Citrix SD-WAN 10.2
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the SD-WAN Appliance Packages on the Clients</td>
<td>154</td>
</tr>
<tr>
<td>Checklist and how to deploy</td>
<td>160</td>
</tr>
<tr>
<td>Deployments</td>
<td>161</td>
</tr>
<tr>
<td>Gateway mode</td>
<td>162</td>
</tr>
<tr>
<td>Virtual inline mode</td>
<td>175</td>
</tr>
<tr>
<td>Build a SD-WAN network</td>
<td>195</td>
</tr>
<tr>
<td>WAN optimization only with Premium (Enterprise) edition</td>
<td>196</td>
</tr>
<tr>
<td>Hairpin Mode</td>
<td>199</td>
</tr>
<tr>
<td>Two box mode</td>
<td>201</td>
</tr>
<tr>
<td>High availability</td>
<td>209</td>
</tr>
<tr>
<td>Enable Edge Mode High Availability Using Fiber Optic Y-Cable</td>
<td>218</td>
</tr>
<tr>
<td>Zero touch</td>
<td>219</td>
</tr>
<tr>
<td>On-prem zero touch</td>
<td>240</td>
</tr>
<tr>
<td>AWS</td>
<td>240</td>
</tr>
<tr>
<td>Azure</td>
<td>251</td>
</tr>
<tr>
<td>Single region deployment</td>
<td>270</td>
</tr>
<tr>
<td>Multi region deployment</td>
<td>272</td>
</tr>
<tr>
<td>Active bandwidth testing</td>
<td>276</td>
</tr>
<tr>
<td>Adaptive bandwidth detection</td>
<td>278</td>
</tr>
<tr>
<td>Domain name system</td>
<td>280</td>
</tr>
<tr>
<td>DHCP server and DHCP relay</td>
<td>285</td>
</tr>
<tr>
<td>Configuring DHCP server and DHCP relay</td>
<td>286</td>
</tr>
<tr>
<td>WAN link IP address learning through DHCP client</td>
<td>290</td>
</tr>
<tr>
<td>GRE tunnel</td>
<td>292</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configure GRE Tunnels for the MCN Site (Optional)</td>
<td>293</td>
</tr>
<tr>
<td>Configure GRE Tunnels for a Branch Site</td>
<td>294</td>
</tr>
<tr>
<td>Internet access</td>
<td>296</td>
</tr>
<tr>
<td>Direct Internet Breakout at Branch with Integrated Firewall</td>
<td>297</td>
</tr>
<tr>
<td>Direct Internet Access with Secure Web Gateway</td>
<td>299</td>
</tr>
<tr>
<td>Backhaul Internet</td>
<td>300</td>
</tr>
<tr>
<td>Link state propagation</td>
<td>302</td>
</tr>
<tr>
<td>Metering and Standby WAN Links</td>
<td>304</td>
</tr>
<tr>
<td>Office 365 optimization</td>
<td>314</td>
</tr>
<tr>
<td>PPPoE Sessions</td>
<td>322</td>
</tr>
<tr>
<td>Quality of service</td>
<td>331</td>
</tr>
<tr>
<td>Customizing Classes</td>
<td>331</td>
</tr>
<tr>
<td>Rules by IP address and port number</td>
<td>334</td>
</tr>
<tr>
<td>Rules by application name</td>
<td>339</td>
</tr>
<tr>
<td>Add Rule Groups and Enable MOS</td>
<td>346</td>
</tr>
<tr>
<td>Application classification</td>
<td>347</td>
</tr>
<tr>
<td>QoS fairness (RED)</td>
<td>353</td>
</tr>
<tr>
<td>MPLS Queues</td>
<td>356</td>
</tr>
<tr>
<td>Reporting</td>
<td>362</td>
</tr>
<tr>
<td>Application QoE</td>
<td>362</td>
</tr>
<tr>
<td>HDX QoE</td>
<td>365</td>
</tr>
<tr>
<td>Multiple Net Flow Collectors</td>
<td>367</td>
</tr>
<tr>
<td>Routing</td>
<td>369</td>
</tr>
<tr>
<td>SD-WAN Overlay Routing</td>
<td>371</td>
</tr>
</tbody>
</table>
## Manual Secure Peering initiated from PE appliance at DC site and Branch PE appliance
462

## Manual Secure Peering initiated from PE appliance at DC site to Branch Standalone SD-WAN SE and WANOP Appliance
465

## Domain join and delegate user creation
469

## Security
474

## IPSec Tunnel Termination
475

## How to configure ipsec tunnels for virtual and dynamic paths
475

## How to configure ipsec tunnel between SD-WAN and third-party devices
476

## How to add IKE certificates
484

## How to view ipsec tunnel configuration
484

## IPSec monitoring and logging
486

## Eligibility for ipsec non-virtual path routes
489

## IPsec null encryption
490

## FIPS Compliance
491

## Citrix SD-WAN secure web gateway
495

## Zscaler Integration by using GRE tunnels and IPsec tunnels
496

## Firewall Traffic Redirection Support by Using Forcepoint in Citrix SD-WAN
505

## Palo Alto Integration by Using IPsec Tunnels
509

## Stateful Firewall and NAT Support
526

## Global firewall settings
529

## Advanced firewall settings
530

## Zones
532

## Policies
535

## Network Address Translation (NAT)
540
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure static NAT</td>
<td>541</td>
</tr>
<tr>
<td>Configure dynamic NAT</td>
<td>542</td>
</tr>
<tr>
<td>Configure dynamic NAT with port forwarding</td>
<td>544</td>
</tr>
<tr>
<td>Configure Virtual WAN Service</td>
<td>546</td>
</tr>
<tr>
<td>Configure firewall segmentation</td>
<td>548</td>
</tr>
<tr>
<td>AppFlow and IPFIX</td>
<td>553</td>
</tr>
<tr>
<td>SNMP</td>
<td>558</td>
</tr>
<tr>
<td>SMB 3.1.1 connection</td>
<td>561</td>
</tr>
<tr>
<td>WAN optimization</td>
<td>563</td>
</tr>
<tr>
<td>Citrix SD-WAN premium edition</td>
<td>564</td>
</tr>
<tr>
<td>Enable optimization and configure the default feature settings</td>
<td>565</td>
</tr>
<tr>
<td>Configure optimization default tuning settings</td>
<td>569</td>
</tr>
<tr>
<td>Configure optimization default application classifiers</td>
<td>570</td>
</tr>
<tr>
<td>Configure optimization default service classes</td>
<td>573</td>
</tr>
<tr>
<td>Configure optimization for a Branch Site</td>
<td>579</td>
</tr>
<tr>
<td>Configure SSL profiles</td>
<td>580</td>
</tr>
<tr>
<td>Citrix WAN optimization client plug-in</td>
<td>584</td>
</tr>
<tr>
<td>Hardware and software requirements</td>
<td>585</td>
</tr>
<tr>
<td>How the WANOP plug-in works</td>
<td>586</td>
</tr>
<tr>
<td>Deploy appliances for Use with plug-ins</td>
<td>593</td>
</tr>
<tr>
<td>Customize the plug-in MSI file</td>
<td>597</td>
</tr>
<tr>
<td>Deploy plug-ins on windows systems</td>
<td>604</td>
</tr>
<tr>
<td>WANOP plug-in GUI commands</td>
<td>608</td>
</tr>
<tr>
<td>Update the WANOP plug-in</td>
<td>612</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Troubleshoot WANOP plug-in 613
How-to-articles 614
Interface Groups 615
Configure Virtual IP Address Identity 616
Configure access interface 616
Configure Virtual IP addresses 617
Configure GRE Tunnels 617
Setup dynamic paths for branch to branch communication 618
Configure static WAN paths 621
Monitoring and Troubleshooting 622
Monitoring Virtual WAN 623
Viewing Statistical Information 624
Viewing Flow Information 625
Viewing Reports 629
Viewing Firewall Statistics 630
Diagnostic Tool 633
Improved Path Mapping and Bandwidth Usage 634
Troubleshooting Management IP 640
Session-based HTTP Notifications 641
Best practices 647
Security 648
Routing 656
QoS 656
WAN Links 657
<table>
<thead>
<tr>
<th>FAQs</th>
<th>658</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference material</td>
<td>667</td>
</tr>
</tbody>
</table>
What’s New

February 15, 2019

The Citrix SD-WAN release 10 version 2 introduces the following new features and enhancements:

Application centric enhancements

Application QoE:

- 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.

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 you can build a custom dashboard to interpret IPFIX template.
- IPFIX version 10 is supported in Citrix SD-WAN release 10 version 2 and above.
- 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.

Configuration, Management, and Supportability

SD-WAN Center dashboard GUI:

- The Virtual Path Summary widget is renamed to Network QoE. It includes a graphical comparison of the overlay virtual path and underlay member paths of the network. You can view the graphs for QoE metrics such as availability, loss, latency and jitter.
- The Site QoE widget is introduced. It provides a graphical comparison of the overlay virtual path and underlay member paths of the selected site. You can view the graphs for QoE metrics such as availability, loss, latency, jitter and throughput.

Change Management process – GUI enhancements:

- To view or update change management settings, you can now click the gear icon on top-right corner on the change management page.
- Change management configuration file details are moved to Details section.
For multi-region set-up:

- Global Site Summary table now provides metrics such as Total Sites, Traffic Impacted Sites, and Staging Sites etc. Each of this table entry is a link which upon clicking provides the full details of all the sites with the chosen filter.

SD-WAN Center scale setup:

- The SD-WAN Center network summary now displays up to 6,000 sites.

SD-WAN Center diagnostics:

- The diagnostic utilities, such as Ping, Trace-Route, and PCAP are added to SD-WAN Center for troubleshooting network connectivity issues.

DHCP configuration:

- An alert notification is raised when DHCP WAN link changes IP subnet on the internet link.

SD-WAN diagnostics:

- A new diagnostics mode page is introduced. This page allows you to run diagnostics test that helps in understanding SD-WAN deployments in the network. You can test the bandwidth usage, ping, and perform traceroute for the WAN links configured at different sites in the SD-WAN network. It provides information which helps in troubleshooting issues in existing configuration.

Office 365 optimization:

- The Office 365 breakout policy allows you to specify which category of Office 365 traffic you can directly break out from the branch. This makes it easy to adhere to Microsoft Office 365 Network Connectivity Principles to optimize the Office 365 user experience for branch office workers. On enabling Office 365 breakout and compiling the configuration, a DNS object, application object, application route, and a firewall policy is auto-created and applied to branch sites with Internet service. The Office 365 Breakout Policy settings are available under global settings in the SD-WAN GUI.

DNS Forwarder:

- You can now use your SD-WAN appliance as a lightweight DNS proxy. DNS requests directed to SD-WAN IP address are intercepted and forwarded to DNS servers. You can configure the DNS forwarder rules on an SD-WAN appliance. These rules are used to filter the DNS requests as per the domain names and forward it to the appropriate DNS servers.

PPPoE:

- 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 10.2

- 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.
- 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.

Bandwidth auto-provisioning:
- 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.

Block UDP to force ICA to TCP- WANOP:
- By changing the protocol to TCP, SD-WAN WANOP provides:
  - Compression/DDup benefits.
  - Visibility (local reports and HDX Insight).

The WANOP GUI shows an option to force the session for TCP protocol.

Cloud services in SD-WAN Center

The following add-on services for Cloud Connectivity using Citrix SD-WAN Center are introduced.

- Citrix SD-WAN and Zscaler help enterprises transform their WAN for cloud migration by providing secure local breakouts to applications and resources hosted on the Internet. New WAN infrastructure technologies such as SD-WAN increase network agility and scale while lowering cost and complexity for an improved user experience in distributed organizations.
- SaaS Gateway Service - The Citrix SD-WAN SaaS Gateway Service delivers SD-WAN functionality as a service through reliable and secure delivery for all internet-bound traffic regardless of the host environment (datacenter, cloud, and internet). This improves network visibility and management. It enables partners to offer managed SD-WAN services and business critical SaaS applications to their end customers.
- SD-WAN Secure Web Gateway to Palo Alto Networks: Global Protect Cloud Service (GPCS). See, SD-WAN secure web gateway.

Platforms, scalability, and deployments

Citrix SD-WAN Center can be installed on the following platforms:

- Microsoft Hyper-V 2012 R2
Cloud platform:

- Microsoft Azure marketplace
- Deploying SD-WAN Center in newer AWS instances (m4 & c4) is supported.

Maximum number of virtual paths

The maximum number of static Virtual Paths for the following platform editions is increased:

- 2100 SE - 128–256.
- 4100 SE: 256–553 – can be configured as an RCN with 550 clients and Geo RCN in the region and Geo MCN in the network.
- 210-SE – 8–16.

SD-WAN LTE platform editions:

- The SD-WAN Center report and the mobile broadband pages for an SD-WAN LTE platform now displays MSISDN and IMSI numbers in Inventory information.

REST API

The following APIs are available:

Configuration:

- Network Adapters
- Config Package – Import, Export, Save As

Monitoring:

- Access Interfaces
- Virtual Path Services
- Ethernet
- Ethernet MAC Learning
- Intranet
- Observed Protocols
- Paths (Detailed)
- Application Routes
- Rule Groups
- Site
- MPLS Queues
- WAN Link Usage
- GRE Tunnel
- IPsec Tunnel
- Multicast Group
Citrix SD-WAN 10.2

- Dynamic Routing Protocol

Configuration editor:
- App QoE
- Application Routes
- DNS Settings
- Office 365
- Wan Optimization Application Classifiers and Service Classes

Release Notes

February 4, 2019

This release note describes known issues, and fixed issues applicable to Citrix SD-WAN software release 10 version 2 for the SD-WAN Standard Edition, WANOP, and Premium Edition appliances.

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

Fixed issues

NSSDW-13639: In a high availability environment, when you select all for multiple sites to perform an Edit operation, the schedule information is not updated for the secondary branch sites.

NSSDW-13538: A failed (auto) status is reported on the Change Management page after activating staged software with release 10 version 2 build 23 from release 10 version 3 on an MCN appliance using the local change management procedure.

NSSDW-14516: In a high availability environment, fluctuating network changes or configuration updates that interrupt communication with HA peers or external tracking IPs can cause both appliances in a high availability pair to be in standby mode for up to 2 minutes.

SDWANHELP-184 (SR# 78095846): On the SD-WAN WANOP 4000 and 5000 platform editions, the appliance GUI restarts after a crash. Restart the accelerator VM from the XenServer to restart the appliance.

NSSDW-13269: When creating routing domains, if you attempt to add multiple routing domains with single configuration GUI workflow, errors occur.

NSSDW-11253: After upgrading existing network to release 10.x, the following error message is displayed when performing audit operation from the configuration editor: “One Site must have Appliance Mode set to primary MCN,” when associating an existing site to the new region.
NSSDW 13944: In release 10 version 2, an audit error occurs when attempting to add default route each pointing to different ZScaler gateways, even if there are gateways of different routing domains.

SDWANHELP-501 (SR# SR78262688): Unable to export or audit SD-WAN configuration after configuring GRE tunnels on an SD-WAN appliance using release 10.0 version 2.

SDWANHELP-509 (SR# SR78343050): On a 5100-SE platform, staging a previously working configuration fails after an upgrade to the latest release version and the routing information cannot be obtained.

SDWANHELP-512 (SR#: 78314443): In release 10 version 4, upon main registry updates such as, adding, deleting, or renaming WAN link, there is a downtime of 15 seconds to 40 seconds for the virtual path routing protocol to converge between SD-WAN deployed sites.

SDWANHELP-537 (SR# 78411542): In release 10 version 4, emails alerts are not reported in the SD-WAN Center for WAN link status.

SDWANHELP-538: In release 10 version 3, after configuration update upon removing a custom application stats object, the SD-WAN service restarts.

SDWANHELP-482 (SR# 78247128): In release 10 version 4, a new option to add local IKE-ID when configuring IPSec is added.

SDWANHELP-485 (SR# 78274277): In release 10 version 2, the application QoS configuration is not displayed in the Monitoring view of the SD-WAN web management interface on a 410-SE appliance.

SDWANHELP-489 (SR# 78293306): When the SD-WAN service is enabled, the SD-WAN routes are missing and all trusted interfaces become inactive.

SDWANHELP-490: A core dump error occurs when an ICMP echo packet that creates a firewall connection causes the packet to offload from the IP host thread to the DPI threads.

SDWANHELP-543 (SR# 78394675): During high availability switchover with multiple routing domains, routes are not synchronized properly in the routing tables.

SDWANHELP-544: The IPSec tunnel fails when changing parameters for the tunnel that is actively receiving packets on a site installed with new package.

SDWANHELP-549: In release 10 version 2, before the main software configuration update, the routes set with path eligibility remain in path state after main registry update without associating the current active path state causing routing issues.

SDWANHELP-550: In release 10 version 4, the Ping output for user-initiated ping displays responses for auto-generated pings.

SDWANHELP-553 (SR# 78428386): In release 10 version 3, the active appliance transmits only the most optimal OSPF routes for deletion or addition causing active and standby route tables to differ.
**SDWANHELP-566 (SR# 78409673):** In release 10 version 4, relayed DHCP packets are redirected or not transmitted, if packets from DHCP relay servers send packets using the client DHCP source port. This occurs even when not using the broadcast IP address.

**NSSDW 13665:** When sites are configured with WAN link templates for MPLS queue configuration, the site deletion takes longer than expected.

### Known issues

**NSSDW-14908:** The application QoE value is reported as “zero,” if network conditions are outside of the configured thresholds for the real-time traffic.

**SDWANHELP-520 (SR# 78300015):** In rare instances, the SD-WAN appliance crashes due to invalid memory reference. The health monitoring process restarts the failed process automatically. This issue exists in all SD-WAN releases.

**NSSDW-14883:** The PPPoE sessions are re-established when activating an interface configuration change on a site. If only PPPoE links exist in the virtual path on that site, it becomes inactive for a brief period until new session is established.

**NSSDW-15519:** SD-WAN Center fails to discover regions for an MCN with high availability enabled. Switch back the primary MCN to active to resolve this issue.

**NSSDW-5182:** While converting a single region network to multi-region network, i.e. when adding regions and associate existing site to the newly created region, the error message “One Site must have Appliance Mode set to primary MCN” appears.

**Workaround:** Create virtual paths manually between MCN and all the RCNs.

**SDWANHELP-651:** On SD-WAN 2100 appliance, license installation fails when using Microsoft Edge browser.

### Release Notes

April 11, 2019

This release note describes known issues, and fixed issues applicable to Citrix SD-WAN software release 10.2 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

The Citrix SD-WAN release version 10.2.1 introduces the following enhancements. See doc.citrix.com for more information.

- Citrix SD-WAN 5100 Premium Edition (PE) platform support.
- Citrix SD-WAN 210 LTE authentication enhancement. See configure 210-SE LTE.

Fixed issues

**SDWANHELP-682**: The Site location field is not saved, while creating a site using basic configuration editor.

**SDWANHELP-671**: The licensing log files consume large amount of disk space while using remote licensing server.

**SDWANHELP-650**: Configuration process such as adding, editing, cloning a site, or performing audit, makes the MCN GUI unresponsive.

**SDWANHELP-649**: Excessive virtual path packet retransmissions might be experienced with low bandwidth utilization, high loss or congestion, and less than 20 ms RTT.

**SDWANHELP-627**: Unable to store OSPF cost value greater than 255 when redistributing routes from SD-WAN to OSPF router.

**SDWANHELP-626**: Unable to access Citrix SD-WAN Center due to memory outage.

**SDWANHELP-605**: Citrix SD-WAN appliance crashes during configuration change management process.

**SDWANHELP-594**: Virtual paths are marked as DEAD for all the sites when corrupted control packet is processed. If the control packet is malformed it is dropped and paths becomes inactive.

**SDWANHELP-590**: Citrix SD-WAN Center security enhancements.

**SDWANHELP-684**: The Citrix SD-WAN appliance becomes unresponsive upon modifying existing import filters that induces changes in route properties.

**NSSDW-15962**: Citrix SD-WAN WANOP plug-in crashes when installed with Citrix Workspace plug-in.

**NSSDW-15741**: A configuration error is not triggered on RCN when site loses connectivity with MCN and its branches after configuration update.

**NSSDW-15519**: SD-WAN Center fails to discover regions for an MCN with high availability enabled. Switch back the primary MCN to active to resolve this issue.
Known issues

NSSDW-14883: The PPPoE sessions are re-established when activating an interface configuration change on a site. If only PPPoE links exist in the virtual path on that site, it becomes inactive for a brief period until new session is established.

NSSDW-5182: When converting a single region network to multi-region network, during adding regions and associate existing site to the newly created region, the error message “One Site must have appliance Mode set to primary MCN” appears.

Workaround: Create virtual paths manually between MCN and all the RCNs.

NSSDW-13227: SD-WAN VPXL VM does not boot on XenServer 7.5 Hypervisor. This is because the VM uses multi-queue NICs and it runs out of grant references. You can resolve this issue by using the following options:

- Increase the grant references given to the guest.
- Decrease the number of queues used by the guest. Add the following to the guest's kernel command-line: xen_netfront.max_queues=1.

SDWANHELP-656: When the SD-WAN 4000/5000 WANOP appliance is configured for WCCP, the NetScaler ADC “Configure Modes” is incorrect. The correct setting in ns.conf should be “enable ns mode FR L3 USIP MBF Edge USNIP PMTUD”.

SDWANHELP-520: In rare instances, the SD-WAN appliance crashes due to invalid memory reference. The health monitoring process restarts the failed process automatically.

Release Notes

March 26, 2019

This release note describes known issues, and fixed issues applicable to Citrix SD-WAN software release 10.2 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

NSSDW-15594: A regenerate appliance certificate upload option for SSL communication between the SD-WAN Center and SD-WAN appliance is introduced. The appliance certificate should be generated on the MCN to regenerate the certificate.
The regenerated certificate from the MCN appliance needs to be uploaded to the SD-WAN Center for SSL communication to work.

To regenerate appliance certificate:

1. Navigate to **Configuration > Virtual WAN > SD-WAN Center Certificates > Appliance Certificate Management**. The following options are available.
   - Regenerate appliance certificate for SSL communication.
   - Download the appliance certificate.

2. In SD-WAN Center, upload the appliance certificate by navigating to, **Configuration > Network Discovery > SSL Certificate > Appliance Certificate**.

For existing deployments, upgrading to release 10.2 version 2 does not require installing the new appliance certificate on the SD-WAN center because the already installed default application certificate is not removed. However, for new deployments, and for SSL communication to work, you should install the appliance certificate to the SD-WAN Center.
NSSDW-17171: Allow default route to be filtered in a BGP NEIGHBOR POLICY using 0.0.0.0/32 or any prefix, such as 16 or 8 which is NON-ZERO.

1. The current BGP neighbor policy uses 0.0.0.0/prefix as a match all prefix and cannot be filtered. The definition of 0.0.0.0 is a default match all criteria.
   - With this enhancement you can specify a 0.0.0.0/32 or a NON-ZERO value which is matched as a particular prefix that needs to be exercised of a policy action in the specified direction.
   - 0.0.0.0/0 exists as a match all route.

2. The number of BGP Policies per neighbor is extended from 8 (7+1 default) to 16 (15 + 1 default)
   - Each BGP neighbor can be configured with neighbor policies.
   - Prior to release 10.2 version 2 the maximum limit was 8 (7 user-defined policies and a single match all filter policy). This has been enhanced to 16 (15 user-defined policies and a single match all filter policy).

NSSDW-16025: Support for high-availability using splitter Y-cable connected to SFP ports for the 1100 appliance is added.

NSSDW-16663: Add Security Admin role to SD-WAN Center and MCN GUI.

Fixed issues

SDWANHELP-520 (SR# 78300015): The SD-WAN appliance might crash due to invalid memory reference. The health monitoring process restarts the failed SD-WAN service automatically.

SDWANHELP-617 (78586601/78435402): Slow file transfer speeds are observed between two branch sites with low permitted bandwidth.

SDWANHELP-650 (SR# 78640419): On the SD-WAN 4,100 appliances, the MCN GUI is unresponsive after an upgrade to release 10.2.

SDWANHELP-674 (SR# 78694895): On the SD-WAN PE appliance, you need to change the hostname for WANOP communication.

SDWANHELP-676 (SR# 78708421): On the SD-WAN 4100 WANOP appliance, 4 out of its 6 instances are disconnected from the active directory, and cannot be rejoined.

SDWANHELP-682 (SR# 78694883): When creating a Site the location field is not saved.

SDWANHELP-698 (SR# 78744599): The SD-WAN appliance does not fail over when the LAN switch goes down.

SDWANHELP-703 (SR# 78765798): IPSec traffic to Zscaler is impacted when memory usage peaks are observed.
SDWANHELP-705 (SR# 78708432): Multiple Core-dump files generated on the standby MCN appliance.

SDWANHELP-712 (SR# 78708319): LTE connected virtual path is reported as DOWN even when the modem is operational on the branch SD-WAN appliance.

SDWANHELP-735 (78811478): The “Active OS partition is completely full…..” alert is observed on the 1100 platform edition configured as PE in releases 10.2.0 and 10.2.1. You need to manually restart the 1100 appliance after upgrading to release 10.2.2.

NSSDW-10133: Port forwarding rules are missing from the Dynamic NAT policies when internet access for all the routing domains is enabled.

NSSDW-15923: SD-WAN BGP configuration does not allow using community string in old format.

NSSDW-16936: The Audit Request from GUI is timed out when you attempt to compile large configuration file.

NSSDW-16165: Subnet added as part of region definition does not get populated in routes table.

NSSDW-17108: Selecting the first autopath group when configuring WAN Link Templates displays as “no group selected”.

NSSDW-17278: WAN to WAN forwarding does not work when configuration is upgraded from non-WAN to WAN configuration to WAN configuration.

NSSDW-17428: Traffic is sent to incorrect routing domain for dynamic routes.

NSSDW-17243: Failed to mount active storage in SD-WAN Center for Azure.

NSSDW-17091: The drill-down option is not working for Virtual path rows in the Services tab on reporting page.

NSSDW-17076 (78662689): PPTP/GRE does not come up through the SD-WAN traffic. The SD-WAN appliance is acting as pass-through and not an endpoint.

Known issues

NSSDW-17427: On the premium edition appliances, make the WANOP hostname persistent when it is incorrect by updating the appliance or site name and perform Local Change Management or Change management.

Software Installation and Upgrade

December 19, 2018
There are two main upgrade scenarios:

1. Upgrade appliances with working Virtual WAN configuration from a previous release version, 8.1, 9.0, 9.1, 9.2 to 9.3 first, and then to the version 10.2.

2. Upgrade appliances to release 10.2 without existing Virtual WAN configuration.

**Important**

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

**Note**

Upgrading to 10.2 release is a single-step process. If you are currently using an earlier version of the software, such as release version 9.2, you should first upgrade to latest software release version 9.3 and then upgrade to 10.0, 10.1, or 10.2.

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

**System requirements**

January 21, 2019

**Hardware requirements**

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

**Firmware requirements**

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

**Note**

Appliances running earlier software versions cannot establish a Virtual Path connection to the appliance running SD-WAN release 9.2. 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 35.0+ (Recommended version 43.x)
- Google Chrome 40.0+ (Recommended version 49.x)
- Microsoft Internet Explorer 11+

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 XenServer 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

SD-WAN platform models and software packages

March 6, 2019

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, please 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
- 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, please refer to the following SD-WAN product platform edition datasheet on the products download site.
SD-WAN standard edition hardware appliances

Citrix SD-WAN release 10.2 supports the following SD-WAN standard edition hardware appliance models:

<table>
<thead>
<tr>
<th>SD-WAN SE PLATFORM MODEL</th>
<th>ROLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>210-SE/210-SE LTE</td>
<td>Small branch appliance</td>
</tr>
<tr>
<td>410-SE</td>
<td>Small branch appliance</td>
</tr>
<tr>
<td>1000-SE</td>
<td>Large branch appliance</td>
</tr>
<tr>
<td>2000-SE</td>
<td>Large branch appliance</td>
</tr>
<tr>
<td>2100-SE</td>
<td>Large branch appliance</td>
</tr>
<tr>
<td>4100-SE</td>
<td>Data Center - Master Control Node (MCN)</td>
</tr>
<tr>
<td>5100-SE</td>
<td>Data Center - Master Control Node (MCN)</td>
</tr>
</tbody>
</table>

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

Citrix SD-WAN 10.2 supports the following SD-WAN WAN Optimization (WANOP) appliance models:

<table>
<thead>
<tr>
<th>SD-WAN WANOP PLATFORM MODELS</th>
<th>ROLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>WANOP 800</td>
<td>Small branch appliance</td>
</tr>
<tr>
<td>WANOP 1000 Windows Server</td>
<td>Large branch appliance</td>
</tr>
<tr>
<td>WANOP 1000</td>
<td>Large branch appliance</td>
</tr>
<tr>
<td>WANOP 2000</td>
<td>Large branch appliance</td>
</tr>
<tr>
<td>WANOP 3000</td>
<td>Large branch appliance</td>
</tr>
<tr>
<td>WANOP 4000, WANOP 4100</td>
<td>Data Center appliance</td>
</tr>
<tr>
<td>WANOP 5000</td>
<td>Data Center appliance</td>
</tr>
<tr>
<td>wANOP 5100</td>
<td>Data Center appliance</td>
</tr>
</tbody>
</table>

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

Citrix SD-WAN 10.2 supports the following SD-WAN VPX Virtual Appliance (VPX-SE) models:
Citrix SD-WAN 10.2

<table>
<thead>
<tr>
<th>SD-WAN VPX-SE PLATFORM MODELS</th>
<th>ROLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPX 20-SE</td>
<td>MCN or client appliance, small branch</td>
</tr>
<tr>
<td>VPX 50-SE</td>
<td>MCN or client appliance, small branch</td>
</tr>
<tr>
<td>VPX 100-SE</td>
<td>MCN or client appliance, small branch</td>
</tr>
<tr>
<td>VPX 200-SE</td>
<td>MCN or client appliance, small branch</td>
</tr>
<tr>
<td>VPX 500-SE</td>
<td>MCN or client appliance, small branch</td>
</tr>
<tr>
<td>VPX 1000-SE</td>
<td>MCN or client appliance, small branch</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>SD-WAN VPX WANOP PLATFORM MODELS</th>
<th>ROLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>WANOP VPX-2</td>
<td>Small branch appliance</td>
</tr>
<tr>
<td>WANOP VPX-6</td>
<td>Small branch appliance</td>
</tr>
<tr>
<td>WANOP VPX-10</td>
<td>Small branch appliance</td>
</tr>
<tr>
<td>WANOP VPX-20</td>
<td>Small branch appliance</td>
</tr>
<tr>
<td>WANOP VPX-50</td>
<td>Large branch appliance</td>
</tr>
<tr>
<td>WANOP VPX-100</td>
<td>Large branch appliance</td>
</tr>
<tr>
<td>WANOP VPX-200</td>
<td>Large branch appliance</td>
</tr>
</tbody>
</table>

**Important**

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

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

Citrix SD-WAN 10.2 supports the following SD-WAN Premium (Enterprise) Edition appliance (SD-WAN PE) models:
**Upgrade paths for release 10.2**

January 7, 2019

For some paths, you cannot upgrade directly to the target release but instead, you must first upgrade to an interim release.

For example, to upgrade from 9.1 to 10.2, you must first upgrade to 9.3.5 using the .tar.gz package and then upgrade to 10.2 using the .zip package.

