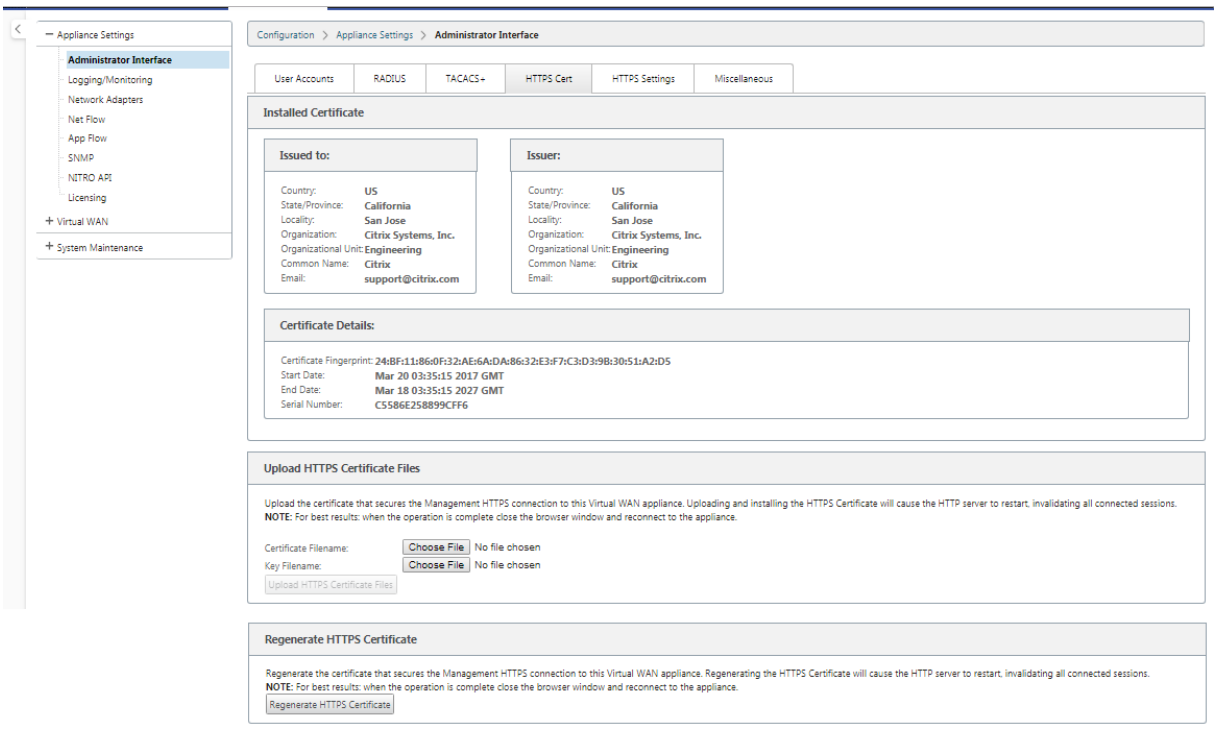
- Change local user password
- Manage users

HTTPS Certs:

- Certificate
- Key

Miscellaneous:

