# net>scaler.

## **Citrix SD-WAN 11.5**

## Contents

New user interface for SD-WAN appliances	9
Citrix SD-WAN 11.5 release upgrade impact	41
System requirements	42
SD-WAN platform models	43
Upgrade paths	44
Configuration	46
Configure LTE functionality on 210 SE LTE appliance	75
Configure LTE functionality on 110-LTE-WiFi appliance	86
Configure external USB LTE modem	96
Deployments	100
Checklist and how to deploy	101
Best practices	102
Gateway mode	108
Inline mode	116
Virtual inline mode	117
Build an SD-WAN network	118
High availability	119
Enable Edge Mode High Availability Using Fiber Optic Y-Cable	125
Zero touch	127
AWS	132
Azure	133
Single-region deployment	134

1

Multi-region deployment	134
Configuration guide for Citrix Virtual Apps and Desktops workloads	136
Domain name system	149
DHCP	151
Dynamic PAC file customization	155
GRE tunnel	158
In-band and backup management	158
Internet access	163
Hosted firewalls	168
Link Aggregation Groups	175
Link state propagation	178
Metering and Standby WAN Links	179
Office 365 optimization	187
Citrix Cloud and Gateway service optimization	196
PPPoE Sessions	201
Quality of service	205
Reporting	226
Routing	234
SD-WAN Overlay Routing	235
Routing Domain	254
Configure Routing Domain	255
Use CLI to Access Routing	255
Dynamic Routing	256
OSPF	259

BGP	266
iBGP	268
eBGP	269
Application Route	269
Route filtering	272
Route Summarization	272
Protocol preference	274
Multicast routing	274
Configure Virtual Path Route Cost	277
Configure Virtual Router Redundancy Protocol	279
Routing Support for LAN Segmentation	283
Inter-routing domain service	284
ECMP load balancing	285
Security	286
IPSec Tunnel Termination	287
Citrix SD-WAN integration with AWS Transit Gateway	287
How to view ipsec tunnel configuration	293
IPSec monitoring and logging	296
Eligibility for ipsec non-virtual path routes	299
FIPS Compliance	300
Citrix SD-WAN secure web gateway	300
Zscaler Integration by using GRE tunnels and IPsec tunnels	301
Firewall Traffic Redirection Support by Using Forcepoint in Citrix SD-WAN	306
Palo Alto integration using IPsec tunnels	308

Stateful Firewall and NAT Support	309
Global firewall settings	309
Advanced firewall settings	310
Zones	310
Policies	312
Network Address Translation (NAT)	312
Static NAT	312
Dynamic NAT	318
Configure Virtual WAN Service	323
Configure firewall segmentation	323
Certificate authentication	327
AppFlow and IPFIX	327
SNMP	337
Administrative interface	341
NDP router advertisement and prefix delegation group	346
How-to-articles	347
Configure access interface	348
Configure Virtual IP addresses	348
Configure GRE Tunnels	348
Setup dynamic paths for branch to branch communication	348
WAN-to-WAN forwarding	350
Monitoring and Troubleshooting	351
Monitoring Virtual WAN	351
Viewing Statistical Information	352

Viewing Flow Information	355
Viewing Reports	359
Viewing Firewall Statistics	365
Diagnostics	368
Improved Path Mapping and Bandwidth Usage	385
Troubleshooting Management IP	391
Session-based HTTP Notifications	392
Active bandwidth testing	398
Adaptive bandwidth detection	400
Best practices	401
Security	402
Routing	408
QoS	409
WAN Links	409
FAQs	411
Reference material	419

## **Release Notes for Citrix SD-WAN 11.5 Release**

## August 24, 2022

This release notes document describes the enhancements and changes, fixed and known issues that exist for Citrix SD-WAN 11.5.

## Notes

This release notes document does not include security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin.

## What's New

The enhancements and changes that are available in SD-WAN 11.5 release.

## Miscellaneous

## Citrix SD-WAN 11.5 release specifications

- Citrix SD-WAN 11.5.0 is a Limited Availability release, recommended and supported only for specific customers/production deployments.
- SD-WAN 11.5.0 release does not support Advanced Edition (AE), Premium Edition (PE), WAN Optimization deployments.
- SD-WAN 11.5.0 supports only the platforms mentioned in SD-WAN platform models and software packages.
- SD-WAN 11.5.0 does not support Citrix SD-WAN Center or Citrix SD-WAN Orchestrator for onpremises.
- SD-WAN 11.5.0 firmware is not available on the Citrix Downloads page.
- SD-WAN 11.5.0 release is available only via Citrix SD-WAN Orchestrator service and only on selected geographical POPs.
- Ensure to get the required approvals and guidance from Citrix Product Management / Citrix Support before deploying 11.5.0 on any production network.

[NSSDW-38486]

## Citrix SD-WAN Orchestrator service replaces SD-WAN Configuration Editor:

From Citrix SD-WAN 11.5 release, SD-WAN Configuration Editor and SD-WAN Center are superseded by Citrix SD-WAN Orchestrator service. Citrix SD-WAN Orchestrator service supports all configurations that are currently done through SD-WAN Configuration Editor. For more details on Citrix SD-WAN Orchestrator service, see Citrix SD-WAN Orchestrator service.

[NSSDW-33528]

## IPv6 support:

From Citrix SD-WAN 11.5.0 release onwards, the following data plane features of Citrix SD-WAN appliances support IPv6 address:

- Application Routes
- Citrix Cloud and Gateway service optimization
- Domain name based application classification
- Dynamic PAC file customization
- Dynamic Routing
- Firewall Defaults
- Multicast
- Office 365 Optimization
- PPPoE
- Site Reports Routing Protocols
- VRRP

After configuring the above-listed features, if you disable IPv4 or IPv6 protocol, then the features do not work as expected.

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

## Monitoring enhancements:

The following Monitoring dashboards are enhanced and are available on the new appliance UI:

- DNS transparent forwarder
- Firewall connections, Firewall filter, Firewall NAT
- IGMP, IGMP proxy, IGMP statistics
- IKE, IPsec
- Multicast group, Multicast group source, Multicast group destination
- PPPoE sessions

• VRRP

[NSSDW-33763]

## **Platform and systems**

Reference material - application signature library The DPI application signature library has been updated. [NSSDW-38209]

## **Fixed Issues**

The issues that are addressed in SD-WAN 11.5 release.

## Miscellaneous

The management interface status of some SD-WAN appliances was displayed as Down on the **Ether-net Interface Settings** page of the UI. This issue occurred when some appliances that had in-band management supported, the option to use out of band was available. Therefore, the appliances used out of band management interface to access SD-WAN Orchestrator service.

[NSSDW-37028]

## **Known Issues**

The issues that exist in SD-WAN 11.5 release.

In case of scaled deployment on configuration change on any site or WAN link, the routing engine restart causes BGP sessions to flap.

## [SDWANHELP-2594]

An SD-WAN appliance crashed unexpectedly. This issue occurred when:

- IPv6 multicast traffic was flowing during a software upgrade.
- IPv6 Multicast traffic was sourced using an Intranet GRE Tunnel and was replicated to multiple branches over the virtual path using MLDv2 proxy configuration.

**Workaround**: Disable IPv6 Multicast traffic during the software upgrade and enable once the upgrade is successful.

[NSSDW-38495]

## New user interface for SD-WAN appliances

## August 24, 2022

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

From Citrix SD-WAN 11.4 release onwards, the New UI is enabled, by default, on all the Citrix SD-WAN appliances that are configured as clients.

Note

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

Change Password	
Current Password	
••••••	
New Password	
••••••	
Confirm New Password	
••••••	
Change Password	

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

new UI.

## **Citrix SD-WAN new user interface**

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

NOTE

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

To access the new UI page, perform the following:

Open a new browser tab and navigate to https: // < management-ip > to access the new UI on the SD-WAN appliance. If you are accessing an IPv6 address, enter https://<[IPv6 address]>.

Example: https://[fd73:xxxx:yyyy:26::9]

Note

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

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

The Citrix SD-WAN user interface page appears.

Username *	
admin	•
Password *	
•••••	
	Sign In

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

≡ Citrix SD-WA	N				
Dashboard		Dashboard			
Basic Settings        Advanced Settings        Monitoring        ARP Statistics        Route Statistics        Ethernet Statistics        Ethernet MAC Learning        DHCP Client WAN Links        DHCP Server/Relay        Firewall Connections		<ul> <li>Site Info</li> <li>Management IP Address</li> <li>10.102.78.57</li> <li>Management IPv6 Address</li> <li>fd73:2039:5849:26::11</li> <li>Site Name</li> <li>BRANCH_1</li> </ul>	Model / Sub Model Name VPX BASE Serial Number 010de 793-c09f-5b42-17be-63cde091502d		
Flows	<				
Diagnostics System Maintenance	<	Version Software Version 11.3.1.18.888881 Hardware Version VPX	Description of the second sec		

## Navigation

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

Dashboard	
Basic Settings	<
Advanced Settings	<
Monitoring	<
Diagnostics	<
System Maintenance	<

## Menu bar

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



## Dashboard

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

- Site Displays the site information with Management IP Address and Site Name
- Model Displays the Model/Sub Model Name and Serial Number
- Version Displays Software and Hardware version
- Uptime Displays Appliance Uptime, Citrix Virtual WAN Service Status and Orchestrator Connectivity Status.
- **High Availability** Displays the local and peer appliance HA status and the last HA update received time.
- Metered Links Displays the usage and billing details for links on which metering is enabled.
- **Orchestrator Connectivity** Displays the appliance connectivity status with Citrix SD-WAN Orchestrator service. The following Status Information is displayed:
  - Online State- Indicates the connection status between the appliance and Citrix SD-WAN Orchestrator service. Periodic heartbeat signals are sent by the appliance to Citrix SD-WAN Orchestrator service to identify the connection state as Good or Bad.
  - Service State- Indicates the https reachability of the appliance to all the required SD-WAN Orchestrator services such as download, home, logging, stats. If the service state is bad, it means that the connection is established but all or some of the services are not reachable. The unreachable service name is displayed.
  - DNS State- Indicates the FQDNs DNS resolution status. If the DNS state is bad, it means that the DNS resolution of one of the FQDNs is failing. The unresolved FQDN's name is displayed.
  - Local Gateway State- Indicates the default gateway status. For an Out-Of-Band connection, the gateway state is determined by pinging the default gateway. For an In-Band connection, the gateway state is determined by pinging the in-band Ethernet interface IP address.
  - **Connected Through** Indicates how the appliance reaches Citrix SD-WAN Orchestrator service. Either through Out-Of-Band, which is the default configuration or through In-Band, if In-band management is configured.
  - Failed Reason: Reason for failure while connecting to SD-WAN Orchestrator service.

Dashboard	
<ul> <li>Site Info</li> <li>Management IP Address</li> <li>10.102.203.219</li> <li>Site Name</li> <li>Spain_Branch1</li> </ul>	Model Model Name VPX BASE Serial Number feef8a22-6579-a3ea-3be3-c717ee04c
E Version	Appliance Uptime
Software Version 11.4.2.36.888881	ds Citrix Virtual WAN Service Status
C Orchestrator Connectivity	
Online State GOOD Service State GOOD	
DNS State GOOD	
Failed Reason N/A Connected Through Out-Of-Band	

## **Basic settings**

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

• Management and DNS

- Interface Settings
- LACP LAG Group
- Date and Time
- RADIUS Server
- TACACS+ Server

## **Management and DNS**

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

The management interface allow list is an approved list of IP addresses or IP domains that have permission to access your management interface. An empty list allows Management Interface to be accessed from all networks. You can add IP addresses to ensure that the management IP address is accessible only by the trusted networks.

To add or remove an IPv4 address to the allowed list, you must access the SD-WAN appliance management interface using an IPv4 address only. Similarly, to add or remove an IPv6 address to the allowed list, you must access the SD-WAN appliance management interface using an IPv6 address only

Managaranti	rfood ID		
Management Inte	erface IP		
Enable IPv4			
IP Address			
Subnet Mask			
255.255.255.0			
Gateway IP Address			
Enable IPv6			
To enable Statele box.	ess DHCP, selec	t both SLAAC an	d DHCP check
Enable SLAAC	Enable DH	HCP	
IPv6 Address			Prefix
IPv6 address			Prefix
DNS Settings			
Primary DNS			
Secondary DNS			
Clear			
Current DNS			
Primary DNS			
Secondary DNS			
Management Inte	erface Whitel	ist	
An empty whitelis	st allows Mana; s.	gement Interface	to be accessed
	be added/remo	oved only from a \	V4 network.
V4 networks can		oved only from a V	√6 network.
V4 networks can V6 networks can	be added/remo		
V4 networks can V6 networks can + IP Address	be added/remo /Prefix		
V4 networks can V6 networks can + IP Address	be added/remo		Ē

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

## **Interface settings**

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



## Ethernet Interface Settings

## LACP LAG group

The Link Aggregation Groups (LAG) functionality allows you to group two or more ports on your SD-WAN appliance to work together as a single port. This ensures increased availability, link redundancy, and enhanced performance.

Earlier, only the Active-Backup mode was supported in LAG. From Citrix SD-WAN 11.3 release onwards, the 802.3AD Link Aggregation Control Protocol (LACP) protocol based negotiations are supported. The LACP is a standard protocol and provides more functionality for LAGs.

In Active-Backup mode, at any time only one port is active and the other ports are in backup mode. The active and backup supports rely on the Data Plane Development Kit (DPDK) package for LAG functionality.

With the LACP, you can send the traffic through all the ports simultaneously. As a benefit, you get more bandwidth along with the link redundancy mechanism. The LACP implementation supports the Active-Active mode. Now with the Active-Backup mode, you also can select full LACP Active-Active mode from the SD-WAN UI.

The LAG functionality is available only on the following DPDK supported platforms:

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 2100 SE/PE
- Citrix SD-WAN 4100, and 5100 SE
- Citrix SD-WAN 6100 SE

## Note

The LAG functionality is not supported on VPX/VPXL platforms.

You can create a maximum of 4 LAGs with a maximum of 4 ports grouped in each LAG on the Citrix SD-WAN appliances.

For the Citrix SD-WAN 210 and 410 appliances, a maximum of 3 LAGs and for the Citrix SD-WAN 110 appliance, a maximum of 2 LAGs can be created.

You can create LAG using the Legacy UI or SD-WAN Orchestrator only. In the New UI, you can only view the details of the created LAG.

To view LAG details navigate to **Basic Settings** > **LACP LAG Group**.

You can view LACP LAG details such as the current state, system, and port priority details of active and partner ports.

Dashboard	L	ACP LAG							
Management & DNS	~				LAGO				
Interface Settings		NAME	SELECTION	STATE	SYSTEM PRIORI	PORT PRIORITY	PARTNER STATE	PARTNER SYST	PARTNER PORT
LACP LAG Group Date & Time		1/1	Selected	ACT AGG SY	65535	65280	AGG SYNC C	128	128
RADIUS Server		1/4	Selected	ACT AGG SY	65535	65280	AGG SYNC C	128	128
NOA00 Server									
Advanced Settings	<								
Monitoring	<								
Diagnostics	<				LAG1				
System Maintenance	<	NAME	SELECTION	STATE	SYSTEM PRIORI	PORT PRIORITY	PARTNER STATE	PARTNER SYST	PARTNER PORT
		1/7	N/A	Inactive	N/A	N/A	N/A	N/A	N/A
		1/8	N/A	Inactive	N/A	N/A	N/A	N/A	N/A

## **Date and Time**

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

vate/Time Settings
If the Appliance date/time is turned back due to NTP or manual changes, reporting artifacts may occur.
NTP Settings
Use NTP Server
Server Address
africa.pool.ntp.org
Save
Date/Time Settings
Date/Time
February 2, 2021 7:10 AM
Save
Timezone Settings
After changing the timezone setting, a reboot will be necessary for the timezone changes to take full effect.
Until then, some logs will continue to use the actual timezone setting in effect at the time of the last reboot, even though events timestamps may reflect the new setting.
Timezone
Africa/Porto-Novo
Save

## **RADIUS Server**

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

To configure the RADIUS server:

- 1. Select the **Enable RADIUS** check box.
- 2. Enter the **Server IP Address** and **Authentication Port**. A maximum of three server IP addresses can be configured.

NOTE

To configure an IPv6 address, ensure that the RADIUS server is also configured with an IPv6 address.

- 3. Enter the Server Key and confirm.
- 4. Enter the **Timeout** value in seconds.
- 5. Click Save.

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

Settings	
Enable RADIUS	
Server 1 IP Address *	Authentication Port
	1812
Server 2 IP Address	Authentication Port
Server 3 IP Address	Authentication Port
Server Key	
Confirm Server Key	
Timeout(seconds)	
30	
Save	
Test RADII IS Server Connection	
User Name	
Password	

## **TACACS+ Server**

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

To configure the TACACS+ server:

- 1. Select the **Enable TACACS+** check box.
- 2. Enter the **Server IP Address** and **Authentication Port**. A maximum of three server IP addresses can be configured.

## NOTE

To configure an IPv6 address, ensure that the TACACS+ server is also configured with an IPv6 address.

- 3. Select **PAP** or **ASCII** as the Authentication Type.
  - PAP: Uses Password Authentication Protocol (PAP) to strengthen user authentication by assigning a strong shared secret to the TACACS+ server.
  - ASCII: Uses ASCII character set to strengthen user authentication by assigning a strong shared secret to the TACACS+ server.
- 4. Enter the **Server Key** and confirm.
- 5. Enter the **Timeout** value in seconds.
- 6. Click **Save**.

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

Settings		
] Enable TACACS+		
ierver 1 IP Address*	4	Authentication Port
		49
erver 2 IP Address	4	Authentication Port
erver 3 IP Address	4	Authentication Port
uthentication Type O PAP O ASCII		
••••••		
onfirm Server Key		
imeout(seconds)		
30		
Save		
est TACACS+ Server Connection		
ser Name		
assword		

## **Advanced settings**

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

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

On-prem Orchestrator

## **Citrix Virtual WAN service**

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

Enable Citrix Virtual WAN Service			
The Citrix Virtual V	VAN Service is currently enabled		
Disable	Perform a diagnostic dump before doing the disable operation		
Disable	Perform a diagnostic dump before doing the disable operation		

## **High Availability**

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

witch HA Mode		
Switch to Standby		

## **Mobile broadband**

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

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

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

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

• Configure LTE functionality on 210 SE LTE appliance

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

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

## Note

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

## Perquisites for external LTE modem:

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

## Note

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

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

Nobile Broadband Status		
Modem Type	Status Of	
Internal Modem 🗸 🗸	Device	~
Status		
Active SIM		SIM Two
Data Service Capability		non-simultaneous-cs-ps
ESN		0
Expected Data Format		802-3
Hardware Revision		10000
IMEI		867698040400825
MEID		86769804040082
MSISDN		
Manufacturer		QUALCOMM INCORPORATED
Max RX Channel Rate (bps)		10000000
Max TX Channel Rate (bps)		5000000
Model		QUECTEL Mobile Broadband Module
Modem Mode		QMI
Networks		gsm umts Ite
Operating Mode		online
Operating Mode HW Restricted		0
PRL Only Preference		0
PRL Version		0
Revision		EG25GGBR07A07M2G
SIM Capability		supported
Software Version		EG25GGBR07A07M2G
Туре		110-WIFI-LTE

The following are some useful status information:

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

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

Device details for CDC Ethernet external modem.

Modem Type Status 0f External Modem
External Modern V Device V
Status
Product ID 14db
Vendor ID 12d1
Manufacturer HUAWEI_MOBILE
Product HUAWEI_MOBILE

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

Nobile Broadband Status		
Modem Type	Status Of	
External Modem	✓ Device	
Status		
Active SIM		SIM One
Data Service Capability		none
ESN		
Expected Data Format		unknown
Hardware Revision		
IMEI		866785032748294
MEID		
MSISDN		
Manufacturer		
Max RX Channel Rate (bps)		15000000
Max TX Channel Rate (bps)		15000000
Model		CL2E3372HM
Modem Mode		MBIM
Networks		gprs, edge, umts, hsdpa, hsupa, ite, custom
Operating Mode		online
Operating Mode HW Restricted		0
PRL Only Preference		0
PRL Version		0
Revision		
SIM Capability		not-supported
Software Version		
Product ID		157c
Vendor ID		12d1
Manufacturer		HUAWEI_MOBILE
Product		HUAWEI_MOBILE

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

dem Type		Status Of	
External Modem	~	SIM One	, second s
Status			
APN			airtelgprs.com
APN Autodetect			Searching
Application State			unknown
Application Type			unknown
Authentication			None
Card State			present
Connection Status			connected
Home Network			Airtel
CCID			8991000904312026839
MSI			404450994643179
Address			100.108.16.42
Sateway			100.108.16.41
VITU			1500
Netmask			255.255.255.252
Primary DNS			125.22.47.102
Secondary DNS			59.144.144.106
Data Session			Not Available
Enabled			
исс			404
MNC			45
PIN Retries			0
PIN State			disabled
PUK Retries			0
Radio Interface			Ite
Roaming Status			off
Signal Strength			Excellent

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

Internal modem	External modem - CDC Ethernet	External modem - MBIM and NCM
Yes - For appliances that support dual SIM	No	No
Yes	No	No
Yes	No	Yes
Yes	No	No
Yes	No	No
Yes	No	No
	Internal modem Yes - For appliances that support dual SIM Yes Yes Yes Yes Yes	External modem - CDCInternal modemEthernetYes - For appliances that support dual SIMNoYesNoYesNoYesNoYesNoYesNoYesNoYesNoYesNoYesNoYesNoYesNoYesNoYesNo

Operations	Internal modem	External modem - CDC Ethernet	External modem - MBIM and NCM
Enable/Disable modem	Yes	No	Yes
Reboot modem	Yes	No	No
Refresh SIM	Yes	No	No

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

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

## Note

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

SIM Preference	
Preferred SIM	
SIM One Preferred	~
Apply	

## SIM PIN

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

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

SIM PIN Status (SIM Two)						
PIN State	disabled					
PIN Retries Remaining	3					
PUK Retries Remaining	10					
Enable	Verify	Modify	Unblock			

You can perform the following operations:

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

Note

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

## **APN settings**

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

Note

Obtain the APN information from the carrier.

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

## Note

All these fields are optional.

## 3. Click Apply.

APN Settings	
SIM	
SIM One 🗸	
APN	Authentication
internet	None ~
Username	Password
Apply	

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

Network Settings	
SIM	
SIM One	~
Network Mode	
Both	~
Apply	

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

Roaming	
SIM	
SIM One	~
Roaming Status	
Enabled	~
Apply	

## **Manage Firmware**

Every LTE enabled appliance has a set of firmware available. You can select from the existing list of firmware or upload a firmware and apply it. If you are unsure of which firmware to use, select

the **AUTO-SIM** option. The AUTO-SIM option allows the LTE modem to choose the most matching firmware based on the inserted SIM card.

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



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



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

#### Note

The Refresh SIM operation is applicable for the active SIM only.

SIM Card (SIM Two)

Refresh SIM

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

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

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

## Licensing

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

icensing	
Status	
State	Licensed
License Server Location	Local
Local License Server Host ID	8a94095ff8c1
Model	V50VW
Maximum Bandwidth (MAXBW)	50 Mbps
License Type	Retail
Maintenance Expiration Date	Wed Dec 1 00:00:00 2021
License Expiration Date	Thu Dec 2 00:00:00 2021

## Note

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

## Default/Fallback configuration

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

≡ Citrix SD-WAI	N 110-100	D-SE					Ģ
Dashboard		'Day 0' Defau	ult / 'Day N' Fall	back Config			
Basic Settings	<	The fallback configuration provides basic network functionality when a critical failure occurs and the system can no longer function.					
Advanced Settings Citrix Virtual WAN Service	~	Enable Fallback Configuration Reset					
High Availability Mobile Broadband	<	LAN Settings					
Licensing		VLAN ID		IP Address			
HTTPS Certificate		0		192.168.101.1	1/24		
On-prem Orchestrator	<	Enable DHCP Server					
Monitoring	<	DHCP Start		DHCP End			
Diagnostics	1	192.168.10	01.50	192.168.101.2	250		
Custom Maintenance		Dynamic	DNS Servers				
System Maintenance	<	DNS Server		Alt DNS Server			
		Internet A	Access				
		Port Setting	gs				
		Port	Mo	ode			
		1/4-MGMT O WAN LAN O Disabled					
		1/1 OWAN OLAN Disabled					
		1/2 • WAN CLAN Disabled					
		1/3 • WAN LAN Disabled					
		LTE-1 • WAN O LAN O Disabled					
		LTE-E1 O WAN LAN Disabled					
		Unassigned Por	t Bypass Mode				
		Fail to Block					
		WAN Settin	gs				
		Port	DHCP Mode	IP Address	Gateway IP Address	s Vlan ID	WAN Tracking IP
		1/2	Enable DHCP	12.12.12.10/24	12.12.12.1	0	9.9.9.9
		1/3	C Enable			0	9.9.9.9
		175.1	DHCP				
		LIE-I	DHCP			0	9.9.9.9
		LTE-E1	Enable DHCP			0	9.9.9.9

## Note

LTE interfaces cannot be configured with static IP address.

For more information see, Default/Fallback configuration.

## **HTTPS certificate**

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

HTTPS Certificate					
Installed Certificate					
Issuer			Issued To		
Country:	US		Country:	US	
State/Province:	California		State/Province:	California	
Locality:	San Jose		Locality:	San Jose	
Organization:	Citrix Systems, Inc.		Organization:	Citrix Systems, Inc.	
Organizational Unit	Engineering		Organizational Unit:	Engineering	
Common Name	Citrix		Common Name:	Citrix	
Email:	support@citrix.com		Email:	support@citrix.com	
Certificate Details					
Certificate Fingerprint:		25:B0:95:45:87	A3:95:F7:8F:29:D9:E0:9F:90:09:	0B:0C:0E:84:44	
Start Date:		Oct 1 04:01:14 20	019 GMT		
End Date:		Sep 28 04:01:14	2029 GMT		
Serial Number:		8B4D85214DDA	ACF9B		
Upload Certificate Upload the certificate that secures the Management HTTPS connection to this Virtual WAN appliance. Uploading and installing the HTTPS Certificate will cause the HTTP server to restart, invalidating all connected sessions. NDTE: For best results: when the operation is complete close the browser window and reconnect to the appliance. Upload Certificate Upload Certificate Click to select or drag n drop file here. Allowed file types are .crt Upload Key Click to select or drag n drop file here. Allowed file types are .key Upload file types are .key					
Regenerate Certificate Regenerate the certificate that secures the Management HTTPS connection to this Virtual WAN appliance. Regenerating the HTTPS Certificate will cause the HTTP server to restart, invalidating all connected sessions. NOTE: For best results: when the operation is complete close the browser window and reconnect to the appliance.					
Regenerate Certificate					

## **On-prem Orchestrator**

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

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

Note

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

#### To enable Orchestrator connectivity:

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

n-Pr	em SD-WAN Orchestrator Identity
	Note: This section is applicable only to On-prem SD-WAN Orchestrator managed networks, and not Cloud Orchestrator or SD-WAN Center managed networks. This is to enable appliances to join an On-prem SD-WAN Orchestrator managed network, in cases where the connectivity options at the appliance end do not allow for automated zero touch provisioning. Configure the On-Prem SD-WAN Orchestrator identity by providing a valial IP address and clicking "Apply" to enable your appliance connect to the On-Prem SD-WAN Orchestrator.
	<sup>1</sup> Enable On-Prem SD-WAN Orchestrator connectivity Advanced Configuration
or	- yorem 52-WAN Orchestrator (P 10.102-78.62
Or	r prem 52-WMA Orchestrator Domain
	saviariz.citrixnetworkapi.net Apply

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

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

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

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

In case of advanced configuration:

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

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

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

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

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

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

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

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

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

Note

- Generated certificates are X509 self-signed certificates.
- Customer must regenerate the certificates if the certificate is expired or compromised.
- Validity of the certificate is 10 years.
- You can view the certificate details such as, fingerprint, start date, and end date
- Customer must ensure that the certificates are regenerated and exchanged between On-prem Orchestrator and SD-WAN appliance to avoid loss of appliance connectivity with On-prem orchestrator.
- 5. Select the **Authentication Type**. The following are the authentications types that are supported between the SD-WAN appliance and On-prem SD-WAN Orchestrator connectivity:
  - No Authentication –No authentication between the On-prem SD-WAN Orchestrator and SD-WAN appliance, and there is no need to use the SD-WAN Appliance or On-prem SD-WAN Orchestrator Certificate. But you can use this option if you have a secure network such as MPLS.

ecure Connectivity
No Authentication - No Authentication between On-prem SD-WAN Orchestrator and SD-WAN Appliance. Customer can use this option if they have already secure network. For eg: MPLS
One-way Authentication - SD-WAN Appliance will authenticate On-prem SD-WAN Orchestrator. On-prem SD-WAN Orchestrator certificate should be uploaded on SD-WAN Appliance.
Two-way Authentication - On-prem SD-WAN Orchestrator and SD-WAN Appliance authenticates each other. SD-WAN Appliance and On-prem SD-WAN Orchestrator certificates should be exchanged each other.
Automatication Trans
Autochanou 1 Jac
No Authentication
Apply

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

No Authentication – No Authentication between On-prem SD-WAN Orchestrator and SD-WAN Appl One-way Authentication – SD-WAN Appliance will authenticate On-prem SD-WAN Orchestrator. On Two-way Authentication – On-prem SD-WAN Orchestrator and SD-WAN Appliance authenticates e	iance. Customer can use this option if they have already secure network. For eg: MPLS -prem SD-WAN Orchestrator certificate should be uploaded on SD-WAN Appliance. ach other. SD-WAN Appliance and On-prem SD-WAN Orchestrator certificates should be exchanged each other.
Authentication Type One-Way Authentication	
On-prem SD-WAN Orchestrator Certificate	
Certificate Details:	
Certificate Fingerprint:	D7:48:7F:10:E9:01:21:75:9A:87:51:41:34:E0:CC:09:23:D6:72:43
Start Date:	Dec 15 07:30:10 2020 GMT
End Date:	Dec 13 07:30:10 2030 GMT
Click here to select the file or drag and drop the selected file. Allowed file type is .pem	

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

sure Connectivity	
No Authentication – No Authentication between On-prem SD-WAN Orch One-way Authentication – SD-WAN Appliance will authenticate On-prem Two-way Authentication – On-prem SD-WAN Orchestrator and SD-WAN J	strator and SD-WAN Appliance. Customer can use this option if they have already secure network. For eg: MPLS iSD-WAN Orchestrator. On-prem SD-WAN Orchestrator certificate should be uploaded on SD-WAN Appliance. Appliance authenticates each other. SD-WAN Appliance and On-prem SD-WAN Orchestrator certificates should be exchanged each other.
uthentication Type	
Two-Way Authentication Apply	~
Jn-prem SD-WAN Orchestrator Certificate	
Certificate Details:	
Certificate Fingerprint:	D7:48:7F:10:E9:01:21:75:9A:87:51:41:34:E0:CC:09:23:D6:72:43
Start Date:	Dec 15 07:30:10 2020 GMT
End Date:	Dec 13 07:30:10 2030 GMT
Click here to select the file or drag and drop the selected file. Allowed file type is .pem	
Upload	
D-WAN Appliance Certificate	
Certificate Details:	
Certificate Fingerprint:	04:DD:E9:14:67:04:90:EB:CB:D4:69:4A:AF:D0:0C:77:31:CE:42:06
Start Date:	Dec 15 14:34:00 2020 GMT
End Data	Dec 12 14:24:00 2020 GMT

#### Note

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

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

## **Upgrade and Downgrade**

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

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

## Monitoring

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

- **ARP, Route, Ethernet, and Ethernet MAC Statistics**: You can see the statistics information for ARP, Route, Ethernet, and Ethernet MAC. Using the statistics information, you can verify any traffic or interface errors. For more information, see Viewing Statistical Information.
- DHCP Client WAN links: The DHCP Client WAN Links page provides the status of learned IPs. You can request to renew the IP, which refreshes the lease time. You can also choose to Release Renew, which issues a new IP address with a new lease. For more details, see Monitoring DHCP client WAN links.
- **SLAAC WAN Links**: The SLAAC WAN links page provides details about the IPv6 addresses that SLAAC assigns to the virtual interfaces. You can also select **Release Renew** to allow SLAAC to assign a new IP address or the same IP address with a new lease to the IPv6 client.
- **DHCP Server/Relay**: You can use the SD-WAN appliance as either DHCP Servers or DHCP Relay agents.
  - The DHCP server feature allows devices on the same network as the SD-WAN appliance's LAN/WAN interface to obtain their IP configuration from the SD-WAN appliance.
  - The DHCP relay feature allows your SD-WAN appliances to forward DHCP packets between DHCP client and server.

For more information, see DHCP server and DHCP relay.

- **Firewall Connections**: The **Firewall Connections** page provides the Firewall connection statistics. You can see how the firewall policies are acting on the traffic for each Application. For more information, see Viewing Firewall Statistics.
- **Flows**: The **Flows** section provides basic instructions for viewing Virtual WAN flow information. For more details, see Viewing Flow Information.
- DNS Proxy Statistics: This page provides details about the configured DNS proxies. Click **Re**fresh to get the current data. For more information, see Domain name system.

## Diagnostics

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

## Note

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

## System maintenance

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

- **Delete Files**: You can delete Log files, Backup files, and Archived Databases. Select the file that you want to delete from the drop-down menu and click the delete button.
- **Restart System**: You can restart the virtual WAN service or reboot the system.
- Local Change Management: The Local Change Management process allows you to upload a new appliance package to this individual appliance.
- **Configuration Reset**: You can reset the configuration. This option clears out the user data, logs, history, and local configuration data on this appliance.
- Factory Reset: Use Factory Reset option to reset the SD-WAN appliance to the shipped version.

Note

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

## **Unsupported platforms**

The new UI does not support the following SD-WAN appliances:

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

# Citrix SD-WAN 11.5 release upgrade impact

August 24, 2022

- Citrix SD-WAN 11.5.0 is a Limited Availability release, recommended and supported only for specific customers/production deployments.
- SD-WAN 11.5.0 release does not support Advanced Edition(AE), Premium Edition(PE), WAN Optimization deployments.

- SD-WAN 11.5.0 supports only the platforms mentioned in SD-WAN platform models and software packages.
- SD-WAN 11.5.0 does not support Citrix SD-WAN Center or Citrix SD-WAN Orchestrator for onpremises.
- SD-WAN 11.5.0 firmware is not available on the Citrix Downloads page.
- SD-WAN 11.5.0 release is available only via Citrix SD-WAN Orchestrator service and only on selected geographical POPs.
- Ensure to get the required approvals and guidance from Citrix Product Management / Citrix Support before deploying 11.5.0 on any production network.

# System requirements

August 24, 2022

## Hardware requirements

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

#### **Firmware requirements**

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

Note

Appliances running earlier software versions cannot establish a Virtual Path connection to the appliance running SD-WAN release 11.4. For additional information, please contact the Citrix support team.

#### Software requirements

From SD-WAN 11.5 release onwards, SD-WAN appliance licensing is managed through Citrix SD-WAN Orchestrator service. For details regarding license requirements, see Licensing.

#### **Browser Requirements**

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

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

- Mozilla Firefox 49+
- Google Chrome 51+
- Microsoft Edge 13+

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

#### Hypervisor

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

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

#### **Cloud Platform**

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

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

# **SD-WAN platform models**

#### August 24, 2022

The following are the supported SD-WAN standard edition hardware appliance models:

SD-WAN SE PLATFORM MODEL	ROLE
110-SE/110-LTE-WiFi/110-WiFi-SE	Small branch appliance
210-SE/210-SE LTE	Small branch appliance
1100-SE	Large branch appliance
2100-SE	Large branch appliance
4100-SE	Data Center - Master Control Node (MCN) appliance

SD-WAN SE PLATFORM MODEL	ROLE
5100-SE	Data Center - Master Control Node (MCN) appliance
6100-SE	Data Center - Master Control Node (MCN) appliance

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

The following are the supported SD-WAN VPX Virtual Appliance (VPX-SE) models:

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

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

# Upgrade paths

August 24, 2022

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

SD-WAN	11.5.0	11.4.1	11.3.2	11.2.3	11.1.3	11.0.3	10.2.8
11.4.x	0						
11.3.x							
	_						
11.2.x		V		V			
11.1.x				-			
11 O v				$\bigcirc$			
11.0.x					-		
10.0.0	-		$\checkmark$				
10.2.8							
	_	-	_	_	_	-	
10.2.x							

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

Note

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

# Configuration

September 19, 2022

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

## **Initial Setup**

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**

This section provides basic navigation instructions, and a navigation roadmap of the SD-WAN web management interface page hierarchy.

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

		Breadcrumbs Page Tabs
Title Bar		10.1.0.112.650295* Legevet
Menu Bar	Dashboard Menitering	Configuration
Section Tabs	- Appliance Settings	Configuration > Appliance Settings
Navigation Tree	Administrator Interface Logging/Monitoring Network Adapters Nat Flow	User Accounts RACOUS TACACS+ HTTPS Cert HTTPS Settings Miscellaneous Change Local User Password
	App Flow SNMP NETRO API Licensing	User Name: admin Current Password:
	+ Virtual WAN + System Maintenance	Contine New Patsucod
		Delete Workspace For User           Delete Workspace For User           Delete Workspace Violation Editor workspace. This action will not delete the user.           Deleting a workspace will remove all saved configurations and networks maps for the selected user.           User Name:         edmin           Delete Selected User's Workspace.
Page Area ·		Manage Users
		Add User Note Deleting a user will also delete local files for that user. User Name:

The basic navigation elements are as follows:

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

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

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

**Web management interface dashboard** Click the **Dashboard** section tab to display basic information for the local appliance.

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

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

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

#### Citrix SD-WAN 11.5

ystem Status	
lame:	MCN 23
fodel:	VPX
ub-Model:	BASE
ppliance Mode:	MCN
erial Number:	67e0772c-5190-a2ee-d183-9244189b30a0
fanagement IP Addre	55: 10.102.78.154
ppliance Uptime:	1 days, 10 hours, 49 minutes, 48.5 seconds
ervice Uptime:	1 days, 10 hours, 42 minutes, 20.0 seconds
outing Domain Enabl	xt Default_RoutingDomain
ocal Versions	
oftware Version: 1	0.1.0.111.690027
uilt On: J	un 21 2018 at 23:42:30
lardware Version: V	PX
05 Partition Version: 4	.6

The following figure shows a sample client appliance Dashboard display.

Dashboard	Monitoring	Configuration	
Sustan Status			
System Status			
Name:	DC2-201		
Model:	5100		
Appliance Mode:	Client		
Management IP Ad	dress: 10.199.107.20	)1	
Appliance Uptime:	2 weeks, 36 m	ninutes, 52.5 seconds	
Service Uptime:	2 weeks, 8 mi	nutes, 26.0 seconds	
Routing Domain En	abled: Default_Routi	ingDomain	
Virtual Path Ser	vice Status		
Virtual Path DC-R	P: Untime: 4 days	5 hours 21 minutes 20.0 seconds	
Virtual Patri DC-b	optime. 4 days	, o nours, or minutes, solo seconds.	

#### Setting up the Appliance Hardware

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

1. Set up the chassis.

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

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

- b) Plug the power cord into the appliance and an AC outlet.
- c) Press the power button on the front of the appliance.
- 4. Connect the appliance Management Port to a personal computer.

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

Note

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

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

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

#### **Configure Management IP Address**

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

Citrix SD-WAN appliances support both IPv4 and IPv6 protocols. You can configure IPv4, IPv6, or both (dual stack). When both IPv4 and IPv6 protocols are configured, the IPv4 protocol takes precedence over the IPv6 protocol.

NOTE

- To configure an IPv4 or IPv6 address in feature specific configurations, ensure that the same protocol is enabled and configured as the management interface protocol. For example, if you want to configure an IPv6 address for an SMTP server, ensure that an IPv6 address is configured as the management interface address.
- Link-local addresses (IPv6 addresses starting with "fe80") are not allowed.

• To configure an IPv6 address, you must have a router in the network that advertises IPv6 address.

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

 SD-WAN VPX Virtual Appliance – See the sections, [Configuring the Management IP Address for the SD-WAN VPX-SE and Differences Between an SD-WAN VPX-SE and SD-WAN WANOP VPX Installation.

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

Note

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

- 1. If you are configuring a hardware SD-WAN appliance, physically connect the appliance to a PC.
  - If you have not already done so, connect one end of an Ethernet cable to the Management Port on the appliance, and the other end to the default Ethernet port on the PC.

Note

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

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

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

3. Change the IP Address for the PC.

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

- 192.168.100.50
- 4. Change the **Subnet Mask** setting on your PC to the following:
  - 255.255.0.0
- 5. On the PC, open a browser and enter the default IP Address for the appliance. Enter the following IP Address in the address line of the browser:
  - 192.168.100.1

#### Note

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

Ignore any browser certificate warnings for the Management Web Interface.

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

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

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

#### Note

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

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

Dashboard	Monitoring Configuration
System Status	
Name: Model: Sub-Model: Serial Number: Management IP Add Appliance Uptime: Service Uptime: Routing Domain Enal	MCN_23 VX BA5E MCN G7e0772-5190-2zee-d183-9244189b30a0 Free:10.102.78.154 1 days, 10 hours, 49 minutes, 48.5 seconds 1 days, 10 hours, 42 minutes, 20.0 seconds 1 days, 10 hours, 42 minutes, 20.0 seconds
Local Versions	
Software Version: Built On: Hardware Version: OS Partition Version:	10.1.0.111.690027 Jun 21 2018 at 23:42:30 VPX 4.6
Virtual Path Serv	ice Status
Virtual Path MCN_23	-Stel:Uptime: 1 days, 10 hours, 39 minutes, 19.0 seconds.

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 **Configura-tion** 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.

	Dashboard Monitoring	Configuration
<	Appliance Settings      Administrator Interface      Logging/Monitoring      Network Adapters	Configuration > Appliance Settings > Administrator Interface           User Accounts         RADBUS         TACACS+         HTTPS Cert         HTTPS Settings         Miscellaneous
	Net Row App Row SNAP NITRO API Licensing + Vietual WAN + System Maintenance	Change Local User Password       User Name     admin       Current Password:
		Delete Workspace For User           Delete the selected user's Configuration Editor workspace. This action will not delete the user.           Deleting a workspace will remove all saved configurations and networks maps for the selected user.           User Name:           admin           Delete Selected User's Workspace.
		Manage Users       Add User       Note: Deleting a user will also delete local Flers for that user.       User Name: a     Delete: Selected User

8. In the **Appliance Settings** branch of the navigation tree, select **Network Adapters**. This displays the **Network Adapters** settings page with the **IP Address** tab preselected by default, as shown in the below figure.

sonnguration >	Appliance Settings > Network Adapters
	Appriance setungs / network Audpiers
IP Address	Ethernet LACP LAG Group Mobile Broadband
Management	Interface IP
IPv4 Protocol	
C Enab	le IPv4
IP Addr	ress:
Subnet	Mask:
Gatewa	y IP Address:
IPv6 Protoco	
🗹 Enab	le IPv6
To enab	sie Stateless DHCP, select both SLAAC and DHCP check box.
SLA/	AC DHCP
Change Set	tings Clear Settings
DNS Informat	ion
DNS Settin	ns
Bris Settin	۲۶۰ 
Primary DNS	
Secondary D	NS: 8.8.8.8
Change Sett	liear settings
Current DN	٧S
Primary DNS	
Secondary D	NS: 8.8.8
Management	Interface Whitelist
Management	Interface Whitelist Illows Management Interface to be accessed from all networks.
Management empty Whitelist a networks can be networks can be	Interface Whitelist Illows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network.
Management e empty Whitelist a e networks can be i networks can be	Interface Whitelist Illows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network.
Management e empty Whitelist a e networks can be i networks can be Add Network(s):	Interface Whitelist Illows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network.
Management empty Whitelist a i networks can be i networks can be Add Network(s):	Interface Whitelist allows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network.
Management a empty Whitelist a i networks can be i networks can be Add Network(s): Change Setting	Interface Whitelist allows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network.
Management e empty Whitelist a inetworks can be inetworks can be Add Network(s): Change Setting Management	Interface Whitelist Illows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network.
Management a empty Whitelist a i networks can be i networks can be Add Network(s): Change Setting Management coupling to use the	Interface Whitelist  Ilows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network.  Is  Interface DHCP Server  DHCR Server on DHCR Server
Management n empty Whitelist a in networks can be in etworks can be Add Network(s): Change Setting Management rou plan to use th plicate IP address	Interface Whitelist  Ilovs: Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network.  Is  Interface DHCP Server  e DHCP Server DHCP Relay services on a Citrix Appliance configured for High Availability (HA), do not configure either service on both the Active and Standby appliance. Doing so will lead te so on the defined management network.
Management empty Whitelist a networks can be i networks can be add Network(s): Change Setting Management /ou plan to use th plicate IP address ten HA switches fr e Management Inl	Interface Whitelist  Ilows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V4 network. added/removed only from a V6 network.  Interface DHCP Server  E DHCP Server or DHCP Relay services on a Citrix Appliance configured for High Availability (HA), do not configure either service on both the Active and Standby appliance. Doing so will lead te so on the defined management network.  Om the Active to the Standby Citrix Appliance, the DHCP Server and DHCP Relay service settings are not applied on the Standby appliance and will stop working.  Service DHCP Server In Use the current Management Interface IP Settings (and the standby appliance and DNS experies) for DHCP Server Jance defined by Start and End IP.
Management n empty Whitelist a n etworks can be is networks can be add Network(s): Change Setting Management /ou plan to use th plicate IP address nen HA switches fr e Management Inf idress, must be va	Interface Whitelist  Ilows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V4 network. added/removed only from a V6 network.  Interface DHCP Server  E DHCP Server or DHCP Relay services on a Citrix Appliance configured for High Availability (HA), do not configure either service on both the Active and Standby appliance. Doing so will lead es on the Active to the Standby Citrix Appliance, the DHCP Server and DHCP Relay service settings are not applied on the Standby appliance and will stop working. Firsface DHCP Server will use the current Management Interface IP settings (gateway, subnet mask, and DNS servers) for DHCP offers. The DHCP Server IP range, defined by Start and End IP lid in the Management Interface subnet.
Management a empty Whitelist a i networks can be i networks can be i networks can be Add Network(s): Change Setting Management Management net pladress use hA switches fr e Management Int idress, must be va ie Management plat ittings are not app	Interface Whitelist  Ilows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V4 network. added/removed only from a V6 network.  Is  Interface DHCP Server  e DHCP Server O DHCP Relay services on a Citrix Appliance configured for High Availability (HA), do not configure either service on both the Active and Standby appliance. Doing so will lead it ses on the defined management network. Interface DHCP Server will use the current Management Interface IP Settings (gateway, subnet mask, and DNS servers) for DHCP offers. The DHCP Server IP range, defined by Start and End IP Itel Management Interface IP Settings (gateway, subnet mask, and DNS servers) for DHCP offers. The DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management interface.
Management a empty Whitelist a a retworks can be is networks can be is networks can be Add Network(s): Change Settling Management Management Int iddress, must be va titings are not app DHCP Server Stat	Interface Whitelist  Illows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network. added/removed only from a V6 network.  Interface DHCP Server  Interface DHCP Server Interface DHCP Server and DHCP Relay services on a Citrix Appliance. In DHCP Server and DHCP Relay services on the defined management Interface IP settings (gateway, subnet mask, and DNS servers) for DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management Interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management Interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management Interface. If only IPv6 protocol is enabled then the DHCP Relay IEver and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management Interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management Interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management Interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management Interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay IEver and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management Interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay IEver ADHCP Relay IEver ADHCP Relay IEver ADHCP Relay IEver ADHCP Relay IEv
Management An empty Whitelist a mempty Whitelist a metworks can be interworks can be context and the empty whitelist a metwork and the empty a	Interface Whitelist  Illows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network. added/removed only from a V6 network.  Interface DHCP Server  E DHCP Server or DHCP Relay services on a Citrix Appliance configured for High Availability (HA), do not configure either service on both the Active and Standby appliance. Doing so will lead is so on the defined management interface IP Server and DHCP Relay service settings are not applied on the Standby appliance and will stop working.  Ierface DHCP Server and DHCP Server and DHCP Relay services or a citrix Appliance interface IP settings (gateway, subnet mask, and DNS servers) for DHCP offers. The DHCP Server and DHCP Relay Iterface DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay Iter is stopped Ver:
Management Management memory Miltelist a metworks can be metworks can be metworks can be commended by Change Settling Management Management Management In titings are not app DHCP Server Stat Lenable DHCP Server Stat Lenab	Interface Whitelist  allows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network. added/removed only from a V6 network.  added/removed only from a V6 network.  added/removed only from a V6 network.  added/removed only from a V6 network.  added/removed only from a V6 network.  added/removed only from a V6 network.  by
Management Management memory Mittelist a metworks can be interworks can be context and the second se	Interface Whitelist  allows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network. added/removed only from a V6 network.  [
Management Management mempty Whitelist a metworks can be is networks can be charter of the second se	Interface Whitelist  allows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V5 network. added/removed only from a V5 network.  added/removed on DHCP Relay services and DHCP Relay service settings are not applied on the Standby appliance and will stop working.  atterface DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management Interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay is applicab
Management An empty Whitelist a in etworks can be in etworks can be in etworks can be change Setting Management Change Setting Management In fdress, must be va tings are not app DHCP Server Sta Enable DHCP Ser Lease Time (min Domain Name: Start IP Address: End IP Address: Change Setting	Interface Whitelist  allows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V5 network.  added/removed only from a V5 network.  B  B  Interface DHCP Server  Interface DHCP Server  Interface DHCP Relay services on a Citrix Appliance configured for High Availability (HA), do not configure either service on both the Active and Standby appliance. Doing so will lead so on the Active to the Standby Citrix Appliance, the DHCP Server and DHCP Relay service settings are not applied on the Standby appliance and will stop working.  Iterface DHCP Server will use the current Management Interface IP settings (gateway, subnet mask, and DNS servers) for DHCP offers. The DHCP Server IP range, defined by Start and End IP Interface DHCP Server and DHCP Relay is applicable only if IPv4 Protocol Is enabled in the Management Interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay Us: stopped
Management Management empty Whitelist a empty Whitelist a metworks can be interworks can be comparison of the second seco	Interface Whitelist
Management Management mempty Whitelist a mempty Whitelist a metworks can be interworks can be control of the second secon	Interface Whitelist
Management  Adnagement  compty Whitelist a  change Setting  Management  compty plan to use th  policate IP address  ren HA switches fr  ae Management IP  dHCP Server Stat  Lease Time (min  Domain Name:  Start IP Address:  End IP Address:  Change Setting  Management  Enable DHCP Rel  DHCP Compty Plan  Change DHCP Rel  CHANGE DHCP	Interface Whitelist  Illows Management Interface to be accessed from all networks. added/removed only from a V4 network. added/removed only from a V6 network. added/removed only from a V6 network. added/removed only from a V6 network.  Betterface DHCP Server  Interface DHCP Relay services on a Citrx Appliance configured for High Availability (HA), do not configure either service on both the Active and Standby appliance. Doing so will lead to so the defined by Start and End IP Relay services on a Citrx Appliance in DHCP Relay services extings are not applied on the Standby appliance. Doing so will lead to so the defined by Start and End IP Relay services upplicate the Stardby Appliance submet. Interface DHCP Server and DHCP Relay is applicable only if IPv4 Protocol is enabled in the Management interface. If only IPv6 protocol is enabled then the DHCP Server and DHCP Relay utes: tus: stopped tus: tus: stopped tus: tus: stopped tus: tus: tus: tus: tus: tus: tus: tus:

- 9. In the IP Address tab, enable one of the following:
  - **IPv4 Protocol**: To enable IPv4 address, select the **Enable IPv4** check box. Dynamic Host Control Protocol (DHCP) assigns an IP address and other network configuration parameters dynamically to each device on the network. Select **Enable DHCP** for assigning IP address dynamically. To configure the IP address manually, provide the following details:
    - IP Address
    - Subnet Mask
    - Gateway IP Address
  - **IPv6 Protocol**: To enable IPv6 address, select **Enable IPv6** check box. You can configure IPv6 address manually or enable DHCP or SLAAC to assign IP address automatically.

To configure manually, provide the following details:

- IP Address
- Prefix

To configure SLAAC, select the **SLAAC** check box. SLAAC automatically assigns an IPv6 address to each device on the network. SLAAC enables an IPv6 client to generate its own addresses using a combination of locally available information and information advertised by routers through Neighbor Discovery Protocol (NDP).

To configure DHCP, select the **DHCP** check box. To enable stateless DHCP, select both **SLAAC** and **DHCP** check boxes.

• Both IPv4 and IPv6 Protocols: Select both Enable IPv6 and Enable IPv4 check boxes to enable both IPv4 and IPv6 protocols. In such scenarios, the SD-WAN appliance has one IPv4 management IP address and one IPv6 management address.

#### NOTE

- The management IP address must be unique for each appliance.
- The **Management Interface DHCP Server** and **DHCP Relay** sections on the IP Address tab are applicable only if IPv4 Protocol is enabled in the Management interface.
- When the management interface acts as the DHCP client, the host name is used in DHCP client messages as option 12. From Citrix SD-WAN release 11.2.3 onwards and up to release 11.4.1, the host name was set as **sdwan**. From Citrix SD-WAN release 11.4.1 onwards, the host name is the same as the site name.

If the site name is changed or configured for the first time, then until the configuration update is completed and the virtual WAN service is up, the old site name or **sdwan** is used as the host name in DHCP client messages. After the configuration update is completed and the virtual WAN service is up, the subsequent DHCP client messages use the new site name.

- 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 in the following format:

For IPv4 address: https://<IPv4 address>

Example: https://10.10.2.3

For IPv6 address: https://<[IPv6 address]>

Example: https://[fd73:xxxx:yyyy:26::9]

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

#### Тір

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.

**Management interface allow list** Allowed list is an approved list of IP addresses or IP domains that have permission to access your management interface. An empty list allows Management Interface to be accessed from all networks. You can add IP addresses to ensure that the management IP address is accessible only by the trusted networks.

To add or remove an IPv4 address to the allowed list, you must access the SD-WAN appliance management interface using an IPv4 address only. Similarly, to add or remove an IPv6 address to the allowed list, you must access the SD-WAN appliance management interface using an IPv6 address only.

Management Interface Whitelist						
An empty Whitelist allows Management Interface to be accessed from all networks. V4 networks can be added/removed only from a V4 network.						
V6 networks can be added/removed only from a V6 network.						
Add Network(s):						
Change Settings						

#### Set date and time

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

Note

- You must repeat this process for each appliance you want to add to your network.
- If the current time is changed either manually or through NTP server, and the newly set time is more than the session time-out timer, then the UI session gets logged out.

#### 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.

#### Citrix SD-WAN 11.5

appliance Settings	Configuration > System Maintenance > Date/Time Settings
/irtual WAN	
vstem Maintenance	Note: If the Appliance date/time is turned back due to NTD or manual chapper. Reporting artifacts may occur. These can be cleared
Delete Files	creating a new archive of the current database on the Reports screens.
Restart System	
Date/Time Settings	NTP Settings
Local Change Management Diagnostics Update Software Configuration Reset	Use NTP Server  Server Address: time.nist.gov Change Settings Date/Time Settings Date: April  11  2016  Time: 09  57  57
	Change Date Timezone Settings
	Note: After changing the timezone setting, a reboot will also be necessary for any timezone changes to take full effect. Until then, so logs will continue to use the actual timezone setting in effect at the time of the last reboot, even though events timestamps may refl the new setting.

#### 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 can 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**

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.

#### Citrix SD-WAN 11.5

<ul> <li>Appliance Settings</li> </ul>	Configuration > App	liance Settings					
<ul> <li>Administrator Interface</li> <li>Logging/Monitoring</li> <li>Network Adapters</li> <li>Net Flow</li> </ul>	User Accounts	RADIUS	TACACS+	HTTPS Cert	Miscellaneous		
	Change Local User Password						
SNMP Licensing	User Name: Current Password:	admin	•				
+ System Maintenance	New Password:						

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

#### This displays the **Miscellaneous** tab page.

		1	mirs cert	Miscellaneous	
hange Web Conso	ole Timeout			De la constante	
neout: 60		Enter the new tin	neout value in min	utes (1-9999).	
Ihange Timeout					

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

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

Note

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

#### 4. Click Change Timeout.

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

Configuration > Appliance Settings		
Timeout Change Success		
Your timeout has been changed.		
You will be automatically logged out in 3	seconds.	

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

citrıx	You have been successfully logged out. Username Password
	Copyright(©) Citrix Systems, Inc. All rights reserved.

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**

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.

Dashboard Monitoring	Configuration	,												
- Appliance Settings	Configura	ation > Ap	opliance Settings )	Logging/Monitoring										
Administrator Interface     Logging/Monitoring	Log C	Options	Alert Options	Alarm Options		Syslog Server								
<ul> <li>Network Adapters</li> <li>Net Flow</li> </ul>	Alarm	Configura	ntion											
- SNMP Licensing	Add Ala	arm												
+ Virtual WAN	Event 1	Туре		Trigger State		Trigger Duration (sec)	Clear State	Clear Duration (sec)	Severity		Email	Syslog	SNMP	
System Maintenance	PATH		۲	DEAD	۲	0	GOOD •	0	EMERGENCY	۲				×
	VIRTU	JAL PATH	•	DEAD	۲	0	GOOD •	0	CRITICAL	۲		•		×
							0000	1	50000		_	_		

- 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.

ystem Maintenance	Ping	Traceroute	Packet Capture	Path Bandwidth	System Info	Diagnostic Data	Events	Alarms	Diagnostics	Tool				
Delete Files Restart System Date/Time Settings Local Change Management	Alarms Enable Auto Ref	fresh 🔲 Time Inte	erval 5	▼ seconds	Refresh				Clear Ch	ecked Alarms Clea	ır All Alarms 🛛 👔			
Diagnostics														
Update Software Configuration Reset	Triggered Al	arms Summary												
	Filter:	Any	column	Apply										
	Show 100	• entries	s Showing 1 to 11	of 11 entries			. Trigger			First Previous	1 Next			
	Severity	Event Type	Object Name			Trigger State	Duration (	ecl	Clear State	Duration (sec)	Clear Acti			
	Severity EMERGENCY	Event Type PATH	Object Name Client-1-WL		LS	DEAD	Duration (s	ec)	GOOD GOOD	Duration (sec)	Clear Acti			
	Severity EMERGENCY EMERGENCY	PATH PATH	Object Name Client-1-WL Client-1-WL	: 1-36->MCN-WL-1-MP 1-MPLS->MCN-WL-1-	'LS MPLS	DEAD DEAD	Duration (s 0 0	ec)	GOOD GOOD	Duration (sec) 0 0	Clear Act			
	Severity EMERGENCY EMERGENCY CRITICAL	PATH PATH PATH VIRTUAL_PATH	Object Name Client-1-WL Client-1-WL H MCN-DC:Cli	: :1-3G->MCN-WL-1-MP :1-MPLS->MCN-WL-1- ent-1	LS MPLS	DEAD DEAD DEAD DEAD	0 0 0 0	ec)	Gear State 600D 600D 600D	0 0 0	Clear Act			
	Severity EMERGENCY EMERGENCY CRITICAL EMERGENCY	Event Type PATH PATH VIRTUAL_PATH PATH	Object Name Client-1-WL Client-1-WL H MCN-DC:Cli MCN-WL-1-	: :1-3G->MCN-WL-1-MP :1-MPLS->MCN-WL-1- ent-1 MPLS->Client-1-WL-1-	LS MPLS 3G	DEAD DEAD DEAD DEAD DEAD DEAD	Duration (: 0 0 0	ec)	Geor State GOOD GOOD GOOD GOOD	Duration (sec) 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Clear Act			
	Severity EMERGENCY EMERGENCY CRITICAL EMERGENCY EMERGENCY	Event Type PATH PATH VIRTUAL_PATH PATH PATH	Object Name Client-1-WL Client-1-WL MCN-DC:Cli MCN-WL-1- MCN-WL-1-	: 1-3G->MCN-WL-1-MP 1-MPLS->MCN-WL-1- ent-1 MPLS->Client-1-WL-1- MPLS->Client-1-WL-1-	LS MPLS 3G MPLS	DEAD DEAD DEAD DEAD DEAD DEAD DEAD	Duration (: 0 0 0 0 0	ec)	GOOD GOOD GOOD GOOD GOOD GOOD	Duration (sec) 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Clear Act			
	Severity EMERGENCY EMERGENCY CRITICAL EMERGENCY EMERGENCY	Event Type PATH PATH VIRTUAL_PATH PATH PATH PATH	Object Name Client-1-WL Client-1-WL H MCN-DC:Cli MCN-WL-1- MCN-WL-1- Client-2-WL	: 1-3G->MCN-WL-1-IMPLS->MCN-WL-1-I ent-1 MPLS->Client-1-WL-1- MPLS->Client-1-WL-1-I-I-I-I-I-I-I-I-I-I-I-I-I-I-I-I-I-I-	LS MPLS 3G MPLS MPLS	Trigger State DEAD DEAD DEAD DEAD DEAD DEAD DEAD DEA	Duration (s 0 0 0 0 0 0	ec)	GOOD GOOD GOOD GOOD GOOD GOOD GOOD	0 0 0 0 0 0 0 0 0 0 0				
	Severity EMERGENCY EMERGENCY CRITICAL EMERGENCY EMERGENCY EMERGENCY	Event Type PATH PATH VIRTUAL_PATH PATH PATH PATH PATH	Object Name Client-1-WL Client-1-WL MCN-UC-Cli MCN-WL-1- Client-2-WL Client-2-WL	: 1-36->MCN-WL-1-MP 1-MPLS->MCN-WL-1-1 MPLS->Client-1-WL-1- MPLS->Client-1-WL-1- 1-MPLS->MCN-WL-1-MP	LS MPLS 3G MPLS MPLS LS	Trigger State DEAD DEAD DEAD DEAD DEAD DEAD DEAD DEA	Duration (s 0 0 0 0 0 0 0 0 0 0	ec)	Good         Good	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Clear Acti			
	Severity EMERGENCY EMERGENCY CRITICAL EMERGENCY EMERGENCY EMERGENCY CRITICAL	Event Type           PATH           PATH           VIRTUAL_PATH           PATH           PATH           PATH           PATH           PATH           PATH           PATH           VIRTUAL_PATH           PATH           VIRTUAL_PATH           VIRTUAL_PATH	Object Name Client-1-WL Client-1-WL MCN-DC:Cli MCN-WL-1- Client-2-WL Client-2-WL dlient-2-WL	: 1-3G->MCN-WL-1-IMP 1-MPLS->Client-1-WL-1- MPLS->Client-1-WL-1- MPLS->Client-1-WL-1- 1-MPLS->MCN-WL-1-MP 1-3G->MCN-WL-1-MP ent-2	LS MPLS 3G MPLS MPLS LS	Trigger State       DEAD	Duration (s 0 0 0 0 0 0 0 0 0 0 0	ec)	George         George           George         George	Duration (sec) 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Clear Acti			
	Severity EMERGENCY CRITICAL EMERGENCY EMERGENCY EMERGENCY CRITICAL EMERGENCY	Event Type       PATH       PATH       PATH       VIRTUAL_PATH       PATH       PATH       PATH       PATH       PATH       PATH       PATH       PATH       PATH       VIRTUAL_PATH       PATH       VIRTUAL_PATH       PATH       PATH       PATH       PATH       PATH	Object Name Client-1-WL Client-1-WL MCN-WL-1- MCN-WL-1- Client-2-WL Client-2-WL MCN-DC:Cli MCN-WL-1-	: 1-36->MCN-WL-1-4MP 1-4MPLS->MCN-WL-1-4 MPLS->Client-1-WL-1- MPLS->Client-1-WL-1- 1-4MPLS->MCN-WL-1-4MP 1-36->MCN-WL-1-4MP ent-2 MPLS->Client-2-WL-1-	LS MPLS 36 MPLS MPLS LS 36	Trigger State       DEAD       DEAD	Duration (s 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	æc)	Good         Good	Duration (sec) 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Clear Acti			
	Severity EMERGENCY CRITICAL EMERGENCY EMERGENCY EMERGENCY CRITICAL EMERGENCY EMERGENCY	Event Type       PATH       PATH       PATH       VIRTUAL_PATH       PATH       PATH       PATH       PATH       PATH       PATH       VIRTUAL_PATH       PATH       PATH	Object Name Client-1-WL Client-1-WL MCN-WL-1- MCN-WL-1- Client-2-WL Client-2-WL MCN-WL-1- MCN-WL-1- MCN-WL-1-	: 1-3G->MCN-WL-1-MP 1-MPLS->MCN-WL-1- ant-1 MPLS->Client-1-WL-1- 1-MPLS->MCN-WL-1- 1-MPLS->MCN-WL-1-MP ent-2 MPLS->Client-2-WL-1-	LS MPLS 36 MPLS LS 36 MPLS	Frigger State       DEAD	Duration (s 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	ec)	Cear State 600D 600D 600D 600D 600D 600D 600D 600D 600D 600D	Duration (sec) 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Clear Acts			

#### Clearing triggered alarms To manually clear triggered alarms:

- 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.

## Setup Master Control Node

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

From Citrix SD-WAN 11.5 release onwards, you can set up an MCN through Citrix SD-WAN Orchestrator service. For more information, see Deployment and Site configuration.

## Connecting the client appliances to your network

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.

#### Accessing the shell command

From SD-WAN 11.4.1 release onwards, Admin account users can run the shell command from the SD-WAN CLI console directly, without being prompted for the login credentials of the CBVWSSH static account. This feature enhances the security of your SD-WAN appliances as it removes the hard coded

password of the CBVWSSH account and replaces it using a more secure method. To run the shell command, login to the SD-WAN CLI console and type shell.

Note

- This functionality is supported only for Admin account users. It is not supported for Network administrators, Security administrators, or Viewer account users.
- This functionality is meant for troubleshooting purposes only. Any system-specific changes that are made through the shell command are supervised by Citrix.

**Upgrade** When you upgrade your SD-WAN appliance to the 11.4.1 version, the password of the default admin account gets synchronized with the CBVWSSH account. This synchronization between the CBVWSSH account and the default admin account happens every time you edit/update the admin account.

**Downgrade** When you downgrade your SD-WAN appliance from 11.4.1 to an older version, you get an option to and reset the password of the default admin account. However, the new password does not get synchronized to the CBVWSSH account. Therefore, to be able to access the shell command even after a downgrade, it is mandatory to remember the current password before downgrading your appliance.

## Deploy Citrix SD-WAN Standard Edition in OpenStack using CloudInit

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

NOTE

Create Citrix image to support config-drive functionality.

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

- Mgmt. ipv4 address
- Mgmt. gateway
- Name-server1
- Name-server2
- Serial number Used for authentication and it must be reused for the new instance. Serial number passed in clouding must overwrite the autogenerated trial number in the VPX instance.

## Note

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

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

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

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

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

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

## **Pre-requisites**

Go to Images and click Create Image.

Create Image			x
Image Details * Metadata	Image Details Specify an image to upload to the Image Service. Image Name <sup>*</sup>	Image Description	0
	Image Source File <sup>*</sup> Browse		
	Format <sup>*</sup>		
	Image Requirements	Dameliek	
	Choose an image \$	Choose an image	¢
	Architecture	Minimum Disk (GB) 0 0	
	Image Sharing Visibility Public Private	Yes     No	
× Cancel		< Back Next > Create Image	

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

#### Click Create Image.

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

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

Create Port	~
Info Security Groups	
Name	
Mgt-port	Description:
S Enable Admin State	You can create a port for the network. If you specify device ID to be attached, the device specified will be attached to the port created.
Device ID 😧	
Device Owner 🕑	
Specify IP address or subnet	
Fixed IP Address	•
Fixed IP Address* 0	
10.106.36.xx	
MAC Address 😧	
☑ Port Security Ø	
VNIC Type 🚱	
Normal	•

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

Drainat								-,		
Project		*	Proj	ject / Network / Netw	vorks / public					
	API	Access								
	Compute	>	pu	blic						Edit Network 💌
	Volumes	>								
	Network	~	Ove	erview Subnets	Ports					
	Network T	одноду	Por	ts				lter	Q + Create Port	1 Delete Ports
		-								
	N	etworks	Displ	aying 12 items						
	N	etworks Routers	Displ	aying 12 items Name	Fixed IPs	MAC Address	Attached Device	Status	Admin State	Actions
	N Security	etworks Routers Groups	Displ	aying 12 items Name Mgt-Port	Fixed IPs <ul> <li>10.106.36.41</li> </ul>	MAC Address fa:16:3e:24:8a:8c	Attached Device	Status Down	Admin State	Actions Edit Port 💌
	N Security Floa	etworks Routers Groups ting IPs		Aying 12 items Name Mgt-Port (0b1273e8-1205)	Fixed IPs 10.106.36.41 10.106.36.31	MAC Address fa:16:3e:24:8a:8c fa:16:3e:c4:bc:eb	Attached Device Detached compute:compute1	Status Down Active	Admin State	Actions Edit Port V Edit Port V
C	N Security Floa Dbject Store	etworks Routers Groups ting IPs Trunks		aying 12 items Name Mgt-Port (0b1273e8-1205) test1	Fixed IPs • 10.106.36.41 • 10.106.36.31 • 10.106.36.36	MAC Address fa:16:3e:24:8a:8c fa:16:3e:c4:bc:eb fa:16:3e:52:24:8b	Attached Device Detached compute compute1 compute.compute2	Status Down Active Active	Admin State UP UP UP	Actions Edit Port • Edit Port • Edit Port •

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

Cancel

Create

Create OpenStack instance to enable config-drive and pass the user\_data.

3. Log in to OpenStack and configure Instances.

Project		~	Pro	ject / Compute / In:	stances										
	Compute	API Access	Ins	stances											
		Overview													
		Instances					Instance ID = •				Filter	& Laund	ch Instance	🛱 Delete Instan	ces More Actions -
		Images	Disp	laying 9 items											
		Key Pairs	0	Instance Name	Image	IP Address	Flavor	Key	Status		Availability	Task	Power	Age	Actions
					Name			Pair			Zone		State	190	Actions
	Ser	ver Groups	0	router_image	Name test_linux	10.106.36.43	m1.mediur	Pair	Active	÷.	Zone compute1	None	State	1 day, 5 hours	Create Snapshot -
	Ser Volumes Network	ver Groups	0	router_image sdwan-11configd ata	Name test_linux sdwan-finalti ny	10.106.36.43	m1.mediur	Pair	Active	е е	Zone compute1 compute2	None	State Running Running	1 day, 5 hours 1 week, 1 day	Create Snapshot - Create Snapshot -
	Ser Volumes Network Object Store	ver Groups		router_image sdwan-11configd ata sdwan-release11	Name test_linux sdwan-finalti ny sdwan-finalti	10.106.36.43 10.106.36.36 10.106.36.31	m1.mediur m1.large m1.large	Pair	Active Active Active	ч 9 9	Zone compute1 compute2 compute1	None None	State Running Running Running	1 day, 5 hours 1 week, 1 day 1 week, 1 day	Create Snapshot     •       Create Snapshot     •       Create Snapshot     •

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

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

## NOTE

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

> :	admin	sdwan-finaltiny	Image	Active	Public	No	QCOW2	1.33 GB	Launch -
> :	admin	sdwan_mtu_check	Image	Active	Public	No	QCOW2	1.32 GB	Launch -
> :	admin	sdwan_priv	Image	Active	Public	No	QCOW2	1.29 GB	Launch -

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

Launch Instance		×
Details	Please provide the initial hostname for the instance, the availability zone where count. Increase the Count to create multiple instances with the same settings.	it will be deployed, and the instance
Source *	Instance Name *	Total Instances
Flavour *	sdwan-openstack	(30 Max)
Networks *	Description	40%
Network Ports	Availability Zone	11 Current Usage
Security Groups	Any Availability Zone \$	18 Remaining
Key Pair	Count *	
Configuration	1	
Server Groups		
Scheduler Hints		
Metadata		
X Cancel	< Back	Next >

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

ails Irce *	Instance source is the tem (image snapshot), a volum creating a new volume.	plate used to create an instanc e or a volume snapshot (if enab	e. You can use an im bled). You can also cl	hage, a snapshot of ar hoose to use persister	i instance ht storage by
	Select Boot Source		Create New Vo	lume	
/our *	Image	\$	Yes No		
works *	Allocated				
ork Ports	Name L	Jpdated Size	Туре	Visibility	
/ Groups		Select an item from	n Available items bel	ow.	
	✓ Available 10				Select
ation	Q Click here for filters	or full text search.			
oups	Name	Updated	Size	Type Visibi	lity
its	> cirros	8/7/19 9:25 PM	12.65 MB	qcow2 Public	•
	> sdwan-finaltiny	11/7/19 10:42 AM	1.33 GB	qcow2 Public	•
	> sdwan_mtu_check	8/19/19 1:34 PM	1.32 GB	qcow2 Public	•
	> sdwan_priv	11/5/19 10:34 AM	1.29 GB	qcow2 Public	<b>^</b>
	SDWAN_VPX_IMG_N	EW 8/8/19 8:31 PM	1.31 GB	qcow2 Public	•
	> test_branch_1	10/4/19 10:07 AM	1.72 GB	qcow2 Public	<b>^</b>
	> test_brnach_2	10/4/19 10:08 AM	1.72 GB	qcow2 Public	•
	> test_dynamips	10/4/19 10:06 AM	1.72 GB	qcow2 Public	<b>^</b>
	> test_linux	10/4/19 10:07 AM	1.72 GB	qcow2 Public	•
	> test_mcn	10/4/19 10:08 AM	1.72 GB	qcow2 Public	•

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

#### NOTE

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

Administrators are responsible for creating and managing flavours. Click the arrow (at the right side) to allocate.
etails	Flavours manage Allocated	the sizing fo	or the comp	ute, memory an	id storage capac	ity of the instance.		
ource *	Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public	
lavour	> m1.large	4	8 GB	80 GB	80 GB	0 GB	Yes	4
etworks *	✓ Available	4						Select
etwork Ports	Q Click here	e for filters or	r full text sea	arch.				50.00
ecurity Groups	Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public	
ey Pair	> m1.tiny	1	512 MB	1 GB	1 GB	0 GB	Yes	1
onfiguration	> m1 small	1	2 GB	20 GB	20 GB	0 GB	Yes	
erver Groups	· · · · · · · · · · · · · · · · · · ·		2 00	20 00	20 00	0.05	100	
cheduler Hints	> m1.medium	2	4 GB	40 GB	40 GB	0 GB	Yes	1
letadata	> m1.xlarge	8	16 GB	160 GB	160 GB	0 GB	Yes	1

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

#### NOTE

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

ails	Networks provide the com	nunication channels for instan	ces in the cloud	Ι.			
Irce *	✓ Allocated ①			Select	networks fro	om those list	ed b
	Network	Subnets Associated	Shared	Admin	State	Status	
vour	¢1 ≯ public	public_subnet	Yes	Up		Active	
works	Ausilabla 🔿						
work Ports	V Available 30				Selec	t at least on	e ne
urity Groups	Q Click here for filters	or full text search.					
Pair	Network	Subnets Associa	ted	Shared	Admin State	Status	
figuration	> 08c39ca9-c86e-4e80- 775497069c	8dd2-5b 09408ac1-6dfb-43 34c128f5280c	81-bd2b-	No	Up	Active	
ver Groups	> 0ce9e8b1-ad5d-4210 917c827c17	-87dc-62 76268f54-7faf-45f b97fb72e3d6b	f-ae2a-	No	Up	Active	
adata	> 26a6e41d-6f64-4f6b-t 938d9a669	0510-810 c81c3a0e-e84e-4 3300b8e7323c	6b1-9e29-	No	Up	Active	
	> 272165f0-443b-4f81-5 9e2ea0fa3	9358-38a 373b775b-9576-4 9011362284da	84d-abd8-	No	Up	Active	
	> test_4	subnet_4		No	Up	Active	
	> 8b69e4a3-c47a-4821- aca96a4fe9	bb17-09 ab3c53f6-ca4b-49 7c444b21c257	958-aedf-	No	Up	Active	
	> test_1	subnet_1		No	Up	Active	
	> Hw_provider3_vlan20	provider3_subnet		No	Up	Active	
	f1d4edbe-8272-400c- 50864eecdf	bba1-c3 366f5024-cf0a-46 c3fe946df958	48-8053-	No	Up	Active	
	f3158a09-c8dc-421a- 14860b955	9e8f-048 736e9da4-7526-4 666071df24f8	072-aa93-	No	Up	Active	
	> test_3	subnet_3		No	Up	Active	
	> network_ipv6	subnetwork_ipv6 ipv4_subnet		No	Up	Active	

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

NOTE

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

Details	Ports provide extra communication channels of both.	nels to your instances. You can se	lect ports instead o	of networks or a mix
Source *	✓ Allocated 1		Select ports	from those listed below
lavour	Name IP		Admin State	Status
etworks	\$1 > tiny_mgmt 10.106.36.4	4 on subnet public_subnet	Up	Down
etwork Ports	V Available 31			Select or
ecurity Groups	Q Filter			
Cey Pair	Name	IP	Admin State	Status
erver Groups	> 3865f021-d8df-40a9-964a-7bb7f372	28 192.168.234.239 on subnet	Up	Down
cheduler Hints	3f7888d2-dd2b-487d-ad88-6cf3261 bf8b	e 192.168.234.113 on subnet	Up	Down <b>↑</b>
letadata	> 7847377d-6f82-4a7f-9e8d-26703bfd b0b	7 192.168.234.240 on subnet	Up	Down
	> 2bd26300-4af2-4503-8ec8-728ad59 7c5f	192.168.237.88 on subnet	Up	Down
	<ul> <li>6ca1aeab-4b38-41f3-86cc-8973a3b</li> <li>3bd</li> </ul>	ofc 192.168.240.223 on subnet	Up	Down
	> 9dc0d02b-7933-4689-92a3-18c317 c7c0d	7 192.168.240.251 on subnet	Up	Down
	> c378ba39-0c61-4e35-8a2c-0419fa8	192.168.240.4 on subnet	Up	Down
	> 958ad235-94b0-4ccd-8f07-88539b0 b584	<sup>25</sup> 172.16.22.1 on subnet	Up	Down
	> Mgt-Port	10.106.36.41 on subnet public_subnet	Up	Down

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

Launch Instance		×
Details	You can customise your instance after it has launched using th analogous to "User Data" in other systems.	e options available here. "Customisation Script" is
Source *	Load Customisation Script from a file	
	Choose file No file chosen	
Flavour	Customisation Script (Modified)	Content size: 213 bytes of 16.00 KB
Networks	#config	
Network Ports	management_jp address 10.106.36.43	
Security Groups	netmask 255.255.255.0 gateway 10.106.36.1	
Key Pair	dns	
Configuration	Disk Partition	
Server Groups	Automatic	\$
Scheduler Hints	Configuration Drive	
Metadata		
× Cancel		< Back Next > Caunch Instance

13. Click Launch Instance.

# Configure LTE functionality on 210 SE LTE appliance

#### August 24, 2022

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

#### Note

The LTE connectivity depends on the SIM carrier or service provider network. For information on how to configure and manage LTE sites in your network, see LTE firmware upgrade.

## **Getting started with Citrix SD-WAN 210-SE LTE**

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

#### Note:

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

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

Note

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

SIM Card	
Refresh SIM Card	

- 4. Configure the APN settings. In the SD-WAN GUI navigate to Configuration > Appliance Settings
   > Network Adapters > Mobile Broadband > APN settings.
  - **Note:** Obtain the APN information from the carrier.

APN Settings		
APN:	fast.t-mobile.com	
Username:	demo-user1	
Password:	•••••	
Authentication:	None	~
Change APN Se	ettings	

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

You can view the Mobile broadband settings status information.

IP Address	Ethernet Mobi	le Broadband		
Status Info				0
Modem		Cellular network	Network	Refresh
Operating Moder	online	Home Network IDEA	ID Address (Schwarze 10 72 220 160/10 72 220 161	
IMEI Number:	359075062410393	Radio Interface: Ite	Primary/Secondary DNS: 112.110.241.1/8.8.8.8	
Active SIM:	SIM One	Signal Strength: Good		
IMSI Number:	404446068985937	Session State: connecte	4	
ICCID Number:	89911100001445614	166 APN Name: internet		
Card State (SIM On	e): present			
				Detailed info

The following are some useful status information:

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

IP Address	Ethernet	Mobile Broadband				
Status Info						0
Modem						Refresh
Manufacturen Operating Model Software Version: Model: Type Hardware Revisions: Expected Data Formur PRL Version PRL Version PRL Version ESN Number MED Number: IMED Number: IMED Number: IMED Number: IMED Number: MED Software Version: Software Version:	Sierra Wir online .2.5.1.c1-0 EM7430 210-LTE-R 1.0 traw-ip 0 0 0 35907506 35907506 89911100 40444606 SWI9X300 .2.5.1.c1-0	eless, Incorporated 0168-M9635TAAAANAZ 2 taneous-cs-ps 2410393 241039 001445614166 9985937 ;02.33.00, r8209 CARR	M-1 MD-EV-FRMWR2 2019/08/28 20:59:30 IM-1			
Cellular Network			Call Statist	tics		
Home Network: Roaming Status: Session State: Card State:	IDEA off connected present	I	Call Status:		connected	
<b>RF Information</b>			Profile			
Radio Interface: Active Band Class: Active Channel: Signal Strength:	lte eutran-3 1405 Good		PDP Type: Authenticatic Profile Name IP Address Gateway Add Primary DNS Secondary D	on: :: dress: i: iNS:	None Internet 10.73.220.160 10.73.220.161 112.110.241.1 8.8.8.8	Show less

## SIM PIN

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

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

SIM PIN	
SIM PIN Status	
PIN State: Enabled and Not Verified PIN Tries: 3 PUK Tries: 10	
Disable PIN Verify PIN Modify PIN	

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

	×
SIM PIN:	]
Verify PIN	
Verify PIN	

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

PIN
I <u>PIN Status</u>
State: Enabled and Verified
Tries Remaining: 3
Tries Remaining: 10
able PIN Verify PIN Modify PIN

#### **Disable SIM PIN**

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

SIM PIN	
SIM PIN Status	
PIN State: Enabled and Verified PIN Tries Remaining: 3 PUK Tries Remaining: 10	
Disable PIN Verify PIN Modify PIN	
SIM PIN:	
Disable	

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

#### **Enable SIM PIN**

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

SIM PIN	
SIM PIN Status	
PIN State: Disabled PIN Tries: 3 PUK Tries: 10	
Enable PIN Verify PIN Modify PIN	

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

	×
SIM PIN:	
Enable	

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

SIM PIN	
SIM PIN Status	
PIN State: Enabled and Not Verified PIN Tries: 3 PUK Tries: 10	
Disable PIN Verify PIN Modify PIN	

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



#### **Modify SIM PIN**

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

SIM PIN	
SIM PIN Status	
PIN State: E	nabled and Verified
PIN Tries Remaining: 3 PUK Tries Remaining: 1	0
Disable PIN Verify F	IN Modify PIN

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

	د ا
Old SIM PIN:	
New SIM PIN:	
Confirm New SIM PIN:	

#### **Unblock SIM**

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



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

Note:

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

#### Citrix SD-WAN 11.5

Configuration > Appliance Settings > Network Adapters			
IP Address	Ethernet	Mobile Broadband	
Status Info			
This SIM Card is Permanently Blocked. Please contact the carrier service for a new SIM card.			