For more information, see the following upgrade paths table.
**Steps to upgrade from previous releases to release 10 version 2**

<table>
<thead>
<tr>
<th>Starting Version</th>
<th>Supported steps to 10.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.0 .tar.gz</td>
<td>9.3.5 or latest .zip</td>
</tr>
<tr>
<td>9.2 .tar.gz</td>
<td>9.3.5 or latest .zip</td>
</tr>
<tr>
<td>9.3 .zip</td>
<td>9.3.5 or latest .zip</td>
</tr>
<tr>
<td>10 .zip</td>
<td>10.2</td>
</tr>
</tbody>
</table>

**Important:**
- If you are upgrading from a previous releases version such as 9.0.x, 9.1.x, 9.2.x to 9.3 with working virtual WAN configuration, follow the steps outlined in the procedure Upgrade to 9.3 with working virtual WAN configuration.
- If you are upgrading from a previous release version such as 9.0.x, 9.1.x, 9.2.x to 9.3 without Virtual WAN Configuration, follow the steps outlined in the procedure Upgrading to 9.3 without virtual WAN configuration.
- If you are upgrading from release 9.3.5 or later to 10.2 with working virtual WAN configuration, follow the steps outlined in the procedure Upgrade to 10.2 with working virtual WAN.
• If you are upgrading from release 9.3.5 or later to 10.2 without virtual WAN configuration, follow the steps outlined in the procedure Upgrade to 10.2 without virtual WAN configuration.

Upgrading to 10.2 with working virtual WAN configuration

December 18, 2018

Note:
This upgrade procedure is for a multi-region network set-up.

1. In the Configuration Editor, select the required configuration, click Export, and select Change Management Inbox as the destination. Click Export.

2. In the Change Management > Change Preparation page, click Choose Files and select the ctx-sdw-sw-10.2.0.x.zip software package file. Click Upload.

Note:
You can download the Citrix SD-WAN release 10, version 2 software package from the Downloads page.
3. 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.
4. 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**.

5. 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.
6. 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.

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

8. After the countdown, a message indicates that activation is completed. Click **Done**.
9. 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.
Upgrading to 10.2 without virtual WAN configuration

December 18, 2018

1. Prepare the configuration using the Configuration Editor and save the configuration with a valid name.

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-10.2.0.x.zip software package file. Click Upload.

**Note:**
You can download the Citrix SD-WAN release 10, version 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.

Change management settings

December 17, 2018

You can schedule the installation of non-Virtual WAN software packages like WANOP, SVM, and XenServer Hotfixes using change management settings.

By default, the MCN assigns schedules installation to be attempted every day at 21:20:00 (local appliance time) based on software availability on the branches.

To edit schedule information:

Navigate to Configuration > Virtual WAN > Change Management Settings. Select the site for which you want to edit schedule information and click Edit.
You can edit the following parameters:

- **Site Name**: Appliance name as given by user in Config Editor for each site.
- **Date**: Date on which scheduled installation/upgrade will start from.
- **Time**: Local time of the appliance when the installation should begin once the files are received. Valid Format is HH:MM:SS
- **Maintenance Window**: The amount of time given by the user for installation. If “0” is provided installation will start immediately once the files are present on the appliance irrespective of the date and time values given under date and time fields.
- **Repeat Window**: Frequency after which the system will check for a new upgrade version and perform upgrade only when a new version is available.
- **Unit**: Unit chosen to check for new versions can be any one of Hours/Days/Weeks/Months.
Following is a sample scheduling information with the supported status details.

<table>
<thead>
<tr>
<th>Scheduling Information Status</th>
<th>Scheduling Information Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green check mark</td>
<td>Upgrade is Successful.</td>
</tr>
<tr>
<td>Orange exclamation</td>
<td>Appliance has received all necessary components, waiting for its scheduled installation window to start.</td>
</tr>
<tr>
<td>Yellow circle</td>
<td>Change Management has not been done, no action is required.</td>
</tr>
</tbody>
</table>
Scheduling Information Status | Scheduling Information Status
---|---
Red cross mark | An error has occurred during installation of OS components. Try Change Management once again, if problem persists, contact tech support.
Orange dotted circle | Files are being transferred to the appliance.
Yellow dotted circle | Upgrade is in progress.

### Single-step upgrade for SD-WAN appliances

**December 18, 2018**

**Note**

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

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

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

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

**Note**

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

Upload ctx-sdw-sw-10.1.0.122.zip (Single Step Upgrade Package) file if you are currently running release version 9.3.3 or newer.

Follow these procedures to upgrade:

- Upgrade to 10.2 with working Virtual WAN configuration
- Upgrade to 10.2 without working Virtual WAN configuration
Supported upgrade and downgrade scenarios

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

Factory shipped appliances

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

Appliances with legacy Virtual WAN software

1. The appliances currently in an active network with virtual paths up and running.
   • The appliances receive packages from MCN. The components are installed and all files from MCN are received, and are available in the scheduled time window.
2. The appliances are currently out of the network with virtual paths down.
   • This process is similar to upgrading appliances which are factory shipped. You need to download local change management from MCN and upload the software package to the branch site appliances.

Appliances with single-step upgrade support

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

Version switch or revert

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

You can reinstall the legacy software with the required configurations (using tar.gz files).

**Downgrade to previous software version:**

If you upgraded an existing software version to release version 10.2 using the tar.gz upgrade process, you can downgrade the software version to a previous software version.

If you used the .zip (single step upgrade) procedure to upgrade to version 10.2, you cannot downgrade the software version to a previous software version.

**Single-step upgrade in high availability deployment mode:**

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

**Partial software upgrade using local change management**

December 14, 2018

**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

December 14, 2018

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

Convert Standard Edition to Premium Edition

November 22, 2018

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.tar.gz file. Where x.x.x.x is the SD-WAN software release version.
5. Click **Upload**. Select **Accept** and click on **Install** to proceed.


7. Perform **Local Change Management** on the appliance using the downloaded active package in step 2 above.

**Citrix SD-WAN license options**

January 21, 2019

There are three 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, and Premium 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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 7.x</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Release 8.x</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Release 9.0</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Release 9.1, 9.2, 9.3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Release 10.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Release 10.1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (Premium Edition)</td>
</tr>
<tr>
<td>Release 10.2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (Premium Edition)</td>
</tr>
</tbody>
</table>
Earlier version of licenses, including those compatible with release 7.x, are not supported with the newer SD-WAN software release. The existing process to obtain SD-WAN licenses remains consistent with the CloudBridge 8.0.x, and 9.0.x releases. Once obtained, the licenses can be activated through the appliance’s management web interface.

The following table lists all the appliance models supported in Citrix SD-WAN release 10.2:

<table>
<thead>
<tr>
<th>Platform Edition</th>
<th>License Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Edition VPX</td>
<td>VPX-020, 050, 100, 200, 500, 1000</td>
</tr>
<tr>
<td>Standard Edition VPX-L</td>
<td>VPX-L-020, 050, 100, 200, 500, 1000</td>
</tr>
<tr>
<td>Standard Edition 210/210 LTE (R1/R2/RC), 410</td>
<td>210-20, 210-50, 210–100, 210-200, 410-050, 410-100, 410-200, 410-300</td>
</tr>
<tr>
<td>Standard Edition 1000 and 1100</td>
<td>1000-020, 1000-050, 1000-100, 1100-200, 1100-300, 1100-500</td>
</tr>
<tr>
<td>Standard Edition 4100</td>
<td>4100-2000, 4100-3000</td>
</tr>
<tr>
<td>Standard Edition 5100</td>
<td>5100-4000, 5100-5000, 5100-6000</td>
</tr>
<tr>
<td>WANOP Edition VPX</td>
<td>VPX-2, 6, 10, 20, 50, 100, 200</td>
</tr>
<tr>
<td>WANOP Edition 800</td>
<td>800-002, 800-006, 800-010</td>
</tr>
<tr>
<td>WANOP Edition 1000</td>
<td>1000-006, 1000-010, 1000-020</td>
</tr>
<tr>
<td>WANOP Edition 3000</td>
<td>3000-050, 3000-100, 3000-155</td>
</tr>
<tr>
<td>WANOP Edition 4100</td>
<td>4100-310, 4100-500, 4100–1000</td>
</tr>
<tr>
<td>WANOP Edition 5100</td>
<td>5100–1500, 5100-2000</td>
</tr>
<tr>
<td>Premium (Enterprise) Edition 1000</td>
<td>1000-010, 1000-020, 1000-050, 1000-100</td>
</tr>
<tr>
<td>Premium (Enterprise) Edition 1100</td>
<td>1100-200, 1100-300, 1100-500</td>
</tr>
<tr>
<td>Premium (Enterprise) Edition 2100</td>
<td>2100-200, 2100-300, 2100-500, 2100–1000</td>
</tr>
<tr>
<td>Premium (Enterprise) Edition 5100</td>
<td>5100-3000, 5100-4000</td>
</tr>
</tbody>
</table>

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

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.

**Returning and Reallocating Licenses**

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

**Local licensing**

December 18, 2018

With local license, you are required to login to each appliance in the network and upload the license file. Even with the ZTD service, the appliance becomes available with only a grace license. You will have to upload a license file for 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

December 18, 2018

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

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

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

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

Use Cases:

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

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

Remote license:

1. In the SD-WAN web management interface, navigate to Configuration > Appliance Settings > Licensing.

2. Select Remote and enter the Remote Server-IP address details.

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

December 18, 2018

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

In the new centralized license model, the SD-WAN center web management interface (SD-WAN appliance management and reporting portal), provides licensing services to individual SD-WAN appliances in the network without you having to 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; such as the Standard Edition or Enterprise Edition. Click **Apply**.

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

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

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
</table>
| 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 |
Managing licenses

December 18, 2018

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 heartbeats, 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 an 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 is 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

December 18, 2018
The SD-WAN appliance goes into a 30-day grace period and you have to upload the license after the license expires.

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

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

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

Grace Period:

1. 30 day grace period is provided for Out-of-Box client nodes. Notification indicates that the appliance is in Out-of-Box mode and needs a valid license. This option uses a grace license file.

2. License expiry: Once the license expires, a 30 day grace period is provided. Notification indicates that the reason for grace period is the license expiry and needs a renewal.

3. Loss of communication with SD-WAN center: After 2 heart beats loss, the appliance goes into the grace mode for 30 days. Notification indicates that the reason for the grace period is a communication failure.

Configuration

December 14, 2018
After you have installed the SD-WAN software and licenses, you can configure SD-WAN appliance settings to start managing your network and deployment.

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 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**

December 18, 2018

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

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

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

**Warning**

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

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

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

- About SD-WAN VPX.
- Installing and Deploying a SD-WAN VPX-SE on ESXi.

Overview of Web Interface (UI) Layout

December 14, 2018

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

Basic navigation

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

The basic navigation elements are as follows:
• **Title bar** – This displays the appliance model number, Host IP Address for the appliance, the version of the software package currently running on the appliance, and the user name for the current login session. The title bar also contains the **Logout** button for terminating the session.

• **Main menu bar** – This is the bar displayed below the title bar on every Management Web Interface screen. This contains the section tabs for displaying the navigation tree and pages for a selected section.

• **Section tabs** – The section tabs are located in the main menu bar at the top of the page. These are the top-level categories for the Web Management Interface pages and forms. Each section has its own navigation tree for navigating the page hierarchy in that section. Click a **section tab** to display the navigation tree for that section.

• **Navigation tree** – The navigation tree is located in the left pane, below the main menu bar. This displays the navigation tree for a section. Click a section tab to display the navigation tree for that section. The navigation tree offers the following display and navigation options:
  - Click a section tab to display the navigation tree and page hierarchy for that section.
  - Click + (plus sign) next to a branch in the tree to reveal the available pages for that branch topic.
  - Click a page name to display that page in the page area.
  - Click – (minus sign) next to a branch item to close the branch.

• **Breadcrumbs** – This displays the navigation path to the current page. The breadcrumbs are 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 navigation tree hierarchy

<table>
<thead>
<tr>
<th>TOP LEVEL SECTION TAB</th>
<th>TREE LEVEL 1</th>
<th>TREE LEVEL 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>System Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local Versions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Virtual Path Service Status</td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td>Statistics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flows</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Routing Protocols</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IKE/IPsec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IGMP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Performance Reports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>QoS Reports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Usage Reports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Appliance Reports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCP Server/Relay</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VRRP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WAN Optimization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compression</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Usage Graph</td>
<td></td>
</tr>
<tr>
<td></td>
<td>App Flow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Filesystem (CIFS/SMB)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Citrix (ICA/CGP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICA Advanced</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outlook (MAPI)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Partners</td>
<td></td>
</tr>
<tr>
<td>Configuration</td>
<td>Appliance Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administrator Interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Logging/Monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Adapters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Net Flow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>App Flow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NITRO API</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Licensing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Virtual WAN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration Editor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change Management Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restart/Reboot Network</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable/Disable/Purge Flows</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamic Virtual Paths</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SD-WAN Center Certificates</td>
<td></td>
</tr>
<tr>
<td>System Maintenance</td>
<td>Delete Files</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restart System</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Date/Time Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local Change Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Diagnostics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Update Software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration Reset</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Factory Reset</td>
<td></td>
</tr>
</tbody>
</table>
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.  
2. Select the Configuration tab.  
3. In the navigation tree, click + next to the Virtual WAN branch in the tree. This displays the available pages for the Virtual WAN category.  
4. In the Virtual WAN branch of the tree, select Configuration Editor.

The 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

December 14, 2018

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.
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**

December 14, 2018

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 personal computer. You can then open a browser on the PC and connect directly to the Management Web Interface on the appliance, where you can set the Management IP Address for that appliance. The Management IP Address must be unique for each appliance.

The procedures are different for setting the Management IP Address for a hardware SD-WAN Appliance and a VPX Virtual Appliance (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 need to change the Ethernet port settings on the PC before you can set the appliance Management IP Address. Be sure to record the original settings so you can restore them after configuring the Management IP Address.

3. Change the IP Address for the PC.
   On the PC, open your network interface settings and change the IP Address for your PC to the following:
   • 192.168.100.50

4. Change the **Subnet Mask** setting on your PC to the following:
   • 255.255.0.0

5. On the PC, open a browser and enter the default IP Address for the appliance. Enter the following IP Address in the address line of the browser:
   • 192.168.100.1

   **Note**
   It is recommended that you use Google Chrome browser when connecting to 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 Adaptors**. This displays the **Network Adaptors** settings page with the **IP Address** tab preselected by default, as shown in the below figure.

![Network Adaptors settings page]

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**

December 18, 2018

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

December 14, 2018

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
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**

December 14, 2018

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

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

1. In the SD-WAN web management interface, navigate to Configuration > Appliance Settings > Logging/Monitoring and click Alarm Options.

2. Click Add Alarm to add a new alarm.

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**

December 14, 2018
The Configuration Rollback feature allows the Change Management system to detect and recover from certain software / configuration errors by reverting to the previously active software/configuration. Not all failure modes result in a rollback. This feature can detect network outage and appliance crash.

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

If a system configuration error occurs on a client while activating 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 10 minutes. If the software crashes within 10 minutes, or if the network is down (unable to establish a Virtual Path to the MCN) for 10 minutes, then a rollback is triggered.

On the MCN, an error message appears as shown in the 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

December 18, 2018

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:
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

December 18, 2018

The Master Control Node (MCN) is the central Virtual WAN Appliance that acts as the master controller of the Virtual WAN, and the central administration point for the client nodes. All configuration activities, as well as preparation of the appliance packages and their distribution to the clients, are performed on the MCN. In addition, certain Virtual WAN monitoring information is available only on the MCN. The MCN can monitor the entire Virtual WAN, whereas client nodes can monitor only their local Intranets, along with some information for those clients with which they are connected.
The primary purpose of the MCN is to establish and utilize Virtual Paths with one or more client nodes located across the Virtual WAN, for Enterprise Site-to-Site communications. An MCN can administer and have Virtual Paths to multiple client nodes. There can be more than one MCN, but only one can be active at any given time.

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

### Switch to MCN Console

December 14, 2018

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

**Note**

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

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

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

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**

December 18, 2018

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, please 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 should then reset it to a lower threshold after completing those tasks. For instructions, see the section Setting the Console Session Timeout Interval (Optional)

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

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

2. Click New to start defining a new configuration. This displays the New configuration settings
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.
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 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.

**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
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**, and **VLAN ID** ids.

9. Enter the **Name** and **VLAN ID** for this Virtual Interface Group.
   - **Name** – This is the name by which this Virtual Interface 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.

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. Click **Apply**. This adds the address information to the site and includes it in the site **Virtual IP Addresses** table.

6. To add more Virtual IP Addresses, click + to the right of the **Virtual IP Addresses**, and proceed as above.

**How to configure WAN links for the MCN**

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

1. Continuing in the **Sites** view for the new MCN site, click the **WAN Links** label.
2. Click **Add Link** to the right of the **WAN Links** to add a new WAN link. This opens the **Add** dialog box.

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

4. Select the **Access Type** from the drop-down menu. The options are **Public Internet**, **Private Intranet**, or **Private MPLS**.

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

---

**Auto Learn of bandwidth consumption**

Auto learn runs on system startup and repeats every 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.

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 checkbox 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.

The options are as follows:

   • **Virtual Path** – This service manages traffic across the Virtual Paths. A Virtual Path is a logical link between two WAN links. It comprises a collection of WAN Paths combined to provide high service-level communication between two SD-WAN nodes. This is accomplished by constantly
measuring and adapting to changing application demand and WAN conditions. SD-WAN Appliances measure the network on a per-path basis. A Virtual Path can be static (always exists) or dynamic (exists only when traffic between two SD-WAN Appliances reaches a configured threshold).

- **Internet** – This service manages traffic between an Enterprise site and sites on the public Internet. Traffic of this type is not encapsulated. During times of congestion, the SD-WAN actively manages bandwidth by rate-limiting Internet traffic relative to the Virtual Path, and Intranet traffic according to the SD-WAN configuration established by the Administrator.

- **Intranet** – This service manages Enterprise Intranet traffic that has not been defined for transmission across a Virtual Path. As with Internet traffic, it remains unencapsulated, and the SD-WAN manages bandwidth by rate-limiting this traffic relative to other service types during times of congestion. 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.

- **Gateway IP Address** – Enter 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.

Depending on the “Service Type,” the following settings are displayed:

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

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.

<table>
<thead>
<tr>
<th>Network IP Address</th>
<th>Cost</th>
<th>Service Type</th>
<th>Gateway IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>5</td>
<td>Virtual Path</td>
<td></td>
</tr>
</tbody>
</table>

Next Hop Site: Branch1 ▼

Eligibility Based On Path

Path: Branch1-WL-1->MCN-DC-WL-1 ▼

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)

December 14, 2018

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

Note

Enabling Virtual WAN security and encryption is optional.

1. Navigate to the Basic tab in the Configuration Editor, Select Global from View mode. The Virtual Network Settings configuration form is displayed.
2. Click **Edit** (pencil icon) to enable editing for the form.

![Edit icon]

**Note:** Changing the **Network Encryption Mode** may cause Site Secure Keys to be truncated or regenerated if they do not meet the requirements of the new mode.

- **Network Encryption Mode**
  - AES 128-Bit
  - AES 256-Bit

- **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**

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**

December 14, 2018

You can configure a site as the secondary MCN to support MCN redundancy. The secondary MCN continuously monitors the health of the primary MCN. If the primary MCN fails, the secondary MCN assumes the role of the MCN. To create a secondary MCN, while adding a new site in the **Mode** option select secondary MCN. You 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](#).

The secondary MCN appliance need not be the same platform model as the primary MCN. You can choose an appliance model based on the usage, bandwidth requirement, and the number of sites to be supported.

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

The best way to configure a secondary MCN would be to clone the existing MCN as it retains most of the MCN configuration. When a site is cloned, the entire set of configuration settings for the site are copied and displayed in a single form screen. You can then modify the settings according to the requirements quickly and easily.
Note
You can clone an MCN to create a secondary MCN or branch sites. You can configure only one secondary MCN.

To clone an MCN site and create a secondary MCN:

1. In the Configuration Editor, navigate to Basic > Sites, and click the clone icon for the MCN site.

2. Enter the configuration parameter settings for the new site.
3. In the **Mode** field, select **secondary MCN**. Resolve all Audit Alerts.

4. Click **Clone** to create the secondary MCN site.

## Manage MCN Configuration

**December 14, 2018**

The next step is to name and save the new configuration, seen also as a configuration package. This step is optional at this point in the configuration, but recommended. The configuration package is saved to your workspace on the local appliance. You then 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](/en-us/citrix-sd-wan/10-2/configuration/setup-branch-nodes.html).

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/10-2/configuration/setup-branch-nodes.html).

**Export backup copy of the configuration package**

In addition to saving the configuration-in-progress to your appliance workspace, it 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.

![Name Conflict dialog box](image)

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

November 22, 2018

This chapter provides instructions for adding and configuring the branch sites. The procedure for adding a branch site is very similar to creating and configuring the MCN site. However, some of the configuration steps and settings do vary slightly for a branch site. In addition, once you have added
an initial branch site, for sites that have the same appliance model you can use the Clone (duplicate) feature to streamline the process of adding and configuring those sites.

As with creating the MCN site to set up a branch site you must use the Configuration Editor in the Management Web Interface on the MCN appliance. The Configuration Editor is available only when the interface is set to MCN Console mode.

Supplemental Branch Site Deployment Information

In addition to this guide, the following Knowledge Base support articles are also recommended:

- Virtual WAN PBR Mode Deployment Steps (CTX201577)
  http://support.citrix.com/article/CTX201577
- 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

To add a new branch site to the Sites table and begin configuring the site, do the following:

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.

   • **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 auto-
matically 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.

![Basic Settings configuration form](image)

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. Click Apply. The address information to the site is added and includes it in the site Virtual IP Addresses table.

6. To add more Virtual IP Addresses, click + to the right of the Virtual IP Addresses, and proceed as above.
How to configure WAN links for the branch

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

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

2. Click Add Link to the right of the WAN Links to add a new WAN link. The Add dialog box appears.

3. (Optional) type a name for the WAN Link if you do not want to use the default.
   
   The default is the site name, appended with the following suffix:

   -WL:<number>

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

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

   The options are Public Internet, Private Intranet, or Private Multiprotocol Label Switching.

5. Click Add. The WAN Links Basic Settings configuration page appears and adds the new unconfigured WAN link to the page.
6. Type the link details for the new WAN link. Configure the LAN to WAN, WAN to LAN settings. Some guidelines are as follows:
   - Some Internet links might be asymmetrical. Misconfiguring the permitted speed can adversely affect performance for that link.
   - Avoid using burst speeds that surpass the Committed Rate.
   - For Internet WAN links, be sure to add the Public IP Address.

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

8. Type the Advanced Settings for the link.
• **Provider ID** – (Optional) type a unique ID number 1–100 to designate WAN Links connected to the same service provider. Virtual WAN uses the Provider ID to differentiate paths when sending duplicate packets.

• **Frame Cost (bytes)** – type the size (in bytes) of the header/trailer added to each packet. For example, the size in bytes of added Ethernet IPG or AAL5 trailers.

• **Congestion Threshold** – type the congestion threshold (in microseconds) after which the WAN link throttles packet transmission to avoid further congestion.

• **MTU Size (bytes)** – type the largest raw packet size (in bytes), not including the Frame Cost.

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

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

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

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

  \[\text{WAN\_link\_name-\text{AI-number}}\]

  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 Fall-back on the Virtual Path, traffic that ordinarily travels with a Virtual Path can instead be treated as Intranet traffic, to maintain network reliability.

  • **Passthrough** – This service manages traffic that is to be passed through the Virtual WAN. Traffic directed to the Passthrough Service includes broadcasts, ARPs, and other non-IPv4 traffic, and traffic on the Virtual WAN Appliance local subnet, configured subnets, or Rules applied by the Network Administrator. This traffic is not delayed, shaped, or changed by the SD-WAN. Therefore, you must ensure that Passthrough traffic does not consume substantial resources on the WAN links that the SD-WAN Appliance is configured to use for other services.

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

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

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

  • **Gateway IP Address** – type the Gateway IP Address for this route.
- **Eligibility Based on Path** (checkbox) – (Optional) If enabled, the route 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)

December 14, 2018

This section provides instructions for cloning the new branch site for use as a partial template for adding more branch sites.

Note

Cloning the site is optional. The Virtual WAN appliance models must be the same for both the original and the cloned sites. You cannot change the specified appliance model for a clone. If the appliance model is different for a site, you must manually add the site, as instructed in the previous sections.
Cloning a site streamlines the process of adding and configuring 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

November 22, 2018

An Audit Alert icon (a red dot or goldenrod delta) next to an item indicates a configuration error or missing parameter information for that item. A number next to the icon indicates the number of associated errors for that alert. To see bubble help for a particular alert, roll your cursor over the alert icon. This displays a brief description of the specific errors flagged by that alert. You must resolve all Audit Alerts in the configuration, or you will not be able to verify, stage, and activate the configuration package, later in the deployment process.

Resolving all of the Audit Alerts (if any), completes the Sites phase of the configuration. The next step is to save the completed Sites configuration.
Configuring the virtual path service between the MCN and client sites

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.

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.

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.
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
Citrix SD-WAN 10.2

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).

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 Enterprise Edition** – The Enterprise Edition includes the full set of WAN Optimization features. If you want to configure WAN Optimization for your sites, please proceed to the Enabling and Configuring WAN Optimization topic. Otherwise, you can proceed directly to Preparing the SD-WAN Appliance Packages on the MCN.

- **SD-WAN Edition** – This Edition does not include the WAN Optimization features. You can now proceed directly to Preparing the SD-WAN Appliance Packages on the MCN.

**Deploy MCN Configuration**

December 14, 2018

The next step is to prepare the SD-WAN Appliance Packages for distribution to the client nodes. This involves the following two procedures:

1. Export the Configuration Package to Change Management.

   Before you can generate the Appliance Packages, you must first export the completed configuration package from the Configuration Editor to the global Change Management staging inbox on the MCN. Instructions are provided in the section Perform Change Management.

2. Generate and stage the Appliance Packages.

   After you have added the new configuration package to the Change Management inbox, you can generate and stage the Appliance Packages. To do this, you will use the Change Management wizard in the Management Web Interface on the MCN. Instructions are provided in the section Deploy Configuration to Branches.
Perform MCN Change Management

December 14, 2018

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

To export the configuration package to Change Management, do the following:

1. In the Configuration Editor page, click Export (at the top of the page).

   ![Configuration Editor](image)

   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.

   ![Export Configuration](image)

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

December 18, 2018

After you have prepared the configuration using the configuration editor and exported the configuration package to the change management inbox, the next step is to prepare the SD-WAN Appliance Packages for distribution to the client nodes. 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.

![Appliance Staging Page](image)

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.

Select **Ignore incomplete**, when adding more sites to the network or if the site is in **not connected** state. This indicates that the client sites should be ignored for this staging operation, and only the MCN should be updated and staged.

9. Select **Revert on Error** to revert to previous application package on encountering some error. For more information, see Configuration Rollback.

10. Click **Activate Staged**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
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, 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 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.

   ![Message 1](image1.png)

   13. Click **OK**.

   14. Click **Activate staged**.

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

   ![Message 2](image2.png)
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/10-2/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**

December 14, 2018
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.

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

November 22, 2018

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

December 14, 2018

After you have prepared the appliance packages and connected the MCN, and the branch site administrators have connected their respective client appliances to the LAN and WAN, the next step is to
upload and activate the appropriate SD-WAN appliance package on each client. The Change Management wizard guides you through this process.

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

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

   ![Change Process Overview](image)

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 appliance packages.
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.

Checklist and how to deploy

January 22, 2019

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 Enterprise Editions.

To view some of the deployment 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

**Deployments**

December 14, 2018
Following are some of the use case scenarios implemented by using Citrix SD-WAN appliances:

- Deploying SD-WAN in Gateway Mode
- Deploying SD-WAN in PBR mode (Virtual Inline Mode)
- Dynamic Paths for Branch to Branch Communication
- Static WAN Paths
- Building an SD-WAN Network
- Routing for LAN Segmentation
- Utilizing Enterprise Edition Appliance to Provide WAN Optimization Services Only
- Two Box Mode
- Zero Touch Deployment
- Single Region Deployment
- Multi Region Deployment
- High Availability

**Gateway mode**

December 18, 2018

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.

Gateway mode places the SD-WAN appliance physically in the path (two-arm deployment) and requires changes in the existing network infrastructure to make the SD-WAN appliance the default gateway for the entire LAN network for that site.

**Note**

An SD-WAN deployed in Gateway mode acts as a Layer 3 device and cannot perform fail-to-wire. All interfaces involved will be configured for “Fail-to-block”. In the event of appliance failure, the default gateway for the site will also fail, causing an outage until the appliance and default gateway are restored.

**Topology**

The following illustrations describe the topologies supported in an SD-WAN network.
DataCenter in gateway deployment

Branch in inline deployment

Deployment requirements

Deployment requirements and related information are described below to assist you in building the configuration.

<table>
<thead>
<tr>
<th>Site Name</th>
<th>DataCenter Site</th>
<th>Branch Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Name</td>
<td>A_DC1</td>
<td>A_BRI</td>
</tr>
</tbody>
</table>
### 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 should 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.

### Datacenter site gateway mode configuration

Following are the high-level configuration steps to configure Datacenter 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.

![Image of Access Interfaces setup]

**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.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Virtual Interface</th>
<th>Firewall Zone</th>
<th>Identity</th>
<th>Private</th>
<th>Security</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.20.92</td>
<td>INET_BR-3-4 (0)</td>
<td>Default_LAN_Zone</td>
<td>✔️</td>
<td>✔️</td>
<td>Trusted</td>
<td></td>
</tr>
<tr>
<td>192.168.20.92</td>
<td>MPLS_BR-1-2 (0)</td>
<td>Default_LAN_Zone</td>
<td>✔️</td>
<td>✔️</td>
<td>Trusted</td>
<td></td>
</tr>
<tr>
<td>192.133.58.82</td>
<td>VirtualInterface-2</td>
<td>Default_LAN_Zone</td>
<td>✔️</td>
<td>✔️</td>
<td>Trusted</td>
<td></td>
</tr>
</tbody>
</table>

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 backend 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.

Virtual inline mode

April 19, 2019

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 needs to be configured either at the core switch or further upstream at the router. The router must monitor the health of the SD-WAN appliance so that the appliance can be bypassed if it fails.
- Virtual Inline Mode places the SD-WAN appliance physically out of path (one-arm deployment) that is, only a single Ethernet interface to be used (Example: Interface 1/1) with bypass mode set to fail-to-block (FTB).
Citrix SD-WAN appliance needs to be configured to pass traffic to the proper gateway. Traffic intended for the Virtual Path is directed towards the SD-WAN appliance and then encapsulated and directed to the appropriate WAN link.

**Gather information for configuration**

- Accurate network diagram (example diagram show below) 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 (example diagram shown below)

**Data center topology – Virtual inline mode**
# Branch topology – inline mode

![Diagram of branch topology](image)

<table>
<thead>
<tr>
<th>Site Name</th>
<th>DataCenter Site</th>
<th>Branch Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Name</td>
<td>SJC-DC</td>
<td>SJC-BR</td>
</tr>
<tr>
<td>Management IP</td>
<td>172.30.2.10/24</td>
<td>172.30.2.20/24</td>
</tr>
<tr>
<td>Security Key</td>
<td>If any</td>
<td>If any</td>
</tr>
<tr>
<td>Model/Edition</td>
<td>4000</td>
<td>2000</td>
</tr>
<tr>
<td>Mode</td>
<td>Virtual Inline Mode</td>
<td>Inline</td>
</tr>
<tr>
<td>Topology</td>
<td>2 x WAN Path</td>
<td>2 x WAN Path</td>
</tr>
<tr>
<td>VIP Address</td>
<td>192.168.1.10/24 – MPLS, 192.168.1.11/24 – Internet, Public IP w.x.y.z</td>
<td>10.17.0.9/24 - MPLS, 10.18.0.9/24 – Internet, Public IP a.b.c.d</td>
</tr>
<tr>
<td>Gateway MPLS</td>
<td>10.20.0.1</td>
<td>10.17.0.1</td>
</tr>
<tr>
<td>Gateway Internet</td>
<td>10.19.0.1</td>
<td>10.18.0.1</td>
</tr>
<tr>
<td>Link Speed</td>
<td>MPLS – 100 Mbps, Internet – 20 Mbps</td>
<td>MPLS – 10 Mbps, Internet – 2 Mbps</td>
</tr>
</tbody>
</table>

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Need to add a route on the SD-WAN SE Appliance on how to reach the LAN Subnets (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, etc) through any of the physical interfaces: Gi0/1 - 192.168.1.1, Configuration > Virtual WAN > Configuration Editor > SJC_DC > Routes. In this example interface 192.168.1.1 was used: - 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

Steps to configure a site in Virtual Inline Mode:

- Enable the MCN functionality.
- Create a New site.
- Create an Interface Group and Virtual Interfaces.
- Assign Virtual IP Address to Virtual Interfaces.
- Create WAN Links and assign IP address.
- Add Routes.
- Troubleshooting.
- Routing policy configuration on the router.