- Web Console Timeout



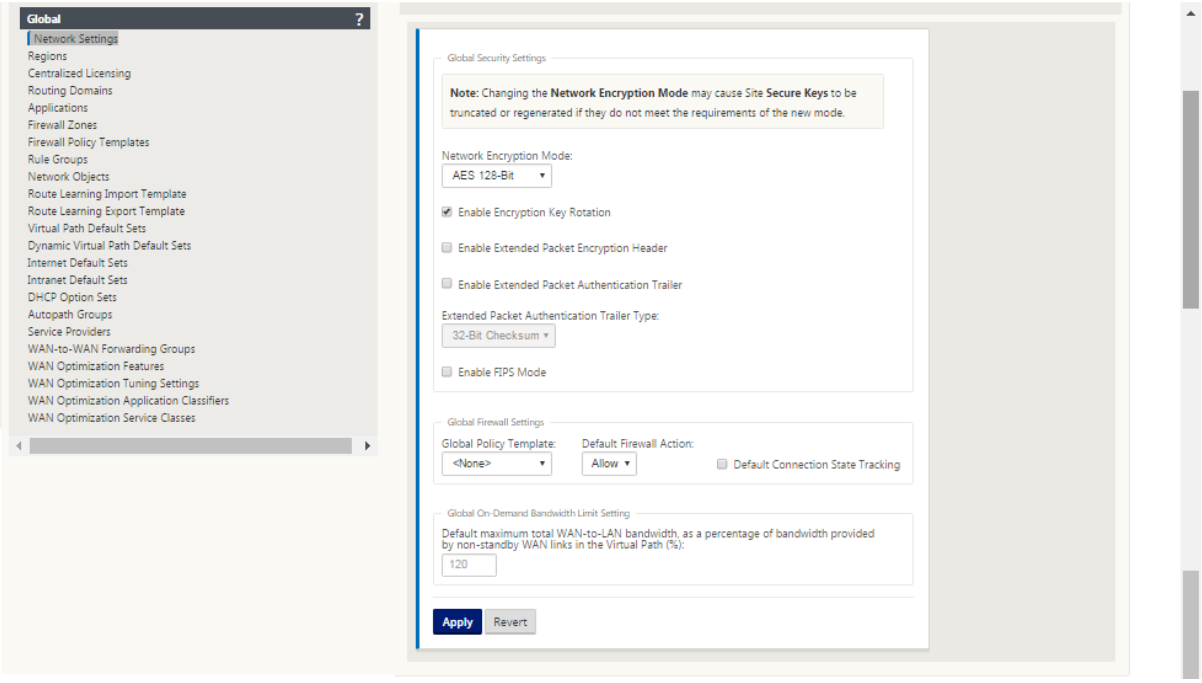
Configuration Editor > **Global** > **Network Settings**

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 more 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 (that is, 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 serves as a random initialization vector, deterministic only with the encryption key. This randomizes the output of the encryption, providing strong message indistinguishably. Keep in mind that when enabled this option increases 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 increases packet overhead.

Firewall Security

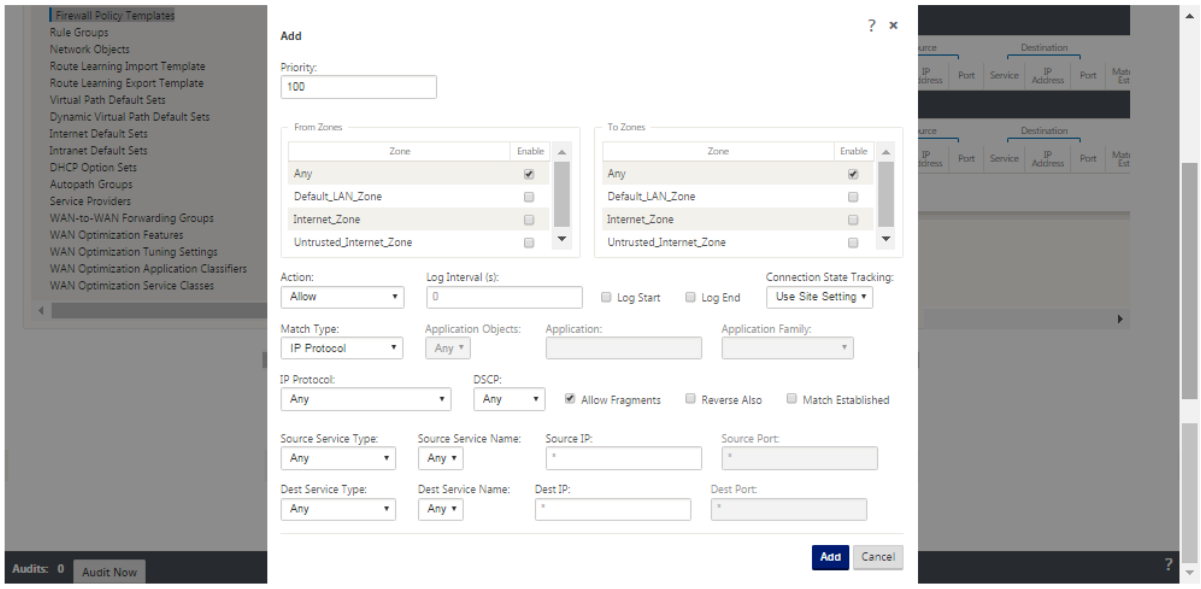
The recommended Firewall configuration is with a default Firewall action as deny all at first, then add exceptions. Prior to adding any rules, document and review the purpose of the firewall rule. Use Stateful inspection and Application level inspection where possible. Simplify rules and eliminate redundant 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 are 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 Citrix 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 is sent 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.