#### **Manage Firmware**

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

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

Manage Firmware	
Filename: Choose File No file chosen	Upload
Available Firmwares	
Delete Apply	

## **Network Settings**

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



## Roaming

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

#### Citrix SD-WAN 11.5

Roaming		
Roaming: Disabled	~	
Apply		

## Enable/Disable modem

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

## **Reboot modem**

Reboots the modem. It can take up to 3-5 minutes for the reboot operation to complete.

#### **Refresh SIM**

Use this option when you hot swap the SIM card to detect the new SIM card by the 210-SE LTE modem.

Manage Firmware
Filename: Choose File No file chosen Upload
Available Firmwares
AUTO-SIM V
Delete
Enable/Disable Modem
Disable Mobile Broadband
Reboot Modem
Reboot Modem
SIM Card
Refresh SIM Card

## Configure the LTE functionality using CLI

To configure the 210-SE LTE modem using the CLI.

- 1. Log into the Citrix SD-WAN appliance console.
- 2. At the prompt, type the user name and password to gain CLI interface access.

3. At the prompt, type the command **lte**. Type **>help**. This displays the list of LTE commands available for configuration.

site210>lte		
lte>help		
status	#	Show status
show	#	Show settings
disable	#	Disable LTE modem
enable	#	Enable LTE modem
apn <apn> [<user name=""> [<password> [<pap]< td=""><td>CHA</td><td>AP PAPCHAP&gt;]]]</td></pap]<></password></user></apn>	CHA	AP PAPCHAP>]]]
sim-power <off on reset></off on reset>	#	Off, on, reset SIM card power
sim-pin <show></show>	#	SIM card pin status
<pre>sim-pin <verify disable enable> <sim pin=""></sim></verify disable enable></pre>	+ #	Verify/Disable/Enable SIM card PIN
sim-pin <modify> <old pin=""> <new pin=""></new></old></modify>	#	Modify SIM card PIN
sim-pin <unblock> <sim puk=""> <sim pin=""></sim></sim></unblock>	#	Unblock SIM card PIN
reboot	#	Reboot modem
ping	#	Check if modem manager ready
list-fw	#	List available firmware
apply-fw <fw></fw>	#	Apply the specified firmware

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

Command	Description
Help {lte>help}	Lists the available LTE commands and parameters
Status {lte>status}	Displays LTE connectivity status
Show {Ite>show}	Displays LTE settings
Disable {lte>disable}	Disables LTE modem
Enable {lte>enable}	Enables LTE modem
Apn {lte>apn}	Configures APN settings information
Sim-power off, on, reset>{lte>sim-power off,on,reset} SIM PIN {lte>sim-pin}	Powers off SIM card, Power on SIM card, Refresh SIM card Powers off SIM card, Power on SIM card, Refresh SIM card
Reboot {Ite>reboot}	Restarts LTE modem
Ping {lte>ping}	Pings LTE modem
List-fw {lte>list-fw}	Lists firmware available on the R1 or R2 LTE modems
Apply-fw {lte>apply-fw}	Applies firmware specific to a carrier

## Zero-touch deployment over LTE

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

- 1. Install the antenna and the SIM card for the 210-SE LTE appliance.
- 2. Ensure that the SIM card has an activated data plan.
- 3. Ensure that the management port is not connected.
  - If the management port is connected, disconnect the management port and then restart the appliance.
  - If a static IP address on the Management Interface is configured, you need to configure the Management Interface with DHCP, apply the configuration, and then disconnect the Management port, and restart the appliance.
- 4. Ensure that the 210-SE appliance configuration has the internet service defined for the LTE interface.

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

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

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

## LTE REST API

For information about the LTE REST API, navigate to the SD-WAN GUI and go to **Configuration > Appliance Settings >NITRO API**. Click **Download Nitro API** Doc. The REST API for SIM PIN functionality is introduced in Citrix SD-WAN 11.0.

#### Citrix SD-WAN 11.5

Dashboard Monitoring	Configuration
- Appliance Settings	Configuration > Appliance Settings > NITRO AP
<ul> <li>Administrator Interface</li> <li>Logging/Monitoring</li> <li>Network Adapters</li> <li>Net Flow</li> <li>App Flow</li> <li>SNMP</li> </ul>	CITRIX NetScaler SD-WAN NITRO API DOC
+ Virtual WAN	
+ System Maintenance	

## **AT commands**

AT commands help in monitoring and troubleshooting LTE modem configuration and status. AT is the abbreviation for **ATtension**. As every command line starts with **at**, they are called AT commands. Citrix SD-WAN platform models that support LTE support running AT commands. AT commands are modem specific and therefore the list of AT commands varies across the platforms.

To run AT commands, perform the following steps:

- 1. Log into the Citrix SD-WAN appliance console.
- 2. At the prompt, type the user name and password to gain CLI interface access.
- 3. At the prompt, type **lte**.
- 4. Enter **at** and then enter the AT command.

The following is an example:

- at at+cpin Provides SIM status information.
- at at!gstatus Provides LTE modem status information.

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

• at at!impref? - Provides modem firmware and network carrier information.

```
lte> at at!impref?
Running at!impref? command
AT command state: success
  ! TMPREF:
  preferred fw version:
                           00.00.00.00
  preferred carrier name:
                           AUTO-SIM
  preferred config name:
                           AUTO-SIM 000.000 000
  preferred subpri index:
                           000
   current fw version:
                           02.33.03.00
   current carrier name:
                           VERIZON
   current config name:
                           VERIZON 002.079 001
   current subpri index:
                            000
 OK
success
```

# Configure LTE functionality on 110-LTE-WiFi appliance

#### August 24, 2022

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

Note

- The LTE connectivity depends on the SIM carrier or service provider network.
- For information on how to configure and manage all the LTE sites in your network, see LTE firmware template.

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

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

Note

Citrix SD-WAN 110-LTE-WiFi appliance has two standard (2FF) SIM slots. To use Micro (3FF) and Nano (4FF) size SIMs, use a SIM adapter. Snap the smaller SIM into the adapter. You can obtain the adapter from Citrix as a Field Replaceable Unit (FRU) or from the SIM provider.

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

#### Note

Obtain the APN information from the carrier.

APN Setting	s	
SIM:	SIM One	•
APN:	fast.t-mobile.com	
Username:		
Password:		
Authentication	None	•
Character ADN	·	
Change APN	Settings	

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

Note

All these fields are optional.

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

You can view the Mobile broadband settings status information.

IP Address	Ethernet	Mobile Bro	badband				
Status Info							6
Modem			Cellular network		Network		Refresh
Operating Mode:	online		Home Network:	airtel	IP Address/Gateway:	100.105.88.189/100.105.88.190	
IMEI Number:	8676980403	97609	Radio Interface:	Ite	Primary/Secondary DNS:	125.22.47.102/59.144.144.106	
Active SIM:	SIM One		Signal Strength:	Excellent			
IMSI Number:	4044509860	42323	Session State:	connected			
ICCID Number:	8991000902	2637718627f	APN Name:				
Card State (SIM One	present		Card State (SIM Two)	absent			
							Detailed info

The following are some useful status information:

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

#### **SIM Preference**

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

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

• **SIM Two**: Only SIM Two is used, irrespective of the SIM state on both the SIM slots. SIM Two is always active.

SIM Preference	
Preffered SIM: SIM One preferred •	
Apply	

#### SIM PIN

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

Note

The SIM PIN operations are applicable for the active SIM only.

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

SIM PIN
SIM PIN Status
PIN State: enabled-not-verified
PIN Retries Remaining: 3
POK ketries kemaining: 10
Disable PIN     Verify PIN     Modify PIN     Unblock

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

×

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

SIM PIN	
SIM PIN Status	
PIN State:	enabled-verified
PIN Retries Remaining:	3
PUK Retries Remaining	: 10
Disable PIN Verify F	IN Modify PIN Unblock

#### **Disable SIM PIN**

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

SIM PIN
SIM PIN Status
PIN State: enabled-verified PIN Retries Remaining: 3
PUK Retries Remaining: 10
Disable PIN Verify PIN Modify PIN Unblock

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

	×
SIM PIN:	
Disable	

#### Enable SIM PIN

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

SIM PIN	
SIM PIN Status	
PIN State	disabled
PIN Retries Remaining	3
PUK Retries Remaining	: 10
Enable PIN Verify P	IN Modify PIN Unblock

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

	×
SIM PIN:	
Enable	

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

IM PIN	
IM PIN Status	
IN State: enabled-not-verified IN Retries Remaining: 3 UK Retries Remaining: 10	
Disable PIN Verify PIN Modify PIN Unblock	

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

-

#### **Modify SIM PIN**

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



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

#### **Unblock SIM**

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

#### Citrix SD-WAN 11.5

IP Addres	s	Ethernet	Mobile Broadband
Status Inf	o		
This SIM Ca	urd is B	locked. Please	contact the carrier service f
PIN State:	Block	ed	
PIN Tries: PUK Tries:	3 10		
Unblock			

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

×

#### Note:

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

Configuration >	Appliance Setting	s > Network Adapters	
IP Address	Ethernet	Mobile Broadband	
Status Info	Status Info		
This SIM Card is	This SIM Card is Permanently Blocked. Please contact the carrier service for a new SIM card.		

## **Network Settings**

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

Network Settin	gs	
SIM:	3G	\$
Network Typ	4G	Ð
	Both	

#### Roaming

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

SIM:	3G	•
Network Typ	/ 4G	Ð
	Both	

#### Enable/Disable modem

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

Enable/Disable Modem	
Enable Mobile Broadband	

#### **Reboot modem**

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

## **Refresh SIM**

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

Note

The Refresh SIM operation is applicable for the active SIM only.

SIM Card (SIM One)

Refresh SIM Card

## **Configure the LTE functionality using CLI**

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

- 1. Log into the Citrix SD-WAN appliance console.
- 2. At the prompt, type the user name and password to gain CLI interface access.

3. At the prompt, type the command **lte**. Type **>help**. This displays the list of LTE commands available for configuration.

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

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

Command	Description
Help {lte>help}	Lists the available LTE commands and parameters
Status {Ite>status}	Displays LTE connectivity status
Show {Ite>show}	Displays LTE settings
Disable {lte>disable}	Disables LTE modem
Enable {lte>enable}	Enables LTE modem
Apn {lte>apn}	Configures APN settings information
Sim-power off, on, reset>{lte>sim-power off,on,reset} Select [1l2] [1l2] {lte>select [1l2] [1l2]}	Powers off sim card, Power on sim card, Refresh sim card Select the SIM for LTE modem.
SIM-prefer {lte>sim-prefer}	Select the SIM preferred or to be used.
SIM PIN {lte>sim-pin}	SIM PIN related operations
Reboot {Ite>reboot}	Restarts LTE modem

## Note

The firmware related operations are not supported on the 110-LTE-WiFi appliance.

## Zero-touch deployment over LTE

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

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

- 1. Install the antenna, power ON the appliance, and insert the SIM card.
- 2. Ensure that the SIM card has an activated data plan.
- 3. Ensure that the management/data port is not connected.
  - If the management/data port is connected, disconnect the management/data port.
  - If a static IP address on the management/data Interface is configured, you must configure the management/data interface with DHCP, apply the configuration, and then disconnect the management/data port.
- 4. Ensure the 110-LTE-WiFi appliance configuration has the internet service defined for the LTE interface.

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

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

Connect the management/data port to the Internet and use the standard zero-touch deployment procedure that is supported on all other non-LTE platforms.

## LTE REST API

For information about the LTE REST API, navigate to the SD-WAN GUI and go to **Configuration > Appliance Settings >NITRO API**. Click **Download Nitro API** Doc. The REST API for SIM PIN functionality is introduced in Citrix SD-WAN 11.0.

#### Citrix SD-WAN 11.5

Dashboard Monitoring	Configuration
- Appliance Settings	Configuration > Appliance Settings > NITRO AP
<ul> <li>Administrator Interface</li> <li>Logging/Monitoring</li> <li>Network Adapters</li> <li>Net Flow</li> <li>App Flow</li> <li>SNMP</li> </ul>	CITRIX NetScaler SD-WAN NITRO API DOC
+ Virtual WAN	
+ System Maintenance	

## **AT commands**

AT commands help in monitoring and troubleshooting LTE modem configuration and status. AT is the abbreviation for **ATtension**. As every command line starts with **at**, they are called AT commands. Citrix SD-WAN platform models that support LTE support running AT commands. AT commands are modem specific and therefore the list of AT commands varies across the platforms.

To run AT commands, perform the following steps:

- 1. Log into the Citrix SD-WAN appliance console.
- 2. At the prompt, type the user name and password to gain CLI interface access.
- 3. At the prompt, type **lte**.
- 4. Enter **at** and then enter the AT command.

The following is an example:

• at at+cpin – Provides SIM status information.

# **Configure external USB LTE modem**

August 24, 2022

You can connect an external 3G/4G USB modem on certain Citrix SD-WAN appliances. The appliances use the 3G/4G network along with other connections to form a virtual network that aggregates bandwidth and provides resiliency. If there is a connectivity failure on the other interfaces, traffic is automatically redirected through the USB LTE modem. The following appliances support an external USB modem:

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

The Citrix SD-WAN 210 SE LTE and Citrix SD-WAN 110 LTE Wi-Fi SE appliances have a built-in LTE modem. Active dual LTE is supported on these appliances.

CDC Ethernet, MBIM, and NCM are the three types of external USB modems supported. You can configure the **APN** settings and Enable/Disable modem on MBIM and NCM USB modems. Mobile broadband operations are not supported on CDC Ethernet USB modems.

Note

The external LTE dongles with modem type as MBIM do not work on Citrix SD-WAN 2100 platform.

## Connecting the USB modem

Enable and test the USB modem according to the guidelines provided by your wireless carrier.

Perquisites for external LTE modem:

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

Note

• The Citrix SD-WAN appliances support only one USB LTE dongle at a time. If more than one

USB dongle is plugged in, unplug all the dongles and plug in only one dongle.

- The Citrix SD-WAN appliances do not support user name and password for USB modems. Ensure that the user name and password feature are disabled on the modem during setup.
- Unplugging or rebooting an external MBIM dongle impacts the internal LTE modem data session. This is an expected behavior.
- When an external LTE modem is plugged-in, the SD-WAN appliance takes about 3 minutes to recognize it.

To view the external modem details, in the appliance UI navigate to **Configuration > Appliance Set**tings > Network Adapters > Mobile Broadband. Select External Modem as the modem type.

Dashboard Monitoring	Configuration
- Appliance Settings	Configuration > Appliance Settings > Network Adapters
Administrator Interface Logging/Monitoring	IP Address Ethernet Mobile Broadband
Network Adapters	Modem Type
- App Flow/IPFIX - SNMP	Select Modem Type External Modem
Licensing Fallback Configuration	Status Info
+ Virtual WAN	Product ID: 9030
+ System Maintenance	Vendor ID: 1410 Manufacturer Name: Novatel Wireless Product Name: MiFi USB730L

## Note

The LTE USB dongle model number is not displayed in **Status Info** section.

## **Mobile broadband operations**

Operations that are supported on CDC Ethernet and MBIM / NCM external modems:

Operations	External modem - CDC Ethernet	External modem - MBIM and NCM
SIM preference	No	No
SIM PIN	No	No
APN settings	No	Yes
Network settings	No	No
Roaming	No	No

Operations	External modem - CDC Ethernet	External modem - MBIM and NCM
Manage firmware	No	No
Enable/Disable modem	No	Yes
Reboot modem	No	No
Refresh SIM	No	No

#### Configure the external USB modem

You can configure an LTE sites using an external USB modem through Citrix SD-WAN Orchestrator service. For more infomation, see LTE firmware upgrade.

## Zero-touch deployment over LTE

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

- Insert the USB modem in the Citrix SD-WAN appliance. For more information, see Connecting the USB modem.
- Ensure that the SIM card on the USB modem has an activated data plan.
- Ensure that the management/data port is not connected. If the management/data port is connected, disconnect it.
- Ensure that the appliance configuration has the internet service defined for the LTE interface.

When the appliance is powered ON, the zero-touch deployment service uses the LTE-E1 port to obtain the latest SD-WAN software and configuration.

For information about zero-touch deployment through the SD-WAN Orchestrator service see, Zero Touch Deployment.

## **Supported USB modems**

#### The following modems are compatible with Citrix SD-WAN appliances.

#### Note

Citrix does not control the wireless carrier firmware updates. Therefore compatibility of new modem firmware to Citrix SD-WAN software is not guaranteed. The customer controls the modem firmware update. Citrix recommends testing a firmware update on a single site before pushing it across the entire network.

	Wireless Carrier/		Modem Type	
Region	Manufacturer	USB Modem	Supported	Interfaces
USA	Verizon	Global Modem	cdc_ether	4G only
1154	AT 2.T	USB730L	cdc other	4G only
	Alal	Modem USB800	cac_ettiel	40 0119

## **AT commands**

AT commands help in monitoring and troubleshooting LTE modem configuration and status. AT is the abbreviation for **ATtension**. As every command line starts with **at**, they are called AT commands. Citrix SD-WAN platform models that support LTE support running AT commands. AT commands are modem specific and therefore the list of AT commands varies across the platforms.

To run AT commands, perform the following steps:

- 1. Log into the Citrix SD-WAN appliance console.
- 2. At the prompt, type the user name and password to gain CLI interface access.
- 3. At the prompt, type **lte**.
- 4. Enter **at** and then enter the AT command.

The following is an example:

at at+cpin – Provides SIM status information.

# Deployments

#### August 24, 2022

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

- Deploying SD-WAN in Gateway Mode
- Inline Mode
- Deploying SD-WAN in PBR mode (Virtual Inline Mode)
- Dynamic Paths for Branch to Branch Communication
- WAN to WAN forwarding
- Building an SD-WAN Network
- Routing for LAN Segmentation

- Zero Touch Deployment
- Single Region Deployment
- Multi Region Deployment
- High Availability

# Checklist and how to deploy

#### August 24, 2022

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 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

# **Best practices**

#### August 24, 2022

This article outlines deployment best practices for the Citrix SD-WAN solution. It provides general guidance, advantages, use cases for the following Citrix SD-WAN deployment mode.

#### Edge/Gateway Mode

#### Recommendations

The following are the recommendations for the **Gateway** mode deployment:

- 1. The Gateway mode is best used for SD-WAN branches where router consolidation happens and customers are ready to allow SD-WAN to be the edge device terminating connections.
- 2. A great network architecture can be rendered with a scrupulous design when a project is built from scratch.

## Note

The Gateway mode can be used on the data center side for the existing projects with some infrastructure disruption.

#### Advantages/Use cases

The following are the advantages/use cases for the Gateway mode deployment:

- 1. Best use case for Router/Firewall/Network element consolidation at the customer branch.
- 2. Simple and easy LAN host management via DHCP.
  - Allows SD-WAN to become the next-hop and offer DHCP based IP addressing to all LAN hosts for data ports.
- 3. All connections terminate at the SD-WAN edge/gateway and management becomes easy.
- 4. SD-WAN is the focal point of edge routing and is steered of all traffic. The decisions are made on the edge to breakout or backhaul or overlay including the bandwidth/capacity accounting.
- 5. All LAN subnets hosts as the LAN hosts are allowed to have SD-WAN LAN VIP as the next-hop. If SD-WAN LAN connects to a core switch, you can run dynamic routing to get visibility to all LAN subnets.
- 6. Great flexibility for High Availability (HA) Strict recommendation for the gateway mode so that the site operates with an Active/Standby mode. Also, it helps to prevent traffic blackhole if the SD-WAN device goes down.
  - Switches available at the branch Parallel high availability can work in gateway mode.
  - Switches not available at the branch SD-WAN can also operate on SD-WAN edge high availability mode (fail-to-wire high availability mode) where the two SD-WAN boxes are daisy-chained to make use of fail-to-wire ports to act as a converged high availability pair.
- 7. Allow the Internet to be defined as **UNTRUSTED** interfaces which automatically create a dynamic NAT for breakout and source NAT the connection so the response comes back to SD-WAN.
- 8. Security considerations to **UNTRUSTED** interfaces are implied naturally, in that only ICM-P/ARP/UDP control packets on 4980 are allowed.

## Cautions

The following are the information that you need to be careful about in the Gateway mode:

- **Careful design and Network Architecture** Gateway mode might need careful design and networking considerations as the entire branch/edge networking is in SD-WAN. What to block, what to route, how to network LAN, how to terminate WANs, and so on.
- **Failure of Device** Edge mode cannot have the fail-to-wire capability. The entire branch goes down when the device is down.
- **Security Posture** As the routing is managed at the edge, the security postures such as firewall, breakout/backhaul considerations are crucial and that must be conceived with the customer.
- **High Availability** Fail-to-wire high availability must have some port availability considerations and depending on deployments might become tricky to design.
  - SD-WAN 110 is NOT an option as it does not have fail-to-wire ports.

For instance, if you need 2 WAN Links to operate, you need 5 ports including a dedicated port for the high availability interface including the LAN interface.

## Inline Mode – Fail-to-wire/Fail-to-block

## Recommendations

The following are the recommendations for the **Inline** mode deployment:

- 1. The inline mode is best for the branches where the existing infrastructure is not to be changed and SD-WAN sits transparently inline to the LAN segment.
- 2. Data center's can also employ inline fail-to-wire or inline parallel high availability as it is immensely important to ensure that the data center workloads are not blackholed due to device down/crash.

#### Advantages and use-cases

The following are the advantages/use cases for the Inline mode deployment:

- 1. Keeping the MPLS router therefore fail-to-wire is a lovely feature. Fail-to-wire capable devices enable seamless failover to underlay infrastructure if the box went down.
  - If your devices support fail-to-wire (SD-WAN 210 and above), this allows placing a single SD-WAN inline to hardware bypass the LAN traffic to the customer edge router when the SD-WAN crashes/goes down.
  - If the MPLS Links are present that yield a natural extension to the customer's LAN/Intranet, the fail-to-wire bridge-pair port is the best choice (fail-to-wire capable pairs) such that,

when the device crashes or goes down the LAN traffic is hardware bypassed to the customer edge router (still maintained the next hop).

- 2. Networking is simple.
- 3. SD-WAN sees all traffic through the inline mode, so it is the best-case scenario for the proper bandwidth/capacity accounting.
- 4. Few integration requirements as you need only an IP of the L2 segment. LAN segments are well known as you have an arm to the LAN interface. If you connect to a core switch, you can also run dynamic routing to get visibility to all LAN subnets.
- 5. Customer's expectations are that SD-WAN must blend into the existing infrastructure as a new network node (nothing else changes).
- 6. **Proxy ARP** –In inline mode, it is a blessing for SD-WAN to proxy ARP requests to LAN next-hop if the gateway went down or the SD-WAN interface towards next-hop went down.
  - Generally, in inline mode with bridge-pair (fail-to-block or fail-to-wire) with multiple WAN connections (MPLS/Internet), it is recommended to enable Proxy ARP for the bridge pair interface that connects the LAN hosts to their next-hop gateway.
  - For any reason when the next-hop is down or the SD-WAN interface to the next-hop is down rendering the gateway unreachable, SD-WAN acts as a proxy for ARP requests allowing the LAN hosts to still seamlessly send packets and use the remaining WAN connections that keep the virtual path up.
- 7. **High availability** If fail-to-wire is not an option, devices can be placed in parallel high availability (common LAN and WAN interfaces for the Active/Standby) devices to achieve redundancy.
  - If your appliances don't support fail-to-wire, like the SD-WAN 110, you have to go with inline parallel high availability that enables to have a standby device kick in if the primary went down.

## Cautions

The following are the information that you need to be careful about in the **Inline** mode:

- Plumbing network with two arms to the SD-WAN (LAN and WAN side), needs some downtime as the network must be plumbed in two arms.
- Must ensure if fail-to-wire is used, it is behind a customer edge router/firewall in a **TRUSTED** zone so that security is not compromised.
- MPLS QoS changes a little in this as the previous QoS policies might have depended on the source IP addresses or DSCP based which will now be masked because of an overlay.

- Care must be taken to repurpose the MPLS router with a well-designed SD-WAN specific reserved bandwidth with a specific DSCP tag, such that SD-WAN's QoS takes care of prioritizing traffic and sends out high priority applications immediately followed by other classes (but be able to account for the overall bandwidth reserved for SD-WAN on the MPLS router). MPLS queues are an alternative or MPLS with a single DSCP set on the auto path group that can take care of this.
- If the Internet interfaces are **TRUSTED** as the links terminate on the customer edge router, to use Internet service, you must write an exclusive dynamic NAT rule to enable internet breakout from the appliance.
- If the Internet links are the only WAN connections and still terminate on the customer edge router, it is still fine to bypass the connections if the customer edge router takes precautions to steer the packets via their existing underlay infrastructure.
  - Proper care must be taken to account for the flow of bypassing LAN traffic over bridgepair with an Internet connection and when the appliance is down. Since this is a sensitive enterprise Intranet traffic, in the eve of failure, the customer must know how to handle it.

## Virtual Inline/One-arm mode

## Recommendations

The following are the recommendations for the **Virtual Inline** mode deployment:

- 1. The virtual inline mode is best for data center networking as the SD-WAN network plumbing can be worked on parallel while the data center is serving its existing workloads with existing infrastructure.
- 2. SD-WAN is in a one-arm interface that is managed with an SLA tracking on VIPs. If the tracking goes down, the traffic resumes routing via existing underlay infrastructure.
- 3. Branches can also be deployed in virtual inline mode, however are more predominant with Inline/Gateway deployments.

#### Advantages and Use-cases

The following are the advantages/use cases for the **Virtual Inline** mode deployment:

- 1. Simplest and recommended way to network SD-WAN in the data center.
  - The virtual inline mode allows parallel network plumbing of SD-WAN with the head-end core router.

- The virtual inline mode allows us to easily define PBRs to divert LAN traffic must go through SD-WAN and get overlay benefits.
- 2. Seamless failover to underlying infrastructure if SD-WAN is to fail, and seamless forwarding to SD-WAN for overlay benefits under normal conditions.
- 3. Simple **Networking** and **Integration** requirements. The single one-arm interface from headend router to SD-WAN in virtual inline.
- 4. Easy to deploy dynamic routing in **Import only mode** (export nothing) to get visibility of LAN subnets so they can be sent to remote SD-WAN peer appliances.
- 5. Easy to define PBR on the routers (1 per WAN VIP) to indicate how to choose the physical.

## Cautions

The following are the information that you need to be careful about in the **Virtual Inline** mode:

- Proper care must be taken to distinctly MAP the SD-WAN logical VIP of a WAN link defined to the right physical interface (else this might cause undesirable issues in WAN metric assessment and choice of wan paths).
- Proper design considerations are to be made to know if all traffic is diverted via SD-WAN or only specific traffic.
- This means SD-WAN must be dedicated some share of bandwidth exclusively for itself that must be set on the interfaces such that SD-WAN's capacity is not used by other non-SD-WAN traffic causing undesirable outcomes.
  - Bandwidth accounting issues and congestion issues might occur if SD-WAN WAN links capacity is defined incorrectly.
- Dynamic routing can cause some issues if improperly designed where if the SD-WAN routes data center and branch VIPs are exported to the headend and if routing is influenced towards SD-WAN, overlay packets start looping and cause undesirable outcomes.
- Dynamic routing must be properly administered considering all potential factors of what to learn/what to advertise.
- One-arm physical interface might become a bottleneck sometimes. Needs some design considerations in those lines as it caters to both upload/download and also acts as LAN to LAN and LAN to WAN/WAN to LAN traffic from SD-WAN.
- Excessive LAN to LAN traffic might be a point to note during design.
- If the dynamic routing is not used, there must be proper care if administering all LAN subnets, which if not, might cause undesirable routing issues.
• There are potential routing loop issues if you define some default route (0.0.0/0) on the SD-WAN in the virtual inline to point back to the headend router. In such situations, if the virtual path went down, any traffic coming from the data center LAN (like monitoring traffic) is looped back to the headend and back to SD-WAN causing undesirable routing issues (If the virtual path is down, the remote branch subnets become reachable **NO** causing the default route to be HIT, that causes the loop issues).

# **Gateway mode**

## August 24, 2022

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

- To view all traffic to and from the WAN
- To perform local routing

Gateway deployment mode is supported on Citrix SD-WAN Orchestrator service. For more information, see Interfaces.



## Note

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

In the **Inline** mode, the SD-WAN appliance appears to be an Ethernet bridge. Most of the SD-WAN appliance models include a fail-to-wire (Ethernet bypass) feature for inline mode. If power fails, a relay closes and the input and output ports become electrically connected, allowing the Ethernet signal to pass through from one port to another. In the fail-to-wire mode, the SD-WAN appliance looks like a cross-over cable connecting the two ports. Inline mode used to integrate into already well-defined networks.



This article provides step-by-step procedure to configure an SD-WAN appliance in Gateway mode in a sample network setup. Inline deployment is also described for the branch side to complete the configuration. A network can continue to function if an Inline device is removed, but loses all access if the Gateway device is removed.

## Topology

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



## Data Center in gateway deployment



## Branch in inline deployment

## Data center site gateway mode configuration

Following are the high-level configuration steps to configure data center site Gateway deployment:

- 1. Create a DC site.
- 2. Populate Interface Groups based on connected Ethernet interfaces.
- 3. Create Virtual IP address for each virtual interface.
- 4. Populate WAN links based on physical rate and not burst speeds using Internet and MPLS Links.
- 5. Populate Routes if there are more subnets in the LAN infrastructure.

## To create 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.

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delet
0.0.10.9/24	INET_DC-WAN-1-4 (0)	Default_LAN_Zone			Trusted	Û
92.168.10.9/24	MPLS-DC-VWAN-1-2 (0)	Default_LAN_Zone	•		Trusted	Û
92.168.30.1/24	DC-LAN-1-1 (0)	Default_LAN_Zone			Trusted	圓

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.

or removed. Link Name: BR571-WL-1 Access Type: WAN Link Template: Public Internet  VAN black VAN	cause automatically generated Paths to this link t	c may o be added
Link Name: BR571-WL-1 Access Type: WAN Link Template: Public Internet • <a href="https://www.wanternet.org">wan to Lan</a> LAN to WAN Physical Rate (kbps): 10000 Set Permitted From Physical Auto Learn Permitted Rate (kbps): 10000 Permitted Rate (kbps): 10000	or removed.	
BR571-WL-1         Access Type:       WAN Link Template:         Public Internet          Physical Rate (kbps):         10000         Set Permitted From Physical       Auto Learn         Permitted Rate (kbps):         10000	Link Manage	
Access Type: WAN Link Template:          Public Internet          Physical Rate (kbps):       10000         Set Permitted From Physical       Auto Learn         Permitted Rate (kbps):       10000         10000       Image: Set Permitted From Physical         Permitted Rate (kbps):       10000         10000       Image: Set Permitted From Physical         Permitted Rate (kbps):       10000	BR571-WL-1	
Access Type: WAN Link Template:          Public Internet          Physical Rate (kbps):       10000         10000       Image: Set Permitted From Physical       Auto Learn         Permitted Rate (kbps):       10000         10000       Image: Set Permitted From Physical       Auto Learn         Permitted Rate (kbps):       10000         10000       Image: Set Permitted From Physical       Auto Learn		
LAN to WAN         Physical Rate (kbps):         10000         Image: Set Permitted From Physical         Auto Learn         Permitted Rate (kbps):         10000         Image: Set Permitted Rate (kbps):         10000         Image: Set Permitted Rate (kbps):         10000	Access Type: WAN Link Template:	
DAN to WAN     WAN to DAN       Physical Rate (kbps):     10000       10000     10000       Set Permitted From Physical     Auto Learn       Permitted Rate (kbps):     10000       10000     10000	Public Internet •	
Priysical Rate (kbps).     10000       Image: Set Permitted From Physical Auto Learn     Image: Set Permitted From Physical Auto Learn       Permitted Rate (kbps):     10000       10000     10000	Devriced Pate (Haw):	WAN to LAN
Set Permitted From Physical     Auto Learn       Permitted Rate (kbps):     10000	10000	10000
Set Permitted From Physical       Auto Learn         Permitted Rate (kbps):       10000		
Permitted Rate (kbps): 10000 Permitted Rate (kbps): 10000	🗷 Set Permitted From Physical 📃 Auto Lea	ern 🕑 Set Permitted From Physical 🔲 Auto Learn
10000	Permitted Rate (kbps):	Permitted Rate (kbps):
	10000	10000
Tracking IP Address: Autodetect Public IP	Tracking IP Address:	Autodetect Public IP
Tracking IP Address: Autodetect Public IP	10000 Tracking IP Address:	10000

## 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.

Ba	sic Settings						
	Note: Changin cause automat or removed.	g the access type of thi ically generated <b>Paths</b>	s <b>WAN Link</b> may to this link to be added				
	Link Name: BR571-WL-1						
	Access Type:	WAN Link Te	mplate:	1			
	LAN to WAN		-	WAN to LAN			
	Physical Rate (kb 10000	atas):		Physical Rate (kbp	s):		
	Set Permitter	d From Physical		Set Permitted	From Physical		
	10000	(cops).		10000	ops).		
	Name	Virtual Interface	IP Address	Gateway IP Address	Virtual Path Mode	Picky ARP	Delete
SJO	_DC-MPLS	MPLS-DC-WAN-1-2	192.168.10.9	192.168.10.1	Primary		

## **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.

+

					Search:			
Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	192.168.31.0/24	5	Local		192.168.30.2	0	0	Û
2	192.175.58.0/24	5	Virtual Path	BR571		0	0	Û
З	192.175.59.0/24	5	Virtual Path	BR572		0	0	Û
4	192.175.60.0/24	5	Virtual Path	BR573		0	0	Ē
5	192.175.61.0/24	5	Virtual Path	BR574		0	0	Û
6	192.175.62.0/24	5	Virtual Path	BR575		0	0	Û
7	172.111.64.5/24	5	Local			0	0	Ü
8	172.111.65.5/24	5	Local			0	0	Ü
9	0.0.0.0/0	65535	Passthrough			0	0	Ü
					•**	<	1	

#### 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 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.

T ID Address ( De Co	Mar II.	C	T-local to a	0.1.1.1	C	0.1.1
IP ADDress / Prenx	virtual interface	Firewall Zone	Loenbity	Private	Security	Delete
10.0.20.9/24	INET_BR-3-4 (0) •	Default_LAN_Zone	1		Trusted	Û
192.168.20.9/24	MPLS_BR-1-2 (0)*	Default_LAN_Zone			Trusted	Û
192.113.58.6/24 VirtualInterface-2		Default_LAN_Zone			Trusted	
Defease	1					

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.

Note: Char	nging the ac	cess type of this WAN I	ink may				
cause auto	matically ge	nerated <b>Paths</b> to this lin	k to be added				
or removed	I.						
Link Name:							
BR571-W	1						
Access Type	20	WAN Link Template:					
Public Int	ternet 🔹	<none></none>	•				
- LAN to WAN				WAN to LAN			
Physical Rate	e (kbps):			Physical Rat	e (kbps):		
10000				10000			
Set Dorm	itted From D	Devical Auto	0.00	Sat Darm	vitted From Dh	vsical	Auto Learn
(g) bet reini	itted from r		Lealin	(a) bet rem	intee from Fig	ysical	- Auto ceani
Permitted Ra	ate (kbps):			Permitted R	ate (kbps):		
10000				10000			
Tracking ID /	ddrass						
Tracking IP /	NUMICOS.			Autodet	ect Public IP		
				Public IP Ad	dress:		

## 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.

or removed.	laucany gen	elated Fat	is to this link	to be added				
Link Name:								
BR571-WL-	1							
Access Type:		WAN Link	Template:					
Private MP	PLS ▼	<none></none>		•				
LAN to WAN					- WAN to	LAN		
Physical Rate	(kbps):				Physical	Rate (kbps):		
10000					10000			
🗷 Set Permit	ted From Ph	iysical			🗷 Set F	Permitted From P	hysical	
Permitted Rate (kbps):					Permitte	ed Rate (kbps):		
10000								

## To populate routes

+

Routes are auto-created based on above configuration. In case there are more subnets specific to this remote branch office, then specific routes need to be added identifying which gateway to direct traffic to reach those back-end subnets.

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

## **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).

From Site:	From WAN Link:
DC_site	DC_site-MPLS
To Site:	To WAN Link:
BR_site	BR_site-MPLS .

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

# Inline mode

## August 24, 2022

This article provides the detail on configuring a branch with **Inline Deployment** mode. In this mode, the SD-WAN appliance appears to be an Ethernet bridge. Most of the SD-WAN appliance models include a **fail-to-wire** (Ethernet bypass) feature for inline mode. If power fails, a relay closes and the input and output ports become electrically connected, allowing the Ethernet signal to pass through from one port to another. In the fail-to-wire mode, the SD-WAN appliance looks like a cross-over cable connecting the two ports.

In the following diagram interfaces 1/1 and 1/2 are hardware bypass pairs and will fail-to-wire connecting the Core to the edge MPLS Router. Interfaces 1/3 and 1/4 are also hardware bypass pairs and will fail-to-wire connecting the Core to the edge Firewall. For more information on SD-WAN Orchestrator service-based Inline mode deployment, see Interfaces.



# Virtual inline mode

August 24, 2022

In virtual inline mode, the router uses routing protocol such as PBR, OSPF, or BGP to redirect incoming and outgoing WAN traffic to the appliance, and the appliance forwards the processed packets back to the router.

The following article describes the step-by-step procedure to configure two SD-WAN (SD-WAN SE) appliances:

- Data Center appliance in virtual inline mode
- Branch appliance in Inline mode
- Routing protocol must be configured either at the core switch or further upstream at the router. The router must monitor the health of the SD-WAN appliance so that the appliance can be bypassed if it fails.
- Virtual inline mode places the SD-WAN appliance physically out of path (one-arm deployment) that is, only a single Ethernet interface to be used (Example: Interface 1/5) with bypass mode set to fail-to-block (FTB).

Citrix SD-WAN appliance must be configured to pass traffic to the proper gateway. Traffic intended for the Virtual Path is directed towards the SD-WAN appliance and then encapsulated and directed to the appropriate WAN link.

## **Gather information**

Gather the following information required for configuring virtual inline mode:

- Accurate network diagram of your local and remote sites including:
  - Local and Remote WAN links and their bandwidths in both directions, their subnets, Virtual IP Addresses and Gateways from each link, Routes, and VLANs.

• Deployment Table

For information on SD-WAN Orchestrator service-based Virtual Inline mode deployment, see Interfaces.

The following is a sample network diagram and deployment table:

#### Data center topology –Virtual inline mode



## **Resolving audit errors**

After completing the configuration for Data Center and Branch sites, you will be alerted to resolve the audit errors on both DC and BR sites. Resolve the audit errors (if any).

# **Build an SD-WAN network**

#### August 24, 2022

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) 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



# **High availability**

## August 24, 2022

This topic covers the High Availability (high availability) deployments and configurations supported by SD-WAN appliances (Standard Edition).

Citrix SD-WAN appliances can be deployed in high availability configuration as a pair of appliances in Active/Standby roles. There are three modes of high availability deployment:

• Parallel Inline high availability

- Fail-to-Wire high availability
- One-Arm high availability

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

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

## High availability deployment modes

#### One-Arm mode:

In One-Arm mode, the high availability appliance pair is outside of the data path. Application traffic is redirected to the appliance pair with Policy Based Routing (PBR). One-Arm mode is implemented when a single insertion point in the network is not feasible or to counter the challenges of fail-to-wire. The Standby appliance can be added to the same VLAN or subnet as the Active appliance and the router.

In One-Arm mode, it is recommended that the SD-WAN appliances do not reside in the data network subnets. The virtual path traffic does not have to traverse the PBR and avoids route loops. The SD-WAN appliance and router have to be directly connected, either through an Ethernet port or be in the same VLAN.

## • IP SLA monitoring for fall back:

The active traffic flows even if the virtual path is down, as long as one of the SD-WAN appliances is active. The SD-WAN appliance redirects traffic back to the router as Intranet traffic. However, if both active/standby SD-WAN appliances become inactive, the router tries to redirect traffic to the appliances. IP SLA monitoring can be configured at the router to disable PBR, if the next appliance is not reachable. It allows the router to fall back to perform a route lookup and forward packets appropriately.

## Parallel Inline high availability mode:

In Parallel Inline high availability mode, the SD-WAN appliances are deployed alongside each other, inline with the data path. Only one path through the Active appliance is used. It is important to note that bypass interface groups are configured to be fail-to-block to avoid bridging loops during a failover. The high availability state can be monitored through the inline interface groups, or through a direct connection between the appliances. External Tracking can be used to monitor the reachability of the upstream or downstream network infrastructure. For example; switch port failure to direct high availability state change, if needed.

If both active and standby SD-WAN appliances are disabled or fail, a tertiary path can be used directly between the switch and router. This path must have a higher spanning tree cost than the SD-WAN paths so that it is not used under normal conditions. Failover in parallel inline high availability mode depends on the configured failover time, the default failover time is 1000 ms. However, a failover has a traffic impact of 3-5 seconds. Fall back to the tertiary path impacts traffic for the duration of spanning tree re-convergence. If there are out of path connections to other WAN Links, both appliances must be connected to them.



In more complex scenarios, where multiple routers might be using VRRP, non-routable VLANs are recommended to ensure that the LAN side switch and routers are reachable at layer 2.



## Fail-to-Wire mode:

In fail-to-wire mode, the SD-WAN appliances are inline in the same data path. The bypass interface

## groups must be in the fail-to-wire mode with the Standby appliance in a passthrough or bypass state. A direct connection between the two appliances on a separate port must be configured and used for the high availability interface group.

Note

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

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



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

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

If minimal loss of service is acceptable during a failover, then Fail-to-Wire high availability mode is a better solution. The Fail-to-Wire high availability mode protects against appliance failure and parallel

inline high availability protects against all failures. In all scenarios, high availability is valuable to preserve the continuity of the SD-WAN network during a system failure.

For more information on SD-WAN Orchestrator service-based HA deployment, see Device details.

## 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.

Dashboard	Monitoring	Configuration
System Status		
Name:	BLR_DC-App	liance
Model:	4000	
Appliance Mode:	MCN	
Management IP Ad	dress: 10.105.58.17	2
Appliance Uptime:	3 days, 7 hou	urs, 1 minutes, 43.0 seconds
Service Uptime:	3 days, 6 hou	urs, 39 minutes, 51.0 seconds
Routing Domain En	abled: Default_Rou	tingDomain
High Availability	/ Status	
Local Appliance:	Active	
Peer Appliance:	Standby	
Last Update Receive	d: <b>0 seconds ago</b>	

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

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

For Network Adapter details of Active and Standby high availability appliances, navigate to **Configu**ration > Appliance Settings > Network Adapters > Ethernet tab.

- Appliance Settings	Configuration > Appliance Settings > Net	work Adapters	
· Administrator Interface · Logging/Monitoring	IP Address Ethernet		
Network Adapters			
Net Flow	Ethernet Interface Settings		
SNMP	For the CB4000 platform, settings for ports 1/1, 1/	/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 10/1 and 10/2 will o	nly take effect when the Citrix Virtual WAN Se
Licensing	in the Citrix configuration. The settings for the high speed port 10/1 cannot I	be changed.	
Virtual WAN	0/1: • MAC Address: 0a:c4:7a:14:c9:d6	Autonegotiate: 🗹 Speed: 1000Mb/s	Duplex: Full
System Maintenance	1/1 : • MAC Address: 5a:4c:f8:f0:71:b2	Autonegotiate: 🖉 Speed: Unknown	Duplex: Unknown
	1/2: • MAC Address: d6:1e:72:d5:d1:18	Autonegotiate: 🗹 Speed: 1000Mb/s	Duplex: Full
	1/3 : • MAC Address: 66:4f:9d:c5:48:d2	Autonegotiate: 🗹 Speed: Unknown	Duplex: Unknown
	1/4 : • MAC Address: 46:63:cb:5d:39:db	Autonegotiate: 🗹 Speed: 1000Mb/s	▼ Duplex: Full
	1/5 : • MAC Address: 06:7b:ce:9a:c5:dd	Autonegotiate: 🕑 Speed: 1000Mb/s	▼ Duplex: Full

#### Citrix SD-WAN 11.5

Dashboard Monitoring	Configuration
- Appliance Settings	Configuration > Appliance Settings > Network Adapters
Administrator Interface	IP Address Ethernet
Network Adapters	
Net Flow	Ethernet Interface Settings
SNMP	For the CB4000 platform, settings for ports 1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 10/1 and 10/2 will only take effect when the Citrix Virtual WAN Service is enabled and the port is included
Licensing	in the Citrix configuration. The settings for the high speed port 10/1 cannot be changed.
+ Virtual WAN	0/1: • MAC Address: 0a:25:90x5:70:b4 Autonegotiate: ☑ Speed: 1000Mb/s ▼ Duplex Full ▼
+ System Maintenance	1/1 : • MAC Address: b2:1f:d0:ab:70:ea Autonegotiate: 🕢 Speed: Unknown 🔻 Duplex: Unknown 🔻
	1/2 : • MAC Address: 36:1f:0e:02:91:03 Autonegotiate: 🗹 Speed: Unknown 🔻 Duplex: Unknown 🔻
	1/3 : • MAC Address: aa:af:3e:1f:3b:2b Autonegotiate: 🗹 Speed: Unknown 🔻 Duplex: Unknown 🔻
	1/4 : • MAC Address: c2:3exe5:22:93:05 Autonegotiate: 🕢 Speed: Unknown 🔻 Duplex: Unknown 🔻
	1/5 : • MAC Address: ee:6fcd3:aa:6b:bc Autonegotiate: 🖉 Speed: 1000Mb/s 🔻 Duplex: Full 🔻

## Troubleshooting

Perform the following troubleshooting steps while configuring the SD-WAN appliance in High Availability (HA) mode:

- 1. The primary reason for split-brain issue is due to communication problem between the HA appliances.
  - Check if any issue with the connectivity (such as, the ports on both the SD-WAN appliance are up or down) between the SD-WAN appliances.
  - Must disable SD-WAN service on one of the SD-WAN appliances to ensure only one SD-WAN appliance be active.
- 2. You can verify the HA related logs that is logged into **SDWAN\_common.log** file.

#### NOTE

All the HA related logs is logged with the key word **racp**.

- 3. You can verify the port related events in **SDWAN\_common.log** file (such as, the HA enabled ports goes down or up).
- 4. For every HA state change, one SD-WAN event is logged. So if the logs are rolled over, you can verify the event logs to get the event details.

# Enable Edge Mode High Availability Using Fiber Optic Y-Cable

August 24, 2022

Note: In release 10.2 version 2, this functionality is applicable to the 1100 SE appliance only.

The following procedure describes the steps to enable High Availability (HA) on 1100 SE 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 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 appliances deployed in HA pair. The splitter cable is used to divide one incoming signal into multiple signals.

For information on SD-WAN Orchestrator service-based Edge Mode HA deployment, see Device details.



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

## August 24, 2022

#### Note

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

- SD-WAN 110 Standard Edition
- SD-WAN 210 Standard Edition
- SD-WAN 1100 Standard Edition
- SD-WAN 2100 Standard Edition
- SD-WAN AWS VPX instance

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

The zero-touch deployment Cloud Services securely communicate with back-end Citrix services hosting stored identification of Citrix customers who have purchased Zero Touch capable devices (for example 2100-SE). The back-end services are in place to authenticate any Zero Touch Deployment request, properly validating the association between the Customer Account and the Serial Numbers of Citrix SD-WAN appliances.

For more information, see the Citrix SD-WAN Orchestrator service Zero touch deployment topic.

## 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:

• Citrix Cloud Login to initiate the Zero Touch Deployment Service for new site node deployment.

**Network Administrator** – A user responsible for Enterprise network management (DHCP, DNS, internet, firewall, and so on).

## Remote Site:

**Onsite Installer** –A local contact or hired installer for on-site activity with the following primary responsibilities:

• Physically unpack the Citrix SD-WAN appliance.

- Reimage non-ZTD ready appliances.
  - Required for: SD-WAN 1000-SE, 2000-SE, 1000-EE, 2000-EE
  - Not required for: SD-WAN 410-SE, 2100-SE
- Power cable the appliance.
- Cable the appliance for internet connectivity on the Management interface (for example MGMT, or 0/1).
- Cable the appliance for WAN link connectivity on the Data interfaces (for example apA.WAN, apB.WAN, apC.WAN, 0/2, 0/3, 0/5, and so on).

Note

The interface layout is different for each model, so reference the documentation for identification of data and management ports.



The following prerequisites are required before starting any Zero Touch Deployment service:

- Actively running SD-WAN promoted to Master Control Node (MCN).
- Citrix Cloud Login credentials created on https://onboarding.cloud.com (reference the instruction below on account creation).
- Management network connectivity (SD-WAN Appliance) to the Internet on port 443, either directly or through a proxy server.
- (Optional) At least one actively running SD-WAN appliance operating at a branch office in Client Mode with valid Virtual Path connectivity to MCN to help validate successful path establishment across the existing underlay network.

The last prerequisite is not a requirement, but allows the SD-WAN Administrator to validate that the underlay network allows Virtual Paths to be established when the Zero Touch Deployment is complete with any newly added site. Primarily, this validates that the appropriate Firewall and Route policies are in place to either NAT traffic accordingly or confirm the ability for UDP port 4980 can successfully penetrate the network to reach the MCN.



## Zero Touch Deployment Service Overview:

To use the Zero Touch Deployment Service (or zero-touch deployment Cloud Service), an Administrator must begin by deploying the first SD-WAN device in the environment.

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. Logging into the Zero Touch Service authenticates the Customer ID associated with the particular SD-WAN environment.

When the SD-WAN Administrator initiates a site for deployment using the zero-touch deployment process, you have the option to pre-authenticate the appliance to be used for zero-touch deployment by pre-populating the serial number, and initiating email communication to the on-site installer to begin on-site activity.

The Onsite Installer receives email communication that the site is ready for Zero Touch Deployment and can begin the installation procedure of powering on and cabling the appliance for DHCP IP address assignment and internet access on the MGMT port. Also, cabling in any LAN and WAN ports. Everything else is initiated by the zero-touch deployment Service and progress is monitored by using the activation URL. In the event the remote node to be installed is a cloud instance, opening up the activation URL begins the workflow to automatically install the instance in the designated cloud environment, no action is needed by a local installer.

The Zero Touch Deployment Cloud Service automates the following actions:

Download and Update the zero-touch deployment Agent if new features are available on the branch appliance.

- Authenticate the branch appliance by validating the serial number.
- Push the configuration file specific for the targeted appliance to the branch appliance.
- Install the configuration file on the branch appliance.
- Push any missing SD-WAN software components or required updates to the branch appliance.
- Push a temporary 10 Mbps license file for confirmation of Virtual Path establishment to the branch appliance.
- Enable the SD-WAN Service on the branch appliance.

## More steps are required of the SD-WAN Administrator to install a permanent license file on the appliance.

Note

While performing a branch configuration that already has the same version of appliance software used in MCN, the zero-touch-deployment process will not download the appliance software file again. This change is applicable for fresh factory shipped appliances, appliances reset to factory defaults, and configuration reset administratively. If there is the configuration reset, select the **Reboot after revert** check box to initiate the zero-touch deployment process.

The appliance configuration can be validated using the **Configuration** > **Virtual WAN** > **View Configuration** page.

#### Citrix SD-WAN 11.5

Warning: Grace license installed. Please obt Clear Warning	ain license from Citrix license portal and install it.
+ Appliance Settings	Configuration > Virtual WAN > View Configuration
- Virtual WAN	
View Configuration	Configuration
- Enable/Disable/Purge Flows - Dynamic Virtual Paths SD-WAN Center Certificates	View: Site •
+ System Maintenance	Site Configuration
	Site 4 = ThiBR Network Properties: Encryption Node=aesi28 Encryption Rekey is Enabled. Scr WiC Learning is disabled. dateway ARP Timer (ms): 1000 Max dynamic virtual paths configured is 8. Routing Domains Enabled: Default_RoutingDomain(ID: 0)
	<pre>Interface Group 0: Properties: secure Ione=trusted is overlay=true bypass mode=fail_to_vire Ethernet Interface: api.LAW, api.NAW Bridge Pairs: api.LAW &lt;&gt; api.NAW Virtual IP Addresses for Routing Domain: Default_RoutingDomain and Network Interface ThiBR_46 (VLAN ID=0):</pre>

The appliance license file can be updated to a permanent license using the **Configuration > Appliance** Settings > Licensing page.

#### Citrix SD-WAN 11.5

Dashboard	Monitoring	Configuration	-
Warning: Grace license     Clear Warning	installed. Please obtair 9	n license from Citrix license portal an	d install it.
- Appliance Setting	35	Configuration > Appliance Set	ttings > Licensing
- Administrator - Logging/Moni	interface toring	License Status	
- Net Flow - SNMP	ters	State: License Server Location: Local License Server HostiD:	Licensed Local 02×47=512±40
Licensing		System Platform:	NetScaler SD-WAN 1000 Series
+ Virtual WAN		Model: Maximum Bandwidth (MAXBW	1000VW-020 /j: 10 Mbps
+ System Maintena	nce	License Type: Action Required:	N/A Grace license installed. Please obtain license from Citrix license portal and install it.
		Maintenance Expiration Date: License Expiration Date:	N/A Sat May 27 02:48:57 2017
		License Configuration	
		Local      Remote     Rem	
		Upload License for this A	ppliance
		Filename: Choose File No	file chosen Upload and Install

After uploading and installing the permanent license file, the Grace License warning banner disappears and during the license install process no loss in connectivity to the remote site will occur (zero pings are dropped).

## AWS

#### August 24, 2022

With SD-WAN release 11.5, zero touch deployment in an AWS environment is supported through SD-WAN Orchestrator service.

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.

# Azure

## August 24, 2022

With SD-WAN release 11.5, zero touch deployment in an Azure environment is supported through SD-WAN Orchestrator service.

Note

- Cloud deployed SD-WAN instances must be deployed in Edge/Gateway mode.
- The template for the cloud instance is limited to three interfaces; Management, LAN, and WAN (in that order).
- The available Azure cloud templates for SD-WAN VPX are currently hard-set to obtain the 10.9.4.106 IP for the WAN, 10.9.3.106 IP for the LAN, and 10.9.0.16 IP for the Management address. The SD-WAN configuration for the Azure node targeted for Zero Touch must match this layout.
- The Azure site name in the configuration must be all lowercase with no special characters (e.g. ztdazure).



**Azure Cloud Topology with NetScaler SD-WAN** 

This is an example deployment of an 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.

# Single-region deployment

## August 24, 2022

Regions allow you to define a network hierarchy with distributed management. A Region must define a Regional Control Node (RCN) which will take over functions performed by the Network Control Node (MCN) for its Region. The MCN is the controller for the Default Region. Static and Dynamic Virtual Paths are not permitted between Regions. RCNs manage traffic between Regions. A single-region deployment in an SD-WAN network can support network sites less than 550.

For more information about Single region deployment through Citrix SD-WAN Orchestrator service, see Regions.

# Multi-region deployment

## August 24, 2022

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

With MCN as the control node of the network and RCNs as the control nodes of the regions, SD-WAN can manage up to 6000 sites.

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

An MCN with a single region can be configured with a maximum of 1000 sites. You can keep the existing sites in the default region and add new regions with RCNs and their sites for multi-region deployment.

For more information about Multi-region deployment through Citrix SD-WAN Orchestrator service, see Regions.



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

## NOTE

Use the Citrix SD-WAN 210 SE appliance as an MCN only in the SD-WAN Orchestrator managed networks.

Platform Edition	Primary/Secondary MCN	Primary/Secondary RCN
110-SE	No	No
210-SE	Yes	Yes
1100-SE	Yes	Yes
VPX-SE, VPXL-SE	Yes	Yes

Platform Edition	Primary/Secondary MCN	Primary/Secondary RCN
2100-SE, 4100-SE, 5100-SE,	Yes	Yes
6100-SE		

# **Configuration guide for Citrix Virtual Apps and Desktops workloads**

#### August 24, 2022

Citrix SD-WAN is a next-generation WAN Edge solution that accelerates digital transformation with flexible, automated, secure connectivity, and performance for SaaS, cloud, and virtual applications to ensure an always-on workspace experience.

Citrix SD-WAN is the recommended and best way for organizations using the Citrix Virtual Apps and Desktops Service to connect to Citrix Virtual Apps and Desktops workloads in the Cloud. For more information, see Citrix blog.

This document focuses on configuring Citrix SD-WAN for connectivity to/from Citrix Virtual Apps and Desktops workloads on Azure.

## Benefits

- Easy to set up SD-WAN in Citrix Virtual Apps and Desktops through a guided workflow
- Always-on, high performance connectivity through advanced SD-WAN technologies
- Benefits across all connections (VDA-to-DC, user-to-VDA, VDA-to-cloud, user-to-cloud)
- Reduces latency compared to backhauling traffic to the data center
- Traffic management to ensure Quality of Service (QoS)
  - QoS across HDX/ICA traffic streams (single-port multi-stream HDX AutoQoS)
  - QoS between HDX and other traffic
  - HDX QoS Fairness between users
  - End-to-end QoS
- Link bonding delivers more bandwidth for faster performance
- High Availability with seamless link failover and SD-WAN redundancy on Azure
- Optimized VoIP experience (packet racing for reduced jitter and minimal packet loss, QoS, local break-out for reduced latency)
- Major cost savings and must be faster and easier to deploy compared to Azure ExpressRoute

## **Pre-requisites**

Adhere the following pre-requisites to evaluate and deploy the Citrix Virtual Apps and Desktops workloads capabilities:

- You must have either have an existing SD-WAN network or build a new one.
- You must have a subscription to Citrix Virtual Apps and Desktops Service.
- To make a use of SD-WAN features such as, multi-stream HDX AutoQoS and deep visibility, the Network Location Service (NLS) must be configured for all the SD-WAN sites in your network.
- You must have a DNS server and AD deployed where the client endpoints are present (often co-located in your data center environment) or you can utilize Azure Active Directory (AAD).
- The DNS server must be capable of resolving both internal (private) and external (public) IPs.
- Ensure that the FQDN (sdwan-location.citrixnetworkapi.net) is added to the allowed list in the firewall. This is the FQDN for Network Location Service which is critical in sending traffic over the SD-WAN virtual path. Also, a better way if you are comfortable with whitelisting wild card FQDN's would be to add \*.citrixnetworkapi.net to the allowed list as this is the subdomain for other Citrix Cloud services such as zero touch provisioning.
- Enroll at sdwan.cloud.com to use the SD-WAN orchestrator for managing your SD-WAN network. SD-WAN Orchestrator is a Citrix Cloud based multitenant management platform for Citrix SD-WAN.



## Deployment architecture

The following entities are required for deployment:

- An on-premises location hosting the SD-WAN appliance which can either be deployed in branch mode or as an MCN (Master control Node). The branch mode or MCN contains the client machines, active directory, and DNS. However, you can also choose to use Azure's DNS and AD. In most scenarios, the on-premises location serves as a data center and houses the MCN.
- Citrix Virtual Apps and Desktops cloud service –Citrix Virtual Apps and Desktops provides virtualization solutions that give IT control of virtual machines, applications, and security while providing anywhere access for any device. End users can use applications and desktops independently of the device's operating system and interface.

Using the Citrix Virtual Apps and Desktops Service, you can deliver secure virtual apps and desktops to any device, and leave most of the product installation, setup, configuration, upgrades, and monitoring to Citrix. You maintain complete control over applications, policies, and users while delivering the best user experience on any device.

- **Citrix connector/cloud connector** You connect your resources to the service through Citrix Cloud Connector, which serves as a channel for communication between Citrix Cloud and your resource locations. Cloud Connector enables cloud management without requiring any complex networking or infrastructure configuration such as VPNs or IPsec tunnels. Resource locations contain the machines and other resources that deliver applications and desktops to your subscribers.
- SD-WAN Orchestrator –Citrix SD-WAN Orchestrator is a cloud-hosted, multitenant management service available to Do It Yourself enterprises and Citrix Partners. Citrix partners can use SD-WAN Orchestrator to manage multiple customers with a single pane of glass, and suitable role-based access controls.
- Virtual and physical SD-WAN appliances –This runs as multiple instances within the cloud (VMs) and on-premises in the data center and in the branches (physical appliances or VMs) to provide connectivity among these locations and to/from the public Internet. SD-WAN instance in Citrix Virtual Apps and Desktops is created as a single or a set of virtual appliances (in case of HA deployment) by provisioning these instances via Azure Marketplace. SD-WAN appliances in other locations (DC and branches) are created by the customer. All of these SD-WAN appliances are managed (in terms of configuration and software upgrades) by SD-WAN Administrators through SD-WAN Orchestrator.



## **Deployment and configuration**

In a common deployment, a customer would have the Citrix SD-WAN appliance (H/W or VPX) deployed as an MCN in their DC/large office. The customer DC would usually host on-prem users and resources such as AD and DNS servers. In some scenarios the customer can make use of Azure Active Directory services (AADS) and DNS, both of which are supported by Citrix SD-WAN and CMD integration.

Within the customer managed Azure subscription, the customer needs to deploy the Citrix SD-WAN virtual appliance and VDAs. The SD-WAN appliances are managed via SD-WAN Orchestrator. Once the SD-WAN appliance gets configured, it connects to the existing Citrix SD-WAN network and further tasks such as configuration, visibility, and management are handled via SD-WAN Orchestrator.

The third component in this integration is the **Network Location Service (NLS)** that allows internal users to bypass the gateway and connect to the VDA's directly, reducing latency for internal network traffic. You can configure NLS manually or through Citrix SD-WAN Orchestrator. For more information, see NLS.

## Configuration

Citrix SD-WAN VM is deployed within a specified region (as needed by the customer) and can be connected to multiple branch office locations through MPLS, Internet, or 4G/LTE. Within a Virtual Network (VNET) infrastructure, SD-WAN Standard Edition (SE) VM is deployed in gateway mode. The VNET has routes towards the Azure gateway. The SD-WAN instance has a route towards the Azure gateway for internet connectivity. This route needs to be created manually.

1. In a web browser, go to Azure portal. Log into Microsoft Azure account and search for Citrix SD-WAN Standard Edition.

2. In the search results, choose the Citrix SD-WAN Standard Edition solution. Click **Create** after going through the description and making sure the solution chosen is correct.

Microsoft Azure	. م	earch resources, services, i	and docs			Ð		CITRIX SYSTEMS, INC.
×	Home > Marketplace							
+ Create a resource	Marketplace		\$1					
n Home								
Dashboard	, Citrix SD WAN 10.2			×				
E All services	Pricing Operating System		Publisher					
* FAVORITES	All V All	~	AI	Y				
All resources	Results							
💓 Resource groups	NAME	PUBLISHER	CATEGORY					
🔇 App Services	Citrix SD WAN 10.2	Citrix	Compute					
5 Function Apps								
🗧 SQL databases	Citrix SD WAN 10.2 (Staged)	Citrix	Compute					
🥭 Azure Cosmos DB	Citrix SD-WAN Center 10.2	Citrix	Compute					
Virtual machines	Citrix SD-WAN Center 10.2 (Staged)	Citrix	Compute					
🔶 Load balancers	Citrix SD-WAN (500mbos/lobos) (Staged)	Citrix	Compute					
Storage accounts								
Virtual networks								
Azure Active Directory								
Monitor								
Advisor								
Security Center								
O Cost Management + Billing								
Help + support								

On click of **Create**, a wizard prompting with necessary details to create the virtual machine.

3. In the **Basic settings** page, choose the resource group in which you want to deploy the SD-WAN SE solution.

A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You can decide how you want to allocate resources to resource groups based on your deployment.

For Citrix SD-WAN, it's recommended that the resource group you choose must be empty. Similarly, pick the Azure region where you want to deploy the SD-WAN instance. The region must be the same as the region in which your Citrix Virtual Apps and Desktops resources are deployed.



4. Under **Administrator settings** page, provide a name for the Virtual Machine. Choose a user name and strong password. The password must consist of an upper-case letter, special character and must be more than nine characters. Click **OK**.

This password is required to log in to the management interface of the instance as a guest user. To get admin access to the instance, use admin as the user name and the password created while provisioning the instance. If you use the user name created while provisioning the instance, you get read-only access. Also, choose the deployment type here.

If you want to deploy a single instance then make sure that you choose disabled from the HA Deployment mode option, else pick enabled. For production networks, Citrix always recommends deploying instances in HA mode as it guards your network against failures of the instance.

Create	e Citrix SD-WAN Stand	a ×	Administrator settings	
1	Basics Done	~	★ Virtual Machine name SDWSEA	<b>~</b>
2	Administrator settings Configure deployment settings	>	HA Deployment Mode ① Enabled Disabled * Username ①	
3	SDWAN settings Configure Netscaler SD-WAN a	>	* Password ()	~ ~
4	SDWAN Route settings Configure the route settings	>	* Confirm password	~

- 5. Under the **SD-WAN settings** page, choose the instance in which you want to run the image. Choose the following instance type as per your requirement:
  - Instance type D3\_V2 for maximum uni-directional throughput of 200 Mbps with direct connectivity to a maximum of 16 branches.
  - Instance type D4\_V2 for maximum uni-directional throughput of 500 Mbps with direct connectivity to a maximum of 16 branches.
  - Instance type F8 standard for maximum uni-directional throughput of 1 Gbps with direct connectivity to a maximum of 64 branches.
  - Instance type F16 standard for maximum uni-directional throughput of 1 Gbps with direct connectivity to a maximum of 128 branches.

+ Create a resource	×	SDWAN Settings	×	Choose Browse the ave	a size	ir features								
A Home				Search			Compute type		Disk type			VCPUs		
Dashboard		<ul> <li>Virtual machine size</li></ul>	>	1			Current generation	*	All disk types		*	1 0		128
i All services		Tx standard US V2		NCOMME.		THE	COMPLETE METHOD	20.04H			10001000	Portania.	100/000	1070-04004
* FAVORITES	-	Virtual network	>	NECOWINE	540	1170	COMPUTE - VCPUS	UD KAM	DATA DISKS	MAA 10PS	LUCAL SSU	PRENIUM	ADDITION	030/180/84
All resources		(new) vnec		Available										
Resource groups		Subnets   Configure subnets	0>	*	D3_v2	Standard	General purpos- 4	14	16	16x500	200 G8	No		\$209.06
🔇 App Services		-		*	D4_v2	Standard	General purpos 8	28	32	32×500	400 G8	No		\$418.13
Function Apps					E8	Standard	Commits ontin 8	16	22	22-600	129.08	No		\$282.72
🧧 SQL databases				-	10	Juan Natiru	compose openni o	10		324,540	120 00	140		30.00-16
🧟 Azure Cosmos DB					F16	Standard	Compute optim 16	32	64	64x500	256 G8	No		\$565.44
Virtual machines														
Load balancers														
Storage accounts														
Virtual networks														
Azure Active Directory														
Monitor														
🔷 Advisor														
Security Center				Prices presen	ted are estimate	es in your local curre	nov that include Asure infrastruc	ture applicable soft	ware costs, as we	Las any discount	s for the subscript	tion and location.	inal charges will a	opear in your
O Cost Management + Billing				local currency	y in cost analysis	s and billing views. If	you purchased Azure services th	hrough a reseller, co	ntact your reselle	r for full pricing o	details. Recomme	nded sizes are dete	rmined by the put	blisher of the
Help + support					pe oniced on nam	unare and summare	- education of the							
				Select										

 Create a new Virtual Network (VNet) or use an existing VNet. This is the most critical step for the deployment as this step chooses the subnets to be assigned to the interfaces of the SD-WAN VPX VM.



The aux subnet is only needed when you are deploying the instances in HA mode. Ensure that the SD-WAN instance is being deployed in the same VNet as your Citrix Virtual Apps and Desktops resources and is on the same subnet as the LAN interface of the SD-WAN VPX appliance.
ent subnet name * nt ~ ent subnet address prefix *
nt v
ent subnet address prefix *
4 🗸
t name *
~
t address prefix *
4 🗸
et name *
~
et address prefix *
4 🗸
t name *
~
t address prefix *
4 🗸

7. Verify the configuration in the **Summary** page and click **OK**.

*	Home >	Citrix SD-WAN Standard Editio	on 10.2.4	> Create Citrix SD-WAN Standard Ec	dition 10.2.4 > Summary	
+ Create a resource	Create	Citrix SD-WAN Stand	la ×	Summary		×
🟫 Home				Validation passed		
Dashboard	1	Basics	~	•		 
😑 All services		Done		Basics		
+ FAVORITES	2	General settings	~	Subscription Resource group	NSDev SDWAN CA ravisankar.pegada@citrix.com SDWANIND2	
All resources	~	Done		Location	(Asia Pacific) South India	
C Resource groups	2	SDWAN Setting		General settings Virtual Machine name	Branch3HA	
COL data bases	3	Done	~	HA Deployment Mode Username	Enabled citrixsdwan	
SQL databases				Password	*********	
Virtual machines	4	Summary Citrix SD-WAN Standard Edition	>	SDWAN Settings Virtual machine size	Standard D3 v2	
Load balancers				Virtual network Manangement subnet	BR3vnet snet-mgmt	
Storage accounts	5	Buy	>	Manangement subnet addre LAN subnet	10.4.0.0/24 snet-lan	
Virtual networks				LAN subnet address prefix WAN subnet	10.4.1.0/24 snet-wan	
Azure Active Directory				WAN subnet address prefix AUX subnet	10.4.2.0/24 snet-aux	
📀 Monitor				AUX subnet address prefix	10.4.3.0/24	
Advisor						
Conter Security Center						
Ocost Management + Billing				OK Download temp	niate and narameters	
Help + support				Download temp	place and parameters	

8. On the **Buy** page, click **Create** to start the provisioning process for the instances. It can take around 10 minutes for the instance to get provisioned. You get a notification in the Azure management portal suggesting the success/failure of instance creation.

eate	Citrix SD-WAN Stand	a ×	Create	>
1	Basics Done	~	Citrix SD-WAN Standard Edition 10.2 by Citrix Terms of use   privacy policy	
2	General settings Done	~	Deploying this template will result in various actions being performed, which may include the deployment of one of more Azure resources or Marketplace offerings and/or transmission of the information you provided as part of the deployment process to one or more parties, as specified in the template. You are responsible for reviewing the text of the template to determine which actions will be performed and which resources or	
3	SDWAN Settings Done	~	offerings will be deployed, and for locating and reviewing the pricing and legal terms associated with those resources or offerings. Current retail prices for Azure resources are set forth here and may not reflect discounts	
4	Summary Citrix SD-WAN Standard Editio	~	applicable to your Azure subscription. Prices for Marketplace offerings are set forth here, and the legal terms associated with any Marketplace offering may be found in the Azure portal; both are subject to change at any time prior to deployment.	
5	Buy	>	Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately. If any Microsoft products are included in a Marketplace offering (e.g., Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.	

Once the instance is created successfully, fetch the public IP assigned to the management interface of the SD-WAN instance. It can be found under the networking section of the resource group within which the instance has been provisioned. Once retrieved you might use it to log

#### in to the instance.

### Note

For admin access, the user name is **admin** and the password is the one that you have set during instance creation.

- 9. Once the site has been provisioned, log into the SD-WAN Orchestrator to configure it. As mentioned in the pre-requisites, you must have the entitlement to SD-WAN Orchestrator to configure the site. If you do not have it yet, refer Citrix SD-WAN Orchestrator Onboarding.
- 10. If you have an SD-WAN network already, then proceed to creating the configuration for the site that you provisioned in Azure. Otherwise you must create an MCN. For more information, see Network configuration.
- 11. Once you have access to SD-WAN Orchestrator and already have set up an MCN, login to SD-WAN orchestrator and click the **+New site** to start configuring the SD-WAN VPX appliance (that you have provisioned in Azure).

Site Details		
Site Name *		
Name		
Site Address *		Lat/Lng
Search for Site Address		

12. Provide a unique site name and enter the address based on the region in which you are provisioning the image. To set up the instance in Azure, refer Basic settings.

## Note

To fetch the serial number of the instance in Azure, log in to the instance via the public management IP. You can see the serial number on the dashboard screen. If you are configuring instances in HA then both the serial numbers must be captured. Also, while configuring the instance, ensure that the interfaces are chosen as **Trusted**.

 For fetching the IP addresses associated with LAN and WAN interfaces on Azure. Navigate to the Azure portal > Resource groups > Resource group where the SD-WAN is provisioned >SD-WAN VM > Networking.

Dashboard	Monitoring Configuration	
System Status		
Name:	DCAzure	
Model:	VPX	
Sub-Model:	BASE	
Appliance Mode:	MCN	
Serial Number:	0000-0007-5714-8818-8276-7561-41	
Management IP Addres	255: 10.2.0.4	
Appliance Uptime:	6 days, 8 hours, 59 minutes, 5.8 seconds	
Service Uptime:	4 days, 8 hours, 29 minutes, 10.0 seconds	
Routing Domain Enable	ed: Default RoutingDomain	

14. Once you are done with the configuration of the instance. Click **Deploy Config/Software** by navigating to **Configuration > Network config Home**.

+ Add S	ite Batch Add	Sites Deploy Co	onfig/Software	Back Up/Rev	iew Checkpoints	More Actions		Search	n Q
							Deployment Tracker		
Availability	Cloud Connectivity	Site Name	Site Role	Device Model	Serial No	Bandwidth Tier	Management IP	Actions	
	Offline	AzureBranch	MCN	VPX-SE	0000-0009-9954	1000		1	

15. If there are no issues and the configuration is accurate, you must have the virtual paths up between the instance in Azure and your MCN once the configuration deployment is run.

## **Citrix Virtual Apps and Desktops configuration**

As highlighted in the Deployment and configuration section, the AD/DNS is present in the on-premises location acting as the DC and in a deployment featuring SD-WAN it presents behind the SD-WAN that is on the LAN network. It is the IP of your AD/DNS that you need to configure here. In case you are making use of Azure Active Directory service/DNS, configure **168.63.129.16** as the DNS IP.

If you are making use of an on-premises AD/DNS.Check if you are able to ping the IP of your DNS from your SD-WAN appliance. You can do this by navigating to **Troubleshooting > Diagnostics**. Check the **Ping** check box and initiate a ping from the LAN interface/Default interface of the SD-WAN appliance to the IP of your AD/DNS.

E Citrix Cloud	SD-WAN Orchestrator	Þ	•
Customer Site <u>cloudDNATest</u> / All Sites ~			
Dashboard	Network TroubleShooting : Diagnostics		
Lill Reports	Ping Traceroute Packet Capture Bandwidth Test		
Configuration	Source Site		
Troubleshooting Audit Logs Device Logs	Source Site CDNTestCMD		
Diagnostics	IP Address Interface Gateway IP (Optional)		
Q Administration →	Default     Default       Routing Domain     Default   Packet Size (KB)		
	Default_RoutingDomaii 70		

If the ping succeeds, then it signifies that your AD/DNS can be reached successfully, if not then it means there is routing issue in your network which is preventing reachability to your AD/DNS. If possible, try to host your AD and SD-WAN appliance on the same LAN segment.

In case there is still an issue, get in touch with your network admin. Without completing this step successfully, the catalog creation step will not succeed and you get an error message as **Global DNS IP not configured**.

Note

Ensure that the DNS is capable of resolving both internal and external IPs.

## **Network location service**

With the **Network Location** service in Citrix Cloud, you can optimize internal traffic to the apps and desktops you make available to subscribers'workspaces to make HDX sessions faster. Users on both internal and external networks have to connect to VDAs through an external gateway. While this is expected for external users, internal users experience slower connections to virtual resources. The **Network Location** service allows internal users to bypass the gateway and connect to the VDAs directly, reducing latency for internal network traffic.

## Configuration

To set up the **Network Location** service, use one of the following methods:

- **Citrix SD-WAN Orchestrator**: For detailed information on configuring NLS using Citrix SD-WAN Orchestrator, see Network location service.
- Network Location service PowerShell module that Citrix provides: For detailed information on configuring NLS using PowerShell module, see PowerShell module and configuration.

The network locations share the public IP ranges of the networks where your internal users are connecting from. When subscribers launch Virtual Apps and Desktops sessions from their workspace, Citrix Cloud detects whether subscribers are internal or external to the company network based on the public IP address of the network from which they are connecting.

If a subscriber connects from the internal network, Citrix Cloud routes the connection directly to the VDA, bypassing Citrix Gateway. If a subscriber connects externally, Citrix Cloud routes the subscriber through Citrix Gateway as expected and then redirects the subscriber to the VDA in the internal network.

NOTE

The public IP that needs to be configured in network location service needs to be the public IP assigned to the WAN links.

# Domain name system

## August 24, 2022

**Domain Name System (DNS)** translates human readable domain names to machine-readable IP addresses, and vice versa. Citrix SD-WAN provides the following DNS features:

- DNS Proxy
- DNS Transparent Forwarding

You can configure a DNS proxy or DNS transparent forwarding through Citrix SD-WAN Orchestrator service using the following types of DNS service:

- **Static DNS service**: Allows you to configure the static IPv4 DNS server IP addresses. You can create Internal, ISP, google, or any other open source DNS service. Static DNS service can be configured at global and site level.
- **Dynamic DNS service**: Allows you to configure the dynamic IPv4 DNS server IP addresses. Dynamic DNS service can be configured at site level only. Only one dynamic DNS service is permitted per site.

- **StaticV6 DNS service**: Allows you to configure the static IPv6 DNS server IP addresses. You can create Internal, ISP, google, or any other open source DNS service. StaticV6 DNS service can be configured at global and site level.
- **DynamicV6 DNS service**: Allows you to configure the dynamic IPv6 DNS server IP addresses. DynamicV6 DNS service can be configured at site level only. Only one dynamic DNS service is permitted per site.

## **DNS proxy**

You can configure a proxy with multiple forwarders that helps steering DNS requests based on application domain names. DNS forwarding works for the requests that are received through UDP connections. For information on how to configure DNS proxy through SD-WAN Orchestrator service, see DNS proxy.

## **DNS transparent forwarder**

Citrix SD-WAN can be configured as a transparent DNS forwarder. In this mode, SD-WAN can intercept DNS requests that are not destined to its IP address and forward them to the specified DNS service. Only the DNS requests coming from local service on trusted interfaces are intercepted. If the DNS requests match any applications in the DNS forwarder list, then it is forwarded to the configured DNS service. DNS forwarding is supported only for requests coming over UDP connections. For information on how to configure DNS tranparent forwarder through SD-WAN Orchestrator service, see DNS tranparent forwarders.

## 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** 

Proxy Statistics						
Refresh					Search	Q
Proxy Name	C Application Name	DNS Service Name	0 DNS Service Active	0 Hits 0	DNS Service IPv6 Name	: 0
Local_Proxy210	ECOMM	GoogleV4	YES	0	GDNSv6	Y
Local_Proxy210	ms_teams_realtime	Quad9	YES	0	Quad9v6	Y
Local_Proxy210	ms_sharepoint_optimize	Quad9	YES	0	Quad9v6	Y
Local_Proxy210	ms_exchange_online	Quad9	YES	0	Quad9v6	Y
Local_Proxy210	ms_teams_fallback	Quad9	YES	0	Quad9v6	Y
Local_Proxy210	ms_exchange_mail	Quad9	YES	0	Quad9v6	Y
Local_Proxy210	ms_sharepoint_allow	Qual9	YES	0	Quad9v6	Y
Local_Proxy210	ms_office365_common	Quad9	YES	0	Quad9v6	Y
Local_Prexy210	office365_default	Quad9	YES	0	Quad9v6	Y
Local_Proxy210	citrix_cloud_web_ui_api	Quad9	YES	167	Quad9v6	Y
¢			Showing 1-1	D of 17 items	Page 1 of 2 <	▶ 10 rows ∨

#### **Transparent Forwarder Statistics**

DNS Transparent Forwarder Statistics

Refresh					Search	Q
Application Name	DNS Service Name	DNS Service Active	Hits 🗦 🌐	DNS Service IPv6 Name	DNS Service IPv6 Active	Hits $\diamond$ +
ECOMM	GoogleV4	YES	0	GDNSv6	YES	0
ms_teams_realtime	Quad9	YES	0	Quad9v6	YES	0
ms_sharepoint_optimize	Quad9	YES	0	Quad9v6	YES	0
ms_exchange_online	Quad9	YES	0	Quad9v6	YES	0
ms_teams_fallback	Quad9	YES	0	Quad9v6	YES	0
ms_exchange_mail	Quad9	YES	0	Quad9v6	YES	0
ms_sharepoint_allow	Quad9	YES	0	Quad9v6	YES	0
ms_office365_common	Quad9	YES	0	Quad9v6	YES	0
office365_default	Quad9	YES	0	Quad9v6	YES	0
citrix_cloud_web_ui_api	Quad9	YES	0	Quad9v6	YES	0
				Showing 1-10 of 16 items	Page 1 of 2	10 rows 🗸

# DHCP

#### September 19, 2022

Citrix SD-WAN introduces the ability to use Standard 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.



## WAN link IP address learning through DHCP client

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 and data port can be enabled on MCN/RCN only if Public IP address is configured.
- 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.

From Citrix SD-WAN 11.5 release onwards, you can configure DHCP for an untrusted virtual interface on fail-to-block mode through Citrix SD-WAN Orchestrator service. For more information, see WAN link IP address learning through DHCP client.

## **DHCP support on Fail-to-Wire port**

Earlier, the DHCP client was only supported on Fail-to-block port. With 11.2.0 release, the DHCP client capability is extended on fail-to-wire port for the branch site with serial High Availability (HA) deployments. This enhancement:

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

DHCP client is now supported on the private intranet link.



#### Note:

A LAN interface must not be connected into the fail-to-wire pair as packets might be bridged between the interfaces.