**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 should only be one active MCN in an SD-WAN network.

2. Enable Virtual WAN Service. Navigate to **Configuration > Virtual WAN > Enable/Disable/Purge Flows**.

3. Start Configuration by navigating to **Configuration > Virtual WAN > Configuration Editor**. Click **New** to begin configuration.
   
   This operation creates an Untitled_1 initial configuration file which can be renamed [optional] later using the **Save As** button.

Following are the high-level configuration steps to configure Datacenter site in virtual inline deployment mode:

1. Create a DC site.

2. Configure Interface Groups based on connected Ethernet interfaces.

3. Configure Virtual IP address for each virtual interface.

4. Populate WAN links based on physical rate and not burst speeds using Internet and MPLS Links.

5. Populate Routes if there are more subnets in the LAN infrastructure.

**Datacenter site virtual inline mode configuration**

**Create a DC site**

1. Navigate to **Configuration Editor > Sites**, and click the **+ Site** button.

2. Populate the fields as shown below.

3. Keep default settings unless instructed to change.
Configure interface groups based on connected Ethernet interfaces

1. In the Configuration Editor, navigate to **Sites \[Site Name\] \Interface Groups**. Click “+” to add interfaces intended to be used. In virtual inline mode, configuration on only a single Ethernet interface is used that is, interface connecting the upstream router providing routing policy implications (Example- Interface 1/1). Configure MPLS and internet virtual interfaces with VLAN ID 10 and 20 respectively.

2. Bypass mode is set to fail-to-block since only one Ethernet/physical interface is used per virtual interface. There are also no Bridge Pairs.

3. In this example, expand Virtual Interfaces + option and configure the Virtual Interfaces.
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.

Create Internet WAN link

To populate WAN links based on physical rate and not on burst speeds using Internet and MPLS link:

1. Navigate to WAN Links, click the “+” button to add a WAN Link for the Internet link.
2. Populate Internet link details, including the supplied Public IP address as shown below. Note that Auto Detect Public IP cannot be selected for SD-WAN appliance configured as MCN.
3. Navigate to Access Interfaces, click the “+” button to add interface details specific for the Internet link.
4. Populate Access Interface for IP and gateway addresses as shown below. The Proxy ARP is not checked for less than two Ethernet interfaces.
Create MPLS Link

1. Navigate to **WAN Links**, click the “+” button to add a WAN Link for the MPLS link.
2. Populate MPLS link details as shown below.
3. Navigate to **Access Interfaces**, click the “+” button to add interface detail specific for the MPLS link.
4. Populate Access Interface for MPLS Virtual IP and gateway addresses as shown below.

---

**Note**

The Proxy ARP is not checked for less than two Ethernet interfaces.
Citrix SD-WAN 10.2

**Populate routes**

On the Data center site, add a route on the SD-WAN SEE appliance to reach the LAN Subnets (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, etc) through any of the physical interfaces:

0/1/0.1 – 192.168.1.1 on VLAN 10

0/1/0.2 – 192.168.2.1 on VLAN 20

<table>
<thead>
<tr>
<th>Order</th>
<th>Network ID Address</th>
<th>Cost</th>
<th>Service Type</th>
<th>Service Name</th>
<th>Gateway IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.10.13.0/24</td>
<td>5</td>
<td>Local</td>
<td></td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>2</td>
<td>10.10.12.0/24</td>
<td>5</td>
<td>Local</td>
<td>BR571</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>3</td>
<td>10.10.11.0/24</td>
<td>5</td>
<td>Local</td>
<td>BR572</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>4</td>
<td>192.175.60.0/24</td>
<td>5</td>
<td>Virtual Path</td>
<td>BR573</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>192.175.61.0/24</td>
<td>5</td>
<td>Virtual Path</td>
<td>BR574</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>192.175.62.0/24</td>
<td>5</td>
<td>Virtual Path</td>
<td>BR575</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>172.111.64.5/24</td>
<td>5</td>
<td>Local</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.
   • Virtual Interface “INTERNET” configured on Bridge pair 1/3 and 1/4
   • Virtual Interface “MPLS” configured con Bridge Pair 1/1 and 1/2

5. Populate Routes if there are more subnets in the LAN infrastructure.

Create a branch site

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. Bypass mode is set to fail-to-wire since two Ethernet/physical interfaces are used per virtual interface. There are two bridge Pairs.

3. Populate WAN links based on physical rate and not burst speeds using Internet and MPLS Links.
   • Virtual Interface “INTERNET” configured on Bridge pair 1/3 and 1/4
   • Virtual Interface “MPLS” configured con Bridge Pair 1/1 and 1/2.

4. Refer to the sample “Remote Site Inline Mode” topology above and populate the Interface Groups fields as shown below.
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.

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 “+” button to add a WAN Link for the Internet link.
2. Populate Internet link details, including the AutoDetect Public IP address as shown below.
3. Navigate to Access Interfaces, click the “+” button to add interface details specific for the Internet link.
4. Populate Access Interface for Virtual IP address and gateway as shown below.
Create MPLS Link

1. Navigate to **WAN Links**, click the “+” button to add a WAN Link for the MPLS link.

2. Populate MPLS link details as shown below.

3. Navigate to **Access Interfaces**, click the “+” button to add interface details specific for the MPLS link.

4. Populate Access Interface for Virtual IP address and gateway as shown below.
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 to reach those backend subnets.

<table>
<thead>
<tr>
<th>Network IP Address</th>
<th>Cost</th>
<th>Service Type</th>
<th>Gateway IP Address</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.17.0.9/24</td>
<td>5</td>
<td>Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.18.0.9/24</td>
<td>5</td>
<td>Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>16</td>
<td>Passthrough</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Resolving audit errors

After completing configuration for DC and Branch sites, you will be alerted to resolve audit error on both DC and BR sites. In this example, we will resolve the Audit Error related to Private Intranet WAN Link [SJC_DC-MPLS].

Note

By default the system generates paths for WAN Links defined as access type Public Internet (highlighted).

Audit Error:

At Site 'SJC_DC' WAN Link 'SJC_DC-MPLS': no 'add Virtual Path usage' command was successful

Audit Error:

WAN link 'SJC_DC-MPLS' has usage for Virtual Path 'SJC-BR-SJC_DC', but no paths were added to or from this WAN link for this Virtual Path

You would be required to use the auto-path group function or enable paths manually for WAN Links with an access type of Private Internet. Paths for MPLS links can be enabled by clicking the Add operator (in the green rectangle).
Create an Autopath Group:

1. Navigate to **Global** tab. Click on the [+ ] sign next to **Autopath Groups**.

2. Configure the Autopath Group created as per requirement and click **Apply**.

3. Rename the Autopath Group [Optional].

4. Map the Autopath Group to the Virtual Paths of Intranet WAN links at respective sites.

   No two Autopath Groups can be marked as default. If marked would lead to an Audit Error.

After mapping the Autopath Group to the Virtual Paths of Intranet WAN, the paths should be automatically populated (highlighted).
Manually add WAN links with access type Private Intranet

1. Select the Virtual Paths under WAN Links for respective sites and no Autopath Group would be mapped.
2. Click the [+] sign next to Paths to add Virtual Paths manually.
3. Select the Virtual Paths WAN Links for each site.

After manually adding the virtual paths for WAN links with access type Private Intranet, it gets populated under Paths (highlighted).

After completing all the above steps, proceed to Preparing the SD-WAN Appliance Packages on the MCN topic.

Policy based routing configuration on the PBR router:

Interface connected to the LAN

- Router# configure terminal
Router(config)# interface FastEthernet0/1
Router(config-if)# description ToLAN
Router(config-if)# ip address 10.10.11.1 255.255.255.0
Router(config-if)# duplex auto
Router(config-if)# speed auto

Interface connects to the MPLS WAN Link

Router# configure terminal
Router(config)# interface GigabitEthernet0/0
Router(config-if)# description To-MPLS-WAN
Router(config-if)# ip address 10.20.0.2 255.255.255.0
Router(config-if)# duplex auto
Router(config-if)# speed auto

Interface connected to the INET WAN Link

Router# configure terminal
Router(config)# interface GigabitEthernet0/2/0
Router(config-if)# description To-INET-WAN
Router(config-if)# ip address 10.19.0.2 255.255.255.0
Router(config-if)# duplex auto
Router(config-if)# speed auto

Interface GigabitEthernet0/1 on the PBR router is connected to the SD-WAN port 1/1, it is in 1-arm mode and this one port will serve traffic for MPLS and INET links.

Router# configure terminal
Router(config)# interface GigabitEthernet0/1
Router(config-if)# description To-SDWAN-link
Router(config-if)# ip address 192.168.1.1 255.255.255.0

Static Route Configuration (Route to the client/remote subnets):

MPLS 10.17.0.0/24 via next hop WAN router MPLS 10.20.0.1
INET 10.18.0.0/24 via next hop WAN router/FW INET 10.19.0.1

Router# configure terminal
Router(config)# ip route 10.17.0.0 255.255.255.0 10.20.0.1
Citrix SD-WAN 10.2

- Router(config)# ip route 10.18.0.0 255.255.255.0 10.19.0.1

**Route map definition:**

**Access Control List Configuration:**

Configure ACLs to define the traffic to be sent to and from the SD-WAN appliance.

1. From LAN to SD-WAN Appliance

   As per topology, the LAN subnets are 10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, etc. To send traffic from LAN to the SD-WAN, configure a unidirectional ACL (from LAN to any).

   ```
   1 - Router\# configure terminal
   2 - Router(config)# ip access-list extended server\_side
   3 - Router(config)# permit ip 10.10.0.0 0.0.255.255 any
   
   1. From SD-WAN Appliance to physical WAN Links
   ```

   ```
   1 - Router\# configure terminal
   2 - Router(config)# ip access-list extended MPLS\_Link
   3 - Router(config)# permit ip 192.168.1.10 0.0.0.0 any
   4 - Router(config)# ip access-list extended INET\_Link
   5 - Router(config)# permit ip 192.168.1.11 0.0.0.0 any
   
   **Route Map Configuration:**

   Define the route-map matching the ACLs.

   **Route map for LAN traffic:**

   Next hop will be any of SD-WAN Virtual IPs (VIP).

   MPLS VIP 192.168.1.10

   INET VIP 192.168.1.11

   In this case, we chose MPLS VIP 192.168.1.10 as next hop and also added a health check to make sure if the SD-WAN fails, traffic is not routed to it.

   ```
   1 - Router\# configure terminal
   
   © 1999-2019 Citrix Systems, Inc. All rights reserved.
The above command configures the route map to verify the reachability of the tracked object. The tracking process provides the ability to track individual objects, such as ICMP ping reachability, routing adjacency, an application running on a remote device, a route in the Routing Information Base (RIB) or to track the state of an interface line protocol.

**Route map for WAN traffic:**

Next hop will be MPLS Router and Firewall for respective WAN links.

**Apply the Route Map to the interface:**
Build a SD-WAN network

December 14, 2018

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.

SD-WAN overlay dynamic network routing

WAN optimization only with Premium (Enterprise) edition

December 18, 2018

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 Enterprise Edition appliances to utilize WAN optimization services.

Citrix SD-WAN Product Platform Editions include the following appliances:

- SD-WAN: SD-WAN Standard 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 Enterprise 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.

**Hairpin Mode**

December 14, 2018

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.
Two box mode

February 22, 2019

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 exam-
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.
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 Settings](image)

**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 upgrade upg for SD-WAN WANOP.
- Data path integration should be configured between SD-WAN SE and External WANOP appliances through the WCCP deployment mode.
  - At data path level both WCCP and Virtual WAN features are offered through data path integration between WANOP and SE externally in one-arm mode to obtain optimization benefits.

**Unified Configuration and Monitoring**

When you enable the two box mode with SD-WAN SE and SDWAN-WANOP appliances, you can view the configuration in the SD-WAN SE appliance similar to how you can view two box configuration with the SD-WAN-EE appliance.

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 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_wa_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**

April 30, 2019

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 Virtual Router Redundancy Protocol (VRRP) and use a proprietary SD-WAN protocol. Both Client Nodes (Clients) and Master Control Nodes (MCNs) within an SD-WAN network can be deployed in a high availability configuration. The primary and secondary appliance must be the same platform models.

In high availability configuration, one SD-WAN appliance at the site is designated as the Active appliance and is monitored by the Standby appliance. Configuration is mirrored across both appliances. If the Standby appliance loses connectivity with the Active appliance for a defined period, the Standby appliance assumes the identity of the Active appliance and takes over the traffic load. Depending on the deployment mode, this fast failover has minimal impact on the application traffic passing through the network.

**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 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:**

If both active and standby SD-WAN appliances become inactive, the router tries to redirect traffic to the SD-WAN appliances. You can tracked through an IP to verify if the virtual path is up or down. IP SLA monitoring can be configured at the router to disable PBR, if the next appliance is not reachable. This allows the router to fall back to perform a route lookup and forward packets appropriately.

**Parallel Inline high availability mode:**

In Parallel Inline high availability mode, the SD-WAN appliances are deployed alongside each other, inline with the data path. Only one path through the Active appliance is used. It is important to note that bypass interface groups are configured to be fail to block and not fail to wire so that you don’t get bridging loops during a failover.

The high availability state can be monitored through the inline interface groups, or through a direct connection between the appliances. External Tracking can be used to monitor the reachability of the upstream or downstream network infrastructure. For example; switch port failure to direct high availability state change, if needed.

If both active and standby SD-WAN appliances are disabled or fail, a tertiary path can be used directly between the switch and router. This path must have a higher spanning tree cost than the SD-WAN paths so that it is not used under normal conditions. Failover in parallel inline high availability mode is a quick and nearly hitless, because no physical state change occurs. Fallback to the tertiary path is not hitless and can block traffic for 5-30 seconds depending on the spanning tree configuration. If there are out of path connections to other WAN Links, both appliances must be connected to them.
In more complex scenarios, where multiple routers might be using VRRP, non-routable VLANs are recommended to ensure that the LAN side switch and routers are reachable at layer 2.

**Fail-to-Wire mode:**

In fail-to-wire mode, the SD-WAN appliances are inline in the same data path. The bypass interface groups should be in the fail-to-wire mode with the Standby appliance in a passthrough or bypass state. A direct connection between the two appliances on a separate port must be configured and used for the high availability interface group.

**Note**

- High availability switchover in fail-to-wire mode takes longer period, approximately 10–12 seconds because of delay in ports to recover from Fail-to-Wire state.
- If the high availability connection between the appliances fails, both appliances go into Active state and cause a service interruption. This can be mitigated by assigning multiple high availability connections so that there is no single point of failure.
- It is imperative that in high availability Fail-to-Wire Mode, a separate port is used in the hardware appliance pairs for high availability control exchange mechanism to help with state convergence.

- Because of a physical state change when the SD-WAN appliances switch over from Active to Standby, failover can cause partial loss of connectivity depending on how long the auto-negotiation takes on the Ethernet ports.

- It is recommended that Fail-to-Wire mode is used on ports that are auto negotiated, as this increases failover time.

The following illustration shows an example of the Fail-to-Wire deployment.

The One-Arm high availability configuration or Parallel Inline high availability configuration is recommended for data centers or Sites that forward a high volume of traffic to minimize disruption during failover.

If minimal loss of service is acceptable during a failover, then Fail-to-Wire high availability mode is a better solution. The Fail-to-Wire high availability mode protects against appliance failure and parallel inline high availability protects against all failures. In all scenarios, high availability is valuable to preserve the continuity of SD-WAN network during a system failure.

**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**: This is the name of the high availability (secondary) appliance.

- **Failover Time**: This specifies the wait time (in milliseconds) after contact with the primary appliance is lost, before the standby appliance becomes active.

- **Shared Base MAC**: This is the shared MAC address for the high availability pair appliances. When a failover occurs, the secondary appliance has the same virtual MAC addresses as the failed primary appliance.

- **Swap Primary/Secondary**: When this is selected, if both appliances in the high availability pair come up simultaneously, the secondary appliance becomes the primary appliance, and takes precedence.

- **Primary Reclaim**: When this is selected, the designated primary appliance reclaimed control
upon restart after a failover event.

- **High availability Fail-to-Wire Mode:** Select this for Fail-to-wire high availability deployment mode.

  **Note**

  For hypervisor and cloud based platforms an extra parameter **Disable Shared Base MAC** is available. Choose this option to disable the shared virtual MAC address.

  **Note**

  For hypervisor based platforms ensure that the promiscuous mode is enabled on the hypervisors to allow packet sourcing from high availability shared MAC address. If promiscuous mode is not enabled, you can enable Disable **Shared Base MAC** option.

Click + next to **high availability IP Interfaces to configure interface groups**. Type Values for the following parameters:

- **Virtual Interface** – This is the Virtual Interface to be used for communication between the appliances in the high availability pair. This interface monitors the Active appliance for reachability. For One-Arm high availability mode, only one interface group is required.

- **Primary** – This is the unique Virtual IP address for the primary appliance. The secondary appliance uses this for communication with the primary appliance.

- **Secondary** – This is the unique Virtual IP address for the secondary appliance. The primary appliance uses this for communication with the secondary appliance.

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.
### System Status

<table>
<thead>
<tr>
<th>Name</th>
<th>BLR_DC-Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>4000</td>
</tr>
<tr>
<td>Appliance Mode</td>
<td>MCN</td>
</tr>
<tr>
<td>Management IP Address</td>
<td>10.105.58.172</td>
</tr>
<tr>
<td>Appliance Uptime</td>
<td>3 days, 7 hours, 1 minutes, 43.0 seconds</td>
</tr>
<tr>
<td>Service Uptime</td>
<td>3 days, 6 hours, 39 minutes, 51.0 seconds</td>
</tr>
<tr>
<td>Routing Domain Enabled</td>
<td>Default_RoutingDomain</td>
</tr>
</tbody>
</table>

### High Availability Status

<table>
<thead>
<tr>
<th>Local Appliance</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Appliance</td>
<td>Standby</td>
</tr>
<tr>
<td>Last Update Received</td>
<td>0 seconds ago</td>
</tr>
</tbody>
</table>
For Network Adapter details of Active and Standby high availability appliances, navigate to Configuration > Appliance Settings > Network Adapters > Ethernet tab.
Enable Edge Mode High Availability Using Fiber Optic Y-Cable

April 11, 2019

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**

December 14, 2018

**Note**

The Zero Touch Deployment service is supported only on select Citrix SD-WAN appliances:

- 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)
- SD-WAN 2000 Standard Edition
- SD-WAN AWS VPX instance

Zero Touch Deployment (ZTD) Cloud Service is a Citrix operated and managed cloud-based service which allows discovery of new appliances in the Citrix SD-WAN network, primarily focused on streamlining the deployment process for Citrix SD-WAN at branch or cloud service office locations. The ZTD Cloud Service is publicly accessible from any point in a network via public Internet access. The ZTD Cloud Service is accessed over Secure Socket Layer (SSL) Protocol.

The ZTD Cloud Services securely communicates with backend Citrix services hosting stored identification of Citrix customers who have purchased Zero Touch capable devices (e.g. SD-WAN 410-SE, 2100-SE). The backend services are in place to authenticate any Zero Touch Deployment request, properly
validating association between the Customer Account and the Serial Numbers of 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, etc.)

- 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 (e.g. MGMT, or 0/1).
- Cable the appliance for WAN link connectivity on the Data interfaces (e.g. apA.WAN, apB.WAN, apC.WAN, 0/2, 0/3, 0/5, etc).

*Note*

The interface layout is different each model, so please reference the documentation for identification of data and management ports.
The following prerequisites are required before starting any Zero Touch Deployment service:

- Actively running 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 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 utilize the Zero Touch Deployment Service (or ZTD 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 necessary components to unlock the Zero Touch Deployment features and to make the Zero Touch Deployment option available in the GUI of SD-WAN Center. Zero Touch Deployment is not available by default in the SD-WAN Center software. This is purposely designed to make sure the proper preliminary components on the underlay network are present before allowing an Administrator to initiate any on-site activity involving Zero Touch Deployment.

After a working SD-WAN environment is up and running registration into the Zero Touch Deployment Service is accomplished through creating a Citrix Cloud account login. With SD-WAN Center able to communicate with the ZTD service, the GUI 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 ZTD appliance deployments.

Using the Network Configuration tool in SD-WAN Center, the SD-WAN Administrator will then need to utilize the templates or clone site capability to build out the SD-WAN Configuration to add new sites. The new configuration is used by the SD-WAN Center to initiate the deployment of ZTD for the newly added sites. When the SD-WAN Administrator initiates a site for deployment using the ZTD process, he or she has the option to pre-authenticate the appliance to be used for ZTD by pre-populating
the serial number, and initiating email communication to on-site installer to begin on-site activity.

The Onsite Installer 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 ZTD Service and progress is monitored by utilizing 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 ZTD Agent if new features are available on the branch appliance.

• Authenticate the branch appliance by validating the serial number.
• Authenticate that the SD-WAN Administrator accepted the site for ZTD using the SD-WAN Center.
• Pull the configuration file specific for the targeted appliance from the SD-WAN Center.
• Push the configuration file specific for the targeted appliance to the branch appliance.
• Install the configuration file on the branch appliance.
• Push any missing SD-WAN software components or required updates to the branch appliance.
• Push a temporary 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.

**Zero touch deployment service 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, as well as established Virtual Paths confirming connectivity across the underlay network. The following steps are required of the SD-WAN Administrator to initiate the deployment of zero touch:
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 existing configuration and save it.

- Log in to Citrix Workspace Cloud to enable ZTD service. The Zero Touch Deployment menu option is now displayed in the SD-WAN center web management interface.

- In SD-WAN Center, navigate to Configuration > Zero Touch Deployment > Deploy New Site.

- Select an appliance, click Enable, and click Deploy.

- Installer receives activation email > Enter the serial number > Activate > Appliance is deployed successfully.

To configure Zero Touch Deployment service:

1. Install SD-WAN Center with enabled Zero Touch Deployment capabilities:
   a) Install 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 (ZTD) Cloud Service and automatically download and install any firmware updates specific to ZTD, if this call home procedure fails the following Zero Touch Deployment option will not be available in the GUI.

![Citrix SD-WAN Center](image)

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) Login into the Citrix Cloud account, and upon receiving the following message of successful login, **PLEASE DO NOT CLOSE THIS WINDOW UP, THE PROCESS REQUIRES ANOTHER ~20 SECONDS FOR THE SD-WAN CENTER GUI TO BE REFRESHED.** The window should close on its own when it is complete.

![Citrix Cloud Login](image)

2. To create a Cloud Login account follow the below procedure: Open a web browser to [https://onboarding.cloud.com](https://onboarding.cloud.com)

3. Click on 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 may notice that no sites are available for ZTD 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 (e.g. 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 should be used to add a new site targeted for zero touch deployment.

a) Design the new site for SD-WAN appliance deployment by first outlining the details of the new site (that is, Appliance Model, Interface Groups usage, Virtual IP Addresses, WAN Links with bandwidth and their respective Gateways).

**Important**

You may notice any site node that has VPX selected as the model is also listed, but currently ZTD support is only available for the AWS VPX instance.

**Note**

- Make sure that you are using a support web browser for Citrix SD-WAN Center
- Make sure the web browser is not blocking any pop-up windows during the Citrix Workspace Login

![Branch Office Topology](image)

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 automatically assign a default IP address of 192.168.100.1/16. With DHCP enabled by default, the DHCP Server in the network may provide the appliance a second IP address in a subnet that overlaps the default. This can possibly result in a routing issue on the appliance where the appliance may fail to connect to the ZTD Cloud Service. 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 may 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 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 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 build the configuration for the new site by utilizing 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 may have to be redefined since the updated appliance may have a new interface layout then 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 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.

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, will result in a change in on-site activity the Installer is responsible for.
in not required to enter serial number into the
activation URL generated with the deploy site command

2>3
If Serial Number field is left blank - The installer
will be responsible for entering in the correct serial
number of the appliance into the activation URL
generated with the deploy site command

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 ZTD Cloud Service, to share the configuration of this particular site to be temporarily
stored in the ZTD 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.

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 (e.g. https://sdwanzt.citrixnetworkapi.net).

c) If the SD-WAN Administrator did not pre-populate the serial number in the deploy site step, then the Installer would be responsible for locating the serial number on the physical appliance and entering the serial number manually into the activation URL, then click the Activate button.

d) If the Admin pre-populating the Serial Number information, the Activation URL will have already progressed to the next step.

e) The installer must physically be on-site to perform the following actions:
• Cable all WAN and LAN interfaces to match the topology and configuration built in earlier steps.
• Cable the management interface (MGMT, 0/1) in the segment of the network that 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 may have to be powered on using the power switch on the front of the appliance, others may have the power switch on the rear of the appliance. Some power switches require holding the power button until the unit powers up.

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 should 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 ability to resolve FQDNs
• IP assignment can be configured manually, as long as the other pre-requisites are meet
  a) The appliance obtains an IP address from the networks DHCP Server, in this example topology this is achieved through the bypassed data interfaces of a factory default state appliance.
  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 ZTD related software updates.
c) With successful connectivity to the ZTD Cloud Service, the deployment process automatically perform 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 may not immediately show in a connected state because the MCN may not trust the configuration handed down from the ZTD 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 utilized 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 on-site appliance utilizing 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.
The appliance license file can be updated to a permanent license using the Configuration > 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
On-prem zero touch

December 14, 2018

For instructions about how to deploy an SD-WAN appliance with Zero Touch Service, see the topic; How to Configure Zero Touch Deployment Service.

AWS

December 14, 2018

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.
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.

```
View: Global Sites
```

```
DC AWS-SE Azure-SE Branch DavidS410 ZTDBR1000 ZTDBR2000 ZTDBR2100 ZTDBR410
```

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.

![Image of Basic Settings](image1.png)

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.

![Provision and Deploy]

![Next]

e) After clicking Next, Select the appropriate Region, Instance size, populate the SSH Key name and Role ARN fields appropriately.

![Provision and Deploy AWS]

![Back Deploy]

**Note**

Make use of the help links for guidance on how to setup the SSH Key and Role ARN on the Cloud account. Also make sure the select region matches what is available on the account and that the selected Instance Size matches VPX or VPXL as the selected model in the SD-WAN configuration.

f) Click Deploy, triggering the SD-WAN Center, which was previously registered with the ZTD Cloud Service, to share the configuration of this site to be temporarily stored in the ZTD Cloud Service.

g) Navigate to the Pending Activation tab to confirm that the site information populated successfully and was put into a provisioning status.
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
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

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.
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).

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 complies with the requirements on Azure (lowercase with no special characters). Populate an email address where the activation URL can be delivered, and select Azure as the **Provision Type** for the desired Cloud, before clicking **Next**.

5. After clicking **Next**, the Provision and Deploy Azure (step 1 of 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**.

<table>
<thead>
<tr>
<th>Add API access</th>
<th>Select an API</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Select an API</td>
<td>Windows Azure Service Management API</td>
</tr>
<tr>
<td>2 Select permissions</td>
<td>Delegated Permissions</td>
</tr>
</tbody>
</table>

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).

m) Additional steps are required to assign the application a role. Navigate back to More Services, then Subscriptions.
Select the active subscription, then **Access control (AIM)**, next click **Add**.

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**.
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.
Regions allow you to define a network hierarchy with distributed management. A Region must define a Regional Control Node (RCN) which will take over functions performed by the Network Control Node (MCN) for its Region. The MCN is the controller for the Default Region.

Static and Dynamic Virtual Paths are not permitted between Regions. Traffic between Regions is managed by RCNs.

A single region deployment in an SD-WAN network can support network sites less than 550.

You can configure default region in the Configuration Editor of the SD-WAN appliance GUI. The Basic editor is useful to create only a small network with MCN and Client SD-WAN nodes. For configuring multi-region network with MCN, RCN, Clients or advanced features, you should use other configuration options in the configuration editor.

To configure single region deployment:

1. Navigate to the Global tab in the Configuration Editor. Select Regions. The default region configuration options are displayed.

   You can change the name and description for the default region by editing it.
2. Edit the Default Region to change the name and configure subnets.

3. Enable Interval VIP matching based on whether you want Forced Internal VIP Matching or Allow External VIP Matching.
   - Forced Internal VIP: When enabled, all non-private Virtual IP addresses in the Region is 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. This is the IP address and mask for the subnet.
Multi region deployment

February 25, 2019

An SD-WAN appliance configured as Master Control Node (MCN) supports multi-region deployment. The MCN manages multiple Regional Control Nodes (RCNs). Each RCN, in turn, manages multiple client sites. The MCN can also be used to manage some of the client sites directly.

With MCN as the control node of the network and RCNs as the control nodes of the regions, SD-WAN can manage more than 2,500 sites.

This enables you to fragment network into regions and set up a tiered network; such as branch (client) > RCN > MCN.

An MCN with single region can be configured with maximum of 550 sites. You can keep the existing sites in the default region and add new regions with RCNs and their sites for multi-region deployment.

The table below provides list of platforms supported for configuring primary and secondary MCN/RCN.

<table>
<thead>
<tr>
<th>Platform Edition</th>
<th>Primary/Secondary MCN</th>
<th>Primary/Secondary RCN</th>
</tr>
</thead>
<tbody>
<tr>
<td>210-SE</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>400-SE</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>410-SE</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>1000-SE, 1000-EE (Premium edition)</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
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**. This is the IP address and mask for the subnet. The newly created region is added to the existing list of regions.

   You can select the **Default** checkbox to use a desired region as the Default.

---

**Note**

You can clone MCN to a GEO or client site.

SD-WAN Center supports multi-region deployment. For more information, see SD-WAN Center Multi-Region Deployment and Reporting.

**Change management summary view**

When you perform Change Management process for appliances configured in multi-region deployment, the change management summary table is displayed in the SD-WAN appliance GUI.

The Region column displays a list of regions currently configured in the network. You can view change management summary for specific region by selecting it in the summary table.
### Default region summary:

<table>
<thead>
<tr>
<th>Region</th>
<th>Total Sites</th>
<th>Not Connected</th>
<th>Preparing/Staging</th>
<th>Staged</th>
<th>Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Region</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>AMER1</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>APAC1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EMEA1</td>
<td>Data not available</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Region Summary:

<table>
<thead>
<tr>
<th>Region</th>
<th>Total Sites</th>
<th>Not Connected</th>
<th>Preparing/Staging</th>
<th>Staged</th>
<th>Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Region</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>AMER1</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>APAC1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EMEA1</td>
<td>Data not available</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Note
In some instances, the Total Sites value displayed in the Global Multi-Region Summary table is less than the sum of the remaining columns. For example, when a branch node is not connected, it is possible that the branch is counted twice; once as “Not Connected” and once as “Preparing/Staging.”