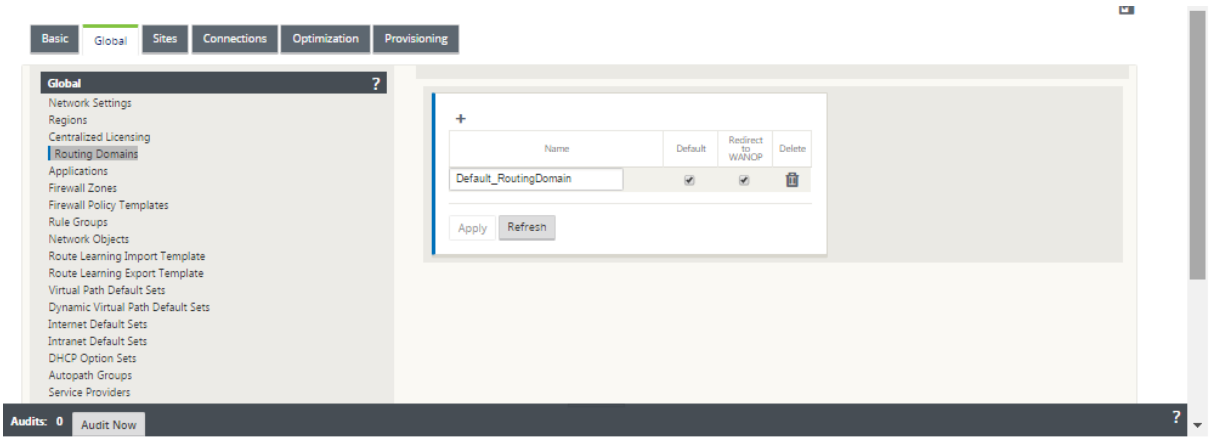
Configuration Editor > **Global**

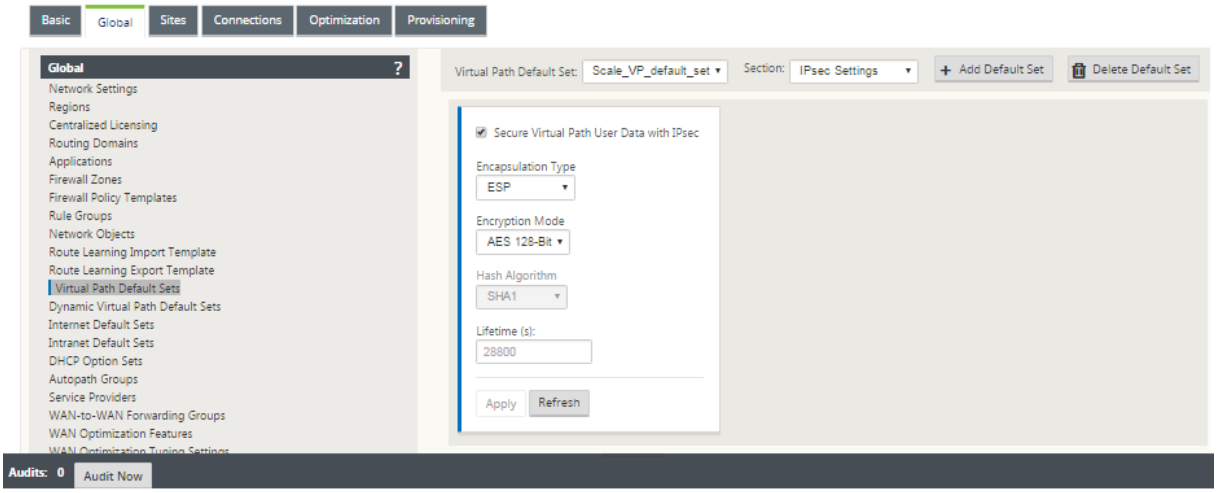
Routing Domains

- Default_RoutingDomain

IPsec Tunnels

- Default Sets
- Secure Virtual Path User Data with IPsec





IPSec Tunnels

IPsec Tunnels secure both user data and header information. Citrix 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.