## **Monitoring DHCP client WAN links**

The runtime Virtual IP address, Subnet Mask, and Gateway settings are logged and archived in a log file called *SDWANVW\_ip\_learned.log*. Events are generated when Dynamic Virtual IPs are learned, released, or expired, and when there is a communication issue with the learned Gateway or DHCP server. Or when duplicate IP addresses are detected in the archived log file. If duplicate IPs are detected at a site, Dynamic Virtual IP addresses are released and renewed until all Virtual Interfaces at the site obtain unique Virtual IP addresses.

To monitor DHCP client WAN links:

-----

- 1. In the SD-WAN appliance, **Enable/Disable/Purge Flows** page, the DHCP Client WAN Links table provides the status of learned IPs.
- 2. You can request to renew the IP, which refreshes the lease time. You can also choose to **Release Renew**, which issues a new IP address or the same IP address with a new lease.

DHCF CIR	ETTE VYZEN ETT	15							
Ethernet Interface	Virtual Interface	WAN Link	IP Address / Prefix	Gateway IP Address	Lease Duration Seconds	Remaining Seconds	Expiration Date	Action	
X2	VLAN349	SFWL3-Inter	10.30.30.55/24	10.30.30.2	1800	1640	9:13 on 1/8/2016	Renew	Submit
X2	VLAN350	SFWL4-Inter	10.20.20.53/24	10.20.20.2	86400	71035	4:29 on 1/9/2016	Renew	Submit

## **DHCP** logs

Citrix SD-WAN enables you to generate DHCP server logs for IP addresses. Whenever IP addresses are allocated to endpoints, the logs are generated. The logs contain details such as the timestamp of the IP address allocation and lease duration, MAC address, the client ID and so on. The client ID **none** indicates that it is not present in the DHCP request.

To generate and view DHCP logs, navigate to **Configuration** > **Logging/Monitoring**. Select the **SD-WAN\_dhcp.log** option from the drop-down list and click **View Log**.

Feb	4 11:58:30 BR1-Primary dhood:	Internet Systems Consortium DHCP Server 4.3.2	
Feb	4 11:58:30 BR1-Primary dhcpd:	Copyright 2004-2015 Internet Systems Consortium.	
Feb	4 11:58:30 BR1-Primary dhcpd:	All rights reserved.	
Feb	4 11:58:30 BR1-Primary dhcpd:	For info, please visit https://www.isc.org/software/dhcp/	
Feb	4 11:58:30 BR1-Primary dhcpd:	wrote 0 deleted host decls to leases file.	
Feb	4 11:58:30 BR1-Primary dhcpd:	Wrote 0 new dynamic host decls to leases file.	
/Feb	4 11:58:30 8R1-Primary dhcpd:	Wrote 1 leases to leases file.	
Feb	4 11:58:30 8R1-Primary dhcpd:	Listening on LPF/vn1-1/36:d0:d6:52:9f:cc/172.58.3.0/24	
Feb	4 11:58:30 BR1-Primary dhcpd:	Sending on LPF/vn1-1/36:d0:d6:52:9f:cc/172.58.3.0/24	
Feb	4 11:58:30 BR1-Primary dhcpd:	Server starting service.	
Feb	4 11:58:30 BR1-Primary dhcpd:	Listening on LPF/vn1-0/de:82:2f:9e:4c:3d/172.58.30.0/24	
Feb	4 11:58:30 BR1-Primary dhcpd:	Sending on LPF/vn1-@/de:82:2f:9e:4c:3d/172.58.30.0/24	
Feb	4 11:58:30 8R1-Primary dhcpd:	Server starting service.	
Feb	4 11:58:31 BR1-Primary dhcpd:	DHCPDISCOVER from 02:63:f0:6e:19:3f vla vnl-0	
740	4 11:58:31 BR1-Primary dhcpd:	DHCPOFFER on 172.58.30.151 to 02:03:f0:00:19:3f v1a vn1-0	
740	4 11:58:31 881-Primary dhcpd:	DHCPRIQUEST for from 02:03:10:00:19:34 via vn1-0	
740	4 11:58:31 BR1-Primary dhipdi	DMCPACE ON 172.50.30.151 TO 02/03/F0/00/19/37 VIA VML-0	
*e0	4 11:38:31 881-Primary dh(pd)	Lease time start : 4 1970/01/01 00:00:00: Lease time end : 4 1970/01/01 00:00:00: for IP :	MAC-Address   02:03:F0:de:19:3f; Client-1d   <none></none>

#### Note

These logs are generated only when Citrix SD-WAN acts as a DHCP server.

# **Dynamic PAC file customization**

#### August 24, 2022

With the increase in enterprise adoption of mission-critical SaaS applications and distributed workforce, it becomes highly critical to reduce latency and congestion. Latency and congestion are inherent in traditional methods of backhauling traffic through the Data Center. Citrix SD-WAN allows direct internet break out of SaaS applications such as Office 365. For more information, see Office 365 Optimization.

If there are explicit web proxies configured on the enterprise deployment all traffic are steered to the web proxy making it difficult for classification and direct internet breakout. The solution is to exclude SaaS application traffic from getting proxied by customizing the enterprise PAC (Proxy Auto-Config) file.

Citrix SD-WAN 11.0 allows proxy bypass and local Internet breakout for Office 365 application traffic by dynamically generating and serving custom PAC file. PAC file is a JavaScript function that defines whether web browser requests go directly to the destination or to a web proxy server.

## How PAC file customization works

Ideally, the enterprise network host PAC file on the internal web server, these proxy settings are distributed via group policy. The Client browser requests for PAC files from the enterprise web server. The Citrix SD-WAN appliance serves the customized PAC files for sites where Office 365 breakout is enabled.



- 1. Citrix SD-WAN periodically requests and retrieves the latest copy of the enterprise PAC file from the enterprise web server. The Citrix SD-WAN appliance patches office 365 URLs to the enterprise PAC file. The enterprise PAC file is expected to have a placeholder (SD-WAN specific tag) where the Office 365 URLs are seamlessly patched.
- 2. The Client browser raises a DNS request for enterprise PAC file host. Citrix SD-WAN intercepts the request for the proxy configuration file FQDN and responds with the Citrix SD-WAN VIP.
- 3. The Client browser requests for the PAC file. Citrix SD-WAN appliance serves the patched PAC file locally. The PAC file includes enterprise proxy configuration and Office 365 URL exclusion policies.
- 4. On receiving a request for Office 365 application, the Citrix SD-WAN appliance performs a direct internet breakout.

## Prerequisites

- 1. The enterprises should have a PAC file hosted.
- 2. The PAC file should have a placeholder *SDWAN\_TAG* or one occurrence of *findproxyforurl* function for patching Office 365 URLs.
- 3. The PAC file URL should be domain based and not IP based.
- 4. The PAC file is served only over the trusted identity VIPs.
- 5. Citrix SD-WAN appliance should be able to download enterprise PAC file over its management interface.

## **Configure PAC file customization**

You can enable PAC file customization using Citrix SD-WAN Orchestrator service. For more information, see Proxy auto config.

## Troubleshooting

You can download the customized PAC file from the Citrix SD-WAN appliance for troubleshooting. Navigate to **Configuration > Appliance Settings > Logging/Monitoring > Application and click Download**.

Dashboard Monitoring	Configuration							
- Appliance Settings	Configuration > A	ppliance Settings >	Logging/Monitoring					
Administrator Interface	Log Options	Alert Options	Alarm Options	Syslog Server	HTTP Server	Application		
Network Adapters Net Flow	Download PAC File							
· App Flow/IPFIX · SNMP	Download							
NITRO API Licensing								
+ Virtual WAN								
+ System Maintenance								

You can also view the PAC file patching status in the **Events** section, navigate to **Configuration** > **System Maintenance** > **Diagnostics**, click **Events** tab.

													_
+ Appliance Settings	Configurati	on > System Maint	enance > Diagnostics										
+ Virtual WAN													
- System Maintenance	Ping	Traceroute	Packet Capture	Path Bandwidth	System Info	Diagnostic Data	Events	Alarms	Diagnostics Tool	Site Diagnostics			
Delete Files	Insert Ex	vent											
Restart System													
Date/Time Settings	Object Ty	pe:				APPLICA	TIONS V						
- Local Change Management	Event typ	*				UNDEFIN	IED 🔻						
- Undete Software	Severity:					INFO	•						
Configuration Reset	Add Ever	nt											
	Downlo	ad Events											
	There are curr	ently 261 in the Event	s database, spanning from	n event 1 at 2019-05-27	18:09:46 to event 261	at 2019-05-28 08:39:0	2.	1 min					
	Download eve	ents starting from 20	19 •	May	<ul> <li>27</li> </ul>	<ul> <li>18</li> </ul>	T	09	▼ 46	<ul> <li>Downlop</li> </ul>	ad (261 ever	ents)	
	Alert Co	unt											
	along Top									Aluma			-
	Emails:	pe								Alerts Se	int	0	- 1
	Syslog M	essages:								į		0	=
	SNMP Tra	aps:										0	
	View Ev	ents											
	View Ew Quantity:	ents		25 .	•								
	View Ew Quantity: Filter:	ents	[	25 vibject Type = Any	▼ ▼ Ever	nt type = Any	▼ Se	erity = Any	T				
	View Ew Quantity: Filter: Reload E	ents vents Table	[: c	25 Ibjett Type = Any	• • •	nt type = Any	▼ Se	erity = Any	T				
	View Ew Quantity: Filter: Reload E	vents Table Object ID	C Object Name	25 · · · · · · · · · · · · · · · · · · ·	Even     Object Type	nt type = Any Time	▼ Se	erity = Any	▼ Event Type	Severity	D	Dewription	
	View Ew Quantity: Filter: Reload E ID 261	vents Table Object ID 25	Object Name PAC File Patching	25 Itgiect Type = Any	Ever Object Type APPLICATIONS	nt type = Any Time 2019-	▼ 5#	erity = Any	Event Type     SUCCESS	Severity	9	Description Society pattern SHC Re with Office 355 URLS	
	View Ew Quantity: Filter: Reload E 261 260	vents Table Object ID 26 26	Object Name PAC File Patching PAC File Patching	25 v Itiject Type = Any 9	Object Type     Applications     Applications	nt type = Any Time 2019- 2019-	▼ Se 05-28 08:39:02 05-28 08:29:02	erity = Any	Event Type SUCCESS SUCCESS	Severity INFO INFO	9	Deuropsion Societ/Up packed the entropylie 34C (Te with Diffice 355 URLs Societ/Up packed the entropylie 34C (Te with Diffice 355 URLs	
	View Ew Quarrity: Filter: Reload E 10 261 260 259	vents Table Object ID 26 26 26	Object Name PAC File Patching PAC File Patching PAC File Patching	26 v bject Type = Any 3 3	Object Type APPLICATIONS APPLICATIONS APPLICATIONS	nt type = Any Time 2019- 2019- 2019-	▼ Set 05-28 08:39:02 05-28 08:29:02 05-28 08:29:02	erity = Any	Event Type SUCCESS SUCCESS SUCCESS	Severity INFO INFO INFO	2 2 2 2 2 2	Development Scientification of the entropoles RAC file with OPRice 365 URLS Scientificity control entropoles RAC file with OPRice 365 URLS Scientificity control entropoles RAC file with OPRICe 355 URLS	
	View Eve Quartity: Filter: Reload E 10 261 260 259 258	Vents Table Object ID 26 26 26 26	Object Name PAC File Patching PAC File Patching PAC File Patching PAC File Patching	25 Your Type = Any	Byer     Byer	nt type = Any Time 2019- 2019- 2019- 2019-	▼ Set 05-28 08:39:02 05-28 08:29:02 05-28 08:19:02 05-28 08:19:02	erity = Any	Event Type SUCCESS SUCCESS SUCCESS SUCCESS	Severity INFO INFO INFO INFO	2 2 2 2 2 2	Description Sociality pathod the entropole IAC file vitro Office 365 URLS Sociality pathod the entropole AC file with Office 365 URLS Sociality pathod the entropole AC file with Office 365 URLS	
	View Ev Quantity: Filter: Reload E 200 259 258 257	Vents Table Object ID 26 26 26 26 26	Cbject Name PAC File Patching PAC File Patching PAC File Patching PAC File Patching PAC File Patching PAC File Patching	25 v Hoject Type = Any 2 3 3 3 3 3 3 3 3 3 3	Dbject Type     Dbject Type     Applications     Applications     Applications     Applications     Applications     Applications	nt type = Any Time 2019- 2019- 2019- 2019- 2019- 2019- 2019-	▼ S+ -05-28 08:39:02 -05-28 08:29:02 -05-28 08:19:02 -05-28 08:09:02 -05-28 07:59:02	erity = Any	Event Type SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Severity INPO INPO INPO INPO INPO	2 2 2 2 2 2 2 2 2	Deurgeon Sociality patch the energies 34C file with Office 355 URLS Sociality patch of the energies 34C file with Office 355 URLS Sociality patch of the energies 34C file with Office 355 URLS Sociality patch of the energies 34C file with Office 355 URLS Sociality patch of the energies 34C file with Office 355 URLS	
	View Ev           Quantity:           Filter:           Reload E           10           261           200           259           258           257           256	Object ID           26	Cbject Name PAC File Patching PAC File Patching PAC File Patching PAC File Patching PAC File Patching PAC File Patching	25 v bbject Type = Any 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	•         •           •         •	nt type = Any Time 2019- 2019- 2019- 2019- 2019- 2019- 2019- 2019-	<ul> <li>Set</li> <li>05-28 08:39:02</li> <li>05-28 08:29:02</li> <li>05-28 08:19:02</li> <li>05-28 08:09:02</li> <li>05-28 07:59:02</li> <li>05-28 07:49:01</li> </ul>	eity = [Any	Event Type     SUCCESS     SUCCESS     SUCCESS     SUCCESS     SUCCESS     SUCCESS	Severity INFO INFO INFO INFO INFO	2 2 2 2 2 2 2 2 2 2 2 2 2	Description Sociately patched the entropole IAC file vitro Office 365 URLS Sociately patched the entropole IAC file vitro Office 365 URLS Sociately patched the entropole IAC file vitro Office 365 URLS Sociately patched the entropole IAC file vitro Office 365 URLS Sociately patched the entropole IAC file vitro Office 365 URLS	
	View Ev Quantity: Filter: Reload E 201 200 259 258 257 258 257 256 255	Object ID           26	Chiject Name PAC File Patchiny PAC File Patchiny PAC File Patchiny PAC File Patchiny PAC File Patching PAC File Patching PAC File Patching	25 Xanger Versen		nt type = Any Time 2019- 2019- 2019- 2019- 2019- 2019- 2019- 2019- 2019- 2019-	▼ Se 05-28 08:3902 05-28 08:9902 05-28 08:9902 05-28 08:0902 05-28 07:902 05-28 07:9021	erity = Any	Event Type SUCCESS SUCCES	Severity INFO INFO INFO INFO INFO INFO	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Description Sociality pathed the entropole 34C file with Office 355 ULS Sociality pathed the entropole 34C file with Office 355 ULS Sociality pathed the entropole 34C file with Office 355 ULS Sociality pathed the entropole 34C file with Office 355 ULS Sociality pathed the entropole 34C file with Office 355 ULS Sociality pathed the entropole 34C file with Office 355 ULS Sociality pathed the entropole 34C file with Office 355 ULS	
	View Ex Quantity: Filter: Reload E 201 200 259 258 257 256 255 255 254		Cobject Name RAC File Patching RAC File Patching	25 • • • tbject Type = Any 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3	•         Even           •         Even           •         Even           •         APPUCATIONS	nt type = Any Time 2019- 2019- 2019- 2019- 2019- 2019- 2019- 2019- 2019-	▼ 5+ 05-28 08:3902 65-28 08:2902 65-28 08:2902 65-28 07:5902 65-28 07:5902 65-28 07:5901 65-28 07:5901 65-28 07:2901	erity = [Arry	Event Type SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Severity INFO INFO INFO INFO INFO INFO INFO INFO	2 2 2 3 3 3 3 3 2 3 2 3 3 3 3 3 3 3 3 3	Description Excertably particles the entropole RAC file with Office 355 URLS Excertably particles the entropole RAC file with Office 355 URLS Excertably particle the entropole RAC file with Office 355 URLS Excertably particle the entropole RAC file with Office 355 URLS Excertably particle the entropole RAC file with Office 355 URLS Excertably particle the entropole RAC file with Office 355 URLS Excertably particle the entropole RAC file with Office 355 URLS Excertably particle the entropole RAC file with Office 355 URLS Excertably particle the entropole RAC file with Office 355 URLS	
	View Ev Quantity: Filter: Reload E 261 260 259 258 257 256 255 255 255 254 253	ents Table Verta Table Object ID 26 26 26 26 26 26 26 26 26 26 26 26 26	Cibject Name PAC File Patching PAC File Patching	25 • • • • • • • • • • • • • • • • • • •	Disject Type     APPUCATIONS	nt type = Any Time 2019- 2019- 2019- 2019- 2019- 2019- 2019- 2019- 2019- 2019- 2019-	▼ See 05-20 06:3902 05-28 08:2902 05-28 08:2902 05-28 07:5902 05-28 07:5902 05-28 07:5901 05-28 07:5901 05-28 07:901 05-28 07:1901	erity = Ary	Event Type     SUCCESS	Severity INFO INFO INFO INFO INFO INFO INFO INFO	2 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	Description Socially patched the entropole IAC file vitro Office 395 URL5 Socially patched the entropole IAC file with Office 395 URL5 Socially patched the entropole IAC file with Office 395 URL5 Socially patched the entropole IAC file with Office 395 URL5 Socially patched the entropole IAC file with Office 395 URL5 Socially patched the entropole IAC file with Office 395 URL5 Socially patched the entropole IAC file with Office 395 URL5 Socially patched the entropole IAC file with Office 395 URL5 Socially patched the entropole IAC file with Office 395 URL5 Socially patched the entropole IAC file with Office 395 URL5 Socially patched the entropole IAC file with Office 395 URL5 Socially patched the IAI Social	
	View Ex           Quantity:           Filter:           Reload E           261           263           259           258           257           256           255           254           253           253           253	ents Table Object ID 26 26 26 26 26 26 26 26 26 26 26 26 26	Clogect Name RAC File Patching RAC File Patching	25 • • • • • • • • • • • • • • • • • • •	Closert Type Apopulcations Apopulcations Apopulcations Apopulcations Apopulcations Apopulcations Apopulcations Apopulcations Apopulcations	rt type = Time 2010 2019 2019 2019 2019 2019 2019 2019	See     S	with a Any	Event Type SUCCESS SUCCES	5ewrthy 1870 1870 1870 1870 1870 1870 1870 1870	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Description  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality protection for exemption EAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient of the emergine FAC file with Office 365 URL3  Sociality patient office FAC file with Office 365 URL3  Sociality patient office FAC file with Office 365 URL3  Sociality patient office FAC file FAC file With Office 365 URL3  Sociality patient office FAC file FAC f	
	View Ex Quantity: Filter: Reload E 201 203 203 203 203 203 203 203 203 203 203	ents vers Table Object ID 26 26 26 26 26 26 26 26 26 26	COBject Name PAC File Paching PAC File Paching	25 V bitet Type = Any 2 2 2 2 2 2 2 2 2 2 2 2 2	Clefect Type     Clefect Type     Applications	rt type = Ary 2019- 2010	<ul> <li>5#</li> <li>5=</li> <li>65-28 08:3902</li> <li>65-28 08:2902</li> <li>65-28 08:2902</li> <li>65-28 08:2902</li> <li>65-28 07:3901</li> </ul>	erity = Any	Event Type     SUCCESS	5welty N/O N/O N/O N/O N/O N/O N/O N/O N/O	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Description Sociality activates the entropole BAC file with Office 355 URLS Sociality activates the entropole BAC file With Office 355 URLS Sociality activates the entropole BAC file With Office 355 URLS Sociality activates the entropole BAC file With Office 355 URLS Sociality activates the entropole BAC file With Of	
	View Ex Quantity: Filter: Reload E 200 259 258 257 256 255 255 255 255 255 255 255 255 255	ents Table verts Table 26 26 26 26 26 26 26 26 26 26 26 26 26	Colject Name           SAC FIL Pach           PAC FIL Pach </td <td>225 * * * Avy 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2</td> <td>Object Type           APPUCATIONS           APPUCATIONS</td> <td>tt type = Any 2019 2019 2019 2019 2019 2019 2019 2019</td> <td>▼ 5+ 05-28 083902 05-28 082902 05-28 082902 05-28 075902 05-28 075902 05-28 075901 05-28 075901 05-28 075901 05-28 075901 05-28 05901 05-28 05500 05-28 05000 05-28 05000 05-28 05000 05-28 050000000</td> <td>erity = Any</td> <td>Event Type     Success     Success</td> <td>5000110 NO NO NO NO NO NO NO NO NO NO</td> <td>2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2</td> <td>Devription  Security pathed the entropice AIC fee with Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355</td> <td></td>	225 * * * Avy 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Object Type           APPUCATIONS	tt type = Any 2019 2019 2019 2019 2019 2019 2019 2019	▼ 5+ 05-28 083902 05-28 082902 05-28 082902 05-28 075902 05-28 075902 05-28 075901 05-28 075901 05-28 075901 05-28 075901 05-28 05901 05-28 05500 05-28 05000 05-28 05000 05-28 05000 05-28 050000000	erity = Any	Event Type     Success     Success	5000110 NO NO NO NO NO NO NO NO NO NO	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Devription  Security pathed the entropice AIC fee with Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355 URLS  Security pathed the entropice AIC is an Office 355	

## Limitations

- HTTPS PAC file server requests are not supported.
- Multiple PAC files in a network are not supported, including PAC files for routing domains or security zones.
- Generating PAC file on Citrix SD-WAN from scratch is not supported.
- WPAD through DHCP is not supported.

# **GRE tunnel**

August 24, 2022

The GRE Tunnel feature allows you to configure Citrix SD-WAN Appliances to terminate GRE tunnels on the LAN or Intranet.To configure a GRE Tunnel using SD-WAN Orchestrator service, see <u>GRE service</u>.

# In-band and backup management

August 24, 2022

## In-band management

Citrix SD-WAN allows you to manage the SD-WAN appliance in two ways, out-of-band management and in-band management. Out-of-band management allows you to create a management IP using a port reserved for management, which carries management traffic only. In-band management allows you to use the SD-WAN data ports for management. It carries both data and management traffic, without having to configure an addition management path.

In-band management allows virtual IP addresses to connect to management services such as web UI and SSH. You can enable In-band management on multiple trusted interfaces that are enabled to be used for IP services. You can access the web UI and SSH using the management IP and in-band virtual IPs.

From Citrix SD-WAN 11.4.2 release onwards, it is mandatory to configure In-band management to establish connectivity to Citrix SD-WAN Orchestrator service through an In-band management port. Otherwise, the appliance loses connectivity to Citrix SD-WAN Orchestrator service when the management port is not connected and the In-band IP address is also not configured.

## Note

- Citrix SD-WAN Orchestrator service does not allow configuring **Service Type** as **Any** for destination NAT policies.
- Avoid disabling the service when the only management connectivity is in-band HA. You can get yourself locked out of the appliance if you disable the service.

From Citrix SD-WAN 11.5 onwards, you can enable in-band management on a virtual IP only through Citrix SD-WAN Orchestrator service. For more information, see Inband management.

From Citrix SD-WAN 11.3.1 release onwards, In-band management supports High Availability appliance pairs. The communication between the primary and secondary appliances happen through the virtual interfaces using NAT.

The following ports allow communication with management services on the HA appliances:

- HTTPS
  - 443 Connects to the HA active
  - 444 Redirects to the HA primary
  - 445 Redirects to the HA secondary
- SSH
  - 22 Connects to the HA active
  - 23 Redirects to the HA primary
  - 24 Redirects to the HA secondary
- SNMP
  - 161 Connects to the HA active
  - 162 Redirects to the HA primary
  - 163 Redirects to the HA secondary

Use destination NAT policies to create IP addresses that allow connectivity to In-band HA without the need to enter a port.

For example, the following in-band IP addresses are used to access the appliances:

- Active appliance 1.0.1.2
- Primary appliance 1.0.1.10
- Secondary appliance 1.0.1.11

#### **Monitoring in-band management**

In the preceding example, we have enabled in-band management on 172.170.10.78 virtual IP. You can use this IP to access the web UI and SSH.

In the web UI navigate to **Monitoring** > **Firewall**. You can see SSH and web UI accessed using the virtual IP on port 22 and 443 respectively in the **Destination IP address** column.

$\rightarrow$	C 🔺 N	Not secure   http://172.170.10.78/cy	-bin/vwmoi	n.cgi																			☆
																			to		-	Logout	c
	Dashboard	Monitoring Configura	tion																				
2	Monitoring	> Firewall																					
	Firewall S	Statistics																					
s t	itatistics: Aaximum entr o display:	Connections																					
F	iltering:	Routing Domain: Any	•	A	pplication:		Any		Family:	Any		•	-										
		IP Protocol: Any		• •	ource Zone:		Any		Destination 20     Seurce ID:	ne: Any			• 	- Dente									
		Destination Service Type: Any			actination Service Ins	a Instan	cer Any	•	Destination IP	172 170 1	1 78		Dertir	ation Port *									
	Refresh Clear Connec Ielp Connectio	Ctions ons	Show Drops	5																			
							s	ource				Destina	ation					Ser	ıt			Recei	ved
	Routing Domain	Application	Family	IP Protocol	IP Adress	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	ls NAT	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS
	Corporate	Secure Shell(ssh)	Encrypted	TCP	172.170.10.135	54257	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	22	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	78	6824	0.364	0.255	53	7429	0.247
	Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54298	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	139	10130	5.692	3.319	234	338338	9.583
	Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54299	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	565	28811	23.147	9.443	1087	1594099	44.533
	Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54300	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	90	9201	3.691	3.019	157	212744	6.439
	Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54301	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	ESTABLISHED	No	111	7987	4.554	2.621	202	291743	8.287
	Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54302	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	CLOSED	No	6	776	0.419	0.434	4	309	0.280
	Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.135	54303	Local	VirtualInterface-1	Default_LAN_Zone	172.170.10.78	443	IPHost	-	Default_LAN_Zone	CLOSED	No	6	776	0.422	0.437	4	309	0.282
	Corporate	Hyperlext Iranster Protocol Secure(https)	Web	ICP	1/2.1/0.10.135	54289	Local	VirtualInterface-1	Detault_LAN_Zone	1/2.1/0.10.78	443	IPHost	1	Detault_LAN_Zone	CLOSED	No	355	20266	13.558 /	-\@(1923)	te \6661	082449	25.435

## **In-band provisioning**

The need to deploy SD-WAN appliances in simpler environments like home or small branches has increased significantly. Configuring separate management access for simpler deployments is an added overhead. Zero-touch deployment along with in-band management feature enables provisioning and configuration management via designated data ports. Zero-touch deployment is now supported on the designated data ports and there is no need to use a separate management port for zero-touch deployment. Citrix SD-WAN also allows to fail over management traffic seamlessly to the management port when the data port goes down and vice versa.

An appliance in factory shipped state, that supports in-band provisioning, can be provisioned by simply connecting the data or management port to the internet. The appliances that support in-band provisioning have specific ports for LAN and WAN. The appliance in factory reset state has a default configuration that allows to establish a connection with the zero-touch deployment service. The LAN port acts as the DHCP server and assigns a dynamic IP to the WAN port that acts as a DHCP client. The WAN links monitor the Quad 9 DNS service to determine WAN connectivity.

## Note

In-band provisioning is applicable to SD-WAN 110 SE and SD-WAN VPX platforms only.

Once the IP address is obtained and a connection is established with the zero-touch deployment service the configuration packages are downloaded and installed on the appliance.

**Note**: For day-0 provisioning of SD-WAN appliances through the data ports, the appliance software version must be SD-WAN 11.1.0 or higher.

The default configuration of an appliance in factory reset state includes the following configurations:

- DHCP Server on LAN port
- DHCP client on WAN port
- QUAD9 configuration for DNS
- Default LAN IP is 192.168.0.1
- Grace License of 35 days.

Once the appliance is provisioned, the default configuration is disabled and is overridden by the configuration received from the zero-touch deployment service. If an appliance license or grace license expiries, the default configuration is activated, to ensure that the appliance remains connected to the zero-touch deployment service and receives licenses managed via zero-touch deployment.

## Default/Fallback configuration

210

VPX

1100

210-LTE

Fallback configuration ensures that the appliance remains connected to the zero-touch deployment service if there is link failure, configuration mismatch, or software mismatch. Fallback configuration is enabled by default on the appliances that have a default configuration profile. You can also edit the fallback configuration as per your existing LAN network settings.

**Note**: After the initial appliance provisioning, ensure that the fallback configuration is enabled for zero-touch deployment service connectivity.

 Platform
 WAN Ports
 LAN Ports

 110
 1/2
 1/1

 110-LTE
 1/2, LTE-1
 1/1

1/4, 1/5

2

1/4, 1/5, LTE-1

1/4, 1/5, 1/6

1/3

1/3

1/3 (FTB)

1

The following table provides the details of pre-designated WAN and LAN ports for fallback configuration on different platforms:

From Citrix SD-WAN 11.3.1 release, the WAN port settings are configurable. WAN ports can be config
ured as independent WAN Links using DHCP client and monitor the Quad9 DNS service to determine

WAN connectivity. You can configure WAN IPs/static IPs for the WAN ports in the absence of DHCP to use In-band management for initial provisioning.

#### Note

You can only configure the Ethernet ports with the static IPs. The static IPs are not configurable with LTE-1 and LTE-E1 ports. Though you can add the LTE-1 and LTE-E1 port as WAN, the configuration fields remain non-editable.

When you add a WAN port, it gets added under the **WAN Settings (Port: 2)** section with the **DHCP Mode** check box selected by default. If the **DHCP Mode** check box is selected, the **IP Address, Gateway IP Address,** and the **VLAN ID** text fields are grayed out. Clear the **DHCP Mode** check box, if you want to configure the static IP.

N Settings (I	Ports: 2)				
DHCP Mode	IP Address	Gateway IP Address	VLAN ID	Wan Tracking IP Address	
	11.11.11.10/24	11.11.11.11	50		
				9.9.9.9	
				9.9.9.9	
	V Settings (I	V Settings (Ports: 2)           : DHCP Mode         IP Address           : 11.11.10/24	V Settings (Ports: 2)       c DHCP Mode     IP Address       Gateway IP Address       11.11.11.0/24       11.11.11.11       Image: Comparison of C	V Settings (Ports: 2)       C DHCP Mode     IP Address     Gateway IP Address     VLAN ID       11.11.11.0/24     11.11.11     50	V Settings (Ports: 2)           C DHCP Mode         IP Address         Gateway IP Address         VLAN ID         Wan Tracking IP Address           11.11.11.0/24         11.11.11         50

By default the **WAN Tracking IP Address** field is auto filled with the 9.9.9.9. You can change the address as needed.

#### Note

If you are selecting the **Dynamic DNS Servers** check box, ensure to add/configure at least one WAN port with the **DHCP Mode** selected.

## **Configurable Management or Data port**

In-band management allows the data ports to carry both data and management traffic, eliminating the need for a dedicated management port. This leaves the management port unused on the low end appliances, which already have low port density. Citrix SD-WAN allows you to configure the management port to operate as either a data port or a management port.

#### Note

You can convert the management port to data port only on the following platforms:

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

You can configure a management port only when in-band management is enabled on other trusted interfaces on the appliance.

## **Backup management network**

You can configure a virtual IP address as a back-up management network. It is used as the management IP address if the management port is not configured with a default gateway.

Note

If a site has an Internet service configured with a single routing domain, a trusted interface with identity enabled is selected as the backup management network by default.

## Monitoring backup management

In the preceding example, we have selected 172.170.10.78 virtual IP as the backup management network. If the management IP address is not configured with a default gateway, you can use this IP to access the web UI and SSH.

In the web UI navigate to **Monitoring** > **Firewall**. You can see this virtual IP address as the source IP address for SSH and web UI access.

Monitoring	> Firewall																					
																						_
Firewall	Statistics																					
Statistics:	Connections •																					
Maximum ent	ries 50 v																					
Filtering:	Routing Domain: Any		Applica	ition:	[	Any		<ul> <li>Family:</li> </ul>	An	,		•										
	IP Protocol: Any		<ul> <li>Source</li> </ul>	Zone:		Anv		• Destinati	on Zone: Am	,		•										
	Source Service Type: Any		Source	Service Instanc	~ [	Any T		Source IP	► 172	170 10	78	Source Port										
	Destination Service Type: Any		Destina	tion Service Ins	tance	Any T		Destinati	on IP:			Destination	Port: *									
Refresh	Show latest data	Show Drops																				
Clear Conne	utions .	now props																				
Help	cuons																					
Connect	ons																					
						Source						Destination					Sei	it			Recei	wed
Routing Domain	Application	Family	IP Protocol	IP Adress	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State *	ls NAT	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS
Corporate	Transmission Control Protocol(tcp)	Network Service	тср	172.170.10.78	49818	IPHost	-	Default_LAN_Zone	18.210.2.1	1 443	Internet	Branch1-Internet	Untrusted_Internet_Zone	SYN_SENT	Yes	1	60	-	-	0	0	-
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	58939	IPHost	÷	Default_LAN_Zone	10.105.147.1	4 53	Internet	Branch1-Internet	Untrusted_Internet_Zone	NEW	Yes	2	148	-		0	0	
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	43012	IPHost		Default_LAN_Zone	10.105.147.1	4 53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	168	0.070	0.047	2	297	0.070
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	36558	IPHost		Default_LAN_Zone	10.105.147.1	4 53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	148	0.011	0.007	2	277	0.011
Corporate	HyperText Transfer Protocol Secure(https)	Web	TCP	172.170.10.78	60624	IPHost	-	Default_LAN_Zone	18.235.40.	8 443	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	9	1271	0.176	0.199	7	4069	0.137
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	60585	IPHost	÷	Default_LAN_Zone	10.105.147.1	4 53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.003	0.002	1	128	0.003
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	58010	IPHost	÷	Default_LAN_Zone	10.105.147.1	4 53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.020	0.013	1	80	0.020
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	36684	IPHost		Default_LAN_Zone	10.105.147.1	4 53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.006	0.004	1	161	0.006
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	33173	IPHost		Default_LAN_Zone	10.105.147.1	4 53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.003	0.002	1	80	0.003
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	53914	IPHost		Default_LAN_Zone	10.105.147.1	4 53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	80	0.006	0.004	1	128	0.006
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	53708	IPHost	-	Default_LAN_Zone	10.105.147.1	4 53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	2	128	ctfNat	e <b>000</b>	dow§	144	0.013
Corporate	Domain Name Service(dns)	Network Service	UDP	172.170.10.78	43704	IPHost	÷	Default_LAN_Zone	10.105.147.1	4 53	Internet	Branch1-Internet	Untrusted_Internet_Zone	ESTABLISHED	Yes	1	<b>80</b> G	0/02001	tti <b>0,013</b> to	activate	e W <b>ize</b> lo	>\0;02C

## **Internet access**

September 19, 2022

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

For information on how to configure an Internet service through Citrix SD-WAN Orchestrator service, see Internet Service.

#### Internet Traffic Control



## **Direct Internet Breakout at Branch with Integrated Firewall**

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.

For information on how to configure an Internet service through Citrix SD-WAN Orchestrator service, see Internet Service.



Direct Internet Breakout at Branch with Integrated Firewall

# **Direct Internet Access with Secure Web Gateway**

To secure traffic and enforce policies, enterprises often use MPLS links to backhaul branch traffic to the corporate data center. The data center applies security policies, filters traffic through security appliances to detect malware, and routes the traffic through an ISP. Such backhauling over private MPLS links is expensive. It also results in significant latency, which creates a poor user experience at the branch site. There is also a risk that users bypass your security controls.

An alternative to backhauling is to add security appliances at the branch. However, the cost and complexity increases as you install multiple appliances to maintain consistent policies across the sites. Most significantly, if you have many branch offices, cost management becomes impractical.

One alternative is to enforce security without adding cost, complexity, or latency would be to route all branch Internet traffic using Citrix SD-WAN to the Secure Web Gateway Service. A third-party Secure Web Gateway Service enables granular and central security policy creation to be using by all connected networks. The policies are applied consistently whether the user is at the data center or a branch site. Because Secure Web Gateway solutions are cloud based, you don't have to add more costly security appliances to the network. For information on how to configure an Internet service through Citrix SD-WAN Orchestrator service, see Internet Service.

## 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
- Citrix Secure Internet Access

## **Backhaul Internet**

The Citrix SD-WAN solution can backhaul Internet traffic to the MCN site or other branch sites. Backhaul indicates that the traffic destined for the Internet is sent back through another predefined site that can access the Internet. It is useful for networks that do not allow Internet access directly because of security concerns or the underlay networks topology. An example would be a remote site that lacks an external firewall where the on-board SD-WAN firewall does not meet the security requirements for that site. For some environments, backhauling all remote site internet traffic through the hardened DMZ at the Data Center might be the best approach to providing Internet access to users at remote offices. This approach does however have its limitations to be aware of following and the underlay WAN links size appropriately.

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

## **Backhaul Internet to Data Center MCN**



All Citrix SD-WAN devices can terminate up to eight distinct Internet WAN links into a single device. Licensed throughput capabilities for the aggregated WAN links are listed per respective appliance on the Citrix SD-WAN data sheet.

## Hairpin Mode

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.

## **Backhaul Internet to Data Center MCN**



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 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.

# **Hosted firewalls**

## September 19, 2022

Citrix SD-WAN Orchestrator service supports the following hosted firewalls:

- Palo Alto Networks
- Check Point

## Palo Alto Networks firewall integration on SD-WAN 1100 platform

Citrix SD-WAN supports hosting Palo Alto Networks Next-Generation Virtual Machine (VM)-Series Firewall on the SD-WAN 1100 platform. The following are the supported virtual machine models:

- VM 50
- VM 100

The Palo Alto Network virtual machine series firewall runs as a virtual machine on SD-WAN 1100 platform. The firewall virtual machine is integrated in **Virtual Wire** mode with two data virtual interfaces connected to it. Required traffic can be redirected to the firewall virtual machine by configuring policies on SD-WAN.

For information on how to provision the firewall virtual machine through SD-WAN Orchestrator service, see Hosted firewalls.

## Benefits

The following are the primary goals or benefits of Palo Alto Networks integration on the SD-WAN 1100 platform:

- Branch device consolidation: A single appliance that does both SD-WAN and advanced security.
- Branch office security with on-prem NGFW (Next Generation Firewall) to protect LAN-to-LAN, LAN-to-Internet, and Internet-to-LAN traffic.

## Firewall virtual machine provisioning through SD-WAN appliance GUI

On SD-WAN platform, provision and boot up the hosted virtual machine. Perform the following steps for provisioning:

- 1. From Citrix SD-WAN GUI, navigate to **Configuration >** expand **Appliance Settings >** select **Hosted Firewall**.
- 2. Upload the software image:
  - Select the Software Images tab. Select the Vendor name as Palo Alto Networks.
  - Choose the software image file.
  - Click Upload.

Dashboard Monitoring	Configuration		
- Appliance Settings	Configuration > Appliance Settings > Host	ted Firewall	
- Administrator interface - Logging/Monitoring - Network Adapters - Net Flow	Hosted Firewalls Software Images	Upload Software Image X J	
– App Flow/IPFIX – SNMP – NITRO API	Search:	Vendor Name Palo Alto Networks Upload Image* Choose file No file chosen	Upload Delete File Size
Licensing Hosted Firewall + Virtual WAN		Upload Cancel	
+ System Maintenance			

#### Note

Maximum of two software image can be uploaded. Uploading of the Palo Alto Networks virtual machine image might take longer time depending on the bandwidth availability.

You can see a status bar to track the upload process. The file detail reflects, once the image is uploaded successfully. The image that is used for provisioning cannot be deleted. Do not perform any action or go back to any other page until the image file shows 100% uploaded.

3. For provisioning, select **Hosted Firewalls** tab and click **Provision** button.

Dashboard Monitoring	Configuration		
Administrator Interface     Logging/Monitoring     Network Adapters     Net Flow     App:Row/PFIX     SNAP	Configuration > Appliance Settings > Hosted Firewall Hosted Firewalls Software Images Hosted Firewall Information Search	Provision Start Shutdown D	Deprovision Refresh
- NITRO API Licensing Fallback Configuration Hosted Firewall	Vendor ▲         Model         File Name         Admin State         Processing State           No Virtual Machines Provisioned.         Model         File Name         Admin State         Processing State	SD-WAN Redirection Counters Packets Sent Packets Received Packets Dropped	Device Access
Cloud Direct Service + Virtual WAN + System Maintenance	Operations Log No operations log available		<u>^</u>

- 4. Provide the following details for provisioning.
  - Vendor Name: Select the Vendor as Palo Alto Networks.
  - Virtual Machine Model: Select the virtual machine model number from the list.
  - Image File Name: Select the Image file.
  - **Panorama Primary IP Address/Domain Name**: Provide the Panorama primary IP address or fully qualified domain name (Optional).
  - **Panorama Secondary IP Address/Domain Name**: Provide the Panorama secondary IP address or fully qualified domain name (Optional).
  - Virtual Machine Authentication Key: Provide the virtual machine authentication key (Optional).

Virtual Machine Authentication Key is needed for automatic registration of the Palo Alto Networks virtual machine to the Panorama.

- **Authentication Code**: Enter the authentication code (virtual machine license code) (Optional).
- Click Apply.

Dashooard monitoring	Configuration			
- Appliance Settings	Configuration > Appliance Settin	ngs > Hosted Firewall		
Administrator Interface Logging/Monitoring	Hosted Firewalls Softw	are Images		
Network Adapters	Hosted Firewall Informati	Provision Virtual Machine		* /
App Flow/IPFIX		Vendor Name*	Palo Alto Networks	+++++++++++++++++++++++++++++++++++++++
SNMP	Search:	Virtual Machine Model*	VM100 \$	utdown Deprovision Refresh
NITRO API	Vendor Model F	Image File Name*	PA-VM-KVM-9.0.1.qco \$	in State Device Access
Hosted Firewall	No Virtual Machines Provisioned.	Panorama Primary IP Address/Domain Name		
+ Virtual WAN	Operations Log	Panorama Secondary IP Address/Domain Name		7111111111
+ System Maintenance	No operations log available	Virtual Machine Authentication Key Authentication Code		
			Apply Cance	A

5. Click **Refresh** to get the latest status. After the Palo Alto Networks virtual machine is completely bootup, it will reflect on the SD-WAN UI with the operations Log detail.

Dashboard Monitoring	Configuration									
- Appliance Settings	Configuration > Appliance Setting	gs > Hosted Firewall								
- Administrator Interface - Logging/Monitoring - Network Adapters	Hosted Firewalls Softwa	re Images								
Net Flow	Hosted Firewall Information	1								
- App Flow/IPFIX - SNMP	Search					Provision	Start	Shutdown	Deprovision	Refresh
- NITRO API	Vendor A Model	File Name	Management Server Primary IP	Management Server Secondary IP	Admin State	Processing State	Packets Sent	Packets Received	Packets Dropped	Device Access
Hosted Firewall	Palo Alto Networks VM100	PA-VM-KVM-9.0.1.qcow2	- NA -	- NA -	Up	Up	3038	3038	0	Click Here
Cloud Direct Service										
+ Virtual WAN	Operations Log									
+ WAN Optimization	Tue Sep 24 04:50:33 UTC 2019::	Shutdown Virtual Machine oper	ation invoked							
+ System Maintenance	Tue Sep 24 04:50:33 UTC 2019:: Tue Sep 24 04:51:05 UTC 2019:: Tue Sep 24 04:51:58 UTC 2019::	Waiting for Virtual Machine to : Virtual Machine shutdown com Shutdown Virtual Machine oper	shutdown pleted ration invoked							
	Tue Sep 24 04:51:58 UTC 2019:: I Tue Sep 24 04:51:58 UTC 2019:: I Tue Sep 24 04:52:28 UTC 2019:: Tue Sep 24 04:52:08 UTC 2019:: Tue Sep 24 04:55:08 UTC 2019::	Failed to shutdown the Virtual Waiting for Virtual Machine to : Virtual Machine shutdown oper Start Virtual Machine operation	Machine shutdown rated timedout i invoked							

- Admin State: Indicates if the virtual machine is up or down.
- Processing State: Datapath processing state of the virtual machine.
- Packet Sent: Packets sent from SD-WAN to the security virtual machine.
- **Packet Received**: Packets received by SD-WAN from the security virtual machine.
- **Packet Dropped**: Packets dropped by SD-WAN (for example, when the security virtual machine is down).
- **Device Access**: Click the link to get the GUI access to the security virtual machine.

You can **Start, Shutdown,** and **Deprovision** the virtual machine as needed. Use **Click Here** option to access the Palo Alto Networks virtual machine GUI or use your management IP along with 4100 port (management IP: 4100).

Note

Always use incognito mode to access the Palo Alto Networks GUI.

## Check Point firewall integration the on SD-WAN 1100 platform

Citrix SD-WAN supports hosting Check Point Quantum Edge on the SD-WAN 1100 platform.

The **Check Point Quantum Edge** runs as a virtual machine on the SD-WAN 1100 SE platform. The firewall virtual machine is integrated in Bridge mode with two data virtual interfaces connected to it. Required traffic can be redirected to the firewall virtual machine by configuring policies on SD-WAN.

For information on how to provision the firewall virtual machine through SD-WAN Orchestrator service, see Hosted firewalls.

#### Note

From Citrix SD-WAN 11.3.1 onwards, the Check Point VM version 80.20 and above are supported for provisioning VM on new sites.

## Benefits

The following are the primary goals or benefits of Check Point integration on the SD-WAN 1100 platform:

- Branch device consolidation: A single appliance that does both SD-WAN and advanced security
- Branch office security with on-prem NGFW (Next Generation Firewall) to protect LAN-to-LAN, LAN-to-Internet, and Internet-to-LAN traffic

## Firewall virtual machine provisioning through SD-WAN appliance GUI

On SD-WAN platform, provision and boot up the hosted virtual machine. Perform the following steps for provisioning:

- 1. From the Citrix SD-WAN GUI, navigate to **Configuration > Appliance Settings >** select **Hosted Firewall**.
- 2. Upload the software image:
  - Select the **Software Images** tab. Select the **Vendor Name** as Check Point.
  - Choose the software image file.
  - Click Upload.

- Appliance Settings	Configuratio	n > Appliance Settings > Hosted Firewall				
Administrator Interface Logging/Monitoring Network Adapters Net Enw	Hosted I	irewalls Software Images	Upload Software Image	×/		
- App Flow/IPFIX - SNMP - NITRO API	Search		Vendor Name Palo Alto Networks   Upload image* Palo Alto Networks sen			Upload Delete
- Licensing	1 Maple 1	シャナイト・アイト・アイト	CHICK P LAN		dor	File Size
- Fallback Configuration	0	fw1_x86_dep_R77_990172961_20_citrix.qcov		Upload Cancel	1111111	134.00 MB
Hosted Firewall		PA-VM-KVM-9.0.1.qcow2				3.02 GB
Cloud Direct Service	11111					
+ Virtual WAN						

#### Note

Maximum of two images can be uploaded. Uploading of the Check Point virtual machine image might take longer time depending on the bandwidth availability.

You can see a status bar to track the upload process. The file detail reflects, once the image is uploaded successfully. The image that is used for provisioning cannot be deleted. Do not perform any action or go back to any other page until the image file shows 100% uploaded.

3. For provisioning, select **Hosted Firewall** tab > click **Provision** button.

Dashboard Monitoring	Configuration		
Appliance Settings     Administrator Interface     Logging/Monitoring     Network Adapters     Net Row     App Flow/IPFDX     SNMP	Configuration > Appliance Settings > Hosted Firewall Hosted Firewalls Software Images Hosted Firewall Information Cauch	Provision Start Studioum Deprovisi	on Refresh
- NITRO API - Licensing - Fallback Configuration	Vendor A Model File Name Admin State Processing State No Virtual Machines Provisioned.	SD-WAN Redirection Counters           Packets Sent         Packets Received         Packets Dropped         Devi	ce Access
Cloud Direct Service + Virtual WAN + System Maintenance	Operations Log No operations iog available		

- 4. Provide the following details for provisioning.
  - Vendor Name: Select the Vendor Name as Check Point.
  - Virtual Machine Model: The virtual machine model is auto filled as Edge.
  - Image File Name: The image file name is auto-populated.
  - Check Point Management Server IP Address/Domain: Provide the check point management server IP address/domain.
  - SIC Key: Provide the SIC key (Optional). SIC creates trusted connections between Check Point components. Click Apply.

Administrator Interface     Logging/Monitoring	Configuration > Appliance Settings > Ho Hosted Firewalls Software Images	sted Firewall		
- Network Adapters - Net Flow	Hosted Firewall Information	Provision Virtual Machine	* /	•
App Flow/IPFIX SNMP NITRO API Licensing Fallback Configuration Hosted Firewall Cloud Direct Service	Search Vendor A Model File N No Virtual Michines Provisioned.	Vendor Name" Virtual Machine Model" Image Pile Name" Check Point Management Server IP Address/Domain Name SIC Key	Check Point  EDC  TOT  TOT  TOT  TOT  TOT  TOT  TOT  T	Skits Dropped Device Access
Virtual WAN System Maintenance	No operations log available		Apply Cancel	

5. Click **Refresh** to get the latest status. After the Check Point virtual machine is completely bootup, it will reflect on the SD-WAN UI with the operations Log detail.

Dashboard Monitoring	Configuration							
- Appliance Settings	Configuration > Applian	e Settings > Hosted Firewall						
Administrator Interface Logging/Monitoring Network Adapters Net Flow	Hosted Firewalls Hosted Firewall Infor	Software Images mation						
App Flow/IPFIX SNMP NITRO API	Search					Provision Start	Shutdown Depre	ovision Refresh
Licensing						SD-WAN Redirection Coun	ters	
Fallback Configuration	Vendor ^ Moo	el File Name	Admin State	Processing State	Packets Sent	Packets Received	Packets Dropped	Device Access
Hosted Firewall	Check Point ED	E fw1_x86_dep_R77_990172961_20_citrix.qcow2	Up	Up	208496	243124	92205	Click Here
Cloud Direct Service     Virtual WAN     System Maintenance	Operations Log	20 Provisioning operation invoked 20.: Preparing the Virtual Machine files						
- apprent monitorianAC	Wed Jun 3 02:44:42 UTC 2 Wed Jun 3 02:44:43 UTC 2 Wed Jun 3 02:44:44 UTC 2	202: Defining the Virtual Machine 202: Start Virtual Machine 202: Start Virtual Machine operation invoked 202: Check Virtual Machine status 202: Virtual Machine is running successfully 202: Virtual Machine is rouning Completed						

- Admin State: Indicates if the virtual machine is up or down.
- **Processing State**: Datapath processing state of the virtual machine.
- Packet Sent: Packets sent from SD-WAN to the security virtual machine.
- **Packet Received**: Packets received by SD-WAN from the security virtual machine.
- **Packet Dropped**: Packets dropped by SD-WAN (for example, when the security virtual machine is down).
- **Device Access**: Click the link to get the GUI access to the security virtual machine.

You can **Start, Shutdown,** and **Deprovision** the virtual machine as needed. Use **Click Here** option to access the Check Point virtual machine GUI or use your management IP along with 4100 port (management IP: 4100).

Note

Always use incognito mode to access the Check Point GUI.

While all the network configuration is up and running mode, you can monitor the connection under **Monitoring > Firewall > Filter Policies**.

atistics	Monito	ing >	Firewa	all															
ows																			
outing Protocols	Firew	all Sta	tistic	s															
rewall	Statistics		Filte	r Policies	•														
E/IPsec	Maximur	n entries	50	\$															
MP	to displa	r:	Annl	ication:	Anv	,		A F	amily	Any		•	IP Protocol:	hrav.		•			
rformanco Poporte	rinering.		- appr	D. I'				s	ource	2007		•	Source	aly		•			
s Penests			Actio	n:	Any	1	\$	S	ervice ype:	Any	\$		Service Name:	Any \$			Source I	IP: *	
s reports			Sour	co Port				D	estinatio	an Anu	•		Destination				Destina	tion .	
age Reports			Sour	ce Port:				S T	ype:	Any	•		Name:	any 🗸			IP:		
11 1 11 1 m			Dest	ination	٠			S Z	ource one:	Any		\$	Destination Zone:	Any			DSCP:	Any	\$
allability Reports			1.016																
ppliance Reports	Refresh			how late	st														
Allability Reports opliance Reports HCP Server/Relay	Refresh Help		□ S data	how late	st														
anability Reports opliance Reports ICP Server/Relay	Refresh Help		□ SI data.	how late	st														
Autability Reports opliance Reports 4CP Server/Relay RRP PoE	Refresh Help Filter f	Policies	□ Si data.	how late	st														
Aliability Reports pliance Reports ICP Server/Relay RP PoE IS D	Refresh Help Filter F Default Pol Match In Po	Policies icy=Allow ogress Pa	(Not T	how late	st ckets=42 B	Sytes=3528													
AITADIITY REPORTS pliance Reports ICP Server/Relay RP PoE IS N	Refresh Help Filter f Default Pol	Policies Icy=Allow ogress Pr	(Not T	how late racked) Par 0 Bytes=0	st ckets=42 B	Sytes=3528		Source					Destination						
Allability Reports pliance Reports CP Server/Relay RP PoE S	Refresh Help Filter I Default Pol Match In Pi	Policies icy=Allow ogress Pa cation F	(Not T sckets=	racked) Pai 0 Bytes=0 IP Protocol	st ckets=42 B DSCP	Bytes=3528 Service Type	Service Name	Source IP Address	Port or s ICMP Type	Zone	Service Type	Service Name	Destination IP Address	Port or ICMP Code	Zone	Action	Conn Match Type	Track	Allo
aliability Reports pliance Reports CP Server/Relay oE S N	Refresh Help Filter F Default Pol Match In Pi ID Appli	Policies icy=Allow ogress Pa cation F	(Not T sckets=	racked) Pai 0 Bytes=0 IP Protocol	ckets=42 B	Bytes=3528 Service Type	Service Name	Source IP Address	Port or s ICMP Type NA	Zone	Service Type Internet	Service Name	Destination IP Address	Port or ICMP Code NA	Zone	Action Redirect	Conn Match Type Symmetric	Track Connection No	Allo Fragm Yes
IIIADIIITY Reports pliance Reports CP Server/Relay RP toE S	Refresh Help Filter F Default Pol Match In Pol ID Appli 1 * 2 *	Policies icy=Allow rogress Pa cation F	amily	how late racked) Par 0 Bytes=0 iP Protocol	st ckets=42 E DSCP	Bytes=3528 Service Type * internet	Service Name -	Source IP Address	Port or s ICMP Type NA NA	Zone *	Service Type Internet	Service Name -	Destination IP Address	Port or ICMP Code NA NA	Zone	Action Redirect Redirect	Conn Match Type Symmetric Symmetric	Track Connection No No	Allo Fragm Ves Ves
AIADHITY REPORTS  pliance Reports  CP Server/Relay  RP  PoE  S  I	Refresh Help Filter I Default Pol Match In Pi Match In	Policies Icy=Allow ogress Pa cation F	<pre>solution Sidata. s(Not T ackets= amily * * * *</pre>	how late racked) Pau 0 Bytes=0 IP Protocol * *	ckets=42 B DSCP	Bytes=3528 Service Type * internet	Service Name - -	Source IP Address *	Port or ICMP Type NA NA NA	Zone * *	Service Type Internet * Virtual Path	Service Name -	Destination IP Address -	Port or ICMP Code NA NA	Zone	Action Redirect Redirect Redirect	Conn Match Type Symmetric Symmetric Symmetric	Track Connection No No No	Allo Fragm Yes Yes Yes
AIADUITY REPORTS  pliance Reports  CP Server/Relay  RP  PoE  S  I	Refresh Help Filter f Default Pol Match In P	Policies Rey=Allow ogress Pa	v(Not T ackets*	how late racked) Pa 0 Bytes=0 iP Protocol * *	st ckets=42 E DSCP a a a a a	Sytes=3528 Service Type * internet * Virtual Path	Service Name - - -	Source IP Address * * *	Port or s ICMP Type NA NA NA	Zone • •	Service Type Internet * Virtual Path *	Service Name - -	Destination IP Address • •	Port or ICMP Code NA NA NA	Zone * * *	Action Redirect Redirect Redirect Redirect	Conn Match Type Symmetric Symmetric Symmetric	Track Connection No No No No	Allo Fragm Ves Yes Yes Yes
IIIADIIITY Reports pliance Reports CP Server/Relay RP SS IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Refresh Help Filter I Default Pol Match In Pi 10 Appli 1 * 2 * 3 * 4 * 5 *	Policies Icy=Allow ogress Pa cation F	<pre>v(Not T data. v(Not T ckets= amily * * * *</pre>	racked) Par 0 Bytes=0 IP Protocol * * *	st ckets= 42 E DSCP - - - - - - - - - - -	Sytes=3528 Service Type * Internet * Virtual Path IPHost	Service Name	Source IP Address * * *	Port or s ICMP Type NA NA NA NA	Zone • • •	Service Type Internet * Virtual Path * *	Service Name - - -	Destination IP Address - - -	Port or ICMP Code NA NA NA	Zone • • •	Action Redirect Redirect Redirect Allow	Conn Match Type Symmetric Symmetric Symmetric Symmetric	Track Connection No No No No No	Allo Fragm Ves Ves Ves Ves Ves Ves
IIIADIIIIY Reports pliance Reports CP Server/Relay RP SS D D	Refresh Help Filter I Default Pol Match In Pi 1 * 2 * 3 * 4 * 5 *	lolicies icy=Allow ogress Pi	e(Not T bckets= amily * * *	how late racked) Pa 0 Bytes=0 IP Protocol * * * * *	st ckets=42 E DSCP	Bytes=3528 Service Type * Internet * Virtual Path IPHost Internet	Service Name - - - - - - -	Source IP Address * *	Port or ICMP Type NA NA NA NA	Zone * * * * internet_Zone	Service Type Internet * Virtual Path * *	Service Name - - - - - - - - - - - - -	Destination IP Address • • • • • • • • • • • • • • • • • •	Port or ICMP Code NA NA NA NA 2 5001	Zone · · · · · ·	Action Redirect Redirect Redirect Allow	Conn Match Type Symmetric Symmetric Symmetric Symmetric	Track Connection No No No No No	Allo Fragm Yes Yes Yes Yes Yes

# **Link Aggregation Groups**

## August 24, 2022

The Link Aggregation Groups (LAG) functionality allows you to group two or more ports on your SD-WAN appliance to work together as a single port. This ensures increased availability, link redundancy, and enhanced performance.

Earlier, only the Active-Backup mode was supported in LAG. From Citrix SD-WAN 11.3 release onwards, the 802.3AD Link Aggregation Control Protocol (LACP) protocol based negotiations are supported. The LACP is a standard protocol and provides more functionality for LAGs.

In Active-Backup mode, at any time only one port is active and the other ports are in backup mode. The active and backup supports rely on the Data Plane Development Kit (DPDK) package for LAG functionality.

With the LACP, you can send the traffic through all the ports simultaneously. As a benefit, you get more bandwidth along with the link redundancy mechanism. The LACP implementation supports the **Active-Active** mode. Now with the Active-Backup mode, you also have an option to select full LACP Active-Active mode from the SD-WAN UI.

The LAG functionality is available only on the following DPDK supported platforms:

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 1100 SE
- Citrix SD-WAN 2100 SE
- Citrix SD-WAN 4100 SE
- Citrix SD-WAN 5100 SE
- Citrix SD-WAN 6100 SE

Note

The LAG functionality is not supported on VPX/VPXL platforms.

## Limitations

- You can create a maximum of four LAGs with a maximum of four ports grouped in each LAG on the Citrix SD-WAN appliances.
- The port priority and system priority options are not supported with the LACP implementation.

With 11.3 release onwards, in SD-WAN with the LACP implementation, the ports are always in active mode. That means SD-WAN can always start the negotiation.

Note

- For Citrix SD-WAN 210 SE appliances, you can create only one LAG with a maximum of three ports grouped in it.
- The Link State Propagation (LSP) feature is not supported if LAGs are used as Ethernet interfaces in Interface Groups.

From Citrix SD-WAN 11.5 onwards, you can configure Link aggregation groups through SD-WAN Orchestrator service. For more information, see Link aggregation groups.

## **Monitoring and Troubleshooting**

To view the statistics or the link state, navigate to **Monitoring > Statistics**. Select **Ethernet** from the **Show** drop-down list.

Statistics	Monitoring >	Statistics					
Flows							
Routing Protocols	Statistics						
irewall	Show: Ethernet	✓ □ E	nable Auto Refresh 5 🗸	econds Refresh			
KE/IPsec							
C110	Ethernet Sta	atistics					
GMP							
erformance Reports	Filter:	in Any column	Apply				
ume Verformance Reports Qos Reports	Filter:	in Any column	Apply				
enr Verformance Reports Qos Reports Jsage Reports	Filter:	in Any column	Apply of 3 entries			First Previ	ous 1 Next
erformance Reports los Reports sage Reports vailability Reports	Filter: Show 100 v en Port	in Any column tries Showing 1 to 3 o Link State	of 3 entries Frames Sent	Bytes Sent	Frames Received	First Previ Bytes Received	ous 1 Next Errors
umr erformance Reports los Reports isage Reports wailability Reports	Filter: Show 100 v en Port	in Any column tries Showing 1 to 3 to Link State	Apply Apply of 3 entries Frames Sent 228799	Bytes Sent 20119310	Frames Received 210823	First Previ Bytes Received 16480420	ous 1 Next Errors 0
verformance Reports 205 Reports Jsage Reports wailability Reports Appliance Reports	Filter: Show 100 v en Port A LAG0 1/4	in Any column tries Showing 1 to 3 o Link State UP UP	Apply Apply Apply 228799 976632	Bytes Sent 20119310 86479280	Frames Received 210823 951719	First Previ Bytes Received 16480420 79790814	ous 1 Next Errors 0 0
erformance Reports Jos Reports Isage Reports vailability Reports pppliance Reports HCP Server/Relay	Filter: Show 100 v en Port A LAG0 1/4 1/1	in Any column tries Showing 1 to 3 i Link State UP UP	Apply           Apply           Gamma Sent           228799           976632           0	Bytes Sent 20119310 86479280 0	Frames Received 210823 951719 10134	First         Previor           Bytes Received         16480420           79790814         718152	ous 1 Next Errors 0 0 0

To view the active and standby LAG ports, navigate to **Configuration** > **Appliance Settings** > **Network Adapters** > **Ethernet**.

- Appliance Settings	Configuration >	Appliance Setting	s > Network Adapter	s				
- Administrator Interface - Logging/Monitoring	IP Address	Ethernet	LACP LAG Group	Mobile Broa	adband			
Network Adapters								
Net Flow	Ethernet Inter	face Settings						
- App Flow/IPFIX - SNMP	For the 2100 platfor enabled and the por	m, settings for po t is included in the	rts 1/1, 1/2, 1/3, 1/4, 1 e Citrix configuration.	1/5, 1/6, 1/7, 1/	8, LAG0, LAG1, LAG2, LA	G3 and LT	E-E1 will only take eff	ect when the Citrix Virtual WAN Service
NITRO API	0/1: • MAC	Address: ac:1f:6b:	01:20:e4 Autonego	tiate: 🗹 Speed:	1000Mb/s	Duplex:	Full	~
- Licensing Fallback Configuration	1/4: • MAC	Address: 00:e0:ed	:7d:2a:6b Autonego	tiate: 🗹 Speed:	1000Mb/s	Duplex:	Full	~
Cloud Direct Service	1/3 : • MAC	Address: 00:e0:ed	:7d:2a:6c Autonego	tiate: 🔄 Speed:	1000Mb/s	Duplex:	Full	~
+ Virtual WAN	1/2: • MAC	Address: 00:e0:ed	:7d:2a:6d Autonego	tiate: 🔄 Speed:	1000Mb/s	Duplex:	Full	~
+ System Maintenance	1/1: • MAC	Address: 00:e0:ed	:7d:2a:6e Autonego	tiate: 🗹 Speed:	1000Mb/s	Duplex:	Full	~
	1/8: • MAC	Address: 00:e0:ed	:78:26:5f Autonego	tiate: 🗹 Speed:	Unknown	Duplex:	Unknown	~
	1/7: • MAC	Address: 00:e0:ed	:78:26:60 Autonego	tiate: 🗹 Speed:	Unknown	Duplex:	Unknown	~
	1/6 : • MAC	Address: 00:e0:ed	:78:26:61 Autonego	tiate: 🗹 Speed:	Unknown	Duplex:	Unknown	~
	1/5 : • MAC	Address: 00:e0:ed	:78:26:62 Autonego	tiate: 🗹 Speed:	Unknown	Duplex:	Unknown	~
	LAG0 : • MAC	Address: 00:e0:ed	:7d:2a:6d Autonego	tiate: 🗹 Speed:	Unknown	/ Duplex:	Full	~
	LAG1: • MAC	Address: Device no	ot configured Autonego	tiate: 🗹 Speed:	Unknown	Duplex:	Unknown	~
	LAG2 : • MAC	Address: Device no	ot configured Autonego	tiate: 🗹 Speed:	Unknown	Duplex:	Unknown	~
	LAG3 : • MAC	Address: Device no	ot configured Autonego	tiate: 🔽 Speed:	Unknown	Duplex:	Unknown	~

## Select the **LACP LAG Group** tab to view the various details related to the LACP LAG group.

- Appliance Settings	Configu	ration > Ap	pliance Settings > Network A	dapters				
- Administrator Interface - Logging/Monitoring	IP A	ddress	Ethernet LACP LAG Gr	oup Mobile Bro	adband			
Network Adapters								
Net Flow	LACP	LAG Group						
App Flow/IPFIX					LAGO			
SNMP	Name	Selection	State	System Priority	Port Priority	Partner State	Partner System Priority	Partner Port Prior
- NITRO API	1/1	Selected	ACT AGG SYNC COL DIST	65535	65280	AGG SYNC COL DIST	128	128
Fallback Configuration	1/2	Selected	ACT AGG SYNC COL DIST	65535	65280	AGG SYNC COL DIST	128	128
Cloud Direct Service	1/3	Selected	ACT AGG SYNC COL DIST	65535	65280	AGG SYNC COL DIST	128	128
<ul> <li>Virtual WAN</li> </ul>	1/4	Selected	ACTIAGGISYNCICOLIDIST	65535	65280	AGGISYNCICOLIDIST	128	128

## Note

You cannot change settings for individual member ports, any configuration changes made to the LAG, is automatically pushed to the member ports.

You can download the log files for further troubleshooting. Navigate to **Configuration > Logging/-Monitoring** and select **SDWAN\_common.log** from the **Log Options** tab.

Dashboard Monitoring	Configuration
Appliance Settings     Administrator Interface     Logging/Monitoring     NetWork Adapters     Net Flow     App Flow/IPFIX     SNNP     NITRO API     Licensing     Fallback Configuration     Cloud Direct Service     + Virtual WAN	Configuration > Appliance Settings > Logging/Monitoring         Log Options       Alert Options       Alarm Options       Syslog Server       HTTP Server       Application         View Log File       Only the most recent 10000 entries will be shown and filtered. To view the full log, download and open it locally.       Filename: SDWAN_common.log v         Filer(Optional):
+ System Maintenance	Download Log File Filename: \$35mount_overlay.log  Download Log

# Link state propagation

#### August 24, 2022

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.

## **Monitoring link statistics**

 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.

Statistics Show: Ethe	omet 🕤	Enable Auto Refre	sh 5 😋 seconds	Refresh		
Ethernet Stat	tistics					
Show 100	entries Showing	1 to 2 of 2 entries			First Previous 1	Next Last
Port 🔺	Link State	Frames Sent	Bytes Sent	Frames Received	Bytes Received	Errors
1	DOWN	132885	8755483	212584	15332801	0
2	DISABLED	17984552	1531084459	18189043	1584612144	3258
Showing 1 to 2	2 of 2 entries				First Previous 1	Next Last

 Navigate to Configuration > Appliance Settings > Network Adapters > Ethernet tab. The ports that are administratively down are indicated by a red asterisk (\*) in the Ethernet Interface Settings list.

Ethernet Interface Settings

C Address: C Address: C Address: C Address: C Address:	0c:c4:7a:12:bc:8c 0c:c4:7a:12:bc:8f 0c:c4:7a:12:bc:8e 0c:c4:7a:12:bc:91 0c:c4:7a:12:bc:90	Autonegotiate: Autonegotiate: Autonegotiate: Autonegotiate: Autonegotiate:		Speed: Speed: Speed: Speed:	Unknown Unknown Unknown Unknown	0 0 0	Duplex: Duplex: Duplex: Duplex:	Unknown Unknown Unknown	000
C Address: C Address: C Address: C Address:	0c:c4:7a:12:bc:8f 0c:c4:7a:12:bc:8e 0c:c4:7a:12:bc:91 0c:c4:7a:12:bc:90	Autonegotiate: Autonegotiate: Autonegotiate: Autonegotiate:		Speed: Speed: Speed:	Unknown Unknown Unknown	0 0	Duplex: Duplex: Duplex:	Unknown Unknown Unknown	0 0 0
C Address: C Address: C Address:	0c:c4:7a:12:bc:8e 0c:c4:7a:12:bc:91 0c:c4:7a:12:bc:90	Autonegotiate: Autonegotiate: Autonegotiate:		Speed: Speed:	Unknown Unknown	0 0	Duplex: Duplex:	Unknown Unknown	0 0
C Address:	0c:c4:7a:12:bc:91 0c:c4:7a:12:bc:90	Autonegotiate: Autonegotiate:	0	Speed:	Unknown	\$	Duplex:	Unknown	0
C Address:	0c:c4:7a:12:bc:90	Autonegotiate:		e					
			-	Speed:	100Mb/s	\$	Duplex:	Full	Ŷ
C Address:	00:25:90:ed:22:9f	Autonegotiate:	•	Speed:	Unknown	\$	Duplex:	Unknown	\$
C Address:	00:25:90:ed:22:9e	Autonegotiate:	•	Speed:	Unknown	\$	Duplex:	Unknown	0
C Address:	00:25:90:ed:22:9d	Autonegotiate:	•	Speed:	Unknown	\$	Duplex:	Unknown	0
C Address:	00:25:90:ed:22:9c	Autonegotiate:	•	Speed:	Unknown	\$	Duplex:	Unknown	¢
	C Address: C Address: C Address: abled by Pe	C Address: 00:25:90:ed:22:9e C Address: 00:25:90:ed:22:9d C Address: 00:25:90:ed:22:9c abled by Port State Reflection	C Address: 00:25:90:ed:22:9e Autonegotiate: C Address: 00:25:90:ed:22:9d Autonegotiate: C Address: 00:25:90:ed:22:9c Autonegotiate: abled by Port State Reflection	C Address: 00:25:90:ed:22:9e Autonegotiate: C Address: 00:25:90:ed:22:9d Autonegotiate: C Address: 00:25:90:ed:22:9c Autonegotiate: abled by Port State Reflection	C Address: 00:25:90:ed:22:9e Autonegotiate: Speed: C Address: 00:25:90:ed:22:9d Autonegotiate: Speed: C Address: 00:25:90:ed:22:9c Autonegotiate: Speed: abled by Port State Reflection	C Address: 00:25:90:ed:22:9e Autonegotiate: Speed: Unknown C Address: 00:25:90:ed:22:9d Autonegotiate: Speed: Unknown C Address: 00:25:90:ed:22:9c Autonegotiate: Speed: Unknown abled by Port State Reflection	C Address: 00:25:90:ed:22:9e Autonegotiate:	C Address: 00:25:90:ed:22:9e Autonegotiate:	C Address: 00:25:90:ed:22:9e Autonegotiate: ♥ Speed: Unknown ♦ Duplex: Unknown C Address: 00:25:90:ed:22:9d Autonegotiate: ♥ Speed: Unknown ♦ Duplex: Unknown C Address: 00:25:90:ed:22:9c Autonegotiate: ♥ Speed: Unknown ♦ Duplex: Unknown abled by Port State Reflection

## **Metering and Standby WAN Links**

#### August 24, 2022

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 nonmetered links are down or degraded. Set Last Resort is typically enabled when there are three WAN Links to a site (that is, MPLS, Broadband Internet, 4G/LTE) and one of the WAN links is 4G/LTE and might be too costly for a business to allow usage unless it is necessary. Metering is not enabled by default and can be enabled on a WAN link of any access type (Public Internet / Private MPLS / Private Intranet). If metering is enabled, you can optionally configure the following:
- Data Cap
- Billing Cycle (weekly/monthly)
- Start Date
- Standby Mode
- Priority
- Active heartbeat interval Interval at which a heartbeat message is sent by an appliance to its peer on the other end of the virtual path when there has been no traffic (user/control) on the path for at least a heartbeat interval

With a local metered link, the dashboard of an appliance shows a **WAN Link Metering** table at the bottom with metering information.

Bandwidth usage on a local metered link is tracked against the configured data cap. When the usage exceeds 50%, 75% or 90% of the configured data cap, the appliance generates an event to alert the user and a warning banner is displayed across the top of the dashboard of the appliance. A metered path can be formed with 1 or 2 metered links. If a path is formed between two metered links, the active heartbeat interval used on the metered path is the larger of the two configured active heartbeat intervals on the links.

A metered path is a non-standby path and is always eligible for user traffic. When there is at least one non-metered path that is in GOOD state, a metered path carries the reduced amount of control traffic and is avoided when the forwarding plane searches for a path for a duplicate packet.

# Standby mode

The standby mode of a WAN link is disabled by default. To enable standby mode, you must specify in which one of the following two modes the standby link operates

• **On-demand**: The standby link that becomes active when one of the conditions is met.

When the available bandwidth in the virtual path is less than the configured on-demand bandwidth limit AND there is sufficient usage. Sufficient usage is defined as more than 95% (ON\_DEMAND\_USAGE\_THRESHOLD\_PCT) of the current available bandwidth, or the difference between current available bandwidth and current usage is less than 250 kbps (ON\_DEMAND\_THRESHOLD\_GAP\_KBPS) both parameters can be changed using t2\_variables when all the non-standby paths are dead or disabled.

- **Last-resort** a standby link that becomes active only when all non-standby links and on-demand standby links are dead or disabled.
- Standby priority indicates the order in which a standby link becomes active, if there are multiple standby links:

- a priority 1 standby link becomes active first whereas a priority 3 standby link becomes active last
- Multiple standby links can be assigned the same priority

When configuring a standby link, you can specify standby priority and two heartbeat intervals:

- Active heartbeat interval the heartbeat interval used when the standby path is active (default 50ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s)
- **Standby heartbeat interval** the heartbeat interval used when the standby path is inactive (default 1s/2s/3s/4s/5s/6s/7s/8s/9s/10s/disabled)

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

- **On-Demand** An on-demand standby path is formed between:
  - a non-standby link and an on-demand standby link
  - 2 on-demand standby links
- Last-Resort A last-resort standby path is formed between:
  - a non-standby link and a last-resort standby link
  - an on-demand standby link and a last-resort standby link
  - 2 last-resort standby links

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

- If standby heartbeat is disabled on at least 1 of the 2 links, heartbeat is disabled on the standby path while inactive.
- If standby heartbeat is not disabled on either link, then the larger of the two values are used when the standby path is standby.
- If active heartbeat interval is configured on both links, then the larger of the two values are used when the standby path is active.

Heartbeat (keep alive) messages:

- On a non-standby path, heartbeat messages are sent only when there has been no traffic (control or user) for at least a heartbeat interval. The heartbeat interval varies depending on the path state. For **non-standby, non-metered** paths:
  - 50 ms when the path state is GOOD
  - 25 ms when the path state is BAD

On a standby path, the heartbeat interval used depends on the activity state and the path state:

• While inactive, if the heartbeat is not disabled, heartbeat messages are sent regularly at the configured standby heartbeat interval since no other traffic is allowed on it.

- the configured active heartbeat interval is used when the path state is GOOD.
- 1/2 the configured active heartbeat interval is used when the path state is BAD.
- While active, like non-standby paths, heartbeat messages are sent only when there has been no traffic (control or user) for at least the configured active heartbeat interval.
- the configured standby heartbeat interval is used when the path state is GOOD.
- 1/2 the configured standby heartbeat interval is used when the path state is BAD.

While inactive, standby paths are not eligible for user traffic. The only control protocol messages sent on inactive standby paths are heartbeat messages, which are for connectivity failure detection and quality metrics gathering. When standby paths are active, they are eligible for user traffic with added time cost. This is done so that the non-standby paths, if available, are favored during forwarding path selection.

The path state of a standby path with disabled heartbeat, while inactive, is assumed to be GOOD and it is displayed as GOOD in the Path Statistics table under **Monitoring**. When it becomes active, unlike a non-standby path that starts in DEAD state until it hears from its Virtual Path peer, it starts in GOOD state. If connectivity with the Virtual Path peer is not detected, the path goes BAD and then DEAD. If connectivity with the Virtual Path peer is re-established, the path goes BAD and then GOOD again.

If such standby path goes DEAD and then becomes inactive, the path state does not immediately change to (assumed) GOOD. Instead, it is kept in DEAD state for time so that it cannot be used immediately. This is to prevent activity from oscillating between a lower priority path group with assumed good DEAD paths and a higher priority path group with actually GOOD paths. This on-hold period (NO\_HB\_PATH\_ON\_HOLD\_PERIOD\_MS) is set to 5 min and can be changed via t2\_variables.

If path MTU discovery is enabled on a Virtual Path, the standby path's MTU is not used to calculate the Virtual Path's MTU while the path is standby. When the standby path becomes active, the Virtual Path' s MTU is recalculated considering the standby path's MTU. (The Virtual Path's MTU is the smallest path MTU among all active paths within the Virtual Path).

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

From SD-WAN 11.5 onwards, you can configure metered and standby WAN links using Citrix SD-WAN Orchestrator service. For more information, see Metering and Standby WAN Links.

Configuration pre-requisites:

- A meter link might be of any access type.
- All links at a site can be configured with metering enabled.
- A standby link might be of Public Internet or Private Intranet access type. A WAN link of Private MPLS access type cannot be configured as a standby link.

- At least one non-standby link must be configured per site. A maximum of 3 standby links per site is supported.
- Internet/Intranet services might not be configured on on-demand standby links. On-demand standby links support Virtual Path service only.
- Internet service might be configured on a last-resort standby link, but only load balance mode is supported.
- Intranet service might be configured on a last-resort standby link, but only secondary mode is supported and primary reclaim must be enabled.

#### Monitor metered and standby WAN links

- The Dashboard page provides the following **WAN Link Metering** information with the usage values:
  - WAN Link Name: Displays the WAN link name.
  - Total Usage: Displays the total traffic usage (Data usage + Control usage).
  - Data Usage: Displays the usage by user traffic.
  - **Control Usage**: Displays the usage by control traffic.
  - Usage (in %): Displays the used data cap value in percentage (Total Usage/Data Cap) x 100.
  - Billing Cycle: Billing frequency (weekly/monthly)
  - Starting From: Start date of the billing cycle
  - Days Elapsed: The time elapsed (in days, hours, minutes, and seconds)

ystem Status		
lame: DC		
fodel: VPX		
ub-Model: BASE		
ppliance Mode: MCN		
erial Number: 2d76a48d-5a48-cfad-	0607-fa1b0bf1350b	
lanagement IP Address: 10.105.172.132		
ppliance Uptime: 1 days, 23 hours, 44 m	inutes, 57.1 seconds	
ervice Uptime: 1 days, 23 hours, 37 m	inutes, 48.0 seconds	
outing Domain Enabled: Default_RoutingDomain	1	
ocal Versions		
oftware Version: 112045859448		
ntware version. 11.2.0.45.059440		
uilt On: May 11 2020 at 01-28-04		
uilt On: May 11 2020 at 01:28:04		
uilt On: May 11 2020 at 01:28:04 lardware Version: VPX		
uilt On: May 11 2020 at 01:28:04 Iardware Version: VPX IS Partition Version: 5.1		
ulit On: May 11 2020 at 01:28:04 lardware Version: VPX S Partition Version: 5.1 irtual Path Service Status		
ulit On: May 11 2020 at 01:28:04 lardware Version: VPX S Partition Version: S.1 irtual Path Service Status lirtual Path DC-BR: Uptime: 1 days, 23 hours, 32	r minutes, 27.0 seconds.	
ulit On: May 11 2020 at 01:28:04 ardware Version: VPX S Partition Version: 5.1 irtual Path Service Status irtual Path DC-BR: Uptime: 1 days, 23 hours, 33 AN Link Metering	' minutes, 27.0 seconds.	
ulit On: May 11 2020 at 01:28:04 ardware Version: VPX S Partition Version: 5.1 irtual Path Service Status irtual Path DC-BR: Uptime: 1 days, 23 hours, 37 AN Link Metering WAN Link Name: DC-ML	' minutes, 27.0 seconds. WAN Link Name: DC-WL-1	
ulit On: May 11 2020 at 01:28:04 ardware Version: VPX S Partition Version: 5.1 irtual Path Service Status irtual Path DC-BR: Uptime: 1 days, 23 hours, 33 AN Link Metering WAN Link Name: DC-ML Total Usage: 1160.69 MBs of 500 MBs	<sup>7</sup> minutes, 27.0 seconds. WAN Link Name: DC-WL-1 Total Usage: 999.35 MBs of 500 MBs	
ult On: May 11 2020 at 01:28:04 andware Version: VPX S Partition Version: 5.1 rtual Path Service Status rtual Path DC-BR: Uptime: 1 days, 23 hours, 37 AN Link Metering WAN Link Name: DC-ML Total Usage: 1160.69 MBs of 500 MBs Data Usage: 0.01 MBs	' minutes, 27.0 seconds. WAN Link Name: DC-WL-1 Total Usage: 999.33 MBs of 500 MBs Data Usage: 0.00 MBs	
ulit On: May 11 2020 at 01:28:04 ardware Version: VPX S Partition Version: 5.1 rtual Path Service Status rtual Path DC-BR: Uptime: 1 days, 23 hours, 37 AN Link Metering WAN Link Name: DC-ML Total Usage: 1160.69 MBs of 500 MBs Data Usage: 0.01 MBs Control Usage: 1160.68 MBs	' minutes, 27.0 seconds. WAN Link Name: DC-WL-1 Total Usage: 99.35 MBs of 500 MBs Data Usage: 0.00 MBs Control Usage: 99.35 MBs	
uilt On:       May 11 2020 at 01:28:04         adware Version:       VPX         Spartition Version:       S.1         rtual Path Service Status       Intervice Status         rtual Path DC-BR:       Uptime: 1 days, 23 hours, 33         AN Link Metering       Intervice Status         WAN Link Name:       DC-ML         Total Usage:       1160.69 MBs of 500 MBs         Data Usage:       0.01 MBs         Control Usage:       1160.68 MBs         Usage(in %):       232	r minutes, 27.0 seconds. WAN Link Name: DC-WL-1 Total Usage: 999.35 MBs of 500 MBs Data Usage: 0.00 MBs Control Usage: 999.35 MBs Usage(in %): 199	
ulit On: May 11 2020 at 01:28:04 ardware Version: VPX S Partition Version: 5.1 irtual Path Service Status irtual Path DC-BR: Uptime: 1 days, 23 hours, 33 AN Link Metering WAN Link Name: DC-ML Total Usage: 1160.65 MBs of 500 MBs Data Usage: 0.01 MBs Control Usage: 1160.68 MBs Usage(in %): 232 Billino Cycle: WEEKLY	' minutes, 27.0 seconds. WAN Link Name: DC-WL-1 Total Usage: 999.35 MBs of 500 MBs Data Usage: 0.00 MBs Control Usage: 999.35 MBs Usage(in %): 199 Billing Cycle: MONTHLY	
ulit On: May 11 2020 at 01:28:04 ardware Version: VPX SPartition Version: 5.1 irtual Path Service Status irtual Path DC-BR: Uptime: 1 days, 23 hours, 37 /AN Link Metering WAN Link Name: DC-ML Total Usage: 1160.69 MBs of 500 MBs Control Usage: 1160.68 MBs Control Usage: 0.01 MBs Control Usage: 0.22 Billing Cycle: WEEKLY Starting From: 05/08/2020	' minutes, 27.0 seconds. WAN Link Name: DC-WL-1 Total Usage: 999.35 MBs of 500 MBs Data Usage: 0.00 MBs Control Usage: 999.35 MBs Usage(in %): 199 Billing Cycle: MONTHLY Starting From: 05/06/2020	

• When path statistics (**Monitoring > Statistics > Paths**) are displayed, metered links and standby links are marked as shown in the screenshot.