Active bandwidth testing

December 14, 2018

Active bandwidth testing enables you the ability to issue an instant path bandwidth test through public internet WAN link, or to schedule public internet WAN link bandwidth testing to be completed at specific times on a recurring basis. This feature is useful for demonstrating how much bandwidth is available between two locations during new and existing installations, also for testing paths to determine the outcome of setting and confirmation changes, such as adjusting DSCP tag settings or bandwidth Permitted Rates.

To use the active bandwidth testing feature:

1. Navigate to System Maintenance > Diagnostics > Path Bandwidth.
2. Select the desired Path and click Test.
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.

Adaptive bandwidth detection

December 14, 2018

This feature is applicable to networks with VSAT, LOS, Microwave, 3G/4G/LTE WAN Links, for which the available bandwidth varies based on weather and atmosphere conditions, location, and line of site obstructions. It allows the 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**.
Domain name system

January 17, 2019

**Domain Name System (DNS)** translates human readable domain names to machine-readable IP addresses, and vice versa. The following DNS features are introduced in SD-WAN release 10 version 2:

- DNS Proxy
- DNS Transparent Forwarding

**DNS proxy**

DNS proxy intercepts the DNS requests destined to SD-WAN IP address and forwards it to the selective DNS services. 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. Navigate to **Global > DNS Service**. Enter the **Service Name** and a pair of **Primary and Secondary DNS server IP addresses**.

You can create internal, ISP, google or any other open source DNS service.

**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 DNS services at individual site level. The site-level DNS service configuration overrides the global configuration. To configure site-specific DNS service,
navigate to Sites > DNS > DNS Services. Enter the Service Name and a pair of Primary and Secondary DNS server IP addresses.

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 will be forwarded to, if none of the applications match in DNS forwarder look-up.

   - **Interfaces**: The interfaces on which the DNS requests will be 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 request will be forwarded to for the specified application.
DNS transparent forwarder

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 interface(s) 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 request will be 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**

<table>
<thead>
<tr>
<th>Search</th>
<th>Application Name</th>
<th>DNS Service Name</th>
<th>DNS Service Active</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS_F1</td>
<td>office1_apps</td>
<td>Google F1</td>
<td>YES</td>
<td>2</td>
</tr>
<tr>
<td>DNS_F1</td>
<td>office1_apps</td>
<td>Google F1</td>
<td>YES</td>
<td>4</td>
</tr>
<tr>
<td>DNS_F1</td>
<td>office1_apps</td>
<td>Google F1</td>
<td>YES</td>
<td>17</td>
</tr>
</tbody>
</table>

**Transparent Forwarder Statistics**

<table>
<thead>
<tr>
<th>Search</th>
<th>Application Name</th>
<th>DNS Service Name</th>
<th>DNS Service Active</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>office1_apps</td>
<td>Google F1</td>
<td>YES</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>office1_apps</td>
<td>Google F1</td>
<td>YES</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>office1_apps</td>
<td>Google F1</td>
<td>YES</td>
<td>17</td>
<td></td>
</tr>
</tbody>
</table>
DHCP server and DHCP relay

February 20, 2019

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

February 20, 2019

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 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**.

To configure a site as a DHCP relay using configuration editor:

1. Navigate to Configuration **Editor > Sites > [Site Name] > DHCP > Relays**. Click +.
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 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 will lead to duplicate IP addresses on the defined management network.

4. Click **Show Client** to view the current DHCP clients, and click **Clear Clients** to release the DHCP Client leases.

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 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.

### Management Interface DHCP Relay

<table>
<thead>
<tr>
<th>Enable DHCP Relay</th>
<th>DHCP Server IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>192.168.51.13</td>
</tr>
<tr>
<td>Change Settings</td>
<td></td>
</tr>
</tbody>
</table>

### WAN link IP address learning through DHCP client

**February 20, 2019**

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:

1. In the **Configuration Editor**, go to **Sites > [Site Name] > Interface Groups > Virtual Interfaces**.

**Note**

The physical interface in the interface group should be a non-bridged pair on a single interface.
2. 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.
Monitoring DHCP client WAN links

The runtime Virtual IP address, Subnet Mask, and Gateway settings are logged and archived in a log file called `SDWANWW_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.

GRE tunnel

December 14, 2018

The SD-WAN GRE tunnel settings enable you to configure SD-WAN Appliances to terminate GRE tunnels on the LAN. If you do not want to configure site as a GRE Tunnel termination node, you can skip this step, and proceed to the section, Configuring the WAN Links for the MCN Site.

To configure a GRE Tunnel:

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)

December 14, 2018

The SD-WAN GRE Tunnels settings enable you to configure SD-WAN Appliances to terminate GRE tunnels on the LAN. If you do not want to configure this site as a GRE Tunnel termination node, you can skip this step, and proceed to the section, Configuring the WAN Links for the MCN Site.

To configure a GRE Tunnel, do the following:

1. Continuing in the connections tab for the new MCN site, click **GRE Tunnels**. This opens the **GRE Tunnels** table for the new site.

2. Click + to the right of the **GRE Tunnels**. This adds a new blank GRE Tunnel entry to the table and opens it for editing.

3. Configure the GRE Tunnel settings.

   Enter the following:
   - **Name** – Enter a name for the new GRE tunnel, or accept the default. The default uses the following naming format:
     - **Appliance-Tunnel-<number>** - Where `<number>` is the number of GRE Tunnels configured for this site, incremented by one.
   - **Firewall Zone** - Select the file zone for the GRE tunnel to you.
   - **Source IP** – Select a source IP Address for the tunnel from the drop-down menu for this field. The menu options 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 public source IP Address for the tunnel.
- **Destination IP**: Enter the destination IP Address for the tunnel.
- **Tunnel IP / Prefix**: Enter the tunnel IP Address and prefix.
- **Checksum**: Select this to enable Checksum for the tunnel GRE header.
- **Keepalive Period**: 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 should attempt before it brings down the tunnel. The default is 3.

4. Click **Apply**. This submits your settings and adds the new GRE Tunnel to the table.

5. To configure more GRE Tunnels, click + to the right of the GRE Tunnels, and proceed as above.

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

**Configure GRE Tunnels for a Branch Site**

December 14, 2018

The Virtual WAN LAN GRE Tunnels settings enable you to configure Virtual WAN Appliances to terminate GRE tunnels on the LAN. If you do not want to configure this branch site as a LAN GRE Tunnel termination node, you can skip this step, and proceed to the section, Configuring WAN Links for the Branch Site.

To configure a LAN GRE Tunnel for the branch site:

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:

- **Name** – Enter a name for the new GRE tunnel, or accept the default. The default uses the following naming format:

  - **Appliance-Tunnel-<number>** - Where `<number>` is the number of GRE Tunnels configured for this site, incremented by one.

- **Firewall Zone** - Select a firewall zone for the GRE tunnel.

- **Source IP** – Select a Source IP Address for the tunnel from the drop-down menu for this field. The menu options 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 public source IP Address for the tunnel.

- **Destination IP** – Enter the destination IP Address for the tunnel.

- **Tunnel IP / Prefix** – Enter the tunnel IP Address and prefix.

- **Checksum** – Select this to enable Checksum for the tunnel GRE header.

- **Keepalive 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 should attempt before it brings down the tunnel. The default is 3.

1. Click **Apply**. This submits your settings and adds the new GRE Tunnel entry to the table.

2. To configure more GRE Tunnels, click + to the right of the **GRE Tunnels** label, and proceed as above.

The next step is to configure the **WAN links for the branch site**.
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
Perform the following steps to enable Internet Service for any site (Client node or MCN):

1. In the Configuration Editor, navigate to the Connections tile. Click the add (+) icon to add an Internet Service for that site. Only one Internet Service can be created per site.

2. In the Basic Settings for the Internet Service, there are several options on how you want the Internet Service to behave during unavailability of WAN links. An Internet Default Set can be defined in the Global tile with a set of Rules that can be applied to any node in the configuration which has Internet Service enabled, giving central control for Internet Service management without having to configure each node separately.

3. In the Internet Service WAN Links node, the WAN links built in the Site tile are made available to select which WAN link you would like to use for Internet traffic. In addition to other options, the Modes available are Primary, Secondary, and Balanced, allowing the admin to use the available WAN links simultaneously or in an active/passive role.
4. Site node specific Rules are available, enabling the capability of customization of each site uniquely overriding any general settings configured in the global default set. Modes include desired delivery over a specific WAN link, or as an Override Service allowing for passthrough or discard of the filtered traffic.

As an Internet Service is created for a node, the Route table for that particular node is automatically updated with a 0.0.0.0/0 route for Service Type equal Internet and a Route cost of 5, otherwise the default route with cost 16 with Passthrough as the Service Type would be enacted, and Internet traffic would be handed off to the underlay network to route.

With Internet Service being enabled for a site node, the Provisioning tile is made available to allow for the bidirectional (LAN to WAN / WAN to LAN) distribution of bandwidth for a WAN link.
among the various services utilizing the WAN link. The Services section allows for users to further fine-tune bandwidth allocation. In addition, fair share can be enabled, allowing for all services to receive their minimum reserved bandwidth before fair distribution is enacted.

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**

December 14, 2018

To secure traffic and enforce policies, enterprises often use MPLS links to backhaul branch traffic to the corporate data center. The data center applies security policies, filters traffic through security appliances to detect malware, and routes the traffic through an ISP. Such backhauling over private MPLS links is expensive. It also results in significant latency, which creates a poor user experience at the branch site. There is also a risk that users 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 utilizing 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 utilizing by all connected networks. The policies are applied consistently whether the user is at the data center or a branch site. Because secure web gateway solutions are cloud based, you don’t have to add more costly security appliances to the network.

Direct Internet Breakout at Branch with forwarding to Secure Web Gateway

Citrix SD-WAN supports the following third party secure web gateway solutions:

- Zscaler
- Forcepoint
- Palo Alto

Backhaul Internet

April 29, 2019

The Citrix SD-WAN solution can backhaul Internet traffic to the MCN site or other SD-WAN client-node sites for access to the Internet. The term “backhaul” indicates traffic destined for the Internet is sent back to another predefined site which has access to the Internet via a WAN link. This might be the case for networks that do not allow Internet access directly at a branch office because of security concerns, or due to the underlay networks topology. An example would be a remote site that lacks an external firewall where the on-board 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 most desired approach to providing Internet access to users at remote offices. This approach does however have its limitations to be aware of following and the underlay WAN links size appropriately.

- Backhaul of internet traffic adds latency to internet connectivity and is variable depending on the distance of the branch site for the data center.
- Backhaul of internet traffic consumes bandwidth on the Virtual Path and should be accounted for in sizing of WAN links.
• Backhaul of internet traffic might over-subscribe the Internet WAN link at the Data Center.

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 datasheet.

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: You only need to enable Internet Service and Export routes if all other sites are in the WAN to WAN forwarding group.

2. On the branch nodes where internet traffic will be backhauled, manually add a 0.0.0.0/0 route to default all default traffic to the Virtual Path Service with the next hop denoted as the MCN, or intermediary site.
3. Verify that the route table of the branch site does not have any other lower cost routes that would steer traffic other than the desired backhaul route through the Virtual Path.

**Link state propagation**

December 14, 2018

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.
Citrix SD-WAN 10.2

Metering and Standby WAN Links

December 14, 2018

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 may 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 frequency (weekly/monthly)
- Start date of the billing cycle
- Active heartbeat interval
  - interval at which a heartbeat message is sent by an appliance to its peer on the other end of the virtual path when there has been no traffic (user/control) on the path for at least a heartbeat interval
  - configurable values: default 50ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s
With a local metered link, the dashboard of an appliance shows a **WAN Link Metering** table at the bottom with metering information.

Bandwidth usage on a local metered link is tracked against the configured data cap. When the usage exceeds 50%, 75% or 90% of the configured data cap, the appliance generates an event to alert the user and a warning banner is displayed across the top of the dashboard of the appliance. This usage alert event can also be viewed in SD-WAN center. A metered path can be formed with 1 or 2 metered links. If a path is formed between 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 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 not greater 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.

- When configuring a standby link, you can specify standby priority and two heartbeat intervals:
  - Standby priority indicates the order in which a standby link becomes active, if there are multiple standby links:
    - a priority 1 standby link becomes active first whereas a priority 3 standby link becomes active last
    - Multiple standby links can be assigned the same priority
  - Active heartbeat interval - the heartbeat interval used when the standby path is active (default 50ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s)
  - Standby heartbeat interval - the heartbeat interval used when the standby path is inactive (default 1s/2s/3s/4s/5s/6s/7s/8s/9s/10s/disabled)

A standby path is formed with 1 or 2 standby links.

- An on-demand standby path is formed between:
  - a non-standby link and an on-demand standby link
- 2 on-demand standby links
  • A last-resort standby path is formed between:
    - a non-standby link and a last-resort standby link
    - an on-demand standby link and a last-resort standby link
    - 2 last-resort standby links

The heartbeat intervals used on a standby path are determined as follows:

- If standby heartbeat is disabled on at least 1 of the 2 links, heartbeat is disabled on the standby path while inactive.
- If standby heartbeat is not disabled on either link, then the larger of the two values 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 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 taking into consideration the standby path’s MTU. (The Virtual Path’s MTU is the smallest path MTU among all active paths within the Virtual Path).

Events and log messages are generated when a standby path transitions between standby and active.

Configuration pre-requisites:

- A meter link may be of any access type.
- All links at a site can be configured with metering enabled.
- A standby link may be of Public Internet or Private Intranet access type. A WAN link of Private MPLS access type cannot be configured as a standby link.
- At least one non-standby link must be configured per site. A maximum of 3 standby links per site is supported.
- Internet/Intranet services may not be configured on on-demand standby links. On-demand standby links support Virtual Path service only.
- Internet service may be configured on a last-resort standby link, but only load balance mode is supported.
- Intranet service may be configured on a last-resort standby link, but only secondary mode is supported and primary reclaim must be enabled.

To configure metered links:

1. In the SD-WAN web management interface, navigate to Configuration Editor > Sites > WAN Links
> Settings. Click Metered/Standby Link to expand it.

2. Check the **Enable Metering** checkbox. You can provide values for data cap, billing frequency, billing cycle start date, and the active heartbeat interval.

To configure standby links:

1. In the SD-WAN web management interface, navigate to **Configuration Editor > Sites > WAN**
**Links > Settings.** Click **Metered/Standby Link** to expand it.

2. By default, standby mode of a WAN link is disabled. To configure the WAN link as standby, click the pencil icon next to **Settings** to enter edit mode and select one of the standby modes.

3. Once a standby mode is selected, select the standby priority, active heartbeat interval, and standby heartbeat interval as appropriate. Click **apply** to validate the configuration.

4. If an on-demand standby link is configured, the global default on-demand bandwidth limit (120%) is applied to the Virtual Path. This specifies the maximum WAN-to-LAN bandwidth allowed for the Virtual Path. It is expressed as a percentage of the total bandwidth provided by all non-standby links in the Virtual Path. As long as the available bandwidth in the Virtual Path is below the limit and if there is sufficient usage, the appliance attempts to activate on-demand paths to supplement bandwidth.

5. To view or change the global default on-demand bandwidth limit, open the sections **Global** >
6. If you want to apply an on-demand bandwidth limit specific to a Virtual Path and keep the global default setting unchanged, a Virtual Path Default Set needs to be created and the on-demand bandwidth limit in the Advanced Settings can be changed.

7. To apply settings for a specific Virtual Path, the user should navigate to the section **Connections > Site > Virtual Paths > Basic Settings** and select the default set for the particular Virtual Path.
How To Monitor Metered and Standby WAN Links

1. When path statistics (Monitoring > Statistics > Paths) are displayed, metered links and standby links are marked as shown below.

2. If the appliance has a Virtual Path that has a local or remote on-demand standby link, when
WAN link usage statistics are viewed, an extra table showing on-demand bandwidth is displayed at the bottom of the page (Monitoring > Statistics > WAN Link Usage).

3. When the usage on a metered link exceeds 50% of the configured data cap, a warning banner is displayed across the top of the dashboard. In addition, if the usage exceeds 75% of the configured data cap, the numerical metering information toward the bottom of the dashboard 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.

2. The configured active and standby heartbeat intervals for each path can be viewed at Configuration > Virtual WAN > View Configuration > Paths.
Office 365 optimization

February 22, 2019

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 additional 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 very 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 significantly 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. A Citrix service agent on the appliance polls the Citrix service, every day to obtain the latest set of end-point signatures. The SD-WAN appliance polls the Citrix service, 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](#).
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. Ensure that the Management interface has internet connectivity.
   
   You can use the Citrix SD-WAN web interface to configure the management interface settings.

2. 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 will be 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
You can also view Office 365 application statistics in SD-WAN Center Application report.
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, 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.

### PPPoE Sessions

**June 6, 2019**

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 in release 10.2:

- 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.

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.
For virtual interface:

- Configure Name, Firewall Zone, VLAN 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.

   ![WAN Link Configuration](image)

   ![WAN Link Configuration](image)

   **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 show 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.

<table>
<thead>
<tr>
<th>PPPoE session type</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured</td>
<td>Yellow</td>
<td>A VNI is configured with PPPoE. This is an initial state.</td>
</tr>
<tr>
<td>Dialing</td>
<td>Yellow</td>
<td>After a VNI is configured, the PPPoE session state moves to dialing state by starting the PPPoE discovery. Packet information is captured.</td>
</tr>
<tr>
<td>Session</td>
<td>Yellow</td>
<td>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.</td>
</tr>
<tr>
<td>PPPoE session type</td>
<td>Color</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Ready</td>
<td>green</td>
<td>IP packets are received and VNI and associated WAN link is ready for use.</td>
</tr>
<tr>
<td>Failed</td>
<td>red</td>
<td>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.</td>
</tr>
<tr>
<td>Stopped</td>
<td>yellow</td>
<td>PPP/PPPoE session is manually stopped.</td>
</tr>
<tr>
<td>Terminating</td>
<td>yellow</td>
<td>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).</td>
</tr>
<tr>
<td>Disabled</td>
<td>yellow</td>
<td>The SD-WAN service is disabled.</td>
</tr>
</tbody>
</table>

**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.

Quality of service

April 29, 2019

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.

For more information on QoS rule guidelines and default rules breakdown, see the support article Citrix SD-WAN QOS and Application Rules.

Customizing Classes

December 14, 2018
The Citrix SD-WAN configuration provides a default set of application-classification, rule-filtering, and class-assignment settings that can be applied to any virtual path service in the SD-WAN environment. You can also customize these settings.

Using classes, you can classify a specific type of traffic on the virtual path, and then you can apply rules to handle this traffic. Traffic is assigned to a specific class, as defined in the rule.

For more information about creating rules, see Rules by IP Address and Port Number.

The SD-WAN system provides 17 classes (0-16). Classes 0-3 are predefined for Citrix HDX QoS prioritization. To use this feature, enable the following options:

- **WAN Optimization**, available under Optimization > Features.
- **HDX QoS Priorities**, available under Optimization > Features.
- **ICA Service Class**, available under Optimization > Service Classes.

These classes are used to classify HDX traffic with different ICA priority tags. You can edit the class types and their assigned bandwidth sharing to obtain the optimal quality of service, but you cannot edit the names of the classes.

Classes 10-16 are predefined and are associated with Realtime, Interactive, and Bulk class types. Each type can be configured further to optimize quality of service for its type of traffic. Classes 4-9 can be used to specify user defined classes. Classes are of one of the following three types:

- **Realtime**: Used for low latency, low bandwidth, time-sensitive traffic. Real-time applications are time sensitive but don’t really need high bandwidth (for example voice over IP). Real-time applications are very sensitive to latency and jitter, but can tolerate some loss.
- **Interactive**: Used for interactive traffic with low to medium latency requirements and low to medium bandwidth requirements. Interactive applications involve human input in the form of mouse clicks or cursor moves. The interaction is typically between a client and a server. The communication might not need high bandwidth but is sensitive to loss and latency. However, server to client does need high bandwidth to transfer graphical information, which might not be sensitive to loss.
- **Bulk**: Used for high bandwidth traffic that can tolerate high latency. Applications that handle file transfer and need high bandwidth are categorized as bulk class. These applications involve very little human interference and are mostly handled by the systems themselves.

**To customize classes**:

1. In the SD-WAN Configuration Editor, navigate to Global > Virtual Path Default Sets.
2. Click **Add Default Set**, enter a name for the default set and click **Add**. In the **Section** field select **Classes**.
3. In the **Name** field, either leave the default name or enter a name of your choice.

4. In the **Type** field, select the class type (Realtime, Interactive, or Bulk).

5. For realtime classes, you can specify the following attributes:

   - **Initial Period**: The time period in milliseconds to apply an initial rate before switching to a sustained rate.
   - **Initial Rate**: Maximum rate at which packets leave the queue during the initial period.
   - **Sustained Rate**: Maximum rate at which the packets leave the queue after the initial period.

   When in contention, the scheduler ensures that the realtime class receives the **Initial Rate** and the **Sustained Rate** that you specify, plus a small percentage of the available bandwidth that is shared with interactive and bulk classes.

6. For interactive classes, you can specify the following attributes:

   - **Initial Period**: The time period, in milliseconds, during which to apply initial percentage of the available bandwidth before switching to the sustained percentage. Typically, 20 ms.
   - **Initial Share %**: The maximum share of virtual-path bandwidth during the initial period.
   - **Sustained Share %**: The maximum share of virtual-path bandwidth after the initial period.

   Interactive classes use the remaining bandwidth after the real-time traffic has been serviced.
7. For bulk classes, you can specify only the **Sustained Share**%, which determines the remaining virtual path bandwidth to be used for a bulk class.

   Bulk traffic is serviced after real-time and interactive traffic are serviced. Typically, a bulk class gets a lower sustained share % than an interactive class.

8. Click **Apply**.

**Note**

Save the configuration, export it to the change management inbox, and initiate the change management process.

**Rules by IP address and port number**

May 3, 2019

Using the configuration editor, you can create rules for traffic flows 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.

For most purposes, the starting point for defining QoS policies is application rules. For more information, see **Rules by application name**.

To create IP rules:

1. In the SD-WAN Configuration Editor, navigate to **Global > Virtual Path Default Sets**.

2. Click **Add Default Set**, enter a name for the default set, and click **Add**. In the Section field, select **Rules** 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 below. After the filtering, the rule settings are applied to the services matching these criteria.
• **Source IP Address**: Source IP address and the subnet mask to match against the traffic.

• **Destination IP Address**: Destination IP address and the subnet mask to match against the traffic.

  **Note**

  Select **Dest = Src**, if the source and destination IP address are the same.

• **Protocol**: Protocol to match against the traffic.

• **Source Port**: Source port number or port range to match against the traffic.

• **Destination Port**: Destination port number or port range to match against the traffic.

• **DSCP**: The DSCP tag in the IP header to match against the traffic.

• **VLAN**: The VLAN ID to match against the traffic.

7. Click the add (+) 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 could override to an intranet, internet, or pass-through service.

  • **Retransmit Lost Packets**: Send traffic that matches this rule to the remote appliance over a reliable service and retransmit lost packets.

  • **Enable TCP Termination**: Enable TCP termination of traffic for this flow. The round-trip time for acknowledgement of packets is reduced, and therefore improves throughput.

  • **Preferred WAN Link**: The WAN link that the flows should use first.
Citrix SD-WAN 10.2

- **Persistent Impedance**: The minimum time in milliseconds for which the traffic would remain in the same path, until 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 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.

For more information on QoS rule guidelines and default rules breakdown, see the support article **Citrix SD-WAN QOS and Application Rules**.

**Rules by application name**

May 3, 2019

The application classification feature allows the Citrix SD-WAN appliance to parse incoming traffic and classify it 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 then apply application QoS rules to them. Rules are filters that define applications and assign them to a traffic class. The application rules are similar to Internet Protocol (IP) rules, but take precedence. For information on IP rules see, Rules **by IP Address and Port Number**.

Citrix SD-WAN includes preset application QoS rules and also allows custom rules to be created. Seven criteria are available to filter application traffic:

- Source IP
- Destination IP
- Source port
- Destination port
- Protocol
- DSCP tag
- VLAN ID

For every application rule, you can specify the mode of transmission for traffic matching that rule. 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 traffic classes. For information on classes, see [Customizing Classes](#).

By default, the following five pre-defined application rules are available for Citrix HDX applications (virtualized apps and desktops):

<table>
<thead>
<tr>
<th>Rule</th>
<th>Class</th>
<th>Transmit Mode</th>
<th>Retransmit Lost Packets</th>
<th>Enable Packet Resequencing</th>
<th>Discard Late Resequencing Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDX_Priority_0</td>
<td>HDX_priority_tag_0</td>
<td>Load Balance</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>HDX_Priority_1</td>
<td>HDX_priority_tag_1</td>
<td>Load Balance</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>HDX_Priority_2</td>
<td>HDX_priority_tag_2</td>
<td>Load Balance</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>HDX_Priority_3</td>
<td>HDX_priority_tag_3</td>
<td>Load Balance</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>HDX</td>
<td>interactive_high</td>
<td>Load Balance</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

The preferred way of delivering virtualized applications and desktop is over Multi-Stream ICA (MSI). This enables each stream of HDX traffic to be assigned the appropriate traffic class type (Realtime, Interactive or Bulk). When Single-Stream ICA (SSI) is used, all HDX traffic is assigned to the same traffic class (by default, Interactive).

**How application rules are applied?**

In the SD-WAN network, when incoming packets reach the SD-WAN appliance, they are inspected for application classification. While some applications can be identified immediately, several packets may need to be inspected before SD-WAN can identify the application. During the inspection and classification process, the IP rule attributes such as Class and TCP termination are applied to the packets. After application classification, the application rule attributes such as Class and transmit mode take effect and override the IP rule attributes.
The IP rules have more attributes than the application rules. The application rule overrides the corresponding IP rule attributes. After the application rule attributes have been processed, the additional attributes in the applicable IP rule are processed.

For example, consider 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 initial packets and classifying the traffic 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 family that is used as a match criteria for this filter.

   For more information on application, application family and application object, see [Application classification](#).

5. In the **Rule Group Name** field, select a rule group. The statistics for rules with the same rule group will be grouped together and can be viewed together.

   For viewing rule groups, navigate to **Monitoring > Statistics**, and in the **Show** field select **Rule Groups**.

   You can also add custom rule groups. For more information, see [Add custom applications and](#)

© 1999-2019 Citrix Systems, Inc. All rights reserved. 350
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**.

For more information on QoS rule guidelines and default rules breakdown, see the support article [Citrix SD-WAN QOS and Application Rules](#).

## Add Rule Groups and Enable MOS

December 14, 2018

A particular application in the network can be defined by the group of rules that is applied to it. The SD-WAN configuration editor provides a default list of rule groups. You can also create custom rule groups and tag individual IP rules or application QoS rules to applications.

For more information about rules, see [Rules by IP Address and Port Number](#) and [Rules by Application Name](#).

The statistics for rules with the same rule group will be grouped together and can be viewed together.

For viewing statistics based on rule groups, navigate to **Monitoring > Statistics**, and in the **Show field** select **Rule Groups**.

The mean opinion score (MOS) is a numerical measure of the quality of the experience that an application delivers to end users. It is primarily used for VoIP applications. In SD-WAN, MOS is also used to assess the quality of non-VoIP applications by judging the traffic as if it were a VoIP call.

The average MoS Score is calculated with a sampling interval of 1 minute. MoS score calculated by other third party tools may vary, depending on the sampling interval used.

SD-WAN Center displays the MOS for existing traffic that passes through the virtual path. For more information about viewing MOS in SD-WAN Center, see [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**

May 3, 2019

Citrix SD-WAN appliances identify and classify applications using three techniques:
• Deep Packet Inspection (DPI)
• Citrix-proprietary ICA protocol
• Application vendor APIs (e.g. Microsoft REST APIs for Office 365)

The Deep Packet Inspection (DPI) library recognizes thousands of commercial applications. This 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.

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. HDX priority tag based QoS is supported in SD-WAN Premium Edition.

Classification of network traffic is done during initial connections or flow establishment; therefore, pre-existing connections will not be classified as ICA. Classification of connections will also be lost when the connection table is cleared manually.

Framehawk traffic and Audio-over-UDP/RTP are not classified as HDX applications. They are reported 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 need to have:

• SD-WAN release 10 version 1 or above.
• Appropriate versions of Citrix Virtual Apps & Desktops (formerly XenApp and XenDesktop) and the Citrix Workspace app (or its predecessor, Citrix Receiver). See the currently supported release versions at HDX Insights.

Once classified, ICA application can be used in application rules and to view application statistics sim-
iliar to other classified applications.

There are five default application rules for ICA applications one each for the following priority tags:

- ICA
- ICA Priority 0 (ICA Real-Time)
- ICA Priority 1 (ICA Interactive)
- ICA Priority 2 (ICA Bulk-Transfer)
- ICA Priority 3 (ICA Background)

For more information, see Rules by Application Name

As priority tag based HDX classification is not available in SD-WAN Standard Edition appliances the four App rules. ICA priority 0–3 are not in effect.

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. Additionally, to match traffic on those ports to valid IP rules, you must update ICA IP rules.

In ICA IP and port list you can specify non-standard ports used in XA/XD policy to process for HDX classification. IP address is used to further restrict the ports to specific destination. Use ‘*’ for port destined to any IP address. IP address with combination of SSL port is also used to indicate that the traffic is likely ICA even though traffic is not finally classified as ICA. This indication is used to send L4 AppFlow records to support multi-hop reports in Citrix Application Delivery Management.

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 may be used for several service types (for example - email, news, and so on). If different services utilize different certificates, the DPI engine would be able to differentiate between services.
- For applications that utilize their own encryption protocol, the DPI engine looks for binary patterns in the flows, for instance in case of Skype the DPI engine looks for a binary pattern inside the certificate and determines the application.

To configure application classification settings:

1. In the Configuration Editor, click Global > Applications > Settings.
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 may still be classified and QoE calculated but statistics on SD-WAN center will not be available. You can, view, and monitor ICA application statistics on the SD-WAN Center. This option is enabled by default. For more information, see *HDX Reports*.

4. Select **Enable Multi-stream ICA** to allow multiple ICA streams in a session. This option is disabled by default and should only be enabled to provide QoS per stream type.

5. In **DPI ICA Port**, specify non-standard ports used in XA/XD policy to process for HDX classifi-
cation. 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.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use ‘*’ for port destined to any IP address.</td>
</tr>
</tbody>
</table>

7. Click Apply

You can configure application classification settings at each site individually. Click Connections, select a site and click Applications Settings. You can also choose to use the global application settings.

**Search applications**

You can search for an application to determine the application family name. A brief description of the application is also provided.

To search for an application:

1. In the Configuration Editor, click Global > Applications > Search.
2. In the Search field type, the name of the application and hit enter.

A brief description of the Application and the Application Family name appears.
Note
For information on applications that the SD-WAN appliance can identify using Deep Packet Inspection, see Application Signature Library.

Application Objects

Application objects enable you to group different types of match criteria into a single object that can be used in firewall policies and application steering. IP Protocol, Application, and Application Family are the available match types.

To create an application object:

1. In the Configuration Editor, click Global > Applications > Application Objects.

2. Click Add and, in the Name field, enter a name for the object.

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 definition with the highest priority is applied.

5. Click + in the Application Match Criteria section.

6. Select one of the following match types:
   - IP Protocol: Specify the protocol, network IP address, port number, and, DSCP tag.
   - Application: Specify the application name, network IP address, port number, and, DSCP tag.
   - Application Family: Select an application family and specify the network IP address, port number, and, DSCP tag.

7. Click + to add more application match criteria.

8. Click Add.
Using Application Classification with a Firewall

The classification of traffic as applications and application families enables you to use the application, application families, and application objects as match types to filter traffic and apply firewall policy and rules. This applies for all Pre, Post, and local policies. For more information about firewall, see Stateful Firewall and NAT Support.