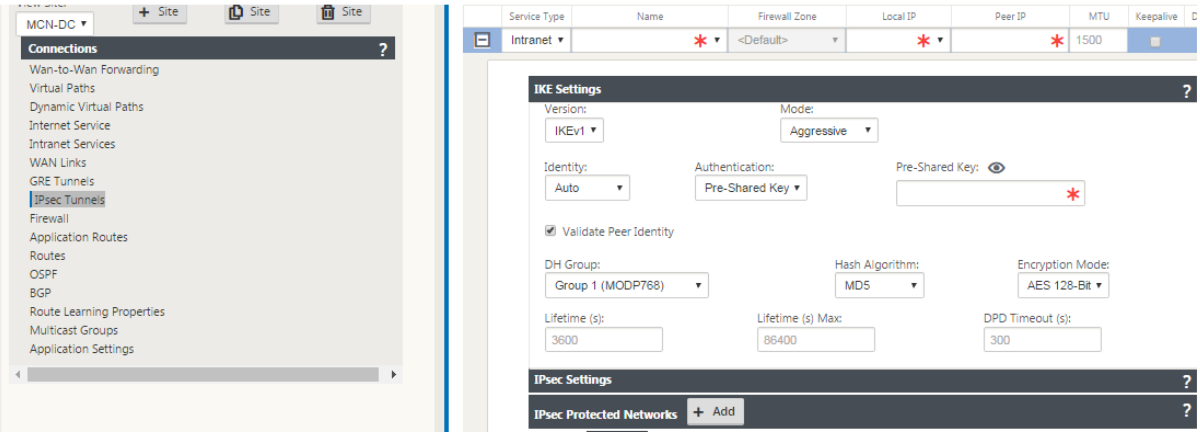
IPsec tunnel is established across the Virtual Path before data can flow across the SD-WAN overlay network.

- 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). Citrix 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 includes 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 Citrix SD-WAN appliance using the right service type (Virtual Path, Internet, Intranet, and Local).

- If traffic has to bypass the Citrix 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 throttles the traffic when it is sent through the Virtual Path (UDP encapsulated).

Routing

March 12, 2021

This article outlines routing best practices for the Citrix SD-WAN solution.

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 prefixes 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

March 12, 2021

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

March 12, 2021

Citrix SD-WAN platforms support upto 8 public internet connections and 32 Private MPLS connections. This article outlines WAN link configuration best practices for the Citrix SD-WAN solution.

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 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.
- Manually configure the MCN/RCN with the Ingress/Egress physical rate for all the WAN links since it is the central point of bandwidth distribution among multiple branches.
- For increased reliability of important datacenter workloads/services, when auto-learn is not used, use reliable links with SLA's that does not have random variation of capacity.

- 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 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 Citrix 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

March 12, 2021

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 is 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?