	Dashboard Monit	ing Configuration								
<	Statistics	Monitoring > Statistics								
	Flows									
	Routing Protocols	Statistics								
	Firewall	Show: Paths (Summary) 🗘 🗹 Enable Auto	Refresh 5 \$	seconds Start 🗹 Show la	atest data.					
	IKE/IPsec									
	IGMP	Path Statistics Summary								
	Performance Reports	ilter: in Any column	Apply					5	show 10	0 🛊 entries
	Qos Reports									
	Usage Reports	Num* From Link To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
	Availability Reports	1 Dallas_MCN-queue1 ANZ_RCN-queue2	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
	Appliance Reports	2 ANZ_RCN-queue1 Dallas_MCN-queu	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
	DHCP Server/Relay	3 Dallas_MCN-queue1 APAC_RCN-queue	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
	VPPP	4 APAC_RCN-queue1 Dallas_MCN-queu	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
	VRR	5 Dallas_MCN-queue1 California-queue	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
	PPPoE	6 California-queue1 Dallas_MCN-queu	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
	DNS	7 Dallas_MCN-queue1 EMEA_RCN-queue	2 DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
		8 EMEA_RCN-queue2 Dallas_MCN-queu	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
		9 Dallas_MCN-WL-2 Newyork-WL-2	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
		10 Dallas_MCN-queue1 Newyork-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
		11 Newyork-WL-2 Dallas_MCN-WL-	2 DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
		12 Newyork-queue1 Dallas_MCN-queu	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
		13 Dallas_MCN-queue1 Texas-queue1	DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
		14 Texas-queue1 Dallas_MCN-que	el DEAD	DEAD	Static	9999	0	0.00	0.00	UNKNOWN
		howing 1 to 14 of 14 entries			_		Firs	Previo	us 1	Next Last
		andwidth calculated over the last 73 55 seconds								

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).

Local W	cal WAN-to-LAN On Demand WAN Link Usages										
Filter:	er: in Any column										
Show	100 🗘 entrie	s Showing	0 to 0 of 0 en	tries					First Previous	Next	Last
				Adaptive Bane	dwidth Detection						
WAN_ Link	WAN Link Mode	Standby Priority	Configured	Minimum Acceptable BW Kbps	Maximum Allowed BW Kbps	Current Allowed BW Kbps	Virtual Path Name	Virtual Path On Demand Bandwidth Limit Kbps	Virtual Path Av Bandwidth K	ailable bps	In Use
No da	ta available ir	table									
Showing Bandwid	howing 0 to 0 of 0 entries First Previous Next Last andwidth calculated over the last 5.078 seconds										

• 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.

Dashboard Monitoring Configurat	on .							
The data usage on the following Meter • DC-WL-1 : 100%. • DC-ML : 100%.	d Wanlinks have reached the threshold:	×						
System Status								
Name:         DC           Model:         VPX           Sub-Model:         BASE           Appliance Mode:         MCN           Serial Number:         2d76a8d-5a48-cfad-06           Management IP Address:         10.105.172.132           Appliance Uptime:         1 days, 23 hours, 44 minu           Service Uptime:         1 days, 23 hours, 37 minu           Routing Domain Enabled:         Default_RoutingDomain	7-falb0bf1350b es, 57.1 seconds es, 48.0 seconds							
Local Versions								
Software Version:         11.2.0.45.859448           Built On:         May 11 2020 at 01:28:04           Hardware Version:         VPX           OS Partition Version:         S,1								
Virtual Path Service Status								
Virtual Path DC-BR: Uptime: 1 days, 23 hours, 37 m	nutes, 27.0 seconds.							
WAN Link Metering	WAN Link Metering							
WAN Link Name: DC-ML           Total Usage:         1160.69 MBs of 500 MBs           Data Usage:         0.01 MBs           Control Usage:         1160.68 MBs           Usage(in %):         232           Billing Cycle:         WEKLY           Starting From:         05/08/2020           Days Elapsed:         6 days of 7 days	WAN Link Name: DC-WL-1         Total Usage:       999.35 MBs of 500 MBs         Data Usage:       0.00 MBs         Control Usage:       999.35 MBs         Usageün %:       199         Billing Cycle:       MONTHLY         Starting From:       05/06/2020         Days Elapsed:       8 days of 31 days							

A WAN link usage event is also generated at the appliance when the usage exceeds 50%, 75%, and 90% of the configured data cap.

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

1. When a standby path transitions between standby and active state, an event is generated by the appliance.

				89.89.34			
24640	3	RL-TB-MCN-WL-2- >RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become standby
24639	1	RL-TB-MCN-WL-1- >RL-TB-CL2-WL-2	PATH	2017-05-26	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become standby
24638	1	RL-TB-CL2-WL-1->RL- TB-MCN-WL-2	PATH	2017-05-26 10:18:27	C000	NOTICE	Virtual Path RL-T8-MCN-RL-T8-CL2 Path RL-T8-CL2-WL-1->RL-T8-MCN-WL-2 state has changed from BAD to GOOD because notified by peer.
24637	2	RL-TB-MCN-WL-2- >RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	0000	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-1 state has changed from BAD to COOD .
24636	2	RL-TB-MCN:RL-TB-CL2	VIRTUAL PATH	2017-05-26 10:18:27	C000	NOTICE	The state of Virtual Path RL-TB-MCN-RL-TB-CL2 has changed from BAD to GOOD
24635	0	RL-TB-CL2-WL-1->RL- TB-MCN-WL-1	PATH	2017-05-26 10:18:27	0000	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-1 state has changed from BAD to GOOD because notified by peer.
24634	0	RL-TB-MCN-WL-1- >RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	C000	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24633	3	RL-TB-MCN-WL-2- >RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become active
24632	1	RL-TB-MCN-WL-1- >RL-TB-CL2-WL-2	PATH	2017-05-26	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become active

2. The configured active and standby heartbeat intervals for each path can be viewed at **Configu**ration > Virtual WAN > View Configuration > Paths.

Dashboard Monitoring	Configuration								
+ Appliance Settings	Configuration > Virtual WAN > View Configur	ation							
- Virtual WAN									
View Configuration	Configuration								_
- Configuration Editor	View: Paths \$								
- Change Management Settings									
- Restart/Reboot Network	Path Configuration								
- Enable/Disable/Purge Flows	Paths on virtual path 3 'Dallas_MCN-ANZ_RC	N':							
SD-WAN Center Certificates	Path ID From Link To Lin	nk	Primary Src IP Address	Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dst Port	Alt Src
+ System Maintenance	0 Dallas_MCN-queuel ANZ_R0 0 ANZ_RCN-queuel Dalla	CN-queuel s MCN-queuel	192.168.1.10 192.168.90.10	192.168.90.10 192.168.1.10	:		4980 4980	4980 4980	
		_ 1				Ct and by	hative		
	From Link To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Heartbeat Interval(ms)	Heartbeat Interval(ms)		
	Dallas_MCN-queuel ANZ_RCN-queuel ANZ_RCN-queuel Dallas_MCN-queuel	YES YES	YES YES	YES YES	0 0	n/a n/a	n/a n/a		
	Paths on virtual path 8 'Dallas_MCN-APAC_R0	CN':							
			Primary Src IP	Primary Dst IP	Secondary Src IP	Secondary Dst IP			Alt
	Path ID From Link To Lin	nk	Address	Address	Address	Address	Src Port	Dat Port	Src
	0 APAC_RCN-queuel Dalla	s_MCN-queuel	192.168.80.10	192.168.1.10	-	-	4980	4980	
	From Link To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)		
	Dallas_MCN-queuel APAC_RCN-queuel APAC_RCN-queuel Dallas_MCN-queuel	YES	YES	YES YES	0	n/a n/a	n/a n/a		
	Paths on virtual path 9 'Dallas_MCN-Califo	rnia':							
			Primary Src IP	Primary Dst IP	Secondary Src IP	Secondary Dst IP			Alt
	0 Dallas_MCN-queuel Calife	ornia-queuel	192.168.1.10	192.168.50.10	Address	Address	4980	4980	SIC
	0 California-queuel Dalla:	s_MCN-queue1	192.168.50.10	192.168.1.10	-	-	4980	4980	
	From Link To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)		
	Dallas_MCN-queuel California-queuel California-queuel Dallas_MCN-queuel	YES YES	YES YES	YES YES	0	n/a n/a	n/a n/a		
	Paths on virtual path 12 'Dallas_MCN-EMEA_i	RCN' :							
			Primary Src IP	Primary Dst IP	Secondary Src IP	Secondary Dst IP			Alt
	0 Dallas MCN-queuel EMEA	nk RCN-gueue2	Address 192.168.1.10	Address 17.1.1.10	Address	Address	Src Port 4980	Dst Port 4980	Src
	0 EMEA_RCN-queue2 Dalla	s_MCN-queuel	17.1.1.10	192.168.1.10	-	-	4980	4980	
	From Link To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)		
	Dallas_MCN-queue1 EMEA_RCN-queue2 EMEA_RCN-queue2 Dallas_MCN-queue1	YES	YES	YES	0	n/a n/a	n/a n/a		
	Paths on virtual path 13 'Dallas_MCN-Newyo:	rk':							
	Path ID From Link To Link	nk	Primary Src IP Address	Primary Dst IP Address	Secondary Src IP Address	Secondary Dst IP Address	Src Port	Dat Port	Alt
	1 Dallas_MCN-queuel Newyo	rk-queuel	192.168.1.10	192.168.70.10	-	-	4980	4980	
	0 Newyork-WL-2 Dallar 1 Newyork-queuel Dallar	s_MCN-WL-2 s_MCN-queue1	192.168.60.10 192.168.60.10 192.168.70.10	192.168.10.10 192.168.1.10	-	-	4980 4980 4980	4980 4980	
	From Link To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)		
	Dallas_MCN-queuel Newyork-queuel Dallas_MCN-WL-2 Newyork-WL-2 Newyork-WL-2 Dallas_MCN-W-2	YES YES YES	YES YES	YES YES YES	0	n/a n/a	n/a n/a		
	Newyork-queuel Dallas_MCN-queuel	YES	YES	YES	0	n/a	n/a		
	Paths on virtual path 14 'Dallas_MCN-Texas	:	De í mary	De la ser	Reporter	Papendaur.			
	Path ID From Link To Lin	nk	Src IP Address	Dst IP Address	Src IP Address	Dst IP Address	Src Port	Dst Port	Alt Src
	0 Dallas_MCN-queuel Texas 0 Texas-queuel Dalla	-queuel s_MCN-queuel	192.168.1.10 192.168.40.10	192.168.40.10 192.168.1.10	-	-	4980 4980	4980 4980	
	From Link To Link	Realtime Eligible	Interactive Eligible	Bulk Eligible	Path Group	Standby Heartbeat Interval(ms)	Active Heartbeat Interval(ms)		
	Dallas_MCN-queuel Texas-queuel Texas-queuel Dallas_MCN-queuel	YES YES	YES YES	YES YES	0	n/a n/a	n/a n/a		

# **Office 365 optimization**

### August 24, 2022

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. Avoid practices such as backhauling to a central proxy. Office 365 traffic such as Outlook, Word are sensitive to latency and backhauling traffic introduces more latency resulting in poor user experience. Citrix SD-WAN allows you to configure policies to break out Office 365 traffic to the Internet.

The Office 365 traffic is directed to the nearest Office 365 service endpoint, which exists at the edges of Microsoft Office 365 infrastructure worldwide. Once traffic reaches a front door, it goes over Microsoft's network and reaches the actual destination. It 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. Office 365 endpoints are classified into **Optimize**, **Allow**, and **Default** categories. Citrix SD-WAN 11.4.0 provides a more granular classification of the **Optimize** and **Allow** categories, enabling selective bookending to improve the performance of network-sensitive Office 365 traffic. Directing network-sensitive traffic to SD-WAN in the cloud (Cloud Direct or an SD-WAN VPX on Azure), or from an at-home SD-WAN device to an SD-WAN at a nearby location with more reliable Internet connectivity, enables QoS and superior connection resilience compared to simply steering the traffic to the nearest Office 365 front door, at the cost of an increase in latency. A bookended SD-WAN solution with QoS reduces VoIP dropouts and disconnects, reduces jitter and improves media-quality mean opinion scores for Microsoft Teams:

• **Optimize** - These endpoints provide connectivity to every Office 365 service and feature, and are sensitive to availability, performance, and latency. It represents over 75% of Office 365 bandwidth, connections, and volume of data. All the Optimize endpoints are hosted in Microsoft data centers. Service requests to these endpoints must breakout from the branch to the Internet and must not go through the data center.

The **Optimize** category is classified into the following subcategories:

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

For information about upgrade considerations, see Important considerations for upgrade.

• **Allow** - These endpoints provide connectivity to specific Office 365 services and features only, and are not so sensitive to network performance and latency. The representation of Office 365 bandwidth and connection count is also lower. These endpoints are hosted in Microsoft data centers. Service requests to these endpoints might breakout from the branch to the Internet or might go through the data center.

The **Allow** category is classified into the following subcategories:

```
1 - Teams TCP Fallback
```

```
2 - Exchange Mail
```

- 3 SharePoint Allow
- 4 Office365 Common

## For information about upgrade considerations, see Important considerations for upgrade.

## Note

The **Teams Realtime** subcategory uses the UDP real-time transport protocol to manage Microsoft Teams traffic, whereas the **Teams TCP Fallback** subcategory uses the TCP transport layer protocol. As media traffic is highly latency sensitive, you might prefer this traffic to take the most direct path possible and to use UDP instead of TCP as the transport layer protocol (most preferred transport for interactive real-time media in terms of quality). While UDP is a preferred protocol for Teams media traffic, it requires certain ports to be allowed in the firewall. If the ports are not allowed, Teams traffic uses TCP as a fallback, and enabling optimization for Teams TCP Fallback ensures better delivery of the Teams application in this scenario. For more information, see Microsoft Teams call flows.

• **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 might not be hosted in Microsoft data centers. The traffic in this category is not susceptible to variations in latency. Therefore, direct breaking out of this type of traffic does not cause any performance improvement when compared to Internet breakout. In addition, the traffic in this category may not always be Office 365 traffic. Hence, it is recommended to disable this option when enabling Office 365 breakout in your network.

# How Office 365 optimization works

The Microsoft endpoint signatures are updated at most once a day. Agent on the appliance polls the Citrix service (sdwan-app-routing.citrixnetworkapi.net), every day to obtain the latest set of end-point signatures. The SD-WAN appliance polls the Citrix service (sdwan-app-routing.citrixnetworkapi.net), once every day, when the appliance is turned on. 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

Except for the Office 365 Default category, first packet detection and classification of Office 365 traffic is performed by default, irrespective of whether the Office 365 breakout feature is enabled or not.

When a request for the Office 365 application arrives, the application classifier, does a first packet classifier database lookup, identifies, and marks Office 365 traffic. Once the Office 365 traffic is classified, the auto created application route and firewall policies take effect and breaks out the traffic directly to the Internet. The Office 365 DNS requests are forwarded to specific DNS services like Quad9. For more information, see Domain name system.



The signatures are downloaded from Cloud Service (sdwan-app-routing.citrixnetworkapi.net).

From Citrix SD-WAN 11.5 onwards, you can configure Office 365 breakout using Citrix SD-WAN Orchestrator service. For more information, see Office 365 optimization.

# **Transparent forwarder for Office 365**

The branch breaks out for Office 365 begins with a DNS request. The DNS request going through Office 365 domains have to be steered locally. If Office 365 Internet break out is enabled, the internal DNS routes are determined and the transparent forwarders list is auto populated. Office 365 DNS requests are forwarded to open source DNS service Quad 9 by default. Quad 9 DNS service is secure, scalable,

and has multi pop presence. You can change the DNS service if necessary. Transparent forwarders for Office 365 applications are created at every branch that has Internet service and office 365 breakout enabled.

If you are using another DNS proxy or if SD-WAN is configured as the DNS proxy, the forwarder list is auto populated with forwarders for Office 365 applications.

# Important considerations for upgrade

## **Optimize and Allow categories**

If you have enabled the Internet breakout policy for the **Optimize** and **Allow** Office 365 categories, Citrix SD-WAN automatically enables the Internet breakout policy for the corresponding subcategories upon upgrade to Citrix SD-WAN 11.4.0.

When you downgrade to a software version older than Citrix SD-WAN 11.4.0, you must manually enable Internet breakout for the **Optimize** or **Allow** Office 365 category irrespective of whether you enabled the corresponding subcategories in the Citrix SD-WAN 11.4.0 version or not.

# Office 365 application objects

If you have created rules/routes using the **O365Optimize\_InternetBreakout** and **O365Allow\_InternetBreakout** auto-generated application objects, ensure to delete the rules/routes before upgrading to Citrix SD-WAN 11.4.0. After the upgrade, you can create rules/ routes using the corresponding new application objects.

If you proceed with Citrix SD-WAN 11.4.0 upgrade without deleting the rules/routes, you see an error and thus, the upgrade becomes unsuccessful. In the below example, a user has configured an Application QoE profile and is seeing an error while trying to upgrade to Citrix SD-WAN 11.4.0 without deleting the rules/routes:



### Note

This upgrade is not required for auto-created rules/routes. It applies only to rules/ routes that you have created.

### DNS

If you have created DNS Proxy rules or DNS transparent forwarder rules using the **Office 365 Optimize** and **Office 365 Allow** applications, ensure to delete the rules before upgrading to Citrix SD-WAN 11.4.0. After the upgrade, you can create the rules again using the corresponding new applications.

If you proceed with Citrix SD-WAN 11.4.0 upgrade without deleting the old DNS proxy or transparent forwarder rules, you do not see any error and upgrade becomes successful too. However, the DNS proxy rules and transparent forwarding rules do not take effect in Citrix SD-WAN 11.4.0.

Note

This activity does not apply to the auto-created DNS rules. It applies only to DNS rules that you have created.

# Monitoring

You can monitor the office 365 application statistics in the following SD-WAN statistic reports:

• Firewall Statistics

Connections															
					Sour	ce		Destination							
Application	Family	IP Protocol	IP Adress	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	Stat		
Microsoft Teams TCP fallback(ms_teams_fallback)	Web	TCP	172.16.30.20	3698	Local	Site1_VI_1	Default_LAN_Zone	52.113.194.132	443	Internet	BRANCH1_KVMVPX-Internet	Internet_Zone	CLOSED		
Microsoft Teams Realtime(ms_teams_realtime)	Web	UDP	172.16.30.20	53	Local	Site1_VI_1	Default_LAN_Zone	52.113.194.132	3478	Internet	BRANCH1_KVMVPX-Internet	Internet_Zone	NEW		
Domain Name Service(dns)	Network Service	UDP	172.16.30.20	50191	Local	Site1_VI_1	Default_LAN_Zone	9.9.9.9	53	Internet	BRANCH1_KVMVPX-Internet	Internet_Zone	ESTABLI		
Domain Name Service(dns)	Network Service	UDP	172.16.30.20	57372	Local	Site1_VI_1	Default_LAN_Zone	9.9.9.9	53	Internet	BRANCH1_KVMVPX-Internet	Internet_Zone	ESTABLI		
Domain Name Service(dns)	Network Service	UDP	172.16.30.20	38314	Local	Site1_VI_1	Default_LAN_Zone	9.9.9.9	53	Internet	BRANCH1_KVMVPX-Internet	Internet_Zone	ESTABLI		
Domain Name Service(dns)	Network Service	UDP	172.16.30.20	42983	Local	Site1_VI_1	Default_LAN_Zone	9.9.9.9	53	Internet	BRANCH1_KVMVPX-Internet	Internet_Zone	ESTABLI		
Domain Name Service(dns)	Network Service	UDP	172.16.30.20	46633	Local	Site1_VI_1	Default_LAN_Zone	9.9.9.9	53	Internet	BRANCH1_KVMVPX-Internet	Internet_Zone	ESTABLI		
Microsoft Exchange Online(ms_exchange_online)	Web	TCP	172.16.30.20	39362	Local	Site1_VI_1	Default_LAN_Zone	13.107.18.11	80	Internet	BRANCH1_KVMVPX-Internet	Internet_Zone	CLOSED		
Microsoft Exchange Mail(ms_exchange_mail)	Web	TCP	172.16.30.20	58871	Local	Site1_VI_1	Default_LAN_Zone	51.5.80.2	443	Internet	BRANCH1_KVMVPX-Internet	Internet_Zone	SYN_SEI		

#### • Flows

Flow	Flows Data																									
Both LAN	th LAN to WAR and WAN to LAN flows																									
Details	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
٠	172.16.30.20	52.111.240.7	LAN to WAN	47944	80	TCP	default	5	INTERNET	-	LOCAL	613247	4	240	0.000	0.000	0.000	0.000	135	N/A	N/A	N/A	N/A	N/A	N/A	ms_office365_common
٠	172.16.30.20	51.5.80.2	LAN to WAN	51200	443	TCP	default	6	INTERNET	-	LOCAL	312835	5	200	0.000	0.000	0.000	0.000	135	N/A	N/A	N/A	N/A	N/A	N/A	ms_exchange_mail
	172.16.30.20	52.111.240.7	LAN to WAN	47940	80	TCP	default	3	INTERNET	-	LOCAL	629624	2	120	0.000	0.000	0.000	0.000	135	N/A	N/A	N/A	N/A	N/A	N/A	ms_office365_common
٠	172.16.30.20	51.4.64.0	LAN to WAN	44869	443	TCP	default	3	INTERNET	-	LOCAL	546042	2	80	0.000	0.000	0.000	0.000	135	N/A	N/A	N/A	N/A	N/A	N/A	ms_exchange_online
٠	172.16.30.20	51.5.80.2	LAN to WAN	33932	443	TCP	default	6	INTERNET	-	LOCAL	580094	5	200	0.000	0.000	0.000	0.000	135	N/A	N/A	N/A	N/A	N/A	N/A	ms_exchange_mail
٠	172.16.30.20	51.5.80.2	LAN to WAN	58871	443	TCP	default	3	INTERNET	-	LOCAL	233205	2	80	0.000	0.000	0.000	0.000	135	N/A	N/A	N/A	N/A	N/A	N/A	ms_exchange_mail
•	172.16.30.20	51.4.64.2	LAN to WAN	26957	443	TCP	default	6	INTERNET	-	LOCAL	528507	5	200	0.000	0.000	0.000	0.000	135	N/A	N/A	N/A	N/A	N/A	N/A	ms_exchange_online

### • DNS Statistics

DNS Proxy Statistics

Refresh					[	Search	Q
Prory Name	Application Name	DN	NS Service Name D	DNS Service Active 1	Hits 1	DNS Service IPv6 Name	: DN
Local_Proxy210	ECOMM	Go	oogleV4	YES	0	GDNSv6	YE
Local_Prexy210	ms_teams_realtime	Qu	uad9	YES	0	Qued9v6	YE
Local_Proxy210	ms_sharepoint_optimize	Qu	uad9	YES	0	Quad9v6	YE
Local_Proxy210	ms_exchange_online	Qu	uad9	YES	0	Quad9v6	YE
Local_Proxy210	ms_teams_failback	Qu	uad9	YES	0	Quad9v6	YE
Local_Proxy210	ms_exchange_mail	Qu	ua#9	YES	0	Quad9v6	YE
Local_Proxy210	ms_sharepoint_allow	Qu	uad9	YES	0	Quad9v6	YE
Local_Proxy210	ms_office365_common	Qu	uad9	YES	0	Quad9v6	YE
Local_Proxy210	office365_default	Qu	uad9	YES	0	Quad9v6	YE
Local_Proxy210	citrix_cloud_web_ui_api	Qu	uad9	YES	167	Quad9v6	YE
<							*
				Showing 1-30 of		Page 1 of 2 4 10 rows	1 × 1

# • Application Route Statistics

Monitorin	g > Statistics											
Statist	ics											
Show: App	lication Routes 💙 🗆 Enable Auto Refresh 🗴 🗙	🖌 seconds 🛛 Refresh 🖉 Clear C	ounters on Refres	h								
Applic	ation Route Statistics											
Maximum a	llawed routes: 64000											
Application	Routes for routing domain : Default_RoutingDomain											
Filter:	in Any column V Apply											
Show 100	✓ entries Showing 1 to 8 of 8 entries										First	Previous 1 Next Last
Num 🔺	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Туре	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	O365TeamsTCPFallback_Breakout	•	Internet	Internet_Zone	YES	BRANCH1_KVMVPX	Static	5	4	YES	N/A	N/A
1	O365TeamsRealtime_Breakout	•	Internet	Internet_Zone	YES	BRANCH1_KVMVPX	Static	5	11	YES	N/A	N/A
2	O365SharepointOptimize_Breakout	•	Internet	Internet_Zone	YES	BRANCH1_KVMVPX	Static	5	0	YES	N/A	N/A
3	O365SharepointAllow_Breakout	•	Internet	Internet_Zone	YES	BRANCH1_KVMVPX	Static	5	0	YES	N/A	N/A
4	O365ExchangeOnline_Breakout		Internet	Internet_Zone	YES	BRANCH1_KVMVPX	Static	5	4	YES	N/A	N/A
5	O365ExchangeMail_Breakout		Internet	Internet_Zone	YES	BRANCH1_KVMVPX	Static	5	0	YES	N/A	N/A
6	O365Default_InternetBreakout	*	Internet	Internet_Zone	YES	BRANCH1_KVMVPX	Static	5	2	YES	N/A	N/A
7	O365Common_InternetBreakout		Internet	Internet_Zone	YES	BRANCH1_KVMVPX	Static	5	0	YES	N/A	N/A
Showing 1	o 8 of 8 entries										First	Previous 1 Next Last

#### Troubleshooting

You can view the service error in the **Events** section of the SD-WAN appliance.

To check the errors, navigate to **Configuration > System Maintenance > Diagnostics**, click **Events** tab.

Dashboard Monitoring	Configuration
+ Appliance Settings + Virtual WAN	Configuration > System Maintenance > Diagnostics
- System Maintenance	Ping Traceroute Packet Capture Path Bandwidth System Info Diagnostic Data Events Alarms Diagnostics Tool
– Delete Files – Restart System – Date/Time Settings	Site Diagnostics Insert Event
- Local Change Management - Diagnostics	Object Type: USER EVENT +
- Update Software - Configuration Reset	Event type: UNDEFINED ¢ Severity: DEBUG ¢
	Add Event

If there is an issue in connecting to the Citrix service (sdwan-app-routing.citrixnetworkapi.net), then the error message reflects under the **View Events** table.

View E	vents						
Quantity Filter: Reload	y: Events Table	25 Object Type = APP	PLICATIONS	Event type = FAILURE	Severity =	ERROR	\$
ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
13839	26	Endpoints Update	APPLICATIONS	2019-02-12 09:02:15	FAILURE	ERROR	Failed to connect to the service API
Times are ir	n UTC						

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 dropdown list under the **Download Log file** section and click **Download Log**.

Dashboard Monitoring	Configuration
Appliance Settings     Administrator Interface     Logging/Monitoring     Network Adapters     Net Flow     App Flow/IPFDX     SNNP     NITRO API     Licensing     + Virtual WAN	Configuration > Appliance Settings > Logging/Monitoring         Log Options       Alert Options       Alarm Options       Syslog Server       HTTP Server         View Log File       Only the most recent 10000 entries will be shown and filtered. To view the full log, download and open it locally.         Filename:       SDWAN_dpi.log •         Filter (Optional):       Image: SDWAN_dpi.log •
+ System Maintenance	View Log Download Log File Filename: SDWAN_dpi.log  Download Log

# Limitations

- If the Office 365 breakout policy is configured, deep packet inspection is not performed on connections destined to the configured category of IP addresses.
- The auto created firewall policy and application routes are uneditable.
- The auto created firewall policy has the lowest priority and is uneditable.
- The route cost for the auto created application route is five. You can override it with a lower cost route.

# Office 365 beacon service

Microsoft provides the Office 365 beacon service to measure the Office 365 reachability through the WAN links. The beacon service is basically a URL - sdwan.measure.office.com/apc/trans.png, which is probed at regular intervals. Probing is done on each appliance for every internet enabled WAN link. With each probe, an HTTP request is sent to the beacon service and an HTTP response is expected. The HTTP response confirms the availability and reachability of the Office 365 service.

Citrix SD-WAN allows you to not only perform beacon probing, but also determines the latency to reach Office 365 endpoints through each WAN link. The latency is the round trip time taken to send a request and get a response from the Office 365 beacon service over a WAN link. This enables network administrators to view the beacon service latency report and manually choose the best internet link for direct Office 365 breakout. Beacon probing is enabled only through Citrix SD-WAN Orchestrator. By default, beacon probing is enabled on all Internet enabled WAN links when Office 365 break-out is enabled through Citrix SD-WAN Orchestrator.

Note

Office 365 beacon probing is not enabled on metered links.

You can choose to disable Office 365 beacon probing and view latency reports on the SD-WAN Orchestrator. For more information, see Office 365 optimization.

To disable Office 365 beacon service, in SD-WAN Orchestrator, at network level navigate to **Configuration > Routing > Routing Policies > O365 Network Optimization Settings** and clear **Enable Beacon Service**.

#### Citrix SD-WAN 11.5

C DASHBOARD	Verify Costing Application Brothers IP Brothers
REPORTS >	Cost Ranges: Custom Application (72-40) Application Group (41-60) IP (1-85335)
$\odot$ configuration $\sim$	Application Group Match Criteria
Network Config Home Delivery Services > Routing ~	Match Type         Application Group           Application Group         03850ptimize_IntermetBreakout           Screene         C
Routing Policies Routing Domains	Global Reute      Site / Group Specific Route
Import Route Profiles Export Route Profiles Transit Nodes	Traffic Steering Debery Service
Link Settings > QoS >	Internet Breakout  COBR5 Network Ontimization Settings
Security > Site & IP Groups > App & DNS Settings > Profiles & Templates WAN Optimization >	Review Office 355 Nature: Connectivity Principles Network connectivity in the Microsoft 355 Admin Center Optimize Evaluate astimization for highly latency another OBS anrives age Exchange. Surgeon, Su
(i) ALERTS >	ALOW (control spinning spinning with a sum of y and sum of the spin spin spin spin spin spin spin spin
$\sim$ troubleshooting >	Contract In the sequence of the sequence
	Cancel Save
<	

To view the beacon probing availability and latency reports, in Citrix SD-WAN Orchestrator, at network level navigate to **Reports** > **O365 Metrics**.

Root Adm	Parent hin / <u>Citrix Systems</u>	. <u>Inc.</u> /	Provider Customer Site Abhishek / Citrix Y / All Sites Y			TRIAL 79 days left 🛛 🛤 📢 🖂 🕢
2	Dashboard		Network Reports : O365 Metrics	e		Relative Time         Intervat         Last 1 Hour         Site Group:         All         Y
ш	Reports	~	Site Name	WAN Link Name	Availability	Latency (ms)
	Alerts		Kolkata	Kolkata-Broadband-ACT-1	Yes	9.20
	Usage		Patna	Patna-Broadband-ACT-1	Yes	9.16
	Inventory		Santa_Clara	Santa_Clara-Internet-AOL-2	Yes	10.08
	Quality					
	QoS					
	Historical Statistics					
	Real Time	>				
	Application Quality					
	0365 Metrics		Ν			

To view a detailed site level report of beacon service, in SD-WAN Orchestrator, at site level navigate to **Reports > 0365 Metrics**.

### Citrix SD-WAN 11.5

Root Parent Admin / Citrix Systems. Inc	Provider Customer Site / <u>Abhishek</u> / <u>Citrix</u> / <b>Patna</b> Y	TRIAL 79 days left 🛛 🗚 🖂 🕐
Dashboard	Site Report : 0365 Metrics C	Relative Time V Interval: Last 1 Hour V
Liti Reports Alerts Alerts Usage Quality QoS Historical Statistics Real Time	Select WAN Link: Patna-Broadband-ACT-1 V Patna-Broadband-ACT-1 Availability: 519am 5:24am 5:29am 5:34am 5:39am 5:44am 5:49am 5:54am 5:59am	6:04am 6:09am 6:14am 6:19am
O365 Metrics Cloud Direct	Latency (ms) :	- <u></u>
F Troubleshooting		

# **Citrix Cloud and Gateway service optimization**

#### August 24, 2022

With the **Citrix Cloud and Gateway Service optimization** feature enhancement, you can detect and route traffic destined for Citrix Cloud and Gateway Service. You can create policies to either break the traffic out to internet directly or, to send it via a backhaul route over virtual path. In the absence of this feature, when the default route is virtual path, gateway service will hairpin back to the customer' s Data Center and then would go out to Internet adding unnecessary latency. In addition to that, you now get visibility into Citrix Gateway service and Citrix Cloud traffic and can create QoS policies to prioritize it over virtual path.

The Citrix Cloud and Gateway Service breakout feature is enabled by default in Citrix SD-WAN software version 11.2.1 and above.

For Citrix SD-WAN software version below 11.3.0, the first packet detection and classification of Citrix Cloud and Gateway Service traffic is performed only if the Citrix Cloud and Gateway Service breakout feature is not disabled.

For Citrix SD-WAN software version 11.3.0 and above, the first packet detection and classification of Citrix Cloud and Gateway Service traffic is performed irrespective of whether the Citrix Cloud and Gateway Service breakout feature is enabled or not.

Note

- You can configure the Citrix Cloud and Gateway Service optimization only through Citrix SD-WAN Orchestrator. For more information, see Gateway service optimization.
- Citrix SD-WAN Orchestrator traffic optimization is introduced from Citrix SD-WAN soft-

ware version 11.2.3 or higher. The goal is to provide a more granular classification, and thus, separately identify Citrix SD-WAN Orchestrator traffic and other dependent services' traffic from Citrix Cloud, and provide an Internet breakout option. As a result, customers can now choose to optimize only the Citrix SD-WAN Orchestrator traffic.

## **Citrix Cloud and Gateway Service categories**

Following are the traffic categories used for classification and optimization purposes:

- Citrix Cloud: Enable to detect and route traffic destined for Citrix Cloud Web UI and APIs.
  - Citrix SD-WAN Orchestrator and dependant critical services:
    - \* **Citrix SD-WAN Orchestrator**: Enables direct internet breakout of heartbeat and other traffic required to establish and maintain connectivity between Citrix SD-WAN appliance, and Citrix SD-WAN Orchestrator.
    - \* **Citrix Cloud Download Service**: Enables direct internet breakout for download of appliance software, configuration, scripts, and so on onto the Citrix SD-WAN appliance.
- **Citrix Gateway Service**: Enable to detect and route traffic (control and data) destined for Citrix Gateway Service.
  - **Gateway Service Client Data**: Enables direct internet breakout of ICA data tunnels between clients and Citrix Gateway Service. It requires high bandwidth and low latency.
  - Gateway Service Server Data: Enables direct internet breakout of ICA data tunnels between Virtual Delivery Agents (VDAs) and Citrix Gateway Service. It requires high bandwidth and low latency and only relevant in VDA resource locations (VDA to Citrix Gateway Service connections).
  - Gateway Service Control Traffic: Enables direct internet breakout of the control traffic.
     No specific QoS considerations.
  - **Gateway Service Web Proxy Traffic**: Enables direct internet breakout of the Web proxy traffic. It requires high bandwidth but latency requirements might vary.

# Monitoring

You can monitor the Gateway service statistics in the following SD-WAN statistic reports:

• Firewall Statistics

						iource				Dest	nation					Sen				Rece	ived						
Application	Family	IP Protocol	IP Adress	Pert	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	IS NAT	ckets	Bytes	PPS	khps	Packets	Bytes	PPS	kbps	Age (5)	Last Activi Uns	ty .	Related Objects	Cenne
trix Cloud Web UI and APticitrix_cloud_web_ui_api	Custom Application	TCP	10.23.1.5	1216	Local	VIF-1-LAN-1	Default_LAN_Zone	52.177.206.73	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	7	825	0.270	0.254	6	4081	0.231	1.25	8 29	6 258	49 (See	rc Filter)(Dst Filter)(Post-Route NAT)	Ce
Iomain Name Service(dns)	Network Service	UDP	10.23.1.5	51545	Local	VIF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	1	20	0.039	0.022	1	198	0.039	0.06	1 24	6 255	58 (See	rc Filter][Dst Filter][Past-Route NAT]	Ce
omain Name Service(dns)	Network Service	UDP	10.23.1.5	59526	Local	VIF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	1	75	0.033	0.020	1	290	0.033	0.061	1 34	9 302	68 (See	c Filter][Dst Filter][Post-Route NAT]	Ge
rix Cloud Web UI and APloitrix_cloud_web_si_apit	Custom Application	TCP	10.23.1.5	1214	Local	VIF-1-LAN-1	Default_LAN_Zone	52.177.206.73	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	7	825	0.245	0.232	6	4081	0.211	1.14	9 21	8 283	17 (See	c Filter][Dst Filter][Post-Route NAT]	0
main Name ServiceUlmi2	Network Service	UDP	10.23.1.5	62651	Local	VIF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	1	71	0.035	0.020	1	148	0.035	0.043	2 21	8 284	23 (See	rc Filter)[Dst Filter][Post-Route NAT]	O
trix Gateway service Client Data(ngs_client_data)	Web	UOP	10.23.1.5	51546	Local	VIF-1-LAN-1	Default_LAN_Zone	13.93.207.26	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHEE	Yes	15	2112	0.587	0.661	13	4534	0.509	1.41	3 25	6 186	35 <u>(Ser</u>	rc Filter][Dst Filter][Post-Route NAT]	O
rix Gateway service Client Data(ngs_client_data)	Web	TCP	10.23.1.5	1223	Local	VIF-1-LAN-1	Default_LAN_Zone	13.93.207.26	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHED	Yes	366	18005	8.875	7.701	247	137919	13.206	58.990	0 19	•	4 (Sn	rc Filter)(Dst Filter)(Post-Route NAT)	0
trix Cloud Web UI and APIcitrix_cloud_web_ui_api	Custom Application	TCP	10.23.1.5	1125	Local	VIF-1-LAN-1	Default_LAN_Zone	52.177.88.75	443	Internet	Branch1_Site-Internet	Internet_Zone	ESTABLISHEE	Yes	45	21111	0.141	0.530	43	21369	0.135	0.534	6 319	9 322	42 (Sm	c Fiter)(Dst Fiter)(Past-Route NAT)	G
400005 IN USE 447 128000																											
nections																											
nections in une way scource					5	DEFCE					Destination							Sent			Receiv	end					
nnections Application +	Family	17 Protocol	IP Adress	Part	Service Type	surce Service Name	Zone	IP Address	Part	Service Type	Destination Service Nam	<b>u</b>	Zane	State	In NAT	Packet	s Byte	Sent 1 1995	khys	Packets	Receiv Bytes	ed PTS	kbps	Age A	Last tivity (ma)	Related Objects	Corr
ennections Application + Coud Downlasd ServiceString.Soud_downlasd_soc	Family	P Protocol TCP	IP Adress 172.16.30.30	Pert 40092	Service Type Local	Service Name	Zone DefaulUAN/Zone	IP Address 34.226.37.219	Part	Service Type Internet	Destination Service Nam BRANCH_XXMV9X-Im	Me Centref	Zone Warnet, Zone	State Sriv_SOV	is NAT	Packet	s Byte	Sent n PPS 0 0.834	khps 0.400	Packets	Receiv Bytes 0	ed 1775	khys 0.000	Aqu A 33	Last tivity (ma) \$77	Related Objects (Src Filter)Pest-Source NAT)	Car
Application = Application = x Cloud Deveload Service(Intra, slove), solves, achestate()	Family Web Web	IP Protocol TCP TCP	IP Adress 172.16.30.30 172.16.30.30	Pert 40092 34934	Service Type Local Local	Service Name VIF-3-LAN-1 VIF-3-LAN-1	Zone Default_LAN_Zone Default_LAN_Zone	IP Address 34.226.37.219 18.213.26.194	Part 80 443	Service Type Internet Internet	Destination Service Nam BRANCH_SCHUPS-Im BRANCH_SCHUPS-Im	termet	Zone Internet_Zone Waternet_Zone	State Sriv_SONT CLOSED	is NAT Te	Packet	s Byte 3 18 1 116	Sent s PPS 0 0.834 (4 1.90)	khps 1 0.400 2 1.611	Packets 0 12	Receiv Bytes 0 6668	ed PPS 0.000 2.076	khys 0.000 9.231	448 4 6	Last tivey (ma) \$77 3678	Related Objects (Src Files()Pest-Fause NAT) (Src Files()Post-Flave(Post-Fause NAT)	Car
Application = a Cloud Description = a Cloud Description and a Content and Application = a Cloud Description and Applications, a Novel, Aleventicad, services and a Star Application and Applications and Applic	Family Web Web Network Service	IP Protocol TCP TCP	JP Adress 172.16.30.30 172.16.30.30 172.16.30.30	Part 40092 34934 43298	Service Type Local Local	Service Name VF-3-LAN-1 VF-3-LAN-1 VF-3-LAN-1	Zone Default_LAN_Zone Default_LAN_Zone Default_LAN_Zone	IP Address 34.226.37.239 18.233.26.334 8.8.8.8	Part 80 443 53	Service Type Internet Internet Virtual Pat	Destination Service Nam BRANCH_XXMV92-In BRANCH_XXMV92-In BRANCH_XXMV92-In	ne Gerinet Gerinet Het_KOMVPX	Zone Internet, Zone Internet, Zone Any	State SYNC, SENT CLOSED ESTABLED	is NAT Te Te	Packet	s Byte 3 18 1 116 2 11	Sent s PPS 0 0.834 4 1.90 2 0.450	khps 0.400 1.611 0.022	Packets 0 12 2	Receiv Bytes 0 6668 216	ed 1975 2 2.076 0.450	khps 0.000 9.231 0.281	Aga A 4 6	Last tivity (ma) 577 3678 4149	Related Objects [Src Filed]Pet-Haute NAT] [Src Filed]Pat-Haute NAT] [Src Filed]Pat-Haute NAT]	Car
Application =  Could Desvited Strivity (Lesson Application =  Could Desvited Strivity), (Meet, Johnshild, vol 50:WKD Obsension(Striv, siless, johnerase) ain Nane Strivity)	Family Web Web Network Service Network Service	IP Presoul TCP TCP UCP	JP Adress 172.16.30.30 172.16.30.30 172.16.30.30 172.16.30.30	Pert 40092 34934 43298 45685	Service Type Local Local Local	Service Name VF-1-LAN-1 VF-2-LAN-1 VF-2-LAN-1 VF-2-LAN-1 VF-2-LAN-1 VF-2-LAN-1	Zone Default_LAN_Zone Default_LAN_Zone Default_LAN_Zone Default_LAN_Zone	IP Address 34.226.37.239 18.233.36.394 8.8.88 9.9.9.9	Part 80 443 53 53	Service Type Internet Internet Virbail Pet Internet	Destination Service Nam BRANCE_COMMYS.in	ernet Gernet HI_SVMV7X Gernet	Zone Internet, Zone Internet, Zone Any Internet, Zone	State SYN_SINT CLOSED ESTABLEP ESTABLEP	Is NAT Te Te ED No ED Te	Packer	s Byte 3 18 1 116 2 11 2 17	Sent s PPS 0 0.834 14 1.901 2 0.450 4 0.274	khys 0.400 1.611 0.222 1.0.211	Packets 0 12 2 2	Receiv Bytes 0 6668 156 388	eed PP5 0.000 2.076 0.450 0.274	khps 0.000 9.231 0.281 0.426	Age A (0) 4 6 4 7	Last tivity (004) 577 )678 4149 6743	Related Objects (Int Filter()Past-Fault NAT) (Int Filter()Dat Filter()Past-Fault NAT (Int Filter) (Int Filter)	
Application - Application - Cloud Ownerland Scinications, solical, provided and the Scinication of the S	Family Web Web Network Service Network Service Network Service	Pressoul TCP TCP UCP UCP	IP Adress 172.16.30.30 172.16.30.30 172.16.30.30 172.16.30.30 172.16.30.30	Part 40092 34934 43298 43298 39368	Service Type Local Local Local Local	VIF-3-LAN-1 VIF-3-LAN-1 VIF-3-LAN-1 VIF-3-LAN-1 VIF-3-LAN-1	Zone Default, UALZone Default, UALZone Default, UALZone Default, UALZone Default, UALZone	IP Address 34.226.37.239 18.23.36.394 8.8.8.8 9.9.9.9 9.9.9.9	Part 80 443 53 53 53	Service Type Internet Internet Virbuil Pet Internet Internet	Destination Service Nam BRANCOL, XMARP- or BRANCOL, XMARP- or BRANCOL, XMARP- or BRANCOL, XMARP- or BRANCOL, XMARP- or BRANCOL, XMARP- or	te Dennet Degraet Degraet Degraet	Zone Internet, Zone Internet, Zone Any Internet, Zone Internet, Zone	State SYNLSENT CLOSED ESTABLISP ESTABLISP ESTABLISP	In NAT Te ED No ED Te ED Te	Packet	s Byte 3 18 1 116 2 11 2 17 2 16	Sent 9775 0 0.834 1.903 2 0.455 4 0.274 4 0.533	hbps 0.400 1.611 0.222 1.0.291 7.0.352	Packets 0 12 2 2 2 2	Receiv Bytes 0 6668 156 388 368	ed 1995 2.020 0.450 0.274 0.537	khps 0.000 9.231 0.281 0.426 0.790	Aga A 4 6 7 4	Last tivily (577 3678 4149 6743 3643	Rained Objects [Fer Filter]Pear-Insue NAT] [Fer Filter]Pear-Insue NAT [Fer Filter]Pear-Insue NAT [Fer Filter]Pear-Insue NAT	0 1 1 1
Application * Application * 4 Charl Downland ServiceUting, Johney, ServiceUting 5 Di-Mich Downland ServiceUting, Johney, ServiceUting and Young ServiceUting and Young ServiceUting and Young ServiceUting and Young ServiceUting (and Young ServiceUting)	Family Web Web Network Service Network Service Web	P Pressoal 1CP 1CP 1CP 1CP 1CP	17 Adress 172.16.30.30 172.16.30.30 172.16.30.30 172.16.30.30 172.16.30.30 172.16.30.30	Pert 40092 34934 43198 43685 39368 54534	Service Type Local Local Local Local Local	VIF-3-LAN-1 VIF-3-LAN-1 VIF-3-LAN-1 VIF-3-LAN-1 VIF-3-LAN-1 VIF-3-LAN-1	Zene Default, UALZone Default, UALZone Default, UALZone Default, UALZone Default, UALZone Default, UALZone	17 Address 14.226.77.239 18.223.26.394 8.8.84 8.9.9.9 9.9.9.9 172.217.31.206	Part 80 443 53 53 53 80	Service Type Internet Internet Internet Internet Virbual Pat	Destination Service Nam BANCOL, CMARS-IN BANCOL, CMARS-IN BANCOL, CMARS-IN BANCOL, CMARS-IN BANCOL, CMARS-IN BANCOL, CMARS-IN BANCOL, CMARS-IN	M Gennet Sci_sciwurkt Gennet Gennet Gennet	Zone Vitarret, Zone Vitarret, Zone May Vitarret, Zone Vitarret, Zone Any	State SYN_SIGNT CLOSED ESTABLISH ESTABLISH CLOSED	Is NAT Te ED No ED Te ED Te No	Packet	s Byte 3 18 1 116 2 11 2 17 2 16 6 39	Sent s PFS 0 0.834 1.901 2 0.450 4 0.274 4 0.531 4 1.524	khys 0.400 1.611 0.232 0.391 7.0.352 0.801	Packets 0 12 2 2 2 5	Receiv Bytes 0 6668 156 388 368 796	ed 1975 0.000 2.476 0.450 0.274 0.537 1.271	khps 0.000 9.231 0.281 0.426 0.790 1.419	Age 4 6 4 7 4	Last (Divily) 577 3678 4149 6743 3943 3718	Robined Objects (See Filter-Davie Autors NAT) (See Filter-Davie Autors NAT)	04 17

## • Flows

Monitori	ing > Flows																									
Select	Rows																									
Nov Type Mar Novi (Per Nov T Nov Opti Refresh	to Display 50 V type: locat: Internet	i to WAN 😢	WAN to LAN	inte	met Loa	d Balan	cing Table	0 10	Terminatio	Table																
Flows	Data																									
Both LAN	to WAN and WAN I	to LAN Flows																								Toggle Columns
٠	172.1670.5	40.112.143.211	LAN to WAN	49927	443	TCP	default	10	INTERNET		LOCAL	6421	9	945	1.392	1.170	0.000	0.000	214	N/A	N/A	N/A	N/A.	N/A	N/A	egs,control_traffic 🔺
۲	172.1670.4	9.9.9.9	LAN to WAN	54577	53	UDP	default	2	INTERNET		LOCAL	8645	1	74	0.116	0.068	0.000	0.000	214	N/4	N/A	N/A	N/A	N/A	N/A	N/A
۲	172.1678.5	\$2.188.75.17	LAN to WAN	63914	46	TCP	default	2	INTERNET		LOCAL	3598198	1	166	0.000	0.000	0.000	0.000	214	N/4	N/A	N/A	N/A	N/A	N/A	https
۲	172.1670.4	40.112.143.211	LAN to WAN	50235	443	TCP	default	9	INTERNET		LOCAL	1079	8	906	7.106	6.438	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	N/A	egs_control_traffic
۲	172.1678.4	40.112.143.211	LAN to WAN	50231	443	TCP	default	9	INTERNET		LOCAL	6401		906	1,240	1.123	0.000	0.000	214	N/A	N/A	N/A	N/A	NOA	N/A	egs_control_traffic
۲	172.1670.5	40.112.143.211	LAN to WAN	49930	443	TCP	default	9	INTERNET		LOCAL	3701		906	2.137	1.926	0.000	0.000	214	N/6	N/A	N/A	N/A	N/A	N/A	egs,control_traffic
۲	172.16.78.5	40.112.143.211	LAN to WAN	62117	443	TCP	default	645	INTERNET		LOCAL	3600642	644	37918	0.112	0.053	0.000	0.000	214	N(4)	N/A	N/A	N/A	N/A	N/A	egs,control_traffic
	172.16.70.4	40.112.143.211	LAN to WAN	64280	46	TCP	default	846	INTERNET		LOCAL	6092	845	49258	0.303	0.141	0.000	0.000	214	N <sub>c</sub> G	N/A	N/A	NJA	NJA	N/A	egs_control_traffic
۰	172.16.70.4	13.91.101.240	LAN to WAN	63394	443	1CP	default	3615	INTERNET		LOCAL	3599757	3634	1012536	0.782	1.752	0.000	0.000	214	N/A	N/A	N/A	N/A	NJA	N/A	ngs_server_data
۲	9.9.3.9	172.16.70.5	WAN to LAN	53	55339	UDP	default	1	INTERNET		LOCAL	3751	1	212	0.267	0.452	0.000	0.000	214	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	40.112.143.211	172.16.70.4	WAN to LAN	443	58233	TCP	default	12	INTERNET		LOCAL	3752	12	5269	3.150	11.065	0.000	0.000	214	N(6)	N/A	N/A	N/A	N/A	N/A	N/A
(±)	40.112.143.211	172.16.70.4	WAN to LAN	443	58229	TCP	default	12	INTERNET		LOCAL	8521	12	5269	1.399	4.913	0.000	0.000	214	N <sub>c</sub> G	N/4	N/A	N/A	NJA	N/A	N/A
	40.112.143.211	172.1670.5	WAN to LAN	443	49932	TCP	default	12	INTERNET		LOCAL	1108	12	5269	10.478	36.805	0.000	0.000	214	N <sub>c</sub> GA	N/A	N/A	N/A	N/A	N/A	N/A
	40.112.143.211	172.16.70.5	WAN to LAN	443	49924	TCP	default	12	INTERNET		LOCAL	9028	12	5269	1.316	4.624	0.000	0.000	214	N/G	N/A	N/A	N/A	N/A	N/A	N/A
	40.112.143.211	172.16.70.5	WAN to LAN	443	64006	TCP	default	412	INTERNET		LOCAL	961	412	34405	0.209	0.122	0.000	0.000	214	N(4	N/A	N/A	N/A	N/A	N/A	N/A
-	40.112.143.211	172.16.70.4	WAN to LAN	443	62453	TCP	default	3.27	INTERNET		LOCAL	3606809	327	28200	0.000	0.000	0.000	0.000	214	N/A	N/A	N/A	N/A.	N/A	N/A	N/A
Total LAN 1 Total WAN	to WAN flows display to LAN flows display	ed: 18 out of 70 ed: 15 out of 69																								~

	Flows D	ata																		
в	th LAN to	WAN an	d WAN to LAN	Flows																Toggle Columns
	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
24	default	3	INTERNET		LOCAL	8034	2	174	0.249	0.173	0.000	0.000	147	N/A	N/A	N/A	N/A	N/A	N/A	N/A
9	default	4	INTERNET		LOCAL	2875	3	180	0.507	0.244	0.000	0.000	147	N/A	N/A	N/A	N/A	N/A	N/A	citrix_cloud_download_svc
2	default	16	INTERNET		LOCAL	4059	15	1372	1.927	1.410	0.000	0.000	147	N/A	N/A	N/A	N/A	N/A	N/A	citrix_sdwan_orchestrator
14	default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6447	2	112	0.310	0.139	0.141	0.000	57	N/A	13	INTERACTIVE	BRANCH1_KVMVPX-Internet-ACT-1->MCN_KVMVPX-Internet-ACT-1	N/A	Load Balanced, Reliable	N/A
2	default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	5967	6	394	0.969	0.509	0.442	0.000	1	N/A	13	INTERACTIVE	BRANCH1_KVMVPX-Internet-ACT-1->MCN_KVMVPX-Internet-ACT-1	N/A	Load Balanced, Reliable	google_gen

• DNS Statistics

Monitoring > DNS				
DNS Statistics				
Refresh				
Proxy Statistics				
Search:				
Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
Default	office365_optimize	Quad9	YES	0
Default	citrix_cloud_web_ui_api	Quad9	YES	4
Default	ngs_client_data	Quad9	YES	14
Default	ngs_server_data	Quad9	YES	0
Default	ngs_control_traffic	Quad9	YES	2286
Default	ngs_web_proxy	Quad9	YES	0
Default	Any	azureDNS	YES	51490
Showing 1 to 7 of 7 entries				
Transparent Forwarder S	tatistics			

Search:				
A	pplication Name	DNS Service Name	DNS Service Active	Hits
citrix_cloud_web_ui_a	pi	Quad9	YES	0
ngs_client_data		Quad9	YES	0
ngs_control_traffic		Quad9	YES	0
ngs_server_data		Quad9	YES	0
ngs_web_proxy		Quad9	YES	0
office365_optimize		Quad9	YES	0
Showing 1 to 6 of 6 ent	ries			

Transparent Forwarder S	tatistic	S		
Search:				
Application Name	•	DNS Service Name	DNS Se	rvice Active Hits
citrix_cloud_download_svc		Quad9	YES	1
citrix_sdwan_orchestrator		Quad9	YES	1

Showing 1 to 2 of 2 entries

# • Application Route Statistics

Monito	ring > Statistics														
Stati	Statistics														
Show: A	pplication Routes 🔽 🗆 Enabl	le Auto Refresh 🛛 🗸 seco	onds Refresh	Clear Counters on Refr	esh										
Appl	ication Route Statistics														
Maximum	aximum allowed routes: 64000														
Applicati	on Routes for routing domain : Defau	lt_RoutingDomain													
Filter:	in Any column	✓ Apply													
Show 10	D ventries Showing 1 to 6 of 6 er	ntries									First Previous	1 Next Last			
Num <sup>▲</sup>	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value			
0	O365Optimize_InternetBreakout	•	Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	7	YES	N/A	N/A			
1	NGS_WebProxy_Breakout		Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	0	YES	N/A	N/A			
2	NGS_ServerData_Breakout		Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	44	YES	N/A	N/A			
3	NGS_ControlTraffic_Breakout		Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	72	YES	N/A	N/A			
4	NGS_ClientData_Breakout		Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	0	YES	N/A	N/A			
5	CitrixCloud_Breakout		Internet	Untrusted_Internet_Zon	YES	azure07	Static	50	0	YES	N/A	N/A			
Showing	1 to 6 of 6 entries										First Previous	1 Next Last			

Application Route Statistics										
Maximum allowed routes: 64000										
Application Routes for routing domain : Default_RoutingDomain										
Filter: in Any column    Apply										
Show 100 • entries Showing 1 to 2 of 2 entries									First	evious 1 Next Last
Num Application Object Gates	way IP Address Service	Firewall Zone	Reachable	Site	Туре	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0 CitrixSdwanOrchestrator_Breakout *	Internet	Internet_Zone	YES	BRANCH1_KVMVPX	Static	50	35	YES	N/A	N/A
1 CitrixCloudDownloadSvc_Breakout *	Internet	Internet_Zone	YES	BRANCH1_KVMVPX	Static	50	8	YES	N/A	N/A
Showing 1 to 2 of 2 entries									First Pr	rvious 1 Next Last

## Troubleshooting

You can view the service error in the **Events** section of the SD-WAN appliance.

To check the errors, navigate to **Configuration > System Maintenance > Diagnostics**, click **Events** tab.

Dashboard Monitoring	Configuration													
+ Appliance Settings	Configuration > System Maintenance > Diagnostics													
- System Maintenance	Ping         Traceroute         Packet Capture         Path Bandwidth         System Info         Diagnostic Data         Events         Alarms         Diagnostics Tool													
– Delete Files – Restart System – Date/Time Settings	Site Diagnostics													
Local Change Management Diagnostics	Object Type: USER EVENT													
- Update Software - Configuration Reset	Event type: UNDEFINED  Seventhy: DEBUTO													
	Add Event													

If there is an issue in connecting to the Citrix service (sdwan-app-routing.citrixnetworkapi.net), then the error message reflects under the **View Events** table.

View E	vents						
Quantity Filter: Reload	r: Events Table	25 Object Type = APP		Event type = FAILURE	Severity =	ERROR	\$
ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
13839	26	Endpoints Update	APPLICATIONS	2019-02-12 09:02:15	FAILURE	ERROR	Failed to connect to the service API
Times are in	n UTC						

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 dropdown list under the **Download Log file** section and click **Download Log**.

#### Citrix SD-WAN 11.5

Dashboard Monitoring	Configuration												
- Appliance Settings	Configuration > Appliance Settings > Logging/Monitoring												
Administrator Interface													
Logging/Monitoring	Log Options Alert Options Alarm Options Syslog Server HTTP Server												
– Network Adapters – Net Flow	View Log File												
- App Flow/IPFIX - SNMP	Only the most recent 10000 entries will be shown and filtered. To view the full log, download and open it locally.												
- NITRO API Licensing	Filename: SDWAN_dpi.log +												
+ Virtual WAN	Filter (Optional):												
+ System Maintenance	View Log												
	Download Log File												
	Filename: SDWAN_dpi.log \$ Download Log												

# **PPPoE Sessions**

#### August 24, 2022

Point-to-Point Protocol over Ethernet (PPPoE) connects multiple computer users on an Ethernet LAN 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 LAN. 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 acts as a PPPoE client. It authenticates with the PPPoE server and obtains dynamic IP address, or uses static IP address to establish PPPoE connections.

The following are required to establish successful PPPoE sessions:

- Configure virtual network interface (VNI).
- Unique credentials for creating PPPoE session.
- Configure WAN link. Each VNI can have only one WAN link configured.
- Configure Virtual IP address. Each session obtains a unique IP address, dynamic, or static based on the provided configuration.

- Deploy appliance in bridge mode to use PPPoE with static IP address and configure the interface as "trusted."
- Static IP is preferred to have a configuration to force the server proposed IP; if different from the configured static IP, otherwise an error can occur.
- Deploy appliance as an Edge device to use PPPoE with dynamic IP and configure the interface as "untrusted."
- Authentication protocols supported are, PAP, CHAP, EAP-MD5, EAP-SRP.
- Maximum number of multiple sessions depends on the number of VNIs configured.
- Create multiple VNIs to support Multiple PPPoE sessions per interface group.

Note:

Multiple VNIs are allowed to create with same 802.1Q >VLAN tag.

## Limitations for PPPoE configuration:

- 802.1q VLAN tagging is not supported.
- EAP-TLS authentication is not supported.
- Address/Control compression.
- Deflate Compression.
- Protocol field compression negotiation.
- Compression Control Protocol.
- BSD Compress Compression.
- IPX protocols.
- PPP Multi Link.
- Van Jacobson style TCP/IP header compression.
- Connection-ID compression option in Van Jacobson style TCP/IP header compression.
- PPPoE is not supported on LTE interfaces

From Citrix SD-WAN 11.3.1 release, an extra 8 bytes PPPoE header is considered for adjusting TCP Maximum Segment Size (MSS). The extra 8 bytes PPPoE header adjusts the MSS in the synchronize packets based on the MTU.

For information on how to configure PPPoE through Citrix SD-WAN Orchestrator service, see Interfaces.

# 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 and stop the sessions for troubleshooting purposes from Citrix SD-WAN Orchestrator service.

- If the VNI is up and ready, the **IP and Gateway IP** columns shows the current values in the session. It indicates that these are recently received values.
- If the VNI is stopped or is in failed state, the values are last received values.

P	PoE Monitoring	5						
	Refresh						Search	Q
	Virtual Interface 🔅	Session ID 🔅	IPv4 Address	Gateway IP 🔅	IPv4 State 🗘	Link Local IPv6 Address	Remote Link Local IPv6 Address 💠	IPv6 State 🗘 🗘 +
1	VIF-2-WAN-1	2	10.0710.0	110.00	Ready	1480-1-0110803-au/9214 af		Ready

The **State** column displays the status of the PPPoE session using three color codes; green, red, yellow, and values. The following table describes the states and descriptions. You can hover over the states to obtain descriptions.

PPPoE session type Configured Dialing	Color	Description
Configured	Yellow	A VNI is configured with PPPoE.
		This is an initial state.
Dialing	Yellow	After a VNI is configured, the
		PPPoE session state moves to
		dialing state by starting the
		PPPoE discovery. Packet
		information is captured.
Session	Yellow	VNI is moved from Discovery
		state to Session state. waiting
		to receive IP, if dynamic or
		waiting for acknowledgment
		from server for the advertised
		IP, if static.
Ready	green	IP packets are received and VNI
-	-	and associated WAN link is
		ready for use.
		-

PPPoE session type	Color	Description
Failed	red	PPP/PPPoE session is
		terminated. The reason for the
		failure can be due to Invalid
		Configuration or fatal error.
		The session attempts to
		reconnect after 30 seconds.
topped	yellow	PPP/PPPoE session is manually
		stopped.
Terminating	yellow	An intermediate state
		terminating due to a reason.
		This state automatically starts
		after certain duration (5
		seconds for normal error or 30
		secs for a fatal error).
Disabled	yellow	The SD-WAN service is disabled.

#### **Troubleshooting PPPoE session failures**

On the Monitoring page, when there is a problem in establishing a PPPoE session:

- Hovering mouse over the Failed status shows the reason for the recent failure.
- To establish a fresh session or for troubleshooting an active PPPoE session, use the monitoring PPPoE page and restart the session.
- If a PPPoE session is stopped manually, it cannot be started until either it is manually started and a configuration change is activated, or service is restarted.

A PPPoE session might fail due to the following reasons:

- When SD-WAN fails to authenticate itself to the peer due to incorrect username/password in the configuration.
- PPP negotiation fails negotiation does not reach the point where at least one network protocol is running.
- System memory or system resource issue.
- Invalid/bad configuration (wrong AC name or service name).
- Failed to open serial port due to operating system error.
- No response received for the echo packets (link is bad or server is not responding).

• There were several continuous unsuccessful dialing sessions with in a minute.

After 10 consecutive failures, the reason for the failure is observed.

- If the failure is normal, it restarts immediately.
- If the failure is an error then restart reverts for 10 seconds.
- If the failure is fatal the restart reverts for 30 seconds before restarting.

LCP Echo request packets are generated from SD-WAN for every 60 seconds and failure to receive 5 echo responses is considered as link failure and it re-establishes the session.

### **PPPoE** log file

The SDWAN\_ip\_learned.log file contains logs related to PPPoE.

To view or download the *SDWAN\_ip\_learned.log* file from the SD-WAN GUI, navigate to **Appliance Set**tings > Logging/Monitoring > Log Options. View or download the *SDWAN\_ip\_learned.log* file.

Dashboard Monitoring	Configuration
Appliance Settings     Administrator Interface     Logging/Monitoring     Network Adapters     Net Flow     App Flow/IPFIX     SNMP     NITRO API     Licensing     Virtual WAN     System Maintenance	Configuration > Appliance Settings > Logging/Monitoring         Log Options       Alert Options       Syslog Server         HTTP Server         View Log File         Only the most recent 10000 entries will be shown and filtered. To view the full log, download and open it locally.         Filename:       SDWAN_ip_learmed lk •         Filter (Optional):
	Download Log File       Filename:     SDWAN_ip_learned.ik ▼       Download Log

# **Quality of service**

#### October 21, 2022

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.

From SD-WAN 11.5 release onwards, QoS features are configurable through Citrix SD-WAN Orchestrator service. For more information, see <u>Quality of Service</u>.

# Classes

The Citrix SD-WAN configuration provides a default set of application and IP/Port based QoS policies that are applied to all traffic going over Virtual Paths. These settings can be customized to fit the deployment needs.

Classes are useful to prioritize the traffic. Application and IP/Port based QoS policies classify traffic and put it into appropriate classes specified in the configuration.

Citrix SD-WAN Orchestrator service supports 13 classes. For more information, see Classes.

The following are the different types of classes:

- **Real-time**: Used for low latency, low bandwidth, time-sensitive traffic. Real-time applications are time sensitive but don't really need high bandwidth (for example voice over IP). Real-time applications are sensitive to latency and jitter, but can tolerate some loss.
- **Interactive**: Used for interactive traffic with low to medium latency requirements and low to medium bandwidth requirements. The interaction is typically between a client and a server. The communication might not need high bandwidth but is sensitive to loss and latency.
- **Bulk**: Used for high bandwidth traffic and applications that can tolerate high latency. Applications that handle file transfer and need high bandwidth are categorized as bulk class. These applications involve little human interference and are mostly handled by the systems themselves.

#### Bandwidth sharing among classes

Bandwidth is shared among classes as follows:

- **Real-time**: Traffic hitting real-time classes are guaranteed to have low latency and bandwidth is capped to the class share when there is competing traffic.
- **Interactive**: Traffic hitting the interactive classes get remaining bandwidth after serving realtime traffic and the available bandwidth is fair shared among the interactive classes.

• **Bulk**: Bulk is best effort. Bandwidth left over after serving real-time and interactive traffic is given to bulk classes on a fair share basis. Bulk traffic can starve if real-time and interactive traffic utilizes all the available bandwidth.

Note

Any class can use all available bandwidth when there is no contention.

The following example explains the bandwidth distribution based on the class configuration:

Consider there is an aggregated bandwidth of 10 Mbps over Virtual Path. If the class configuration is

- Real-time: 30%
- Interactive High: 40%
- Interactive Medium: 20%
- Interactive Low: 10%
- Bulk: 100%

The bandwidth distribution outcome is:

- Real-time traffic gets 30% of 10Mbs (3 Mbps) based on the need. If it needs less than 10%, then the rest of the bandwidth is made available to the other classes.
- Interactive classes share the remaining bandwidth on fair share basis (4 Mbps: 2 Mbps: 1 Mbps).
- Anything leftover when real-time, interactive traffic is not fully using their shares is given to the Bulk class.

## **Rules by IP address and port number**

Rules by IP address and port number feature helps you to create rules for your network and take certain Quality of Service (QoS) decisions based on the rules. You can create custom rules for your network. For example, you can create a rule as –If source IP address is 172.186.30.74 and destination IP address is 172.186.10.89, set **Transmit mode** as Persistent Path and **LAN to WAN Class** as 10(realtime\_class)".

You can create rules locally at a site level or at the global level. If more than one site requires the same rule, you can create a template for rules globally under **Global > Virtual Path Default Sets > Rules**. The template can then be attached to the sites where the rules need to be applied. Even if a site is associated with the globally created rule template, you can create site specific rules. In such cases, site specific rules take precedence and override the globally created rule template.

From Citrix SD-WAN 11.5 release onwards, you can create IP rules using Citrix SD-WAN Orchestrator service. For more information, see IP rules.

## **Verify rules**

Navigate to **Monitoring > Flows**. Select **Flow Type** field located in the **Select Flows** section at the top of the **Flows** page. Next to the **Flow Type** field there is a row of check boxes for selecting the flow information you want to view. Verify if the flow information is according to the configured rules.

### Example:

The rule "If source IP address is 172.186.30.74 and destination IP address is 172.186.10.89, set **Transmit mode** as Persistent Path"shows the following **Flows Data**.



Statistics	Moni	toring >	Statistics																
Flows																			
Routing Protocols	Sta	tistics																	
Firewall	Show:	Rules		•	🗹 Er	able Auto	Refresh 5	▼ seconds	Stop										
IKE/IPsec																			
IGMP	Rule Statistics																		
Performance Reports	Filter	Filter: in Any column   Apply																	
Qos Reports				In the second se															
Usage Reports	Show	100 🔻 er	tries Showin	g 1 to	to 100 of 275 entries														
Availability Reports				Add	P		Por				LAN to V	LAN to WAN					WAN to LAN		
Appliance Reports	Num	Site	Service	Src	Dst	IP Proto	Src	Dst	VLAN ID	IP DSCP	Bytes	Packets	Bytes	Packets	Jitter (ms)	Packets Lost	Avg Latency (ms)	Min Latency (ms)	Ma Late (m
DHCP Server/Relay	0	DC	DC-Client-1	*	*	тср	5003	*	*	*	0	0	0	0					
VRRP	1	DC	DC-Client-1	*	*	TCP		5003			426121168	285604	0	0					
PPPoE	2	DC	DC-Client-1			тср	5060-5061	•		ef	0	0	0	0					
DNS	3	DC	DC-Client-1	*	*	TCP	*	5060-5061	*	ef	0	0	0	0					
	4	DC	DC-Client-1		•	UDP	5060-5061	•	•	ef	0	0	0	0					
	5	DC	DC-Client-1	*	*	UDP	*	5060-5061	*	ef	0	0	0	0					

Navigate to **Monitoring > Statistics** and verify the configured rules.

# **Rules by application name**

The Application classification feature allows the Citrix SD-WAN appliance to parse incoming traffic and classify them as belonging to a particular application or application family. This classification allows us to enhance the QoS of individual application or application families by creating and applying application rules.

You can filter traffic flows based on application, application family, or application object match-types and apply application rules to them. he application rules are similar to Internet Protocol (IP) rules.

For information on IP rules see, Rules by IP Address and Port Number.

For every application rule, you can specify the mode of transmission. The following are the available transmit modes:

- Load Balance Path: Application traffic for the flow is balanced across multiple paths. Traffic is sent through the best path until that path is used. The remaining packets are sent through the next best path.
- **Persistent Path**: Application traffic remains on the same path until the path is no longer available.
- Duplicate Path: Application traffic is duplicated across multiple paths, increasing reliability.

The application rules are associated to classes. For information on classes, see Customizing Classes.

By default, the following five pre-defined application rules are available for Citrix ICA applications:

							Discarc	1				
				Enable			Late					
				Packet	Enable		Rese-					
			Retran	sAngit	Packet	Resequ	enterne-					
			Lost	gre-	Rese-	Hold	ing	Drop	Drop		Disable	Disable
		Transm	ni <b>₽</b> ack-	ga-	quenc-	Time	Pack-	Limit	Depth	Enable	Limit	Depth
Rule	Class	Mode	ets	tion	ing	(ms)	ets	(ms)	(bytes)	RED	(ms)	(bytes)
HDX_F	Priobrity_	0 Load	True	False	True	250	True	350	30000	True	0	128000
	(HDX_	pnBoantity_	tag_0)									
		ance										
		Path										
HDX_F	Pribrity_	1 Load	True	False	True	250	True	350	30000	True	0	128000
	(HDX_	pnBoanlity_	tag_1)									
		ance										
		Path										
HDX_F	Priority_	2 Load	True	False	True	250	True	350	30000	True	0	128000
	(HDX_	prBcantity_	tag_2)									
		ance										
		Path										
HDX_F	Priosrity_ີ	3 Load	True	False	True	250	True	350	30000	True	0	128000
	(HDX_	prBoantity_	tag_3)									
		ance										
		Path										

							Discard	ł					
				Enable			Late						
				Packet	Enable		Rese-						
			Retran	siAngit	Packet	Resequ	uencenc-	epteenc-					
			Lost	gre-	Rese-	Hold	ing	Drop	Drop		Disable	e Disable	
		Transm	ni <b>₽</b> ack-	ga-	quenc-	Time	Pack-	Limit	Depth	Enable	Limit	Depth	
Rule	Class	Mode	ets	tion	ing	(ms)	ets	(ms)	(bytes)	RED	(ms)	(bytes)	
HDX	11	Load	True	False	True	250	True	350	30000	True	0	128000	
	(in-	Bal-											
	ter-	ance											
	ac-	Path											
	tive_hi	igh_clas	s)										

#### How application rules are applied?

In the SD-WAN network, when the incoming packets reach the SD-WAN appliance, the initial few packets do not undergo DPI classification. At this point, the IP rule attributes such as Class, TCP termination are applied to the packets. After DPI classification, the application rule attributes such as Class, transmit mode override the IP rule attributes.

The IP rules have more number of attributes as compared to the application rules. The application rule overrides only a few IP rule attributes, the rest of the IP rule attributes remain processed on the packets.

For example, consider you have specified an application rule for a webmail application such as Google Mail that uses the SMTP protocol. The IP rule set for SMTP protocol is applied initially before DPI classification. After parsing the packets and classifying it as belonging to Google Mail application, the application rule specified for the Google Mail application is applied.

To create application rules using Citrix SD-WAN Orchestrator, see Application rules.

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.

Flows Data	Hows Data																								
Toggie Columns															1										
Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Fransmission Type	2m
172.186.30.74	172.186.10.89	LAN to WAN	35118	5001	UDP	default	4961	Virtual Path	DC-Client-1	LOCAL	0	4959	7428582	292.687	3507.565	126.441	0.000	48	0	11	INTERACTIVE	0C-WL-1->Client-1-WL-1	N/A	Duplicat	19
Total LAN to WAN Total WAN to LAN	I flows displayed:	1 out of 1 0 out of 0																				_			

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.

Dashboard Monitoring Configuration																		
Statistics	Monito	Monitoring > Statistics																
Flows																_		
Routing Protocols	Statis	Statistics																
Firewall	Show: Application QoS 🔹 🗉 Enable Auto Ratherh 🖇 🔹 seconds 🛛 Ratherh																	
IKE/IPsec		Analization Over Statistics																
Performance Reports	Арри	Apprication Qos statistics																
Qos Reports	Filter	Piter In Any column Y Apply																
Usage Reports						_												
Availability Reports	Show 10	Inow 100 V entries Showing to 12 of 12 entries In Previous 1 Previous															Last	
Appliance Reports				IP Address		Port					LAN to WAN		WAN to LAN		Dropped			
DHCP Server/Relay	Num *	Site	Service	Sec	Dst	Sec	Dst	Application Object	Application	Family	Bytes	Packets	Bytes	Packets	Bytes	Packets	Last Hit (D:HH:MM ago)	
Since Samelynaisy	0	DC	DC-Client-1	•				•	iperf	1.00	26325792	32262	0	0	287616	192	00:00	^
	1	DC	DC-Client-1	•	1	•	•		ica_priority_0		0	0	0	0	0	0		
	2	DC	DC-Client-1	•			•	1 C	ica_priority_1	1.0	0	0	0	0	0	0		
	3	DC	DC-Client-1					*	ica_priority_2		0	0	0	0	0	0		
	4	DC	DC-Client-1					*	ica_priority_3		0	0	0	0	0	0		
	5	DC	DC-Client-1				•		ica	1.0	0	0	0	0	0	0		
	6	Client-1	DC-Client-1				•		iperf	1.0	0	0	4710	5	1484	1	00:38	-
	Showing 1	to 12 of 12 ent	tries														First Previous 1 Next	Last
	4																	E F

#### **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.

Тір

You can specify one or more match types.

## **Application classification**

The Citrix SD-WAN appliances perform deep packet inspection (DPI) to identify and classify applications using the following techniques:

- DPI library classification
- Citrix-proprietary Independent Computing Architecture (ICA) classification
- Application vendor APIs (for example Microsoft REST APIs for Office 365)
- Domain name based application classification

# **DPI library classification**

The Deep Packet Inspection (DPI) library recognizes thousands of commercial applications. It enables real-time discovery and classification of applications. Using the DPI technology, the SD-WAN appliance analyses the incoming packets and classifies the traffic as belonging to a particular application or application family. Application classification for each connection takes a few packets.

To enable DPI library classification on Citrix SD-WAN Orchestrator service, see DPI library classification.

# **ICA classification**

Citrix SD-WAN appliances can also identify and classify Citrix HDX traffic for virtual apps and desktops. Citrix SD-WAN recognizes the following variations of the ICA protocol:

- ICA
- ICA-CGP
- Single Stream ICA (SSI)
- Multi-Stream ICA (MSI)
- ICA over TCP
- ICA over UDP/EDT
- ICA over non-standard ports (including Multi-Port ICA)
- HDX Adaptive Transport
- ICA over WebSocket (used by HTML5 Receiver)

## Note

Classification of ICA traffic delivered over SSL/TLS or DTLS is not supported in SD-WAN Standard Edition.

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

Framehawk traffic and Audio-over-UDP/RTP are not classified as HDX applications. They are reported as either "UDP" or "Unknown Protocol."

Since release 10 version 1, the SD-WAN appliance can differentiate each ICA data stream in multistream ICA even in a single-port configuration. Each ICA stream is classified as a separate application with its own default QoS class for prioritization.

• For Multi-Stream ICA functionality to work properly, you must have SD-WAN Standard Edition 10.1 or above. • For HDX user based reports to be shown on SDWAN-Center, you must have SD-WAN Standard Edition 11.0 or above.

Minimum software requirements for HDX information virtual channel:

- A Current Release of Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop), since the prerequisite functionality was introduced in XenApp and XenDesktop 7.17 and is not included in the 7.15 Long-Term Service Release.
- A version of the Citrix Workspace app (or its predecessor, Citrix Receiver) that supports multi-stream ICA and the HDX Insights information virtual channel, CTXNSAP. Look for HDX Insight with NSAP VC and Multiport/Multi-stream ICA in the Citrix Workspace app Feature Matrix. See the currently supported release versions at HDX Insights.
- From 11.2 release onwards, packet duplication is now enabled by default for HDX real-time traffic when multi-stream ICA is in use.

Once classified, the ICA application can be used in application rules and to view application statistics similar to other classified applications.

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

- Independent Computing Architecture (Citrix)(ICA)
- ICA Real-time (ica\_priority\_0)
- ICA Interactive (ica\_priority\_1)
- ICA Bulk-Transfer (ica\_prority\_2)
- ICA Background(ica\_priority\_3)

## For more information, see Rules by Application Name

If you are running a combination of software that does not support Multi-Stream ICA over a single port, then to perform QoS you must configure multiple ports, one for each ICA stream.

To classify HDX on non-standard ports as configured in XA/XD server policy, you must add those ports in ICA port configurations. Also, to match traffic on those ports to valid IP rules, you must update the ICA IP rules.

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

To enable ICA based classification on Citrix SD-WAN Orchestrator service, see ICA classification.

## **Application vendor API based classification**

Citrix SD-WAN supports the following application vendor API based classification:

- Office 365. For more information, see Office 365 optimization.
- Citrix Cloud and Citrix Gateway service. For more information, see Gateway Service Optimization.

## Domain name based application classification

The DPI classification engine is enhanced to classify applications based on the domain name and patterns. After the DNS forwarder intercepts and parses the DNS requests, the DPI engine uses the IP classifier to perform first packet classification. Further DPI library and ICA classification are done and the domain name based application ID is appended.

The Domain name based application feature allows you to group several domain names and treat it as a single application. Making it easier to apply firewall, application steering, QoS, and other rules. A maximum of 64 domain name based applications can be configured.

To define domain name based applications on Citrix SD-WAN Orchestrator service, see Domain name based application classification.

Note

- From 11.4.2 release onwards, the Domain name-based applications support configurable ports and protocol in Citrix SD-WAN Orchestrator service. For more information, see Domains and applications.
- From Citrix SD-WAN 11.5.0 release onwards, AAAA records are supported on Citrix SD-WAN Orchestrator service.

## Limitations

- If there are no DNS request/response corresponding to a domain name based application, the DPI engine does not classify the domain name based application and hence does not apply the application rules corresponding to the domain name based application.
- If an Application Object is created such that the port range includes port 80 and/or port 443, with a specific IP address match type that corresponds to a domain name based application, the DPI engine does not classify the domain name based application.
- If explicit web proxies are configured, you have to add all the domain name patterns to the PAC file, to ensure that the DNS response does not always return the same IP address.