QoS fairness (RED)

December 14, 2018

The QoS fairness feature improves the fairness of multiple virtual path flows by using QoS classes and Random Early Detection (RED). A virtual path can be assigned to one of 16 different classes. A class can be one of three basic types:

- Realtime classes serve traffic flows that demand prompt service up to a certain bandwidth limit. Low latency is preferred over aggregate throughput.
- Interactive classes have lower priority than realtime but have absolute priority over bulk traffic.
• Bulk classes get what is left over from realtime and interactive classes, because latency is less important for bulk traffic.

Users specify different bandwidth requirements for different classes, which 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.
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 MPLS queues associated with the WAN Link. This allows a single VIP with multiple DSCP tags that correspond to the provider’s queuing implementation for the MPLS WAN Link. This maps the Intranet Service to multiple MPLS Queues on a single MPLS WAN Link.

Allows MPLS providers to identify traffic based on DSCP markings so that class of service can be applied by the provider.

Note

If you have existing MPLS configurations and would like to implement the Private MPLS Access Type, please contact Citrix Support for assistance.
**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 level, SD-WAN creates paths automatically between the MCN and Client MPLS Queues based on matching DSCP tags. If the Autopath Group is assigned from the MPLS Queue level, SD-WAN creates paths automatically regardless of whether or not the DSCP tags match.

5. Ensure that the same Autopath Group is configured at the MCN and Client.
6. Verify that the Paths for the WAN Link are built automatically.
7. Assign Intranet Service to a specific queue, if needed.

   **Note**
   
   The SD-WAN configuration may not have a one-to-one mapping for provider-based queues. This is based on specific deployment scenarios. You cannot create Autopath Groups between different Private Access Types. For instance, you cannot create Autopath Groups between a Private Internet Access Type and a Private MPLS Access Type.

**How to Add Private MPLS WAN LINK**

To configure new WAN Link Access Type for Private MPLS:

1. In the Configuration Editor, navigate to Sites > [Site Name] > WAN Links. Click Add Link. Enter WAN Link name and select Private MPLS as the Access Type.
2. Under the **Basic Settings**, there is now a new **MPLS Queues** tab. Click + Add to add specific MPLS Queues. These should correspond with the queues defined by the Service Provider.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Queue Name</td>
<td>The MPLS queue name</td>
</tr>
<tr>
<td>DSCP Tag</td>
<td>Service Provider’s DSCP tag setting for the queue.</td>
</tr>
<tr>
<td>Unmatched</td>
<td>When enabled, any frames arriving that do not match defined tags within the configuration file are mapped to this queue and the bandwidth defined for this queue.</td>
</tr>
<tr>
<td>LAN to WAN Permitted Rate (kbps)</td>
<td>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.</td>
</tr>
</tbody>
</table>
## Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN to WAN Permitted Rate (kbps)</td>
<td>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.</td>
</tr>
</tbody>
</table>

Expand the MPLS Queue definition (by clicking the +), and more options appear. These options include:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking IP Address</td>
<td>WAN Link tracking address</td>
</tr>
<tr>
<td>Congestion Threshold</td>
<td>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.</td>
</tr>
<tr>
<td>Eligibility</td>
<td>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.</td>
</tr>
</tbody>
</table>

Configure the MPLS Queues that correspond to the existing Service Provider WAN Link queue definitions.

**Note**

Any existing MPLS WAN Links that are configured prior to SD-WAN 9.1 are not impacted.

## Define WAN Link properties for private MPLS

Once the Private MPLS WAN Link with its MPLS Queues is defined, you should assign an Autopath Group for the WAN Link under a specific Virtual Path definition.

To assign autopath group:

1. Go to Connections > [Site Name] > WAN Links > [MPLS WAN Link Name] > Virtual Paths > [Virtual Path Name] > [Local Site] > WAN Links and click Edit ().
2. Click the Autopath Group drop-down menu and choose from the available groups. By default, MPLS Queues inherit the Autopath Group assigned to the MPLS WAN Link. You may choose to set the individual MPLS Queues to Inherit the chosen Autopath Group or choose an alternate from the Autopath Group drop-down menu for each MPLS Queue.

Note
If there is no one-to-one mapping, based on DSCP tag, between queues at the local site and the remote site, you must map MPLS Queues to specific Autopath Groups. Inheriting an Autopath Group from the MPLS WAN Link 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 may be in a congested state. In the previous releases, this information was only available in SD-WAN log files and through the CLI. These options are now available in the web interface to 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 menu.

**Monitor MPLS queues**

Go to **Monitor > Statistics**, and select **MPLS Queues** from the **Show** drop-down menu.
**Application QoE**

February 27, 2019

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.

<table>
<thead>
<tr>
<th>Quality</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>8–10</td>
</tr>
<tr>
<td>Fair</td>
<td>4–8</td>
</tr>
<tr>
<td>Poor</td>
<td>0–4</td>
</tr>
</tbody>
</table>

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 than 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 the 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 the 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**

December 18, 2018

Network parameters such as latency, jitter, and packet drop affect the user experience of HDX users. Quality of Experience (QoE) is introduced to help the users understand and check their ICA quality of experience. QoE is a calculated index, which indicates the ICA traffic performance. The users can tune the rules and policy to improve the QoE.

The QoE is a numeric value between 0–100, the higher the value the better the user experience. QoE is enabled by default for all ICA / HDX applications.

The parameters used to calculate QoE is measured between the two SD-WAN appliances at the client side and server side and not, end to end, between the server and the client. Latency, jitter, and packet
drop are measured at the flow level and it could be different from the statistics at the link level. The end host (client or server) application may never know that there is a packet loss on the WAN. If the retransmit succeeds, the flow level packet loss rate is lower than the link level loss. However, as a result, it may increase latency and jitter a bit.

Default configuration for HDX traffic enables SD-WAN to 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:

<table>
<thead>
<tr>
<th>Quality</th>
<th>QoE Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>80–100</td>
</tr>
<tr>
<td>Fair</td>
<td>50–80</td>
</tr>
<tr>
<td>Poor</td>
<td>0–50</td>
</tr>
</tbody>
</table>

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 may show up in ICA_Summary for that minute.
- On session reconnect, since initial protocol information is not exchanged, SD-WAN is not able to identify MSI, hence each connection is counted as SSI information.
- For UDP connections, after the connection is closed, it could take up to 5 minutes for the connection to show as closed and updated in ICA_Summary. For TCP connections, after the connection is closed, it could take up to 2 minutes to show as closed in ICA_Summary.
- QoE of TCP sessions and UDP sessions may not be the same on the same path due to the inherent different between TCP and UDP.
- If one user launches two virtual desktops, the number of users is countered as two.

Multiple Net Flow Collectors

December 14, 2018

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 Enterprise Edition appliances, Virtual Path data is streamed to the designated Netflow collectors. One limitation with this is that one cannot differentiate which physical WAN link is being used by SD-WAN, as the solution reports aggregated Virtual Path information (A Virtual Path may comprise of multiple distinct WAN Paths), there is no way to filter the Netflow records for the distinct WAN paths.

- TCP control Bits report as N/A which indicates SD-WAN does not follow the internet standard for Netflow exports based on RFC 7011 which has element ID 6 for tcpControlBits (IANA). Without TCP Flags, calculating route trip time (RTT), latency, jitter, and other performance metrics in the flow data 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.

Routing

November 22, 2018
Virtual Routing and Forwarding (VRF):
VRF is an IP technology that allows multiple instances of a routing table to exist in a router and work simultaneously. This increases functionality by allowing network paths to be segmented without using multiple devices.

Dynamic Routing:
Citrix SD-WAN introduces support for Dynamic Routing protocols. This feature facilitates discovery of LAN subnets, advertise virtual path routes to work more seamlessly within networks using the BGP and OSPF protocols, allowing SD-WAN to be seamlessly deployed in an existing environment without the need for static route configurations and graceful router failover.

Route Filtering:
For networks with Route Learning enabled, Citrix SD-WAN provides more control over which SD-WAN routes are advertised to routing neighbors rather than advertising all or no routes. Export Filters are used to include or exclude routes for advertisement using OSPF and BGP protocols based on specific match criteria. Route filtering is implemented on LAN routes in an SD-WAN network (Data Center/Branch) and is advertised to a non-SD-WAN network through eBGP.

Route Summarization:
Route summarization reduces the number of routes that a router must maintain. A summary route is a single route that is used to represent multiple routes. It saves bandwidth by sending a single route advertisement, reducing the number of links between routers. It saves memory because only one route address is maintained. The CPU resources are used more efficiently by avoiding recursive lookups.

VRRP:
Virtual Router Redundancy Protocol (VRRP) is a widely used protocol that provides device redundancy to eliminate the single point of failure inherent in the static default-routed environment. VRRP allows you to configure two or more routers to form a group. This group appears as a single default gateway with one virtual IP address and one virtual MAC address.

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 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 routing daemon and view the list of commands.

```bash
dynamic_routing?
```
Citrix SD-WAN 10.2

SD-WAN Overlay Routing

December 14, 2018

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. The article below 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. Below 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 what is reachable down the virtual paths. These routes are normally automatic, however a virtual path route can be added manually at a site. Any traffic for this route is forwarded to the defined Virtual Path for this destination route (subnet).

- **Intranet** – Denotes routes that are reachable through a private WAN link (MPLS, P2P, VPN etc.). For example, a remote branch that is on the MPLS network but does not have an SD-WAN appliance. It is assumed that these routes need to be forwarded to a certain WAN router. Intranet Service is not enabled by default. Any traffic matching this route (subnet) is classified as intranet for this appliance for delivery to a site that does not have an SD-WAN solution.

  **Note**
  
  Notice that when adding an Intranet route there is no next hop, but rather a forward to an 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 be limited as much as possible.

  **Note**

  Passthrough can be useful when conducting a POCs to avoid having to configure numerous routing, however be very careful in production because SD-WAN does not account for WAN link utilization for traffic sent to passthrough. It is also helpful when troubleshooting issues and you want to take a certain IP flow out of delivery over the Virtual Path.

- **Discard** - This is not a service but a last resort route that drops the packets if it matches. Normally this does not occur expect when the SD-WAN appliance is deployed out of path. You must have an Intranet service or local route as a catch all route, otherwise the traffic 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 will prevent 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 above routes, but also include a service type, next hop, or gateway depending on the service type, in addition to route cost. A default route cost will automatically be added to each route type (reference the table below for default route costs). Additionally, only trusted routes are advertised to other SD-WAN appliances. Untrusted routes are only used by the local appliance.

Client node routes are only advertised to the MCN node and no other client nodes by default. For client node routes to be visible to another client nodes WAN to WAN Forwarding should 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.
Each route for remote branch office subnets is advertised as a Service through the Virtual Path connecting through the MCN, with the Site column populated with the client node where the destination resides as a local subnet.

In the below example, with “**WAN-to-WAN Forwarding (Routes Export)**” enabled, Branch A has a route...
table entry for the Branch B subnet (10.2.2.0/24) through the MCN as a next hop.

SD-WAN Overlay Route Tables

How Citrix SD-WAN Traffic Matches on Defined Routes

The match process for defined routes on Citrix SD-WAN is based on longest prefix match for destination subnet (similar to a router operation). The more specific the route, the higher the change on it being matched. 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 below:

- 192.168.1.0/24 Cost 5
- 192.168.1.64/26 Cost 10

A packet destined for 192.168.1.65 host would use the latter route even though the cost is higher. Based on this, it is common for configuration to be in place for only the routes intended to be delivered over the Virtual Path overlay with other traffic falling into catch all routes such as a default route to the passthrough service.
Routes can be configured in a site node route table that have the same prefix. The tie break then goes to the route cost, the service type (Virtual Path, Intranet, Internet, etc.), and the next hop IP.

**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 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). Additionally, SD-WAN can be deployed in “learn only” mode where SD-WAN can receive routes but not advertise routes back to the underlay. This is useful when introducing the SD-WAN solution into a network where the routing infrastructure is complex or uncertain.

**Important**

It is very easy to leak unwanted route, if you are not careful.

The SD-WAN Virtual Path route table works as an External Gateway Protocol (EGP), very similar to BGP (think site-to-site). For example, when SD-WAN advertises routes from the SD-WAN appliance to OSPF they are typically considered external to site and protocol.

**Note**

Be aware of environments that have 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 interop with that protocol.

One challenge in introducing Routing Protocols to an SD-WAN deployment is that the route table is not available until the SD-WAN service is enabled and operation in the network, therefore it is not recommended to enable advertise routes from the SD-WAN appliance initially. Use the import and export filters for a gradual introduction of routing protocols on SD-WAN.

Let us take a closer look by reviewing the following example:

In this example, we examine a routing protocol use case. The above 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 need to consider how to best integrate with existing route protocols to that site to ensure full connectivity between underlay and SD-WAN overlay networks.

In the example network, eBGP is used between all four locations across the MPLS network. Each location has its own Autonomous System Number (ASN).

In the New York Data Center, OSPF is running to advertise the core Data Center subnets to the remote sites and also announce a default route from the New York Firewall (E). In this example, all internet traffic is backhauled to the datacenter, even though London and San Francisco Branches have a path to the internet.

The San Francisco site also should be noted 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>* 172.10.0.0/24 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>* 172.20.0.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
O>* 172.30.0.0/24 [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>* 172.20.0.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
B>* 172.30.0.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0

Note

In this example, you can ignore the 192.168.65.0/24 subnet. This is a management network and not pertinent to the example. All the Routers are connected to the management subnet but the
Citrix SD-WAN 10.2

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 SD-WAN routing table is considered external to the OSPF protocol and so OSPF will prefer a route learned internal (intra-area), therefore routes advertised by SD-WAN may not take precedence.

When OSPF is used across the WAN (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 need to enable eBGP since it will be directly connected to the MPLS network and operating as the customer edge route for the site. BGP can be enabled under Connections > View Site > BGP > Basic Settings.

Note the Autonomous System number of 13.

The eBGP peers with each other location. Each ASN is different.

It is important to understand how routes are passed between the Virtual Path routing table and the dynamic route protocols in use. It is easy to create routing loops or advertise routes in an adverse way. The filter mechanism gives us the ability to control what gets into and out of the routing table. We consider each location in turn.

- The San Francisco location has two local subnets **10.80.1.0/24** and **10.81.1.0/24**. We want to advertise them through eBGP so that sites like Dallas can still reach the San Francisco site over the underlay network and also sites like London and San Francisco can still reach San Francisco.
over the Virtual Path overlay network. We also want to learn from eBGP reachability to all sites in case the SD-WAN Virtual Path overlay goes down and the environment needs to fall back to using just the MPLS. We also do not want to readvertise anything SD-WAN learns from eBGP to the SD-WAN routers. To accomplish this, the filters need to 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:**
Further, the Citrix SD-WAN route table can be viewed on the **Monitoring > Statistics > Show Routes** page.

**San Francisco Citrix SD-WAN:**

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 New York Data Center. This route is being learned in two ways:

- As a Virtual Path route (Num 3), service = NYC-SFO with a cost of 5 and type static. This is a local subnet advertised by SD-WAN appliance in New York. It is static in that it is either directly connected to the appliance or it is a manual static route entered in the configuration. It is reachable
because the Virtual Path between the sites is in a working/up state.

- As an advertised route through BGP (Num 6), with a cost of 6. This is now considered a fallback route.

Since the prefix is equal and cost is different, SD-WAN 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 (Num 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 may 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.
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:

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 it is not advertised across the Virtual Path overlay. All other routes are then included.

For the export filters, we can exclude route for 192.168.10.0/24. This is because, as a directly connected subnet in San Francisco site, we cannot filter this route out at the source, so it is suppressed at this end.

Now let us review the refreshed route table starting at the core route in New York site.

**New York Router B:**

```
vyos@VYOS-ROUTER-B-CORE~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - ISIS, B - BGP, * - selected route, + - FIB route
O:* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 4d22h22m
O:* 10.80.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h49m
O:* 10.81.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h49m
O:* 10.90.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h50m
O:* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 4d22h22m
C:* 127.0.0.0/8 is directly connected, lo
O 172.10.10.24 [110/10] is directly connected, eth1, 4d22h22m
C* 172.10.10.24 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:**
We can see the correct routes for both the local subnets learned via OSPF, a route to Dallas site learned from the MPLS Router A and the remote subnets for San Francisco and London sites. Let us look at the MPLS Router A. This router is participating in OSPF and BGP.

From the route table, this Router A is learning the remote subnets through BGP and OSPF with the Administrative distance and cost of the BGP route (20/5) being lower than OSPF (110/10) and hence preferred. In this example, network where there is only one core route, this may not cause concern. However, traffic arriving here would be delivered via the MPLS network rather than being sent to the SD-WAN Appliance (172.10.10.10). If we want to maintain complete routing symmetry, we would need a route map to adjust the AD/Metric cost so that there is route preference from the route coming from 172.10.10.10 rather than the route learned via eBGP.
Alternatively, a “backdoor” route can be configured to force the router to prefer the OSPF route over the BGP route. Notice the static route for the SD-WAN Virtual IP address to the London site SD-WAN appliance. 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 two sites. The advantage of a dynamic virtual path is that traffic can flow directly from one client node to second without having to traverse the MCN or two virtual paths, which could add latency to the traffic flow. Dynamic virtual paths are built and removed dynamically based on user-defined traffic thresholds. These thresholds are defined as either packets per second (pps) or bandwidth (kbps). This functionality enables a dynamic full mesh SD-WAN overlay topology.

Once the thresholds for dynamic virtual paths are met, the client nodes dynamically create their virtualized path to one another 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 of time, the dynamic virtual path is torn down

Dynamic Virtual Paths have the concept of an Intermediate site. The intermediate site could be an MCN site or any other site in the network that has Static Virtual Path configured and connected to two or more other client nodes. Another design consideration requirement is to have WAN-to-WAN Forwarding enabled, allowing all routes from all sites to be advertised to the client nodes where the dynamic virtual path is desired. “Enable Site as Intermediate Node” must be enabled in addition to WAN-to-WAN Forwarding in order for this intermediate site to monitor client node communication and to dictate when the dynamic path needs to be established and torn down.
Multiple WAN-to-WAN Forwarding Groups can 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**

Below is an example SD-WAN site route table:
Notice from the above 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 above table, we can see 14 defined routes. A description of the routes or groups of routes is described below:

- **Route 0** – On the MCN this is a Host subnet route that resides at the DC site. 172.16.10.0/24 resides in the DC LAN and 192.168.15.1 is the gateway on the LAN that will get to that subnet.

- **Route 1** – This is a local route to this SD-WAN device that displaying the route table.

- **Route 2–4** – These are the subnets that are part of the virtual interfaces configured for the DC site SD-WAN. These subnets are derived from the trusted virtual interfaces defined.

- **Route 5** – This is a shared route to another client node that is shared by the MCN with a Reachability status of No due to the down Virtual Path between that site and the MCN.

- **Route 6–9** – These routes exist at another client site. For this route, a Virtual Path route is created for matching WAN ingress traffic destined for the remote site on the Virtual Path.

- **Route 10** – With the Internet Service defined, the system adds a catch all route for direct internet breakout for this local site.

- **Route 11** – Passthrough is default route the system always adds to allow packets to flow through in case there is no match on any existing routes. The Passthrough is not groomed, typically local broadcasts and ARP traffic are mapped to this service.

- **Route 12** – Discard is default route the system always adds to drop anything undefined.

**Default Route Cost Values:**
• WAN to WAN Forwarding – 10
• Default Direct Route Cost – 5
• Auto Generated Routes – 5
• Virtual Path – 5
• Local – 5
• Intranet – 5
• Internet – 5
• Passthrough – 5
• Optional – route is 0.0.0.0/0 defined as a service level

After defining these routes, it is important to understand how the traffic flows using the defined routes. These traffic flows 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 > Routes 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 should be tested/verified, also test with Virtual Path down/disabled to verify desired behavior

• Route tables are static unless route learning feature is enabled

Below is the maximum supported limit for multiple routing parameters:

• Maximum Routing Domains: 255

• Maximum Access Interfaces per WAN Link: 64

• Maximum BGP neighbors per site: 255

• Maximum OSPF area per site: 255

• Maximum Virtual Interfaces per OSPF area: 255

• Maximum Route Learning import filters per site: 512

• Maximum Route Learning export filters per site: 512

• Maximum BGP routing policies: 255

• Maximum BGP community string objects: 255

Virtual Routing and Forwarding

November 22, 2018

Citrix SD-WAN allows segmenting networks for more security and manageability by using VRF. For example, you can separate guest network traffic from employee traffic, create distinct routing domains to segment large corporate networks, and segment traffic to support multiple customer networks. Each routing domain has its own routing table and enables the support for overlapping IP subnets.

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 VRF functionality:
By default, routing domains are enabled on an MCN.
Routing domains are enabled on the Branch sites.
Each enabled routing domain should have a virtual interface and virtual IP associated with it.
Routing selection is part of all the following configurations:
- Interface group
- Virtual IP
- GRE
- WAN Link -> Access Interface
- IPsec tunnels
- Routes
- Rules
Routing domains are exposed in the web interface configuration only when multiple domains are created.
For a Public Internet link, only one primary and secondary access interfaces can be created.
For a Private Intranet/MPLS link, one primary and secondary access interface can be created per routing domain.

Configure Routing Domain

January 4, 2019
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 checkbox. Click Apply to save the changes. If you plan to implement a single Routing Domain, no explicit configuration is required.

All new configurations are automatically populated with a default Routing Domain.

1. Navigate to Sites → [Client Site Name] > Routing Domains. Click the Enable checkbox to enable a configured Routing Domain for the Site.

2. Click the Default checkbox to make that Routing Domain the default for the Site. Click Apply to save the changes.

Note

Unchecking Enable for a Routing Domain will make it unavailable for use at the Site.

Select Routing Domain for Intranet Service

December 14, 2018

To select routing domain for intranet service:
1. In the Configuration Editor, navigate to Connections > [Site Name] > Intranet Services > [Intranet Service Name] > Basic Settings click the Edit () icon.

2. Choose a Routing Domain from the drop-down menu.

Configure Routes

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

November 22, 2018

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.