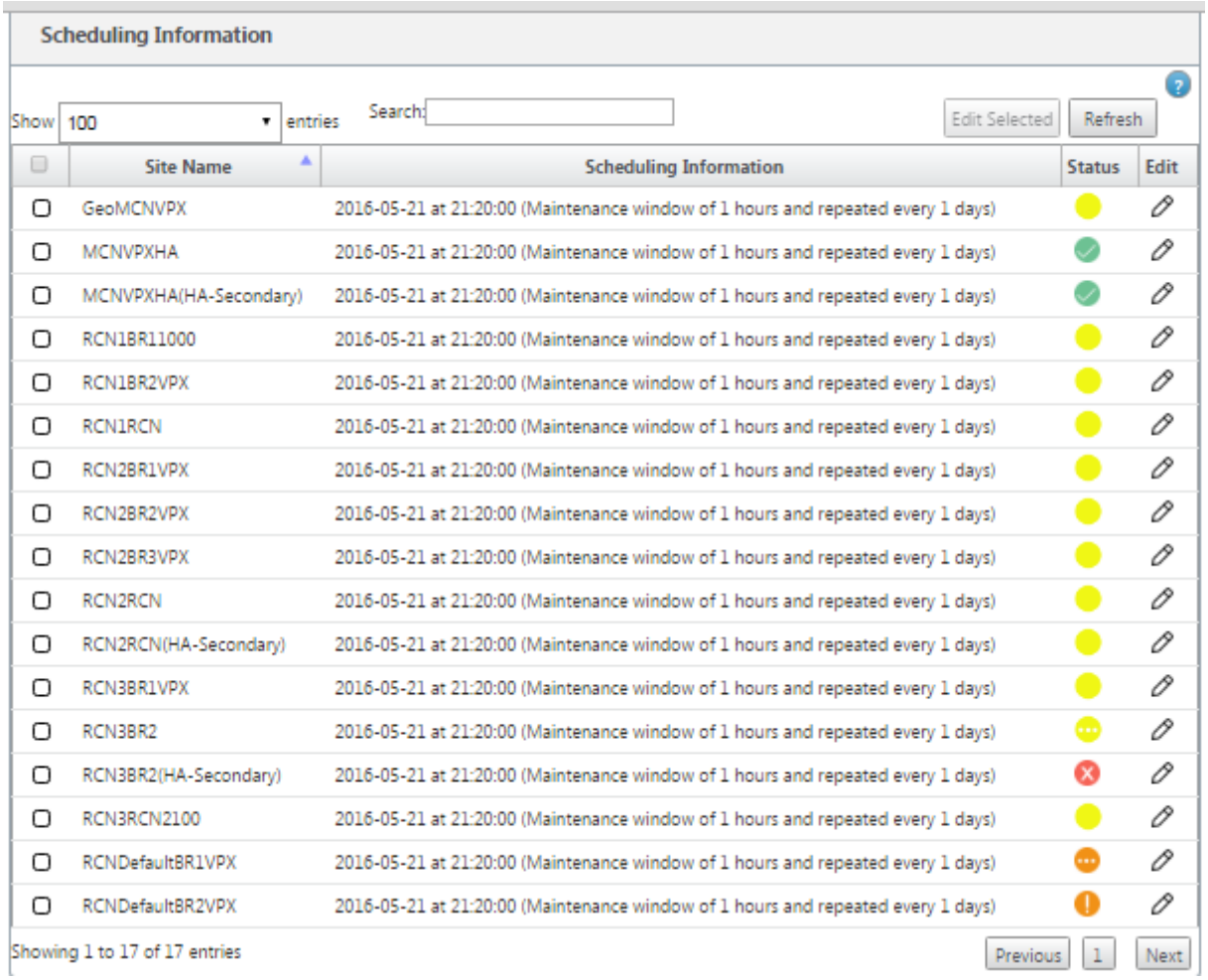
Scheduling for RCN is performed from the MCN **Change Management Settings** page. For RCN branches, you need to log into respective RCN and set the schedule details.

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: Edit Selected Refresh

Site Name	Scheduling Information	Status	Edit
GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
MCNVPXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
MCNVPXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR3VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2RCN(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3RCN2100	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCNDefaultBR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		

Showing 1 to 17 of 17 entries Previous 1 Next

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 depreciated. 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
- 11.0 to 11.y

- 11.0.x to 11.0.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.

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 rollback 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 the configuration 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 30 min interval.
2. MCN - After config/software change, if Virtual Path service is down for 30 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 30 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.

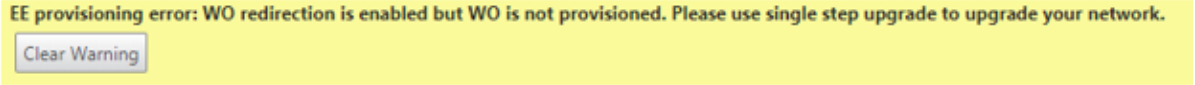
How does roll back interact with Partial Software Upgrade when I have multi-tier network?

- 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 Premium (Enterprise) Edition

What does the following message indicate when a 2100 EE appliance is upgraded to release 10.0?



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.

Related information

- Zero Touch Deployment Over LTE
- Configure the Secondary MCN in HA

Reference material

March 12, 2021

Application Signature Library

A list of applications that the Citrix SD-WAN appliances can identify using Deep Packet Inspection.