- The domain name based application classifications are reset on configuration upgrade. Reclassification happens based on pre 11.0.2 release classification techniques such as DPI library classification, ICA classification and Vendor application APIs based classification.
- The application signatures learned (destination IP addresses) by domain name based application classification are reset on configuration update.
- Only the standard DNS queries and their responses are processed.
- DNS response records split over multiple packets are not processed. Only DNS responses in a single packet are processed.
- DNS over TCP is not supported.
- Only top-level domains are supported as domain name patterns.

# Classifying encrypted traffic

Citrix SD-WAN appliance detects and reports encrypted traffic, as part of application reporting, in the following two methods:

- For HTTPS traffic, the DPI engine inspects the SSL certificate to read the common name, which carries the name of the service (for example Facebook, Twitter). Depending on the application architecture only one certificate might be used for several service types (for example email, news, and so on). If different services use different certificates, the DPI engine would be able to differentiate between services.
- For applications that use 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.

## **Application Objects**

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

The following features use the application object as a match type:

- Application Routes
- Firewall policy
- Application QoS Rules
- Application QoE
#### **Using Application Classification with a Firewall**

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

riority:						
100						
From Zones				lo zones		
Zon	e	Enable	A		Zone	Enable 🔺
Any		1		Any		2
Default_LAN_Zone				Default_LAN_Zo	ne	
Internet_Zone				Internet_Zone		
			_			
Untrusted_Internet_Zon ction: Allow • latch Type:	e Log Interval (s): 0 Application Objects:	Ар	plication:	Untrusted_Interr	Cor Log End U	Innection State Tracking: Jse Site Setting V amily:
Untrusted_Internet_Zon ction: Allow • Iatch Type: IP Protocol • IP Protocol • Application Family Application Objects	e Log Interval (s): 0 Application Objects: Any * DSCP: Any Any	Ap	plication:	Untrusted_Interr	Log End U Application Ra	Innection State Tracking: Ise Site Setting  amily: Match Established
Untrusted_Internet_Zon ction: Allow • Internet_Zon Allow • Internet_Zon Application Application Application Chamily Application Objects ource Service Type:	e Log Interval (s): 0 Application Objects: Any DSCP: Any Source Service Name	Ap	plication: Allo purce IP:	Untrusted_Interr	Cor Log End U Application Fa Reverse Also Source Port:	Innection State Tracking: Jse Site Setting  amily: Match Established
Contrusted_Internet_Zon Ction: Allow • Iatch Type: IP Protocol • IP Protocol • Application Family Application Objects ource Service Type: Any •	e Log Interval (s): 0 Application Objects: Any T DSCP: T Any Source Service Name: Any T	Ap	plication:	Untrusted_Interr	Cor Log End U Application Fa Reverse Also Source Port:	Innection State Tracking: Jse Site Setting T amily: T Match Established
Untrusted_Internet_Zon ction: Allow • IP Protocol • IP Protocol • IP Protocol • Application Family Application Objects ource Service Type: Any • Nest Service Type:	e Log Interval (s): 0 Application Objects: Any * DSCP: * Any Source Service Name: Any * Dest Service Name:	Ap	Plication: Allo Surce IP:	Untrusted_Interr	Log End U Application R Reverse Also Source Port:	Innection State Tracking: Jee Site Setting  amily: Match Established

#### **Viewing Application Classification**

After enabling application classification, you can view the application name and application family details in the following reports:

- Firewall connection Statistics
- Flows information
- Application statistics

**Firewall connection statistics** Navigate to **Monitoring > Firewall**. Under **Connections** section, the **Application** and **Family** columns list the applications and its associated family.

## Citrix SD-WAN 11.5

Da	shboard	Monitoring Co	nfiguration																	
м	onitoring > Firev	wall																		
	Firewall Statisti	cs																		
Stat Max to c	istics: kimum entries lisplay:	Connections V																		
Filt	aring:	Application:	Any	•	<ul> <li>Family:</li> </ul>			Any	~											
		IP Protocol:	Any	~	Source Zone:			Any	<b>v</b> 0	estination Zone: A	ıy		~							
		Source Service Type:	Any	~	Source Servio	ce Instan	ce:	Any 🗸	s	ource IP:			Source Port: *							
		Destination Service T	ype: Any	~	Destination 9	Service Ir	stance:	Any 🗸	C	estination IP: [*			Destination Port: *							
Re	fresh	Show latest data	Show Addi	tional Stat	s															
CI	ear Connections																			
Hel	p																			
	C																			
	connections																			
							Sour	ce				C	Pestination					Sen	nt	
	Appli	cation	Family	IP Protocol	IP Adress	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps
G	oToMeeting Online	Meeting(gotomeeting)	Audio/Video	тср	172.16.30.30	54612	Local	Site1_VI_1	Default_LAN_Zone	216.115.208.241	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	4	259	0.716	0.371
D	omain Name Servic	e(dns)	Network Service	UDP	172.16.30.30	47397	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	1	60	0.262	0.126
N	etwork Time Protoc	col(ntp)	Network Service	UDP	172.16.30.30	48743	Local	Site1_VI_1	Default_LAN_Zone	91.189.94.4	123	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	NEW	No	1	76	0.264	0.160
D	omain Name Servio	e(dns)	Network Service	UDP	172.16.30.30	41348	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	118	0.476	0.225
D	omain Name Servic	e(dns)	Network Service	UDP	172.16.30.30	44961	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	114	0.513	0.234
D	omain Name Servic	e(dns)	Network Service	UDP	172.16.30.30	44119	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	1	60	0.263	0.126
G	oogle Generic(goog	gle_gen)	Web	тср	172.16.30.30	45706	Local	Site1_VI_1	Default_LAN_Zone	172.217.26.206	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	6	394	1.017	0.534
BI	NG		Custom Application	тср	172.16.30.30	45464	Local	Site1_VI_1	Default_LAN_Zone	204.79.197.200	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	31	1348	6.428	2.236
D	omain Name Servic	e(dns)	Network Service	UDP	172.16.30.30	59856	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	116	0.410	0.190
D	omain Name Servic	æ(dns)	Network Service	UDP	172.16.30.30	49607	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	122	0.354	0.173
м	ozilla.com – Mozilla	a.org(mozilla)	Web	тср	172.16.30.30	46324	Local	Site1_VI_1	Default_LAN_Zone	63.245.208.195	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	6	395	1.551	0.817
D	omain Name Servic	e(dns)	Network Service	UDP	172.16.30.30	52889	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	112	0.332	0.149
м	icrosoft(microsoft)		Web	тср	172.16.30.30	51194	Local	Site1_VI_1	Default_LAN_Zone	104.215.148.63	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	6	397	1.433	0.758
Con	nections Displaye	sd: 13																		
Con	nections In Use: 1	3/128000																		

If you do not enable application classification, the **Application** and **Family** columns do not show any data.

Das	shboard	N	donitoring	Config	uration													_					
Мо	onitoring	> Firew	all																				
F	irewall (	Statistic	·c																				
	incinuit .	statistic																					
Stati: Maxi	stics: imum enti	ries	Connection	s 🗸																			
to di	isplay:		50 🗸																				
Filter	ring:		Applicatio	n:	Any		<b>~</b>	Family:	Any		~	1		1									
			IP Protoco		Any		<b>*</b>	Source Zone:	Any		~	Destination Zone: Any						_					
			Source Ser	vice Type:	Any		<b>*</b>	Source Service Insta	nce: Any 🗸			Source IP:		Source Port:	Ľ			_					
_			Destinatio	n Service Type	Any		~	Destination Service I	nstance: Any 🗸			Destination IP:		Destination	Port: [	•							
Ref	resh		Show I	atest data	Sho	w Additi	onal Stats																
Help	ar Conne	ections																					
C	Connecti	ons																					
						Sou	rce					Destination					Se	nt			Rec	eived	
App	lication	Family	IP Protocol	IP Adress	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS	kbps A
•		•	тср	172.16.30.30	54632	Local	Site1_VI_1	Default_LAN_Zone	216.115.208.241	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	4	259	0.909	0.471	3	217	0.682	0.395
•		•	UDP	172.16.30.30	41664	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	112	0.383	0.171	2	156	0.383	0.239
•			UDP	172.16.30.30	36817	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	122	0.408	0.199	2	196	0.408	0.320
•		•	тср	172.16.30.30	45726	Local	Site1_VI_1	Default_LAN_Zone	172.217.26.206	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	6	394	1.207	0.634	4	744	0.804	1.197
•		•	тср	172.16.30.30	45484	Local	Site1_VI_1	Default_LAN_Zone	204.79.197.200	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	26	1136	6.780	2.370	53	63972	13.820	133.449
		*	UDP	172.16.30.30	53904	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	118	0.589	0.278	2	272	0.589	0.641
		•	UDP	172.16.30.30	49809	Local	Site1_VI_1	Default_LAN_Zone	8.8.8.8	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	ESTABLISHED	No	2	116	0.513	0.238	2	354	0.513	0.727
1.							Circl 14.1	Default LAN Zone	104.215.148.63	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	6	397	1.796	0.951	4	361	1.197	0.864
•		•	тср	172.16.30.30	51214	Local	Site1_vi_1	Delaun_Den_zone															
•		•	тср тср	172.16.30.30 172.16.30.30	51214 46344	Local	Site1_VI_1 Site1_VI_1	Default_LAN_Zone	63.245.208.195	80	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No	6	395	1.904	1.003	4	387	1.269	0.982
•		•	TCP TCP UDP	172.16.30.30 172.16.30.30 172.16.30.30	51214 46344 52627	Local Local Local	Site1_VI_1 Site1_VI_1 Site1_VI_1	Default_LAN_Zone Default_LAN_Zone	63.245.208.195 8.8.8.8	80 53	Virtual Path Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone Internet_Zone	CLOSED ESTABLISHED	No No	6 2	395 114	1.904 0.622	1.003 0.283	4	387 210	1.269 0.622	0.982
* * Conr	nections I	* * * Displayed	TCP TCP UDP d: 10 0/128000	172.16.30.30 172.16.30.30 172.16.30.30	51214 46344 52627	Local Local Local	Site1_VI_1 Site1_VI_1 Site1_VI_1	Default_LAN_Zone Default_LAN_Zone	63.245.208.195 8.8.8.8	80 53	Virtual Path Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX MCN_KVMVPX-BRANCH1_KVMVPX	Internet_Zone	CLOSED	No No	6 2	395 114	1.904 0.622	1.003 0.283	4	387 210	1.269 0.622	0.982

**Flows Information** Navigate to **Monitoring > Flows**. Under **Flows Data** section, the **Application** column lists the application details.

Monitoring	> Flow	s																	
Select Fl	ows																		
low Type: lax Flows to Per Flow Typ ilter (Option Refresh	Display e): al):	☑ LAN to ₩/	AN 🗳 WAN to LAN 🗌 Inter	net Load	Balanci	ng Table	🗆 тсі	' Termi	nation Tabl	e									
Flows D	ıta																		
oth LAN to	VAN and	WAN to LAN	Flows																Toggle Column
IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6979	2	112	0.287	0.128	0.131	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4967	2	118	0.403	0.190	0.184	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
default	28	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4963	27	1176	4.950	1.725	2.257	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	bing
default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4811	2	114	0.416	0.190	0.190	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
default	5	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	5715	4	259	0.644	0.334	0.294	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	gotomeeting
default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6717	2	122	0.298	0.145	0.136	0.000	51	N/A	13	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	N/A
default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6692	6	394	0.876	0.460	0.399	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	google_gen
default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4016	6	395	1.254	0.660	0.572	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	mozilla
default	3	INTERNET	-	LOCAL	5711	2	116	0.350	0.162	0.000	0.000	135	N/A	N/A	N/A	N/A	N/A	N/A	N/A
default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4775	6	397	1.222	0.647	0.557	0.000	28	N/A	14	INTERACTIVE	Site1_Test-WL1->HQ1_Test-WL1	N/A	Load Balanced, Reliable	microsoft
default	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6883	2	156	0.288	0.180	0.131	0.000	117	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	N/A
default	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4936	2	272	0.403	0.439	0.184	0.000	117	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	N/A
default	53	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4969	53	64273	9.730	94.396	4.437	0.000	94	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	bing
cs4	2	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	4804	2	210	0.416	0.350	0.190	0.000	117	N/A	N/A	N/A	N/A	N/A	Load Balanced, Reliable	N/A
al LAN to tal WAN to	VAN flow LAN flow	s displayed: 10 s displayed: 10	out of 10 out of 10																

**Application statistics** Navigate to **Monitoring > Statistics**. Under **Application Statistics** section, the **Application** column lists the application details.

#### Troubleshooting

After enabling application classification, you can view the reports under the **Monitoring** section and ensure that they show application details. For more information, see Viewing Application Classification.

If there is any unexpected behavior, collect the STS diagnostics bundle while the issue is being observed, and share it with the Citrix Support team.

The STS bundle can be created and downloaded using **Configuration > System Maintenance > Diagnostics > Diagnostic Information**.

# QoS fairness (RED)

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 the 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.

For information on how to use and enable RED, see How to use RED.

# **MPLS** queues

This feature simplifies creating SD-WAN configurations when adding a Multiprotocol Layer Switching (MPLS) WAN Link. Previously, each MPLS queue required one WAN Link to be created. Each WAN Link required a unique Virtual IP Address (VIP) to create the WAN Link and a unique Differentiated Services Code Point (DSCP) tag corresponding to the provider's queuing scheme. After defining a WAN Link for each MPLS queue, the Intranet Service to map to a specific queue is defined.

Currently, a new MPLS specific WAN Link definition (that is, Access Type) is available. When a new Private MPLS Access Type is selected, you can define the MPLS queues associated with the WAN Link. This allows a single VIP with multiple DSCP tags that correspond to the provider's queuing implementation for the MPLS WAN Link. This maps the Intranet Service to multiple MPLS Queues on a single MPLS WAN Link. For information on how to configure MPLS using Citrix SD-WAN Orchestrator service, see MPLS queues.

## Note

If you have existing MPLS configurations and would like to implement the Private MPLS Access Type, contact Citrix Support for assistance.

# Assign autopath group to virtual path-WAN Link

The Autopath Group defined is the same for the MCN and Client appliance. This allows the system to build the Paths automatically. At the MCN site, you can also expand the WAN Link associated with the virtual path.

# View permitted rate and congestion for WAN links

The SD-WAN web interface now allows you to view the permitted rate for WAN Links and WAN Link Usages and whether a WAN Link, Path, or Virtual Path is in congested state. In the previous releases, this information was only available in SD-WAN log files and through the CLI. These options are now available in the web interface to help with troubleshooting.

**View permitted rate** Permitted Rate is the amount of bandwidth that a particular WAN Link, Virtual Path Service, Intranet Service, or Internet Service is permitted to use at a given point in time. The permitted rate for a WAN Link is static, and is defined explicitly in the SD-WAN configuration. The permitted rate for a Virtual Path Service, Intranet Service, or Internet Service will fluctuate over time, in response to congestion, user demand, and Fair Shares, but will always be greater than or equal to the Minimum Reserved Bandwidth for the Service.

#### **Monitor WAN link**

Go to **Monitor** > **Statistics**, and select **WAN Link** from the **Show** drop-down list.

Monitoring > Statisti	G									
Statistics										
Show: WAN Link	👻 🗹 Enable Auto	Refresh 5 🗸 secor	nds Stop 🗹 Show la	test data. Processing.						
WAN Link Statistic	5									
Filter:	in Any column	✓ Apply								
Show 100 🗸 entries	Showing 1 to 6 of 6 entries					First Previous 1 Next Last				
WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	e MAC	Last ARP Reply Age (ms)				
Client-1-WL-1	N/A	172.186.10.75	N/A	N/A	N/A	N/A				
Client-1-WL-2	N/A	172.186.20.75	N/A	N/A	N/A					
Client-2-WL-1	N/A	172.186.70.50	N/A	N/A	N/A	N/A				
Client-2-WL-2	N/A	172.186.80.50	N/A	N/A	N/A					
DC-WL-1	DC-WL-1-AI-1	172.186.30.85	N/A	DISABLED	N/A	N/A				
DC-WL-2	DC-WL-2-AI-1	172.186.40.85	N/A	DISABLED	N/A	N/A				
Showing 1 to 6 of 6 entries						First Previous 1 Next Last				
Virtual Path Service Data	Rates									
Filter:	in Any column		✓ Apply							
Show 100 🗸 entries	Showing 1 to 4 of 4 entries					First Previous 1 Next Last				
Name <sup>▲</sup> Direction	Virtual Path Service Packets	Virtual Path Delt Service kB	a Virtual Path Service E Packets	elta Virtual Path Service kB	Virtual Path Service kbps	IP,TCP,UDP Header Compression Bytes Saved				
DC-WL-1 Recv	2618687 1	95069.42 289	26	16	37.81	0				

Go to **Monitor > Statistics**, and select **WAN Link Usage** from the **Show** drop-down list.

Statistica									
Show WAN LIN	t Unage 🔍 🖬 🖯	uble Auto Refrech	5	nds Step	Show latest da	a homeng.			
WAN Link U	hage Statistics								
Local WAN Links									
Elber	in Any colu	men v Appl	V						
Show 100 🛥 e	ntries Showing 1 to 6 of 1	Eentries						First Previo	ut 1 Net Lat
WAN Link	* Direction	Packets	Del	ta Pacheta	Delta KB	Klaps	Pere	itted Kips	Congestion
0C-W0-1	Send	2551632	208		17.49	28.34	100000		N/A
DC-WL-1	Recy	2630429	240		21.87	35.10	98000		NQ
41	Send	2008231	345		20.84	38.77	50000		N/A
41	face	110164	200		18.28	29.74	49000		NC
*	Berry	128796	321		19.55	32.21	49000		NO
Desire 1 to 6 of	firettini							Det Desi	
								(111) (111)	
Usages and Perm	itted Rates								
l den	- Any colu	ne v Arel	v.						
Date 100 w m	etties Should be 14 of	Mantries						First Presid	an D. Bart Carl
WANTER A	Service	Direction	Packets	Packets KB	Delta Packet	Data Ki	thes	Paralitical King	a Consection
0C/WL-1	DC-Clert-1	face	1673096	124889-42	116	10.8	16.00	24475.95	NO
DC-WL-1	DC-Client-2	Recy	958409	71427.76	138	12.12	19.07	34490	NO
0C-WL-1	DC-Olent-1	Send	1625818	108311624	134	10.34	1627	24090	NA
0C/W0-1	DC-Client-2	Send	\$90096	64771056	182	9.47	54.9	34990	N/A
DC-WL-1	Internet-Intranet	Send	0	0	0	0	0	50020	N/A
DC-WU-1	Internet-Intranet	Recr	208	\$5.25	0	0	0	49020	74/A
41	DC-Clent-1	Recy	1587987	9671621	208	11.12	17.91	34510	NO
41	DC-Client-2	Recr	631673	\$2305.57	105	7.4	11.64	34490	NO
41	DC-Clert-1	Send	1514280	\$7300168	210	10.81	21.26	25010	N/A
41	DC-Clero-2	Send	647465	\$7391606	109	7.55	11.00	34990	74/4
¢	DC-Clamb-1	Recy	91058	6260.85	237	15.85	34.94	34510	NO
42	DC-Cleve-2	Recy	40379	2232.83	104	5.56	8.75	34490	NO
42	DC-Clare-1	Send	81296	4710784	258	11.12	1731	25010	1/4
47	DC-Cleve-2	Send	40153	2271700	105	5.81	6.63	24990	N/A
Showing 1 to 14 d	/ Mientries							First Previo	us 1 Next Last
Remote WHN Lin	ks								
Fiber	in Any colu	Analy Analy							
Show 100 w e	ntries Showing 1 to 6 of 1	Letties						First Previo	us 1 Net Lat
	MAN Link			Service		Direction		Ca	operation
Ciem-1-86-1		00	-Diero-1		Recy			ND	
Ciere 2-01-1		00	Clert 2		Recv			ND	
ql .		00	-Diero 1		Recy			ND	
94		00	-Clere 1		Recv			ND	
ø		00	Olere-2		Recy			NO	
4		00	-Oiere-2		Recv			ND	
Drawing 1 to 6 of	6 eroies							First Previo	us 1 Net Lat

#### **Monitor MPLS queues**

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

#### Citrix SD-WAN 11.5

Show: MPLS Queues V D Enable Auto Refresh 5 v seconds Stop D Show latest data.										
MPLS Queue Statistics										
Filter:	in Any column	<ul> <li>Appl</li> </ul>	v							
how 100 v entries Showing 1 to 4 of 4 entries Processing										
Private MPLS	MPLS Queue	Access Inte	erface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)		
EE-Branch1-WL-2	SAMPLE-Queue1	EE-Branch1-WL-2	-Al-1 17	2.184.19.19	N/A	DISABLED	N/A	N/A		
EE-Branch1-WL-2	SAMPLE-Queue2	EE-Branch1-WL-2	-Al-1 17	2.184.19.19	N/A	DISABLED	N/A	N/A		
VPX-DC-WL-2	DC-Queuer	N/A	17	2.184.3.19	172.184.3.19	N/A	N/A	N/A		
VPX-DC-WL-2	DC-Queue2	N/A	17	2.184.3.19	172.184.3.19	N/A	N/A	N/A		
Showing 1 to 4 of 4 entries							First	t Previous 1 Next Last		
Virtual Path Service Data	Rates									
Filter:	in Any column		•	Apply						
Show 100 • entries	Showing 1 to 4 of 4 entries						First	t Previous 1 Next Last		
Name A Direc	tion Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Delta Virtual P Service kB	ath Virtual Path Service kbps	Mismatched DSCP Packets	Mismatchee DSCP kB	d IP,TCP,UDP Header Compression Bytes Saved		
SAMPLE-Queue1 Rec	v 14279	1177.77 2	251	20.72	33.15	5932	407.36	0		
SAMPLE-Queue1 Sen	d 13400	919.09 2	217	14.47	23.15	N/A	N/A	0		
SAMPLE-Queue2 Rec	v 12806	705.61 2	216	11.84	18.95	5803	250.8	0		
SAMPLE-Queue2 Sen	d 13953	915.39 2	241	16.73	26.77	N/A	N/A	0		
Showing 1 to 4 of 4 entries							First	t Previous 1 Next Last		

#### **Troubleshooting MPLS queues**

To check the status of MPLS queues, navigate to **Monitor > Statistics** and select **Paths (summary)** from the **Show** drop-down list. In the following example, the path from MPLS queue "q1"to "q3"is in DEAD state and shown in red. The path from MPLS queue "q1"to "q5"is in GOOD state and shown in green.

Statistics										
Show:	Paths (Summary)	✓ 🗹 Enable	e Auto Refresh	5 🖌 seconds Stop	Show latest data. Processir	ng				
Path	Path Statistics Summary									
Filter:		in Any column	•	Apply					Show 1	00 🗸 entries
Num <sup>▲</sup>	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	DC-WL-1	Client-1-WL-1	GOOD	GOOD	Static	5	2	0.00	15.30	NO
2	q1	q3	DEAD	GOOD	Static	9999	0	0.00	12.53	UNKNOWN
3	q1	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
4	q2	q3	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
5	q2	q4	DEAD	GOOD	Static	9999	0	0.00	8.92	UNKNOWN
6	Client-1-WL-1	DC-WL-1	GOOD	GOOD	Static	4	2	0.00	19.96	NO
7	q3	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
8	q3	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
9	q4	q1	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
10	q4	q2	DEAD	GOOD	Static	9999	0	0.00	0.00	UNKNOWN
11	DC-WL-1	Client-2-WL-1	GOOD	GOOD	Static	2	2	0.00	15.12	NO
12	q1	q5	GOOD	GOOD	Static	2	2	0.00	11.53	NO
13	q2	q6	GOOD	GOOD	Static	2	2	0.00	8.51	NO
14	Client-2-WL-1	DC-WL-1	GOOD	GOOD	Static	2	2	0.00	20.09	NO
15	q5	q1	GOOD	GOOD	Static	2	2	0.00	11.69	NO
16	qб	q2	GOOD	GOOD	Static	2	2	0.00	8.82	NO

For detailed information on paths, select **Paths (Detailed)** from the **Show** drop-down list. The information on paths such as reason for the state, duration, source port, destination port, MTU are available

In the following example, the path from MPLS queue "q1"to "q3"is in DEAD state and the reason is PEER. The path from MPLS queue "q3"to "q1"is dead and the reason is SILENCE. The following table provides the list if available reasons and its descriptions.

Reason	Description
GATEWAY	The path is DEAD as the appliance cannot reach or detect the gateway
SILENCE	The path is BAD or DEAD because the appliance has not received packets from the peer site
LOSS	The path is BAD due to packet loss
PEER	The peer site is reporting the path is BAD

Show:	Show: Paths (Detailed) V Schable Auto Refresh 5 V seconds Stop Show latest data, Processing																
Pat	Path Statistics Advanced																
Filter:		in Any co	olumn	~	Apply												
Show	100 🗸 entries	Showing 1 to 16	of 16 entries										First	Previe	ous 1	Nex	t Last
Num	From Link	To Link	Congestion	Path State	Reason	Duration (S)	Virtual Path Service State	Src Port	Dst Port	MTU	BOWT	Jitter (mS)	Packets Received	000	Loss %	kbps	Virtual Path Service Type
1	DC-WL-1	Client-1-WL-1	NO	GOOD	N/A	386	GOOD	4980	4980	1488	5	2	116	0	0.00	13.79	Static
2	q1	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	108	0	0.00	12.75	Static
3	q1	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
4	q2	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
5	q2	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
6	Client-1-WL-1	DC-WL-1	NO	GOOD	N/A	21325	GOOD	4980	4980	N/A	4	2	126	0	0.00	17.45	Static
7	q3	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
8	q3	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
9	q4	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
10	q4	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
11	DC-WL-1	Client-2-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	130	0	0.00	14.41	Static
12	q1	q5	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	111	0	0.00	11.69	Static
13	q2	q6	NO	GOOD	N/A	234	GOOD	4980	4980	1488	2	2	107	0	0.00	8.72	Static
14	Client-2-WL-1	DC-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	142	0	0.00	19.40	Static
15	q5	q1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	110	0	0.00	11.27	Static
16	q6	q2	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	107	0	0.00	8.50	Static

To check the access interface and IP address associated with the MPLS queues, select **Access Interfaces** from the **Show** drop-down list.

Show: Acc	ess Interfaces	🖌 🔽 Er	nable Auto Re	fresh 5 🗸 seco	onds Stop	Show la	itest data.	Processing				
Access	Interface Statis	stics										
Filter:		in Any colur	mn	✓ Apply								
Show 100	✓ entries Sho	wing 1 to 3 of 3	entries							First	Previous 1	Next Last
WAN Li	nk 🔺 Ac	cess Interface		IP Address	Proxy Add	ress	Proxy /	ARP State	MAC	la	ast ARP Reply Ag	e (ms)
DC-WL-1	DC-WL-	1-AI-1	172.	186.30.85	N/A		N/A		N/A	N/A		
q1	DC-WL-	2-AI-1	172.	186.40.85	N/A		N/A		N/A	N/A		
q2	DC-WL-	2-AI-1	172.	186.40.85	N/A		N/A		N/A	N/A		
Showing 1 to	3 of 3 entries									First	Previous 1	Next Last
Virtual Path	Service Data Rat	es:										
Filter:		in Any colur	mn		✓ App	ply						
Show 100	✓ entries Sho	wing 1 to 12 of	12 entries							First	Previous 1	Next Last
WAN Link	Access Interface	Service Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Vir Service	tual Path Packets	Delta Virtual Pa Service kB	th Virt Serv	ual Path rice kbps	IP,TCP,UD Compression	P Header Bytes Saved
DC-WL-1	DC-WL-1-AI-1	DC-Client-2	Recv	953815	71018.84	147		13.04	21.11		0	
DC-WL-1	DC-WL-1-AI-1	DC-Client-1	Recv	1670099	124524.23	112		10.56	17.1		0	
DC-WL-1	DC-WL-1-AI-1	DC-Client-2	Send	925756	62940.27	137		10.22	16.55	5	0	
DC-WL-1	DC-WL-1-AI-1	DC-Client-1	Send	1619424	105451.88	141		11.16	18.07	,	0	
q1	DC-WL-2-AI-1	DC-Client-1	Recv	1530107	96340.46	202		10.82	17.52	2	0	
q1	DC-WL-2-AI-1	DC-Client-2	Recv	828314	52130.2	103		7.21	11.68	1	0	
q1	DC-WL-2-AI-1	DC-Client-1	Send	1507265	94613.25	205		13.25	21.46	;	0	
a1	DC-WL-2-AI-1	DC-Client-2	Send	843865	55794.07	104		7.3	11.81		0	

You can download the log files for further troubleshooting. Navigate to **Configuration > Logging/-**

Monitoring and select SDWAN\_paths.log or SDWAN\_common.log from the Log Options tab.

Dashboard Monitoring	Configuration
- Appliance Settings	Configuration > Appliance Settings > Logging/Monitoring
Administrator Interface	
Logging/Monitoring	Log Options Alert Options Alarm Options Syslog Server HTTP Server Application
- Network Adapters Net Flow - App Flow/IPFIX - SNMP - NITRO API - Licensing - Fallback Configuration	View Log File         Only the most recent 10000 entries will be shown and filtered. To view the full log, download and open it locally.         Filename:       SDWAN_paths.log          Filter (Optional):
+ Virtual WAN	View Log
+ System Maintenance	
	Download Log File
	Filename: \$35mount_overlay.log Download Log

# Reporting

September 22, 2022

#### **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.

Quality	Range
Good	8–10
Fair	4–8
Poor	0–4

**Application QoE** score can be used to measure quality of applications and identify problematic trends.

You can define the quality thresholds for real-time and interactive appliances using QoE profiles, and map these profiles to applications or applications objects.

## Note

To monitor Application QoE, it is essential to enable Deep Packet Inspection. For more information, see Application classification.

## **Real-time application QoE**

The Application QoE calculation for real-time applications uses a Citrix innovative technique, which is derived from MOS score.

The default threshold values are:

- Latency threshold: 160 ms
- Jitter Threshold: 30 ms
- Packet loss threshold: 2%

A flow of a real-time application that meets the thresholds for latency, loss, and jitter is considered to be of good quality.

QoE for Real-time applications is determined from the percentage of flows that meet the threshold divided by the total number of flow samples.

QoE for Real-time = (No of flow samples that meet the threshold / Total no of flow samples) \* 100

It is represented as QoE score ranging from 0 to 10.

You can create QoE profiles with custom threshold values and apply to applications or application objects.

Note

The QoE value can be zero if the network conditions are outside of the configured thresholds for real-time traffic.

## Interactive application QoE

The Application QoE for interactive applications uses a Citrix innovative technique based on packet loss and burst rate thresholds.

Interactive applications are sensitive to packet loss and throughput. Therefore, we measure the packet loss percentage, and the burst rate of ingress and egress traffic in a flow.

The configurable thresholds are:

- Packet loss percentage.
- Percentage of expected egress burst rate in comparison to the ingress burst rate.

The default threshold values are:

- Packet loss threshold: 1%
- Burst rate: 60%

A flow is of good quality if the following conditions are met:

- The percentage loss for a flow is less that the configured threshold.
- The egress burst rate is at least the configured percentage of ingress burst rate.

## **Configuring application QoE**

Map application or application objects to default or custom QoE profiles.

You can create custom QoE profiles for real-time and interactive traffic and map up to 10 applications or application objects with QoE profiles.

To create custom QoE profiles through Citrix SD-WAN Orchestrator service, see Application QoE profiles.

# HDX QoE

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

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

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

Default configuration for HDX traffic enables SD-WAN to retransmit packets, thus improves the QoE index value that was lost due to packet loss in the network.

In the HDX dashboard on Citrix SD-WAN Orchestrator, you can view a graphical representation of the overall quality of HDX applications. The HDX applications are classified into the following three quality categories:

Quality	QoE Range
Good	80–100
Fair	50-80
Poor	0–50

A list of the bottom five sites with the least QoE is also displayed in the HDX 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 on how to configure HDX QoE using Citrix SD-WAN Orchestrator service, see HDX dashboard and reports.

Note

- Do not expect the WAN link latency, jitter, and packet drop would always match application latency, jitter, and packet drop. WAN Link loss correlates to the actual WAN packet loss, while application loss is after retransmit, which is lower than WAN link loss.
- WAN Link latency displayed in the GUI is BOWT (Best One Way Time). It is the best metrics of the link as a means to gauge the health of the link. The application QoE tracks and calculates the total and average latency of all the packets for that application. This often does not match the link BOWT.
- When an MSI session starts, during ICA handshake, the session might be temporarily counted as 4 SSI instead of 1 MSI. After the handshake is complete, it will converge to 1 MSI. If the conversion happens before the SQL table is updated, it might show up in ICA\_Summary for that minute.
- On session reconnect, since initial protocol information is not exchanged, SD-WAN is not able to identify MSI, hence each connection is counted as SSI information.
- For UDP connections, after the connection is closed, it can take up to 5 minutes for the connection to show as closed and updated in ICA\_Summary. For TCP connections, after the connection is closed, it can take up to 2 minutes to show as closed in ICA\_Summary.
- *QoE of TCP sessions and UDP sessions might not be the same on the same path due to the inherent different between TCP and UDP.*
- If one user launches two virtual desktops, the number of users is countered as two.

# **Multiple Net Flow Collectors**

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 Edition appliances.

For information on how to configure Net Flow Hosts using Citrix SD-WAN Orchestrator service, see Netflow host settings.

#### **NetFlow Export**

Net Flow data is exported from the SD-WAN device management port. 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). For more information, see SNMP.

NetFlow Realtime	_ <b>□</b> ×
File Edit Tools Help	
Start Flow Capture Setting up NetFlow	
Select an interface to analyze:	<i>₩</i> X =
Interface 🔯 Traffic In	ic Out Flow Type
<b>a</b> 172.16.10.12	
Interface 3 0 bps	0 bps NetFlow
Interface 5 0 bps	0 bps NetFlow
172.16.10.30	
Interface 3 0 bps	0 bps NetFlow
Interface 5 0 bps	0 bps NetFlow
Capture file:	
C:\Users\citrixservices\Documents\Toolset\WetFlowCapture\capture1.sncf	i i i i i i i i i i i i i i i i i i i
Listen on port: 2055 🗘 Apply	solarwinds
(Default port: 2055)	

#### Citrix SD-WAN 11.5



#### **NetFlow Limitations**

- With Netflow enabled on SD-WAN Standard Edition appliances, Virtual Path data is streamed to the designated Netflow collectors. One limitation with this is that one cannot differentiate which physical WAN link is being used by SD-WAN, as the solution reports aggregated Virtual Path information (A Virtual Path may comprise of multiple distinct WAN Paths), there is no way to filter the Netflow records for the distinct WAN paths.
- TCP control Bits report as N/A which indicates SD-WAN does not follow the internet standard for Netflow exports based on RFC 7011 which has element ID 6 for tcpControlBits (IANA). Without TCP Flags, calculating round trip time (RTT), latency, jitter, and other performance metrics in the flow data is not possible. From the security side, without TCP flags, the Net Flow collector cannot determine if there are FIN, ACK/RST, or SYN scans occurring.

#### **Route statistics**

To view route statistics of your SD-WAN appliances, in the SD-WAN GUI navigate to **Monitoring** > **Statistics** > **Routes**.

#### Citrix SD-WAN 11.5

Dashboard Monit	Dathboard Moniforing Configuration														
Statistics	Monitoring > Statistics														
Flows															
Routing Protocols	Statistics														
Firewall	Show: Routes	Rodes • 🔲 Enable Auto Rettech 5 • seconds Rettech 22 Cour Counters on Retech Parge dynamic routes													
IKE/IPsec															
IGMP	Route Statistics	Route Statistics													
Performance Reports	Maximum allowed routes: 64000	ximum allowed routes 64000													
Qos Reports															
Usage Reports	Routes for routing domain : Default	_RoutingDomain													
Availability Reports	Filter: in Any	r column 🔹 🔺	pply												
Appliance Reports	Show 100 • entries Showing 1	to 10 of 10 entries												First Previous	1 Next Last
DHCP Server/Relay	Details <sup>4</sup> Num Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Туре	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
VRRP	<ul> <li>0 172.186.30.0/24</li> </ul>	*	Local	Default_LAN_Zone	YES	*	DC	Static			5	55365	YES	N/A	N/A
PPPoE	1 172.186.40.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-		5	0	YES	N/A	N/A
DNS	2 172.186.50.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	+	5	11	YES	N/A	N/A
	3 172.186.10.0/24	*	DC-Client-1	Default_LAN_Zone	YES	*	Client-1	Dynamic	Virtual WAN	YES	10	27912	YES	N/A	N/A
	Site Path:	Client-1													
	Optimal Route:	NO													
	Summarized / Summary	Route: NO/NO													
	4 172.186.20.0/24	*	DC-Client-1	Default_LAN_Zone	YES	*	Client-1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
	<ul> <li>5 172.186.10.0/24</li> </ul>	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-		15	0	YES	N/A	N/A
	6 172.186.20.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static			15	0	YES	N/A	N/A
	₱ 7 0.0.0.0/0	*	Internet	Internet_Zone	YES	*	DC	Static	-	-	5	20	YES	N/A	N/A
	8 0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-		65535	238	YES	N/A	N/A
	9 0.0.0/0	*	Discard	Any	YES	*	*	Static	•		65535	0	YES	N/A	N/A
	Showing 1 to 10 of 10 entries													First Previous	1 Next Last

You can view the following parameters:

- Network Address: The Network address and subnet mask of the route.
- **Details**: Click + to display the following information.
  - Site Path: Site Path is a source of truth metric for the received prefix. It is used in situations
    where WAN to WAN forwarding is enabled on multiple devices and in mesh deployment.
    Multiple such prefixes are received and the administrators are able to judge the prefix attributes by viewing the site path.

For example, consider a simple topology of Branch1, Branch2, and MCN along with a Geo MCN. Branch1 has a prefix 172.16.1.0/24 and has to get to Branch2. Geo MCN and MCN have WAN to WAN forwarding enabled.

The prefix 172.16.1.0/24 can get to Branch2 via Branch1-MCN-Branch2, Branch1-Geo-Branch2, and Branch1-MCN-Geo-Branch2. For each of these distinct prefixes the routing table is updated with their site path metric. The site path metric indicates the origin of the route prefix and the cost involved to get to Branch2.

- **Optimal Route**: Optimal route indicates whether the route is the optimal route to reach that subnet compared to all other routes. This optimal route is exported to other sites.
- **Summarized/ Summary Route**: A summary route is a route configured explicitly by an administrator to summarize multiple prefixes that fall in the supernet. Summarized routes are the prefixes that fall under the summary route.

For example, assume that we have a summary route 172.16.0.0/16. This is a summary route only and not a summarized route. A summary route has Summary 'YES' and Summarized 'NO'. If there are few other subnets like 172.16.1.0/24, 172.16.2.0/24 and

172.16.3.0/24, these three routes fall under the summary route or the supernet and hence are called summarized routes. A summarized route has Summarized 'YES' and Summary 'NO'.

- Gateway IP Address: The IP address of the gateway/route used to reach this route.
- Service: The type of Citrix SD-WAN service.
- Firewall Zone: The firewall zone used by the route.
- **Reachable**: Is the route reachable or not.
- Site IP Address: The IP address of the site.
- Site: The name of the site.
- **Type**: Type of a route depends upon the source of the route learning. The routes on the LAN side and routes entered manually during configuration are Static routes. Routes learned from the SD-WAN or dynamic routing peers are Dynamic routes.
- Protocol: The protocol of the prefixes.
  - Local: Local virtual IPs of the appliance.
  - Virtual WAN: Prefixes learned from peer SD-WAN appliances.
  - **OSPF**: Prefixes learned from OSPF dynamic routing peer.
  - **BGP**: Prefixes learned from BGP dynamic routing peer.
- **Neighbor Direct**: Indicates whether the subnet is connected to the branch from which the route came to the appliance.
- Cost: The cost used to determine the best path to a destination network.
- Hit Count: The number of times a route was hit to forward a packet to that subnet.
- **Eligible**: Indicates that the route is eligible and is used for forwarding or routing the packets to the prefix hit during traffic processing.
- Eligibility Type: The following two eligibility types are available.
  - **Gateway eligibility**: Determines if the gateway is reachable or not.
  - **Path eligibility**: Determines if the path is DEAD or NOT DEAD.
- **Eligibility Value**: The value selected for the gateway or the path in the configuration while the route is created in the system. For instance a route can be called eligible based on a path MCN-WL-1->BR1-WL-2. So the eligibility value for this route in the routes section is the value MCN-WL-1->BR1-WL-2.

# Routing

#### September 22, 2022

## Note

From SD-WAN 11.5 release onwards, all the routing configurations are supported only through Citrix SD-WAN Orchestrator service. For information regarding Citrix SD-WAN Orchestrator service routing configurations, see **Routing**.

# **Dynamic Routing**

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

# **Route Filtering**

For networks with Route Learning enabled, Citrix SD-WAN provides more control over which SD-WAN routes are advertised to routing neighbors rather and which routes are received from routing neighbors, rather than advertising and accepting all or no routes.

- Export Filters are used to include or exclude routes for advertisement using OSPF and BGP protocols based on specific match criteria.
- Import Filters are used to accept or not accept routes which are received using OSPF and BGP neighbors based on specific match criteria.

Route filtering is implemented on LAN routes and Virtual Path routes in an SD-WAN network (Data Center/Branch) and is advertised to a non-SD-WAN network through using BGP and OSPF.

# **Route Summarization**

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

#### VRRP

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

Citrix SD-WAN (release version 10.0 and later) supports VRRP version 2 and version 3 to inter-operate with any third party routers. The SD-WAN appliance acts as a master router and direct the traffic to use the Virtual Path Service between sites. You can configure the SD-WAN appliance as the VRRP master by configuring the Virtual Interface IP as the VRRP IP and by manually setting the priority to a higher value than the peer routers. You can configure the advertisement interval and the preempt option.

Using CLI to Access Routing Functionality

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

```
dynamic_routing?
```

```
,
```

# **SD-WAN Overlay Routing**

#### August 24, 2022

Citrix SD-WAN provides resilient and robust connectivity between remote sites, data centers, and cloud networks. The SD-WAN solution can accomplish this by establishing tunnels between SD-WAN appliances in the network enabling connectivity between sites by applying route tables that overlay the existing underlay network. SD-WAN route tables can fully replace or coexist with the existing routing infrastructure.

Citrix SD-WAN appliances measure the paths available unidirectionally in terms of availability, loss, latency, jitter and congestion characteristics, and select the best path on a per-packet basis. This means that the path chosen from Site A to Site B, need not necessarily be the path chosen from Site B to Site A. The best path at a given time is selected independently in each direction. Citrix SD-WAN offers packet-based path selection for rapid adaptation to any network changes. SD-WAN appliances can detect path outages after just two or three missing packets, allowing seamless subsecond failover of application traffic to the next-best WAN path. SD-WAN appliances recalculate every WAN link status in about 50 ms. The following article provides detailed routing configuration within the Citrix SD-WAN network.

# **Citrix SD-WAN Route Table**

The SD-WAN allows static route entries for specific sites, and route entries learned from the underlay network through supported routing protocols; such as OSPF, eBGP, and iBGP. Routes are not only defined by their next hop but by their service type. This determines how the route is forwarded. The following are the main service types in use:

• Local Service: Denotes any route or subnet local to the SD-WAN appliance. This includes the Virtual Interface subnets (automatically creates local routes), and any local route defined in the route table (with a local next hop). The route is advertised to other SD-WAN appliances that have a Virtual Path to this local site where this route is configured when trusted as a partner.

#### Note

Be cautious when adding default routes, and summary routes as local routes as these can result in virtual path routes at other sites. Always check the route tables to make sure the correct routing is in effect.

- Virtual Path –Denotes any local route learned from a remote SD-WAN site that is reachable down the virtual paths. These routes are normally automatic, however a virtual path route can be added manually at a site. Any traffic for this route is forwarded to the defined Virtual Path for this destination route (subnet).
- Intranet –Denotes routes that are reachable through a private WAN link (MPLS, P2P, VPN, and so on). For example, a remote branch that is on the MPLS network but does not have an SD-WAN appliance. It is assumed that these routes must be forwarded to a certain WAN router. Intranet Service is not enabled by default. Any traffic matching this route (subnet) is classified as intranet for this appliance for delivery to a site that does not have an SD-WAN solution.

#### Note

Notice that when adding an Intranet route there is no next hop, but rather a forward to an Intranet Service. The Service is associated with a given WAN link.

• **Internet** –This is similar to Intranet but is used to define traffic flowing to public Internet WAN links rather than private WAN links. One unique difference is that the Internet service can be associated with multiple WAN links and set to load balance (per flow) or be active/backup. A default Internet route gets created when internet service is enabled (it is off by default). Any traffic matching this route (subnet) is classified as Internet for this appliance for delivery to public internet resources.

Note

Internet Service routes can be advertised to the other SD-WAN appliances or prevented from being exported depending on whether you are backhauling Internet access over the Virtual Paths.

• **Passthrough** –This service acts as a last resort or override service when an appliance is in-line mode. If a destination IP address fails to match with any other route, then the SD-WAN appliance simply forwards it onto the WAN link next hop. A default route: 0.0.0.0/0 cost of 16 pass-through route is created automatically. Passthrough does not work when the SD-WAN appliance is deployed out of path or in Edge/Gateway mode. Any traffic matching this route (subnet) is classified as passthrough for this appliance. It is recommended that passthrough traffic is limited as much as possible.

#### Note

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

• **Discard** - This is not a service but a last resort route that drops the packets if it matches. Normally this does not occur expect when the SD-WAN appliance is deployed out of the path. You must have an Intranet service or local route as a catch all route, otherwise the traffic is discarded as there is no passthrough service (even though a passthrough default route will be present).

The route table for the local client node can be monitored on the **Monitoring** > **Statistics** page with Routes selected for the **Show** drop-down list.

	Monito	nng > Statistics														
a Dratasals	Stati	stics														
rotocols	Show D	outes	T Enable	Auto Refresh 5 Too	onds Refrech	1 Clear Count	ers on Refresh	Purge dynamic route	25							
	SHOW R	~~		sec	menesu 6	, clear count	cio on iverresti	. orge ognamic route								
[	Rout	e Statistics														
	Maximum	allowed routes: 640	000													
orts																
	Routes fo	r routing domain	: Default_RoutingD	omain												
	Filter:		in Any column	Apply												
																_
	Show 10	0 • entries Sh	Gateway IP	entries			Cito IP				Naighbor			First	Previous 1	Ne
_	Num	Network Addr	Address	Service	Firewall Zone	Reachable	Address	Site	Туре	Protocol	Direct	Cost	Hit Count	Eligible	Туре	-
	0	172.120.21.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static		•	4	0	YES	N/A	N//
	1	172.120.24.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/.
	2	224 225 1 1/22		Passthrough	Any	YES		MCNI	Static	•		4	0	YES	N/A	N/
	4	224,225,1,2/32	*	Multicast	Any	YES	*	MCN1	Static			5	0	YES	N/A	N/
	5	224.225.1.3/32	*	Multicast	Any	YES		MCN1	Static			5	0	YES	N/A	N/
	6	172.120.21.100/32	*	Passthrough	Any	YES		*	Static			5	0	YES	N/A	N/
	7	172.120.24.64/32	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	9	0	YES	N/A	N/
	8	172.120.24.0/24	*	Local	Default_LAN_Zone	YES	•	MCN1	Static	-	-	5	3458	YES	N/A	N/
	9	182.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N,
	10	172.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	•	APAC_RCN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/
	11	172 120 21 0/24	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/
	12	182.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	•	APAC_RCN	Dynamic	Virtual WAN	TES	10	0	YES	N/A	N/
	14	192.108.255.0/24	•	MCN1-RCN01-2000	Default LAN Zone	YES		AMEA al vov01	Dynamic	Virtual WAN	TE5	10	0	VEC	N/A	N/
	15	192.172.1.0/24	*	MCN1-RCN01-2000	Default LAN Zone	YES		AMEA r1 vpx02	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N
	16	192.172.2.0/24		MCN1-RCN01-2000	Default_LAN_Zone	YES		AMEA_r1_vpx03	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N
	17	192.172.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx04	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N
	18	192.172.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	•	AMEA_r1_vpx05	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N,
	19	192.172.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_rl_vpx06	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N,
	20	192.172.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	•	AMEA_r1_vpx07	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N
	21	192.172.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx08	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N,
	22	192.172.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx13	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/
	23	192.172.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx14	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N
	24	192.172.14.0/24	*	MCN1-RCN01-2000	Default LAN Zone	VES	•	AMEA_r1_vpx15	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/
	26	192 172 16 0/24	*	MCN1-RCN01-2000	Default LAN Zone	YES		AMEA r1 vpx17	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N
	27	192.172.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES		AMEA_r1_vpx18	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N
	28	192.172.18.0/24		MCN1-RCN01-2000	Default_LAN_Zone	YES		AMEA_r1_vpx19	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N
	29	192.172.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx20	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N
	30	192.120.10.0/24		MCN1-APAC_RCN	Default_LAN_Zone	YES	1.00	APAC_RCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A	N
	31	172.108.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx01	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N
	32	172.108.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	•	AMEA_r1_vpx02	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N
	33	172.108.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx03	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N,
	34	172.108.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx04	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N
	36	172.108.5.0/24	*	MCN1-RCN01-2000	Default LAN Zone	YES		AMEA_r1_vpx05	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N
	37	172.108.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx07	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N
	38	172.108.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	•	AMEA_r1_vpx08	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N
	39	172.108.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx13	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N
	40	172.108.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	•	AMEA_r1_vpx14	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N
	41	172.108.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx15	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N
	42	172.108.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx16	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N,
	43	172.108.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_rl_vpx17	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N
	44	172.108.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx18	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N,
	45	172.108.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx19	Dynamic Dynamic	Virtual WAN	NO	15	0	YES	N/A	N,
	47	10 101 0 0/22	*	MCN1-RR1	Any	YES	*	BR1	Static	-		10	0	YPS	N/A	N
	48	10.101.0.0/22	*	MCN1-BR1	Default_LAN Zone	YES		BR1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N
	49	172.105.96.0/20	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N
	50	0.0.0.0/0		Internet	Internet_Zone	YES		MCN1	Static			5	401109	YES	N/A	N
- 1	51	0.0.0.0/0	*	MCN1-BR1	Default_LAN_Zone	YES		BR1	Dynamic	Virtual WAN	YES	10	88	YES	N/A	N
J																
	52	0.0.0.0/0		Passthrough	Any	YES	*	*	Static	÷	÷	65535	40031844	YES	N/A	N

Each route for remote branch office subnets is advertised as a Service through the Virtual Path connecting through the MCN, with the **Site** column populated with the client node where the destination resides as a local subnet.

In the following example, with WAN-to-WAN Forwarding (Routes Export) enabled, Branch A has a

route table entry for the Branch B subnet (10.2.2.0/24) through the MCN as a next hop.



# **How Citrix SD-WAN Traffic Matches on Defined Routes**

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

- 1. Longest prefix matches
- 2. Cost
- 3. Service

Therefore a /32 route always precedes a /31 route. For two /32 routes, a cost 4 route always precedes a cost 5 route. For two /32 cost 5 routes, routes are chosen based on ordered IP host. Service order is as follows: Local, Virtual Path, Intranet, Internet, Passthrough, Discard.

As an example, consider the following two routes as follows:

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

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

## **Citrix SD-WAN Routing Packet Flow**

- LAN to WAN (Virtual Path) Traffic Route Matching:
  - 1. Incoming traffic is received by the LAN interface and is processed.
  - 2. The received frame is compared to the route table for the longest prefix match.
  - 3. If a match is found, the frame is processed by the rule engine and a flow is created in the flow database.
- WAN to LAN (Virtual Path) Traffic Route Matching:
  - 1. Virtual Path traffic is received by SD-WAN from the tunnel and is processed.
  - 2. The appliance compares the source IP address to see if the source is local.
    - If yes then WAN eligible and match IP destination to routing table/Virtual Path.
    - If no –then WAN to WAN forwarding enabled check.
  - 3. (WAN to WAN Forwarding disabled) Forward to LAN based on local routes.
  - 4. (WAN to WAN Forwarding enabled) Forward to Virtual Path based on route table.
- Non-Virtual Path Traffic:
  - 1. Incoming traffic is received on the LAN interface and is processed.
  - 2. The received frame is compared to the route table for the longest prefix match.
  - 3. If a match is found, the frame is processed by the rule engine and a flow is created in the flow database.

# **Citrix SD-WAN Routing Protocol Support**

Citrix SD-WAN release 9.1 introduced OSPF and BGP routing protocols into the configuration. Introducing routing protocols to SD-WAN enabled easier integration of SD-WAN in more complex underlay networks where routing protocols are actively in use. With the same routing protocols enabled on SD-WAN Orchestrator service, configuration of subnets denoted to make use of the SD-WAN overlay was made easier. In addition, the routing protocols enable communication between SD-WAN and non-SD-WAN sites with direct communication to existing customer edge routers using the common routing protocol. Citrix SD-WAN participating in routing protocols operating in the underlay network can be done regardless of the deployment mode of SD-WAN (Inline mode, Virtual Inline mode, or Edge/Gateway mode). Also, SD-WAN can be deployed in "learn only" mode where SD-WAN can receive routes but not advertise routes back to the underlay. This is useful when introducing the SD-WAN solution into a network where the routing infrastructure is complex or uncertain.

Important

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

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

#### Note

Be aware of environments that have IGPs across the entire infrastructure (across the WAN) as it does complicate how SD-WAN advertised routes are used. EIGRP is extensively used in the market and SD-WAN does not interoperate with that protocol.

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



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

37 @ 2017 Citrix

In this example, we examine a routing protocol use case. The preceding network has four locations; New York, Dallas, London, and San Francisco. We deploy SD-WAN appliances at three of these locations, and utilize SD-WAN to create a hybrid WAN network where MPLS and Internet WAN Links will be used to provide a Virtualized WAN. Since Dallas will not have an SD-WAN device, we must consider how to best integrate with existing route protocols to that site to ensure full connectivity between underlay and SD-WAN overlay networks.

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

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

The San Francisco site also must be noted not to have a router. SD-WAN is deployed in Edge/Gateway mode with that appliance being the default gateway for the San Francisco subnet and also participating in eBGP to the MPLS.

- With the New York Data Center, take note that the SD-WAN is deployed in Virtual Inline mode. The intent is to participate in the existing OSPF routing protocol to get traffic forwarded to the appliance as the preferred gateway.
- The London site is deployed in traditional inline mode. The upstream WAN Router (C) will still be the default gateway for the London subnet.
- The San Francisco site is a newly introduced site to this network and the SD-WAN is planned to be deployed in Edge/Gateway mode and act as the default gateway for the new San Francisco subnet.

Review some of the existing underlay route tables before implementing SD-WAN.

#### New York Core Router B:



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: <u>~</u> \$ show ip route Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - ISIS, B - BGP, > - selected route, * - FIB route
O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:09:52
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h09m
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 1d23h10m
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h01m
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
C>* 192.168.10.0/24 is directly connected, eth2
O 192.168.65.0/24 [110/20] via 172.10.10.2, 1d19h57m
C>* 192.168.65.0/24 is directly connected, eth0

For the New York WAN Router (A), OSPF learned routes and routes learned across the MPLS through eBGP are listed routes. Note the route costs. BGP is lower administrative domain and cost by default 20/1 compared to OSPF 110/10.

#### Dallas Router D:

For the Dallas WAN Router (D) all routes are learned across the MPLS.



#### Note

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

not advertised in any routing protocol.

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

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

• The San Francisco location has two local subnets **10.80.1.0/24** and **10.81.1.0/24**. We want to advertise them through eBGP so that sites like Dallas can still reach the San Francisco site over the underlay network and also sites like London and New York can still reach San Francisco over the Virtual Path overlay network. We also want to learn from eBGP reachability to all sites in case the SD-WAN Virtual Path overlay goes down and the environment must fall back to using just the MPLS. We also do not want to readvertise anything SD-WAN learns from eBGP to the SD-WAN routers. To accomplish this, the filters must be configured as follows:

Section	ection: Import Filters + Import Filters +																
+	+															?	
	Order	Source Router	Dest	ination	-	Prefix	Next Hop	Protocol	Route Tag	C	ost	AS P	ath Length	Include	Enabled	Delete	Clone
	100	*	<manual></manual>	•	eq	¢] *	*	Any	•	eq 🛊	•	eq	\$] *			茴	D
□ Export Route to Citrix Appliances     □ Eligibility Based On Gateway       Citrix SD-WAN Cost:     Service Type:       6     □ Local       •     □ Eligibility Based On Path       Path:        <\none>       \$																	
+	200	*	<manual></manual>	•	eq	¢ *	•	Any	•	eq \$	*	eq	\$ ×		<ul> <li>Image: A start of the start of</li></ul>	•	þ
	200	*	<manual> 🕴</manual>	*	eq	÷ *	•	Any	+	eq 🗍	*	eq	\$		$\checkmark$		
Apply	Rever	t															

• 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.

-		Order	Network Address	Prefix	NetSc	aler SD-WAN Cost	Service Type	Site/Service Name	Gateway IP Address	Include	Enabled	Delete	Clone
	+	100	«Manual» 1	eq 24	eq		Local	«Any»	•	2	1	1	ø
	+	200	<manual> 0.0.0.0/0</manual>	eq *	eq	1	Any	<any></any>	*		1	Û	¢
		(auto)	«Manual» 1	eq *	вq	1	Алу	<any></any>		2	1		

After the Citrix SD-WAN appliances have been deployed, we can take a refreshed look at the route tables for the BGP router at the Dallas site. We see 10.80.1.0/24 and 10.81.1.0/24 subnets are being seen correctly through eBGP from the San Francisco SD-WAN.

#### **Dallas Router D:**

vyos@VYATTA-ROUTER-D:~\$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - ISIS, B - BGP, > - selected route, * - FIB route
B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:00:01
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 4d23h38m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 4d23h38m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B 192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 3d19h07m
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0

Further, the Citrix SD-WAN route table can be viewed on the **Monitoring** > **Statistics** > **Show Routes** page.

#### San Francisco Citrix SD-WAN:

Routes for routing domain : Default_RoutingDomain															
Filter:	ilter: in Any column + Apply														
												_			
Show	100 🗘 entries Sh	owing 1 to 16 of 16 entr	ries										First Previous	1 Next Last	
Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Туре	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value	
0	10.81.1.0/24	10.80.1.20	Local	YES	•	SFO	Static	-	-	5	0	YES	N/A	N/A	
1	10.80.1.0/24	•	Local	YES	•	SFO	Static	-	-	5	0	YES	N/A	N/A	
2	192.168.10.0/24	*	Local	YES	*	SFO	Static	-	-	5	122	YES	N/A	N/A	
3	172.10.10.0/24	•	NYC-SFO	YES	•	NYC	Static	-	-	5	0	YES	N/A	N/A	
4	172.30.30.0/24	192.168.10.1	Local	YES	•	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A	
5	172.20.20.0/24	192.168.10.1	Local	YES		SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A	
6	172.10.10.0/24	192.168.10.1	Local	YES	•	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A	
7	10.100.1.0/24	192.168.10.3	Local	YES	•	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A	
8	10.90.1.0/24	192.168.10.2	Local	YES		SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A	
9	172.20.20.0/24	•	NYC-SFO	YES	•	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A	
10	10.100.1.0/24	•	NYC-SFO	YES	•	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A	
11	172.30.30.0/24	•	NYC-SFO	YES	•	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A	
12	0.0.0/0	192.168.10.1	Local	YES	•	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A	
13	0.0.0/0	•	NYC-SFO	YES	•	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A	
14	0.0.0.0/0	•	Passthrough	YES	•	•	Static	-	-	16	0	YES	N/A	N/A	
15	0.0.0/0	•	Discard	YES	•	•	Static	-	-	16	0	YES	N/A	N/A	
Showin	ig 1 to 16 of 16 entrie	s										[	First Previous	1 Next Last	

Citrix SD-WAN shows all the routes learned, including routes available through the Virtual Path overlay.

Let us consider 172.10.10.0/24, which is located in the New York Data Center. This route is being learned in two ways:

• As a Virtual Path route (Number 3), service = NYC-SFO with a cost of 5 and type static. This is

a local subnet advertised by SD-WAN appliance in New York. It is static in that it is either 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 (Number 6), with a cost of 6. This is now considered a fallback route.

Since the prefix is equal and the cost is different, SD-WAN uses the Virtual Path route unless it becomes unavailable in which case the fallback route is learned through BGP.

Now, let us consider the route 172.20.20.0/24.

- This is learned as a Virtual Path route (Number 9) but has a type of dynamic and a cost of 6. This means that the remote SD-WAN appliance learned this route through a routing protocol, in this case OSPF. By default the route cost is higher.
- SD-WAN also learns this route through BGP with the same cost, so in this case this route might be preferred over the Virtual Path route.

To ensure correct routing, we must increase the BGP route cost to make sure if we have a Virtual Path route and it is the preferred route. This can be done by adjusting the import filter route weight to be higher than the default of 6.

	Order	Source Router	Des	stination	_	Prefix	Next Hop	Protocol	Cost	Include	Enabled	Delete	Clone
Ξ	100	•	<manual></manual>	¢ .	eq	¢] *	•	Any \$	eq ‡ *			đ	¢
Ľ	Export	Route to Citrix Appl	ances				<ul> <li>Eligibility Based O</li> </ul>	n Gateway					
	NetScaler	SD-WAN Cost:		Service Type:	ŧ		Service Na	lme:	\$				
	🗆 Eligibil	ity Based On Path											
	Path:												
	<none></none>		\$										
				N.	2			,					
	(auto)	•	<manual></manual>	¢	eq	¢ *	•	Any ¢	eq ‡ *		1		
A	pply Rev	vert											

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.

Routes	outes for routing domain : Default_RoutingDomain														
Filter:	172.20.20.0/24 in	Any column 🗘	Apply												
Show	100 🗘 entries Si	howing 1 to 2 of 2 entries	s (filtered fro	m 16 total ent	ries)								First Previous	1 Next Last	
Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Туре	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value	
5	172.20.20.0/24	•	NYC-SFO	YES	•	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A	
8	172.20.20.0/24	192.168.10.1	Local	YES	•	SFO	Dynamic	BGP	-	10	0	YES	N/A	N/A	
Showin	g 1 to 2 of 2 entries	(filtered from 16 total en	tries)										First Previous	1 Next Last	

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.

Rou	tes fo	or routing doma	in : Default_RoutingDo	main											
Filte	er: 0.0	.0.0/0	in Any column	Apply											
Sho	Show 100 \$ entries Showing 1 to 4 of 4 entries (filtered from 16 total entries) First Previous 1 Next Last														
Nu	m <sup>4</sup> N	letwork Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Туре	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
1	2 0	0.0.0.0/0		NYC-SFO	YES	•	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
1	8 C	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	10	0	YES	N/A	N/A
14	4 C	0.0.0.0/0	•	Passthrough	YES	•	•	Static	-	-	16	0	YES	N/A	N/A
1	5 0	0.0.0.0/0	•	Discard	YES	•	•	Static	-	-	16	0	YES	N/A	N/A
Sho	wing 1	L to 4 of 4 entrie	es (filtered from 16 total	entries)									[	First Previous	1 Next Last

We also see a passthrough and discard route with cost 16. These are automatic routes that cannot be removed. If the device is inline, the passthrough route is used as a last resort so if a packet cannot be matched to a more specific route, SD-WAN will pass it along to the next hop of the interface group. If the SD-WAN is out of path or in edge/gateway mode, there is no passthrough service, in which case SD-WAN drops the packet using the default discard route. The Hit Count indicates the number of packets that are hitting each route, which can be valuable when troubleshooting.

Now focusing on the New York site, we want to get traffic destined for remote sites (London and San Francisco) to be directed to the SD-WAN appliance when the Virtual Path is active.

There are multiple subnets available in the New York site:

- 172.10.10.0/24 (directly connected)
- 172.20.20.0/24 (advertised via OSPF from the core router B)
- 172.30.30.0/24 (advertised via OSPF from the core router B)

We also are required to provide traffic flow to Dallas (10.100.1.0/24) through MPLS.

Lastly, we want all internet bound traffic route to the Firewall E through 172.10.10.3 as a next hop. SD-WAN learns this default route through OSPF and to advertise across the Virtual Path. The filters for the New York site are:

	Order	Source Router		Destination	Pr	refix	Next Hop	Protocol	Cost	Include	Enabled	Delete	Clone			
	100	•	<manual></manual>	192.168.65.0/24	eq °		•	Any	eq *		1	ū	¢			
	Export Route to Citrix Appliances						Eligibility Based On Gateway									
	NetScaler	SD-WAN Cost:			Service	e Type:			Service Na	me:						
	6				Local											
	🗌 Eligibil	ity Based On Path														
	Path:															
	<none></none>															
-																
	200		<manual></manual>	192.168.10.0/24	eq "		•	Any	eq *		4	Ū	Ū.			
Ξ	300		<manual></manual>		ed .			Any	ed .	1	1	Ū	Û			
	(auto)	•	<manual></manual>	*	eq *		•	Any	eq *		$\checkmark$					

The New York SD-WAN site imports all routes for the management network. This can be ignored. We can focus on filter 200.

200 * <manual> 192.168.</manual>	.10.0/24 eq ° °	Any eq *	<b>v</b>	Û	
Export Route to Citrix Appliances	_ E	ligibility Based On Gateway			
NetScaler SD-WAN Cost:	Service Type:	Service N	ame:		
6	Local				
Eligibility Based On Path					
Path:					
<none></none>					

Filter 200 is used to import 192.168.10.0/24 (our MPLS core) for reachability but not to export it to the virtual path. Select the **Include** check box and ensure that the **Export Route to Citrix Appliances** check box is cleared. All other routes are then included.

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

Ч		Order	Network Address	Prefix	NetScaler SD-WAN Cost	Service Type	Site/Service Name	Gateway IP Address	Include	Enabled	Delete	Clone
	+	100	<manual> 192.168.10.0/24</manual>	eq '	eq "	Any	<any></any>	1.00			Ē	¢
		(auto)	<manual> *</manual>	eq *	eq *	Any	<any></any>	•	1	1		

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

#### New York Router B:



We can see the subnets for San Francisco (10.80.1.0 & 10.81.1.0) and London (10.90.1.0) now being advertised via the New York SD-WAN Appliance (172.10.10.10). The route 10.100.1.0/24 is still being advertised through the underlay MPLS Router A. Let us review the New York site SD-WAN route table.

#### New York site SD-WAN Route Table:

Routes	Routes for routing domain : Default_RoutingDomain													
Filter:	in	Any column 💲	Apply											
Show	ihow 100 \$ entries Showing 1 to 11 of 11 entries 1 Next Last													
Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Туре	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.10.10.0/24		Local	YES	•	NYC	Static	-	-	5	0	YES	N/A	N/A
1	10.90.1.0/24	*	NYC-LON	YES	*	LON	Static	-	-	5	0	YES	N/A	N/A
2	10.81.1.0/24	10.80.1.20	NYC-SFO	YES	•	SFO	Static	-	-	5	0	YES	N/A	N/A
3	10.80.1.0/24	•	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
4	192.168.10.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
5	172.30.30.0/24	172.10.10.2	Local	YES	•	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	172.20.20.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	172.10.10.1	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	0.0.0/0	172.10.10.3	Local	YES	•	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	0.0.0/0	•	Passthrough	YES			Static	-	-	16	0	YES	N/A	N/A
10	0.0.0/0	•	Discard	YES	•	*	Static	-	-	16	0	YES	N/A	N/A

We can see the correct routes for both the local subnets learned via OSPF, a route to the Dallas site learned from the MPLS Router A and the remote subnets for the San Francisco and London sites. Let us look at the MPLS Router A. This router is participating in OSPF and BGP.

vyo	s@VYATTA-ROUTER-A:~\$ show ip route
Cod	les: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
	I - ISIS, B - BGP, > - selected route, * - FIB route
O>*	0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:04:12
0	10.80.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>*	10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
0	10.81.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>*	10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
0	10.90.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>*	10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 00:05:11
S>*	10.90.1.10/32 [5/0] via 192.168.10.2, eth2
B>*	10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 00:04:28
C>*	127.0.0.0/8 is directly connected, lo
0	172.10.10.0/24 [110/10] is directly connected, eth1, 00:05:24
C>*	172.10.10.0/24 is directly connected, eth1
O>*	172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
O>*	172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
В	192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 00:05:09
C>*	192.168.10.0/24 is directly connected, eth2
0	192.168.65.0/24 [110/20] via 172.10.10.2, 00:04:12
C>*	192.168.65.0/24 is directly connected, eth0

From the route table, this Router A is learning the remote subnets through BGP and OSPF with the Administrative distance and cost of the BGP route (20/5) being lower than OSPF (110/10) and hence preferred. In this example, network where there is only one core route, this might not cause concern. However, traffic arriving here would be delivered via the MPLS network rather than being sent to the SD-WAN Appliance (172.10.10.10). If we want to maintain complete routing symmetry, we would need a route map to adjust the AD/Metric cost so that there is route preference from the route coming from 172.10.10.10 rather than the route learned via eBGP.

Alternatively, a "backdoor" route can be configured to force the router to prefer the OSPF route over the BGP route. Notice the static route for the SD-WAN Virtual IP address to the London site SD-WAN appliance.

#### S>\* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2

This is necessary to ensure that the Virtual Path is rerouted back to the New York site SD-WAN appliance if the MPLS path goes down. Since there is a route for the 10.90.1.0/24 being advertised via 172.10.10.10 (New York SD-WAN). It is also recommended to create an override service rule to drop any UDP 4,980 packets at the SD-WAN appliance to prevent the Virtual Path from coming back to itself.

## **Dynamic Virtual Paths**

Dynamic Virtual Paths can be allowed between two client nodes to build on-demand virtual paths for direct communication between the two sites. The advantage of a dynamic virtual path is that traffic can flow directly from one client node to the second without having to traverse the MCN or two virtual paths, which can add latency to the traffic flow. Dynamic virtual paths are built and removed dynamically based on user-defined traffic thresholds. These thresholds are defined as either packets per second (pps) or bandwidth (kbps). This functionality enables a dynamic full mesh SD-WAN overlay topology.

Once the thresholds for dynamic virtual paths are met, the client nodes dynamically create their virtualized path to one another using all available WAN paths between the sites and make full use of it in the following manner:

- Send Bulk data if any exists and verify no loss, then
- Send Interactive data and verify no loss, then
- Send Real Time data after the Bulk and Interactive data are considered stable (no loss or acceptable levels)
- If there is no Bulk or interactive data send Real Time Data after the Dynamic Virtual Path has been stable for a period
- If the user data falls below the configured thresholds for a user defined period, the dynamic virtual path is torn down

Dynamic Virtual Paths have the concept of an Intermediate site. The intermediate site can be an MCN site or any other site in the network that has Static Virtual Path configured and connected to two or more other client nodes. Another design consideration requirement is to have WAN-to-WAN Forward-ing enabled, allowing all routes from all sites to be advertised to the client nodes where the dynamic virtual path is desired.

Multiple WAN-to-WAN Forwarding Groups are allowed in SD-WAN, enabling full control to path establishment between certain client nodes and not others.



Each SD-WAN device has its own unique route table with the following details defined for each route:

- Num –order of route of this appliance based on match process (lowest Num processed first)
- Network address subnet or host address
- Gateway if necessary
- Service what service is applied for this route
- Firewall Zone -- the firewall zone classification of the route
- Reachable Identifies if the Virtual Path state is active for this site
- Site The name of the site where the route is expected to exist
- Type –Identification of route type (Static or Dynamic)
- Neighbor Direct
- Cost cost of the specific route
- Hit Count how many times the route has been used per packet. This would be used to verify that a route is being hit correctly.
- Eligible
- Eligibility Type
#### • Eligibility Value

#### The following is an example SD-WAN site route table:

Routes	for routing domain	Default_RoutingDomain	1												
Filter:		in Any column	<ul> <li>Apply</li> </ul>												
Show 1	00 v entries SI	nowing 1 to 13 of 13 entri	25											First Previous	1 Next Last
Num <sup>A</sup>	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Туре	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.16.10.0/24	192.168.15.1	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	4	0	YES	N/A	N/A
1	192.168.100.0/24	x	Local	Default_LAN_Zone	YES	*	AWS	Static	-	-	5	0	YES	N/A	N/A
2	192.168.15.0/24		DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
3	172.16.250.0/24	•	DC-AWS	Default_LAN_Zone	YES	*	DC	Static			5	0	YES	N/A	N/A
4	172.16.150.0/24	•	DC-AWS	Default_LAN_Zone	YES	*	DC	Static			5	0	YES	N/A	N/A
5	192.168.200.0/24	*	DC-AWS	Default_LAN_Zone	NO	*	Azure	Static	-	-	15	0	YES	N/A	N/A
6	192.168.10.0/24	×	DC-AWS	Default_LAN_Zone	YES	×	Branch	Static	-		15	0	YES	N/A	N/A
7	172.16.200.0/24		DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
8	172.16.100.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static			15	0	YES	N/A	N/A
9	172.16.30.0/24	•	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static			15	0	YES	N/A	N/A
10	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	1	YES	N/A	N/A
11	0.0.0.0/0	x	Passthrough	Any	YES	×	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0		Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
Showing	g 1 to 13 of 13 entries													First Previous	1 Next Last

Notice from the preceding SD-WAN route table that there are more elements not normally available in traditional routers. Most notable is the "Reachable" column, which renders the route either active or inactive (yes/no) depending on the WAN path state. Routes listed here are suppressed based on various states of the service (the Virtual Path being down as an example). Other events that can force a route to be ineligible are path down state, next hop unreachable, or WAN link down.

From the preceding table, we can see 14 defined routes. A description of the routes or groups of routes is described as follows:

- Route 0 –On the MCN this is a Host subnet route that resides at the DC site. 172.16.10.0/24 resides in the DC LAN and 192.168.15.1 is the gateway on the LAN that is the next hop that will get to that subnet.
- Route 1 This is a local route to this SD-WAN device that displaying the route table.
- Route 2–4 –These are the subnets that are part of the virtual interfaces configured for the DC site SD-WAN. These subnets are derived from the trusted virtual interfaces defined.
- Route 5 This is a shared route to another client node that is shared by the MCN with a Reachability status of No due to the down Virtual Path between that site and the MCN.
- Route 6–9 These routes exist at another client site. For this route, a Virtual Path route is created for matching WAN ingress traffic destined for the remote site on the Virtual Path.
- Route 10 With the Internet Service defined, the system adds a catch all route for direct internet breakout for this local site.
- Route 11 –Passthrough is the default route the system always adds to allow packets to flow through in case there is no match on any existing routes. The Passthrough is not groomed, typ-ically local broadcasts and ARP traffic are mapped to this service.

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

The Default Route Cost Values:

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

After defining these routes, it is important to understand how the traffic flows using the defined routes. These traffic flows are broken into the following flows:

- LAN to WAN (Virtual Path) Traffic going into the SD-WAN overlay tunnel
- WAN to LAN (Virtual Path) Traffic existing the SD-WAN overlay tunnel
- Non-Virtual Path Traffic Traffic routed to the underlay network

## **Intranet and Internet Routes**

For the Intranet and Internet service types, the user must have defined an SD-WAN WAN Link to support those types of services. It is a pre-requisite for any defined routes for either of these services. If the WAN link is not defined to support the Intranet Service, it is considered as a local route. The Intranet, Internet, and Passthrough routes are only relevant to the site/appliance they are configured for.

When defining Intranet, Internet or Passthrough routes the following are design considerations:

- Must have service defined on the WAN link (Intranet/Internet required)
- Intranet/Internet must have gateway defined for the WAN link
- Relevant to local SD-WAN device
- Intranet routes can be learned via the Virtual Path but are done so at a higher cost
- With Internet Service, there is automatically a default route created (0.0.0.0/0) catch all route with a max cost

- Do no assume that Passthrough works, it must be tested/verified, also test with Virtual Path down/disabled to verify desired behavior
- Route tables are static unless the route learning feature is enabled

The maximum supported limit for multiple routing parameters is as follows:

- Maximum Routing Domains: 255
- Maximum Access Interfaces per WAN Link: 64
- Maximum BGP neighbors per site: 255
- Maximum OSPF area per site: 255
- Maximum Virtual Interfaces per OSPF area: 255
- Maximum Route Learning import filters per site: 512
- Maximum Route Learning export filters per site: 512
- Maximum BGP routing policies: 255
- Maximum BGP community string objects: 255

## **Routing Domain**

#### August 24, 2022

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

Citrix SD-WAN appliances implement OSPF and BGP routing protocols for the routing domains to control and segment network traffic.

A Virtual Path can communicate using all routing domains regardless of the definition of the access point. This is possible because SD-WAN encapsulation includes the routing domain information for the packet. Therefore, both end networks know where the packet belongs to. It is not necessary to create a WAN Link or an Access Interface for each routing domain.

Following are the list of points to consider when configuring the Routing Domain functionality:

- By default, routing domains are enabled on an MCN.
- Routing domains are enabled on the Branch sites.
- Each enabled routing domain must have a virtual interface and virtual IP associated with it.

- Routing selection is part of all the following configurations:
  - Interface group
  - Virtual IP
  - GRE
  - WAN Link -> Access Interface
  - IPsec tunnels
  - Routes
  - Rules
- Routing domains are exposed in the web interface configuration only when multiple domains are created.
- For a Public Internet link, only one primary and secondary access interfaces can be created.
- For a Private Intranet/MPLS link, one primary and secondary access interface can be created per routing domain.

## **Configure Routing Domain**

August 24, 2022

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.

With 11.0.2 release, **Routing domains without routable Virtual IPs (VIPs)** is allowed with the following capabilities:

- Allow a device to have a Routing Domain for untrusted or no Interfaces.
- Allow branches to communicate among one another over a Routing Domain that has no physical presence at an intermediate site.

# **Use CLI to Access Routing**

August 24, 2022

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**

#### August 24, 2022

The following two dynamic routing protocols are supported by Citrix SD-WAN:

- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)

Prior to Citrix SD-WAN 11.3.1 release, the dynamic routing capabilities were available only for a single router ID. You can configure a unique router ID either globally for the entire protocol (one for OSPF and BGP) or provide no router ID. If a router ID is not provided, the lowest IP of the Virtual Network Instances (VNIs) participating in dynamic routing is auto-selected as the default router ID.

From Citrix SD-WAN 11.3.1 release onwards, you can not only configure a router ID for the entire protocol but also configure a router ID for each routing domain. With this enhancement, you can enable stable dynamic routing across multiple instances with different router ID's converging in a stable manner.

If you configure a router ID for a specific routing domain, the specific router ID overrides the protocol level routing domain.

#### OSPF

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

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

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).

#### BGP

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

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

#### Exterior BGP (eBGP)

Citrix SD-WAN appliances connect to a switch on the LAN side and a Router on the WAN side. As SD-WAN technology starts becoming more integral to Enterprise network deployments, SD-WAN appliances replace the Routers. SD-WAN implements eBGP dynamic routing protocol to function as a dedicated routing device.

SD-WAN appliance establishes a neighborship with peer routers using eBGP towards WAN side and is able to learn, advertise routes from and to peers. You can select importing and exporting eBGP learned routes on peer devices. Also, SD-WAN static, virtual path learned routes can be configured to advertise to eBGP peers.

For more information, see the following use cases:

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

### AS path length

BGP protocol uses the **AS path length** attribute to determine the best route. The AS path length indicates the number of autonomous systems traversed in a route. Citrix SD-WAN uses the **BGP AS path length** attribute to filter and import routes.

Non-SD-WAN appliances can choose to route traffic to Primary DC or Secondary DC SD-WAN appliances by importing routes based on their AS path length. You can also dynamically steer traffic from a router to Secondary DC by simply increasing the AS path length of the Primary DC appliance on the router, making it unpreferable. Eliminating the need to change the route cost and perform a configuration update.