```
1 dynamic_routing?
```
Dynamic Routing

December 18, 2018

The following sections describe the routing functionality supported in the Citrix SD-WAN network.

**OSPF Overview**

OSPF is a routing protocol developed for Internet Protocol (IP) networks by the Interior Gateway Protocol (IGP) group of the Internet Engineering Task Force (IETF). It includes the early version of OSI’s Intermediate System to Intermediate System (IS-IS) routing protocol.

OSPF protocol is open, which means that its specification is in the public domain (RFC 1247). OSPF is based on the Shortest Path First (SPF) algorithm called Dijkstra. It is a link-state routing protocol that calls for sending Link-State Advertisements (LSAs) to all other routers within the same hierarchical area. Information on attached interfaces, metrics used, and other variables are included in OSPF LSAs. OSPF routers accumulate link-state information, which is used by the SPF algorithm to calculate the shortest path to each node.

You can now configure 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).

**How To Configure OSPF**

To configure OSPF:

1. In the Configuration Editor, navigate to Connections > View Region > View Site > [Site Name] > OSPF > Section > Basic Settings.

2. Click the Enable checkbox, enter an optional Router ID. If the Router ID is not specified, it is auto-selected as the lowest Virtual IP hosted in the SD-WAN network.

3. Click the Advertise Citrix SD-WAN Routes checkbox if you wish to advertise Citrix SD-WAN Routes, and click Apply to enable OSPF. The routes advertise or redistribute the SD-WAN virtual path routes to peer routes with whom adjacency or peering is established so that the peer...
routes are aware of being able to reach this network prefixes through the SD-WAN network.

4. Expand **OSPF -> Area**, and click **Edit**.
5. Enter an area ID to learn routes from and advertise to.

6. For sites with multiple Routing Domains, from the Virtual Interfaces panel, choose a Routing Domain from the drop-down menu as illustrated in the figure. The Routing Domain determines which Virtual Interfaces are available. If there is only one Routing Domain configured, the Routing Domain column does not appear. If Identity is not checked for a specific Virtual IP Address, the associated Virtual Interface is not available for IP services. For more information, see the Virtual IP Address Identity section.

7. Choose one of the available Virtual Interfaces from the Name drop-down menu. The Virtual Interface determines the Source IP Address.

8. Enter the Interface Cost (10 is the default).

9. Choose an Authentication Type from the drop-down menu.

10. If you chose Password or MD5 in step 8, enter the Password associated text field.

11. In the Hello Interval field, enter the amount of time to wait between sending Hello protocol packets to directly connected neighbors (10 seconds is the default).

12. In the Dead Interval field, enter the amount of time to wait to receive a Hello protocol packet before marking a router as dead (40 seconds is the default).

13. Click Apply to save your changes.

**Stub Area**

Stub areas are shielded from external routes and receive information about networks that belong to other areas of the same OSPF domain.

Enable the Stub Area check box.
BGP Overview

BGP is an inter-autonomous system routing protocol. An autonomous network or group of networks is managed under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between Internet Service Providers (ISPs). Customer networks deploy an Interior Gateway Protocol (IGP) such as RIP or OSPF for the exchange of routing information within their networks. Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between Autonomous Systems (AS), the protocol is called External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is called Interior BGP (IBGP).

BGP is a robust and scalable routing protocol deployed on the Internet. To achieve scalability, BGP uses many route parameters called attributes to define routing policies and maintain a stable routing environment. BGP neighbors exchange full routing information when the TCP connection between neighbors is first established. When changes to the routing table are detected, the BGP routers send to their neighbors only those routes that have changed. BGP routers do not send periodic routing updates, and advertise only the optimal path to a destination network. You can configure Citrix SD-WAN appliances to learn routes and advertise routes using BGP.

How To Configure BGP

To configure BGP:

1. In the Configuration Editor, navigate to Connections > View Region > View Site > [Site Name] > BGP > Basic Settings.
2. Click the Enable checkbox and the Advertise Citrix SD-WAN Routes checkbox if you want to advertise Citrix SD-WAN Routes. Enter an optional Router ID, and enter the number of the Local Autonomous System to learn routes from and advertise routes to in the Local Autonomous System field. The routes advertise or redistribute the SD-WAN virtual path routes to peer routes.
with whom adjacency or peering is established so that the peer routes are aware of being able to reach this network prefixes through the SD-WAN network.

3. Click **Apply** to enable BGP.

4. Expand **Basic Settings > Neighbors** and click the **Add (+)** icon.

   **Note**

   If there is only one Routing Domain configured, the Routing Domain column will not appear. If Identity is not checked for a specific Virtual IP Address (see the Virtual IP Address Identity section for more details), the associated Virtual Interface is not available for IP services.
For Sites with multiple Routing Domains choose a routing domain. Routing Domain determines which Virtual Interfaces are available.

1. Choose a **Virtual Interface** from the drop-down menu. The Virtual Interface determines the Source IP Address.

2. Enter the **IP Address** of the IBGP Neighbor router in the Neighbor IP field, and **Local Autonomous System** number in the Neighbor AS field.

3. In the **Hold Time (s)** field, enter the Hold Time, in seconds, to wait before declaring a neighbor down (the default is 180).

4. 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).

5. Click the **IGP Metric** checkbox to enable the comparison of internal distances to calculate the best route.

6. Click the **Multi Hop** checkbox to enable multiple hops for the route.
7. 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 Citrix SD-WAN network.

### How To 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.
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 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, refer to the following use cases:

- SD-WAN site Communicating with non SD-WAN site over eBGP
- Communication Between SD-WAN sites Using Virtual Path and eBGP
- Implementing OSPF in one-arm topology
- OSPF Type5 to Type1 deployment in MPLS Network
- SD-WAN and non SD-WAN (third-party) appliance OSPF deployment
- Implementing OSPF using SD-WAN network with high-availability setup

**OSPF**

December 14, 2018

**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 learnt are dynamically captured and displayed.

This eliminates the need for SD-WAN administrators to statically define the LAN-side networking environment for each appliance that is part of the SD-WAN network.

**WAN Side: Dynamic Route Sharing**

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 SD-WAN appliance in one-arm mode described below.

**Implementing OSPF in One-Arm Topology**

In one-arm configuration, the router needs complicated PBR or WCCP configuration in OSPF deployments. By changing the default export route type from Type 5 to Type 1 we can simplify this deployment. If SD-WAN routes are advertised as intra-area routes with less cost, and the SD-WAN appliance becomes active, the neighbor router selects SD-WAN routes and automatically begins forwarding traffic through SD-WAN network. Additional PBR or WCCP configuration is not required any longer.

**Prerequisites:**

- SD-WAN Appliances at the DC and Branch sites should be running latest release version.
- End-to-End IP connectivity should be configured and working fine.
- OSPF is enabled on all the sites.

To configure OSPF Type 1:

1. Configure **Virtual Interfaces** and **WAN links** on both the DC and Branch sites so that you can create Virtual Path between them.
2. Under **Connections > [MCN] > Route Learning > OSPF->Basic Settings**, select **Export OSPF Route Type** to be **Type 1 Intra Area**.
3. Save the configuration, stage and activate the configuration.

You should be able to see following route types under **Export OSPF Route Type**

- Type 5 AS External
- Type 1 Intra Area

You should be able to configure **Type 5 AS External** route.
After activation of the changed configuration, you should see the Route Type changes under Configuration > Virtual WAN > View Configuration > Dynamic Routing.

As shown in the illustration above, DC MCN is deployed in one-arm topology. When DC site is up, one-arm router forwards all traffic from local LAN to other sites, such as the Branch's local LAN whose destination IP address is within same subnet to the SD-WAN first, then SD-WAN appliance wraps all packets and sends it to the router with all the packets destination IP address in the Branch Virtual IP address. The router then forwards those packets to WAN.

When the DC site is down, router forwards all traffic from local LAN to other sites (branch site's local LAN, destination IP is within subnet) to WAN directly, and not to the SD-WAN appliance.

**OSPF Type5 to Type1 Deployment in MPLS Network**

The following deployment mode is provided to avoid loop formation in an MPLS network configured using SD-WAN appliances. The illustration below describes the standard MPLS network implementation.
In the above illustration:

- OSPF is configured between **ME-BR1_Router** and **ME-DC_Router** in area 0.
- OSPF is configured between **ME-DC_Router** and **DC** in area 0.

**Recommended Configuration:**

- DC VW and ME-DC_Router on area0
- ME-BR1_Router and ME-DC_Router on area0
- BR1 VW and ME-BR1_Router on area0

On the ME-DC_Router:

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 router to the MCN and this creates a loop continuously.

The static routes which are not PBR routes but the destination Host IP based routes will traverse towards the right link to be chosen from the DC side based on the path chosen and the encapsulation performed thereafter. Therefore, with these static routes configured, the encapsulated packets with any destination Virtual IP of BR1 SD-WAN appliance would use these links as per the best path selected by the DC MCN.
Add ACL to avoid loop formation when IPHOST routes are installed (if no static Virtual IPs configured):

- If the IPHOST routes advertised by BR1 SD-WAN appliance are installed by the MCN router *
  ME-DC_Router * and not added as static routes as mentioned above, there is a possibility of loop formation if the OSPF participating interface (172.58.6.x) between ME-BR1_Router and ME-DC_Router goes down. This is because with this interface down, the IPHOST routes are flushed from ME-DC_Router's routing table.

- If this happens, MCN will forward the encapsulated packet destined to one the BR1 VIPs to ME-DC_Router and back from router to the MCN and loop continuously.

On the ME-BR1_Router:

Advertise 172.58.3.x network to ME-DC_Router with a higher cost than the cost advertised for the same network by DC, if the same AREA-ID is used between ME-BR1_Router <-> ME-DC_Router and ME-DC_Router <-> DC (SD-WAN).

- Based on the cost metric computation of OSPF 10^8/BW and the cost for route prefixes are based on the interface type. SD-WAN appliances advertise the virtual path and virtual WAN specific static routes to the external or peer routers with default SD-WAN cost of 5.

- 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 interal ospf Type 1 route, then according to cost computation, by default the ME-BR1_Router's route will be configured, as the cost is lesser than SD-WAN’s default cost of 5. To avoid this and make SD-WAN appliance chosen as preferred route initially, the interface cost of (172.58.3.1) needs to be manipulated to make it higher on the ME-BR1_Router so that DC SD-WAN route is configured in the routing table of the ME-DC_Router.

This also ensures that when the DC SD-WAN appliance fails, the alternate route to use ME-BR1_Router as the next preferred gateway will ensure uninterrupted traffic flow.

Use ME-DC_Router as a source for advertising 172.58.8.0/24 network to both DC SD-WAN and the ME-BR1_Router:

With this route, the DC SD-WAN can send packets to the upstream router being aware of the LAN subnet after decapsulation. If DC SD-WAN goes down, the legacy routing infrastructure would help ME-BR1_Router use the ME-DC_Router as the next hop to reach the 172.58.8.x network.

To configure OSPF exported routes as Type1 under Basic OSPF Settings:

1. Configure Virtual Interfaces and WAN links on both DC and Branch sites to create Virtual Path between them.

2. Under Connections->[MCN]->Route Learning->OSPF->Basic Settings, select Export OSPF Route Type to be Type 1 Intra Area.

3. Save the configuration, stage and activate the same. You should be able to see 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 should be advertised as Type5 External AS by the SD-WAN appliance. Routes learnt through SD-WAN should be displayed in the neighboring routers as Type5 AS External routes.

To configure OSPF exported route weight under Basic OSPF Settings:

1. Configure Virtual Interfaces and WAN links on both DC and Branch sites to create Virtual Path between them.
2. Under Connections > [MCN] > Route Learning > OSPF > Basic Settings, configure Export OSPF Route Weight.
3. Save the configuration, stage and activate the same.
4. Now, configure Export OSPF Route Weight to any numeric value between 1 to 65529.
5. After activation of the changed config, you can see the Route Weight under Configuration > Virtual WAN > View Configuration > Dynamic Routing. The default route weight exported should be 0. Actual cost of the route should only be the cost of SD-WAN.

To configure OSPF exported routes as Type1 under Export Filter settings:

1. Configure Virtual Interfaces and WAN links on both DC and Branch so that we can create Virtual Path between them.
2. Under Connections > [MCN] > Route Learning > OSPF > Export Filters configure an export filter.
3. Expand the filter. Configure Export OSPF Route Type to Type 1 Intra Area route.
4. Save the configuration, stage and activate the same. You should be able to see following two route types under Export OSPF Route Type
   • Type 5 AS External
   • Type 1 Intra Area

After activation of the changed config, user should be able to see the Route Type changes under Configuration > Virtual WAN > View Configuration. Route type should be displayed as Type 5 AS External.

To configure OSPF exported route weight under Export Filter settings:

1. Configure Virtual Interfaces and WAN links on both DC and Branch so that we can create Virtual Path between them.
2. Under Connections > [MCN] > Route Learning > OSPF > Export Filters configure an export filter.
3. Expand the filter. Configure Export OSPF Route Weight to any numeric value between 1 to 65529.
4. Save the configuration, stage and activate the same.
After activation of the changed config, user should be able to see the Route Type changes under Configuration > Virtual WAN > View Configuration. Route Weight configured under Export Filter should override the Weight configured under Basic OSPF Settings.

SD-WAN and Third-Party (non SD-WAN) Appliance Deployment

As shown in the illustration below, third-party appliance site can get to Site B’s LAN by sending traffic to Site B directly. If it cannot send traffic directly, fallback route goes to Site A, then using virtual path between DC to Branch sites to get to the Branch. If that fails, it will use MPLS2 to get to Branch site.

Configuration Steps:

1. Configure Virtual Interfaces and WAN links on both DC and Branch so that a Virtual Path is created between the sites. 1. Configure Export Route Type as Type1 and assign cost as 195 on the SD-WAN appliance. 1. Save, stage and activate the configuration. 1. Send traffic between the end hosts on DC and Branch sites. 1. Shutdown the link between R1 and R2. 1. Send traffic between the end hosts on DC and Branch sites. 1. Unshut the link between R1 and R2. 1. Send traffic between the end hosts on DC and Branch sites. 1. Disable Virtual WAN Service on the DC site so that Virtual Paths go down. 1. Send the traffic between the end hosts on DC and Branch sites.

Verifying Configuration:

1. Initially, at step 4, all the traffic passes through SD-WAN appliance. 1. At step 6, when the link between R1 and R2 is broken, traffic is routed towards SD-WAN through R3. 1. At step 8, traffic flows through SD-WAN appliance with R2 as the next hop for the LAN Router R1. 1. At step 10, Virtual WAN paths go down between DC and BR1 appliance and traffic should flow normally as before the SD-WAN network was configured.
Traffic flow can be observed in the SD-WAN GUI under **Monitoring > Flows**.

### Implementing OSPF with SD-WAN Network in High Availability Setup

OSPF Type5 to Type1 with high-availability sites during failover to standby appliance and deployed in high-availability setup:

To configure OSPF in HA deployment:

1. Configure **Virtual Interfaces** and **WAN links** on both DC and Branch to create Virtual Path between them.
2. Setup High-Availability.
3. Export **Route Type** configured as **Type 1** and **Route Weight** as **50**.
4. Save the configuration, stage and activate the same.
5. Start traffic flow.
6. Observe that under **Monitor > Statistics > Routes**, the hit count increases for OSPF routes with least costs.
7. Bring the Active MCN down and observe the behavior.
8. Bring the original Active MCN back Up.
9. The **Dashboard > High Availability Status** shows correctly for HA Local Appliance and Peer Appliance for Active and Standby.
10. Under **Configuration > View Configuration > Dynamic Routing**, OSPF is enabled and **export_ospf_route_type** shows **Type1** and **export_ospf_route_weight** as **50**.
11. Even after failover the High Availability Status shows correct OSPF configuration for Local and Peer Appliance.
12. View **Monitor > Statistics > Routes**. The hit count increases for OSPF routes with least costs.
13. After failback, the High Availability Status shows correct OSPF configuration for Local and Peer Appliance.
14. Verify that the hit count increases for OSPF routes with low cost under view **Monitor > Statistics > Routes**.
BGP

December 14, 2018

The SD-WAN BGP routing functionality enables you to:

- Configure the autonomous system (AS) number of a neighbour or other peer router (iBGP or eBGP).
- Create BGP policies to be applied selectively to a set of networks on a per-neighbour basis, in either direction (import or export). An SD-WAN appliance supports eight policies per site, with up to eight network objects (or eight networks) associated with a policy.
- For each policy, users can configure multiple community strings, AS-PATH-PREPEND, MED attribute. Users can configure up to 10 attributes for each policy.

Note

Only local preference and IGP metric for path selection and manipulation is allowed.

Configuring Policies

In the SD-WAN web management interface, the configuration editor has a new section, BGP policy, under Route Learning > BGP. In this section, users can add BGP attributes that constitute a policy. Adding community strings, prepending AS path prepend, and configuring MED are supported.

You can manually configure each community string or select no advertise or no export community string from a drop-down menu. For manual configuration, you can enter an AS number and community. You can select Insert/Remove to tag the routes or remove the community from the routes.

You can configure the number of times you want to prepend the local AS to the AS Path before advertising outside the local network. You can configure MED for matching routes.

To configure BGP policy:

1. In the NetScaler SD-WAN web management interface, go to Configuration > Virtual WAN > Configuration Editor. Open an existing configuration package. Go to Sites > DC or Branch settings.
2. Expand BGP and click **Enable** under **Basic Settings**. Enter **Router ID** and **Local Autonomous System** value and click **Apply**.
3. Click + sign next to the **Community String Lists**. Configure each community string manually or by selecting no advertise or no export community string from the drop-down menu. For manual configuration, you can enter an AS number and community. You can select **Insert/Remove** tag the routes with the community string or remove the community string from the routes received from the peers.

4. Configure BGP policy by expanding **BGP Policies**. Add BGP attributes to the **New Route Policy**.

5. Click the + sign next to **Attributes** to edit BGP attributes. The **Edit Attributes** window is displayed. Select the desired BGP attribute from the drop-down menu. Enter the desired value for
MED, AS Prepend Length, or Community String as per your selection. Click Apply.

Note
Any policy can have only one occurrence of an attribute and cannot take multiple occurrence of the same attribute. You cannot have 2 MED or 2 AS Path Prepend. It can have either MED/AS-PATH Prepend/Community String or a combination.

Configuring Neighbors

To configure eBGP, an additional column to the existing BGP neighbors section is added to configure neighbor AS number. The existing configurations are pre-populated to this field with the local AS number when you import previous configuration using the SD-WAN 9.2 configuration editor.

The neighbor configuration also has an optional advanced section (expandable row) where you can add Policies for each neighbor.

Configuring Advanced Neighbors

With this option, you can add network objects and add a configured BGP policy for that network object. This is similar to creating a route map and ACL to match certain routes and configuring BGP attributes for that neighbor. You can specify the direction to indicate if this policy is applied for incoming or outgoing routes.

The default policy is to <accept> all routes. Note that accept and reject policies are defaults and cannot be modified.
You have the ability to match routes based on Network address (destination address), AS Path, Community string and assign a policy and select direction for the policy to be applied.

To configure neighbors:

1. Configure neighbors by clicking Add as shown below.

2. Click the + sign. Select a Virtual Interface. Enter the Neighbor IP address.

3. Add policies. Select Network Address, BGP Community, and AS Path details as desired. Click Apply.
4. Go to Monitoring > Routing Protocols > Dynamic Routing Protocols to monitor the configured BGP policies and neighbors for the DC or Branch site appliance.

You can enable debug logging and to view log files for routing from the Monitor > Routing Protocol page. The logs for the routing daemon are split into separate log files. The standard routing information is stored in `dynamic_routing.log` while dynamic routing issues are captured in `dynamic_routing_diagnostics.log` which can be viewed from monitoring of routing protocols.

**BGP Soft Reconfiguration**

Routing policies for BGP peer include configurations such as route-map, distribute-list, prefix-list, and filter-list that might impact inbound or outbound routing table updates. When there is a change in the routing policy, the BGP session should be cleared, or reset, for the new policy to take effect.

Clearing a BGP session using a hard reset invalidates the cache and results in negative impact on the operation of networks as the information in the cache becomes unavailable.

The BGP Soft Reset Enhancement feature provides automatic support for dynamic soft reset of inbound BGP routing table updates that are not dependent upon stored routing table update information.
iBGP

November 22, 2018

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

November 22, 2018

SD-WAN site communicating with non SD-WAN site over eBGP:

When a site without SD-WAN appliance is communicating with another site with SD-WAN appliance (Site-A) over a single WAN path (only internet is available), and if the site with SD-WAN appliance (Site-A) loses internet connectivity, then the site without SD-WAN can communicate with Site-A through another SD-WAN appliance site (Site-B). Site-B funnels traffic from the site without SD-WAN appliance to the Site-A.

Communication between SD-WAN sites using Virtual Path and eBGP:

Provides underlay route learning to communicate with remote site local subnets when the virtual path is down between two sites while the Virtual WAN appliance is still up and running.

Application Route

December 14, 2018
In a typical enterprise network, the branch offices access applications on the on premise data center, the cloud data center, or the SaaS applications. The application routing feature, allows you to steer the applications through your network easily and cost-efficiently. For example, when a user on the branch site is trying to access a SaaS application the traffic can be routed such that the branch offices can access the SaaS applications on the internet directly, without having to go through the data center first.

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 the Application Objects section in the 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 the **IPsec Tunnel** field, select one of the configured IPsec tunnels. Select **Eligibility Based on Tunnel** to enable the route to not receive any traffic when the tunnel is not reachable.

  **Note**
  Once you have selected a service for a custom application, do not change it.

• **Eligibility Based on Path:** Select to enable the route not to receive traffic when the specified path is down. In the **Path** field, specify the path to be used for determining route eligibility.

3. Click **Apply**.

To view the application routes configured on your SD-WAN appliance. In the SD-WAN GUI, navigate to **Configuration > Virtual WAN > View configuration**. Select **Application Routes** from the **View** drop-down menu.
To view statistics data for the application routes:

1. In the SD-WAN GUI, navigate to **Monitoring > Statistics**.

2. From the **Show** drop-down list, select **Application Routes**.

You can view the following statistics:

- **Application Object**: Name of the application object.
- **Gateway IP Address**: The gateway IP address used by application objects with GRE Tunnel service type.
- **Service**: The service type mapped to the application object.
- **Firewall Zone**: The firewall zone that this route falls in.
- **Reachable**: The status of the application route.
- **Site**: Name of the site.
- **Type**: Indicates if the route is static or dynamic.
- **Cost**: The priority of the route.
- **Hit Count**: The number of times the application route is used to steer the traffic.
- **Eligible**: Is the application route eligible to send the traffic.
- **Eligibility Type**: The type of route eligibility condition applied to this route. The eligibility type can be Path, Gateway, or Tunnel.
- **Eligibility Value**: The value specified for the route eligibility condition.
Note

In the current release, applications that belong to application family, match type defined in application object, cannot be steered.

Route Filtering

December 14, 2018

How to Configure Route Import and Export Filters

1. In the Configuration Editor, navigate to Connections > View Regions > View Site > [Site Name] > Route Learning Properties.

2. Expand Import Filters and Export Filters to view the existing route filters. Import Filters are separate and distinct from Export Filters. You can configure up to 32 Export Filters.

Note

If there is only one Routing Domain configured, the Routing Domain column does not appear.
3. Navigate to **Import Filters** or **Export Filters** under the **BGP** or **OSPF** section.

Use the following criteria to construct each Export Filter that you want to create.

<table>
<thead>
<tr>
<th>Field Criteria</th>
<th>Description</th>
<th>Value(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>The Order in which filters are prioritized. The first filter that a route matches are applied to that route</td>
<td>100, 200, 300, 400, 500, 600</td>
</tr>
<tr>
<td>Field Criteria</td>
<td>Description</td>
<td>Value(s)</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Routing Domain</td>
<td>To match routes from a specific routing domain, choose one of the configured Routing Domains from the drop-down menu</td>
<td>Any, Def_RD default</td>
</tr>
<tr>
<td>Network Address</td>
<td>Enter the IP Address and Netmask of configured Network Object that describes the route's network</td>
<td>- IP address</td>
</tr>
<tr>
<td>Prefix</td>
<td>To match routes by prefix, choose a match predicate from the drop-down menu and enter a Route prefix in the adjacent field</td>
<td>- eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to</td>
</tr>
<tr>
<td>Citrix SD-WAN Cost</td>
<td>The method (predicate) and the SD-WAN Route Cost that are used to narrow the selection of routes exported</td>
<td>Numeric value</td>
</tr>
<tr>
<td>Service Type</td>
<td>Select the Service types that are assigned to matching routes from a list of the existing, supported Citrix SD-WAN Services</td>
<td>Any, Local, Virtual Path, Internet, Intranet, LAN GRE Tunnel, LAN IPsec Tunnel</td>
</tr>
<tr>
<td>Site/Service Name</td>
<td>For Intranet, LAN GRE Tunnel, and LAN IPsec Tunnel, specify the name of the configured Service Type to use</td>
<td>Text string</td>
</tr>
<tr>
<td>Gateway IP Address</td>
<td>If you choose LAN GRE Tunnel as the Service Type, enter the Gateway IP for the tunnel</td>
<td>IP address</td>
</tr>
<tr>
<td>Include</td>
<td>Click the checkbox to Include routes that match this filter. Otherwise matching routes are ignored</td>
<td>None</td>
</tr>
</tbody>
</table>
Route Summarization

December 14, 2018

With the increase in the size of the enterprise networks, the routers need to maintain large number of routes in their routing table. The routers require increased CPU, memory and bandwidth resources to look up the large routing tables, and maintain individual routes. You can configure a summary route with Local and Discard service types. This summary route is advertised to the next-hop devices.

To configure a summary route for a local subnet:

1. In the Configuration Editor, navigate to **Connections > Routes** and click the + to add a route.

2. On the **Add route** page, set the following parameters 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 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
Multicast groups can be configured to support low bandwidth multicast traffic in simplified networks. You can define multicast groups such that the network administrator can control the source and destination of multicast traffic. You can configure different multicast group IP Address and set the source and destination virtual interfaces to appropriately pass-through multicast traffic.

Two primary use cases supported in SD-WAN are:

1. Support for existing multicast networks in the underlay.
2. Support for manually defined static multicast trees that allow forwarding multicast traffic through the overlay.

**How to configure Multicast Groups in SD-WAN GUI**

1. In the SD-WAN GUI, go to **Configuration > Virtual WAN > Configuration Editor**. Open an existing configuration package.

2. Go to **Connections > View Region > View Site > <Site> > Multicast Groups**.

4. Edit Service for the Multicast traffic.
   
   - Basic settings: define the basic parameters of the multicast group. The only parameter available is the Multicast group IP address. This address may be a single IP address or an address and mask. All addresses or networks must be contained within the Class D address range (224.0.0.0/4).
   
   - Multicast Group IP: Configure a valid class D Multicast IP Address or Subnet.
Routing Domain: For multiple routing domains, configure valid routing domain which is receiving Multicast traffic.

Direction, Send: defines where multicast traffic is accepted from. This section includes the following components:

Service Type: Local, Internet, Intranet, GRE Tunnel, Virtual Path. The Service Type on which Multicast traffic is received.

Service Instance: The Service Name on which Multicast traffic is received.

Direction Receive: defines the services on which traffic is replicated on. This section includes the following components:

Service Type: Local, Internet, Intranet, GRE Tunnel, Virtual Path. The Service Type on which Multicast traffic is sent.

Service Instance: The Service Name on which Multicast traffic is sent.

Note

1. Due to issues with session tracking, particularly as it involves forwarding a single packet on multiple interfaces, NAT lookups are modified to ignore multicast packets. Therefore, Static 1:1 NAT translation for multicast traffic is not supported in Release 9.3.1.

2. IGMP snooping is not supported in Release 9.3.1.

3. Multicast packets routed through the IP forwarder have TTL performed. Since IGMP messages are sent with a TTL of 1, you need to avoid decrementing the TTL for replicated messages.

Monitoring Multicast Traffic

In the SD-WAN GUI, go to Monitoring > Statistics. Select Multicast Group from the drop-down list. This displays the statistics page for existing Multicast groups configured for a specific site in the SD-WAN GUI.
Configure IGMP Proxy

The ability to configure multicast groups to support low bandwidth multicast traffic in simplified networks is supported.

With static multicast group, network administrators can control the source and destination of the multicast traffic. Instead of statically configuring the multicast group, users can configure IGMP proxy for updating the upstream core networks with all the sources in the downstream networks of the edge.

1. In the SD-WAN GUI, go to Connections > View Region > View Site > Site.
2. Select Multicast Groups > Basic Settings. Click Enable IGMP Proxy.
3. Go to Services. Select Virtual Path as the Service Type to configure multicast group traffic.

In the SD-WAN GUI, under the **Virtual WAN > View Configuration** tab, you can view the configured Multicast groups. You can also monitor Multicast Group traffic from the Monitoring tab.

**Configure Virtual Path Route Cost**

December 14, 2018

Citrix SD-WAN supports the following routing enhancements related to data center administration.

For example, consider SD-WAN network with two data centers; one in North America and one in Europe. You want all sites in North America to route traffic through the datacenter in North America and all sites in Europe to use Europe Datacenter. Previously, in SD-WAN 9.3 and earlier release versions, this functionality of datacenter administration was not supported. This is implemented with the introduction of Virtual Path Route cost.

- **Virtual Path Route cost**: You can configure Virtual Path route cost for individual virtual paths that 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 import filters. OSPF Route cost is considered in route selection instead of SD-WAN cost. Cost up to 65534 instead of 15 is supported, but it is advisable to accommodate for appropriate virtual path route cost that is added if route is learned from a remote site.

- **BGP - VP cost to MED**: You can now copy Virtual Path route cost for SD-WAN routes into BGP MED values when exporting (redistributing) SD-WAN routes to BGP peers. This can be set for individual neighbors by creating a BGP policy and applying it in the “OUT” direction for each neighbor.

- 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 could be an MCN and DC2 could be a Geo-MCN, and could 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 should be added to any route shared with neighbor sites to indicate routing preference, including routes learned via Dynamic Routing.

- No Static Virtual Path should have a lower cost than a Dynamic Virtual Path.

**Note**

VP Route cost deprecates the WAN to WAN forwarding cost that existed in release versions earlier than 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 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 datacenters DC1 and DC2 that use both these subnets to transmit traffic to SD-WAN. With default virtual path route cost, you cannot influence routing since it depends on which route got installed first; it could be either the DC2 first or the DC1 next.

With virtual path, you can influence specifically DC2 virtual path to have a higher virtual path route cost (for example, 10) while DC1 has default VP route cost of 5. This manipulation 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.

Viewing Routing Table Summary for Virtual Path Route Cost:

The routing table displays how same subnets advertised by two sites connected to a branch site over virtual path are installed with precedence of cost with Virtual Path route cost addition.

This figure below shows the route table with two different costs for the same route which is 172.16.6.0/24 with cost 10 and 11 for services DC-Branch01 and GEOMCN-Branch01 respectively.
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.
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 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 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 backup router takes-over within milliseconds, ensuring that there is no downtime.

To configuring VRRP instance:
1. In the Configuration Editor, navigate to Sites > Site name > VRRP and click +.

2. Configure a VRRP instance. Enter the values for the following fields:

   - **VRRP group ID**: The VRRP group ID. The group ID should be a value range is 1 - 255. The same group ID should be configured on the back-up routers too.
   
   **Note**
   
   Currently you can configure up to four groups only.
   
   - **Version**: The VRRP protocol version. You can choose between VRRP protocol V2 and V3.
   - **Priority**: The priority of the 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 Interval**: The frequency in milliseconds, with which the VRRP advertisements are sent when the SD-WAN appliance is the master. The default advertisement interval is one second.
   - **Authentication Type**: You can choose Plain Text to enter an authentication string. The authentication string is sent as a plain text without any encryption in the VRRP Advertisements. Choose None, if you do not want to set up authentication.
   - **Authentication Text**: The authentication string to be sent in the VRRP Advertisement. This option is enabled if the Authentication Type is Plain Text.
   
   **Note**
   
   Authentication is supported in VRRPv2 only.
   
   - **Reclaim**: 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 v3 checksum computation method. Certain third party devices may 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.
- VRRP is not supported in HA deployment.

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. When the HA failover time is greater than VRRP failover time, the VRRP failover happens and the router becomes the master. The router remains as the master until the HA failover happens and the secondary SD-WAN appliance becomes the master based on other VRRP attributes like higher priority and pre-emption, and so on. For more information on high availability deployment modes, see High Availability.

Configure Network Objects

December 14, 2018

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 on the name of the Network Object and enter a new name.

---

**Routing Support for LAN Segmentation**

**November 22, 2018**

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 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.

### Secure peering

December 14, 2018

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

December 14, 2018

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
Citrix SD-WAN 10.2

is sent to the remote machine that installs CA Certificate and the Private certificate and key for itself locally (on the remote machine).

Note

- IP Address – IP Address of remote ENTERPRISE EDITION APPLIANCE MANAGEMENT IP
- Username – Username of remote ENTERPRISE EDITION APPLIANCE
- Password – Password of remote 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 Enterprise Edition Appliance.

VIP of Remote EE App
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:


5. On partner appliance, View Secure Partner Information of the Enterprise Edition appliance
Troubleshooting


Auto Secure Peering initiated from PE appliance at DC site and branch site PE appliance

December 14, 2018
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.


**Troubleshooting**


Auto Secure Peering initiated from PE appliance at DC site and branch with standalone SD-WAN SE and WANOP appliance

December 14, 2018

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.
Note

IP Address – IP Address of remote WANOP Standalone or Standard Edition Appliance MANAGEMENT IP.

Username – Username of remote WANOP Standalone or Standard Edition Appliance.

Password – Password of remote WANOP Standalone or Standard Edition Appliance.

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.


Troubleshooting


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

December 14, 2018

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.

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**

December 14, 2018

- 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**


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

**December 14, 2018**

**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

December 14, 2018

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

December 14, 2018

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 cryptographic binary. Citrix SD-WAN also supports resilient IPsec tunneling using a differentiated virtual path tunneling mechanism.

How to configure ipsec tunnels for virtual and dynamic paths

April 30, 2019

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:
How to configure ipsec tunnel between SD-WAN and third-party devices

March 27, 2019

To configure ipsec tunnel for intranet or LAN service:

1. In the Configuration Editor, navigate to Connections > View Site > [Site Name] > IPsec Tunnels. Choose a Service Type (LAN or Intranet).
2. Enter a Name for the service type. For Intranet service type, the configured Intranet Server will determine which Local IP addresses are available.
3. Select the available Local IP address and enter the Peer IP address for the virtual path to peer with.
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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Type</td>
<td>Choose a service type from the drop-down menu</td>
<td>Intranet, LAN</td>
</tr>
<tr>
<td>Name</td>
<td>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</td>
<td>Text string</td>
</tr>
<tr>
<td>Local IP</td>
<td>Choose the local IP address of the IPsec Tunnel from the drop-down menu of available virtual IP addresses configured at this Site</td>
<td>IP address</td>
</tr>
<tr>
<td>Peer IP</td>
<td>Enter the peer IP address of the IPsec Tunnel</td>
<td>IP address</td>
</tr>
<tr>
<td>MTU</td>
<td>Enter the MTU for fragmenting IKE and IPSec fragments</td>
<td>Default: 1500</td>
</tr>
<tr>
<td>IKE Settings</td>
<td>Version: Choose an IKE version from the drop-down menu</td>