### **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.

#### Citrix SD-WAN 11.5

Mor	nitoring > Statisti	cs												
St	atistics													
Show	Paulae		) Carabia da da Rafer		erande P	efrech 5	1 church	terr og Deferek	Purne du	namic r	outer			
JIII M	Routes	Ľ	J Enable Auto Kerre	sh 📮 🖣 sa	rconus 🔤	enesi	Clear Cour	ters on Netresh	ruge oy	indirine i	ouves			
Ro	oute Statistics													
Maxim	um allowed routes:	16000												
Route	s for routing doma	in : Default_Rou	utingDomain											
Filter:		in Any column	✓ Ap	ply										
ľ														
Show	100 V entries	Showing 1 to 2	8 of 28 entries		<i>cu</i> 10					_	First	Previous	1 Next	Last
Num	Network Addr	Address	Service	Reachable	Address	Site	Туре	Protocol	Direct	Cost	Count	Eligible	Type	Value
0	115.1.1.0/30	182.120.1.1	Local	YES	÷	pod2_DC	Dynamic	OSPF	•	6	0	YES	N/A	N/A
1	115.168.0.16/30	182.120.1.1	Local	YES	•	pod2_DC	Dynamic	OSPF	•	6	0	YES	N/A	N/A
2	115.168.0.12/30	182.120.1.1	Local	YES	÷	pod2_DC	Dynamic	OSPF	•	6	0	YES	N/A	N/A
3	115.168.0.8/30	182.120.1.1	Local	YES	•	pod2_DC	Dynamic	OSPF		6	0	YES	N/A	N/A
4	115.168.0.4/30	182.120.1.1	Local	YES	•	pod2_DC	Dynamic	OSPF	•	6	0	YES	N/A	N/A
5	115.168.0.0/30	182.120.1.1	Local	YES	•	pod2_DC	Dynamic	OSPF		6	0	YES	N/A	N/A
6	115.14.14.0/30	182.120.1.1	Local	YES	•	pod2_DC	Dynamic	OSPF	÷	6	0	YES	N/A	N/A
7	115.13.13.0/30	182.120.1.1	Local	YES	÷	pod2_DC	Dynamic	OSPF	•	6	0	YES	N/A	N/A
8	115.12.12.0/30	182.120.1.1	Local	YES	•	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	115.10.10.0/30	182.120.1.1	Local	YES		pod2_DC	Dynamic	OSPF	÷	6	0	YES	N/A	N/A
10	115.9.9.16/30	182.120.1.1	Local	YES		pod2 DC	Dynamic	OSPF		6	0	YES	N/A	N/A
11	115.8.8.12/30	182.120.1.1	Local	YES		pod2_DC	Dynamic	OSPF		6	0	YES	N/A	N/A
12	115.7.7.8/30	182.120.1.1	Local	YES		pod2_DC	Dynamic	OSPF		6	0	YES	N/A	N/A
13	115.6.6.4/30	182.120.1.1	Local	YES	•	pod2_DC	Dynamic	OSPF	•	6	0	YES	N/A	N/A
14	115.5.5.0/30	182.120.1.1	Local	YES	•	pod2_DC	Dynamic	OSPF	1	6	0	YES	N/A	N/A
15	115.4.4.0/30	182.120.1.1	Local	YES		pod2_DC	Dynamic	OSPF	•	6	0	YES	N/A	N/A
16	115.3.3.0/30	182.120.1.1	Local	YES	•	pod2_DC	Dynamic	OSPF	•	6	0	YES	N/A	N/A
17	115.2.2.0/30	182.120.1.1	Local	YES		pod2_DC	Dynamic	OSPF	1	6	0	YES	N/A	N/A
18	182.120.1.0/24	•	Local	YES		pod2_DC	Static		•	5	0	YES	N/A	N/A
19	172.120.1.0/24	•	Local	YES		pod2_DC	Static		•	5	0	YES	N/A	N/A
20	182.120.2.0/24	•	pod2_DC-pod3_Br	YES		pod3_Br	Static	•	•	5	0	YES	N/A	N/A
21	172.120.2.0/24	•	pod2_DC-pod3_Br	r YES	•	pod3_Br	Static	-	•	5	0	YES	N/A	N/A
22	182.120.0.0/24	•	pod2_DC-pod1_Br	YES	•	pod1_Br	Static		÷	5	0	YES	N/A	N/A
23	172.120.0.0/24	•	pod2_DC-pod1_Br	YES	•	pod1_Br	Static	-	•	5	0	YES	N/A	N/A
24	192.120.1.0/24	172.120.1.2	Local	YES	•	pod2_DC	Dynamic	OSPF	•	6	75612	YES	N/A	N/A
25	192.120.0.0/24	•	pod2_DC-pod1_Br	YES		pod1_Br	Dynamic	Virtual WAN	YES	6	75612	YES	N/A	N/A
26	0.0.0.0/0	•	Passthrough	YES	•	-	Static	-	÷	16	0	YES	N/A	N/A
27	0.0.0.0/0	•	Discard	YES	•		Static	•	•	16	0	YES	N/A	N/A

Showing 1 to 28 of 28 entries

First Previous 1 Next Last

## **OSPF**

August 24, 2022

## LAN Side: Dynamic Route Learning

OSPF running on the LAN port of Citrix SD-WAN appliance deployed in Gateway Mode:

Citrix SD-WAN appliances perform route discovery of Layer 3 routing advertisements within a local customer network (both branch and data center) for each of the desired routing protocols (OSPF and BGP). The routes that are learned are dynamically captured and displayed.

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

### **Dynamic Route Learning**

Routes learnt from OSPF (P1) BGP (P2)	SD-WAN	Routes learnt from: OSPF (P1) BGP (P2)
LAN side routing		WAN side routing

## WAN Side: Dynamic Route Sharing

Citrix SD-WAN appliance having an AREA defined as a STUB area by limiting the learning of Type 5 AS-external LSA.

Citrix SD-WAN appliances can advertise the locally learned dynamic routes with the MCN. The MCN can then relay these routes to other SD-WAN appliances in the network. This exchange of information dynamically allows for maintaining connectivity between sites across the changing network.

## **OSPF Deployment Modes**

In previous releases, OSPF instance learned routes from SD-WAN were treated as external routes with Type 5 LSA only. These routes were advertised to its neighbor routers in Type 5 External LSA. This resulted in SD-WAN routes to be less preferred routes according to the OSPF path selection algorithm.

With the latest release, SD-WAN can now advertise routes as intra-area routes (LSA Type 1) to get preference as per its route cost using the OSPF path selection algorithm. The route cost can be configured and advertised to the neighbor router. This allows for deploying the SD-WAN appliance in a one-arm mode described below.

## Implementing OSPF in One-Arm Topology

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

#### **Prerequisites:**

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



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

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

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

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



In the above illustration:

- OSPF is configured between *ME-BR1\_Router* and *ME-DC\_Router* in area 0.
- OSPF is configured between *ME-DC\_Router* and *DC* in area 0.

#### **Recommended Configuration:**

- DC VW and ME-DC\_Router on area0
- ME-BR1\_Router and ME-DC\_Router on area0
- BR1 VW and ME-BR1\_Router on area0

On the ME-DC\_Router:

- 1. Add, static route for 172.58.3.10/32(Virtual IP of BR1 for MPLS Link) through 172.58.6.1
- 2. Add, static route for 172.58.4.10/32(Virtual IP of BR1 for INET) through 172.58.5.1

Adding static routes prevents loop formation between the ME-DC\_Router and DC SD-WAN appliance. If you do not add static routes, the MCN forwards traffic to the ME-DC Router, and back from the router to the MCN and this creates a loop continuously.

The static routes which are not PBR routes but the destination Host IP based routes traverse towards the right link to be chosen from the DC side based on the path chosen and the encapsulation performed thereafter. Therefore, with these static routes configured, the encapsulated packets with any destination Virtual IP of the BR1 SD-WAN appliance would use these links as per the best path selected by the DC MCN.

Add ACL to avoid loop formation when IPHOST routes are installed (if no static Virtual IPs configured):

- If the IPHOST routes advertised by the BR1 SD-WAN appliance are installed by the MCN router *ME-DC\_Router* and not added as static routes as mentioned above, there is a possibility of loop formation if the OSPF participating interface (172.58.6.x) between ME-BR1\_Router and ME-DC\_Router goes down. This is because with this interface down, the IPHOST routes are flushed from ME-DC\_Router's routing table.
- If this happens, MCN forwards the encapsulated packet destined to one the BR1 VIPs to the ME-DC Router and back from the router to the MCN and loop continuously.

On the ME-BR1\_Router:

Advertise 172.58.3.x network to ME-DC\_Router with a higher cost than the cost advertised for the same network by DC, if the same AREA-ID is used between **ME-BR1\_Router <-> ME-DC\_Router** and **ME-DC\_Router <-> DC (SD-WAN)**.

- Based on the cost metric computation of OSPF 10^8/BW and the cost for route prefixes are based on the interface type. SD-WAN appliances advertise the virtual path and virtual WAN specific static routes to the external or peer routers with the default SD-WAN cost of 5.
- If the ME-BR1\_Router is also advertising 172.58.3.0/24 as an internal OSPF type 1 route alongside DC (SD-WAN) which also advertises the same prefix as an internal OSPF Type 1 route, then according to cost computation, by default the ME-BR1\_Router's route will be configured, as the cost is lesser than SD-WAN's default cost of 5. To avoid this and make the SD-WAN appliance chosen as the preferred route initially, the interface cost of (172.58.3.1) must be manipulated to make it higher on the ME-BR1\_Router so that the DC SD-WAN route is configured in the routing table of the ME-DC\_Router.

This also ensures that when the DC SD-WAN appliance fails, the alternate route to use ME-BR1\_Router as the next preferred gateway ensures uninterrupted traffic flow.

Use ME-DC\_Router as a source for advertising 172.58.8.0/24 network to both DC SD-WAN and the ME-BR1\_Router:

With this route, the DC SD-WAN can send packets to the upstream router being aware of the LAN subnet after decapsulation. If DC SD-WAN goes down, the legacy routing infrastructure would help ME-BR1\_Router use the ME-DC\_Router as the next hop to reach the 172.58.8.x network.

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

As shown in the illustration below, the third-party appliance site can get to Site B's LAN by sending traffic to Site B directly. If it cannot send traffic directly, the fallback route goes to Site A, then using

the virtual path between DC to Branch sites to get to the Branch. If that fails, it uses MPLS2 to get to the Branch site.



Traffic flow can be observed in the SD-WAN GUI under **Monitoring** > **Flows**.

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



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

## Troubleshooting

You can view the OSPF parameters under **Monitoring >Routing Protocols**.

#### Citrix SD-WAN 11.5

Dashboard Mo	nitoring Configuration									
Statistics	Monitoring > Routing Protocols									
Flows										
Routing Protocols	Dynamic Routing Protocol									
Firewall	View: OSPF Interface 🗸 Routing Domain : Default_RoutingDomain 🗸 Refresh									
IKE/IPsec										
IGMP	OSPF Interface									
Performance Reports	ospf_rdomain_0: Interface vni+0 (172 58 1 0/24)									
Qos Reports	Type: broadcast Area: 0.0.0.0 (0)									
Usage Reports	State: DROther Priority: 0									
Availability Reports	Hello timer: 10 Wait timer: 40									
Appliance Reports	Dead timer: 40 Retransmit timer: 5									
DHCP Server/Relay	Designated router (10): 103.105.105 Designated router (IP): 172.58.1.28 Backup designated router (ID): 0.0.00									
VRRP	Backup designated router (ID): 0.0.0.0									
Dashboard Statistics Flows	Monitoring Configuration Monitoring > Routing Protocols									
Routing Protocols	Dynamic Routing Protocol									
Firewall	View: OSPF Neighbors V Routing Domain : Default_RoutingDomain V Refresh									
IKE/IPsec										
IKE/IPsec	OSPF Neighbors									
IKE/IPsec IGMP Performance Reports	OSPF Neighbors ospf_rdomain_0: Router ID Pri State DTime Interface Router IP									

## You can also observe the Dynamic routing logs to see if there is any issue with OSPF Convergence.

Diagnose		
Debug Logging:	• On	Ooff
Filename:	dynamic_routing_diagnostics.log $\checkmark$	
	View Log	

#### BGP

#### August 24, 2022

The SD-WAN BGP routing functionality enables you to:

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

Note

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

#### **Configuring Neighbors**

To configure eBGP, an extra column to the existing BGP neighbors section is added to configure the neighbor AS number. The existing configurations are pre-populated to this field with the local AS number when you import the previous configuration using the SD-WAN 9.2 configuration editor.

The neighbor configuration also has an optional advanced section (expandable row) where you can add Policies for each neighbor.

## **Configuring Advanced Neighbors**

With this option, you can add network objects and add a configured BGP policy for that network object. This is similar to creating a route map and ACL to match certain routes and configuring BGP attributes for that neighbor. You can specify the direction to indicate if this policy is applied for incoming or outgoing routes.

The default policy is to <accept> all routes. Accept and reject policies are defaults and cannot be modified.

You have the ability to match routes based on Network address (destination address), AS Path, Community string and assign a policy and select direction for the policy to be applied.

1. 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 Pro-tocol** page. The logs for the routing daemon are split into separate log files. The standard routing information is stored in *dynamic\_routing.log* while dynamic routing issues are captured in *dynamic\_routing\_diagnostics.log* which can be viewed from monitoring of routing protocols.

### **BGP Soft Reconfiguration**

Routing policies for BGP peer include configurations such as route-map, distribute-list, prefix-list, and filter-list that might impact inbound or outbound routing table updates. When there is a change in the routing policy, the BGP session must be cleared, or reset, for the new policy to take effect.

Clearing a BGP session using a hard reset invalidates the cache and results in negative impact on the operation of the networks as the information in the cache becomes unavailable.

The BGP Soft Reset Enhancement feature provides automatic support for dynamic soft reset of inbound BGP routing table updates that are not dependent upon stored routing table update information.

## Troubleshooting

To view the BGP parameters, navigate to **Monitoring > Routing Protocols** > select **BGP State** from the **View** field.

#### Citrix SD-WAN 11.5

Dashboard Mo	nitoring Configuration
Statistics	Monitoring > Routing Protocols
Flows	
Routing Protocols	Dynamic Routing Protocol
Firewall	View: BGP State V Routing Domain : Default_RoutingDomain V BGP Session : <all> V Reset Session Refr</all>
IKE/IPsec	
IGMP	BGP State
Performance Reports	name proto table state since info beol rdomain 0 BGP T0 up 2020-08-27 10:46:44 Established
Qos Reports	Preference: 100 Input filter: neighbour_0_in
Usage Reports	Output filter: neighbour_0_out Routes: 8 imported, 4 exported, 1 preferred Route.change.stats: resived related filtered ignored accented
Availability Reports	Import updates: 16 0 0 8 8 Import withdraws: 0 0 0 0
Appliance Reports	Export updates: 43 19 18 6 Export withdraws: 2 2
DHCP Server/Relay	BGF state: Established Neighbor address: 172.58.1.28 Neighbor AS: 10
VRRP	Citrix SD-WAN Interface: vni-0 Neighbor ID: 105.105.105
PPPoE	Neighbor caps: refresh AS4 Session: internal multihop AS4 Source address: 173 58 1 10
DNS	Hold time: 130/180

You can observe theDynamic routing logs to see if there is any issue with BGP Convergence.

Diagnose		
Debug Logging:	• On	Ooff
Filename:	dynamic_routing_diagnostics.log V	
	View Log	

## **iBGP**

August 24, 2022

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

August 24, 2022

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**

#### August 24, 2022

In a typical enterprise network, the branch offices access applications on the on-premises data center, the cloud data center, or the SaaS applications. The application routing feature, allows you to steer the applications through your network easily and cost-efficiently. For example, when a user on the branch site is trying to access a SaaS application the traffic can be routed such that the branch offices can access the SaaS applications on the internet directly, without having to go through the data center first.

Citrix SD-WAN allows you to define the application routes for the following services:

• Virtual Path: This service manages traffic across the Virtual Paths. A Virtual Path is a logical link between two WAN links. It comprises a collection of WAN Paths combined to provide high service-level communication between two SD-WAN nodes. The SD-WAN appliance measures

the network on a per-path basis and adapts to changing application demand and WAN conditions. A Virtual Path can be static (always exists) or dynamic (exists only when traffic between two SD-WAN Appliances reaches a configured threshold).

- **Internet:** This service manages traffic between an Enterprise site and sites on the public Internet. Internet traffic is not encapsulated. When congestion occurs, the SD-WAN actively manages bandwidth by rate-limiting Internet traffic relative to the Virtual Path, and Intranet traffic.
- **Intranet**: This service manages Enterprise Intranet traffic that has not been defined for transmission across a Virtual Path. Intranet traffic is not encapsulated. The SD-WAN manages bandwidth by rate-limiting this traffic relative to other service types during times of congestion. Under certain conditions, and if Intranet Fallback is configured on the Virtual Path, traffic that ordinarily travels through Virtual Path can instead be treated as Intranet traffic.
- **Local**: This service manages traffic local to the site that matches no other service. SD-WAN ignores traffic sourced and destined to a local route.
- **GRE Tunnel**: This service manages IP traffic destined for a GRE tunnel, and matches the LAN GRE tunnel configured at the site. The GRE Tunnel feature enables you to configure SD-WAN appliances to terminate GRE tunnels on the LAN. For a route with service type GRE Tunnel, the gateway must reside in one of the tunnel subnets of the local GRE tunnel.
- LAN IPsec Tunnel: This service manages IP traffic destined for a LAN IPsec tunnel, and matches the LAN IPsec tunnel configured at the site. The LAN IPsec Tunnel feature enables you to configure SD-WAN Appliances to terminate IPsec tunnels on the LAN or WAN side.

To perform service steering for applications, it is important to identify an application on the first packet itself. Initially, the packets flow through the IP route once the traffic is classified and the application is known, the corresponding application route is used. First packet classification is achieved by learning the IP subnets and ports associated with application objects. These are obtained using historical classification results of the DPI classifier, and user configured IP port match types.

To 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.

ashboard Monit	Configuration											
Statistics	Montoring > Statistics											
ows												
outing Protocols	Statistics											
irewall	Show Application Routes 🔹 🗉 Enable Auto Refresh 5 🔹 acconst: Refresh 🗷 Clear Counters on Refresh											
KE/IPsec	Another Book Statistics											
SMP	Application Route Statustics Meanume allowed routes 40000 Application Routes for routing domains : Default, RoutingDamain											
Performance Reports												
Qos Reports												
Usage Reports												
Availability Reports	Filter in Any column • Apply											
oppliance Reports	Show 100 • entries Showing I to 4 of 4 entries II Next Last											
DHCP Server/Relay	Num <sup>A</sup> Application Object         Gateway IP Address         Stervice         Flewall Zone         Reachable         Site         Type         Cost         Hit Count         Eligibility Type         Eligibility Type											
RRP	0 TEST1 * Internet_Zone YES Branch1 Static 5 0 YES N/A N/A											
	1 Slack * Internet Internet_Zone YES Branch1 Static 5 0 YES N/A N/A											
	2 Salesforce * Internet_Zone YES Branch1 Static 5 173 YES Path Branch1-WL-1->MCH-DC-WL-2											
	3 Salesforce * Internet Internet_Zone YES Branch1 Static 5 0 YES N/A N/A											
	Drawing 15.4 of 4 entries First Previous 3 Res Last											

You can view the following statistics:

- Application Object: Name of the application object.
- **Gateway IP Address**: The gateway IP address used by application objects with GRE Tunnel service type.
- Service: The service type mapped to the application object.
- **Firewall Zone**: The firewall zone that this route falls in.
- **Reachable**: The status of the application route.
- Site: Name of the site.
- **Type**: Indicates if the route is static or dynamic.
- **Cost**: The priority of the route.
- Hit Count: The number of times the application route is used to steer the traffic.
- **Eligible**: Is the application route eligible to send the traffic.
- **Eligibility Type**: The type of route eligibility condition applied to this route. The eligibility type can be Path, Gateway, or Tunnel.
- Eligibility Value: The value specified for the route eligibility condition.

#### Note

In the current release, applications that belong to application family, match type defined in application object, cannot be steered.

#### Troubleshooting

After creating the application route, you can confirm that the application is correctly routed to the intended service using the **Monitoring** section.

To view if the application is correctly routed to the intended service, navigate to the following pages:

- Monitoring > Statistics > Application Routes
- Monitoring > Flows
- Monitoring > Firewall

If there is any unexpected routing behavior, collect the STS diagnostics bundle while the issue is being observed, and share it with the Citrix Support team.

The STS bundle can be created and downloaded using **Configuration > System Maintenance > Diagnostics > Diagnostic Information**.

# **Route filtering**

#### August 24, 2022

For networks with Route Learning enabled, Citrix SD-WAN provides more control over which SD-WAN routes are advertised to routing neighbors rather and which routes are received from routing neighbors, rather than advertising and accepting all or no routes.

- Export Filters are used to include or exclude routes for advertisement using OSPF and BGP protocols based on specific match criteria. Export filter rules are the rules that have to be meet when advertising SD-WAN routes over dynamic routing protocols. All the routes are advertised to peers by default.
- Import Filters are used to accept or not accept routes which are received using OSPF and BGP neighbors based on specific match criteria. Import filter rules are the rules that have to be meet before importing dynamic routes into the SD-WAN route database. No routes are imported by default.

Route filtering is implemented on LAN routes and Virtual Path routes in an SD-WAN network (Data Center/Branch) and is advertised to a non-SD-WAN network through using BGP and OSPF.

You can configure up to 512 Export Filters and 512 Import Filters. This is the overall limit, not per routing domain limit.

# **Route Summarization**

#### August 24, 2022

With the increase in the size of the enterprise networks, the routers need to maintain the large number of routes in their routing table. The routers require increased CPU, memory and bandwidth resources to look up the large routing tables, and maintain individual routes. You can configure a summary route with Local and Discard service types. This summary route is advertised to the next-hop devices.

## Troubleshooting

The summarized routes configured on the MCN are sent to the Branch over the virtual path. In case you do not see the virtual path details in the route table of the Branch, check the Branch dashboard. The dashboard displays the status of the virtual path between the MCN and Branch.

Name:	BR1_VPX
Model:	VPX
Sub-Model:	BASE
Appliance Mode:	Client
Serial Number:	5f4519dd-e39a-d3f6-24a6-6ba0e6578d2c
Management IP Addres	ss: 10.105.172.7
Appliance Uptime:	6 days, 56 minutes, 1.4 seconds
Service Uptime:	6 days, 50 minutes, 39.0 seconds
Routing Domain Enable	ed: Default_RoutingDomain
Local Versions	
Configuration Created	On: Wed Sep 2 11:15:54 2020
Software Version:	11.2.1.53.864510
Built On:	Aug 25 2020 at 19:02:21
Hardware Version:	VPX

If the virtual path is down, check the reason for it under **Configuration > Logging/Monitoring**.

Select one of the following files from the **filename** drop-down list to verify:

- SDWAN\_paths.log
- SDWAN\_common.log

#### Citrix SD-WAN 11.5

Dashboard Monitoring	Configuration								
- Appliance Settings	Configuration > Appliance Settings > Logging/Monitoring								
Administrator Interface     Logging/Monitoring	Log Options         Alert Options         Alarm Options         Syslog Server         HTTP Server         Application								
- Network Adapters - Net Flow	View Log File								
App Flow/IPFIX	Only the most recent 10000 entries will be shown and filtered. To view the full log, download and open it locally.								
- NITRO API - Licensing	Filename: SDWAN_paths.log								
Fallback Configuration	Filter (Optional):								

# **Protocol preference**

#### August 24, 2022

Protocol preference is a Citrix SD-WAN specific feature, which is similar to router administrative distance. The protocol with the highest preference order is the most preferred. The route using the protocol with the highest protocol preference value. The protocol precedence information is local to the Citrix SD-WAN appliance and is not advertised to peer network elements.

## **Multicast routing**

#### August 24, 2022

Multicast routing enables efficient distribution of one-to-many traffic. A multicast source, sends multicast traffic in a single stream to a multicast group. The multicast group contains receivers such as hosts and adjacent routers that use the IGMP protocol for multicast communication. Voice over IP, Video on demand, IP television, and Video conferencing are some of the common technologies that use multicast routing. When you enable multicast routing on the Citrix SD-WAN appliance, the appliance acts as a multicast router.

## Source specific multicast

Multicast protocols typically allow multicast receivers to receive multicast traffic from any source. With source specific multicast (SSM), you can specify the source from which the receivers receive the multicast traffic. It ensures that the receivers are not open listeners to every source that is sending multicast streams but rather listen to a particular multicast source. SSM reduces the cost of resources used in consuming traffic from every possible source and also provides a layer of security by ensuring that the receivers receive traffic from a known sender.

The following topology shows two multicast receivers at a branch site and a multicast server (172.9.9.2) at the Data Center. The multicast server streams traffic over a particular group (232.1.1.1), the receivers join the group. Any traffic streamed on the multicast group is relayed to all the receivers that joined the group.

### Note

For SSM to work, the multicast group IP must fall within the range 232.0.0.0/8.



- 1. The multicast receivers send an IP IGMP join request indicating that the receivers want to join the multicast group and want to receive the multicast stream from the source. The IGMP join includes 2 attributes the multicast source and group (S, G). IGMP Version 3 is used for SSM on the multicast source and the receiver to relay some INCLUDE specific source addresses. SSM allows the receivers to explicitly receive streams from specific Multicast servers, whose source address is explicitly provided by the receivers as part of the JOIN request. In this example, an IGMP v3 join request is triggered with an explicit include source list, which contains the source 172.9.9.2, to be the address that sends the multicast stream over the group 232.1.1.1.
- 2. The Citrix SD-WAN at the branch listens to all the IGMP requests from these receivers and converts it into a membership report and sends it over the Virtual Path to the SD-WAN appliance at the data center.
- 3. The Citrix SD-WAN appliance at the data center receives the membership report over the Virtual Path and forwards it to the Multicast Source, establishing a control channel.
- 4. The Multicast source transmits the multicast stream over the Virtual path to the multicast receivers.

The control channel traffic and the multicast stream flow through the established virtual path between the branch and the data center. The Citrix SD-WAN overlay path insures and insulates multicast traffic from WAN degradation or link brownouts.

## **Configure multicast**

To configure multicast, perform the following on the SD-WAN appliance at both the source and destination.

- 1. Create a multicast group Provide a name and IP address for the multicast group. The multicast group IP must fall within the range 232.0.0.0/8 for source specific multicast.
- 2. Enable IGMP proxy—You can configure the Citrix SD-WAN appliance as an IGMP proxy to carry the IGMP control channel information for multicast routing. IGMP V3 is required for single source multicast.
- Define the upstream and downstream services An upstream interface enables the IGMP PROXY to connect to the SD-WAN appliance closer to the actual multicast source that streams the traffic. A downstream interface enables the IGMP Proxy to connect to the hosts that are farther away from the actual multicast source that streams the traffic.

The upstream and downstream services are different for the appliance at the source and the appliance at the destination.

## Monitoring

#### **IGMP statistics**

When the multicast receivers initiate a join group request, you can see the receiver details under **Mon-itoring** > **IGMP** on the appliance. You can see this information on the appliances at both the source and the destination.

The following image shows an MLD join initiated and the message type RECV is used to receive multicast group addresses. You can also see the IGMP/MLD message statistics below.

IGMP/MLD Statistics				
Select maximum IGMP/MLD Statistics to display 🗸 🗸	Purge IGMP/MLD Statistics	Refresh	Search	Q
Type :	Description	Value		: +
RECV	Receive MLD V1 Leave	0		
RECV	Receive MLD Mode is INCLUDE	0		
RECV	Receive MLD Mode is EXCLUDE	92		
RECV	Receive MLD Change to INCLUDE	0		
RECV	Receive MLD Change to EXCLUDE	0		
RECV	Receive MLD Allow	0		
RECV	Receive MLD Block	0		
RECV	Receive MLD V1 General Query Downstream	0		
RECV	Receive MLD V2 General Query Downstream	0		
RECV	Receive MLD V2 Group Query Downstream	0		

The following image shows information about IGMP/MLD proxy groups. You can also see the IGM-P/MLD proxy group statistics and the version used.

Select the n	naximum P	Yoxy Groups to d	isplay 🥆	/ Purg	e IGMP/M	D Proxy Groups	$\supset$		Refre	sh	Search		C
fype		Name		Group		Filter		Version		Packets Sent		Bytes Sent	
HOST		VIF-1-LAN-1				EXCLUDE		MLDv2		12380158		1832263384	
HOST		VIF-1-LAN-1				EXCLUDE		MLDv2		12380158		1832263384	
HOST		VIF-1-LAN-1				EXCLUDE		MLDv2		12380158		1832263384	
HOST		VIF-1-LAN-1				EXCLUDE		MLDv2		11905188		1761967824	

# **Configure Virtual Path Route Cost**

#### August 24, 2022

Citrix SD-WAN supports the following routing enhancements related to data center administration.

For example, consider the SD-WAN network with two data centers; one in North America and one in Europe. You want all sites in North America to route traffic through the data center in North America and all sites in Europe to use the Europe data center. Previously, in SD-WAN 9.3 and earlier release versions, this functionality of data center administration was not supported. This is implemented with the introduction of Virtual Path Route cost.

• Virtual Path Route cost: You can configure the Virtual Path route cost for individual virtual paths that are added to the route cost when a route is learned from a remote site.

This feature invalidates or deletes the WAN to WAN forwarding Cost.

- OSPF Route Cost: You can now import OSPF route cost (type1 metric) by enabling Copy OSPF Route Cost in the import filters. OSPF Route cost is considered in route selection instead of SD-WAN cost. Cost up to 65534 instead of 15 is supported, but it is advisable to accommodate for an appropriate virtual path route cost that is added if the route is learned from a remote site.
- BGP VP cost to MED: You can now copy the Virtual Path route cost for SD-WAN routes into BGP MED values when exporting (redistributing) SD-WAN routes to BGP peers. This can be set for individual neighbors by creating a BGP policy and applying it in the "OUT" direction for each neighbor.
- Any site can have multiple virtual paths to other sites. Sometimes, if there is a Branch to which there is connectivity to services through more virtual paths, there can be two virtual paths from the Branch site. One virtual path through DC1 and the other through DC2. DC1 can be an MCN and DC2 can be a Geo-MCN, and can be configured as another site with Static Virtual Path.

- Add a default cost for each VP as 1. Virtual Path Route cost helps associate a cost to each virtual path of a site. This helps to manipulate route exchanges/updates over a specific virtual path instead of default site cost. With this, we can manipulate which data center to be preferred for sending out the traffic.
- Allow cost to be configured within a small range of values (for example; 1–10) for each VP.
- Virtual path cost must be added to any route shared with neighbor sites to indicate routing preference, including routes learned via Dynamic Routing.
- No Static Virtual Path must have a lower cost than a Dynamic Virtual Path.

Note

VP Route cost deprecates the WAN to WAN forwarding cost that existed in release versions earlier than release version 10.0. The routing decisions based on WAN to WAN forwarding costs have to be reinfluenced by using VP route cost as the WAN to WAN forwarding cost has no significance when you migrate to release version 10.0.

## **Monitoring and Troubleshooting**

The routing table displays how the same subnets advertised by two sites connected to a branch site over the virtual path are installed with precedence of cost with Virtual Path route cost addition.

To verify the route cost and which routes are used in the routing table, navigate to **Monitoring > Sta-tistics >** under **Show** field, select **Routes**. Route costs and hit counts can be verified in the same page.

The following figure shows the route table with two different costs for the same route which is 172.16.6.0/24 with cost 10 and 11 for services **DC-Branch01** and **GEOMCN-Branch01** respectively.

#### Citrix SD-WAN 11.5

Monito	ring >	Statistics												
Stati	stics													
Show: Routes Clear Counters on Refresh Purge dynamic routes														
				l'arge ayname roace.										
Route Statistics														
Routes f	or routi	ng domain : Defau in Any co	ılt_RoutingI lumn	Domain										
Show 10	10 🗸 er	tries Showing 1	to 18 of 18	entries								First	Previou	JS 1
Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Туре	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type
٠	0	172.16.60.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
٠	1	172.16.61.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	-	-	5	0	YES	N/A
٠	2	172.16.41.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
٠	3	172.16.40.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
۲	4	172.16.6.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
٠	5	172.16.4.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
٠	6	172.16.3.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
٠	7	172.16.2.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
+	8	172.16.51.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
+	9	172.16.50.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
٠	10	172.16.6.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
+	11	172.16.4.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A

# **Configure Virtual Router Redundancy Protocol**

#### August 24, 2022

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

A back-up router automatically takes over if the primary / master router fails. In a VRRP set-up, the master router sends a VRRP packet known as an advertisement to the back-up routers. If the master router stops sending the advertisement, the back-up router sets the interval timer. If no advertisement is received within this hold period, the back-up router initiates the failover routine.

VRRP specifies an election process in which, the router with the highest priority becomes the master. If the priority is the same among the routers, the router with the highest IP address becomes the master. The other routers are in backup state. The election process is initiated again if the master fails, a new router joins the group, or an existing router leaves the group. VRRP ensures a high availability default path without configuring dynamic routing or router discovery protocols on every end-host.

Citrix SD-WAN release version 10.1 supports VRRP version 2 and version 3 to inter-operate with any third party routers. The SD-WAN appliance acts as a master router and direct the traffic to use the Virtual Path Service between sites. You can configure the SD-WAN appliance as the VRRP master by configuring the Virtual Interface IP as the VRRP IP and by manually setting the priority to a higher value than the peer routers. You can configure the advertisement interval and the preempt option.

The below network diagram shows a Citrix SD-WAN appliance and a router configured as a VRRP group. The SD-WAN appliance is configured to be the master. If the SD-WAN appliance fails, the back-up router takes-over within milliseconds, ensuring that there is no downtime.



Data Center

### **VRRP Statistics**

You can view the VRRP statistics under **Monitoring** > **VRRP**.

#### Citrix SD-WAN 11.5

VRR	P Instances						
	inable	Disable					
	VRRP ID	Version	Interface(s)	State	Priority	Virtual Router IP	Advertisement Interval
۲	245	3	VIF-1-LAN-2	Master	130	112.08.1.09	100
0	21	3	VIF-5-LAN-1	Backup	100	1480.7380	1000
0	246	3	VIF-1-LAN-2	Master	100	1480-1-010	1000

You can view the following statistics data:

- VRRP ID: The VRRP group ID
- Version: The VRRP protocol version.
- Interface: The virtual interface used for VRRP.
- **State:** The VRRP state of the SD-WAN appliance. It indicates whether the appliance is a master or a backup.
- Priority: The priority of the SD-WAN appliance for a VRRP Group
- Virtual Router IP: The virtual router IP address for the VRRP group.
- Advertisement Interval: The frequency of VRRP advertisements.
- **Enable:** Select this to enable the VRRP instance on the SD-WAN appliance.
- **Disable:** Select this to disable the VRRP instance on the SD-WAN appliance.

#### Limitations

- VRRP is supported in Gateway Mode deployment only.
- You can configure up to four VRRP IDs (VRID).
- Up to 16 virtual network interfaces can participate in VRID.

#### **High Availability and VRRP**

You can significantly reduce network downtime and traffic disruption by leveraging both the high availability and VRRP features on your SD-WAN network. Deploy a pair of Citrix SD-WAN appliance in active/standby roles along with a standby router to form the VRRP group. This group appears as a single default gateway with one virtual IP address and one virtual MAC address.



The following are 2 cases with the above deployment:

#### 1st case: High availability failover timer on SD-WAN equals the VRRP failover timer.

The expected behavior is high availability switchover to happen before the VRRP switchover, that is the traffic continues to flow through the new Active SD-WAN appliance. In this case SD-WAN continues with the VRRP Master role.

#### 2nd case: High availability failover timer on SD-WAN greater than the VRRP failover timer.

The expected behavior is the VRRP switchover to the router happens, that is the router becomes VRRP Master and traffic might momentarily flow through the router, bypassing the SD-WAN appliance.

But once the high availability switchover happens, SD-WAN again becomes VRRP Master, that is the traffic now flows through the new active SD-WAN appliance.

For more information on high availability deployment modes, see High Availability.

## **Routing Support for LAN Segmentation**

#### August 24, 2022

The SD-WAN Standard 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 Edition appliance.

The above capability is implemented by using a Virtual Routing and Forwarding (VRF) table that is maintained in the SD-WAN Standard 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.

## Inter-routing domain service

#### August 24, 2022

Citrix SD-WAN allows you to segment the network using Routing Domains, ensuring high security and easy management. With the use of the Routing Domain the traffic is isolated from each other in the overlay network. Each routing domain maintains its own routing table. However, sometimes we need to route the traffic between the Routing domains. For example if shared services such as printer, scanner, and mail server are provisioned as a separate Routing Domain. Inter-routing domain is required to enable users from different routing domains to access the shared services.

Citrix SD-WAN provides Static Inter-Routing Domain Service, enabling route leaking between Routing Domains within a site or between different sites. This eliminates the need for an edge router to handle route leaking. The Inter-routing domain service can further be used to set up routes, firewall policies, and NAT rules.

A new Firewall Zone, **Inter\_Routing\_Domain\_Zone** is created by default and serves as the firewall zone for the Inter-Routing Domain Services for routing and filtering.

#### Monitoring

You can view monitoring statistics for connections that use inter-routing-domain services under **Mon**itoring > Firewall Statistics > Connections.

Dashboard	Monitoring Configuration																
Montoing > Firewall																	
Frewall Statistics																	
Statistics:	Instance Connections V																
Maximum entries to display:	50 🗸																
Filtering:	Routing Domain: Any	<ul> <li>Application:</li> </ul>	Any		✓ Family:	Any	$\sim$										
	IP Protocol: Any	V Source Zone:	Any		✓ Destina	tion Zone: Any	~										
	Source Service Type: Any 🗸	Source Service I	nstance: Any	~	Source	IP: *	Sou	ce Ports	8								
	Destination Service Type: Any	Destination Ser	ice Instance: Any	~	Destina	tion IP: *	Dest	ination Port:	8								
Refresh	Show latest data	nal Stats		_													
Clear Connections																	
Help																	
Connections																	
																	_
					506	irce				Dert	nation					260	
Routing Domain	Application	Family Prob	IP Adress	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	NAT	Packets	Bytes	PPS k
Default_RoutingDor	nain Internet Control Message Protocol(icmp	Network Service ICN	P 172.16.25.10	19973	Local	VIF-2-LAN-1	Default_LAN_Zone	172.16.1.10	19973	Inter-Routing-Domain	Default_to_MPLS	Inter_Routing_Domain_Zone	ESTABLISHED	Yes	10124	850416	0.999
RD_MPLS	Internet Control Message Protocol(icmp	) Network Service ICN	P 172.16.15.100	19973	Inter-Routing-Domain	Default_to_MPLS	Inter_Routing_Domain_Zone	172.16.1.10	19973	Virtual Path	DC_MCN-BR3	Default_LAN_Zone	ESTABLISHED	No	10124	850416	0.999 (
Connections Displaye Connections In Use:	Connections In Use: 2/128000																
<																	>

# **ECMP load balancing**

#### August 24, 2022

Equal Cost Multi-Path (ECMP) groups allow you to group multiple paths with the same cost, destination, and service. The connections or session data is load balanced across all the paths in the ECMP group depending on the type of ECMP group. For example, consider a network with two WAN links between a branch and a data center having the same route cost. Traditionally, one of the WAN links would be active and the other remains dormant acting as a fallback link. With ECMP Groups, you can group these WAN links together and allow traffic to be load balanced through both the WAN links. ECMP load balancing ensures:

- Distribution of traffic over multiple equal-cost paths.
- Optimal usage of available bandwidth.
- Dynamic transfer of traffic to other ECMP member path, if a link fails. ECMP supports static routes on IPsec / GRE tunnels.

ECMP load balancing is supported on Virtual Paths and Intranet services. ECMP groups are defined at the global level. You can define a maximum of 254 ECMP groups in your network. The maximum number of ECMP eligible routes in an ECMP group depend on your appliance and license type. The following two types of ECMP groups are supported on Citrix SD-WAN:

- Source/destination IP address: Networks where multiple clients try to connect to the same destination, the connections are load balanced across equal cost WAN links.
- Session: Networks where a single client is connected to a destination and multiple sessions are spawned. The session data is load balanced across equal cost WAN links.

To monitor ECMP load balancing, in the SD-WAN UI, navigate to **Monitoring** > **Statistics** > **Routes** and filter the search results using the ECMP group name.

#### Citrix SD-WAN 11.5

Dashboard Mo	Configuration										
Statistics	Monitoring > Statistics										
Flows											
Routing Protocols	Statistics										
Firewall	Show: Routes V Z Enable Auto Refresh 5 V seconds Stop Z Clear Counters on Refresh										
IKE/IPsec	Routing Domain: <all> V Purge dynamic routes</all>										
IGMP											
Performance Reports	Route Statistics										
Qos Reports	Maximum allowed routes: 64000										
Usage Reports											
Availability Reports	Routes for routing domain : Default_RoutingDomain										
Appliance Reports	Filter: Tonowhere in ECMP Group v Network Address Type: ALL v Apply										
DHCP Server/Relay	Show 100 v entries Showing 1 to 4 of 4 entries (filtered from 35 total entries) First Previous 1. Next Last										
VRRP	Details' Num Network Gateway IP Service Firewall Zone Reachable Site Type Protocol Neighbor Cost Hit ECMP Eligibility Eligibility Zuige Eligibility Value										
PPPoE	🛞 6 6.6.6.0/24 * New_Intranet_Service-3 Intranet_Zone YES BRI Static 5 0 Tonowhere YES N/A N/A										
DNS	[■ 7 5.5.5.0/24 * New_Intranet_Service-3 Intranet_Zone YES BR1 Static 5 630 Tonowhere YES Path BR1_Inet1->DC_Inet1										
	🕐 🗷 8 5.5.5.0/24 * New_Intranet_Service-4 Intranet_Zone YES BR1 Static 5 315 Tonowhere YES N/A N/A										
	1 9 4.4.4.0/24 * New_Intranet_Service-4 Intranet_Zone YES BR1 Static 5 0 Tonowhere YES N/A N/A										
	Showing 1 to 4 of 4 entries (filtered from 35 total entries)										

In the sample data, we see that all the routes within a service having a common ECMP group are part of that ECMP group. For example, 6.6.6.0/24 and 5.5.5.0/24 are in the ECMP Group **Tonowhere**. However, the traffic load is balanced between the services **New\_Intranet\_Service-3** and **New\_Intranet\_Service-4** that share a destination IP 5.5.5.0/24 and are associated to the same ECMP group.

#### Note

For the SIA and Zscaler service, you can load balance across two IPsec tunnel paths with ECMP (Active/Active).

## Security

#### August 24, 2022

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**

#### August 24, 2022

Citrix SD-WAN supports IPsec virtual paths, enabling third-party devices to terminate IPsec VPN Tunnels on the LAN or WAN side of a Citrix SD-WAN appliance. You can secure site-to-site IPsec Tunnels terminating on an SD-WAN appliance by using a 140-2 Level 1 FIPS certified IPsec cryptographicbinary.

Citrix SD-WAN also supports resilient IPsec tunneling using a differentiated virtual path tunneling mechanism.



#### Important Note:

- From SD-WAN 11.5 release onwards, all the IPsec tunnel configurations and IKE settings are supported only through Citrix SD-WAN Orchestrator service. For information regarding Citrix SD-WAN Orchestrator service IPsec/IKE configurations, see IPsec service.
- Citrix SD-WAN supports connectivity to Oracle Cloud Infrastructure (OCI) through IPsec.

# **Citrix SD-WAN integration with AWS Transit Gateway**

#### August 24, 2022

**Amazon Web Service (AWS) Transit Gateway** service enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. As the number of
workloads running on AWS grows, you can scale your networks across multiple accounts and Amazon VPCs to keep up with the growth.

You can now connect pairs of Amazon VPCs using peering. However, managing point-to-point connectivity across many Amazon VPCs, without the ability to centrally manage the connectivity policies, can be operationally costly and cumbersome. For on-premises connectivity, you need to attach your AWS VPN to each individual Amazon VPC. This solution can be time consuming to build and hard to manage when the number of VPCs grows into the hundreds.

With **AWS Transit Gateway**, you only have to create and manage a single connection from the central gateway into each Amazon VPC, on-premises data center, or remote office across your network. The Transit Gateway acts as a hub that controls how traffic is routed among all the connected networks which act like spokes. This hub and spoke model significantly simplifies management and reduces operational costs because each network only has to connect to the Transit Gateway and not to every other network. Any new VPC is connected to the Transit Gateway and automatically available to every other network that is connected to the Transit Gateway. This ease of connectivity makes it easy to scale your network as you grow.

As enterprises migrate an increasing number of applications, services, and infrastructure to the cloud, they are rapidly deploying SD-WAN to realize the benefits of broadband connectivity and to directly connect branch site users to cloud resources. There are many challenges with the complexities of building and managing global private networks using internet transport services to connect geographically distributed locations and users with proximity-based cloud resources. The **AWS Transit Gate-way Network Manager** changes this paradigm. Now, Citrix SD-WAN customers who use AWS can use Citrix SD-WAN with AWS transit gateway by integrating Citrix SD-WAN branch appliance AWS Transit Gateway to deliver the highest quality of experience for users with the ability to reach out to all VPCs connected to the Transit Gateway.

The following are the steps to integrate Citrix SD-WAN with AWS Transit Gateway:

- 1. Create the AWS Transit Gateway.
- 2. Attach a VPN to the Transit Gateway (either existing VPN or a new one).
- 3. Attach VPN to the configured Transit Gateway where the VPN is with SD-WAN site located Onprem or in any cloud (AWS, Azure, or GCP).
- 4. Establish the Border Gateway Protocol (BGP) peering over the IPsec Tunnel with the AWS Transit Gateway from Citrix SD-WAN to learn the networks (VPCs) attached to Transit Gateway.

### Use case

The use case is to reach out to resources deployed within AWS (in any VPC) from the branch environment. Using AWS Transit Gateway allows the traffic to reach to all VPCs connected to the Transit Gateway without dealing with BGP routes. To achieve this, perform the following methods:

- Establish the IPsec to AWS Transit Gateway from the branch Citrix SD-WAN appliance. In this deployment method you will not get full SD-WAN benefits as the traffic will go over IPsec.
- Deploy a Citrix SD-WAN appliance within AWS and connect it to your On-prem Citrix SD-WAN appliance via virtual path.

Regardless of which method is chosen, the traffic reaches to the VPCs connected to the Transit Gateway without manually manage the routing within AWS infra.



### **AWS Transit Gateway configuration**

To create the AWS Transit Gateway, navigate to VPC dashboard and go to Transit Gateway section.

1. Provide the Transit Gateway Name, Description, and Amazon ASN number as highlighted in the following screenshot and click **Create Transit Gateway**.

Create Transit Gatew	ay			
A Transit Galoway (TGW) is a network tran	sit hub that interconnects attachment	s (VPCs and VPNs) within the same acc	ount or across accounts.	
Name tag	Citrie-TOW	0		
Description	Citrix Transit Galeway	0		
Configure the Transit Galaway				
Amazon side ASN	65500 <b>O</b>			
DNS support	enable 0			
VPN ECMP support.	i <sup>2</sup> enable 0			
Default route table association	enable 0			
Default route table propagation	H enable O			
Configure sharing options for cros	s account			
Auto accept shared attachments	enable 0			
* Required				Cance Create Transit Gateway

Once the Transit Gateway creation is completed, you can see the status as **Available**.

VPC Dashboard Filter by VPC:	Create Transit Gateway	ions ¥			÷	۰	6
Q Select a VPC	Q, Filter by tags and attributes or	search by keyword		K	< 1 to 1 of 1	> >	A.
■ VIRTUAL PRIVATE     CLOUD	Name - Transit G	ateway ID + Owmer ID	- State -				
security	Citrix-TGW Igw-01871	92c78b28a8c8 558897391706	available				
■ VIRTUAL PRIVATE     NETWORK (VPN)	-						
TRANSIT GATEWAYS	Transit Gateway: tgw-0f87192c7	8b28a8c8					
Transit Gateways	Details Tags Sharing						
Transit Galeway Attachments							
Transit Gateway Route	Transit Gateway ID	<ul> <li>tgw-0f87192c78b28a8c8</li> <li>gwallable</li> </ul>	Owner account ID	558897391706 65500			
Tables	DNS suppor	t enable	VPN ECMP support	enable			
Network Manager	Auto accept shared	disable	Default association route table	enable			
■ TRAFFIC MIRRORING	attachments						
Mirror Sessions	Association route table II	tgw-rtb-0f2c2307c1b642e45	Default propagation route table	enable 🖄			
Mirror Targets	Propagation route table IC	Igw-rtb-0f2c2307c1b642e45					

2. To create the **Transit Gateway Attachments**, navigate to **Transit Gateways > Transit Gateway Attachments** and click **Create Transit Gateway Attachment**.

VPC Dashboard	Create Transit Gateway Attachment Actions *	0 ¢
Q Select a VPC	Q Fiter by tags and attributes or search by keyword	IC < None found >
VIRTUAL PRIVATE	You do not have any Transit Gateway Attachments in this region	
00000	Click the Create Transit Gateway Attachment button to create your first Transit Gateway Attachme	nt
SECURITY	Courts Zerrati Columna Attractments	
VIRTUAL PRIVATE NETWORK (VPN)	Create Inarcal Gateway Attacoment	
TRANSIT GATEWAYS		
Transit Gateways		
Transit Gateway Attachments		
Transit Gateway Route Tables		
Network Manager		
TRAFFIC MIRRORING		
Mirror Sessions		
Mirror Targets		
Mirror Filters		

 Select the Transit Gateway created from the drop-down list and select attachment type as VPC. Provide the attachment name tag and select the VPC ID that you want to attach to the Transit Gateway created. One of the subnets from the selected VPC will be auto selected. Click Create Attachment to attach VPC to the Transit Gateway.

	unit Salevas Abschmed				
Create Transit Gatewa	ay Attachmen				
Saled a Transit Galaxy and the type of all	ladered you enablish to	and a			
Transit Galenay ID*	Quell'102/102644	- a			
Allachment (ge	e MC o Vita O Peering Concellos				
VPC Attachment Select and configure your VPC ellachment					
Attackment name tag	VPC102168	0			
DND response	* max 0				
PM report					
ALC 101	go-850,08147,449348	- C 0			
Setue: Dr.	subset #108030-0170	0 0			
	Availability Jone	Sebrat ID			
	R an end la	NAME DESCRIPTIONS (CAN/1728)	•		
	i weath				

4. After attaching the VPC to the transit gateway, you can see that the **Resource type VPC** got associated to the Transit Gateway.



5. To attach SD-WAN to the Transit Gateway using VPN, select the **Transit Gateway ID** from the drop-down list and select **Attachment type** as **VPN**. Ensure that you select the correct Transit Gateway ID.

Attach a new VPN Customer Gateway by providing the SD-WAN WAN link Public IP address and its BGP ASN Number. Click **Create Attachment** to attach VPN with Transit Gateway.

tered Griene Alecherotic - Garle Tarel Gelon, Alecherot	
Create Transit Gateway Attachment	
Iculta Turat Outroug and the type of adactives ( pro-small life to counts,	
NewsColourg 07 yes/https://vit/NB • 0	
Alastenitis Carlos	
OW Alachmed	
Social areas solations palicing as which as soliding solations palicing that is somed the to samed the to same the top of top of the top of	
Convert Lake 0 = Kang Formation (1995) Market (1995) Ma	
basis PORTa based 1 Generative descent	
Real Public Research	
Pre-alexand/large ter bane(2) Granulating Assessment O	
Report .	Create attachment

6. Once the VPN Attached to the Transit Gateway, you can view the details as shown in the following screenshot:

VPC Dashboard Filter by VPC	Create Transit Gateway Atlachment Actions *	00
Q Select a VPC	Q, Filter by tags and attributes or search by keysord	< < 1 to 2 of 2 > >
VIRTUAL PRIVATE	Name - Transit Gateway attachment ID - Transit Gateway ID - Resource type - Resource ID - State - Associated route table ID	- Association state -
	VPC192.168 tge ettach 05ee985td551728de tge 0e805cl67e306588 VPC vpc 07ec5459659753e evelative tge rb 05e65953227709	essociated
SECURITY	VPN-SCWAN tax-ettach-040057a662aa0dde tax-0e0060017a500668 VPN vpn-0e028de106b40e50 evaluatie tax-etb-005e669652227709	associated
VERTUAL PREVATE NETWORK (VPR)		
Transit Galeways	Transit Gateway Attachment: tow-stoch-04816/e062as0dde	
Attachmente	Details Tax	
Transit Galeway Route Tables		
	Tranal Calment P 104-000 AUDIA AUDIA AUDIA AUDIA	
Network Manager	Transfer Galaxies D. Intro (1997) 2010 Decision and an annual decision of the second decisi	
Network Manager	Transit Generation for Conductor Con	
Network Manager TRAFFIC HIRDRING Mirror Sessions	memory watering adult may be graduated and advances         memory watering adult may be graduated and advances           If assure to year advances         Resource and advances         0.0007/371/30           If assure to year advances         Babe         0.0007/371/30           Resource To year advances         Babe         0.0007/371/30           Resource To year advances         Babe         0.0007/371/30	

7. Under **Customer Gateways**, SD-WAN Customer Gateway and Site-to-Site VPN Connection is created as part of VPN Attachment to Transit Gateway. You can see that the SD-WAN Customer Gateway is created along with the IP address of this Customer Gateway that represents the WAN link Public IP address of SD-WAN.

VPC Dashboard Filter by VPC:	Create Customer Gateway Actions *
Q, Select a VPC	Q. Filer by lags and altributes or search by keyword
VIRTUAL PRIVATE	Name - ID - State - Type - IP Address - BGP ASN - VPC
E SECURITY	SD-WWW-GW cge-0777d2307948ff737 available bsec 1 52.172.195.2 65501 -
VIRTUAL PRIVATE NETWORK (VPN) Customer Gateways	<     Customer Geteway: opv 0777423070a807737
Virtual Private Gateways Site-to-Site VPN Connections	Details Tags D can 077h220Tb487737 Bate webbits
Client VPN Endpoints	Type         ipinc.1         IP Address         52.172.186.2           BCP ASN         65501         VPC         -
Transit Gatoways	Certificate ARN Device -
Transit Geleanay Attachments	
Transit Galeway Route Tables	

8. Navigate to **Site-to-Site VPN Connections** to download **SD-WAN Customer Gateway VPN Configuration**. This configuration file has two IPsec Tunnel details along with the BGP peer information. Two tunnels are created from SD-WAN to Transit Gateway for redundancy.

You can see that SD-WAN WAN link Public IP address was configured as the Customer Gateway Address.

VPC Dashboard Filter by VPC:	Create VPN Connection Download Configuration Actions *		0 ¢ (
Q, Select a VPC	Q. Filter by tags and attributes or search by keyword		< 1 to 1 of 1 > >
VIRTUAL PRIVATE	Name - VPN ID - State - Virtual Private Gateway	- Transit Gateway	- Customer Gateway - Customer Gateway Address
SECURITY	SO-WPN-VPN vpn-0e3/20de100040e50 available -	Igw-0e8060c787e308088	- cgw-0/77d2307ee88737   SD 52 172 190 2
VIRTUAL PRIVATE NETWORK (VPN)	1		
Customer Gateways	VPN Connection: vpn-0e328de16fdb40e50		880
Virtual Private Gateways Site-to-Site VPN Connections	Details Turnel Detaits Tags		
Client VPN Endpoints	VPN ID vpn-0e328de16fdb40e50	State	available
TRANSIT GATEWAYS  Transf Gateways	Virtual Private Gateway - Transit Gateway 10w-0e6bt/5ct87e300568	Customer Gateway Customer Gateway Address	cgw-0777d23079e8#737   SD-WAN-GW 52 172 195 2
Transit Gatoway Attachments	Type (psoc.1 VPC -	Category Routing	VPN Dynamic
Transit Gateway Route	Acceleration Enabled Talse	Authentication Type	Pre Shared Key

9. Click **Download Configuration** and download the VPN configuration file. Select the **Vendor**, **Platform** as **Generic**, and **Software** as **Vendor Agnostic**.

VPC Dashboard Filter by VPC:	Create VPN Connection Download Configuration	Actions ~		
VURTUAL PRIVATE	Name - VPN ID - 5     SD-WW-VPN vpn-0e328de166b40e50 a	tate - Virtual Private Gateway - Transit Gateway valiable - tgw-0e8045c87e300568	<ul> <li>Customer</li> <li>cgw-0777d</li> </ul>	Gateway         *           Customer Gateway Address           I2007968ff737   SD         52:172:195:2
VIRTUAL PRIVATE NETWORK (VPN) Customer Gateways	VPN Connection: vpn 0e328de16fdb40e50	Download Configuration	× stomer gateway	880
Virtual Private Gateways Site-to-Site VPN Connections Client VPN Endpoints	Details Tunnel Details Tags VPN ID vpn-0e328de16fsb4	Vendor Ceneric •	0	170aur#1717 I SD JMAAL02#
TRANSIT GATEWAYS Transit Gateways Transit Gateway Altachments	Transit Cateway Ign=0e8/5ct87e300 Type (psec 1 VPC -	Software [Vendor Agnostic *]		
Transit Gateway Route Tables	Accessration chabled 1850	Cancel	Download	"

The downloaded configuration file contains the following information:

- IKE config
- IPsec configuration for AWS Transit Gateway
- Tunnel interface configuration
- BGP configuration

This information is available for two IPsec tunnels for High Availability (HA). Ensure that you configure both the tunnel end points while configuring this in SD-WAN. See the following screenshot for reference:

#### **Configure Intranet service on SD-WAN**

To configure an Intranet service through Citrix SD-WAN Orchestrator service, go to Delivery services.

#### **Monitoring and Troubleshooting on AWS**

 To verify the IPsec Tunnel establishment status on AWS, Navigate to VIRTUAL PRIVATE NET-WORK(VPN) > Site-to-Site VPN Connections. In the following screenshot, you can observe that the Customer Gateway Address represents SD-WAN Link Public IP address using which you have established tunnel. The Tunnel status is shown as **UP**. Also it can be observed that AWS has learned **8 BGP ROUTES** from SD-WAN. This means SD-WAN is able to establish Tunnel with AWS Transit Gateway and also able to exchange routes over BGP.

for hy VPC	Create VPN Connection	Download Configura	ation Actions ~				a 6
Select a VPC	Q, Filter by tags and attr	butes or search by keyword					K < 1 to 1 of 1
IRTUAL PRIVATE	Name -	VPN ID	State - Virtua	I Private Gateway	- Transit Gateway	Customer Gateway	- Customer Gateway Add
.000	SD-WAN-VPN	pn-0e328de16fdb-10e50	avaiable -		tgw-0e8b#5ct87e309568	cpw-0777d23079w8#737	SD 62.172.195.2
ECURITY							
IRTUAL PRIVATE ETWORK (VPN)							
ustomer Gateways	4						
irtual Private Gateways	VPN Connection: vpn-0	e320de161db40e50					
ite-to-Site VPN onnections	Details Tunnel De	tails Togs					
liont VPN Endpoints	Toronto Banka						
ANSIT GATEWAYS	tunnel state						
ATTIC MIRRORING							< < 1 to 2 of 2 ⇒ >
irror Sessions	Tunnel Number	Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details	Certificate ARN
ing Filters	Tunnel 1	3 133 37 22	169 254 216 176/30	UP	April 15, 2020 M 8:54:05 PM UTC+5:30	8 BGP ROUTES	
	Turneyi 2	13.68.66.104	180 254 123 240/20	DOWN	And 15, 2020 of 12,03,49 PM LITC+	IDSEC IS DOWN	

2. Configure IPsec and BGP details related to the second tunnel based on the downloaded configuration file on SD-WAN.

Dashboard Monit	oring Configuration									
Statistics	Monitoring > Statistics									
Flows										
Routing Protocols	Statistics									
Firewall	Show: IPsec Tunnel 🔹 🗇 (nable Auto Refresh 🗧 💌 seconds: Rafrisch 🕷 Show latest data.									
IKE/1Psec										
IGMP	IPsec Tunnel Statistics									
Performance Reports	Filter: in	Any column	<ul> <li>Apply</li> </ul>							
Qos Reports										
Usage Reports	Show 100 • entries Showi	ng 1 to 2 of 2	entries					First	Previous 1	Next Last
Availability Reports	Name	State	Service Type	Packets Received	Kbps Received	Packets Sent	Kbps Sent	Packets Dropped	Bytes Dropper	d MTU
Applace Reports	New_Intranet_Service+1	GOOD	Intranet	1	0.27	1	0.24	0	0	1434
represente néports	New_Intranet_Service-2	GOOD	Intranet	1	0.27	1	0.24	0	0	1434
DHCP Server/Relay	Showing 1 to 2 of 2 entries							First	Previous 1	Next Last
VRRP										

Status related to both the tunnels can be Monitored on SD-WAN as follows:

3. Status related to both the tunnels can be Monitored on AWS as follows:

VPC Dashboard Filter by VPC:	Create VPN Connec	Download Configura	ation Actions ~					• • • •
Q, Select a VPC	Q, Filter by tags and	attributes or search by keyword					< < 1	to 1 of 1 $>$ >
WIRTUAL PRIVATE	Name -	VPNID	- State - Virtu	al Private Gateway	<ul> <li>Transit Gateway</li> </ul>	· Customer Gateway	~ Customer Ga	teway Address
- CLOOD	SD WAN-VPN	vpn-0e328de16ldb10e50	available -		tgw-0e85/6c/67e309568	cgw-0777d23079e0ff	737   SD 52.172.195.2	
VIRTUAL PRIVATE NETWORK (VPN)								
Customer Geteways								,
Virtual Private Galeways	VPN Connection: vp	m-0e328de16fdb10e50						888
Site-to-Site VPN Connections	Details Tunnel	Details Tags						
Client VPN Endpoints								
	Tunnel State							
TRAFFIC MIRRORING							< < 1 to 2 of	2 > >
Mirror Sessions	Tunnel Number	Outside ID Address	Inside ID CIDD	Status	Status Last Channel	Details	Cartificate ADM	
Mirror Targets	rundet Number	Contende IP Address	make in Clot	warned	contra case crianĝeo	Cetains	Can an Canal ADDN	
Mirror Filters	Tunnel 1	3 133 37 22	169 254 215 176/30	UP	April 16, 2020 M 11 58:30 AM UTC+5	11 BGP ROUTES		
	Tunnol 2	13.58.66.184	169.254.133.240/30	UP	April 16, 2020 at 11.57.33 AM UTC+5	11 BGP ROUTES		

## How to view ipsec tunnel configuration

August 24, 2022

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.

Dashboard Monitoring	Configuration			
+ Appliance Settings	Configuration > Virtual WAN > View Configuration			
- Virtual WAN				
View Configuration	Configuration			
Configuration Editor				
- Change Management	View: Virtual Path Service			
- Change Management Settings				
Restart/Reboot Network	Virtual Path Service Configuration			
Enable/Disable/Purge Flows				
<ul> <li>Dynamic Virtual Paths</li> </ul>	Virtual Path 515 = MCN-5100-8R572			
SD-WAN Center Certificates	Local site=HCN-5100			
+ System Maintenance	Remote site=BR572 Local send rate=20000 kbps			
	Remote send rate=20000 kbps On-demand standby kiN link trigger thresho	old= %		
	IPsec settings <u>e entit</u> Routing Domains Enabled:			
	Default_RoutingDomain PATHS:			
		Primary Primary	Secondary Secondary	Sensitive
	Path ID From Link To Link	Address Address	Address Address Src Port	Diternate Alternate to Dit Port Src Port Dit Port IP DSCP Encrypt Loss Percent
	0 MCN-5100-WL-1 BR572-WL-1	172.111.64.5 172.113.59.5	4980	4980 * ses128 YES -
	1 MCN-5100-WL-1 BR572-WL-2	172.111.64.5 192.113.59.6	4988	4980 * aesi28 YES -
	0 BR572-WL-1 MCN-5100-WL-1	1 172.113.59.5 172.111.64.5	4980	4980 - * aesi28 YES -
	1 BR572-WL-2 MCN-5100-WL-2 1 BR572-WL-1 MCN-5100-WL-2 2 BR572-WL-2 MCN-5100-WL-2	2 192.113.59.5 172.111.65.5 2 172.113.59.5 172.111.65.5	4960 4980	4900 Tesico Yos - 4980 Tesico Yos - 4980 Tesico Yos -
	2 083/248042 064451004804	1 192.113.39.0 172.111.04.3		4500
		ltime Internetive Bulk	Standby Active	
	From Link To Link Elig	gible Eligible Eligible	Group Interval(ms) Interval(ms)	
	MCN-5100-WL-1 BR572-WL-1 YES MCN-5100-WL-2 BR572-WL-2 YES	YES YES YES YES	0 n/a n/a 0 n/a n/a	
	MCN-5108-WL-1 8R572-WL-2 YES MCN-5108-WL-2 8R572-WL-1 YES	YES YES	0 n/a n/a	
	8R572-WL-1 MCN-5100-WL-1 YES 8P572-WL-2 MCN-5100-WL-2 YES	YES YES	0 n/a n/a	
	8R572-WL-1 MCN-5100-WL-2 YES 8R572-WL-2 MCN-5100-WL-1 YES	YES YES	0 n/a n/a	
	Classes on virtual path 'MCN-5100-BR572':			
	Initial Initial Sustain			
	# Type (kbps) (mS) (kbps)	)		
	0 REALTIME 0 0 6000 1 INTERACTIVE 0 0 2800			
	2 INTERACTIVE 0 0 800 3 INTERACTIVE 0 0 200			
	4 BULK 0 0 1			
	6 BULK 0 0 1 7 BULK 0 0 1			
	8 BULK 0 0 1 9 BULK 0 0 1			
	10 REALTINE 0 0 6000 11 INTERACTIVE 0 0 4400			
	12 INTERACTIVE 0 0 3000 13 INTERACTIVE 0 0 1400			
	14 INTERACTIVE 0 0 600 15 BULK 0 0 6600			
	16 BULK 0 0 1			

3. Select **IPsec Tunnels** from the drop-down menu to view the IPsec Tunnel configuration.





	- UDM_AGA_1
Namo	· · · · · · · · · · · · · · · · · · ·
	insec service type=intranet
	ike local in addr=10.0.0.6
	ike remote ip addr=10,101,0,100
	network mtu=1500
	ike version=2
	ike auth-psk
	ike_identity=auto
	ike peer_auth=cert
	ike_validate_peer_identity=1
	ike hash algorithm-sha256
	ike_integ_algorithm=sha256
	ike_encryption_mode=aes256
	ike_dhgroup=group2
	ike_lifetime_s=300
	ike_lifetime_s_max=86400
	ike_dpd_s=300
	ipsec_tunnel_mode=tunnel
	ipsec_tunnel_type=esp_auth
	ipsec_encryption_mode=aes128
	ipsec_hash_algorithm=sha
	lpsec_pfsgroup=none
	ipsec_lifetime_s=28800
	ipsec_lifetime_s_max=86400
	ipsec_lifetime_Kb=0
	ipsec_iiittime_ko_max=v
	Protocial Methodika
	111 10 0.0 0/16 -> 10.101 0.0/16
	$(1)$ 10.4.0.0/16 $\rightarrow$ 10.101.0.0/16
	$(3)$ 10.3.0.0/16 $\rightarrow$ 10.101.0.0/16
	$(4)$ 10,2,0,0/16 $\rightarrow$ 10,101,0,0/16

4. Each virtual path will show its own IPsec tunnel status as shown below.

Dashboard	Monitoring	Configuration	
System Status			
Name:	MCN-5100		
Model:	5100		
Appliance Mode:	MCN		
Serial Number:	4H30GCNPD	)	
Management IP Add	ress: 10.199.107.20	1	
Appliance Uptime:	1 weeks, 3 da	ys, 2 hours, 7 minutes, 28.6 seconds	
Service Uptime:	6 hours, 21 m	inutes, 54.0 seconds	
Routing Domain Enal	bled: Default_Rout	ngDomain	
Software Version: Built On: Hardware Version: OS Partition Version:	10.0.0.193.659091 Feb 17 2018 at 17 5100 4.6	32:45	
Virtual Path Serv	ice Status		
Virtual Path MCN-51	00-BR572:		Uptime: 5 hours, 59 minutes, 34.0 seconds Psec state: 60
Virtual Path MCN-51	00-BR573:		Uptime: 5 hours, 45 minutes, 0.0 seconds. IPsec state: 60
Virtual Path MCN-51	00-BR574:		Uptime: 4 hours, 56 minutes, 48.0 seconds.
Virtual Path 'MCN-51	.00-BR575' is current	y dead.	
Virtual Path MCN-51	00-RCN1-5100:		Uptime: 2 hours, 7 minutes, 3.0 seconds.
Virtual Path 'MCN-51	.00-RCN3-2100' is cu	rrently dead (Configuration version mismatch	0
Virtual Path 'MCN-51	00-KCN3Geo-2100' i	s currently dead.	
virtual Path MCN-51	UU-RUN4-ESXIL IS CU	rrentiy dead.	

## **IPSec monitoring and logging**

#### August 24, 2022

To monitor IPsec/IKE SA statistics:

1. Navigate to Monitor > IPsec. Choose IPsec SAs:

ec SAs							
Select maximum IPSec to d	isplay	✓ Refresh				Search	Q
Name 0	Service Type 🛛 🗧	Intranet Service Type 🔅	SPI	Direction 0	Host		Peer
IPv61-Tunnel_IPv61-Tunnel	Intranet	Default	f18c41a5	IN	fdf8:f::100		fdf8:cc::10
IPv61-Tunnel_IPv61-Tunnel	Intranet	Default	c5bf208c	OUT	fdf8:cc:10		fdf8:f=100
IPv62-Tunnel_IPv62-Tunnel	Intranet	Default	cdd241d7	OUT	edf8:cb:10		edf8:f:100
IPv62-Tunnel_IPv62-Tunnel	Intranet	Default	68468e4f	IN	edf8:f:100		edf8:cb:10

2. Navigate to **Monitor** > **IKE SAs**. Observe the configured IPsec tunnels, the IKE and IPsec service associations between two or mode VPN endpoints configured within the SD-WAN network.

IKE	SAs						
	Select maximum IKE to disp	olay	~ Refresh			Search	Q
	Name 0	Service Type 0	Intranet Service Type	Initiator Cookie	Responder Cookie	Host	
	IPv61-Tunnel_IPv61-Tunnel	Intranet	Default	5476506b6a5df0cf	0876d5a5e792790d	fdf8:cc::10:4500	
	IPv62-Tunnel_IPv62-Tunnel	Intranet	Default	b609da9c78244d04	95eb4dd7a3480166	edf8:cb:10:4500	

### How to monitor IPsec logs

- 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

Dashboard	Monitoring	Configuration										
- Appliance Settings		Configuration >	Appliance Settings >	Logging/Monitoring								
Administrator in	errace	Log Ontions	Alert Options	Alarm Ontions	Suclog Server	HTTP Server	Application					
Network Adapte	~	Log options	Alert Options	Alarin options	Systog Server	TITTF Server	Application					
Net Flow	3	View Log File										
App Flow/IPFIX												
SNMP		Only the most	ecent 10000 entries	will be shown and filt	ered. To view the fu	ll log, download an	nd open it locally.					
NITRO API												
Licensing		Filename:	SDWAN_security.log	~								
Default/Fallback	Config	Filter (Optional):										
+ Virtual WAN		View Log										
+ System Maintenand	e											
		Download Log	File									
		Filename:	SDWAN_security.log	· ~								
		Download Log										
		bennedd tog										
322-07-23T13:03:51.11	5798+0000 INFO	Log file opened										
022-07-23T13:04:09.12	0692+0000 INFO	tvp_set_packet_virtual	path_and_path_num_a	nd_learn@control/tvp	.c:1326 TVP set v	irtual path_id=0x2	path_num=0 for	site HAMCN,	from [fdf8:ab:	:10]:4980 t	to [fdf8:cb::	10]:4980
2022-07-23T13:04:45.12	8635+0000 INFO	tvp_set_packet_virtual	path_and_path_num_a	nd_learn@control/tvp	.c:1326 TVP set v	intual path_id=0x2	path_num=2 for	site HAMCN,	from [fdf8:ac:	:10]:4980 t	to [fdf8:cb::	10]:4980
2022-07-23T13:05:39.14	1415+0000 INFO	tvp_set_packet_virtual ***Pre	vious log entry was	repeated 1 times ove	r the last 54013327	uS (54.01 Seconds	()	site union,	from [fdf0.ek.	.10].4000 4		10].4900
222-07-23113:05:57.14	5423+0000 INFO	tvp_set_packet_virtual	path_and_path_num_a	nd_learn@control/tvp	.c:1326 TVP set v	irtual path_id=0x2	path_num=0 for	site HAMCN,	from [fdf8:ab:	:10]:4980 t	to [fdf8:cb::	10]:4980
2022-07-23T13:06:22.07 2022-07-23T13:06:22.07	3213+0000 INFO 3213+0000 INFO	***Pre set_next_dh_key@forwar	/ious log entry was J/virtual path_servi	repeated 1 times ove ce/crypto.c:4647	r the last 42932356 ECDH complete for	uS (42.93 Seconds remote site HAMCN	i)					
022-07-23T13:06:33.15 022-07-23T13:06:51.15	1524+0000 INFO 220+0000 INFO	<pre>tvp_set_packet_virtual tvp_set_packet_virtual</pre>	path_and_path_num_a path_and_path_num_a	nd_learn@control/tvp nd_learn@control/tvp	.c:1326 TVP set v .c:1326 TVP set v	irtual path_id=0x2 irtual path_id=0x2	<pre>2 path_num=0 for 2 path_num=0 for</pre>	site HAMCN, site HAMCN,	from [fdf8:ab: from [fdf8:ab:	:10]:4980 t :10]:4980 t	to [fdf8:cb:: to [fdf8:cb::	10]:4980 10]:4980
022-07-23T13:07:45.17	2772+0000 INFO 2772+0000 INFO	***Pre tvp set packet virtual	vious log entry was path and path num a	repeated 2 times ove nd learn@control/tvp	r the last 72018990 .c:1326 TVP set v	uS (72.02 Seconds irtual path_id=0x2	) 2 path_num=2 for	site HAMCN.	from [fdf8:ac:	:10]:4980 1	to [fdf8:cb::	10]:4980
022-07-23T13:08:03.17	7053+0000 INFO	tvp_set_packet_virtual	path_and_path_num_a	nd_learn@control/tvp	.c:1326 TVP set v	irtual path_id=0x2	path_num=0 for	site HAMCN,	from [fdf8:ab: from [fdf8:ab	:10]:4980 t	to [fdf8:cb::	10]:4980
022-07-23T13:08:57.19	260+0000 INFO	***Pre	vious log entry was	repeated 1 times ove	r the last 54013936	uS (54.01 Seconds	() ()					

## 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.

Dashboard Monite	oring	Configuration										
- Appliance Settings		Configuration >	Appliance Settings >	.ogging/Monitor	ng							
- Administrator Interface												
Logging/Monitoring		Log Options	Alert Options	Alarm Option	s Syslog Server	HTTP 5	erver Application					
Network Adapters		Email Alarta										
Net Flow		Email Alerts										
App Flow/IPFIX		🗹 Enable Emai	l Alerts			Send Test Em	ail					
NITRO API												
Licensing		Destination Emai	il Address(es):									
Default/Fallback Config		SMTP Server Hos	stname or IP Address:			-	-					
+ Virtual WAN		SMTP Server Por	t									
+ System Maintenance		Source Email Ad	dress:			-						
		You may enter m	ultiple destination email	addresses separate	d with semicolons (;)							
				En	able SMTP Authentication							
		SMTP User Name	P:									
		SMTP Password:										
		Verify SMTP Pass	word:									
		General Event	Configuration									
												?
2	Event Type	e	Alert if State Persists	Email	Email Severity Filter	Syslog	Syslog Severity Filter	SNMP	SNMP Severity Filter	нтт	HTTP Severity Filter	
	SERVICE		0		Warning	~	Warning	~	Warning	~	Warning	~
	VIRTUAL PA	đН	0		Warning	~ 0	Warning	~ 0	Warning	~ 0	Warning	~
	WAN LINK		0		Warning	× •	Warning	~ 0	Warning	~ 0	Warning	~
	PATH		0		Warning	×	Warning	× п	Warning	~ n	Warning	~
	DYNAMIC	(DTUAL DATH	0		Warning		Woming		Warning		Maming	
	DINAMIC		0		warning	•	warning		wanning			
	WAN_LINK_	CONGESTION	U		vvarning	× .	vvarning		vvarning		vvarning	~
	USAGE_CON	NGESTION	0		Warning	~	Warning	~	Warning	~	Warning	~
	HARD_DISK				Warning	~	Warning	× 🗆	Warning	~ □	Warning	~
	APPLIANCE				Warning	~	Warning	~	Warning	~	Warning	$\sim$
	USER EVEN	т			Warning	<b>~</b>	Warning	~ O	Warning	~ 0	Warning	~
	CONFIG_UP	PDATE			Warning	~	Warning	~ 🗆	Warning	~	Warning	~
	SOFTWARE,	_UPDATE			Warning	~ 0	Warning	~ O	Warning	~ 0	Warning	~
	PROXY_ARP	,			Warning	~ 0	Warning	~ 0	Warning	~ 0	Warning	~
	PROXY ND	р			Warning	~ 0	Warning	~ 0	Warning	~ 0	Warning	~
	ETHERNET				Warning	~	Warning	V 0	Warning	~ •	Warning	
	WATCHDOG			_	Warning		Warning		Warning		Warning	~
	ADDUALSE	GETTINGS UPS T			Warning		Mamina		Mamina		Mamina	
	APPLIANCE,	S			Warning	~ 0	Warning	~ 0	Warning	~ 0	Warning	~
	APPLIANCE DISCOVERE	G _SETTINGS_UPDATE ID_MTU			Warning Warning	<ul><li></li><li></li><li></li></ul>	Warning Warning	<ul><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li></ul>	Warning	~ 0 ~ 0	Warning	~
	APPLIANCE DISCOVERE GRE_TUNNI	S _SETTINGS_UPDATE ID_MTU EL			Warning Warning Informational	<ul><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li></ul>	Warning Warning Warning	<ul><li>✓</li><li>✓</li><li>✓</li><li>✓</li><li>✓</li></ul>	Warning Warning Warning	<ul> <li></li> &lt;</ul>	Warning Warning Warning	~
	APPLIANCE DISCOVERE GRE_TUNNE IPSEC_TUNNE	S _SETTINGS_UPDATE D_MTU EL NEL			Warning Warning Informational	<ul> <li></li> &lt;</ul>	Warning Warning Warning Warning		Warning Warning Warning Warning		Warning       Warning       Warning       Warning	~ ~ ~

## 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.

Dashboard Monitoring	Configuration	
+ Appliance Settings	Computation > System Naintenance > Diagnostics	
= Sustan Maintanana	Ping         Traceroute         Packet Capture         Path Bandwidth         System Info         Diagnostic Data         Events         Alarms         Diagnosticit Tool	
Delete Files	Incert Event	
Restart System		_
Date/Time Settings	Object Type: USER EVENT •	
Diagnostics	Event type: UNDEFINED •	
Update Software	Severity DEBUG •	
Configuration Reset	Add Event	
Factory Reset	Download Events	
	There are currently 487678 in the Events database, spanning from event 183412 at 2018-01-18 18:2455 to event 671289 at 2018-02-17 18:14:15	_
	You can download some or all of them in CSV format. You may with to limit the amount to download because some common spreadheet programs limit you to 6538 rows.	
	Alert Count	
	Alert Type Alerts Sent	
	Enair:         0           Stato Metaas:         0	
	SNMP Traps: 0	
	View Events	
	Quantific 25 V	
	Filter: Object Type = Any   Event type = Any  Ev	
	Reload Events Table	
	ID Deject Name Object Time Event Type Severity Description	
	671289 0 MCN-5100-WL-1->BR572- PATH 2018-92-17 GOOD NOTC: Virtual path MCN-5100-BR572 Path MCN-5100-WL-1->BR572-WL-1 state has changed from BAD to GOOD because by peer.	e notified
	871288         1         MCN-S100-WL-1->BR572- WL-2         PATH         2018-02-17 181-1415         GOOD         NOTICE         VTrue path MCN-S100-BR572 Path MCN-S100-BR572-VWL-2 state has changed from BAD to GOOD because the path MCN-S100-WL-1->BR572-WL-2 state has changed from BAD to GOOD because	e notified
	671287 0 MCN-5100-WL-1->88574- PATH 2018-92-17 GOOD NOTCE Virtual path MCN-5100-88574 Path MCN-5100-88574-WL-1 state has changed from BAD to GOOD becaus	e notified
	671286 2 MX-15100-WL-2->BR572- PATH 151/814 GOOD NOTICE Virtual path MCN-5100-BR572 Path MCN-5100-WL-2->BR572-WL-1 state has changed from BAD to GOOD becaus https://www.action.org/action	e notified
	671285 1 MR-79-5100-WL-1->88572- PATH 2018-92-17 BAD NOTICE Virtual Path MCN-5100-88572 Path MCN-5100-WL-1->88572-WL-2 state has changed from GOOD to BAD becaus	e notified
	11224 0 MCN-5100-WL-1->BR572- PATH 2018-02-17 BAD NOTCE Virtual Path MCN-5100-BR572 Path MCN-5100-BR572-WL-1->BR572-WL-1 tate has changed from GOOD to BAD becaus	e notified
	VIC-1 18.4.MO V/VIC-1-> 8R574	e notified
	WU-1 48.44VH of years any MCN-1810-WL-2-98.8572- partu 20.86-21.7 partu AVM CV-1010-86572 Path MCN-5100-88.572 Path Path Path Path Path Path Path Path	e notified
	VILL         WIL1         MICH 5100-WIL2-98573           VILL         MICH 5100-WIL2-98573         MICH 5100-WIL2-98573           VILL         MICH 5100-WIL2-98573         MICH 5100-WIL2-98573	e notified
	VIIILE 3 WL-2 PAIN 18:13:17 USOU NOTE by period to the second sec	e notified
	011200 1 WL-2 PAIN 181317 0000 NOILE by per MCN-5100-WL-1-98574 - 2018-0-17 Virtuel Path MCN-5100-88574 Path MCN-5100-88574 WL-2 state has changed from BAD to GOOD because	e notified
	8/12/9 1 WL-2 PAIN 181337 GOOD NOILE by per MINIS100.88574 WL-1 state has channel from B4D to (OOD heaving	te notified
	871278 2 W-1 PATH 181337 GOOD NOTICE by perf. W-N 100 W 2, 28572 2004 2017 View Berk MrN, 100 28772 Berk M	a notified
	6/12/7 2 Wu-1 Microsoft PATH 18:13:06 BAD NOTICE by parts in the control of the c	e notified
	671276 1 WL-2 2007 C2-07872-2 PATH 12:1368 BAD NOTCE WILd Plan Increased Plan Inc	enouned
	671275 3 ML-2124/ML-224/BL-212	enouned
	671274 1 MCR-3L0U-WC-L->BK3/4- PATH 2018-02-17 BAD NOTICE WINAWARM MCR-3L0U-BK3/4-Yah MCR-3L0U-BK3/4	e notified
	671273 3 MCN-5100-WL-2->8K5/4- PATH 2016-92-17 GOOD NOTICE VITUAL PAIM MCN-5100-3K5/4 Path MCN-5100-3K5/4	a notified
	671272 0 MCN-5100-WL-1->8R574 PATH 2018-02-17 GOOD NOTICE Virtual Path MCN-5100-WL-1->8R574-WL-1 state has changed from 8AD to GOOD becaus by peer.	e notified
	671271 1 MCIV-5100-WL-1->88572- PATH 2018-02-17 GOOD NOTICE Virtual Path MCIV-5100-88572 Path MCIV-5100-WL-1->88572-WL-2 state has changed from 84D to GOOD because by peer.	e notified
	671270 1 MCN-5100-WL-1->88572- PATH 2018-02-17 BAD NOTICE Virtual Path MCN-5100-88572 Path MCN-5100-WL-1->88572-WL-2 state has changed from GOOD to BAD because by peer.	e notified
	671269 0 MCN-5100-WL-1->88574- PATH 2018-02-17 BAD NOTICE Virtual Path MCN-5100-88574 Path MCN-5100-WL-1->88574-WL-1 state has changed from GOOD to BAD because by peer.	e notified
	671268 3 MCN-5100-WL-2->BR574- PATH 2018-02-17 BAD NOTICE Virtual Path MCN-5100-BR574 Path MCN-5100-WL-2->BR574-WL-2 state has changed from GOOD to BAD because by peer.	e notified
	671267 1 MCN-5100-WL-1->BR573- PATH 2018-02-17 GOOD NOTICE Virtual Path MCN-5100-BR573 Path MCN-5100-WL-1->BR573-WL-2 state has changed from BAD to GOOD because by peer.	e notified
	671266 3 MCN-5100-WL-2->8R572- PATH 2018-02-17 GOOD NOTICE Virtual Path MCN-5100-8R572 Path MCN-5100-WL-2->8R572-WL-2 state has changed from BAD to GOOD becaus	e notified
	671265 1 MCN-5100-WL-L->88573- PATH 2018-02-17 BAD NOTICE Virtual Path MCN-5100-88573 Path MCN-5100-WL-L->88573-WL-2 state has changed from GOOD to BAD becaus	e notified

# Eligibility for ipsec non-virtual path routes

## August 24, 2022

In previous releases, ipsec tunnel routes would remain in the route table, even if the tunnel became unavailable.

#### Citrix SD-WAN 11.5

Monitoring	>	Statistics

		_								
Show:	Routes	٠	Enable Auto Refresh	5	٠	seconds	Refresh	1	Clear Counters on Refresh	Purge dynamic routes

Route Statistics

Routes for routing	domain : Defau	It_RoutingDomain

Filter:		in Any column	<ul> <li>Apply</li> </ul>												
Show 1	00 • entries Sho	owing 1 to 13 of 13 entries	1											First Previous	1 Next Last
Num <sup>*</sup>	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Туре	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.186.120.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11369	YES	N/A	N/A
1	172.186.50.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-		5	0	YES	N/A	N/A
2	172.186.40.0/24	*	Local	Default_LAN_Zone	YES		DC	Static	-		5	11389	YES	N/A	N/A
з	172.186.75.0/24	*	DC-BRANCH2	Default_LAN_Zone	YES		BRANCH2	Static	-		5	0	YES	N/A	N/A
4	172.186.30.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-		5	0	YES	N/A	N/A
5	172.186.20.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
6	172.185.160.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	155.155.155.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	172.186.30.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES		DC	Static	-		15	0	YES	N/A	N/A
9	172.186.20.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	•	15	0	YES	N/A	N/A
10	16.16.0.0/16	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	÷	6	0	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-		16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

## **FIPS Compliance**

#### August 24, 2022

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 Orchestrator service, see FIPS mode.

## **Citrix SD-WAN secure web gateway**

August 24, 2022

To secure traffic and enforce policies, enterprises often use MPLS links to backhaul branch traffic to the corporate data center. The data center applies security policies, filters traffic through security appliances to detect malware, and routes the traffic through an ISP. Such backhauling over private MPLS links is expensive. It also results in significant latency, which creates a poor user experience at the branch site. There is also a risk that users bypass your security controls.

An alternative to backhauling is to add security appliances at the branch. However, the cost and complexity increases as you install multiple appliances to maintain consistent policies across the sites. And if you have many branch offices, cost management becomes impractical.

### Zscaler:

The ideal solution to enforce security without adding cost, complexity, or latency is to route all branch Internet traffic from the Citrix SD-WAN appliance to the Zscaler Cloud Security Platform. You can then use a central Zscaler console to create granular security policies for your users. The policies are applied consistently whether the user is at the data center or a branch site. Because the Zscaler security solution is cloud based, you don't have to add more security appliances to the network.

### **FIPS Compliance:**

The National Institute for Standards and Technology (NIST) develops Federal Information Processing Standards (FIPS) in areas for which no voluntary standards exist. FIPS addresses the following issues:

- Compatibility between different systems.
- Data and software portability.
- Cost-effective computer security and privacy of sensitive information.

FIPS specifies the security requirements for a cryptographic module used in security systems. To apply these security standards to the processing done by a Citrix SD-WAN appliance, configure FIPS mode.

### Forcepoint:

By using Citrix SD-WAN, you can use the Firewall redirect (transparent proxy by Destination NAT) feature to redirect internet (HTTP and HTTPS) traffic from an SD-WAN appliance at the enterprise edge to the Forcepoint cloud-hosted security module. You can redirect HTTP traffic from port 80 to port 8081 and HTTPS traffic from port 443 to port 8443 of the nearest Forcepoint cloud proxy server.

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

### August 24, 2022

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



#### CURRENT DEPLOYMENT MODEL WITH ON-PREMISE FIREWALL



ZSCALER SECURITY AS SERVICE DEPLOYMENT MODEL

To use GRE tunnel or IPsec Tunnel traffic forwarding:

- 1. Log into the Zscaler help portal at: https://help.zscaler.com/submit-ticket.
- 2. Raise a ticket and provide the static public IP address, which is used as the GRE tunnel or IPsec tunnel source IP address.

Zscaler uses the source IP address to identify the customer IP address. The source IP needs to be a static public IP. Zscaler responds with two ZEN IP addresses (Primary and Secondary) to transmit traffic to. GRE keep alive messages can be used to determine the health of the tunnels.

Zscaler uses the source IP address value to identify the customer IP address. This value must be a static public IP address. Zscaler responds with two ZEN IP addresses [DR1] to which to redirect traffic. GRE keep-alive messages can be used to determine the health of the tunnels.

## Sample IP addresses

### Primary

Internal Router IP address: 172.17.6.241/30 Internal ZEN IP address: 172.17.6.242/30

### Secondary

Internal Router IP address: 172.17.6.245/30 Internal ZEN IP address: 172.17.6.246/30

### **Configuring an Internet Service**

To configure an internet service through Citrix SD-WAN Orchestrator service, see Delivery services. For more information about enabling Internet service for a site, see Direct Internet Breakout.

## **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 through Cirix SD-WAN Orchestrator service, see 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 match the default route 0/0 and be transmitted over the GRE tunnel. Ensure that the 0/0 route used for [DR1 the GRE tunnel has a lower Cost than Passthrough or any other Service type.
- Similarly, the backup GRE tunnel to Zscaler must have a higher cost than that of the Primary GRE tunnel.
- Ensure that nonrecursive routes exist for the ZEN IP address.

#### 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.

To monitor GRE and IPsec tunnel statistics:

In the SD-WAN web interface, navigate to IPsec Tunnel]. Monitoring > Statistics > [GRE Tunnel

For more information, see; monitoring IPsec tunnels and GRE tunnels topics.

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

### August 24, 2022

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<sup>1</sup>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.

You can configure NAT using Citrix SD-WAN Orchestrator service. For more information, see Network address translation.



## 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.

Dashboard	Ionitoring Configuration														
Statistics	Montoring > Firewall	٦													
Flows															
Routing Protocols	Firewall Statistics														
Firewall	Satirica: NAT Poloies *														
IKE/IPsec	NACTURE enterne enterne 50 v od oppige: NAT: IP Protocol: Any v NAT Type: Any v Service Type: Any v Service Name: Any v														
IGMP															
Performance Reports	Service Type: Any V Service Name: Any V Inside IP: * Inside Port: * Outside Port: * Outside IP: * Inside IP: * Outside Port: *														
Qos Reports	Inside Port: " Janide Port: " Outside Pr: " Outside Port: " Outside Pr: " Outside Port: "														
Usage Reports															
Availability Reports	NAT Policies														
Appliance Reports	Inside Outside	1													
DHCP Server/Relay	ID         Rule Type         Parter         IP         Service         Service         Service         Service         Service         Service         Related         Parkets         Parkets         Dytes Service         Related         Related         Parkets         Dytes Service         Related         Rela														
VRRP	1 Dynamic PR - Outbound * Internet - * * 17216.2.10.1/32 0-45535 No No No 253825 26477410 452874 614179776 3 [Connections	1													
	NAT Policies Displayed: 1 NAT Policies In Use: 1/100 Port Restricted Dynamic NAT Policies In Use: 1/100 Destination NAT Policies In Use:0/100														

Dashboard Monito	ring Configuration												
Statistics	Monitoring > Firewall												
Flows													
Routing Protocols	Firewall Statistics												
Firewall	Statistics: Connections V	]											
IKE/IPsec	Maximum entries to display: Filter Policies												
IGMP	Filtering: A NAT Policies	Any	▼ Fi	amily:		Any	•						
Performance Reports	IP Protocol:	Any	▼ 5	ource Zone:		Any	▼ Destinatio	n Zone: Any			•		
Qos Reports	Source Service 1	ype: Any	• •	ource Service	e Instance:	Any V	Source IP:	- TP: (*			Source Port:	n n n n n n n n n n n n n n n n n n n	
Usage Reports	Refresh Show latest o	tata Show Dro	• 0	escination se	ervice instan	Ally •	Descinacio				Destination	ora	
Availability Reports	Clear Connections												
Appliance Reports	Help												
DHCP Server/Relay	Connections												
VRRP						Source				D	estination		
			IP		Service					Service			
	Application	Family Pr	otocol IP Adress	Port	Туре	Service Name	Zone	IP Address	Port	Туре	Service Name	Zone	State
	Domain Name Service(dns)	Network Service U	IDP 172.16.6.1	10 36080	Virtual Path	DC-MCN-BR1-CB2000	Default_LAN_Zone	10.140.50.5	53	Internet	DC-MCN-Internet	Internet_Zone	ESTABLISHED
	Domain Name Service(dns)	Network Service U	IDP 172.16.16	1 56451	Virtual Path	DC-MCN-BR1-CB2000	Default_LAN_Zone	10.140.50.5	53	Internet	DC-MCN-Internet	Internet_Zone	ESTABLISHED

## **Palo Alto integration using IPsec tunnels**

#### August 24, 2022

Palo Alto networks deliver cloud-based security infrastructure for protecting remote networks. It provides security by allowing organizations to set up regional, cloud-based firewalls that protect the SD-WAN fabric.

Prisma Access service for remote networks allows you to onboard remote network locations and deliver security for users. It removes the complexity in configuring and managing devices at every remote location. The service provides an efficient way to easily add new remote network locations and minimize the operational challenges with ensuring that users at these locations are always connected and secure, and it allows you to manage policy centrally from Panorama for consistent and streamlined security for your remote network locations.

To connect your remote network locations to the Prisma Access service, you can use the Palo Alto Networks next-generation firewall or a third-party, IPSec-compliant device including SD-WAN, which can establish an IPsec tunnel to the service.

- Plan the Prisma Access Service for Remote Networks
- Configure the Prisma Access Service for Remote Networks
- Onboard Remote Networks with Configuration Import

The Citrix SD-WAN solution already provided the ability to break out Internet traffic from the branch. This is critical to delivering a more reliable, low-latency user experience, while avoiding the introduction of an expensive security stack at each branch. Citrix SD-WAN and Palo Alto Networks now offer distributed enterprises a more reliable and secure way to connect users in branches to applications in the cloud. Citrix SD-WAN appliances can connect to the Palo Alto cloud service (Prisma Access Service) network through IPsec tunnels from SD-WAN appliances locations with minimal configuration.

## **Stateful Firewall and NAT Support**

### August 24, 2022

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

### Note

It is not recommended to use firewall in Fail-to-Wire inline mode due to security reasons.

## **Global firewall settings**

August 24, 2022

Once you have created the firewall policy templates you can use this policy to configure firewall settings for Citrix SD-WAN Network. Using the Global firewall settings, you can configure the global firewall parameters, these settings are applied to all the sites on the virtual WAN network.

## **Advanced firewall settings**

August 24, 2022

You can configure the advanced firewall settings for every site individually. This will override the global settings.

To configure advanced firewall settings at the site level, see Firewall settings.

## Zones

August 24, 2022

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 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.



## Policies

August 24, 2022

Policies provide the ability to allow, deny, reject, or count and continue specific traffic flows. You can configure Firewall policies through Citrix SD-WAN Orchestrator service. For more information, see Firewall policies.

## **Network Address Translation (NAT)**

### August 24, 2022

Network Address Translation (NAT) performs IP address conservation to preserve the limited number of registered IPv4 addresses. It enables private IP networks that use unregistered IP addresses to connect to the Internet. The NAT feature on Citrix SD-WAN connects your private SD-WAN network with the public internet. It translates the private addresses in the internal network into a legal public address. NAT also ensures extra security by advertising only one address for the entire network to the internet, hiding the entire internal network. Citrix SD-WAN supports the following NAT types:

- Static one-to-one NAT
- Dynamic NAT (PAT- Port Address Translation)
- Dynamic NAT with Port Forwarding rules

## Note

The NAT capability can only be configured through Citrix SD-WAN Orchestrator service 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. For more information, see Network address translation.

## **Static NAT**

### August 24, 2022

Static NAT is a one-to-one mapping of a private IP address or subnet inside the SD-WAN network to a public IP address or subnet outside the SD-WAN network. Configure Static NAT by manually entering

the inside IP address and the outside IP address to which it has to translate. You can configure Static NAT for the Local, Virtual Paths, Internet, Intranet, and Inter-routing domain services.

## Inbound and Outbound NAT

The direction for a connection can either be inside to outside or outside to inside. When a NAT rule is created, it is applied to both the directions depending on the direction match type.

- Inbound: The source address is translated for packets received on the service. The destination
  address is translated for packets transmitted on the service. For example, Internet service to
  LAN service –For packets received (Internet to LAN), the source IP address is translated. For
  packets transmitted (LAN to Internet), the destination IP address is translated.
- Outbound: The destination address is translated for packets received on the service. The source
  address is translated for packets transmitted on the service. For example, LAN service to Internet service –for packets transmitted (LAN to Internet) the source IP address is translated. For
  packets received (Internet to LAN) the destination IP address is translated.

## **Zone Derivation**

The source and destination firewall zones for the inbound or outbound traffic should not be the same. If both the source and destination firewall zones are the same, NAT is not performed on the traffic.

For outbound NAT, the outside zone is automatically derived from the service. Every service on SD-WAN is associated to a zone by default. For example, Internet service on a trusted internet link is associated with the trusted internet zone. Similarly, for an inbound NAT, the inside zone is derived from the service.

For a Virtual path service NAT zone derivation does not happen automatically, you have to manually enter the inside and outside zone. NAT is performed on traffic belonging to these zones only. Zones cannot be derived for virtual paths because there might be multiple zones within the Virtual path subnets.

## Static NAT Policies for IPv6 Internet service

Citrix SD-WAN supports static NAT policies for IPv6 Internet service from release 11.4.0 onwards. A static NAT policy for IPv6 Internet service specifies the mapping of an inside network prefix to an outside network prefix. The number of static NAT policies required depends on the number of inside networks and the number of outside networks (WAN links). If there are **M** number of inside networks and **N** number of WAN links, then the number of static NAT policies required is **M x N**.

From Citrix SD-WAN release 11.4.0 onwards, while creating a static NAT policy, you can either enter the outside IP address manually or enable **Autolearn via PD**. When **Autolearn via PD** is enabled, the Citrix SD-WAN appliance receives delegated prefixes from the upstream delegating router through DHCPv6 Prefix Delegation. Before Citrix SD-WAN release 11.4.0, the outside IP address was derived from the service automatically and there was no option to enter the outside IP address manually. If you are upgrading an appliance to 11.4.0 or a later release and have static NAT policies configured for IPv6 Internet service, then you must manually update the policies.

### **Configuration example**

In the following topology, the Citrix SD-WAN appliance is configured with 2 inside networks and 2 WAN links:

- Inside network 1 resides in the CORPORATE routing domain with network prefix FD01:0203:6561::/64
- Inside network 2 resides in the Wi-Fi routing domain with network prefix FD01:0203:1265::/64
- Through WAN Link 1, the SD-WAN appliance receives from the upstream delegating router through DHCPv6 Prefix Delegation, 2 delegated prefixes 2001:0D88:1265::/64. These 2 delegated prefixes are used as the outside network prefixes when the traffic from the inside networks transits WAN link 1.
- Through WAN Link 2, the SD-WAN appliance receives from the upstream delegating router through DHCPv6 Prefix Delegation, 2 delegated prefixes 2001:DB8:8599::/64. These 2 delegated prefixes are used as the outside network prefixes when the traffic from the inside networks transits WAN link 2.



In this scenario, there are M=2 inside networks and N=2 WAN links. Therefore, the number of static NAT policies required for proper deployment of IPv6 Internet service is  $2 \times 2 = 4$ . These 4 static NAT policies specify the address translation for:

- Inside network 1 through WAN link 1
- Inside network 1 through WAN link 2
- Inside network 2 through WAN link 1
- Inside network 2 through WAN link 2

### Monitoring

To monitor NAT, navigate to **Monitoring** > **Firewall Statistics** > **Connections**. For a connection you can see if NAT is done or not.

Dashboard	Monitoring	Configuration																						
Monitoring > Fir	critering > Firewall																							
Firewall Statist	tics																							
Statistics:	Connections •																							
Maximum entries to display:	winner methics 50 • ering: Application: Any • Family: Any •																							
Filtering:	rring: Application: Any  Family: Any  IP Protocol: Any  Source Zone: Any  Destination Zone: Any																							
	IP Protocol: Any Destination Zone: Any Destination Zone: Any																							
	Source Service Type: Any  Source Service Instance: Any  Source IP:  Source Port:																							
	Source Sarvice Type:     Any     Source Sarvice Instance:     Any     Source IP:     *     Source Port:       Destination Service Type:     Any     Destination Service Instance:     Any     Destination IP:     *     Destination Port:																							
Refresh	Show latest da	ata 🔲 Show	w Addition:	al Stats																				
Clear Connections																								
Help																								
Connections																								
						Sou	rce				Desti	nation			_		Sen				Receiv	red		
Appli	cation	Family	IP Protocol	IP Adress	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS	kbps	Age (s)
Internet Control Me	essage Protocol(icmp)	Network Service	ICMP	172.57.79.179	3261	Local	Guest_ite_rd	Default_LAN_Zone	172.57.70.176	3261	Internet	MCN-PA-Internet	Internet_Zone	ESTABLISHEE	Yes	6	504	1.004	0.675	6	504	1.004	0.675	6
Connections Display Connections In Use:	ed: 1 1/128000																							•

To check if Auto-learn via PD is configured for any NAT rule, navigate to **Configuration > Virtual WAN > View Configuration** and choose **Firewall** from the **View** drop-down list. **Auto-learn via PD** and **PD prefix ID** columns display the details.

Interval (s)	Source Firewall Zone	Source Service Type	Source Service Inst-	ance Source IP Address	Source Port	Source ICMP Type	Source ICMP Code	e Destination Firevall Zone	Destination Service Type	Destination Service Instance	Destination I
0											
		ANY									
	Untrusted_Internet_Ione	INTERNET									
		INTERNET									
	Untrusted_Internet_Bone	INTERNET									
		INTERNET									
											*************
	/ = h	Teelds Bigmunll Rees	Tee/de 10 144		Xanida Bee	and the second second	a an needly th	destaids Rissen11 Assa	ferbalde ID bddares		
11 900 1	258	Inside Firewall bone	188100 IP A00	cess	TURIDE POE	Ward-Teatu AT# 1	O PD Pretia ID	Outside Firewall zone	Outside IP Address	Outside Port	
0365+3-10	r_1	DC 155 Free Defeult	2006 /64		0	Yes	1	Detroyated Televent Tens			
034312-4	P.41	oc_oss-roos_osteric	200411764		0	No		Control Coloring Loope			
					ő	No	ő	Detroated Televiset Tone	11/128		
					ő	No	ő		/32	, in the second s	
						No	ő		/128		
					53				9.9.9.9	53	
					53				149.112.112.112	53	
						L					

To further see the inside IP address to outside IP address mapping, click **Post-Route NAT** under **Re-lated Objects** or navigate to **Monitoring > Firewall Statistics > NAT policies**.

The following screenshot shows the mapping of inside address to outside address in an IPv4 static NAT policy.

#### Citrix SD-WAN 11.5

	_	_																
Dashboard	Monitor	ring	Configurati	n														
Market A	C	_																
Monitoring >	Firewall																	
Firewall Sta	atistics																	
Statistics:	NAT Policies																	
Maximum entries to display:	50 •																	
NAT:	IP Protocol:	1	Any		NAT Type:	Any	۲	Dynamic NA	Type:	Any	•							
	Service Type	e /	Any	•	Service Name:	Any 🔻												
	Inside IP:	*			Inside Port:	*		Outside IP:			Outside	Port: *						
Refresh	Show lat	est data.																
Help																		
NAT Policie	25																	
						Inside		Outside										
ID Rule Type	Rule Parent	Direction	IP Protocol	Service Type	Service Name	IP Address	Port	IP Address	Port	llow Related	Allow IPSec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received	Bytes Received	Connections	Related Objects
1 Static		Outbound		Internet		172.57.79.179/	32 *	172.57.52.174/32	•	No	No	No	1971	165564	1635	137340	1	[Connections]
NAT Policies Dis NAT Policies In U Port Restricted I Destination NAT	played: 1 Jse: 1/1000 Dynamic NAT P Policies In Use	olicies In Us 20/100	se: 0/100															

The following screenshot shows the mapping of inside address to outside address in an IPv6 static NAT policy.

Mo	onitoring >	Firewall														
F	irewall Sta	tistics														
Stati	stics:	NAT Polic	ies 🛊													
Max to d	imum entries isplay:	50 \$														
NAT	:	IP Protoco	l: /	Any	\$	NAT	Type: Any	,	Dynam	ic NA	Ar	ıy	\$			
	Service Type: Any Name: Any Inside IP: Inside Port: Outside IP: Outside IP: Outside IP: Outside IP: Outside IP:															
	Name:     Outside IP:     Outside Port:       Inside IP:     •     Inside Port:       Show latest     •															
Re	Refersh data.															
Help	Refresh data.															
N	IAT Policies	5								_						
							Inside		Outside	L						
ID	Rule Type	Rule Parent	Direction	IP Protocol	Service Type	Service Name	IP Address	Port	IP Address	Port	Allow Related	Allow IPSec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Pack Rece
1	Static	-	Outbound	*	Internet	-	2006::/64	*	2004::/64	*	Yes	No	No	26	2144	
2	Dynamic PR	-	Outbound	*	Internet	-	*	*	172.170.11.85/32	*	No	No	No	390832	71419346	409
3	Dynamic Sy	m –	Outbound	*	Internet	-	*	*	2004::85/128	*	No	No	No	51	4112	
NAT NAT Port Dest	Policies Disp Policies In U Restricted D ination NAT	olayed: 3 se: 3/1000 ynamic NAT Policies In I	F Policies In Use:0/100	Use: 2/100												

### Logs

You can view logs related to NAT in firewall logs. To view logs for NAT, create a firewall policy that matches your NAT policy and ensure that logging is enabled on the firewall filter. NAT logs display the following information:

- Date and time
- Routing domain
- IP protocol
- Source port

- Source IP address
- Translated IP address
- Translated port
- Destination IP address
- Destination port

riority:	Policy Type:			
100	Built-in Firewall 🔻			
Match Criteria				
From Zones		To Zones		
Zone	Enable	*	Zone	Enable
Any		Any		
Default_LAN_Zone		Default_LAN_Zon	e	
gre_zone		gre_zone		
Inter Routing Domain 7or	ne 🗐	<ul> <li>Inter Routing Do</li> </ul>	main 7one	•
Traffic Match Type:	IP Protocol:	DSCP:		
Traffic Match Type:	IP Protocol:	DSCP:		
IP Protocol 🔹	Any	<ul> <li>Any</li> </ul>	Match Establish	red
Application:	Application Family:	Application Objects:		
		* Any	Ŧ	
Source Service Type:	Source Service Name:	Source IP:	Source Port:	
Any 🔻	Any 🔻	*	*	
Dest Service Type:	Dest Service Name:	Dest IP:	Dest Port:	
Any 🔻	Any 🔻	×	*	
Actions				
Action:	Allow Fragments	Use Site Setting		
- Allow ·	<ul> <li>Allow Haginents</li> </ul>	Use like betang		
Logging & Other Options				
Logging & Other Options Log Interval (s):				

To generate NAT logs, navigate to Logging/Monitoring > Log Options, select SDWAN\_firewall.log, and click View Log.

2022-02-14T11:18:01.527774+0000	INFO	t2_firewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP
2022-02-14T11:18:03.734510+0000	INFO	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain
2022-02-14T11:18:03.735008+0000	INFO	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain
2022-02-14T11:18:24.549695+0000	INFO	t2_firewall_monitor.pl	NAT Connection DELETED for (Routing Domain Default_RoutingDomain) TCP
2022-02-14T11:33:08.856441+0000	INFO	t2_firewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP
2022-02-14T11:33:11.813149+0000	INFO	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain
2022-02-14T11:33:11.813553+0000	INFO	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain
2022-02-14T11:33:12.416871+0000	INFO	t2_firewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) UDP
2022-02-14T11:33:20.822305+0000	INFO	<pre>t2_firewall_monitor.pl</pre>	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain
2022-02-14T11:33:20.822660+0000	INFO	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain

The NAT connection details are displayed in the log file.

2022-02-14T11:43:53.184990+0000 W	ARN find	_and_update_connecti	on@forward/firewall/connection.c:4828 CONN 0x7fffdbf5f168 Aborted, NAT
2022-02-14T11:43:53.185044+0000 I	NFO t2_f	irewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:43:53.565134+0000 I	NFO t2_f	irewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:43:59.572977+0000 I	NFO t2_f:	irewall_monitor.pl	Connection DELETED for (Routing Domain Default_RoutingDomain) IPv6_ICMP
2022-02-14T11:45:12.399564+0000 I	NFO t2_f	irewall_monitor.pl	NAT Connection DELETED for (Routing Domain Default_RoutingDomain) UDP 1
2022-02-14T11:45:48.516174+0000 I	NFO t2_f	irewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:45:48.717951+0000 I	NFO t2_f	irewall_monitor.pl	Filter (1) ALLOWED 488 packets for (Routing Domain Default_RoutingDomai
2022-02-14T11:46:18.786955+0000 I	NFO t2_f	irewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:21.760939+0000 I	NFO t2_f	irewall monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:21.761368+0000 I	NFO t2_f	irewall monitor.pl	Filter (1) ALLOWED 3 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:27.766610+0000 I	NFO t2_f	irewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:32.774464+0000 I	NFO t2 f	irewall monitor.pl	NAT Connection CREATED for (Routing Domain Default RoutingDomain) TCP 2
2022-02-14T11:46:32.775063+0000 I	NFO t2 f	irewall monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default RoutingDomain)
	_	-	
2022-02-14T11:43:53.184990+0000 W	ARN find	_and_update_connecti	ion@forward/firewall/connection.c:4828 CONN 0x7fffdbf5f168 Aborted, NAT
2022-02-14T11:43:53.185044+0000 I	NFO t2_f	irewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:43:53.565134+0000 I	NFO t2_f	irewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:43:59.572977+0000 I	NFO t2_f:	irewall_monitor.pl	Connection DELETED for (Routing Domain Default_RoutingDomain) IPv6_ICMP
2022-02-14T11:45:12.399564+0000 I	NFO t2_f	irewall_monitor.pl	NAT Connection DELETED for (Routing Domain Default_RoutingDomain) UDP 1
2022-02-14T11:45:48.516174+0000 I	NFO t2_f	irewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:45:48.717951+0000 I	NFO t2_f	irewall_monitor.pl	Filter (1) ALLOWED 488 packets for (Routing Domain Default_RoutingDomai
2022-02-14T11:46:18.786955+0000 I	NFO t2_f	irewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:21.760939+0000 I	NFO t2_f	irewall monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:21.761368+0000 I	NFO t2_f	irewall monitor.pl	Filter (1) ALLOWED 3 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:27.766610+0000 I	NFO t2_f	irewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:32.774464+0000 I	NFO t2_f	irewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:32.775063+0000 I	NFO t2 f	inewall monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default RoutingDomain)

## **Dynamic NAT**

#### August 24, 2022

Dynamic NAT is a many-to-one mapping of a private IP address or subnets inside the SD-WAN network to a public IP address or subnet outside the SD-WAN network. The traffic from different zones and subnets over trusted (inside) IP addresses in the LAN segment is sent over a single public (outside) IP address.

### **Dynamic NAT types**

Dynamic NAT does Port Address Translation (PAT) along with IP address translation. Port numbers are used to distinguish which traffic belongs to which IP address. A single public IP address is used for all internal private IP addresses, but a different port number is assigned to each private IP address. PAT is a cost effective way to allow multiple hosts to connect to the Internet using a single Public IP address.

- **Port Restricted**: Port Restricted NAT uses the same outside port for all translations related to an Inside IP Address and Port pair. This mode is typically used to allow Internet P2P applications.
- **Symmetric**: Symmetric NAT uses the same outside port for all translations related to an Inside IP Address, Inside Port, Outside IP Address, and Outside Port tuple. This mode is typically used to enhance security or expand the maximum number of NAT sessions.

### **Inbound and Outbound NAT**

The direction for a connection can either be inside to outside or outside to inside. When a NAT rule is created, it is applied to both the directions depending on the direction match type.

- **Outbound**: The destination address is translated for packets received on the service. The source address is translated for packets transmitted on the service. Outbound dynamic NAT is supported on Local, Internet, Intranet, and Inter-routing domain services. For WAN services such as Internet and Intranet services, the configured WAN link IP address is dynamically chosen as the outside IP address. For Local and Inter-routing domain services, provide an outside IP address. The Outside zone is derived from the selected service. A typical use case of outbound dynamic NAT is to simultaneously allow multiple users in your LAN to securely access the internet using a single Public IP address.
- **Inbound**: The source address is translated for packets received on the service. The destination address is translated for packets transmitted on the service. Inbound dynamic NAT is not supported on WAN services such as Internet and Intranet. There is an explicit audit error to indicate the same. Inbound dynamic NAT is supported on Local and Inter-routing domain services only. Provide an outside zone and outside IP address to be translated to. A typical use case for inbound dynamic NAT is to allow external users access email or web servers hosted in your private network.

## **Port Forwarding**

Dynamic NAT with port forwarding allows you to port forward specific traffic to a defined IP address. This is typically used for inside hosts like web servers. Once the dynamic NAT is configured you can define the port forwarding policies. Configure dynamic NAT for IP address translation and define the port forwarding policy to map an outside port to an inside port. Dynamic NAT port forwarding is typically used to allow remote hosts to connect to a host or server on your private network. For a more detailed use case see, Citrix SD-WAN Dynamic NAT explained.

### **Auto-created Dynamic NAT policies**

Dynamic NAT policies for the Internet service are auto created in the following cases:

- Configuring internet service on an untrusted interface (WAN link).
- Enabling internet access for all routing domains on a single WAN link using Citrix SD-WAN Orchestrator service. For more details, see Configure firewall segmentation.
- Configuring DNS forwarders or DNS proxy on SD-WAN Orchestrator service. For more details, see Domain name system.

### Monitoring

To monitor dynamic NAT, navigate to **Monitoring** > **Firewall Statistics** > **Connections**. For a connection you can see if NAT is done or not.

Dashboard Monito	configuration																				
Statistics	Monitoring > Firewall																				
Flows																					
Routing Protocols	Firewall Statistics																				
Firewall	Statistics: Con	nections 👻																			
IKE/IPsec	Maximum entries 50	~																			
IGMP	Filtering: Appl	ication:	Any		¥ F	amily:		Any	~												
Performance Reports	IP Pr	otocol:	Any		✓ s	ource Zo	ne:	Any		~ 0	estination	Zone: Any	~								
Qos Reports	Sour	ce Service Type:	Any		✓ s	ource Ser	vice Instance:	Any 🗸		s	ource IP:		Source	Port:							
Usage Reports	Desti	ination Service Typ	e: Any		• c	estinatio	n Service Insta	ince: Any 🗸		D	estination	IP:	Destina	ation Port:							
Availability Reports	Refresh S	how latest data	□ Sho	w Additional S	stats																
Appliance Reports	Clear Connections																				
DHCP Server/Relay	Help																				
VRRP	Connections																				
PPPoE						Sou	urce.					Destination					See	at			
DNS			IP			Service	Service				Service	Connadon			ls						
	Application	Family	Protocol	IP Adress	Port	Туре	Name	Zone	IP Address	Port	Туре	Service Name	Zone	State	NAT	ackets	Bytes	PPS	kbps	Packets	By
	Domain Name Service(dns)	Network Service	UDP	172.57.48.50	34202	Local	VIF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHE	Yes	2	140	0.008	0.004	2	4
	Domain Name Service(dns)	Network Service	UDP	172.57.48.50	42261	Local	VIF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHE	Yes	2	140	0.008	0.004	2	4
	Domain Name Service(dns)	Network Service	UDP	172.57.48.50	34058	Local	VIF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHE	Yes	2	114	0.008	0.004	2	4
	Domain Name Service(dns)	Network Service	UDP	172.57.48.50	50486	Local	VIF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHE	Yes	2	114	0.008	0.004	2	4
	Domain Name Service(dns)	Network Service	UDP	172.57.48.50	33928	Local	VIF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHE	Yes	2	124	0.008	0.004	2	4
	Domain Name Service(dns)	Network Service	UDP	172.57.48.50	50354	Local	VIF-1-LAN-1	Default_LAN_Zone	10.140.50.5	53	Internet	BR210_UTM-Internet	Untrusted_Internet_Zone	ESTABLISHE	Yes	2	124	0.008	0.004	2	-
	I Damein Nama Caniss/dae)	Makanda Camilan	1100	177 67 40 60	60544	I a cal	VAC 1 FAM 1	Default I Abl 7ana	10140 60 6	6.5	Tettere st	DD11A UTL4 Laborate	Hate-stad Interest Taxa	CETABITCUE	V.s.	2	154	0.007	0.003	2	

To further see the inside IP address to outside IP address mapping, click **Pre-Route NAT** or **Post-route NAT** under **Related Objects** or navigate to **Monitoring** > **Firewall Statistics** > **NAT policies**.

The following screenshot shows the statistics for the Dynamic NAT rule of type symmetric and its corresponding port forwarding rule.

Dashboard	Monitoring	; Co	nfiguration															
Monitoring	> Firewall																	
Firewall S	tatistics																	
Statistics:	NAT Policies	•																
Maximum entri	50 🗸																	
NAT:	IP Protocol:	Any		~	NAT Type:	Any	~ D	ynamic NAT Type:	Any	~								
	Service Type:	Anv		~	Service Name:	Any 🗸												
	Inside IP:	*			Inside Port:	*	c	utside IP:	*		Outside Port: *							
Refresh	Show latest	data.																
Help																		
NAT Polic	ies																	
						Inside		Outside										
ID Rule Ty	pe Rule Parent	Direction	IP Protocol	Service Type	Service Name	IP Address	Port	IP Address	Port	Allow Related	Allow IPSec Passthrough	Allow GRE Passthrough	Packets Sent	Bytes Sent	Packets Received	Bytes Received	Connections	Related Objects
1 Dynamic	Sym -	Outbound		Internet				172.147.12.83/32	•	No	No	No	0	0	0	0	0	
2 Port Forv	vard 1	Outbound		Internet		172.147.90.12/32	5001-5010	172.147.12.83/32	5001-5010	No	No	No	82	47232	8928	13374144	0	
NAT Policies D NAT Policies In Port Restricted Destination N	isplayed: 2 Use: 2/1000 Dynamic NAT Polio T Policies In Use:0/	cies In Use: 0, '100	/100															

When a port forwarding rule is created a corresponding firewall rule is also created.

Site: Branch1																						?
WAN-to-WAN Forwarding	Pre-Appliance Tem	olate Poli	cies																			2
Virtual Paths		_																				
Dynamic Virtual Paths	Local Policies 🛨	Add																				?
Internet Service				Zones								Source			Destination							
Intranet Services												Г.			ř							
WAN Links GRE Tunnels	Priority	Routing Domain	Action	From	То	Application	Application Family	Application Objects	IP Protocol	DSCP	Service	[P Address	Port	Service	IP Address	Port	Match Est.	Add Reverse Policy	Info	Edit	Delete	Clone
IPsec Tunnels	(auto)	*	Allow	*	*	*	*	*	Any	*	IP Host	*	*	*	*	*			0			
Application Routes	(auto)	*	Allow	Internet_Zone					Any	*	Internet		*	•		•	Yes		0			
Routes OSPF BGP	(auto)		Allow	Internet_Zone		*		•	TCP (6)		Internet	•	0- 65535	·	15.15.15.1	443			0			
Route Learning Properties Inter Routing Domain Services	(auto)	•	Allow	Internet_Zone		*	*		UDP (17)		Internet		0+ 65535		15.15.15.1	443			0			
Applications	(auto)		Drop		*	*	•	*	Any	*	Internet	*	*	*		*			0			
	Post-Appliance Ten	nplate Poi	licies																			?
	Apply Refresh																					_

You can see the filter policy statistics by navigating to **Monitoring** > **Firewall Statistics** > **Filter Policies**.

Dasi	nboard	Monitorin	9	Configu	ration																			
Mor	Monitoring > Firevall																							
_																								
Fi	rewall Sta	tistics																						
Statis	tics:	Filter Policies	•																					
Maxin to dis	num entries play:	50 🗸																						
Filteri	ng:	Routing Domai	in:	Any		~	Application	c	Any		Famil	ly:	Any		~	IP P	rotocol: A	iny	~					
		Filter Policy Ac	tion:	Any 🗸	•		Source Serv	vice Type:	Any	~	Source	ce Service Na	me: Any	~		Sou	rce IP:							
		Source Port:	(	*			Destination	Service Ty	pe: Any	~	Desti	nation Servi	e Name: Any	~		Des	tination IP:							
		Destination Po	nt: [				Source Zon	e:	Any		✓ Desti	nation Zone:	Any			✓ DSC	P: A	iny 🗸						
Ref	Estable Concentration of the second sec																							
Help	Internation of the second seco																							
_																								
Fi	Iter Policie	15																						
Defau Match	It Policy=A In Progres	llow(Not Tracked s Packets=0 Byte	i) Packe s=0	ts=3414 Byt	tes=2134	489																		
								Sour	ce				Destination											
ID	Routing Domain	Application	Family	IP Protocol	DSCP	Service Type	Service Name	IP Address	Port or ICMP Type	Zone	Service Type	Service Name	IP Address	Port or ICMP Code	Zone	Action	Conn Match Type	Track Connection	Allow Fragments	Log Connection Start	Log Connection End	Packets	Bytes	Related Objects
1	•				•	IPHost			NA					NA		Allow	Default	No	Yes	No	No	0	0	
2	*	*	*	*		Internet		*	NA	Internet_Zone				NA	*	Allow	Established	No	Yes	No	No	0	0	
3				TCP		Internet				Internet_Zone			15.15.15.1/32	443		Allow	Default	No	Yes	No	No	0	0	
4				UDP		Internet				Internet_Zone			15.15.15.1/32	443		Allow	Default	No	Yes	No	No	0	0	
5						Internet			NA					NA		Drop	Default	No	Yes	No	No	0	0	

### Logs

You can view logs related to NAT in firewall logs. To view logs for NAT, create a firewall policy that matches your NAT policy and ensure that logging is enabled on the firewall filter. NAT logs contain the following information:

- Date and time
- Routing domain
- IP protocol
- Source port
- Source IP address
- Translated IP address
- Translated port
- Destination IP address
- Destination port

iority:	Policy Type:						
100	Built-in Firewall	•					
Match Criteria							
From Zones			To Zones				
Zone		Enable		Zone	Enable		
Any			Any		1		
Default LAN Zone		0	Default LAN Zon	e		1	
are zone			are zone				
Inter Routing Domain 7	one	-	Inter Routing Do	main Zone		-	
Application:	Application Fam	ily: *	Application Objects: Any	Ŧ			
Source Service Type: Any <b>v</b>	Source Service Na	ime: Sou	rce IP:	Source Port:			
Source Service Type: Any • Dest Service Type:	Source Service Na Any <b>v</b> Dest Service Name	e: Dest II	rce IP:	Source Port:			
Source Service Type: Any • Dest Service Type:	Source Service Na Any <b>v</b> Dest Service Nam	e: Dest II	rce IP:	Source Port: * Dest Port:			

To generate NAT logs, navigate to **Logging/Monitoring** > **Log Options**, select **SDWAN\_firewall.log**, and click **View Log**.

2022-02-14T11:18:01 527774+0000	TNEO	+2 finewall monitor ol	NAT Connection (PEATED for (Pouting Domain Default PoutingDomain) TCP
EVEC-VC- 141 11.10.01.02.02///4+0000	THE O	cs_rarenoss_monscor.ps	the connection exertise for (Roacing ponetti person choocingponeti) for
2022-02-14T11:18:03.734510+0000	INFO	<pre>t2_firewall_monitor.pl</pre>	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain
2022-02-14T11:18:03.735008+0000	INFO	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain
2022-02-14T11:18:24.549695+0000	INFO	t2_firewall_monitor.pl	NAT Connection DELETED for (Routing Domain Default_RoutingDomain) TCP
2022-02-14T11:33:08.856441+0000	INFO	t2_firewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP
2022-02-14T11:33:11.813149+0000	INFO	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain
2022-02-14T11:33:11.813553+0000	INFO	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain
2022-02-14T11:33:12.416871+0000	INFO	t2_firewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) UDP
2022-02-14T11:33:20.822305+0000	INFO	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain
2022-02-14T11:33:20.822660+0000	INFO	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain

# The NAT connection details are displayed in the log file.

2022-02-14T11:43:53.184990+0000	WARN	find_and_update_connection	<pre>on@forward/firewall/connection.c:4828 CONN 0x7fffdbf5f168 Aborted, NAT</pre>
2022-02-14T11:43:53.185044+0000	INFO 1	t2_firewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:43:53.565134+0000	INFO 1	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:43:59.572977+0000	INFO 1	t2_firewall_monitor.pl	Connection DELETED for (Routing Domain Default_RoutingDomain) IPv6_ICMP
2022-02-14T11:45:12.399564+0000	INFO 1	t2_firewall_monitor.pl	NAT Connection DELETED for (Routing Domain Default_RoutingDomain) UDP 1
2022-02-14T11:45:48.516174+0000	INFO 1	t2_firewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:45:48.717951+0000	INFO 1	<pre>t2_firewall_monitor.pl</pre>	Filter (1) ALLOWED 488 packets for (Routing Domain Default_RoutingDomai
2022-02-14T11:46:18.786955+0000	INFO 1	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:21.760939+0000	INFO 1	t2_firewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:21.761368+0000	INFO 1	t2_firewall_monitor.pl	Filter (1) ALLOWED 3 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:27.766610+0000	INFO 1	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:32.774464+0000	INFO 1	t2_firewall_monitor.pl	NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:32.775063+0000	INFO 1	t2_firewall_monitor.pl	Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)

## **Configure Virtual WAN Service**

August 24, 2022

The Citrix SD-WAN configuration describes and defines the topology of your Citrix SD-WAN network. For information on how to configure virtual WAN service using Citrix SD-WAN Orchestrator service, see Flows.

## Security and encryption

Enabling encryption for SD-WAN (for the Virtual Paths) is 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.

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.

## **Configure firewall segmentation**

### August 24, 2022

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. From SD-WAN 11.5 release onwards, you can configure firewall segmentation using Citrix SD-WAN Orchestrator service. For more information, see Firewall segmentation.

- 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.
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**.

E	Toggle Columns Both WAN Ingress and WAN Egress Flows																								
	Routing Domain	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Conduit Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
	Guest	11.20.20.20	12.125.10.20	WAN Ingress	8	3335	ICMP	default	62	INTERNET	-	LOCAL	74	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
	Default	10.200.247.200	12.125.10.20	WAN Ingress	8	16185	ICMP	default	66	INTERNET	-	LOCAL	311	66	5544	1.009	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
	Guest	12.125.10.20	11.20.20.20	WAN Egress	0	18456	ICMP	default	62	INTERNET	-	LOCAL	94	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
	Default	12.125.10.20	10.200.247.200	WAN Egress	0	3968	ICMP	default	66	INTERNET	-	LOCAL	328	66	5544	1.008	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
T	Fotal INGRESS	flows displayed: 2	2 out of 2 out of 2			,		,									,							<u> </u>	

#### You can also check the routing table for each routing domain under **Monitor > Statistics > Routes**.

		-											Filter:		in Any column	Apply
Show	how 100 v entries Showing 1 to 5 of 5 entries															
Nu	m 🔺	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Туре	Protocol	Neighbor Direct	Cost	HIt Count	Eligible	Eligibility Type	Eligibility Value
	0	11.20.20.0/24	*	Local	Default_LAN_Zone	YES	*	Angelina-CFB	Static	-	-	5	318	YES	N/A	N/A
	1	11.10.10.0/24	*	DC-Angelina-CFB	Default_LAN_Zone	YES	*	DC	Static		-	5	0	YES	N/A	N/A
	2	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	159	YES	N/A	N/A
	3	0.0.0/0	*	Passthrough	Any	YES	*	*	Static		-	16	0	YES	N/A	N/A
	4	0.0.0/0	*	Discard	Any	YES	*	*	Static		-	16	0	YES	N/A	N/A
Show	wing	1 to 5 of 5 entries													First Previou	is 1 Next Last

#### **Use Cases**

In previous Citrix SD-WAN releases, virtual routing and forwarding had the following issues, which have been resolved.

- Customers have multiple routing domains at a branch site without the requirement to include all domains at the data center (MCN). They need the ability to isolate different customers' traffic in a secure manner
- Customers must be able to have a single accessible firewalled Public IP address for multiple routing domains to access the internet at a site (extend beyond VRF lite).
- Customers need an Internet route for each routing domain supporting different services.
- Multiple routing domains at a branch site.
- Internet Access for different routing domains.

#### Multiple routing domains at a branch site

With the Virtual Forwarding and Routing Firewall segmentation enhancements, you can:

- Provide an infrastructure, at the branch site, that supports secure connectivity for at least two user groups, such as employees and guests. The infrastructure can support up to 16 routing domains.
- Isolate each routing domain's traffic from the traffic of any other routing domain.

- Provide internet access for each routing domain,
  - A common Access Interface is required and acceptable
  - An Access Interface for each group with separate Public facing IP addresses
- Traffic for the employee can be routed directly out to the local internet (specific applications)
- Traffic for the employee can be routed or backhauled to the MCN for extensive filtering (0 route)
- Traffic for the routing domain can be routed directly out to the local internet (0 route)
- Supports specific routes per routing domain, if necessary
- Routing domains are VLAN based
- Removes the requirement for the RD to have to reside at the MCN
- Routing Domain can now be configured at a branch site only
- Allows you to assign multiple RD to an access interface (once enabled)
- Each RD is assigned a 0.0.0.0 route
- Allows specific routes to be added for an RD
- Allows traffic from different RD to exit to the internet using the same access interface
- Allows you to configure a different access interface for each RD
- Must be unique subnets (RD are assigned to a VLAN)
- Each RD can use the same FW default Zone
- The traffic is isolated through the Routing Domain
- Outbound flows have the RD as a component of the flow header. Allows SD-WAN to map return flows to correct Routing domain.

Prerequisites to configure multiple routing domains:

- Internet access is configured and assigned to a WAN Link.
- Firewall configured for NAT and correct policies applied.
- Second routing domain added globally.
- Each routing domain added to a site.
- Ensure that the Internet service has been defined correctly.

#### **Deployment scenarios**



#### Limitations

• The internet service must be added to the WAN link before you can enable Internet access for all Routing Domains. (Until you do, the check box for enabling this option is grayed out).

After enabling internet access for all routing domains, auto add a dynamic-NAT rule.

• Up to 16 Routing Domains per site.

- Access Interface (AI): Single AI per subnet.
- Multiple AIs require a separate VLAN for each AI.
- If you have two routing domains at a site and have a single WAN Link, both domains use the same public IP address.
- If Internet access for all routing domains is enabled, all sites can route to Internet. (If one routing domain does not require internet access, you can use the firewall to block its traffic.)
- No support for the same subnet in multiple routing domains.
- There is no audit functionality
- The WAN links are shared for Internet access.
- No QOS per routing domain; first come first serve.

# **Certificate authentication**

#### August 24, 2022

Citrix SD-WAN ensures secure paths are established between appliances in the SD-WAN network by using security techniques such as network encryption and virtual path IPsec tunnels. In addition to the existing security measures, certificate based authentication is introduced in Citrix SD-WAN 11.0.2.

Certificate authentication allows organizations to use certificates issued by their private Certificate Authority (CA) to authenticate appliances. The appliances are authenticated before establishing the virtual paths. For example, if a branch appliance tries to connect to the data center and the certificate from the branch does not match with the certificate that the data center expects, the virtual path is not established.

The certificate issued by the CA binds a public key to the name of the appliance. The public key works with the corresponding private key possessed by the appliance identified by the certificate.

You can enable Certificate authentication of your SD-WAN appliance using Citrix SD-WAN Orchestrator service. For more information about Certificate authentication, see Certificate authentication.

## **AppFlow and IPFIX**

August 24, 2022

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 or IPv6 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.

AppFlow Collectors like Splunk and Citrix ADM have dashboards to interpret and present these templates.

#### IPFIX

IPFIX is a collector export protocol used for exporting flow level data for all connections. For any connection, you can view information such as packet count, byte count, type of service, flow direction, routing domain, application name and so on. IPFIX flows are transmitted through the management interface. Most collectors can receive IPFIX flow records, but may need to build a custom dashboard to interpret IPFIX template.

The IPFIX template defines the order in which the data stream is to be interpreted. The collector receives a template record, followed by the data records. Citrix SD-WAN uses templates 611 and 613 to export IPv4 IPFIX flow data, 615 and 616 to export IPv6 IPFIX flow data along with Options template 612.

Application Flow Info (IPFIX) exports data sets as per templates 611 for IPv4 flows, 615 for IPv6 flows and 612 options Template with Application info.

Basic Properties (IPFIX) exports data sets as per templates 613 for IPv4 flows and 616 for IPv6 flows.

The following tables provide the detailed list of flow data associated with each IPFIX template.

#### Application Flow Info (IPFIX) - V10 templates

Template ID - 611

Info Element (IE)	IE name & ID	Type and len	Description
Observation point ID	observationPointId, 138	Unsigned32, 4	
Export process ID	exportingProcessId, 144	Unsigned32, 4	
Flow ID	flowId, 148	Unsigned64, 8	
Ipv4 SRC IP	sourceIPv4Address, 8	lpv4address, 4	
lpv4 DST IP	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	ipVersion, 60	Unsigned8, 1	Set to 4.
IP protocol number	protocoldentifier,4	Unsigned8, 1	
Padding	N/A	Unsigned16, 2	
SRC Port	sourceTransportPort, 7	Unsigned16, 2	
DST Port	destinationTransportPor	rt, <b>ሀ</b> 1signed16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Time for first pkt in microseconds Time for lastpkt in microseconds IP ToS	flowStartMicroseconds, 154 flowEndMicroseconds, 155 ipClassOfService, 5	dateTimeMicroseconds, 8 dateTimeMicroseconds, 8 Unsigned8, 1	
Flow Flags	tcpControlBits, 6	Unsigned8, 2	Currently set to 0.
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.

Info Element (IE)	IE name & ID	Type and len	Description
Output Interface	egressInterface, 14	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Input Vlan ID	vlanId, 58	Unsigned16, 2	
Output Vlan ID	postVlanId, 59	Unsigned16, 2	
VRF ID	ingressVRFID, 234	Unsigned32, 4	
Flow Key Indicator	flowKeyIndicator, 173	Unsigned64, 8	Set to 0x1E037F.
Application ID	applicationId, 95	octetArray, variable	The Application ID is same as the ID of the applications classified by the DPI engine. The application IDs remain constant. The application IDs for Custom domain name based applications change with every configuration update.

# Template ID –615 (IPv6 flows)

Info Element (IE)	IE name & ID	Type and len	Comment					
Observation	observationPointId,	Unsigned32, 4						
point ID	138							
Export process ID	exportingProcessId, Unsigned32, 4							
	144							
Flow ID	flowId, 148	Unsigned64, 8						
Ipv6 SRC IP	sourceIPv6Address, 27	Ipv6address, 16						

Info Element (IE)	IE name & ID	Type and len	Comment
lpv6 DST IP	destinationIpv6Adc 28	lr <b>ep</b> y6address, 16	
Ipversion	ipVersion, 60	Unsigned8, 1	Set to 6
IP protocol number	protocoldentifier, 4	Unsigned8, 1	
Padding	N/A	Unsigned16, 2	
SRC Port	sourceTransportPo 7	rtUnsigned16, 2	
DST Port	destinationTranspo 11	or <b>tPosi</b> gned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Time for first pkt	flowStartMicroseco	n <b>da</b> țeTimeMicroseco	onds,
in microseconds	154	8	
Time for lastpkt	flowEndMicrosecor	ndsateTimeMicroseco	onds,
in microseconds	155	8	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Flags	tcpControlBits, 6	Unsigned8, 2	Currently set to 0.
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN
			flows are a

possibility in SDWAN

Info Element (IE)	IE name & ID	Type and len	Comment
Input Interface	ingressInterface,	Unsigned32, 4	Citrix SD-WAN
	10		load balances
			data flows
			through multiple
			member paths,
			hence a single
			data flow can
			have multiple
			input/output
			interface
			combinations.
Output Interface	egressInterface,	Unsigned32, 4	Citrix SD-WAN
	14		load balances
			data flows
			through multiple
			member paths,
			hence a single
			data flow can
			have multiple
			input/output
			interface
			combinations.
Input Vlan ID	vlanId, 58	Unsigned16, 2	
Output Vlan ID	postVlanId, 59	Unsigned16, 2	
VRF ID	ingressVRFID, 234	Unsigned32, 4	
Flow Key Indicator	flowKeyIndicator, 173	Unsigned64, 8	Set to 0x1E037F.

Info Element (IE)	IE name & ID	Type and len	Comment
Application ID	applicationId, 95	octetArray,	The Application
		variable	ID is same as the
			ID of the
			applications
			classified by the
			DPI engine. The
			application IDs
			remain constant.
			The application
			IDs for Custom
			domain name
			based
			applications
			change with
			every
			configuration
			update.

## Template 612 (Options Template)

Info Element (IE)	IE name & ID	Туре	Comment
Application ID	applicationId, 95	octetArray	The Application ID is same as the ID of the applications classified by the DPI engine. The application IDs remain constant. The application IDs for Custom domain name based applications change with every
Application Name	applicationName, 96	string	Specifies the name of the Citrix SDWAN specific proprietary application.

Info Element (IE)	IE name & ID	Туре	Comment
Application	applicationDescription,	string	Specifies the
Description	94		description of the
			application.

#### Basic Properties (IPFIX) – V9 compliant template - Template 613 (IPv4 flows)

Info Element (IE)	IE name & ID	Type and len	Comment
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
Ipv4 DST IP	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	ipVersion, 60	Unsigned8, 1	
IP protocol number	protocoldentifier, 4	Unsigned8, 1	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN
SRC Port	sourceTransportPort, 7	Unsigned16, 2	
DST Port	destinationTransportPo 11	rt,Unsigned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple

member paths, hence a single data flow can

input/output interface

have multiple

combinations.

Info Element (IE)	IE name & ID	Type and len	Comment
Output Interface	egressInterface, 14	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Input Vlan ID	vlanId, 58	Unsigned16, 2	
Output Vlan ID	postVlanId, 59	Unsigned16, 2	

# Template ID –616 (IPv6 flows)

Info Element (IE)	IE name & ID	Type and len	Comment
lpv6 SRC IP	sourceIPv6Address, 27	Ipv6address, 16	
Ipv6 DST IP	destinationIpv6Add 28	r <b>ŧps</b> y6address, 16	
Ipversion	ipVersion, 60	Unsigned8, 1	Set to 6
IP protocol number	protocoldentifier,4	Unsigned8, 1	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN
SRC Port	sourceTransportPor 7	tUnsigned16, 2	
DST Port	destinationTransport	r <b>tPosi</b> gned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	

Info Element (IE)	IE name & ID	Type and len	Comment
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Output Interface	egressInterface, 14	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Input Vlan ID	vlanId, 58	Unsigned16, 2	
Output Vlan ID	postVlanId, 59	Unsigned16, 2	

#### Limitations

- AppFlow does not support IPv6 collector and flow records.
- 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 down-graded 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 only through Citrix SD-WAN Orchestrator service. For more informtion, see AppFlow and IPFIX.

#### Log files

For troubleshooting issues related to AppFlow / IPFIX export protocols, you can view and download the SDWAN\_export.log files. Navigate to **Configuration > Logging / Monitoring** and select the **SD-WAN\_export.log** files.

<ul> <li>Appliance Settings</li> </ul>	Configuration > A	ppliance Settings 🗦 L	.ogging/Monitoring						
- Administrator Interface									
Logging/Monitoring	Log Options	Alert Options	Alarm Options	Syslog Server	HTTP Server				
- Network Adapters - Net Flow	View Log File								
- App Flow/IPFIX - SNMP	Only the most re	Only the most recent 10000 entries will be shown and filtered. To view the full log, download and open it l							
·· NITRO API Licensing	Filename:	DWAN_export.log	•						
F Virtual WAN	View Log								
+ WAN Optimization									
System Maintenance	Download Log	File							
+ System Maintenance	Download Log	File							

## **SNMP**

August 24, 2022

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.

NOTE

To configure an IPv6 address, ensure that the SNMP server is also configured with an IPv6 address.

#### Citrix SD-WAN 11.5

- Appliance Settings	Configuration > Appliance Settings > SNMP
Administrator Interface	
Logging/Monitoring	Managers Download MIB File
Network Adapters	
• Net Flow	SNMP
- App Flow	
SNMP	UDP Port: 181
NITRO API	System Description: Citrix Virtual WAN Applian
Licensing	System Contact: support@citrix.com
+ Virtual WAN	System Location: Citrix
+ System Maintenance	
	SNMP v1/v2
	Enable v1/v2 Agent
	Community String: public
	Enable v1/v2 Traps Send v1/v2 Test Trap
	Destination IP Address(es):
	Port: 162
	SNMP v3
	Enable v3 Agent
	User Name:
	Password:
	Verify Password:
	Authentication: MD5 T
	Encryption: None *
	Fnable v3 Trans Send v3 Test Tran
	Destination IP Address(es)
	Port: 162
	User Name:
	Password:
	Verify Password:
	Authentication: MD5 *
	Encryption: None *

#### **Standard MIB Support**

The following standard MIBs are supported by the SD-WAN Appliances.

MIB	RFC (Definition Link)
DISMAN-EVENT-MIB	https://www.ietf.org/rfc/rfc2981.txt
IF-MIB	https://www.ietf.org/rfc/rfc2863.txt
IP-FORWARD-MIB	https://www.ietf.org/rfc/rfc4292.txt
IP-MIB (Partial)	https://www.ietf.org/rfc/rfc4293.txt
Q-BRIDGE-MIB (Partial)	http://www.ieee802.org/1/files/public/MIBs/IE EE8021-Q-BRIDGE-MIB-201112120000Z.mib
RFC1213-MIB	https://www.ietf.org/rfc/rfc1213.txt
SNMPv2-MIB	https://www.ietf.org/rfc/rfc3418.txt
TCP-MIB	https://www.ietf.org/rfc/rfc4022.txt
P-BRIDGE-MIB.txt	http://www.icir.org/fenner/mibs/extracted/P- BRIDGE-MIB-rfc2674.txt
RMON2-MIB.txt	https://www.ietf.org/rfc/rfc3273.txt
TOKEN-RING-RMON-MIB.txt	http://www.icir.org/fenner/mibs/extracted/TOK EN-RING-RMON-MIB-rmonmib-01.txt

You must download the following SNMP files before you can start monitoring a Citrix SD-WAN appliance:

- CITRIX-COMMON-MIB.txt
- APPACCELERATION-SMI.txt
- APPACCELERATION-PRODUCTS-MIB.txt
- APPACCELERATION-TC.txt
- APPACCELERATION-STATUS-MIB.txt
- APPCACHE-MIB.txt
- SDX-MIB-smiv2.mib

The MIB files are used by SNMPv3 managers and SNMPv3 trap listeners. The files include the SD-WAN appliance enterprise MIBs, which provide SD-WAN-specific events. To download MIB files, in the SD-WAN web management interface:

- 1. Navigate to **Configuration > Appliance Settings > SNMP > Download MIB File** page.
- 2. Select the required **MIB** file.
- 3. Click View.

The MIB file opens in MIB browser.

Dashboard Monitoring	Configuration
- Appliance Settings	Configuration > Appliance Settings > SNMP
Administrator Interface	Managers Download MIB File
Network Adapters Net Flow Add Flow	CITRIX-NetScaler-SD-WAN-MIB
SNMP	Download MIB File
NITRO API Licensing	
+ Virtual WAN	
+ System Maintenance	

#### Note

- Support for these MIBs is provided by default by the **net-snmp snmpd** daemon process on Linux systems. The MIBs provide the basis for supporting Network Management applications.
- The Ethernet port packet and byte counters are in the **IF-MIB** inside the **ifTable**. System information is in the system object.
- Ethernet ports are included in the **ifTable**, so walking that must be sufficient to ensure that the SNMP subsystem is running.
- Support for the **Q-BRIDGE-MIB** and the **IP-MIB** provides support for the network mapping application.

# **Administrative interface**

#### August 24, 2022

You can manage and maintain your Citrix SD-WAN appliances using the following administrative options using Citrix SD-WAN Orchestrator service. For more information, see Appliance settings.

- User accounts
- RADIUS server
- TACACS+ server
- HTTPS Cert
- HTTPS Settings
- Miscellaneous

#### **User accounts**

You can add new user accounts and manage the existing user accounts under **Configuration > Appliance Settings > Administrator Interface page > User Accounts** tab.

You can choose to authenticate the newly added user accounts either locally by the SD-WAN appliance or remotely. User accounts that are authenticated remotely, are authenticated through RADIUS or TACACS+ authentication servers.

#### **User roles**

The following user roles are supported:

- Viewer: Viewer account is a read-only account with access to **Dashboard**, **Reporting**, and **Mon-**itoring pages.
- Admin: Admin account has the administrative privileges and read-write access to all the sections.

A super administrator (admin) has the following privileges:

- Can export the configuration to the change management inbox to perform a configuration and software update to the network.
- Can also toggle the read-write access of the Network and Security Admins.
- Maintains both network and security related settings.
- **Security Admin**: A security administrator has the read-write access only for the firewall and security related settings, while having read-only access to the remaining sections. Security administrator also has the capability to enable or disable write access to the firewall for other users except the super administrator (admin).
- **Network Admin**: A network administrator has read-write permissions to all the sections and can fully provision a branch except for the firewall and security related settings. The hosted firewall node is not available for the network administrator. In this case, the network administrator must import a new configuration.

# Both network administrator and security administrator can make changes to the configuration and also deploy them on the network.

#### NOTE

The network administrator and security administrator cannot add or delete user accounts. They can only edit their own account passwords.

	Citrix SD-WAN	VPX-50-SE	ite Name MCN_DC-MCN_DC-VPX	Info 11.3.0.123.8888881 ▼	Logout	citrix					
	Dashboard Monito	ng Configuration									
<	- Appliance Settings	Configuration > Appliance Settings > Administrator Interface									
	Administrator Interface										
	Logging/Monitoring	User Accounts RADIUS TACACS+ HTTPS Cert	HTTPS Settings	Miscellaneous							
	Network Adapters	Change Local User Password	Change Local User Password								
	App Flow/IPFIX SNMP	User Name:									
	NITRO API	Current Password:									
	Licensing Fallback Configuration	New Password:									
	+ Virtual WAN	Confirm New Password:									
	+ System Maintenance	Change Password									
		Delete Workspace For User           Delete the selected user's Configuration Editor workspace. This action will no Deleting a workspace will remove all saved configurations and networks maps           User Name:         admin	t delete the user. s for the selected user. ace								
		Manage Users									
		Add User									
		Note: Deleting a user will also delete local files for that user. User Name:									
		Firewall Access									
		User Name: admin    Disable Firewall Access									

#### Add a user

To add a user, click **Add User** in the **Manage Users** section. Provide the **User Name** and **Password**. Select the user role from the **User Level** drop-down list and click **Apply**.

You can also delete a user account, if needed. Deleting a user also deletes the local files belonging to that user. To delete, under **Manage Users** section, select the user from the **User Name** drop-down list and click **Delete Selected User**.

Configuration > Appliance Settings								
Add a New User Account								
User Name:	newuser							
Password:								
Confirm Password User Level: v Apply Can	Viewer Admin Security Admin Network Admin							

#### Change password of a user

The administrator role can change the password of a user account that is authenticated locally by the SD-WAN appliance.

To change the password, under **Change Local User Password** section, select the user from the **User Name** drop-down list. Enter the current password and the new password. Click **Change Password**.

#### **RADIUS** server

You can configure an SD-WAN appliance to authenticate user access with one or a maximum of three RADIUS servers. The default port is 1812.

To configure the RADIUS server:

- 1. Navigate to **Configuration > Appliance Settings > Administrator Interface > RADIUS**.
- 2. Select the **Enable RADIUS** check box.
- 3. Enter the **Server IP Address** and **Authentication Port**. A maximum of three server IP addresses can be configured.

NOTE

To configure an IPv6 address, ensure that the RADIUS server is also configured with an IPv6 address.

- 4. Enter the Server Key and confirm.
- 5. Enter the **Timeout** value in seconds.
- 6. Click Save.

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

User Accounts	RADIUS	TACACS+	HTTPS Cert	HTTPS Settings	Miscellaneous
ADIUS			<u> </u>	<u> </u>	<u> </u>
Enable RADIUS					
Server 1 IP Address:	fd73	2039 5849 27 181	6 Juli fe85 al 5e	Authentication Po	ort: 1812
Server 2 IP Address (C	)ptional):			Authentication Po	ort:
Server 3 IP Address (C	ptional):			Authentication Po	ort:
Server Key:		•••••			
Confirm Server Key:		•••••			
Timeout (seconds):			(Optional)		
Apply					
Test RADIUS Server Co	onnection				
User Name:					
Deseurend					

#### **TACACS+** server

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

To configure the TACACS+ server:

- 1. Navigate to Configuration > Appliance Settings > Administrator Interface > TACACS+.
- 2. Select the **Enable TACACS+** check box.
- 3. Enter the **Server IP Address** and **Authentication Port**. A maximum of three server IP addresses can be configured.

#### NOTE

To configure an IPv6 address, ensure that the TACACS+ server is also configured with an IPv6 address.

- 4. Select **PAP** or **ASCII** as the Authentication Type.
  - PAP: Uses Password Authentication Protocol (PAP) to strengthen user authentication by assigning a strong shared secret to the TACACS+ server.
  - ASCII: Uses the ASCII character set to strengthen user authentication by assigning a strong shared secret to the TACACS+ server.
- 5. Enter the **Server Key** and confirm.

- 6. Enter the **Timeout** value in seconds.
- 7. Click Save.

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

onfiguration > App	liance Settings	> Administrator	Interface			
User Accounts	RADIUS	TACACS+	HTTPS Cert	HTTPS Settings	Miscellaneous	
TACACS+						
Enable TACACS+						
Server 1 IP Address:	filling	2039 5849 27.181	985:a15e	Authentication Po	ort: 49	
Server 2 IP Address (	(Optional):			Authentication Po	ort:	
Server 3 IP Address (	(Optional):			Authentication Po	ort:	
Authentication Type:	• PA	POASCII				
Server Key:						
Confirm Server Key:						
Timeout (seconds):			(Optional)			
Apply						
Test TACACS+ Serve	r Connection					
User Name:						
Password:						
Verify						

## NDP router advertisement and prefix delegation group

August 24, 2022

#### NDP router advertisement

In an IPv6 network, SD-WAN appliance periodically multicasts Router Advertisement (RA) messages to announce its availability and convey information to the neighboring appliances in the SD-WAN network. The router advertisements include the IPv6 prefix information. Neighbor Discovery protocol (NDP) running on SD-WAN appliances uses these router advertisements to determine the neighboring devices on the same link. It also determines each other's link-layer addresses, find neighbors, and maintain reachability information about the paths to active neighbors.

You can configure the NDP router advertisement using Citrix SD-WAN Orchestrator service. For more information, see NDP router advertisement.

## **Prefix delegation group**

#### NOTE

Prefix delegation is not supported in Citrix SD-WAN 11.3 release.

Citrix SD-WAN appliances can be configured as a DHCPv6 client to request a prefix from the ISP using the configured WAN port. Once Citrix SD-WAN appliance receives the prefix, it uses the prefix to create a pool of IP addresses to cater the LAN clients. Citrix SD-WAN appliance then behaves as a DHCP server and advertise the prefix on the LAN ports to the LAN side clients.

You can configure prefix delegation through Citrix SD-WAN Orchestrator service. For more information, see Prefix delegation groups.

## How-to-articles

#### August 24, 2022

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
- Zero touch Deployment

## **Configure access interface**

August 24, 2022

To configure access interface through Citrix SD-WAN Orchestrator service, see WAN links.

## **Configure Virtual IP addresses**

August 24, 2022

To configure Virtual IP Addresses through Citrix SD-WAN Orchestrator service, see WAN links.

## **Configure GRE Tunnels**

August 24, 2022

To configure GRE Tunnels using Citrix SD-WAN Orchestrator service, see GRE service.

# Setup dynamic paths for branch to branch communication

#### August 24, 2022

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 using Citrix SD-WAN Orchestrator service, see Virtual paths.

## **WAN-to-WAN** forwarding

#### August 24, 2022

Enabling WAN-to-WAN forwarding on the MCN, allows the MCN to advertise remote site routes.

- Clients are aware of MCN local routes and other client site routes
- From client perspective, all routes are considered as MCN routes

When WAN-to-WAN forwarding is not enabled on the MCN, Branch to Branch communication issues are encountered in the customer network.

Appliances running in client mode are unaware of other branches subnets until WAN-to-WAN forwarding is enabled on the MCN. Enabling this option makes the branch SD-WAN nodes aware of other branch subnets. The traffic destined to other branches is forwarded to MCN. MCN routes it to the correct destination.



# **Monitoring and Troubleshooting**

#### August 24, 2022

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 Active bandwidth testing

Adaptive bandwidth detection

# **Monitoring Virtual WAN**

August 24, 2022

## **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.

Dashboard	Monitoring Configuration
System Status	
Name: Model: Sub-Model: Appliance Mode: Serial Number: Management IP Addr Appliance Uptime: Service Uptime: Routing Domain Enab	MCN_23 VPX BASE MCN 67e0772c-5190-a2ee-d183-9244189b30a0 ***: 10.02.78.154 6 days, 13 hours, 22 minutes, 23.0 seconds 6 days, 13 hours, 14 minutes, 46.0 seconds
Local Versions	
Software Version: Built On: Hardware Version: OS Partition Version:	10.1.0.111.690027 Jun 21 2018 at 23:42:30 VPX 4.6
Virtual Path Servi	ice Status
Virtual Path MCN_23-	

# **Viewing Statistical Information**

August 24, 2022

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).

	Dashboard Moni	toring	Configuration									
٢	Statistics	Monitoring > Statistics										
	Flows											
	Routing Protocols	pretocols Statistics										
	Frewall Show: Petha (Summary) • Enable Auto Refresh 5 • seconds Refresh Ø Show Iasest data.											
	IKE/IPsec											
	IGMP	Path	Statistics Summary									
	Performance Reports	Filter:	in An	/ column •	Apply						Sho	w 100 • entries
	Qos Reports											
	Usage Reports	Num *	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (m5)	Loss %	kbps	Congestion
		1	MCN-DC-WL-1	Branch1-WL-1	GOOD	GOOD	Static	2	3	0.00	59.95	NO
	Availability Reports	2	MCN-DC-WL-1	Branch1-WL-2	GOOD	GOOD	Static	2	3	0.00	8.72	NO
	Appliance Reports	3	MCN-DC-WL-2	Branch1-WL-1	GOOD	GOOD	Static	2	3	0.00	8.72	NO
	DHCP Server/Relay	4	MCN-DC-WL-2	Branch1-WL-2	GOOD	GOOD	Static	2	3	0.00	11.82	NO
	VRRP Protocol	5	Branch1-WL-1	MCN-DC-WL-1	GOOD	GOOD	Static	2	3	0.00	8.89	NO
		6	Branch1-WL-1	MCN-DC-WL-2	GOOD	GOOD	Static	2	3	0.00	25.19	NO
		7	Branch1-WL-2	MCN-DC-WL-1	GOOD	GOOD	Static	2	3	0.00	11.84	NO
		8	Branch1-WL-2	MCN-DC-WL-2	GOOD	GOOD	Static	2	3	0.00	8.73	NO
		Showing 1	to 8 of 8 entries							First	Previous	1 Next Last
		Bandwidth	calculated over the last 412	78.42 seconds								

With 11.1.0 release, Neighbor Discovery Protocol (NDP) option is added for debugging neighbor discovery issues.

1. Select the NDP option from the Show drop-down menu and you can view the state of NDP along with the IPv6 addresses.

Statis	stics							
Show:	NDP	4	Enable Auto Refresh	5 \$ seconds Refresh				
NDP	Statistics							
Filter:		in Any	column					
Show 10	0 🗘 entries	Showing	1 to 2 of 2 entries				First Previou	us 1 Next Last
Num 🔺	Interface	VLAN	IP Addr	MAC Addr	Type	State	Is Router	Clear NDP Entry
0	2	0	2607:f0d0:2001:a::20	02:63:d7:64:85:4e	PERSISTENT	NDP_STATE_REACHABLE	Y	
1	2	0	fe80::63:d7ff:fe64:854e	02:63:d7:64:85:4e	END_USER	NDP_STATE_STALE	N	Clear
Showing	1 to 2 of 2 entr	ies					First Previou	us 1 Next Last

2. Select WAN Link from the drop-down menu. You can view the IPv6 address as well if you configured under IP Address tab.

Statistics						
Show: WAN Link	🖨 🗆 Enable Auto Refresh	5 🕏 seconds Refresh 🗹	Show latest data.			
WAN Link Statistics						
Filter: in Show 100 🗘 entries Sh	Any column	Apply	_		[	First Previous 1 Next Last
WAN Link	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age (ms)
demo_cl1_inet	N/A	2607:f0d0:2001:b::10	N/A	N/A	N/A	N/A
demo_cl1_inet2	N/A	172.16.100.1	N/A	N/A	N/A	N/A
demo_cl2_inet	N/A	2607:f0d0:2001:c::10	N/A	N/A	N/A	N/A
demo_cl2_inet2	N/A	172.16.150.1	N/A	N/A	N/A	N/A
demo_mcn_inet	demo_mcn_inet-Al-1	2607:f0d0:2001:a::10	N/A	N/A	N/A	N/A
demo_mcn_inet2	demo_mcn_inet2-AI-1	172.16.200.1	N/A	DISABLED	N/A	N/A
Showing 1 to 6 of 6 entries						First Previous 1 Next Last
Virtual Path Service Data R	ates					
Filter: in	Any column	Apply				

3. You can also view the Access Interface statistics.

Dashboard Mor	oring Configuration
Statistics	Monitoring > Statistics
Flows	
Routing Protocols	Statistics
Firewall	Show: Access Interfaces 🗘 🗅 Enable Auto Refresh 🛛 5 🗬 seconds Refresh 🖉 Show latest data.
IKE/IPsec	
IGMP	Access Interface Statistics
Performance Reports	Filter: In Any column C Apply
Qos Reports	
Usage Reports	Show 100 \$ entries Showing I to 2 of 2 entries First Previous 1 Next Last
Availability Reports	WAN Link Access Interface IP Address Proxy Address Proxy ARP State MAC Last ARP Reply Age (ms)
Appliance Reports	demo_mcn_inet demo_mcn_inet-Al-1 2607:f0d0:2001:a::10 N/A N/A N/A N/A N/A
DHCP Server/Relay	demo_mcn_inet2 demo_mcn_inet2-Al-1 1/2.16.200.1 N/A N/A N/A N/A N/A
VRRP	Showing 1 to 2 or 2 entries
PPPoE	Virtual Path Service Data Rates:
DNS	Filter: in Any column C Apply
	Show 100 🛊 entries Showing 1 to 8 of 8 entries 11 Next Lass
	WAN Link         Access Interface         Service Name         Direction         Virtual Path Service         Virtual Path Service R         Delta Virtual Path Service         Delta Virtual Path Service         Delta Virtual Path Service         Virtual Path Path Service         Virtual Path Service R         Delta Virtual Path Service         Delta Virtual Path Service         Virtual Path Service         Virtual Path Service         Delta Virtual Path Service         Virtual Path Service         Virtual Path Service <th< td=""></th<>
	demo_mcn_inet demo_mcn_inet-Al-1 demo_mcn-demo_cl2 Recv 20220845 3240115.88 413 74.23 46.47 0
	demo_mcn_inet demo_mcn_inet-Al-1 demo_mcn-demo_ci1 Recv 20196856 3252489.44 289 30.05 18.82 0

4. Open the **Show** drop-down menu.

In addition to the **Paths, NDP, Access Interface,** and **WAN Links statistics**, the **Show** menu also offers several more options for filtering and viewing statistical information.

Dashboard	Monitoring		ccess Interfaces opplications RP IDP											
Statistics	N	0	Classes											
Flows		E	thernet											
Routing Protocols		St II	ntranet											
Firewall	Sho	w √ P	aths (Summary)	🗆 Enal	ble Auto I	Refresh 5	🕏 seconds Refresh 🗹 Sho	ow latest data.						
IKE/IPsec		R	aths (Detailed) loutes											
IGMP		Pi A	pplication Routes											
Performance Reports	Filte	R R	tules tule Groups	olumn		Apply						Show 10	00 ± entries	
Qos Reports		S	ite VAN Link			•						311011	no v entres	
Usage Reports	Nu	m N	APLS Queues	To Lin	k	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion	
Availability Reports	1	0	WAN Link Usage GRE Tunnel	GRE Tunnel	io_cl1_in	et	BAD	GOOD	Static	2	2	4.44	41.89	NO
Appliance Reports	2	II N	Psec Tunnel Aulticast Group	io_cl1_in	et2	GOOD	GOOD	Static	2	2	3.01	16.03	NO	
DHCP Server /Relay	3	-	neuroTerzTurer n	ento_mcn_i	inet	GOOD	GOOD	Static	2	2	4.35	43.29	NO	
Lines Server/Relay	4		demo_cl1_inet2 d	lemo_mcn_i	inet2	GOOD	GOOD	Static	2	2	3.94	18.87	NO	
VRRP	5	(	demo_mcn_inet d	lemo_cl2_in	et	GOOD	GOOD	Static	2	2	4.12	37.61	NO	
PPPoE	6		demo_mcn_inet2 d	lemo_cl2_in	net2	GOOD	GOOD	Static	2	2	3.26	15.57	NO	
DNS	7		demo_cl2_inet d	lemo_mcn_i	inet	BAD	GOOD	Static	2	2	4.35	37.10	NO	
	8		demo_cl2_inet2 d	lemo_mcn_i	inet2	GOOD	GOOD	Static	2	2	3.73	16.71	NO	
	Sho	wing 1	to 8 of 8 entries							F	First Prev	ious 1	Next Last	
	Ban	dwidth	calculated over the last	234.578 s	econds									

Select a filter from the **Show** menu to view a table of statistical information for that topic.

## **Viewing Flow Information**

#### August 24, 2022

This section provides basic instructions for viewing Virtual WAN flow information.

To view flow information, do the following:

- 1. Log into the Management Web Interface for the MCN, and select the **Monitoring** tab. It opens the **Monitoring** navigation tree in the left pane.
- 2. Select the **Flows** branch in the navigation tree. It displays the **Flows** page with **LAN** to **WAN** preselected in the **Flow Type** field.

Statistics	Monitoring	Flows																				
Flows																						
Routing Protocols	Select Flo	ws																				
Firewall	Flow Type: Max Flows to D	LAN to	wan 🕑 w	AN to LA	N 🗏 1	interne	t Load Ba	lancing	Table 🔲 T	CP Termination Tal	ole											
IKE/IPsec	(Per Flow Type)	50 1																				
IGMP	Refresh		(rei)	,																		
Performance Reports																						
Qos Reports	Flows Dat	a																				
Usage Reports	Both LAN to W	AN and WAN to L	AN Flows																		Toggle	Columns
Availability Reports				-	_											-	Virtual	IPsec		App	_	
Appliance Reports	Address	Address	Direction	Port	Port	IPP	IP DSCP	Count	Type	Service Name	GW IP	Age (mS)	Packets	Bytes	PPS	kbps	Path Overhead khos	Overhead kbps	ID	Rule ID	Class	Class Typ
DHCP Server/Relay	172.147.21.5	172.147.12.83	LAN to WAN	2312	50829	тср	default	3	Virtual Path	MCN-DC-Branch1	LOCAL	5292	2	104	0.237	0.099	0.100	0.000	65	N/A	13	INTERACT
VRRP Protocol	172.147.12.8	172.147.21.53	WAN to LAN	50829	2312	тср	default	3	Virtual Path	MCN-DC-Branch1	LOCAL	5328	3	180	0.355	0.170	0.151	0.000	132	N/A	N/A	
	Total LAN to W. Total WAN to L	AN flows displayed: AN flows displayed:	l out of l l out of l																			
	4																					

3. Select the **Flow Type**. The **Flow Type** field is located in the **Select Flows** section at the top of the **Flows** page. Next to the **Flow Type** field is a row of check box options for selecting the flow

information you want to view. You can check one or more boxes to filter the information to be displayed.

- 4. Select the Max Flows to Display from the drop-down menu next to that field.
- It determines the number of entries to display in the Flows table. The options are: 50, 100, 1000.
- 6. (Optional) Enter search text in the **Filter** field. It filters the table results so that only entries containing the search text display in the table.

Тір

To see detailed instructions for using filters to refine **Flow** table results, click **Help** to the right of the **Filter** field. To close the help display, click **Refresh** in the bottom left corner of the **Select Flows** section.

7. Click **Refresh** to display the filter results. The figure shows a sample **Flows** page filtered display with all flow types selected.

Select Flows															
Flow Type: Max Flows to Display Per Flow Type): Filter (Optional): Refresh	Ø LAN to V 50 ▼ 172.79.2.83	NAN 🗷 N	WAN to LA	N 🗷 İr	ternet Load E	alancing Ta	ible 🗷 TC	P Termination	Table						
Flows Data															
Both LAN to WAN :	and WAN to LA	N Flows												To	ggle Columns
Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP IP DSC	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps
172.79.2.83	172.79.1.42	LAN to WAT	N 9281	58689	TCP defaul	t 9577	Virtual Path	DC-BR	LOCAL	5332	12038	1020734	0.079	0.033	0.031
172.79.2.83	172.79.1.42	LAN to WAR	N 9281	58690	TCP defaul	9631	Virtual Path	DC-BR	LOCAL	5346	12199	1075706	0.079	0.033	0.031
172.79.1.42	172.79.2.83	WAN to LAN	N 58689	9281	TCP defaul	t 18025	Virtual Path	DC-BR	LOCAL	5346	18025	1294598	0.157	0.052	0.062
172.79.1.42	172.79,2.83	WAN to LAP	N 58690	9281	TCP defaul	t 18244	Virtual Path	DC-BR	LOCAL	5360	18244	1389118	0.157	0.052	0.062
iotal LAN to WAN B Total WAN to LAN B Internet Load Balan	ows displayed: 2 ows displayed: 2 ocing Flows	2 out of 305 2 out of 305													
LAN IP WAN IP	Age (mS) W/	AN Link Flo	w Count												
Note: Only the active	e flows will be di	splayed and t	he total nur	nber of flow	s include active	and inactive	flows.								
Source IP Address	Dest IP Addre	ess Source Port	Dest Port IPP	Age (mS)	From Wan k	bps To Wa	in kbps Byte	es Pending To LA	N Byte	s Pending	To WAN	State			
fotal TCP Terminates	d flows displaye	d: 0 out of 30	5												

- 8. (Optional) Select the columns to include in the table. Do the following:
- 9. Click **Toggle Columns** at the top right corner of the **Flows Data** table. It reveals any deselected columns, and opens a check box above each column for selecting or deselecting that column. Deselected columns display grayed out, as shown in the figure.