<td>IKEv1 IKEv2</td>
</tr>
<tr>
<td>Mode</td>
<td>Choose a mode from the drop-down menu</td>
<td>FIPS compliant: Main, Non-FIPS compliant: Aggressive</td>
</tr>
<tr>
<td>Identity</td>
<td>Choose an Identity from the drop-down menu</td>
<td>Auto IP Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manual IP Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User FQDN</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication</td>
<td>Choose the authentication type from the drop-down menu</td>
<td>Pre-Shared Key: If you are using a pre-shared key, copy and paste it into this field. Click on the Eyeball () icon to view the Pre-Shared Key. Certificate: If you are using an identity certificate, choose it from the drop-down menu.</td>
</tr>
<tr>
<td>Validate Peer Identity</td>
<td>Select this checkbox to validate the IKE’s peer. If the peer’s ID type is not supported, do not enable this feature</td>
<td>None</td>
</tr>
<tr>
<td>DH Group</td>
<td>Choose Diffie–Hellman group to use for IKE key generation from the drop-down menu</td>
<td>Non-FIPS compliant: Group 1, FIPS-compliant: Group 2 Group 5 Group 14 Group 15 Group 16 Group 19 Group 20 Group 21</td>
</tr>
<tr>
<td>Hash Algorithm</td>
<td>Choose an algorithm from the drop-down menu to authenticate IKE messages</td>
<td>Non-FIPS compliant: MD5 FIPS compliant: SHA1 SHA-256</td>
</tr>
<tr>
<td>Encryption Mode</td>
<td>Choose the Encryption Mode for IKE messages from the drop-down menu</td>
<td>AES 128-bit AES 192-bit AES 256-bit</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Lifetime (s)</td>
<td>Enter the preferred duration, in seconds, for an IKE security association to exist</td>
<td>3600 seconds (default)</td>
</tr>
<tr>
<td>Lifetime (s) Max</td>
<td>Enter the maximum preferred duration, in seconds, to allow an IKE security association to exist</td>
<td>86400 seconds (default)</td>
</tr>
<tr>
<td>DPD Timeout (s)</td>
<td>Enter the Dead Peer Detection timeout, in seconds, for VPN connections</td>
<td>300 seconds (default)</td>
</tr>
<tr>
<td>IKEv2</td>
<td>Peer Authentication: Choose Peer Authentication from the drop-down menu</td>
<td>Mirrored Pre-Shared Key Certificate</td>
</tr>
<tr>
<td>IKE2 - Pre-shared key</td>
<td>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</td>
<td>Text string</td>
</tr>
<tr>
<td>Integrity Algorithm</td>
<td>Choose an algorithm as the hashing algorithm to use for HMAC verification from the drop-down menu</td>
<td>Non-FIPS compliant: MD5 FIPS compliant: SHA1 SHA-256</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Value(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Type</td>
<td>Choose the Tunnel Type from the drop-down menu</td>
<td>ESP ESP+Auth ESP+NULL AH</td>
</tr>
<tr>
<td>PFS Group</td>
<td>Choose Diffie–Hellman group to use for perfect forward secrecy key generation from the drop-down menu</td>
<td>None Group 1 Group 2 Group 5 Group 14 Group 15 Group 16 Group 19 Group 20 Group 21</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Value(s)</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encryption Mode</td>
<td>Choose the Encryption Mode for IPsec messages from the drop-down menu</td>
<td>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</td>
</tr>
<tr>
<td>Lifetime (s)</td>
<td>Enter the amount of time, in seconds to allow an IPsec security association to exist</td>
<td>28800 seconds (default)</td>
</tr>
<tr>
<td>Lifetime Max (s)</td>
<td>Enter the maximum amount of time, in seconds to allow an IPsec security association to exist</td>
<td>86400 seconds (default)</td>
</tr>
<tr>
<td>Lifetime (KB)</td>
<td>Enter the amount of data, in kilobytes, for an IPsec security association to exist</td>
<td>Kilobytes</td>
</tr>
<tr>
<td>Lifetime (KB) Max</td>
<td>Enter the maximum amount of data, in kilobytes, to allow an IPsec security association to exist</td>
<td>Kilobytes</td>
</tr>
<tr>
<td>Network Mismatch Behavior</td>
<td>Choose the action to take if a packet does not match the IPsec Tunnel’s Protected Networks from the drop-down menu</td>
<td>Drop, Send Unencrypted, Use Non-IPsec Route</td>
</tr>
</tbody>
</table>
### 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

December 14, 2018

To implement certificates for IKE negotiation:

1. Navigate to Sites > Certificates and add any necessary certificates.

How to view ipsec tunnel configuration

December 14, 2018

To view ipsec tunnel configuration:

1. Navigate to Configuration > Virtual WAN > View Configuration.

2. Select Virtual Path Service from the drop-down menu. The IPsec settings are displayed only if IPsec is enabled in the configuration editor.
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

December 14, 2018

To monitor ipsec tunnel statistics:

1. Navigate to Monitor > Statistics. Choose IPsec Tunnel from the Show drop-down menu as shown below:

   ![IPsec tunnel statistics screenshot]

2. Navigate to Monitor > IKE/IPsec. Observe the configured IPsec tunnels, the IKE and IPsec service associations between two or more VPN endpoints configured within the SD-WAN network.
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

December 14, 2018

In previous releases, ipsec tunnel routes would remain in the route table, even if the tunnel became unavailable.
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

December 14, 2018

In previous releases, the tunnel type ESP+NULL was introduced. When using IPsec ESP protocol, traffic is typically encrypted and authenticated. However, you can choose not to use encryption by using Null
encryption. In ESP + NULL tunnel type the packets are authenticated but not encrypted.

You can configure the IPsec tunnel with ESP+NULL tunnel type in the Configuration editor, under **IPsec Settings** section.

![Image of Citrix SD-WAN UI](image.png)

### FIPS Compliance

**December 14, 2018**

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**

November 22, 2018

To secure traffic and enforce policies, enterprises often use MPLS links to backhaul branch traffic to the corporate data center. The data center applies security policies, filters traffic through security appliances to detect malware, and routes the traffic through an ISP. Such backhauling over private MPLS links is expensive. It also results in significant latency, which creates a poor user experience at the branch site. There is also a risk that users 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 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

December 18, 2018

The Zscaler Cloud Security Platform acts as a series of security check posts in more than 100 data centers around the world. By simply redirecting your internet traffic to Zscaler, you can immediately secure your stores, branches, and remote locations. Zscaler connects users and the internet, inspecting every byte of traffic, even if it is encrypted or compressed.

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.
To use GRE tunnel or IPsec Tunnel traffic forwarding:

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 [DRI] 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.
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 traffic needs this IP address as the gateway address.
To configure GRE Tunnel:

1. In the configuration editor, navigate to **Connections > Site > GRE Tunnels**, and configure routes to forward internet prefix services to the Zscaler GRE Tunnels.

   The source IP address can only be chosen from the Virtual network interface on trusted links. See, [How to configure GRE tunnel](#).

Configure routes 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 [DRI] 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-NUL** 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 > IPsec Tunnel]

For more information, see; monitoring IPsec tunnels and GRE tunnels topics.

Firewall Traffic Redirection Support by Using Forcepoint in Citrix SD-WAN

December 14, 2018

Forcepoint supports the following features, although SD-WAN supports only the firewall redirect feature:

- IPSec with PKI
- IPsec with PSK
- Proxy chaining using PAC file configuration
- Proxy chaining with standard headers
• Proxy chaining with proprietary headers removing the need to configure the client’s IP range - partnership/development
• Firewall redirect (transparent proxy by Destination NAT)

The Destination NAT policy enables enterprises to route internet traffic through cloud-hosted security service using ForcePoint.

Review the following use case to understand how to configure Destination NAT in SD-WAN appliances and redirect internet traffic through a secure cloud-based firewall service.

**Pre-requisites:**

1. 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 by Using IPsec Tunnels

December 11, 2018

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.

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 (GlobalProtect Cloud Service) network through IPsec tunnels at the customer’s site.
The key benefits include:

- Next-generation security delivered globally.
- Add and manage locations - users and policy deployment centrally.
- Forward IPsec tunnel traffic to the Palo Alto network.
- Have SD-WAN appliance configured in high availability mode - If an appliance fails, the IPsec tunnel is established through another appliance.
- Virtual routing and forwarding deployments.
- One WAN link as part of internet services.
Configure the following in Citrix SD-WAN GUI:

- Configure IPsec Tunnel.
- Configure IPsec Protected network with local LAN networks as Source subnet and Destination subnet as 0.0.0.0/0 (to send all internet traffic through tunnel).

Configure the following in Palo Alto:

- Configure all necessary IP tunnel details.
- Configure IPsec Peer with SD-WAN IPsec Tunnel Public source IP address.

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 Palo Alto global protect cloud service.
- Verify that Palo Alto security policy is applied on traffic.
- Verify response from internet to host in a branch comes through.
Use case 1: Branch-to-Internet

- Establish IPsec tunnel from each branch to the Palo Alto GlobalProtect Cloud Service GPCS.
- For branch-to-internet communication, configure protected networks with networks belonging to both the branches.
- For direct Internet breakout through the GPCS, configure IPsec protected networks on SD-WAN with destination subnet as 0.0.0.0/0.
Use case 2: Active-Standby-Tunnels from SDWAN to internet via Palo Alto

For active/standby, two IPsec tunnels are established with same parameters and the same protected networks to the GPCS and only one tunnel will be active all the time and another one will be on standby mode. This will act as a single conversed unit. To all the protected networks you want to provide IPsec protection, has to be configured on both active and standby tunnel. So that if one tunnel goes down another tunnel comes up with all active networks. This allows tunnels to be available all the time for redirecting Internet traffic by configuring IPsec protected networks.

1. Ability to have multiple IPsec tunnels created with Palo Alto from SD-WAN
   - Active
   - Standby

2. SD-WAN is created with multiple IPsec tunnels using Intranet services and matching IKE/IPSec settings (One for Active and one for standby).

3. Add all protected networks redundantly for all IPsec tunnel configurations.

4. Palo Alto hosts the active and standby tunnel.

5. SD-WAN will form tunnels with both and process traffic for the protected networks via the active IPsec tunnel first (if the primary tunnel is eligible)

6. If the primary tunnel goes down either at the SD-WAN end or at Palo Alto end, the traffic goes through the secondary tunnel (The same case for old and new traffic).

   The IPsec Security Associations (SAs) are formed as part of the primary and secondary tunnel formation. Hence transition of traffic takes some time (3–5 seconds) to detect new secondary and process all traffic through the newly active IPsec tunnel. The primary tunnel detection to process traffic depends on the route eligibility and is turned to NO if the tunnel goes down and is made YES if it is up.

7. If the primary tunnel comes back up, then the traffic is sent via the primary tunnel again.
To configure IKE and IPsec Tunnel with Palo Alto SWG on SD-WAN:

1. Navigate to **Connection > Site > IPsec Tunnels**.

2. Configure IKE and IPsec parameters.

For more information about configuring IPsec tunnels, see configure IPsec tunnels between SD-WAN and third party cloud services/devices.

You can specify which traffic to be protected by IPsec using **Protected Networks**.
Monitoring IPsec tunnel to Palo Alto SWG on SD-WAN:

In the Citrix SD-WAN appliance GUI, go to Monitoring > Statistics. Select IPsec Tunnel from the dropdown list to check the statistics against the tunnel processing the traffic. Traffic that is sent over tunnel can be monitored in the sent and received columns.

![Monitoring IPsec Tunnel Statistics](image)

Monitoring Route hits for traffic towards Palo Alto IPsec tunnel (to Intranet service as the IPsec tunnel is bound to Intranet service):

Routes indicate traffic that hits against the Intranet service which is currently processing the traffic. To see the route statistics, go to Monitoring > Statistics > Routes and check the statistics against the route processing the traffic.

![Monitoring Route Statistics](image)

**Use case 3: Branch-to-Branch traffic via Palo Alto SWG**

Helps to communicate between the branches and apply security policies on an SWG for branch to branch connection without going via the SD-WAN intermediate node.

For branch-to-branch communication, specify the IPsec policies go through the Palo Alto GlobalProtect Cloud Service (GPCS) first through an IPsec tunnel. GPCS determines if it’s getting traffic from branch 1, and then sends it to branch 2 via an IPsec tunnel by creating policies.
1. Create separate tunnel endpoints at Palo Alto one for each branch.

2. Each branch uniquely creates an IPsec tunnel with Palo Alto using Intranet services and matching IKE/IPSec Settings.

3. Configuration of protected networks in Branch 1 to Palo Alto tunnel 1:
   - Source as Branch 1 subnet to destination as Branch 2 subnet
   - Mirror the Protected Network on the Palo Alto tunnel Proxy ID side

   Follow the similar protected network using Branch 2 to Palo Alto tunnel 2

4. Traffic from Branch 1 to Branch 2 is carried out using Branch 1 to Palo Alto Tunnel 1 IPsec tunnel and then forwarded by Palo Alto into the new tunnel between Palo Alto tunnel 2 to Branch 2 IPsec tunnel. Same is the case for the return traffic.

   **NOTE:**
   This traffic is unique in a way that the MCN need not be WAN to WAN forwarding enabled.

5. If the branches are NAT’d of the IPs then they would need to be enabled with WAN link NAT address (if static) on the **WAN link** settings where the intranet service would be enabled to use for IPsec tunnel. If the IP is dynamic, then the branches have to be enabled with **Auto Detect Public IP** knob.

6. If there is exclusive port NATting then the MCN needs to be enabled with UDP hole punching.

Configuration for Branch 1 SD-WAN to Palo Alto IPsec tunnel 1:
Configuration of Branch 2 SD-WAN to Palo Alto IPsec tunnel 2:

Monitoring IKE/IPsec SA's for tunnel 1 between Branch 1 to Palo Alto:
Monitoring IKE/IPsec SA's for tunnel 2 between Branch 1 to Palo Alto:

Monitoring Flows and Firewall for Branch 1 to Palo Alto tunnel 1:

The following screenshot provides the combined monitoring information on flow data and firewall statistics for Branch 1 to Palo Alto tunnel 1.

Monitoring Flows and Firewall for Branch 2 to Palo Alto tunnel 2:
The following screenshot provides the combined monitoring information on flow data and firewall statistics for Branch 2 to Palo Alto tunnel 2.

IPsec tunnel statistics monitoring for Branch 1 to Palo Alto 1 tunnel:

IPsec tunnel statistics monitoring for Branch 2 to Palo Alto 2 tunnel:

Use case 4: SD-WAN edge device in high availability mode

- Configure SD-WAN appliance in high availability mode.
- Establish IPsec tunnel from each branch to GPCS.
- Traffic redirection from SD-WAN to GPCS always occurs through the active appliance.
- Upon a high availability event, secondary SD-WAN appliance takes over and starts sending traffic towards GPCS.

To configure IPsec Tunnel:

1. Navigate to **Connection > Site > IPsec Tunnels**.
2. Configure IKE and IPsec parameters.

   For more information about configuring IPsec tunnels, see [configure IPsec tunnels between SD-WAN and third party cloud services/devices](#).

   You can specify which traffic to be protected by IPsec using Protected Networks. You can configure maximum of eight protected networks per tunnel.
Monitor IPsec Tunnels:

In the Citrix SD-WAN appliance GUI, go to Monitoring > Statistics. Select **IPsec Tunnel** from the Show dropdown list. Traffic that is sent over tunnel can be monitored in the sent and received columns.

- **Monitoring > IKE/IPsec** - You can monitor all IKE and corresponding IPsec SAs.
Configure IPsec in Palo Alto Global Protect Cloud Service (GPCS):

1. Log in to Palo Alto Panorama.
2. Navigate to **Network Profile** -> **IKE Crypto** and configure the IKE crypto suite.
Configure IKE gateway:

1. Add IKE Gateway.
2. Configure IKE Version.
3. Choose the **Peer IP Address Type** as **IP**.
4. Enter the **IKE Peer IP address**. This is the Citrix SD-WAN Public IP.
5. Configure Authentication type, Pre-Shared Key, Certificate.
6. Configure Pre-shared Key that you are going to use.
7. Click **Enable NAT Traversal** in the **Advanced Options** tab page.

Create IPsec Tunnel:

Add an IPsec Tunnel with already created IKE Gateway and IPsec Crypto Profile. Provide the protected network to allow traffic from SD-WAN through the tunnel.
Block applications:

You can block certain applications by configuring firewall rule as follows. This rule is bound to the tunnel created.

Verify end-to-end traffic:

From the branch host access internet and check for internet traffic to appear under the IPsec tunnel statistics in the SD-WAN GUI monitoring page.
Check for any blocked sites in Palo Alto GPCS and ensure that the blocked sites are inaccessible from the branch network.

Stateful Firewall and NAT Support

December 14, 2018

This feature provides a firewall built into the SD-WAN application. The firewall allows policies between services and zones, and supports Static NAT, Dynamic NAT (PAT), and Dynamic NAT with Port Forwarding. 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
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**

December 14, 2018

You can configure the advanced firewall settings for every site individually. This will override the global settings.

To configure advanced firewall settings:
1. In the Configuration Editor, navigate to Connections > View Site > Firewall > Settings.

![Configuration Editor Screenshot](image)

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

December 14, 2018

You can configure zones in the network and define policies to control how traffic enters and leaves zones. By default, the following zones are created:

- **Internet_Zone**
  - Applies to traffic to or from an Internet service using a Trusted interface.

- **Untrusted_Internet_Zone**
  - Applies to traffic to or from an Internet service using an Untrusted interface.

- **Default_LAN_Zone**
  - Applies to traffic to or from an object with a configurable zone, where the zone has not been set.

You can create your own zones and assign them to the following types of objects:

- Virtual Network Interfaces (VNI)
- Intranet Services
- GRE Tunnels
- LAN IPsec Tunnels
The following illustration displays the three zones pre-configured. Additionally, you can create your own zones as required. In this example, the zone “ZoneA_Intranet” is a user created zone. It is assigned to the Virtual Interface of the bypass segment (ports 1 and 2) of the SD-WAN appliance.

The source zone of a packet is determined by the service or virtual network interface a packet is received on. The exception to this is virtual path traffic. When traffic enters a virtual path, packets are marked with the zone that originated the traffic and that source zone is carried through the virtual path. This allows the receiving end of the virtual path to make a policy decision based on the original source zone before it entered the virtual path.

For example, a network administrator may want to define policies so that only traffic from VLAN 30 at Site A is allowed to enter VLAN 10 at Site B. The administrator can assign a zone for each VLAN and create policies that permit traffic between these zones and blocks traffic from other zones. The screenshot below shows how a user would assign the “ZoneA_Intranet” zone to VLAN 10. In this example, the “ZoneA_Intranet” zone was previously defined by the user in order to assign it to Virtual Interface “VirtualInterface-2”.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
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).

Policies

December 18, 2018

Policies provide the ability to allow, deny, reject, or count and continue specific traffic flows. Applying these policies individually to each site would be difficult as the SD-WAN networks grows. To resolve this issue, groups of firewall filters can be created with a Firewall Policy Template. A Firewall Policy Template can be applied to all sites in the network or only to specific sites. These policies are ordered as either Pre-Appliance Template Policies or Post- Appliance Template Policies. Both network-wide Pre-Appliance and Post-Appliance Template Policies are configured at the Global level. Local policies are configured at the site level under Connections and apply only to that specific site.
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 policies.

- **Zone** – flows have a source zone and destination zone.
  - **From Zone** – source zone for the policy.
  - **To Zone** – destination zone for the policy.

- **Action** – action to perform on a matched flow.
  - **Allow** – permit the flow through the Firewall.
  - **Drop** – deny the flow through the firewall by dropping the packets.
  - **Reject** – deny the flow through the firewall and send a protocol specific response. TCP will send a reset, ICMP will send an error message.
  - **Count and Continue** – count the number of packets and bytes for this flow, then continue down the policy list.

- **Log Interval** – time in seconds between logging the number of packets matching the policy to the firewall log file or the syslog server, if it is configured.
  - **Log Start** – if selected, a log entry is created for the new flow.
  - **Log End** – log the data for a flow when the flow is deleted.

**Note**
The default Log Interval value of 0 means no logging.

- **Track** – allows the firewall to track the state of a flow and display this information in the Monitoring > Firewall > Connections table. If the flow is not tracked, the state will show NOT_TRACKED. See the table for the state tracking based on protocol below. Use the setting defined at the site level under Firewall > Settings > Advanced > Default Tracking.
  - **No Track** – flow state is not enabled.
  - **Track** – displays the current state of the flow (which matched this policy).

- **Match Type** – select one of the following match types –
  - **IP Protocol** – If this match type is selected, select an IP protocol that the filter will match with. Options include ANY, TCP, UDP ICMP and so
  - **Application** – If this match type is selected, specify the application that is used as a match criteria for this filter.
  - **Application Family** – If this match type is selected, select an application family that is used as a match criteria for this filter.
The track option provides much more detail about a flow. The state information tracked in the state tables is included below.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
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)

November 22, 2018

The SD-WAN firewall allows the user to configure static NAT and dynamic NAT for different use cases. The following configurations are supported for NAT:

- Static one-to-one NAT
- Dynamic NAT (PAT- Port Address Translation)
- Dynamic NAT with Port Forwarding rules
At this time, the NAT capability can only be configured at the site level; there is no global configuration (templates) for NAT. All NAT policies are defined from a Source-NAT (“SNAT”) translation. Corresponding Destination-NAT (“DNAT”) rules are created automatically for the user.

**Configure static NAT**

December 14, 2018

Static NAT allows the user to configure one-to-one NAT, where an inside IP address will match a public IP address. The configuration options are shown below. You must also define the filter policies to allow traffic back in for the static NAT configuration. You can configure static NAT by navigating to **Connections > View Site > Firewall > Section > Static NAT Policies.**

![Configuration options](image)

**Configuration options**

- **Priority** - the order the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority policies.

- **Direction** – the direction, from the perspective of the virtual interface or service, that the translation will operate.

- **Outbound** – the destination address for a packet will be translated for packets received on the service. The source address will be translated for packets transmitted on the service.

For example, LAN service to Internet service – for packets outbound, (LAN to Internet) the source IP address is translated. For packets inbound or received (Internet to LAN) the destination IP address are translated.
- **Inbound** - the source address for a packet will be translated for packets received on the service. The destination address will be translated for packets transmitted on the service.

For example, Internet service to LAN service – For packets received on the Internet service, the source IP address is translated. For packets transmitted on the Internet service, the destination IP address is translated.

- **Service Type** – in reference to a SD-WAN service. For static NAT, these include Local (to the appliance), Intranet, and Internet.

- **Service Name** – specific service name that corresponds to the defined Service Type above.

- **Inside Zone** – one of the existing inside zones configured on the appliance.

- **Inside IP address** – source IP address and mask of the direction selected above.

- **Outside IP address** – the outside IP address and mask of packets that are translated to.

**Configure dynamic NAT**

December 14, 2018

Dynamic NAT is used when the user wants to forward traffic from a LAN segment to the Internet on an untrusted port. In this case, the user would configure the NAT in an outbound direction, as well as make sure the corresponding filter policies are defined to allow traffic back in. By default, once the dynamic NAT has been configured the system will add in three filter policies.

These policies will:

- allow Any IPhost route, Any zone, Any source and destination.
- allow match established rule, for reverse traffic of sessions initiated from the inside network.
- drop all other traffic from the source zone to the destination zone (zone specific).

The following screenshot displays the configuration options for the dynamic NAT configuration.
Configuration Options

- **Priority** – the order the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority policies.

- **Direction** – the direction from the virtual interface or service perspective the translation will operate.

- **Outbound** – the destination address for a packet will be translated for packets received on the service. The source address will be translated for packets transmitted on the service.

  For example, LAN service to Internet service – for packets outbound, (LAN to Internet) the source IP address is translated. For packets inbound or received (Internet to LAN) the destination IP address are translated.

  - **Inbound** - the source address for a packet will be translated for packets received on the service. The destination address will be translated for packets transmitted on the service.

  For example, Internet service to LAN service – for packets received on the Internet service the source IP address is translated. For packets transmitted on the Internet service, the destination IP address is translated.

- **Type** – the type of dynamic NAT to perform.

  - **Port-Restricted** - Port-Restricted NAT is what most consumer grade gateway routers use. Inbound connections are generally disallowed unless a port is specifically forwarded to an inside address. Outbound connections allow return traffic from the same remote IP and port (this is known as endpoint independent mapping). This requirement limits a Port-
Restricted NAT firewall to 65535 simultaneous sessions, but facilitates an often used internet technology known as hole punching.

- **Symmetric** – Symmetric NAT is sometimes known as enterprise NAT because it allows for a much larger NAT space and enhances security by making translations less predictable. Inbound connections are generally disallowed unless a port is specifically forwarded to an inside address. Outbound connections allow return traffic from the same remote IP and port. Connections from the same inside IP and port need to map to the same outside IP and port (this is known as endpoint dependent mapping). This mode explicitly prevents hole punching.

- **Service Type** – in reference to a SD-WAN service. For static NAT these include Local (to the appliance), Intranet, Internet.

- **Service Name** – the specific service name that corresponds to the defined Service Type above.

- **Inside Zone** – select the inside zone for the packets that require NAT.

- **Inside IP address** - define an IP host address or a subnet based on traffic that requires NAT. This should be an IP address that resides in the Inside Zone.

- **Allow Related** – allow traffic related to the flow matching the rule. For example, ICMP redirection related to the specific flow that matched the policy, if there was some type of error related to the flow.

- **IPsec Passthrough** – allow IPsec traffic to pass through unchanged.

- **GRE/PPTP Passthrough** – allow GRE or IPsec to pass through unchanged.

- **Port Parity** - allows parity for NAT connections.

### Configure dynamic NAT with port forwarding

December 14, 2018

Dynamic NAT with port forwarding allows the user to port forward specific traffic to a defined IP address. This is typically used for inside hosts like web servers. Once the dynamic NAT is configured the user would define the port forwarding policy. From the example in figure below, we can see that dynamic NAT is configured for a specific IP host address. The NAT example will map an inside IP host to an outside IP host. Port forwarding can then be configured which will define a specific inside and outside port mapped to an inside IP address. In this example, HTTP port 80 is defined for port forwarding.
Configuration Options

- **Protocol** – TCP, UDP, or both.
- **Outside Port** – outside port the user will port forward into the inside port.
- **Inside IP address** – inside address to forward matching packets.
- **Inside Port** – map the packet to the same, or a different, outside port.
- **Fragments** – allow the forwarding of fragmented packets.
- **Log Interval** – time in second between logging the number of packets matching the policy to a syslog server.
- **Log Start** – If selected, a new log entry is created for the new flow.
- **Log End** – log the data for a flow when the flow is deleted.

**Note**

The default Log Interval value of 0 means no logging.

- **Track** – allows the firewall to track the state of a flow and display this information in the Monitor > Firewall > Connections. If the flow is not tracked, the state will show NOT_TRACKED. See the table for the state tracking based on protocol below. Use the setting defined at the site level under Firewall > Settings > Advanced > Default Tracking.
  - **No Track** – flow state is not enabled.
  - **Track** – displays the current state of the flow (which matched this policy).
Configure Virtual WAN Service

December 14, 2018

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.
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

December 14, 2018

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.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
You should see that 0.0.0.0/0 routes added, one per routing domain, under Connections > View Region > View Site > [Site Name] > Routes.

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**.

4. You can also check the routing table for each routing domain under **Monitor > Statistics > Routes**.

**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.
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.

**AppFlow and IPFIX**

December 18, 2018

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.

IPFIX version 10 is supported in Citrix SD-WAN release 10 version 2 and above.

There are a few architectural changes, resulting in low performance impact when Net Flow, AppFlow, and IPFIX are enabled together as these protocol reuse resources.

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.

- **Application Flow Info (IPFIX)**: The IPFIX template to collect and send flow records of all connections to IPFIX collector.

- **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.
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.
- **Application Flow Info**: The IPFIX template to collect and send flow records of all connections to IPFIX collector.
- **Citrix ADM**: Select this to use Citrix ADM as the AppFlow collector.
  
  **Note**: Select this to use Citrix ADM as the AppFlow collector. 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 SDWAN_export.log files.
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.

<table>
<thead>
<tr>
<th>MIB</th>
<th>RFC (Definition Link)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-MIB (Partial)</td>
<td><a href="https://www.ietf.org/rfc/rfc4293.txt">https://www.ietf.org/rfc/rfc4293.txt</a></td>
</tr>
<tr>
<td>SNMPv2-MIB</td>
<td><a href="https://www.ietf.org/rfc/rfc3418.txt">https://www.ietf.org/rfc/rfc3418.txt</a></td>
</tr>
<tr>
<td>P-BRIDGE-MIB.txt</td>
<td><a href="http://www.icir.org/fenner/mibs/extracted/P-BRIDGE-MIB-rfc2674.txt">http://www.icir.org/fenner/mibs/extracted/P-BRIDGE-MIB-rfc2674.txt</a></td>
</tr>
<tr>
<td>RMON2-MIB.txt</td>
<td><a href="https://www.ietf.org/rfc/rfc3273.txt">https://www.ietf.org/rfc/rfc3273.txt</a></td>
</tr>
</tbody>
</table>

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.

![MIB browser screenshot](image)

**Note**

- Support for these MIBs is provided by default by the **net-snmp snmpd** daemon process on Linux systems. The MIBs provide the basis for supporting Network Management applications.

- The Ethernet port packet and byte counters are in the **IF-MIB** inside the **ifTable**. System information is in the system object.

- Ethernet ports are included in the **ifTable**, so walking that should be sufficient to ensure that the SNMP subsystem is running.

- Support for the **Q-BRIDGE-MIB** and the **IP-MIB** provides support for the network mapping application.

For additional information about adding SNMP manager, configuring SNMP View/Alarm, and adding SNMP server, see the CloudBridge 7.4 documentation at: CloudBridge

**SMB 3.1.1 connection**

December 14, 2018

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”.

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
<th>SMB version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10</td>
<td>Win 2016, 2012R2</td>
<td>SMB 3.1.1, 3.0.2</td>
</tr>
<tr>
<td>Windows 8.1</td>
<td>SMB 3.0</td>
<td>SMB 3.0</td>
</tr>
<tr>
<td>Windows 7</td>
<td>SMB 3.0</td>
<td>SMB 3.0</td>
</tr>
</tbody>
</table>

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.
WAN optimization

May 29, 2019

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, including cross-session tokenized compression
- TCP protocol acceleration
- Traffic management
- Application acceleration
- Citrix Virtual Apps and Desktops (HDX) acceleration and compression offload
- Decryption of HDX traffic secured by SSL/TLS
- 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.
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

**December 18, 2018**

Enabling WAN Optimization in your Virtual WAN entails the following procedures:

1. Enable WAN Optimization in the **Features** settings of the **Optimization** section.
   
   Instructions for this part of the process are provided in this section.

2. Configure the **Acceleration** policy setting for each applicable Service Class in the **Service Classes** table.

   This procedure occurs further on, after you have completed the rest of the **Optimization** configuration. Instructions are provided in the section, **Configuring Optimization Default Service Classes**. At this point, WAN Optimization has been enabled in your configuration, but not yet enabled and activated in your Virtual WAN. To enable and activate WAN Optimization in your Virtual WAN, you must complete the Virtual WAN configuration, and then generate, stage, and activate the Virtual WAN Appliance Packages on the eligible sites in your deployment, as outlined in the subsequent chapters of this guide.

To enable WAN Optimization and configure the **Defaults** section **Features** settings, do the following:

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 will be available in the **Configuration Editor**.

**Note**

If the **Optimization** section is not available, please check that you have installed a SD-WAN Enterprise Edition license in your Virtual WAN. SD-WAN Standard Edition does not support WAN Optimization features.

For details and instructions, see the following sections:

- **The SD-WAN Editions**
- **Licensing**


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**.

![WAN Optimization Features](image)

e) Select the **WAN Optimization** checkbox.

The **WAN Optimization** checkbox is in the upper left corner of the **WAN Optimization Features** section. This enables the form for editing, and reveals the **Apply** and **Revert** buttons.
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 checkbox to select or deselect an option. You can accept the default settings pre-selected in the form, or customize the settings.

Note

By default, the settings you configure in the Global tab are automatically applied to each branch site included in the tree. However, you can customize the Optimization configuration for a specific branch, as outlined in the section, Configuring Optimization for a Branch Site.

The Features configuration form contains two sections:

- WAN Optimization Features
- CIFS Optimization Protocols

The WAN Optimization Features settings are as follows:

- WAN Optimization – Select this to enable WAN Optimization for this configuration. This also enables compression, deduplication, and TCP Protocol Optimization.

  Note

  The WAN Optimization option must be selected for the other Optimization section options to be available.

- SCPS – Select this to enable TCP Protocol optimization for Satellite Links.

- HDX QoS Priorities – Select this to enable optimization of ICA traffic based on prioritization of HDX sub-channels.

- MAPI Cross Protocol Optimization – Select this to enable cross-protocol optimization of Microsoft Outlook (MAPI) traffic.
- **SSL Optimization** – Select this to enable optimization for traffic streams with SSL encryption.

- **RPC Over HTTP** – Select this to enable optimization of Microsoft Exchange traffic that uses RPC over HTTP.

- **User Data Store Encryption** – Select this to enable enhanced security of data through the encryption of WAN Optimization compression history.

- **Native MAPI** – Select this to enable optimization of Microsoft Exchange traffic.

The **CIFS Optimization Protocols** options are as follows:

- **SMB1** – Select this to enable Optimization of Windows File Sharing (SMB1)

- **SMB2** – Select this to enable Optimization of Windows File Sharing (SMB2)

- **SMB3** – Select this to enable Optimization of Windows File Sharing (SMB3). You must first select the **SMB2** option before you can select **SMB3**.

  g) Click **Apply**.

  This enables and adds the selected **Default Features** to the configuration package.

The next step is to configure the **Optimization** default **Tuning Settings**.

---

**Configure optimization default tuning settings**

December 14, 2018

You can configure the WAN optimization default tuning settings in the **Global** tab.

To configure the WAN Optimization default **Tuning Settings**, do the following:

1. In the **Global** tab, click **WAN Optimization Tuning Settings**.
2. Select and configure the **Tuning Settings**.

The **Tuning Settings** options are as follows:

- **Maximum MSS** – Enter the maximum size (in bytes) for the Maximum Segment Size (MSS) for a TCP segment.

- **Default MSS** – Enter the default size (in octets) for the MSS for TCP segments.

- **Enable Connection Timeout** – Select this to enable automatic termination of a connection when the idle threshold is exceeded.

- **Idle Timeout** – Enter a threshold value (in seconds) to specify the amount of idle time permitted before an idle connection is terminated. You must first select **Enable Connection Timeout** before this field can be configured.

3. Click **Apply**.

This applies the modified **Tuning Settings** to the global configuration.

The next step is to configure the default set of WAN Optimization Application Classifiers.

**Configure optimization default application classifiers**

December 14, 2018
You can configure the WAN optimization default application classifier settings in the **Global** tab.

To configure the default set of WAN Optimization Application Classifiers, do the following:

1. In the **Global** tab, click **WAN Optimization Application Classifiers**.

   This opens the **Application Classifiers** table, displaying the default set of Application Classifiers.

   ![Application Classifiers Table]

   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**

December 14, 2018

You can configure the WAN optimization default service class settings in the **Global** tab.

To configure the default set of WAN Optimization Service Classes, do the following:

1. In the **Global** tab, click **WAN Optimization Service Classes**.

   This opens the **Service Classes** table, displaying the default set of Service Classes.
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.

![Diagram of Citrix SD-WAN 10.2 user interface]

   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.
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

December 18, 2018

After you have completed the default global configuration, you have the option of customizing the sets and settings for each of the branch sites.

The global settings you just configured are automatically applied to each branch site included in the Optimization section. You can elect to accept the defaults, or customize the configuration for any given branch. The procedures for configuring the Optimization sets and settings for a branch site are the same as for configuring the global defaults, with a few minor differences.

To customize the Optimization configuration for a branch site, do the following:

1. Click Optimization tab, in the View Site field, select a site.
2. Select the **Override Defaults** checkbox.

This reveals the top-level configuration form for that configuration category, and opens it for editing.

The below image shows an example top-level settings configuration form, in this case for the **Features** set.

3. Enter your configuration changes.

From this point on, the configuration process for each branch site Optimization category is the same as for the corresponding global section category. For instructions on configuring a particular category of sets or settings, see the appropriate section listed below:

- Enabling Optimization and Configuring the Defaults Features Settings.
- Configuring Optimization Default Tuning Settings.
- Configuring Optimization Default Application Classifiers.
- Configuring Optimization Default Service Classes.

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**

December 14, 2018
All SSL related configuration is available through the new configuration editor of the appliance for security and usability. On the SD-WAN Enterprise Edition and two-box deployments, service classes are configured from the configuration editor and hence you cannot attach any SSL profiles. To accommodate the expression of SSL profile mapping to a service class, the work flow for SSL profiles is changed to allow for attaching Service classes in the profile node.

One of the limitations is that the SSL profile will get attached to all rules in a service class. If you need to attach the SSL profile selectively to a particular rule, the service class configuration is split into detailed rules for further selection.

To create SSL profile on new Enterprise Edition appliance at the data center:

1. In the SD-WAN web GUI, go to the Configuration > Secure Acceleration page. Click Add Profile. Create the SSL Profile.
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

December 14, 2018

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

November 22, 2018

On the client side of the accelerated link, the WANOP Client Plug-in is supported on Windows desktop and laptop systems, but not on netbooks or thin clients. Citrix recommends the following minimum hardware specifications for the computer running the WANOP Client Plug-in:

- Pentium 4-class CPU
Citrix SD-WAN 10.2

- 2 GB of RAM
- 2 GB of free disk space

WANOP Client Plug-in is supported on Windows 10 platform and needs following system requirements:
- 4GB RAM
- 10GB free disk space

The WANOP Client Plug-in is supported on the following operating systems:
- Windows XP Home
- Windows XP Professional
- Windows Vista (all 32-bit versions of Home Basic, Home Premium, Business, Enterprise, and Ultimate)
- Windows 7 (all 32-bit and 64-bit versions of Home Basic, Home Premium, Professional, Enterprise, and Ultimate)
- Windows 8 (32-bit and 64-bit versions of Enterprise Edition)
- Windows 10 (32-bit and 64-bit versions of Enterprise Edition)

On the server side, the following appliances currently support WANOP Client Plug-in deployments:
- Repeater 8500 Series
- Repeater 8800 Series
- WANOP Client Plug-in VPX
- WANOP Client Plug-in 2000
- WANOP Client Plug-in 3000
- WANOP Client Plug-in 4000
- WANOP Client Plug-in 5000

**How the WANOP plug-in works**

December 14, 2018

WANOP Client Plug-in products use your existing WAN/VPN infrastructure. A computer on which the plug-in is installed continues to access the LAN, WAN, and Internet as it did before installation of the plug-in. No changes are required to your routing tables, network settings, client applications, or server applications.
Citrix Access Gateway VPNs require a small amount of WANOP Client Plug-in-specific configuration.

There are two variations on the way connections are handled by the plug-in and appliance: transparent mode and redirector mode. Redirector is a legacy mode that is not recommended for new deployments.

- **Transparent mode** for plug-in-to-appliance acceleration is very similar to appliance-to-appliance acceleration. The WANOP Client Plug-in appliance must be in the path taken by the packets when traveling between the plug-in and the server. As with appliance-to-appliance acceleration, transparent mode operates as a transparent proxy, preserving the source and destination IP address and port numbers from one end of the connection to the other.

- **Redirector mode** (not recommended) uses an explicit proxy. The plug-in readdresses outgoing packets to the appliance’s redirector IP address. The appliance in turn readdresses the packets to the server, while changing the return address to point to itself instead of the plug-in. In this mode, the appliance does not have to be physically inline with the path between the WAN interface and the server (though this is the ideal deployment).

Best Practice: Use transparent mode when you can, and redirector mode when you must.

**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

December 14, 2018

Client acceleration requires special configuration on the WANOP Client Plug-in appliance. Other considerations include appliance placement. Plug-ins are typically deployed for VPN connections.

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.


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
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 communication
with the server if the plug-in and appliance were not present. That is, when a client opens an HTTP connection on port 80, it connects to the appliance on port 80. The appliance in turn contacts the server on port 80.

In redirector mode, only the well-known port (that is, the destination port on the TCP SYN packet) is preserved. The ephemeral port is not preserved. In transparent mode, both ports are preserved.

The appliance assumes that it can communicate with the server on any port requested by the client, and the client assumes that it can communicate with the appliance on any desired port. This works well if appliance is subject to the same firewall rules as the servers. When such is the case, any connection that would succeed in a direct connection succeeds in an accelerated connection.

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

January 4, 2019

You can change parameters in the WANOP Client Plug-in distribution file, which is in the standard Microsoft Installer (MSI) format. Customization requires the use of an MSI editor.

Note

The altered parameters in your edited. MSI file apply only to new installations. When existing plug-in users update to a new release, their existing settings are retained. Therefore, after changing the parameters, you should advise your users to uninstall the old version before installing the new one.

Best Practices:

Create a DNS entry that resolves to the nearest plug-in-enabled appliance. For example, define “Repeater.mycompany.com” and have it resolve to your appliance, if you have only one appliance. Or,
if you have, say, five appliances, have Repeater.mycompany.com resolve to one of your five appliances, with the appliance selected on the basis of closeness to the client or to the VPN unit. For example, a client using an address associated with a particular VPN should see Repeater.mycompany.com resolve to the IP address of the WANOP Client Plug-in appliance connected to that VPN. Build this address into your plug-in binary with an MSI editor, such as Orca. When you add, move, or remove appliances, changing this single DNS definition on your DNS server updates the appliance list on your plug-ins automatically.

You can also have the DNS entry resolve to multiple appliances, but this is undesirable unless all appliances are configured identically, because the plug-in takes some of its characteristics from the leftmost appliance in the list and applies them globally (including SSL compression characteristics). This can lead to undesirable and confusing results, especially if the DNS server rotates the order of IP addresses for each request.

**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**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSAPPLIANCES</td>
<td>List of appliances</td>
<td>None</td>
<td>Enter the IP or DNS addresses of your WANOP appliances here, in a comma-separated list in the form of <code>{ appliance1, appliance2, appliance3 }</code>. If the port used for signaling connections is different from the default (443), specify the port in the form <code>Appliance1:port_number</code>.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Default</td>
<td>Comments</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DBCMINSIZE</td>
<td>Minimum amount of disk space to use for compression, in megabytes</td>
<td>250</td>
<td>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.</td>
</tr>
<tr>
<td>EKEYPEM</td>
<td>Private key for the plug-in. Part of the certificate/key pair used with SSL compression</td>
<td>None</td>
<td>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—– )</td>
</tr>
<tr>
<td>X509CERTPEM</td>
<td>Certificate for the plug-in. Part of the certificate/key pair used with SSL compression</td>
<td>None</td>
<td>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 —– )</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Default</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CACERTPEM</td>
<td>Certification Authority Certificate for the plug-in. Used with SSL compression</td>
<td>None</td>
<td>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 —– )</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSAPPLIANCES</td>
<td>List of appliances</td>
<td>None</td>
<td>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 Appli- ance1:port_number .</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Default</td>
<td>Comments</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DBCMINSIZE</td>
<td>Minimum amount of disk space to use for compression, in megabytes</td>
<td>250</td>
<td>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.</td>
</tr>
<tr>
<td>PRIVATEKEYPEM</td>
<td>Private key for the plug-in. Part of the certificate/key pair used with SSL compression</td>
<td>None</td>
<td>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—– )</td>
</tr>
<tr>
<td>X509CERTPEM</td>
<td>Certificate for the plug-in. Part of the certificate/key pair used with SSL compression</td>
<td>None</td>
<td>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 —– )</td>
</tr>
</tbody>
</table>
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.
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**

January 4, 2019

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 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 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 appli-
ance. 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**

December 14, 2018
The WANOP Client Plug-in GUI appears when you right-click the Citrix Accelerator Plug-in icon and select Manage Acceleration. The GUI’s Basic display appears first. There is also an Advanced display that can be used if desired.

**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 systems. Clicking More displays the same information as with accelerated connections, plus a status field that reports Active if the CIFS connection is running with WANOP Client Plug-in's special CIFS optimizations.

- **Accelerated MAPI Connections**—The number of open, accelerated Outlook/Exchange connections.

- **Accelerated ICA connections**—The number of open, accelerated XenApp and XenDesktop connections using the ICA or CGP protocols.

- **Unaccelerated Connections**—Open connections that are not being accelerated. You can click More to display a brief description of why the connection was not accelerated. Typically, the reason is that no appliance accelerates the destination address, which is reported as Service policy rule.

- **Opening/Closing Connections**—Connections that are not fully open, but are in the process of opening or closing (TCP “half-open” or “half-closed” connections). The More button displays some additional information about these connections.

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.

![Image of Citrix Acceleration Plug-in Manager](image)

**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.
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**

November 22, 2018

To install a newer version of the WANOP Client Plug-in, follow the same procedure you used when installing the plug-in for the first time.
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

November 22, 2018

- **Issue**: I am facing signaling channel connectivity issues. How can I resolve these issues?
  
  **Resolution**: To resolve signaling channel connectivity issues, perform the following troubleshooting steps:
  
  - Verify that you have correctly configured the signaling IP address. You can do so by pinging the signaling IP address and verifying the response.
  - Verify that the signaling status is enabled on the WANOP appliance.
  - Verify that the firewall installed on the network does not remove the WANOP TCP options.
  - Verify that a valid WANOP plug-in license is installed on the WANOP appliance.
  - Verify that the Signaling Channel Source Filtering configuration does not block the Client Source IP address.
  - If you have enabled LAN Detection, verify that the Round Trip Time between the WANOP plug-in and WANOP appliance is an acceptable value.

- **Issue**: On a WANOP 4000 appliance, I am not able to disable the WANOP plug-in.
  
  **Cause**: This is a known issue.
  
  **Resolution**: None. You cannot disable the WANOP plug-in on a WANOP 4000 appliance.

- **Issue**: When connecting to the WANOP appliance by using the WANOP plug-in, the following error message entry is logged on the Alerts tab:

  More WANOP Plug-ins than the current limit of <Number> have attempted to connect to this Appliance.

  **Cause**: The number of connections to the WANOP appliance has exceeded the licensed user limit.
  
  **Resolution**: Either wait for a user to disconnect or terminate a connection.
• Issue: Incorrect signaling IP address is configured on a WANOP 4000 or 5000 appliance.

Resolution: To update the signaling IP address on a WANOP 4000 or 5000 appliance, complete the following procedure:

1. Log on to the NetScaler instance of the WANOP appliance.
3. Update the signaling IP address.
4. Save the configuration.

• Issue: CIFS and ICA traffic is not getting accelerated.

Resolution: To resolve this issue, perform the following troubleshooting steps:

– Verify that acceleration rules for IP address and port numbers are correctly defined for the WANOP plug-in.
– Verify that CIFS or ICA connections are established after signaling connection is successful.
– Verify the acceleration policy for the service class being used.

How-to-articles

December 14, 2018

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

Dec 14, 2018

To configure interface groups:

1. In the Configuration Editor, navigate to Sites > [Client Site Name] > Interface Groups, choose a Routing Domain from the drop-down menu when configuring Virtual Interfaces. For detailed instructions, see configuring interface groups.

Note

After Virtual Interfaces are associated with a specific Routing Domain, only those interfaces will be available when using that Routing Domain.
Configure Virtual IP Address Identity

December 14, 2018

To configure Virtual IP Address identity:

1. In the Configuration Editor, navigate to Sites > [Site Name] > Virtual IP Addresses.
2. Click the Identity checkbox for a Virtual IP Address to use it for IP services.

Configure access interface

January 3, 2019

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**

December 14, 2018

To configure Virtual IP Addresses:

1. In the **Configuration Editor**, navigate to **Sites > [Client Site Name] > Virtual IP Addresses**.
2. Choose a **Routing Domain** from the dropdown menu when configuring Virtual IP Addresses.

   For detailed instructions, see configuring Virtual IP addresses.

The Routing Domain you choose determines which Virtual Interfaces are available from the drop-down menu.

![Virtual IP Addresses](image)

**Configure GRE Tunnels**

December 14, 2018

To configure GRE Tunnels:

1. In the configuration editor, navigate to **Connections > Site > GRE Tunnels**. The source IP address can only be chosen from the Virtual network interface on trusted links.
2. Enter a name for the GRE Tunnel.
3. Select the **Source IP** address available from the drop-down menu. The Routing Domain determines which Source IP Addresses are available from the drop-down menu.
4. (Optional) Select the **Public Source IP**. This field can be empty if this address is the same as Source IP.
5. Enter the **Destination IP** address of the GRE Tunnel.
6. Enter the **Tunnel IP/Prefix** address of the GRE Tunnel.
7. Click **Checksum**, if you want to use checksum in the GRE Tunnel Header.

8. Enter a value for the **Keepalive Period** in seconds. If you configure 0, no keepalive packet are transmitted, but the GRE Tunnel will be active.

9. Enter a value for the **Keepalive Retries.** This value determines the number of times the keepalive retries are attempted before the SD-WAN appliance deactivates the GRE Tunnel.

Refer to the configuring GRE tunnels on the MCN site for more information.

For more information about securing web gateway using GRE tunnels, see; [Secure Web Gateway](#)

### Setup dynamic paths for branch to branch communication

December 18, 2018

With demand for VoIP and video conferencing, the traffic is increasingly moving between offices. It is inefficient to set up full mesh connections through datacenters which can be time consuming.

With 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.

Configure static WAN paths

December 14, 2018

With WAN to WAN enabled on the MCN, remote site routes are advertised by MCN.

- Clients are aware of MCN local routes as well as other client site routes
- From client perspective, all routes are considered as MCN routes

When WAN-to-WAN forwarding is not enabled on the MCN, Branch to Branch communication issues are encountered in the customer network.

Citrix SD-WAN appliances running in client mode are not aware of other branches subnets until WAN-to-WAN forwarding is enabled on MCN. Once this option is enabled, branch SD-WAN nodes become aware of other branch subnets and all the traffic destined to other branches is forwarded to MCN. MCN routes it to the correct destination.
Monitoring and Troubleshooting

December 14, 2018

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
Viewing Statistical Information
Viewing Flow Information
Viewing Reports
Viewing Firewall Statistics
Diagnostic Tool
Improved Path Mapping and Bandwidth
Troubleshooting Management IP
Monitoring Virtual WAN

December 14, 2018

Viewing Basic Information for an Appliance

Use a browser to connect to the Management Web Interface of the appliance you want to monitor, and click the **Dashboard** tab to display basic information for that appliance.

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

**System Status:**

- **Name** – This is the name you assigned to the appliance when you added it to the system.
- **Model** – This is the Virtual WAN appliance model number.
- **Appliance Mode** – This indicates whether this appliance has been configured as the primary or secondary MCN, or as a client appliance.
- **Management IP Address** – This is the Management IP Address for the appliance.
- **Appliance Uptime** – This specifies the duration for which the appliance has been running since the last reboot.
- **Service Uptime** – This specifies the duration for which the Virtual WAN Service has been running since the last restart.

**Virtual Path Service Status:**

**Virtual Path [site name]** – This displays the 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

December 14, 2018

This section provides basic instructions for viewing Virtual WAN statistics information.

1. Log into the Management Web Interface for the MCN.

2. Select the Monitoring tab.

   This opens the Monitoring navigation tree in the left pane. By default, this also displays the Statistics page with Paths preselected in the Show field. This contains a detailed table of path statistics.

   Note

   If you navigate to another Monitoring page (for example, Flows), you can return to this page by selecting Statistics in the Monitoring navigation tree (left pane).
3. Open the **Show** drop-down menu next to the **Show** field.

   In addition to the **Paths** statistics, the **Show** menu also offers several more options for filtering and viewing statistical information.

4. Select a filter from the **Show** menu to view a table of statistical information for that topic.

**Viewing Flow Information**

December 18, 2018

This section provides basic instructions for viewing Virtual WAN flow information.

To view flow information, do the following:

1. Log into the Management Web Interface for the MCN, and select the **Monitoring** tab. This opens the **Monitoring** navigation tree in the left pane.

2. Select the **Flows** branch in the navigation tree. This displays the **Flows** page with **LAN to WAN** preselected in the **Flow Type** field.
3. Select the **Flow Type**. The Flow Type field is located in the Select Flows section at the top of the Flows page. Next to the Flow Type field is a row of checkbox options for selecting the flow information you want to view. You can check one or more boxes to filter the information to be displayed.

4. Select the **Max Flows to Display** from the drop-down menu next to that field.

5. This 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. This filters the table results so that only entries containing the search text display in the table.

   **Tip**

   To see detailed instructions for using filters to refine Flow table results, click Help to the right of the Filter field. To close the help display, click Refresh in the bottom left corner of the Select Flows section.

7. Click Refresh to display the filter results. The below 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. This reveals any deselected columns, and opens a checkbox above each column for selecting or deselecting that column. Deselected columns display grayed out, as shown in the below figure.

**Note**

By default, all of the columns are selected, which can cause the table to be truncated in the display, obscuring the **Toggle Columns** button. If so, a horizontal scroll bar displays beneath the table. Slide the scroll bar to the right to view the truncated section of the table and reveal the **Toggle Columns** button. If the scroll bar is not available, try resizing the width of your browser window until the scroll bar is revealed.
### 10. Click a checkbox to select or deselect a column.

### 11. Click **Apply** (above the top right corner of the table). This dismisses the selection options, and refreshes the table to include only the selected columns.

#### Flow Data

<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Dest IP Address</th>
<th>Direction</th>
<th>Source Port</th>
<th>Dest Port</th>
<th>Hit Count</th>
<th>Service Type</th>
<th>Service Name</th>
<th>LAN/GW IP</th>
<th>Age (mS)</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.79.2.283</td>
<td>172.79.1.42</td>
<td>LAN to WAN</td>
<td>9281</td>
<td>5889</td>
<td>9615</td>
<td>Virtual Path</td>
<td>DC-BR</td>
<td>LOCAL</td>
<td>12022</td>
<td>12084</td>
<td>1024628</td>
</tr>
<tr>
<td>172.79.2.283</td>
<td>172.79.1.42</td>
<td>LAN to WAN</td>
<td>9281</td>
<td>58690</td>
<td>9667</td>
<td>Virtual Path</td>
<td>DC-BR</td>
<td>LOCAL</td>
<td>12050</td>
<td>12246</td>
<td>10860066</td>
</tr>
<tr>
<td>172.79.1.42</td>
<td>172.79.2.283</td>
<td>WAN to LAN</td>
<td>58609</td>
<td>9281</td>
<td>18092</td>
<td>Virtual Path</td>
<td>DC-BR</td>
<td>LOCAL</td>
<td>12040</td>
<td>12809</td>
<td>1299440</td>
</tr>
<tr>
<td>172.79.1.42</td>
<td>172.79.2.283</td>
<td>WAN to LAN</td>
<td>58690</td>
<td>9281</td>
<td>18312</td>
<td>Virtual Path</td>
<td>DC-BR</td>
<td>LOCAL</td>
<td>12056</td>
<td>18312</td>
<td>1384758</td>
</tr>
</tbody>
</table>
Viewing Reports

January 4, 2019

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 is more than 30 entries.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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.

**Viewing Firewall Statistics**

December 14, 2018

Once you have configured firewall and NAT policies, you can view the statistics of the connections, firewall policies and NAT policies as reports. You can filter the reports using the various filtering parameters.

For information on configuring firewall and NAT policies, see [Stateful Firewall and NAT Support](#).

**Connections**

You can check the statistics for Applications for the Firewall Policy. This enables you to see all connections that match to the selected Application, where they are coming from, where they are going to, and how much traffic they are generating. You can see how the firewall policies are acting on the traffic for each Application.

You can filter the connections statistics using the following parameters:

- Application - The application used as filter criteria for the connection.
- Family - The application family the used as filter criteria for the connection.
- IP Protocol - The IP protocol used by the connection.
• Source Zone - The zone from which the connection originated.
• Destination Zone - The zone from which responding traffic originates.
• Source Service Type - The service from which the connection originated.
• Source Service Instance - The instance of the service from which the connection originated.
• Source IP - The IP address from which the connection originated, input in dotted decimal notation with an optional subnet mask.
• Source Port - The port or range of ports from which the connection originated. A single port or a range of ports using the “-“ character is accepted.
• Destination Service Type - The service from which responding traffic originates.
• Destination Service Instance - The instance of the service from which responding traffic originates.
• Destination IP - The IP address of the responding device, input in dotted decimal notation with an optional subnet mask.
• Destination Port - The port or range of ports used by the responding device. A single port or a range of ports using the “-“ character is accepted.

Filter Policies

Policies enable you to specify actions for traffic flows. Group of firewall filters are created using Firewall Policy Templates and can be applied to all sites in the network or only to specific sites.

You can view statistics report for all the filter policies and filter it using the following parameters.

• Application object - The Application object used as a filter criteria in the firewall policy.
• Application - The application used as a filter criteria in the firewall policy.
• Family - The application family used as filter criteria in the firewall policy.
• IP Protocol - The IP protocol that the filter policy matches.
• DSCP: The DSCP tag that the filter policy matches.
• Filter Policy Action - The action taken by the policy when a packet matches the filter.
• Source Service Type - The service from which the connection originated.
• Source Service Name - The instance of the service from which the connection originated.
• Source IP - The IP address from which the connection originated, input in dotted decimal notation with an optional subnet mask.
• Source Port - The port or range of ports from which the connection originated. A single port or a range of ports using the “-“ character is accepted.
• Destination Service Type - The service to which responding traffic is destined.
• Destination Service Name - When applicable, the service to which responding traffic is destined.
• Destination IP - The IP address of the responding device, input in dotted decimal notation with an optional subnet mask.
• Destination Port - The port or range of ports used by the responding device. A single port or a range of ports using the “-“ character is accepted.
• Source Zone - The origination zone matched by the filter policy.
• Destination Zone - The responding zone matched by the filter policy.

**NAT Policies**

You can view the statistics of all the Network Address Translation (NAT) policies and filter the report using the following parameters.

• IP Protocol - The IP protocol that the NAT policy matches.
• NAT Type - The type of NAT in use by the NAT policy.
• Dynamic NAT Type - The type of Dynamic NAT in use by the NAT policy.
• Service Type - The service type used by the NAT policy.
• Service Name - The instance of the service used by the NAT policy.
• Inside IP - The inside IP address, input in dotted decimal notation with an optional subnet mask.
• Inside Port - The inside port range used by the NAT policy. A single port or a range of ports using the “-“ character is accepted.
• Outside IP - The outside IP address, input in dotted decimal notation with an optional subnet mask.
• Outside Port - The outside port range used by the NAT policy. A single port or a range of ports using the “-“ character is accepted.

To view Firewall Statistics:

1. Navigate to Monitoring > Firewall.
2. In the Statistics field select, Connections, Filter Policies, or NAT Policies as required.
3. Set the filtering criteria as required.
   
4. Click Refresh.
Diagnostic Tool

December 14, 2018

This diagnostic tool is used to generate test traffic which allows you to troubleshoot network issues that may result in:

- Frequent change in path state from Good to Bad.
- Poor application performance.
- Higher packet loss

Most often, these problems arise due to rate limiting configured on firewall / router, incorrect bandwidth settings, low link speed, priority queue set by network provider and so on. The diagnostic tool allows you to identify the root cause of such issues and troubleshoot it.

The diagnostic tool removes the dependency on third party tools such as iPerf which has to be manually installed on the Data Center and Branch hosts. It provides more control over the type of diagnostic traffic sent, the direction in which the diagnostic traffic flows, and the path on which the diagnostic traffic flows.

The diagnostic tool allows to generate the following two types of traffic:

- Control: Generates traffic with no QOS/scheduling applied to the packets. As a result, the packets are sent over the path selected in the UI, even if the path is not the best at the time. This traffic is used to test specific paths and helps to identify ISP related issues. You can also use this to determine the bandwidth of the selected path.
- Data: Simulates the traffic generated from the host with SD-WAN traffic processing. Since QoS/scheduling is applied to the packets, the packets are sent over the best path available 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 other appliance.

3. In the **Traffic Type** field, select the type of diagnostic traffic, either **Control** or **Data**. Select the same traffic type on both the appliances.

4. In the **Port** field, specify the **TCP / UDP** port number on which the diagnostic traffic 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.

6. Select the WAN to LAN paths on which you want to send the diagnostic traffic. Select the same path on both the appliances.

7. Click **Start** on both the appliances.

---

**Improved Path Mapping and Bandwidth Usage**

December 14, 2018
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**.

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.

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 when traffic is flowing, it can be noticed that two paths are shown to be processing the traffic. Unlike any other mode, even if traffic demands less bandwidth that can be provided by just one path, this mode will always duplicate traffic across two paths for reliable application delivery.

You 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.

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.

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.
Citrix SD-WAN 10.2

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.

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.

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.

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). This 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, this might affect clarity of data, particularly if we want to track/graph the usage of an application over time and the application falls out of the top 100 limit.

**Troubleshooting Management IP**

November 22, 2018

The following are the possible scenarios that you might encounter when configuring DHCP IP address. It also includes best practices and recommendations for configuring DHCP Management IP address when deploying SD-WAN appliances.

These recommendations are applicable to all platform models of SD-WAN; Standard Edition, WANOP, and Enterprise Edition - Physical and Virtual appliances.

*Note*

All hardware models of SD-WAN appliances are shipped with a factory default management IP address. Ensure that you configure the required DHCP IP address for the appliance during the setup process.

All Virtual models of SD-WAN appliances (VPX models) and appliances which can be deployed in AWS environment do not have a factory default IP address assigned.

**Appliances power on without DHCP 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**

December 14, 2018

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**.
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
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 up-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:
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**

November 22, 2018

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**

November 22, 2018

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

November 22, 2018

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.

• 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

December 14, 2018

High availability

What is the difference between High Availability and Secondary (Geo) appliance?

- High Availability ensures fault tolerance. Secondary (Geo) appliance enables disaster recovery.
- High Availability can be configured for the MCN, RCN, and branch appliances. Secondary (Geo) appliance can be configured for MCN and RCNs only.
• High Availability appliances are configured within the same site or geographical location. A branch appliance in a different geographical location is configured as Secondary (Geo) MCN/RCN appliance.
• High Availability primary and secondary appliance should be the same platform models. The Secondary (Geo) appliance might or might not be the same platform model as the primary MCN/RCN.
• High Availability has higher priority over secondary (Geo). If an appliance (MCN/RCN) is configured with High Availability and Secondary (Geo) appliance, when the appliance fails the secondary high availability appliance becomes active. If both the high availability appliances fail or if the Data Center site crashes, the secondary (Geo) appliance becomes active.
• In High Availability, the primary/secondary switchover happens instantaneously or within 10-12 seconds depending upon the high availability deployment. The primary MCN/RCN to secondary (Geo) MCN/RCN switch over, happens after 15 seconds of the primary being inactive.
• High Availability configuration allows you to configure primary reclaim. You cannot configure primary reclaim for Secondary (Geo) appliance, the primary reclaim happens automatically after the primary appliance is back and the hold timer expires.

Single step upgrade

Note

The WANOP, SVM, and XenServer Supplemental/HFs are seen as OS Components.

Should I use .tar.gz, or single step upgrade .zip package to upgrade to 9.3.x from my current version (8.1.x, 9.1.x, 9.2.x)?

Use the .tar.gz files of the concerned platforms to upgrade the SD-WAN software to 9.3.x. After the SD-WAN software is upgraded to 9.3.x version, perform change management using the .zip package to transfer/stage OS component software packages. After activation, the MCN transfers/stages OS components for all the relevant branches.

After upgrading to 9.3.0 using single step upgrade package (.zip file) do, I need to perform .upg upgrade on each appliance?

No, OS software update/upgrade will be taken care by the single step upgrade .zip package and it is installed as per the scheduling details provided by you in the Change Management Settings of the respective sites.

Why should I use .tar.gz followed by .zip package to upgrade from earlier than 9.3 to 9.3.x, and why not directly use .zip package of 9.3.x?

Single Step upgrade package is supported from 9.3.0.161 onwards and on earlier release versions (prior to release 9.3) this package is not recognized. When the single step upgrade .zip package is uploaded into the Change Management inbox, the system throws an error stating that the package is
not recognized. Hence, first upgrade the SD-WAN software to 9.3 or above version and then perform Change Management using the .zip package.

**How will the OS Components be installed through single step upgrade, if `upg` upgrade is not performed?**

The MCN will transfer/stage OS components software packages based on the appliance model, after the Change Management is completed using single step upgrade .zip package. After activation, the MCN starts transferring/staging the OS components software packages for the branches that need them for the scheduled update/upgrade.

**How do I install OS components, without scheduling for later installations?**

Set the **Maintenance Window** value to ‘0’ for instant installation of the OS components.

*Note*

The installation starts only when the appliance has received all the package that 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.
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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
How does my branch site behind the RCN obtain OS component packages if RCN is a VPX appliance, and branch is an appliance that needs these packages?

RCN stages the relevant package to the branch that needs the OS component packages after activation of SD-WAN VW software package.

Can I choose Ignore Incomplete during staging and proceed to next stage of change Management? What impact does it have for sites that have not completed staging when this button is selected?

Yes, you can click Ignore Incomplete. This enables Next button and the Progress bar is displayed. This option is provided for scenarios where the site is not reachable and change management is still waiting for staging to complete for those site, so users can proceed to next stage by ignoring the stage state and proceed to activation. After the site comes up, MCN stages the package after completion of activation.

Partial software upgrade

What is partial site upgrade and how can I use it?

Partial site software upgrade is a new feature introduced in release 10.0. You can stage newer version of release 10.x from the MCN and activate staged software version from Local Change Management page on selected sites/branches. Before activating staged software on site/branch, ensure that check box is enabled from MCN.

• This feature is disabled by default. The existing correction mechanism keeps the network in sync. The user has to choose to allow partial site upgrades by enabling a check box on the “Configuration -> Change Management Settings” page.
• Partial Software Upgrade can be done only on a Branch or RCNs and not at the MCN.

Below is the usecase/scenario when partial site software upgrade can be used:

Validate if a software patch with relevant changes is compatible and working for a specific site (where partial site upgrade is done). Validate that the upgraded software is working as expected. This helps validate the new software and fix at a specific site before upgrading entire network with the new software.

Can I use this feature to upgrade from:

• 10.0 to 10.x
• 10.0.x to 10.0.y
• 10.x to 11.y
• All of the above

Partial Site Software Upgrade is applicable only when appliance is running software release 10.x and newer, and can be used within the same major version of software. It can be used between releases
10.0 to 10.0.x/10.x. Only as part of partial site software upgrade, configuration cannot be changed. This feature is good when active software version is 10.x.y, and Staged software version is 11.x or higher as long as there is no change in the control protocol.

**Can I test new feature to test as part of partial software upgrade by enabling them from the config?**

No, partial software upgrade requires that now Active and Staged config to be identical. Only software version can change.

**Can I disable Partial Software Upgrade for RCN?**

No, Partial Software Upgrade can be enabled or disabled from MCN only. At RCN the feature is in read-only mode.

**Can I use Partial Software Upgrade when I have active as 9.3.x and 10.0.x as staged?**

No, the appliance should be running on release 10.0 as active software.

**What happens when Partial Software Upgrade option is disabled from MCN, while some branches are already upgraded through this feature?**

MCN sends notification to all appliances in the network that Partial Software Upgrade feature is disabled, and then all appliances in the network are auto-corrected by MCN to match to its active and staged version. However, note that MCN is expecting for Activate Staged option to be clicked from Activation page of Change Management. You can choose to activate the network by clicking **Activate Staged** button or click **Change Preparation** to cancel state by accepting the confirmation.

**Change Management Roll Back**

**What is rolled back feature in Change management process?**

From release 9.3, the Change management 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 10 min interval.
2. MCN - After config/software change, if Virtual Path service is down for 10 minutes or longer after activation. The Rollback feature is initiated at the sites.
3. Site - After config/software change, if the Site loses its communication with MCN, then the rollback feature is initiated.
4. Site - After config/software change t2_app service gets disabled due to crash within 10 min interval.

What happens after rollback?

After configuration rollback, the faulty config/software is presented as Staged software.

How are users notified that rollback 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 rollback 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 rollback interact with Partial Software Upgrade when I have multi-tier network?

- If partial software upgrade is disabled, and if a site in a region (or the RCN) rolls back, the region with the problem is rolled back and once completed the rollback propagates up to the MCN. As a result, the MCN and the rest of the network to rolled back. Both the RCN in the region that rolled back, and the MCN display the rollback banner that the MCN cannot auto-dismiss the rollback banner at the RCN.
- If partial software upgrade is enabled, and if a site in a region (or the RCN) rolls back, only that region is rolled back. The rollback event does not propagate back to the MCN. As a result, the MCN leaves the region. The MCN does not show rollback banner and does not roll back itself or the network.

In both these scenarios, the RCN displays the rollback banner until it is dismissed. Because, it cannot be auto-dismissed by MCN.

2100 Enterprise Edition

What does the following message indicate when a 2100 EE appliance is upgraded to release 10.0?
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**

December 14, 2018

**Application Signature Library**

A list of applications that the Citrix SD-WAN appliances can identify using Deep Packet Inspection.