#### Note

By default, all the columns are selected, which can cause the table to be truncated in the display, obscuring the **Toggle Columns** button. If so, a horizontal scroll bar displays beneath the table. Slide the scroll bar to the right to view the truncated section of the table and reveal the **Toggle Columns** button. If the scroll bar is not available, try resizing the width of your browser window until the scroll bar is revealed.

Balanci	ing Table	TCP TO	erminatio	on Table	2											
																Apply
8	8	8	×	8	8	8	8	8	8		0	0	0	0	0	Apph
I Hit ount	Service Type	Service Name	E LAN GW IP	Age (mS)	Ø Packets	Ø Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Typ
Hit ount 9598	Service Type Virtual Path	Service Name DC-BR	LAN GW IP LOCAL	Age (mS) 2435	Packets 12065	Bytes 1023038	PPS 0.033	Customer kbps 0.023	Virtual Path Overhead kbps 0.013	IPsec Overhead kbps	Rule ID 12	Class 9	Class Type REALTIME	Path DC-WL-2->BR-WL-1	Hdr Compression Saved Bytes N/A	App)
Hit ount 9598 9652	Service Type Virtual Path Virtual Path	Service Name DC-BR DC-BR	LAN GW IP LOCAL LOCAL	Age (mS) 2435 2434	Packets 12065 12226	Bytes 1023038 1078010	PPS 0.033	Customer kbps 0.023 0.023	Virtual Path Overhead kbps 0.013 0.013	Dverhead kbps 0.000	Rule ID 12	Class 9	Class Type REALTIME REALTIME	Path DC-WL-2->BR-WL-1 DC-WL-2->BR-WL-1	Hdr Compression Saved Bytes N/A N/A	Transmission Typ Duplicate, Reliab
<ul> <li>₩</li> /ul>	Service Type Virtual Path Virtual Path Virtual Path	Service Name DC-BR DC-BR	EAN GW IP LOCAL LOCAL LOCAL	Age (mS) 2435 2434 2448	Packets 12065 12226 18064	Bytes 1023038 1078010 1297454	PPS 0.033 0.034	Customer kbps 0.023 0.023 0.028	Virtual Path Overhead kbps 0.013 0.013 0.019	Drsec     Overhead     kbps     0.000     0.000	Rule ID 12 12 89	Class 9 9 N/A	Class Type REALTIME REALTIME N/A	Path DC-WL-2->BR-WL-1 DC-WL-2->BR-WL-1 N/A	United Served Bytes N/A N/A N/A N/A	App)

10. Click a check box to select or deselect a column.

- Source IP Address The source IP address for packets on this flow.
- Dest IP Address The destination IP address for packets on this flow.
- **Direction** The direction for packets on this flow LAN to WAN or WAN to LAN.
- Source Port The source port for packets on this flow.
- **Dest Port** The destination port for packets on this flow.
- IPP The IP protocol number for packets on this flow.
- IP DSCP The IP DSCP tag setting for packets on this flow.
- Hit Count The number of times this flow has been searched for and found.
- Service Type Indicates whether this flow type is Virtual path, Internet, or Intranet traffic.
- Service Name The name of the virtual path that the virtual path traffic is using.
- LAN GW IP IP address for the LAN gateway, if one is specified.
- Age (mS) The time (in milliseconds) since a packet was classified in this flow.
- Packets Number of packets sent over the life of the flow.
- Bytes Number of bytes sent over the life of the flow.

- **PPS** Packets per second over the period since the last refresh.
- Customer kbps/ Virtual Path Overhead kbps / IPsec Overhead kbps Kilobits per second over the period since the last refresh.
- Rule ID The ID of the rule that the traffic on this flow matched.
- App Rule ID The ID of app the rule that the traffic on this flow matched.
- Class The ID of the virtual path class that the traffic is using.
- **Class Type** The type of the virtual path class (Realtime, Interactive, Bulk) the traffic is using.
- Path The path that the traffic is using.
- Hdr Compression Saved Bytes The number of saved bytes due to header compression.
- Transmission Type The transmission type the traffic is using.
- Application The name of the application in use.
- 11. Click **Apply** (above the top right corner of the table). It dismisses the selection options, and refreshes the table to include only the selected columns.

Y 9.2.83		VAN to L	AN	Internet				<b>T</b> •	A T 1 1	
▼ 79.2.83				internet	Load Balanci	ng Table		Termina	tion Table	
9.2.83										
	Hel	p								
N to I AN Flo	14/5								1099	e containintia
		Source	Dest	Hit	Service	Service	LAN	Age		2.4
s Directi	ion	Source Port	Dest Port	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes
Directi	ion WAN	Source Port 9281	Dest Port 58689	Hit Count 9613	Service Type Virtual Path	Service Name DC-BR	LAN GW IP LOCAL	Age (mS) 12022	Packets 12084	<b>Bytes</b>
Directi .42 LAN to .42 LAN to	ion WAN WAN	Source Port 9281 9281	Dest Port 58689 58690	Hit Count 9613 9667	Service Type Virtual Path Virtual Path	Service Name DC-BR DC-BR	LAN GW IP LOCAL LOCAL	Age (mS) 12022 12040	Packets 12084 12246	Bytes 1024626 1080066
<b>Directi</b> .42 LAN to .42 LAN to .42 LAN to	ion WAN WAN	Source Port 9281 9281 58689	Dest Port 58689 58690 9281	Hit Count 9613 9667 18092	Service Type Virtual Path Virtual Path Virtual Path	Service Name DC-BR DC-BR DC-BR	LAN GW IP LOCAL LOCAL LOCAL	Age (mS) 12022 12040 12040	Packets 12084 12246 18092	Bytes 1024626 1080066 1299440
										Togg

#### **DPI Applications in SD-WAN Center**

In earlier releases, around 4,000 applications and configured with 800 services (550 Virtual Paths, 256 Intranet Services) can be identified. Storing this data would impact overall system performance (CPU cycles and disk space needed to store the data). It also has an impact, if reporting on data per Usage or Path is supported.

While the data path provides information on every application gathered in a minute, the per minute stats reporting determines the top 100 applications and report on the aggregate of all other applications as "other." If there is high diversity of trackable applications in their network, it might affect clarity of data, particularly if we want to track/graph the usage of an application over time and the application falls out of the top 100 limit.

## **Viewing Reports**

#### August 24, 2022

This section provides basic instructions for generating and viewing Virtual WAN reports about the local appliance using the Management Web Interface. An appliance can maintain up to 30 archives and purge the oldest archives which are more than 30 entries.

Dashboard	Monitoring Configuration
Statistics	Monitoring > Performance Reports
Flows	
Routing Protocols	Select Data Range
Firewall	Range 1 Day V Ending At: January V 3 V 2019 V 9 V 33 V am V Refresh
IKE/IPsec	
IGMP	Report
Performance Repo	ts Virtual Path: MCN_23-Site1 ▼ Direction: LAN to WAN ▼ Report: Bandwidth ▼
Qos Reports	
Usage Reports	
Availability Reports	01/02 01/02 01/02 01/02 01/02 01/02 01/02 01/02 01/03
Appliance Reports	
DHCP Server/Relay	Path: MCN 23-WL-1-
VRRP	Patr MCN 22-WL22     State WL3     Virtual Path: MCN 23-     Virtual Path: MCN 23-     Virtual Path: MCN 23-
PPPoE	Show All   Hide All interest in the graph above.
DNS	
	Data in this graph has had a sliding-average applied and is presented in 2-minute intervals
	Manage Database Archives
	Database: Current V Create New Delete
	Image: A second seco

#### Note

Reports generated on the Management Web Interface apply to the local appliance, only. To generate and view reports for the Virtual WAN, use the Virtual WAN Center Web Interface.
To generate and view Virtual WAN reports, do the following:

1. Log on to the Management Web Interface for the MCN, and select the **Monitoring** tab.

This opens the **Monitoring** navigation tree in the left pane.

2. Select a report type from the navigation tree.

The report types are listed as branches in the navigation tree, just below the **Flows** branch.

Performance Reports	
Qos Reports	
Usage Reports	
Availability Reports	
Appliance Reports	

The available report types are as follows:

- Performance Reports
- QoS Reports
- Usage Reports
- Availability Reports
- Appliance Reports
- 3. Select the report options.

In addition to the various types of reports, for each report type there are numerous options and filters for refining report results.

# Performance reports

Citrix SD-WAN can show performance statistics at the site, virtual path, or Direction (LAN to WAN and WAN to LAN) level. With Citrix SD-WAN, you can collect metrics that show the efficiency of each link in milliseconds. To view more detail, left-click and select a specific area of path or time frame in the graph line.

Statistics	Monitoring > Performance Reports
Flows	
Routing Protocols	Select Data Range
Firewall	Range:         1 Day         €         Ending At:         January         \$         30         \$         2020         7         \$         07         pm #         Refresh
IKE/IPsec	The range selected extends beyond the start time. Only available data is shown.
IGMP	Report
Performance Reports	
Qos Reports	Virtual Path: site2100-site1000  Direction: LAN to WAN  Report: Bandwidth
Usage Reports	wander han marked and a share a
Availability Reports	
Appliance Reports	01/30 01/30
DHCP Server/Relay	
VRRP	Path: site2100/L1-     site2100-site1000 Send Bandwidth
PPPoE	Virtual Path: site2100- site1000     30 kbps
DNS	Show All   Hide All 25 kbps
+ WAN Optimization	
	15 kbps m home home home mal
	10 kbps
	5 liber
	3 xuya e
	0 kbps 01/30 01/30 01/30 01/30 01/30 08:00 08:30 09:00 09:30 10:00
	Data in this graph is presented in 1-minute intervals
	Manage Database Archives
	Database: Current   Create New Delete

You can select the data range as needed with the following fields to view the performance report:

- Virtual Path: Select the Virtual Path from the drop-down list.
- Direction: Select the Direction as required (LAN to WAN or WAN to LAN).
- **Report:** Select the following network parameters to view the report:
  - Bandwidth
  - Latency
  - Jitter
  - Loss
  - Quality

### **QoS reports**

You can monitor the application QoS report such as the number of packets or bytes uploaded, downloaded, or dropped at each Site, WAN Link, Virtual Path, and Path level.

#### Citrix SD-WAN 11.5



You can view the following metrics:

- **Real-time:** Bandwidth consumed by applications that belong to the real-time class type in the Citrix SD-WAN configuration. The performance of such applications depends on a great extent upon network latency. A delayed packet is worse than a lost packet (for example, VoIP, Skype for Business).
- **Interactive:** Bandwidth consumed by applications that belong to the interactive class type in the Citrix SD-WAN configuration. The performance of such applications depends on a great extent upon network latency, and packet loss (for example, XenDesktop, XenApp).
- **Bulk:** Bandwidth consumed by applications that belong to the bulk class type in the Citrix SD-WAN configuration. These applications involve little human intervention and are mostly handled by the systems themselves (for example, FTP, backup operations).
- **Control:** Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.

### Usage reports

The Usage reports deliver the Virtual paths usage information.

	intering y objections
ows	
outing Protocols	Select Data Range
rewall	Range: 1 Day   Ending At: January   27   2020   7   00   am   Refresh
KE/IPsec	
GMP	Report
erformance Reports	Report: Site   Name: Dallas_MCN   Direction: LAN to WAN   Plot Type: Line
los Reports	Virtual Path: 00 25 kbps
Jsage Reports	Virtual Path: Dallas MCN-APAC RCN 22.5 kbps
vailability Reports	Virtual Path:     Dallas_MCN-California
Appliance Reports	Virtual Path:     20 kbps     20 kbps
HCP Server/Relay	Dallas MCN-Newyork Virtual Path: 17.5 kbps
/RRP	Dallas_MCN-Texas Internet: Dallas_MCN- Internet: Dallas_MCN-
PPoE	Show All   Hide All
DNS	
	10 kbps
	7.5 kbps
	5 kbps
	2.5 kbps
	0 kbps 01/26 01/26 01/26 01/26 01/26 01/27 01/27 01/27

- **Report:** Select **Site** or **WAN Link** from the drop-down list to view the report.
- Name: Select the name of the site or WAN link from the drop-down list.
- Direction: Select the direction as required (LAN to WAN or WAN to LAN).
- **Plot Type:** Select the Plot type from the drop-down list (Line or Area).

# **Availability reports**

In this report, you can view the availability data of WAN Links, Paths, and Virtual Paths. You can also switch to or choose a specific time frame, such as 1 hour, 24 hours, and 7 days to see the available data. The Paths and Virtual Paths data are represented in a **DD:HH:MM:SS** format.

Dashboard Mo	Configuration													
Statistics	Monitoring > Availability Reports													
Flows														
Routing Protocols	Select Timeframe													
Firewall	For the period from 7:01 on 1/26/2020 to 7:01 or All times are represented in days (if available), hou	n 1/27/2020   S urs (if available),	witch to: 1 hou minutes and se	r   24 ho conds. D	urs   7 days   A D:HH:MM:SS	dl Availab	le Data							
IKE/IPsec														
IGMP	Paths and Virtual Paths													
Performance Reports		Uptime	Goodtime		Badtim	e		D	owntime			Inc	dents	
Qos Reports	-			Total	Loss	Silence	Peer	Total	Silence	Peer	Total	Loss	Silence	Pe
Usage Reports	Virtual Path Dallas_MCN-ANZ_RCN	1:00:00:00	1:00:00:00	0:00	0:00	5								
osage reports	Dallas_MCN-queue1->ANZ_RCN-queue1	1:00:00:00	1:00:00:00	0:00		0:00	0:00	0:00	0:00	0:00	0		0	
Availability Reports	ANZ_RCN-queue1->Dallas_MCN-queue1	1:00:00:00	23:59:10	0:50	0:00	0:50		0:00	0:00		5	0	5	-
Appliance Reports	Virtual Path Dallas_MCN-APAC_RCN	1:00:00:00	1:00:00:00	0:00	0:00	14								
DHCP Server/Relay	Dallas_MCN-queue1->APAC_RCN-queue1	1:00:00:00	1:00:00:00	0:00		0:00	0:00	0:00	0:00	0:00	0		0	
VRRP	APAC_RCN-queue1->Dallas_MCN-queue1	1:00:00:00	23:57:40	2:20	0:00	2:20		0:00	0:00		14	0	14	
PPPoE	Virtual Path Dallas_MCN-California	1:00:00:00	23:59:42	0:18	0:00	2								
DNS	Dallas_MCN-queue1->California-queue1	23:58:36	23:58:36	0:00		0:00	0:00	0:00	0:00	0:00	2		0	
	California-queue1->Dallas_MCN-queue1	1:00:00:00	23:59:40	0:20	0:00	0:20		0:00	0:00		2	0	2	
	Virtual Path Dallas_MCN-EMEA_RCN	0:00	0:00	0:00	1:00:00:00	0								
	Dallas_MCN-queue1->EMEA_RCN-queue2	0:00	0:00	0:00		0:00	0:00	1:00:03:45	1:00:03:45	0:00	0		0	
	EMEA_RCN-queue2->Dallas_MCN-queue1	0:00	0:00	0:00	0:00	0:00		1:00:03:45	1:00:03:45		0	0	0	
	Virtual Path Dallas_MCN-Newyork	1:00:00:00	1:00:00:00	0:00	0:00	8								
	Dallas_MCN-WL-2->Newyork-WL-2	0:00	0:00	0:00		0:00	0:00	0:00	0:00	0:00	0		0	
	Dallas_MCN-queue1->Newyork-queue1	1:00:00:00	1:00:00:00	0:00		0:00	0:00	0:00	0:00	0:00	0		0	
	Newyork-WL-2->Dallas_MCN-WL-2	0:00	0:00	0:00	0:00	0:00		1:00:03:45	1:00:03:45		0	0	0	
	Newyork-queue1->Dallas_MCN-queue1	1:00:00:00	23:58:40	1:20	0:00	1:20		0:00	0:00		8	0	8	
	Virtual Path Dallas_MCN-Texas	1:00:00:00	23:59:42	0:18	0:00	12								
	Dallas_MCN-queue1->Texas-queue1	23:58:35	23:58:35	0:00		0:00	0:00	0:00	0:00	0:00	2		0	
	Texas-queue1->Dallas_MCN-queue1	1:00:00:00	23:58:00	2:00	0:00	2:00		0:00	0:00		12	0	12	
	WAN Links													
					Uptim	e		Do	wntime				Inc	ider
	Dallas_MCN-WL-2				0:0	0		1:0	0:00:00					
	Dallas_MCN-queue1				1:00:00:0	0			0:00				No do	wnti

# **Appliance reports**

Appliance report delivers Network traffic and System usage reports. Click each link to view or monitor the appliance graph by day, weekly, monthly, and yearly.



# **Viewing Firewall Statistics**

### August 24, 2022

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.

To view Firewall Statistics:

- 1. Navigate to **Monitoring > Firewall.**
- 2. Select, Connections, Filter Policies, or NAT Policies as required.
- 3. Set the filtering criteria as required.
- 4. Click Refresh.

## 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.

# **Diagnostics**

#### August 24, 2022

**Citrix SD-WAN Diagnostics** utilities provide the following options to test and investigate connectivity issues:

- Ping
- Traceroute
- Packet Capture
- Path Bandwidth
- System Info
- Diagnostics Data
- Events
- Alarms
- Diagnostics Tool
- Site Diagnostics

The diagnostic options in the Citrix SD-WAN Dashboard control data collection.

## Ping

To use the **Ping** option, navigate to **Configuration > Diagnostics** and select **Ping**. You can use Ping to check host reachability and network connectivity.

#### Citrix SD-WAN 11.5

Appnance seconds	Configuration > System Maintenance > Diagnostics
- Virtual WAN	
- System Maintenance	Ping Traceroute Packet Capture Path Bandwidth System Info Diagnostic Data Events Alarms Diagnostics Too
Delete Files	Site Diagnostics
- Restart System - Date/Time Settings	Ping
- Diagnostics	Routing Domain: Default_RoutingDom: \$ IP address: 192.168.10.XX Ping count: 5 Packet size: 70
- Update Software - Configuration Reset Factory Reset	Ping
	Routing Domain:     IP address:     Ping count:     Packet size:     VirtualInterface-4:19 €       Ping Interface     5     70     Via:     VirtualInterface-4:19 €
	Results

Select the routing domain. Provide a valid IP address, number of ping counts (number of times to send the ping request), and packet size (number of data bytes). Click **Stop Ping** to stop an ongoing ping search.

You can ping through a specific interface. Select the routing domain and specify the IP address with ping count, packet size, and select the virtual interface from the drop-down list.

#### Traceroute

To use **Traceroute** option, navigate to **Configuration > expand System Maintenance > Diagnostics** and select **Traceroute**.

Dashboard Monitoring	Configuration
+ Appliance Settings	Configuration > System Maintenance > Diagnostics
+ Virtual WAN	
- System Maintenance	Ping Traceroute Packet Capture Path Bandwidth System Info Diagnostic Data Events Alarms Diagnostics Tool
Delete Files	Site Diagnostics
- Restart System - Date/Time Settings	Trace Route
- Local Change Management Diagnostics	Path: Dallas_MCN-queue1-\$
- Update Software - Configuration Reset	Тгасе
Factory Reset	Results
	Trace Route initiated on Virtual Path Dallas_MCN-ANZ_RCN, Path Dallas_MCN-queuel->ANZ_RCN-queuel. Please wait while the trace is completed. Trace Route Results: Trace Route Successful Virtual Path: Dallas_MCN-ANZ_RCN Path: Dallas_MCN-queuel->ANZ_RCH-queuel Trace Route to 192.168.90.10, destination was unreachable, 50 hops attempted. hops rttl rtt2 rtt3 mean rtt 1 *.*.* 3 *.*.* 4 *.*.* 5 *.*.* 6 *.*.*

**Traceroute** helps to discover and show the path or route to a remote server. Use the **Traceroute** option as a debugging tool to detect the points of failure in a network.

Select a path from the drop-down list and click **Trace**. You can view the details under **Results** section.

# **Packet capture**

You can use the **Packet Capture** option to intercept the real-time data packet that is traversing over the selected active interface present in the selected site. Packet capture helps you to analyze and troubleshoot the network issues.

#### Citrix SD-WAN 11.5

Dashboard Monitoring	Configuration						
Sushbourd monitoring	comgutation						
+ Appliance Settings	Configuration > System	Maintenance > Diagnos	tics				
+ Virtual WAN	-						
- System Maintenance	Ping Tracerout	e Packet Capture	Path Bandwidth	System Info	Diagnostic Data	Events Alarm	ns
Delete Files Restart System	Diagnostics Tool	Site Diagnostics					
· Date/Time Settings	Packet Capture						
Local Change Management	Interfaces:		1/1 ×1/2 × 1/4 ×	1/6			
Diagnostics	Duration (seconds):	3					
Configuration Reset	May # of packats to view						
Factory Reset	Capture Eilter (Optional)		•			Halp	
	Capture					Tielp	
	Note: Capture file size w Atleast 1 interface needs	II not exceed 575 MB. On to be selected to trigger a	ce the packet capture file r a packet capture.	eaches this size, packet ca	pturing will be stopped	1.	
		-					_
	Gathering Requested	Data					_
	Generating packet capture in Packet Capture Successfi	formation					
	Packet Capture File						
	A binary file containir	ng the packet data cap	ured during the last su	ccessful packet captur	e. This file can be or	pened in the	-
	Wireshark for analysi	5.	-			ne	
	The downloaded Packet MGMT -> tn-mgt0	capture file displays intern	al labels for interface nam	es. Here are the mappings	for this platform:		
	1/1 -> dpdk-1_1 1/4 -> dpdk-1_4						
	1/2 -> dpdk-1_2 1/6 -> dpdk-1_6						
	Download						
	Packet View						
							_
	# Interface	Name Protocol	Time	Length	Source	Destination	Src
	1. 1/2 2. 1/2	UDP UDP	May 8, 2019 06:06:30 May 8, 2019 06:06:30	.415518572 UTC 1442 .415524972 UTC 1442	172.168.1.10	152.168.1.10 172.168.1.10	4980 4980
	3. 1/2 4. 1/2	UDP UDP	May 8, 2019 06:06:30 May 8, 2019 06:06:30	.415628324 UTC 1442	152.168.1.10 172.168.1.10	172.168.1.10 152.168.1.10	4980 4980
	5. 1/2	UDP	May 8, 2019 06:06:30	.415858329 UTC 1442	152.168.1.10	172.168.1.10	4980
	7. 1/2	UDP	May 8, 2019 06:06:30	.416073413 UTC 1442	172.168.1.10	152.168.2.10	4980
	9. 1/1	TCP	May 8, 2019 06:06:30 May 8, 2019 06:06:30	.321504133 UTC 1384	152.168.1.10	172.168.1.10	80
	10. 1/2 11. 1/2	UDP UDP	May 8, 2019 06:06:30 May 8, 2019 06:06:30	.416266227 UTC 1442 .416435190 UTC 1442	152.168.1.10 172.168.1.10	172.168.1.10 152.168.1.10	4980 4980
	12. 1/2	UDP	May 8, 2019 06:06:30	.416525402 UTC 114	172.168.1.10	152.168.2.10	4980
	13. 1/1 14. 1/2	UDP	May 8, 2019 06:06:30 May 8, 2019 06:06:30	.416529932 UTC 114	172.168.1.10	152.168.2.10	4980
	15. 1/1 16. 1/2	TCP	May 8, 2019 06:06:30 May 8, 2019 06:06:30	.321514773 UTC 54 .416651685 UTC 1442	152.168.1.52	172.168.1.51	2163 4980
	17. 1/2	UDP	May 8, 2019 06:06:30	.416693075 UTC 1442	152.168.1.10	172.168.1.10	4980
	18. 1/2 19. 1/2	UDP	May 8, 2019 06:06:30 May 8, 2019 06:06:30	.416783167 UTC 1442 .416881149 UTC 1442	172.168.1.10 172.168.1.10	152.168.2.10	4980 4980
	20. 1/2	UDP	May 8, 2019 06:06:30	.417039802 UTC 1442	152.168.1.10	172.168.1.10	4980
	22. 1/2	UDP	May 8, 2019 06:06:30	.417132114 UTC 114	172.168.1.10	152.168.1.10	4980
	23. 1/2 24. 1/1	UDP TCP	May 8, 2019 06:06:30 May 8, 2019 06:06:30	.417135804 UTC 1442 .321517954 UTC 54	172.168.1.10 152.168.1.52	152.168.2.10 172.168.1.51	4980 6265
	25. 1/2 26. 1/1	UDP TCP	May 8, 2019 06:06:30 May 8, 2019 06:06:30	.417178605 UTC 114 .321648046 UTC 1384	172.168.1.10 172.168.1.51	152.168.1.10 152.168.1.52	4980 80

Provide the following inputs for packet capture operation:

• **Interfaces** - Active interfaces are available for packet capture for the SD-WAN appliance. Select an interface or add interfaces from the drop-down list. At least one interface needs to be selected to trigger a packet capture.

### Note:

The ability to run packet capture across all the interfaces at once helps to speed up the troubleshooting task.

- **Duration(seconds)** Duration (in seconds) for how long the data have to be captured.
- Max # of packets to view Maximum limit of packets to view in the packet capture result.
- **Capture Filter (Optional)** The optional Capture Filter field accepts a filter string that is used to determine which packets are captured. Packets are compared to the filter string and if the comparison result is true, then the packet is captured. If the filter is empty, then all packets are captured. For more information, see Capture Filters.

Following are some examples of this capture filter:

- Ether proto\ARP Captures only ARP packets
- Ether proto\IP Captures only IPv4 packets
- VLAN 100 Captures only packets with a VLAN of 100
- Host 10.40.10.20 Captures only IPv4 packets to or from the host with the address 10.40.10.20
- Net 10.40.10.0 Mask 255.255.255.0 Captures only IPv4 packets in the 10.40.10.0/24 subnet
- IP proto \ TCP Captures only IPv4/TCP packets
- Port 80 Captures only IP packets to or from port 80
- Port range 20–30 Captures only IP packets to or from ports 20 through 30

Note

The maximum capture file size limit is up to 575 MB. Once the packet capture file reaches this size, packet capturing is stopped.

Click **Capture** to view the packet capture result. You can also download a binary file containing the packet data captured during the last successful packet capture.

### Gathering requested data

You can see the status of generating packet capture information (whether packet capture is successful or no packet capture) in this table.

### Packet capture file

Packets are captured as a binary data during the last successful packet capture. You can download the binary file to analyze the packet information offline. The interfaces name is different in the downloaded file as compared to the GUI interface. To view the internal interface mapping, click the Help option.

Packet Capture File	
A binary file containing the packet data captured during the last successful packet capture. This file can be opened in Wireshark for analysis.	Help
The downloaded Packet capture file displays internal labels for interface names. Here are the mappings for this platform: MGMT -> tn-mgt0 1/4 -> dpdk-1_4 1/5 -> dpdk-1_1 1/5 -> dpdk-1_5 1/2 -> dpdk-1_2 LTE-1 -> dpdk-1te_1 Download	

You need **Wireshark** software 2.4.13 version or higher to open and read the binary file.

🚄 📕 🧕 💿 🚞 🗋 🕺 🗳 🍝 🏓	警 🐔 👱 🗔	📃 🔍 Q, Q, 🎹			
Apply a display filter <೫/>					Expression +
Time	Source	Destination	Protocol Length	Interface name	Src Mac
1 2019-04-26 05:53:09.403929649	10.103.40.80	192.168.60.15	UDP	306 dpdk-lte_1	9e:15:
2 2019-04-26 05:53:09.808203024	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
3 2019-04-26 05:53:09.808215048	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
4 2019-04-26 05:53:10.026787042	fe80::5834:4eff:fe.	. ff02::2	ICMPv6	70 dpdk-1_1	5a:34:
5 2019-04-26 05:53:10.811549725	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
6 2019-04-26 05:53:10.811561358	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
7 2019-04-26 05:53:11.404405624	10.103.40.80	192.168.60.15	UDP	306 dpdk-lte_1	9e:15:
8 2019-04-26 05:53:11.815088189	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
9 2019-04-26 05:53:11.815100522	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
10 2019-04-26 05:53:12.818065232	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
11 2019-04-26 05:53:12.818156899	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
12 2019-04-26 05:53:13.405512485	10.103.40.80	192.168.60.15	UDP	306 dpdk-lte_1	9e:15:
13 2019-04-26 05:53:13.821801944	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
14 2019-04-26 05:53:13.821813477	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
15 2019-04-26 05:53:14.834919479	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
16 2019-04-26 05:53:14.834931891	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
17 2019-04-26 05:53:15.406160515	10.103.40.80	192.168.60.15	UDP	306 dpdk-lte_1	9e:15:
18 2019-04-26 05:53:15.838934651	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
19 2019-04-26 05:53:15.838946928	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
20 2019-04-26 05:53:16.842346703	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
21 2019-04-26 05:53:16.842358521	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
22 2019-04-26 05:53:17.406642988	10.103.40.80	192.168.60.15	UDP	306 dpdk-lte_1	9e:15:
23 2019-04-26 05:53:17.845891359	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
24 2019-04-26 05:53:17.845903254	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
25 2019-04-26 05:53:18.850000114	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
26 2019-04-26 05:53:18.850012213	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
27 2019-04-26 05:53:19.407464852	10.103.40.80	192.168.60.15	UDP	306 dpdk-lte_1	9e:15:
28 2019-04-26 05:53:19.867551012	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte_1	9e:15:
29 2019-04-26 05:53:19.867562750	10.103.40.80	192.168.60.15	UDP	226 dpdk-lte 1	9e:15:e7:2
Frame 1: 306 bytes on wire (2448 bits), 306 bytes ca	ptured (2448 bits) or	interface 0			
<pre>&gt; Interface id: 0 (dpdk-lte_1)</pre>					
Encapsulation type: Ethernet (1)					
Arrival Time: Apr 26, 2019 11:23:09.403929649 IST					
[Time shift for this packet: 0.000000000 seconds]					
Epoch Time: 1556257989.403929649 seconds					
[]ime delta from previous captured frame: 0.000000	0000 seconds]				
[lime delta from previous displayed frame: 0.00000	seconds]				
[]ime since reference or first frame: 0.000000000	seconds]				
Frame Number: 1					

### **Packet view**

If the packet capture file size is more, it takes more time to complete the rendering process for the packet view. In this case, it is recommended to download the file and use **Wireshark** for analysis instead of relying on the **Packet View** result.

### Path bandwidth

To use the **Path Bandwidth** feature, navigate to **Configuration > expand System Maintenance > Diagnostics** and select **Path Bandwidth**.

	Configurat	tion						
<ul> <li>Appliance Settings</li> </ul>	Configura	Jtion > System Maintena	nce > Diagnostics					
· Virtual WAN	Rea	Tracemute	Darbat Cantura Dath Ran	ukuidth Suttam Info	Diagonatic Data	Fuente Alarme	Diagonatics Tool	
System Maintenance	ring	Insceloute	Packet captore Paul bai	Systematic	Diagnostic Data	Evens Manns	Diagnosocs room	
Delete Files	Instant	t Path Bandwidth Test	ing					
Restart System	Dath							
Local Change Management	Tert		1014010040000800					
Diagnostics	1834							
- Update Software	Decult	re .						
Configuration Reset	nesure	,						
ractory neset	Minimum Ba Maximum Ba Average Ba	andwidth:936564 kbps andwidth:1213863 kbps andwidth:1109046 kbps						
	Schedu	ule Path Bandwidth Te	sting					
	Add	1						
	Pa	ith Name	Frequency		Day of Week		Hour	Minute
	Apply	Settings						
	Histor	y Path Bandwidth Tes	ting Result					
	Show 50	• ent	ies Showing 1 to 27 of 27 entries	Search				
								First Previous 1 Next La:
	Num	From Link	To Link	Test Time	Min Bandwidth	h (kbps) N	lax Bandwidth (kbps)	Avg Bandwidth (kbps)
	1	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 2:01:03 PM	2883972	5	099707	4357330
	2	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 4:01:03 PM	3109115	3	872000	3616157
	3	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 6:01:04 PM	3041280	4	119960	3518949
	4	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 8:01:04 PM	2769377	3	700672	3276124
	5	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 10:01:04 PM	409245		574153	2429269
						-		2405205
	6	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 12:01:04 AM	2481755	4	001684	3198214
	6 7	RCN1-5100-WL-1 RCN1-5100-WL-1	MCN-5100-WL-1 MCN-5100-WL-1	2/18/2018, 12:01:04 AM 2/18/2018, 2:01:04 AM	2481756 2549853	4	001684 872000	3198214 3236546
	6 7 8	RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1	MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1	2/18/2018, 12:01:04 AM 2/18/2018, 2:01:04 AM 2/18/2018, 4:01:03 AM	2481756 2549853 3204413	3	001684 872000 982628	3198214 3236546 3642643
	6 7 8 9	RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1	MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1	2/18/2018, 12:01:04 AM 2/18/2018, 2:01:04 AM 2/18/2018, 4:01:03 AM 2/18/2018, 4:01:03 AM 2/18/2018, 6:01:03 AM	2481756 2549853 3204413 2997677	3	001684 872000 982628 672357 288360	2405053 3190214 3226546 36642643 3664015 3013666
	6 7 8 9 10	RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1	MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1	2/18/2018, 12:01:04 AM 2/18/2018, 2:01:04 AM 2/18/2018, 4:01:03 AM 2/18/2018, 6:01:03 AM 2/18/2018, 8:01:04 AM	2481756 2549853 3204413 2997677 2248258 2410356	4	001684 872000 982628 672357 288360 272387	3136214 3226546 3642643 3664018 3654018 3612666 3812600
	6 7 8 9 10 11	RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1	MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1	2/18/2018, 12:01:04 AM 2/18/2018, 201:04 AM 2/18/2018, 4:01:03 AM 2/18/2018, 6:01:03 AM 2/18/2018, 6:01:04 AM 2/18/2018, 10:01:04 AM 2/18/2018, 10:01:04 AM	2481755 2549853 3204413 2997677 2248256 2410236 2410236	4 3 4 6 3	001684 872000 982628 672357 288360 372387 401852	3136214 3226546 3640543 3664018 3612666 2816032 260752
	6 7 8 9 10 11 12 13	RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1	MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1	2/18/2018, 1220104 AM 2/18/2018, 20104 AM 2/18/2018, 20104 AM 2/18/2018, 40103 AM 2/18/2018, 60104 AM 2/18/2018, 100104 AM 2/18/2018, 100104 AM	2481755 2548653 3204413 2997677 2248258 2410236 2613800 2304766	4 3 4 6 3 4 4 4 4	001684 872000 982638 672357 288360 372387 401852 059961	3158214 3226546 3640149 3664018 360322 2816032 38063752 31001900
	6 7 8 9 10 11 12 13 14	RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1 RCN1-5100-WL-1	MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1	2/18/2018, 12/01/4 AM 2/18/2018, 2010/4 AM 2/18/2018, 401/03 AM 2/18/2018, 401/03 AM 2/18/2018, 801/04 AM 2/18/2018, 1001/04 AM 2/18/2018, 12/01/04 AM 2/18/2018, 2010/4 PM 2/18/2018, 2010/4 PM	2481756 2548653 8204413 2997677 2240258 2410236 2613600 22304266 2173340	4 3 4 6 3 4 4 4 4	001684 872000 982628 672857 288860 372887 401852 059961 059961	3158214 3226546 3640148 3664018 360502 2816032 356032 356032 3101510 2235146
	6 7 8 9 10 11 12 13 14 15	RCN-5100-W-1 RCN-5100-W-1 RCN-5100-W-1 RCN-5100-W-1 RCN-5100-W-1 RCN-5100-W-1 RCN-5100-W-1 RCN-5100-W-1 RCN-5100-W-1 RCN-5100-W-1	MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1 MCN-5100-WL-1	2/18/2018, 12/01/4 AM 2/18/2018, 2010/4 AM 2/18/2018, 401/03 AM 2/18/2018, 401/03 AM 2/18/2018, 801/04 AM 2/18/2018, 12/01/04 AM 2/18/2018, 12/01/05 PM 2/18/2018, 2010/4 PM 2/18/2018, 2010/4 PM 2/18/2018, 2010/4 PM	2461756 254853 8204413 2597677 2240258 2410236 2613600 2334266 2173340 2613600	4 3 4 6 4 4 4 3 3 4 4 3 3 3 3 3	001684 972000 982628 882628 882628 882628 882628 982628 98270 988428 888428	3158214 3226546 36443643 3664018 36012666 2816032 38563752 3101510 2325146 3022890
	6 7 8 9 10 11 12 13 14 15 16	RCIG-5100-W-1 RCIG-5100-W-1 RCIG-5100-W-1 RCIG-5100-W-1 RCIG-5100-W-1 RCIG-5100-W-1 RCIG-5100-W-1 RCIG-5100-W-1 RCIG-5100-W-1 RCIG-5100-W-1	MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1	2/18/2018, 120104 AM 2/18/2018, 20104 AM 2/18/2018, 40103 AM 2/18/2018, 40103 AM 2/18/2018, 80104 AM 2/18/2018, 120105 PM 2/18/2018, 20104 PM 2/18/2018, 20104 PM 2/18/2018, 40103 PM 2/18/2018, 60103 PM	2481756 254853 8204413 2997677 2248258 2410236 2613600 2334266 213340 2613600 1676656	4 3 3 4 6 3 4 4 3 3 3 3 3 3 3 3 3	001684 972000 972000 972357 972387 97259 97259 97259 97259 97259 977597	3158214 3226546 3643048 3664018 360302 2816032 38563752 3100510 22278146 3002890 2655280
	6 7 8 9 10 11 12 13 14 15 16 17	R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3	MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1	2/18/2018.1201.04 AM 2/18/2018.201.04 AM 2/18/2018.401.03 AM 2/18/2018.601.03 AM 2/18/2018.601.03 AM 2/18/2018.1001.04 AM 2/18/2018.1201.08 PM 2/18/2018.201.08 PM 2/18/2018.611.03 PM 2/18/2018.611.03 PM	2481756 254853 8204413 2997677 2248258 2410236 2613600 2334265 2173340 2613600 2613600 1676656 1954099	4 3 3 4 6 3 3 4 4 3 3 3 3 3 3 3 3	001684 972000 972357 772357 772387 972589 905961 059661 059661 059661 958949 958944	2150200 3136214 3236546 3664018 3654018 360322 3816032 3816032 3816032 3816032 3816032 3816032 3816032 3816032 3816032 3816032 381604 3910300 2552146 3910300 2553200 257584
	6 7 8 9 10 11 12 13 14 15 16 17 18	R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3	MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1	2/18/2018.120104 AM 2/18/2018.20104 AM 2/18/2018.20104 AM 2/18/2018.60103 AM 2/18/2018.60103 AM 2/18/2018.100104 AM 2/18/2018.120108 PM 2/18/2018.20104 PM 2/18/2018.61103 PM 2/18/2018.61103 PM 2/18/2018.00103 PM 2/18/2018.100103 PM	2481756 254853 254853 2597677 2248258 2410236 2613600 2613600 2613600 2613600 1676656 1954089 2161116	4 3 4 4 6 3 4 4 3 3 3 3 3 3 3 3 3 3	001684 982628 982628 972357 772387 772387 905961 059661 059661 059661 059661 059662 059664 0596666 0596666 0596666 05966666 05966666 059666666666 0596666666666	2400200 3158214 3236546 3664018 3664018 36032 2806032 2806032 300390 2829146 30021890 2655280 2855280
	6 7 8 9 10 11 12 13 14 15 16 17 18 19	R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3 R04-520046-3	MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1	2/18/2018.120104 AM 2/18/2018.20104 AM 2/18/2018.20104 AM 2/18/2018.40103 AM 2/18/2018.60103 AM 2/18/2018.100104 AM 2/18/2018.120108 PM 2/18/2018.20104 PM 2/18/2018.40103 PM 2/18/2018.61103 PM 2/18/2018.00103 PM 2/18/2018.100103 PM 2/19/2018.120103 AM	2481756 254853 22967677 2248258 2410236 2613600 2613600 2613600 2613600 1676656 1954099 2161116 2986571	4 3 3 4 6 3 3 4 4 3 3 3 3 3 3 3 3 4 4 3 3 3 3	001684 982628 982628 972357 772387 772387 905961 059661 059661 059661 059661 059661 059661 059661 059664 059765	140000 3158214 3236546 3664018 3664018 36032 2806032 2806032 2806032 2806032 2806032 2806032 2806032 2806032 2800068 2805280
	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	R01-5100/W-1	MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1	2/18/2018.120104 AM 2/18/2018.20104 AM 2/18/2018.20104 AM 2/18/2018.40103 AM 2/18/2018.60103 AM 2/18/2018.100104 AM 2/18/2018.20108 PM 2/18/2018.20108 PM 2/18/2018.40103 PM 2/18/2018.61103 PM 2/18/2018.00103 PM 2/18/2018.100103 PM 2/19/2018.120103 AM 2/19/2018.20104 AM	2481756 248853 254853 200413 2997677 2248258 2410236 2613600 2613600 2613600 2613600 1676656 1954089 2161116 2986971 26154084	4 3 3 4 6 3 4 4 4 3 3 3 3 3 3 3 3 4 4 4 4	001684 982628 982628 982628 982628 982628 982628 98262 9826 9826	1400000 3158214 3236546 3664018 3664018 360322 2816032 2816032 2816032 2816032 2816032 2816032 2816032 281604 300058 28158 285280 2855280 2855280 2855280 2855280 2855280
	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21	R01-5100-W-1	MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1 MCN-5100-W-1	2/18/2018.120104 AM 2/18/2018.20104 AM 2/18/2018.20104 AM 2/18/2018.60103 AM 2/18/2018.60103 AM 2/18/2018.00104 AM 2/18/2018.20108 PM 2/18/2018.20108 PM 2/18/2018.60108 PM 2/18/2018.60108 PM 2/18/2018.00108 PM 2/18/2018.00108 PM 2/19/2018.100108 AM 2/19/2018.20104 AM 2/19/2018.40104 AM	2481756 248853 2548653 2597677 2248258 2410236 2613600 2334265 2173340 2613600 2613600 2613600 1676656 1954093 2161116 2986971 2514084 2358043	4 3 3 4 6 3 3 4 4 3 3 3 3 3 3 3 3 3 4 4 4 4	001684 982628 982628 982628 982628 982628 982628 98260 98960 98960 98980 98980 98980 97848 978498 079765 182760 059961	140000 3198214 3236546 3664018 3664018 36032 2816032 38063752 38063752 3001900 2929146 3001900 2929146 3001900 29295146 300190 295584 2900068 3821158 3899381 3756691
	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22	RCII-5100-W-1	MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1	2/18/2018, 120104 AM 2/18/2018, 20104 AM 2/18/2018, 20104 AM 2/18/2018, 40108 AM 2/18/2018, 60103 AM 2/18/2018, 100104 AM 2/18/2018, 120108 PM 2/18/2018, 20104 PM 2/18/2018, 40108 PM 2/18/2018, 60108 PM 2/18/2018, 100108 PM 2/19/2018, 120108 AM 2/19/2018, 120108 AM 2/19/2018, 40104 AM 2/19/2018, 40104 AM	2481756 248853 2548653 2597677 2248258 2410236 2613600 2613600 2613600 2613600 1676656 1954093 2161116 2986971 2514084 2514084 2358843 2215738	4 3 4 4 6 3 4 4 4 3 3 3 3 3 3 3 3 4 4 4 4	001684 982628 982628 982628 982628 982628 982628 98262 9826 9826	240,000 3196214 3236546 3664018 3664018 360,000 281,0032 356,0752 30,01500 2925146 3001,080 2055280 2655280 2655280 2655384 2900008 3821158 3893381
	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23	RCII-5100-W-1	MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1	2/18/2018, 120104 AM 2/18/2018, 20104 AM 2/18/2018, 20104 AM 2/18/2018, 40108 AM 2/18/2018, 60103 AM 2/18/2018, 100104 AM 2/18/2018, 120108 PM 2/18/2018, 20104 PM 2/18/2018, 40108 PM 2/18/2018, 60108 PM 2/18/2018, 100108 PM 2/19/2018, 120108 AM 2/19/2018, 120108 AM 2/19/2018, 40104 AM 2/19/2018, 40104 AM	2481756 248053 2548653 2597677 2248258 2410236 2613600 2613600 2613600 1676656 1954093 2161116 2986971 2514084 2358043 22514084	4 3 3 4 6 3 3 4 4 4 3 3 3 3 3 3 3 4 4 4 4	001684 982628 982628 982628 982628 982628 982628 98262 98269 98069 98269	140000 3154214 3226546 3664018 3664018 3604018 360402 2816032 3506752 3500580 2925146 300180 2925146 300180 2955380 2975884 290008 3802118 3805381 3756691 3716551 3932908
	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24	RCII-5100-W-1	MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1	2/18/2018, 120104 AM 2/18/2018, 20104 AM 2/18/2018, 20104 AM 2/18/2018, 40108 AM 2/18/2018, 60103 AM 2/18/2018, 100104 AM 2/18/2018, 120108 PM 2/18/2018, 20104 PM 2/18/2018, 40108 PM 2/18/2018, 60108 PM 2/18/2018, 100108 PM 2/19/2018, 120108 AM 2/19/2018, 120108 AM 2/19/2018, 40104 AM 2/19/2018, 60108 AM 2/19/2018, 60108 AM	2481756 248853 2548653 2597677 2248258 2410236 26136000 2613600000000000000000000000000000000000	4 3 3 4 6 3 3 4 4 4 3 3 3 3 3 3 3 4 4 4 4	001684 982628 982628 982628 982628 982628 982628 982628 98269 98260 98269 9826	140000 3196214 3236546 3664018 3664018 3604018 360402 2816032 2816032 2816032 2816032 2816032 2816032 281603 201080 281518 3899381 3716851 3905900 3886552
	6 7 8 9 10 11 12 13 14 15 16 15 16 17 18 19 20 21 22 23 24 25	RCII-5100-W-1	MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1	2/18/2018, 120104 AM 2/18/2018, 20104 AM 2/18/2018, 20104 AM 2/18/2018, 40108 AM 2/18/2018, 60103 AM 2/18/2018, 100104 AM 2/18/2018, 120108 PM 2/18/2018, 20104 PM 2/18/2018, 40108 PM 2/18/2018, 60108 PM 2/18/2018, 100108 PM 2/19/2018, 120108 AM 2/19/2018, 120108 AM 2/19/2018, 40104 AM 2/19/2018, 60108 AM 2/19/2018, 100104 AM	2481756 248853 2548653 2597677 2248258 2410236 26136000 2613600000000000000000000000000000000000	4 3 3 4 6 3 3 4 4 4 3 3 3 3 3 3 3 3 4 4 4 4	001684 982628 982628 982628 982628 982628 982628 982628 98269 9826	240000 3196214 3236546 3664018 3664018 36032 2816032 2816032 2816032 2816032 2816032 2816032 2816032 2816032 281603 201080 28151 3809381 3716691 3716551 3933908 3836552 3800676
	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 24 25 26	RCII-5100-W-1           RCII-5100-W-1	MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1	2/18/2018, 120104 AM 2/18/2018, 20104 AM 2/18/2018, 20104 AM 2/18/2018, 40108 AM 2/18/2018, 60103 AM 2/18/2018, 100104 AM 2/18/2018, 120108 PM 2/18/2018, 20104 PM 2/18/2018, 40108 PM 2/18/2018, 60108 PM 2/18/2018, 100108 PM 2/19/2018, 120108 AM 2/19/2018, 120108 AM 2/19/2018, 40104 AM 2/19/2018, 100104 AM 2/19/2018, 100104 AM 2/19/2018, 100104 AM	2481756 2481756 254853 204413 2997677 2248258 2410236 2613600 2613600 2613600 2613600 2613600 2613600 2613600 2613600 2613600 2613600 2613600 2613600 261360 2005 2005 2005 2005 2005 2005 2005 20	4 3 3 4 6 3 3 4 4 4 3 3 3 3 3 3 3 3 4 4 4 4	001684 982628 982628 982628 982628 982628 982628 982629 972387 972387 905961 98989 98989 978498 978498 978498 978498 978498 97849 97777 9778 9778	140.000 3196214 3236546 3664018 3664018 3604018 360402 2816032 2816032 2816032 2816032 2816032 2816032 281603 201080 281538 280008 281538 280008 281538 280038 281538 280038 281538 281538 280038 281558 281558 28
	6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27	RCIU-5100-WL-1	MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1 MCN-5100-WL1	2/18/2018, 120104 AM 2/18/2018, 20104 AM 2/18/2018, 20104 AM 2/18/2018, 40108 AM 2/18/2018, 60103 AM 2/18/2018, 100104 AM 2/18/2018, 120108 PM 2/18/2018, 20104 PM 2/18/2018, 40108 PM 2/18/2018, 60108 PM 2/18/2018, 100108 PM 2/19/2018, 120108 AM 2/19/2018, 120108 AM 2/19/2018, 40104 AM 2/19/2018, 100104 PM 2/19/2018, 100104 PM 2/19/2018, 100104 PM 2/19/2018, 100104 PM 2/19/2018, 100104 PM 2/19/2018, 120108 PM 2/19/2018, 120108 PM 2/19/2018, 120108 PM	2481756 248853 254853 2597677 2248258 2410236 2613600 2613600 2613600 2613600 2613600 2613600 2613600 2613600 2613600 2613600 2613600 2613600 2613600 261360	4 3 3 4 6 3 4 4 4 3 3 3 3 3 3 3 3 4 4 4 4	001684 982628 982628 982628 982628 982628 982628 972387 972387 972387 905961 98980 98980 98980 97845 98980 97845 98980 97845 98980 97845 98980 98090 98090 9800 90000 90000 90000 90000 90000 90000 90000 90000 90000 90000 9000000	2405633 3196214 3286546 36642643 3664018 3664018 3612666 2816032 2816032 3803752 300100 2929346 3001800 2929346 3001800 2955280 2957584 290006 3821158 389381 3756691 3756591 3756591 3756591 3756591 3756591 3922900 3838552 3808552 3808656 4165337 1109046

Active bandwidth testing enables you the ability to issue an instant path bandwidth test through public internet WAN link, or to schedule public internet WAN link bandwidth testing to be completed at specific times on a recurring basis.

The **Path Bandwidth** feature is useful for demonstrating how much bandwidth is available between two locations during new and existing installations. The values from the Path Bandwidth indicate max-

imum possible bandwidth. For an accurate allowed bandwidth, navigate to **Configuration** > **System Maintenance** > **Diagnostics** > **Site Diagnostics** > **Bandwidth Test**. For more information, see Active Bandwidth Testing.

# System info

The **System Info** page provides the system information, ethernet ports detail, and license status.

To view the System Info, navigate to **Configuration > expand System Maintenance > Diagnostics** and select **System Info**.

Dashboard Monitoring	Configuration							
+ Appliance Settings	Configuration > System Main	ntenance > Diagnostic	s					
+ Virtual WAN								
- System Maintenance	Ping Traceroute	Packet Capture	Path Bandwidth	System Info	Diagnostic Data	Events	Alarms	Diagnostics Tool
Delete Files	Site Diagnostics							
Restart System	Sustem Information							
Date/Time Settings	System information							
Local Change Management	Name:		Da	las MCN				
Diagnostics	Appliance Mode:		MC	N				
- Update Software	Hardware Model:		40	00				
Configuration Reset	Software Version:		11.	0.0.72.760315				
Factory Reset	Built On: OS Partition Version:		Ap 5.1	r 10 2019 at 19:08	::49			
	Serial Number:		HN	XCJCRGJX				
	BIOS version:		4.2	a				
	Hard Disk Usage							
	Partition Usage							
	Active OS 51%							
	/home 18%							
	View Details							
	Ethernet Ports							
	0/1:	mgt0	0a:c4:7a:8	5:ce:62				
	1/1:	la0	be:0a:f7:b	e:76:3d				
	1/2:	wa0	e6:18:31:2	2:b9:84				
	1/3:	la1 wa1	86:c0:b7:3	c:03:5d				
	1/5:	la2	da:6c:7c:7	3:d4:84				
	1/6:	wa2	be:e3:26:7	e:2b:99				
	1/7:	la3	82:af:6a:d	3:74:72				
	1/8:	wa3	a2:af:76:6	:90:a2				
	10/2:	wa4	76:5d:15:0	9:f0:26				
	License Status							
	State:			License	d			
	License Server HostID:			02c47a	85ce62			
	Model:			4000VV	V-2000			
	Maximum Bandwidth (MAXB)	N):		2000 M	bps			
	License Type: Maintenance Expiration Date			Retail	1 00:00:00 2010			
	License Expiration Date:			Sun Dec Mon De	c 2 00:00:00 2019			

The **System Info** lists all the parameters that are not set to their defaults. This information is read-only. It is used by Support when some kind of misconfiguration is suspected. When you report a problem, you might be asked to check one or more values on this page.

# Diagnostic data

**Diagnostic Data** allows you to generate a diagnostic data package for analysis by the Citrix Support team. You can download the **Diagnostics Log Files** package and share it with the Citrix Support team.

To view the **Diagnostic Data**, navigate to **Configuration > expand System Maintenance > Diagnostic tics** and select **Diagnostic Data**.

#### Citrix SD-WAN 11.5

	Configuration
Appliance Settings	Configuration > System Maintenance > Diagnostics
Virtual WAN	
System Maintenance	Ping         Traceroute         Packet Capture         Path Bandwidth         System Info         Diagnostic Data         Events         Alarms         Diagnostic
Delete Files	Site Diagnostics
Restart System	
Date/Time Settings	FTP Information
Local Change Management	
Diagnostics	<ul> <li>These fields define the parameters used when connecting to an FTP server in order to upload either Diagnostic information packages or memory Dump packages.</li> </ul>
Update Software	Upload connections from this appliance to the FTP server are done in passive mode, so the server must support this and be in passive mode.
Configuration Reset	Note: All fields are required in order to FTP Apply.
	Customer:
	Username:
	Password:
	FTP Server:
	FTP Apply
	Diagnostic Information
	NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.
	Disapartie Los Filos
	Diagnostic Log Files
	<ul> <li>Inese packages contain important real-time system information you can forward to Clirix support kepresentatives. Iney may be downloaded directly tr the browser or uploaded via FTP to the FTP server defined in the FTP Information area above.</li> </ul>
	Only 5 diagnostics packages can exist on the system at a time.
	Create New
	Filename:
	Download Salartad
	Oprimula servera
	Memory Dumps
	Memory Dumps NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.
	Memory Dumps       NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.
	Memory Dumps           NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.           System Error Memory Dumps
	Memory Dumps           NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.           System Error Memory Dumps           • Download, upload via FTP any saved memory dumps (caused by system error events) that you can forward to Citrix Support Representatives or delete an are not required. The Upload option transfers the memory dump file via FTP to the FTP server defined in the FTP Information area above.
	Memory Dumps           NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.           System Error Memory Dumps           • Download, upload via FTP any saved memory dumps (caused by system error events) that you can forward to Citrix Support Representatives or delete an are not required. The Upload option transfers the memory dump file via FTP to the FTP server defined in the FTP Information area above.           There are no memory dumps available for download.
	Memory Dumps           NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.           System Error Memory Dumps           • Download, upload via FTP any saved memory dumps (caused by system error events) that you can forward to Citrix Support Representatives or delete ar are not required. The Upload operation transfers the memory dump file via FTP to the FTP server defined in the FTP Information area above.           There are no memory dumps available for download.
	Memory Dumps         MOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.         System Error Memory Dumps         • Download, upload via FTP any saved memory dumps (caused by system error events) that you can forward to Citrix Support Representatives or delete ar are not required. The Upload operation transfers the memory dump file via FTP to the FTP server defined in the FTP Information area above.         There are no memory dumps available for download.         Download       Upload
	Memory Dumps         NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.         System Error Memory Dumps         • Download, upload via FTP any saved memory dumps (caused by system error events) that you can forward to Citrix Support Representatives or delete ar are not required. The Upload operation transfers the memory dump file via FTP to the FTP server defined in the FTP Information area above.         There are no memory dumps available for download.         Download       Upload         Delete
	Memory Dumps         NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.         System Error Memory Dumps         • Download, upload via FTP any saved memory dumps (caused by system error events) that you can forward to Citrix Support Representatives or delete at are not required. The Upload operation transfers the memory dump file via FTP to the FTP server defined in the FTP Information area above.         There are no memory dumps available for download.         Download       Upload         Download       Delete
	Memory Dumps         NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.         System Error Memory Dumps         • Download, upload via FTP any saved memory dumps (caused by system error events) that you can forward to Citrix Support Representatives or delete at are not required. The Upload operation transfers the memory dump file via FTP to the FTP server defined in the FTP Information area above.         There are no memory dumps available for download.         Download       Upload         Download       Delete
	Memory Dumps         NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.         System Error Memory Dumps         • Download, upload via FTP any saved memory dumps (caused by system error events) that you can forward to Citrix Support Representatives or delete at are not required. The Upload operation transfers the memory dump file via FTP to the FTP server defined in the FTP Information area above.         There are no memory dumps available for download.         Download       Upload         Download       Delete         Configuration Diagnostic Information         NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.         Configuration Diagnostic Files
	Memory Dumps         NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.         System Error Memory Dumps         • Download, upload via FTP any saved memory dumps (caused by system error events) that you can forward to Citrix Support Representatives or delete at are not required. The Upload operation transfers the memory dump file via FTP to the FTP server defined in the FTP Information area above.         There are no memory dumps available for download.         Download       Upload         Diagnostic Information       Delete         NOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.         Configuration Diagnostic Information you can forward to Citrix Support Representatives. This is an additional package to the STI captured on Branches. This package contains configuration orachive and log files which help debug issue
	Implementation       Implementation         Memory Dumps       More: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.         System Error Memory Dumps       System Error Memory Dumps (caused by system error events) that you can forward to Citrix Support Representatives or delete at are not required. The Upload operation transfers the memory dump file via FTP to the FTP server defined in the FTP Information area above.         There are no memory dumps available for download.       Implementation         Implementation       Implementation         MOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.       Implementation         Configuration Diagnostic Information       Implementation         MOTE: To enable Upload option, please configure DNS settings and an FTP Customer Name for this appliance.       Configuration Diagnostic Files         • This package contains Configuration Diagnostics information you can forward to Citrix Support Representatives. This is an additional package to the ST captured on Branche. They may be downloaded direct through the browser or uploaded via TTP to the FTP server defined in the FTP Information area above.         • Only 5 Configuration diagnostics packages can exist on the system at a time.       Implementation
	Implementation       Implementation         Implementation       Implementa
	Improve sectors       Improve sectors

The **Diagnostics Data** includes:

- **FTP Information** Provide the FTP parameters detail and click **FTP Apply**. The FTP information required to connect an FTP server to upload diagnostic information package.
- **Diagnostics Information** The diagnostics log file package contains real-time system information that can be downloaded through the browser or uploaded via FTP to the FTP server.

#### Note:

Only five diagnostics packages can exist on the system at a time.

• **Configuration Diagnostic Information** - In the Citrix SD-WAN 11.0 release, the Network configuration file will not be available in the Diagnostic information collected for branch. For any support case, provide the diagnostic information of branch and Configuration diagnostic information from the control node the branch is connected to.

To collect configuration diagnostic information from the Control Node GUI, navigate to **Configuration > System Maintenance > Diagnostics > Diagnostic Data >** under **Configuration Diagnostic Information**, click **Create New**.

Configuration Diagnostic Information	
NOTE: To enable Upload option, please configure DNS settings and an F	TP Customer Name for this appliance.
Configuration Diagnostic Files	
<ul> <li>This package contains Configuration Diagnostics information you captured on Branches. This package contains configuration archiv through the browser or uploaded via FTP to the FTP server defined</li> <li>Only 5 Configuration diagnostics packages can exist on the system</li> </ul>	can forward to Citrix Support Representatives. This is an additional package to the STS e and log files which help debug issues on the Branch. They may be downloaded directly d in the FTP Information area above. m at a time.
Create New	
Filename: Download Selected	Upload Delete Selected

On completion of the **Configuration Diagnostic Information** creation, click **Download Selected** file and provide this file to Citrix Support OR use the FTP apply operation available in the same page to FTP this file.

• **Memory Dumps** –You can download or upload the system error memory dumps file and share with the Citrix Support team. You can also delete the files if not required.

NOTE:

By default the **Upload** option is in disabled mode. To enable it, configure **DNS** settings and an **FTP Customer Name** for this appliance.

### Events

Use the **Events** feature to add, monitor, and manage the events generated. It helps to identify events in real-time, that helps you address issues immediately and keep the Citrix SD-WAN appliance running effectively. You can download events in CSV format.

To add an event, select object type, event type, and severity from the drop-down list and click **Add Event**.

To view **Events**, navigate to **Configuration >** expand **System Maintenance > Diagnostics** and select **Events**.

Dashboard Monitoring	Configur	ation																
+ Appliance Settings	Configur	ration > Sys	stem Maintenance > D	liagnostic	5													
+ Virtual WAN																_		
- System Maintenance	Ping	Trace	eroute Packet C	apture	Path Ba	andwi	idth 5	System Info		Diagno	ostic Data	Ev	ents	AI	larms		Diagnostics T	ool
- Delete Files	Site I	Diagnostics																
Restart System	Incode	E.com																
Date/Time Settings	insert	Event																
- Local Change Management	Object	Type			LISE		ENT	•										
Diagnostics	object	Type.			USE	K EV	ENT	<u> </u>										
Update Software	Event t	type:			UND	EFIN	IED	¢										
- Configuration Reset	Severit	y:			DEB	UG		•										
Pactory Reset	Add E	vent																
	Down There are o You can do Download	load Event: currently 85 in ownload some events startin	s n the Events database, s e or all of them in CSV f ng from 2019	ipanning f ormat. Yo \$	from event 2 u may wish March	4547 to lim	71 at 2019-0 hit the amour 2	3–24 05:35: nt to downloa 24	54 to e ad beca	vent 24 iuse so t	45555 at 20 me commo 5	)19-04-2 n spreads	1 06:23 heet pr	3:16. ograms 5	limit yo	u to 6	5,536 rows.	
	54		Download (85 even	nts)														
	Alert	Count																
	Alert	Туре							A	lerts S	ent							
	Emails								0									
	Syslog	Messages:							0							- 1		
	STRIME	rraps.												,				
	View	Events																
	Quanti	ity:	1000		•													
	Filter:		Object Type =	Any		÷	Event type =	Any		\$	Severity =	Any			•			
	Reloa	d Events Tabl	e															
	ID	Object ID	Object Name	Obje	ct Type		Time	Event Type	Sever	rity	Descriptio	on						
	245555	25	License_Alert	LICE	NSE_EVENT		2019- 04-21 06:23:16	WARNING	CRITI	ICAL	The total (Kbps) mu (Kbps).	configure ust not ex	d permi ceed tw	itted rat vice the	te (WAN License	to LAI Rate v	4) 13670000 which is 40000	000
	245554	25	License_Alert	LICE	NSE_EVENT		2019- 04-20 06:23:01	WARNING	CRITI	ICAL	The total (Kbps) mu (Kbps).	configure st not ex	d permi ceed tw	itted rat vice the	te (WAN License	to LAI Rate v	4) 13670000 which is 40000	000
	245553	25	License_Alert	LICE	NSE_EVENT		2019- 04-19 06:22:46	WARNING	CRITI	ICAL	The total (Kbps) mu (Kbps).	configure ust not ex	d permi ceed tw	itted rat vice the	te (WAN License	to LAI Rate v	4) 13670000 which is 40000	000
	245552	25	License_Alert	LICE	NSE_EVENT		2019- 04-18 06:22:31	WARNING	CRITI	ICAL	The total (Kbps) mu (Kbps).	configure ust not ex	d permi ceed tw	itted rat vice the	te (WAN License	to LAI Rate v	4) 13670000 which is 40000	000
	245551	25	License_Alert	LICE	NSE_EVENT		2019- 04-17 06:22:15	WARNING	CRITI	ICAL	The total (Kbps) mu (Kbps).	configure ist not ex	d permi ceed tw	itted rat vice the	te (WAN License	to LAI Rate v	4) 13670000 which is 40000	000
	245550	25	License_Alert	LICE	NSE_EVENT		2019- 04-16 06:22:00	WARNING	CRITI	ICAL	The total (Kbps) mu (Kbps).	configure ist not ex	d permi ceed tw	itted rat vice the	te (WAN License	to LAI Rate v	<ul> <li>N) 13670000</li> <li>which is 40000</li> </ul>	000
	245549	25	License_Alert	LICE	NSE_EVENT		2019- 04-15 06:21:44	WARNING	CRITI	ICAL	The total (Kbps) mu (Kbps).	configure ust not ex	d permi ceed tw	itted rat vice the	te (WAN License	to LAI Rate v	13670000 which is 40000	000
	245548	25	License_Alert	LICE	NSE_EVENT		2019- 04-14 06:21:29	WARNING	CRITI	ICAL	The total (Kbps) mu (Kbps).	configure ust not ex	d permi ceed tw	itted rat vice the	te (WAN License	to LAI Rate v	4) 13670000 which is 40000	000

You can configure Citrix SD-WAN to send event notifications for different event types as **Emails, SNMP Traps,** or **Syslog Messages**.

Once the email, SNMP, and syslog notification settings are configured, you can select the severity for different event types and select the mode (email, SNMP, syslog) to send event notifications.

Notifications are generated for events equal to or above the specified severity level for the event type.

You can view the events detail under **View Events** table. The event details include the following information.

- ID –Event ID.
- **Object ID** The ID of the object generating the event.
- Object Name The name of the object generating the event.
- **Object Type** The type of the object generating the event.
- **Time** The time the event was generated.
- **Event Type** The state of the object at the time of the event.
- Severity The severity level of the event.
- **Description** –A text description of the event.

### Alarms

You can view and clear the triggered alarm. To view Alarms, navigate to Configuration > expand System Maintenance > Diagnostics and select Alarms.

Dashboard Monitoring	Configuration													
+ Appliance Settings	Configuration > System Maintenance > Diagnostics													
+ Virtual WAN - System Maintenance	Ping         Traceroute         Packet Capture         Path Bandwidth         System Info         Diagnostic Data         Events         Alarms         Diagnostics Tool													
Delete Files	Site Diagnostics													
- Restart System - Date/Time Settings	Alarms													
- Local Change Management Diagnostics	Enable Auto Refresh 🖉 Time Interval 5 🛊 seconds Refresh Clear Checked Alarms 🖓													
- Update Software - Configuration Reset														
- Factory Reset	Triggered Alarms Summary													
	Filter: virtual path Severity ¢ Apply													
	Severity         Event Type         Object Name         Trigger State         Trigger Duration (sec)         Clear State         Clear Duration (sec)         Clear Action													

Select the alarms that you want to clear and click **Clear Checked Alarms** or click **Clear All Alarms** to clear all the alarms.

You can view the following summary of all the triggered alarms:

- **Severity** The severity is displayed in the alerts sent when the alarm is triggered or cleared and in the triggered alarm summary.
- **Event Type** The SD-WAN appliance can trigger alarms for particular subsystems or objects in the network. These alarms are called event types.
- **Object Name** The name of the object generating the event.
- Trigger State The event state that triggers an alarm for an Event Type.
- **Trigger Duration (sec)** The duration in seconds determines how quickly the appliance triggers an alarm.
- Clear State The event state that clears an alarm for an Event Type after the alarm is triggered.
- **Clear Duration (sec)** The duration in seconds determines how long to wait before clearing an alarm.
- **Clear Action** The action that is taken while clearing alarms.

# **Diagnostics tool**

The **Diagnostic tool** is used to generate test traffic which allows you to troubleshoot network issues that might results in:

- Frequent change in path state from Good to Bad.
- Poor application performance.
- Higher packet loss

Most often, these problems arise due to rate limiting configured on firewall and router, incorrect bandwidth settings, low link speed, priority queue set by network provider and so on. The diagnostic tool allows you to identify the root cause of such issues and troubleshoot it.

The diagnostic tool removes the dependency on third-party tools such as iPerf which has to be manually installed on the Data Center and Branch hosts. It provides more control over the type of diagnostic traffic sent, the direction in which the diagnostic traffic flows, and the path on which the diagnostic traffic flows.

The diagnostic tool allows to generate the following two types of traffic:

- **Control**: Generates traffic with no QOS/scheduling applied to the packets. As a result, the packets are sent over the path selected in the UI, even if the path is not the best at the time. This traffic is used to test specific paths and helps to identify ISP-related issues. You can also use this to determine the bandwidth of the selected path.
- **Data**: Simulates the traffic generated from the host with SD-WAN traffic processing. Since QoS/scheduling is applied to the packets, the packets are sent over the best path available then. Traffic is sent over multiple paths if load balancing is enabled. This traffic is used to troubleshoot QoS/scheduler related issues.

### Note

To run a diagnostic test on a path, you have to start the test on the appliances at both ends of the path. Start the diagnostic test as a server on one appliance and as a client on the other appliance.

### To use diagnostics tool:

1. On both the appliances, click **Configuration** > **System Maintenance** > **Diagnostics** > **Dia** 

Diagnostics Tool		
Tool Mode: Server •	Traffic Type: Data •	Port: 10
lperf:	WAN to LAN Paths: DC-INET-1->BR1-INET-1	
Start		
Results		
stop		
Server listening on TCP port 10		
TCP window size: 85.3 KByte (default)		

- 2. In the **Tool Mode** field, select **Server** on one appliance and select **Client** on the appliance residing on the remote end of the selected path.
- 3. In the **Traffic Type** field, select the type of diagnostic traffic, either **Control** or **Data**. Select the same traffic type on both the appliances.
- 4. In the **Port** field, specify the **TCP / UDP** port number on which the diagnostic traffic is sent. Specify the same port number on both the appliances.
- 5. In the **Iperf** field, specify IPERF command-line options, if any.

#### Note

You need not specify the following IPERF command-line options:

- -c: Client mode option is added by the diagnostic tool.
- -s: Server mode option is added by the diagnostic tool.
- -B: Binding IPERF to specific IP/interface is done by the diagnostic tool depending on the path selected.
- -p: Port number is provided in the diagnostics tool.
- -i: Output interval in seconds.
- -t: Total duration of the test in seconds.
- 6. Select the WAN to LAN paths on which you want to send the diagnostic traffic. Select the same path on both the appliances.
- 7. Click **Start** on both the appliances.

The result displays the mode (client or server) of the selected appliance and the TCP or UDP port on which the test is run. It periodically displays the data transferred and bandwidth utilized for the interval specified until the total duration of the test is reached.

#### Citrix SD-WAN 11.5

ing indecidate	Packet Capture	Path Bandwidth	System Info	Diagnostic Data	Events	Alarms	Diagnostics Tool
Site Diagnostics							
Diagnostics Tool							
Teel Made: Olient	▲ Traffi	Tunai	•		De	10	
Chent	• Hall	Data	•		FU		
		WAN Dethe					
lperf:	DANT	MCN_184	_78-Broadband	, ,			
Start							
Results							
stop							
ient connecting to 172.16	.31.10, TCP port 10						
ient connecting to 172.16 nding to local address 17	5.31.10, TCP port 10 72.16.21.10						
ient connecting to 172.16 nding to local address 17 P window size: 112 KByte	5.31.10, TCP port 10 (2.16.21.10 (default)						
ient connecting to 172.16 nding to local address 17 P window size: 112 KByte	5.31.10, TCP port 10 (2.16.21.10 e (default)	ith 172.16.31.10 po	rt 10				
ient connecting to 172.16 ading to local address 17 P window size: 112 KByte 3] local 172.16.21.10 po ID] Interval Transf	5.31.10, TCP port 10 (2.16.21.10 (default) 	 ith 172.16.31.10 po	rt 10				
ient connecting to 172.16 nding to local address 17 P window size: 112 KByte 	5.31.10, TCP port 10 2.16.21.10 (default) 	 ith 172.16.31.10 po	rt 10				
ient connecting to 172.16 nding to local address 17 P window size: 112 KByte 3] local 172.16.21.10 po ID] Interval Transf 3] 0.0- 1.0 sec 10.1 M 3] 1.0- 2.0 sec 11.9 M	5.31.10, TCP port 10 2.16.21.10 5 (default) ort 39993 connected w Ver Bandwidth Bytes 84.9 Mbits/se Bytes 99.6 Mbits/se	 ith 172.16.31.10 po	rt 10				
ient connecting to 172.16 nding to local address 17 P window size: 112 KByte 3] local 172.16.21.10 po ID] Interval Transf 3] 0.0- 1.0 sec 10.1 M 3] 1.0- 2.0 sec 11.9 M 3] 2.0- 3.0 sec 13.4 M	i.31.10, TCP port 10 (2.16.21.10 (default) ort 39993 connected w (er Bandwidth Bytes 84.9 Mbits/se Bytes 99.6 Mbits/se Bytes 112 Mbits/se	 ith 172.16.31.10 po c	rt 10				
ient connecting to 172.16 nding to local address 17 P window size: 112 KByte 3] local 172.16.21.10 po ID] Interval Transf 3] 0.0- 1.0 sec 10.1 M 3] 1.0- 2.0 sec 11.9 M 3] 2.0- 3.0 sec 13.4 M 3] 3.0- 4.0 sec 15.1 M	i.31.10, TCP port 10 (2.16.21.10 (default) ort 39993 connected w (er Bandwidth Bytes 84.9 Mbits/se Bytes 99.6 Mbits/se Bytes 112 Mbits/se Bytes 127 Mbits/se	 ith 172.16.31.10 po	rt 10				
<pre>ent connecting to 172.16 ding to local address 17 e window size: 112 KByte 3] local 172.16.21.10 pc D] Interval Transf 3] 0.0- 1.0 sec 10.1 M 3] 1.0- 2.0 sec 11.9 M 3] 2.0- 3.0 sec 13.4 M 3] 3.0- 4.0 sec 15.1 M 3] 4.0- 5.0 sec 14.5 M</pre>	5.31.10, TCP port 10 2.16.21.10 (default) ort 39993 connected w er Bandwidth Bytes 84.9 Mbits/se Bytes 112 Mbits/se Bytes 127 Mbits/se Bytes 122 Mbits/se	 ith 172.16.31.10 po	rt 10				
Lient connecting to 172.16 adding to local address 17 P window size: 112 KByte 3] local 172.16.21.10 pc (D] Interval Transf 3] 0.0- 1.0 sec 10.1 M 3] 1.0- 2.0 sec 11.9 M 3] 2.0- 3.0 sec 13.4 M 3] 3.0- 4.0 sec 15.1 M 3] 4.0- 5.0 sec 14.5 M	5.31.10, TCP port 10 2.16.21.10 (default) 	 ith 172.16.31.10 po c c c c	rt 10				
Lent connecting to 172.16 hding to local address 17 P window size: 112 KByte 3] local 172.16.21.10 pc ID] Interval Transf 3] 0.0- 1.0 sec 10.1 M 3] 1.0- 2.0 sec 11.9 M 3] 2.0- 3.0 sec 13.4 M 3] 3.0- 4.0 sec 15.1 M 3] 4.0- 5.0 sec 14.5 M 3] 5.0- 6.0 sec 14.5 M 3] 6.0- 7.0 sec 15.1 M	5.31.10, TCP port 10 2.16.21.10 (default) ort 39993 connected w Fer Bandwidth Bytes 84.9 Mbits/se Bytes 112 Mbits/se Bytes 122 Mbits/se Bytes 122 Mbits/se Bytes 122 Mbits/se Bytes 122 Mbits/se Bytes 122 Mbits/se	 ith 172.16.31.10 po c c c c c c c c	rt 10				
<pre>ient connecting to 172.16 nding to local address 17 P window size: 112 KByte 3] local 172.16.21.10 po ID] Interval Transf 3] 0.0- 1.0 sec 10.1 M 3] 1.0- 2.0 sec 11.9 M 3] 2.0- 3.0 sec 13.4 M 3] 3.0- 4.0 sec 15.1 M 3] 4.0- 5.0 sec 14.5 M 3] 5.0- 6.0 sec 14.5 M 3] 6.0- 7.0 sec 15.1 M 3] 7.0- 8.0 sec 15.1 M</pre>	5.31.10, TCP port 10 22.16.21.10 (default) ort 39993 connected w Ver Bandwidth Bytes 84.9 Mbits/se Bytes 112 Mbits/se Bytes 122 Mbits/se Bytes 122 Mbits/se Bytes 122 Mbits/se Bytes 122 Mbits/se Bytes 127 Mbits/se	 ith 172.16.31.10 po c c c c c c c c c c c c c c c c c c c	rt 10				
ient connecting to 172.16 nding to local address 17 P window size: 112 KByte 3] local 172.16.21.10 pc ID] Interval Transf 3] 0.0- 1.0 sec 10.1 M 3] 1.0- 2.0 sec 11.9 M 3] 2.0- 3.0 sec 13.4 M 3] 3.0- 4.0 sec 15.1 M 3] 4.0- 5.0 sec 14.5 M 3] 5.0- 6.0 sec 14.5 M 3] 6.0- 7.0 sec 15.1 M 3] 7.0- 8.0 sec 15.1 M	i.31.10, TCP port 10 2.16.21.10 (default) ort 39993 connected w ver Bandwidth Bytes 84.9 Mbits/se Bytes 127 Mbits/se Bytes 122 Mbits/se Bytes 122 Mbits/se Bytes 127 Mbits/se Bytes 127 Mbits/se Bytes 127 Mbits/se Bytes 127 Mbits/se Bytes 127 Mbits/se Bytes 127 Mbits/se	 ith 172.16.31.10 po c c c c c c c c c c c c c c c c c c c	rt 10				
<pre>ient connecting to 172.16 nding to local address 17 P window size: 112 KByte</pre>	5.31.10, TCP port 10 22.16.21.10 (default) ort 39993 connected w ver Bandwidth Bytes 84.9 Mbits/se Bytes 127 Mbits/se Bytes 122 Mbits/se Bytes 122 Mbits/se Bytes 127 Mbits/se Bytes 127 Mbits/se Bytes 127 Mbits/se Bytes 121 Mbits/se Bytes 131 Mbits/se Bytes 134 Mbits/se	 ith 172.16.31.10 po c c c c c c c c c c c c c c c c c c c	rt 10				

### **Site diagnostics**

You can test the bandwidth usage, ping, and perform traceroute for the WAN links configured at different sites in the Citrix SD-WAN network. It provides information which helps in troubleshooting issues in the existing configuration.

To use **Site Diagnostics**, navigate to **Configuration >** expand **System Maintenance > Diagnostics** and select **Diagnostics Tool**.

Dashboard Monitoring	Configuration
+ Appliance Settings	Configuration > System Maintenance > Diagnostics
+ Virtual WAN - System Maintenance	Ping         Traceroute         Packet Capture         Path Bandwidth         System Info         Diagnostic Data         Events         Alarms         Diagnostics Tool
- Delete Files - Restart System - Date/Time Settings - Local Change Management	Site Diagnostics Site Diagnostics
Diagnostics Update Software	Virtual Path: Paths: Download Test Result
- Configuration Reset - Factory Reset	Dallas_MCN-California   Select Paths  Select all paths
	Tests: 🏚 Ping Traceroute Bandwidth Test
	Run

The results section displays the following:

- **Interface Status**: Provides the name of the interface, number of firewall zones associated with the interface, VLAN ID, and its associated ports.
- **Path Status**: Provides the details of target private IP, Gateway IP, Target Public IP, Partner IP, Partner Public IP addresses. It also displays the status of Gateway ARP and path MTU.
- **Ping Result**: Provides the direction, status, count (including the number of attempts and failures), and RTT of the ping.
- **Traceroute Result**: Provides the direction, status, number of hops, and IP address or RTT of the hops.
- **Bandwidth Result**: Provides the status of TCP and UDP along with the bandwidth used (in kbps) for the overlay and underlay network. Compared to UDP, the bandwidth used by TCP is more, because UDP is bandwidth based and therefore uses only the configured bandwidth. TCP is a ramp up protocol; based on underlying network configuration, usage might report higher bandwidth compared to configured bandwidth.

ath:							
BR1_184-Broad	band-AARNet-1->MCN_1	184_78-Broadband-A0	cT-1 ¢				
nterface Status							
Virtual Interface		Firewall Zone		VLAN ID		Associated Ports	
VIF-2-WAN-1		2		0		=	
Port	MAC				Status		
2	2e:25:47:ba:45:c1				ETH_LINK_	UP	
ath Status							
Target Private IP	Gateway IP	Gateway ARP	Target Public	c IP	Partner IP	Partner Public IP	Path MTU
172.16.31.10	172.16.31.1	READY_ACTIVE	-		172.16.21.10		1348
<u>'ing Result</u>							
Direction		Status	Ping Cou	int		RTT	
Direction		Status pass	Ping Cou	int		RTT 2.354ms	
Direction LAN to WAN WAN to LAN		Status pass pass	Ping Cou 5/5 5/5	int		RTT 2.354ms 2.2286ms	
Traceroute Result Direction LAN to UAN Traceroute Result Direction	Statu	Status pass pass	Ping Cou 5/5 5/5	int	Hop IP/R1	RTT 2.354ms 2.2286ms	
ring Result Direction LAN to WAN WAN to LAN  Fraceroute Result Direction LAN to WAN	Statu Succ	Status pass pass	Ping Cou 5/5 5/5 Hop Count 50	Int	Hop IP/RT	RTT 2.354ms 2.2286ms	
Ping Result Direction LAN to WAN WAN to LAN Traceroute Result Direction LAN to WAN	Statu Succ	Status pass pass s s	Hop Count 50	int	Hop IP/R1	RTT 2.354ms 2.2286ms T	
Ping Result Direction LAN to WAN WAN to LAN Graceroute Result Direction LAN to WAN WAN to LAN	Statu Succ Succ	Status pass pass s ess	Ping Cou 5/5 5/5 Hop Count 50	int	Hop IP/R1	RTT 2.354ms 2.2286ms T 1.1/0.737 1/1.136	
Ping Result Direction LAN to WAN WAN to LAN Direction LAN to WAN WAN to LAN	Statu Succ Succ	s Status Pass pass s Status Pass s Status Pass	Ping Cou           5/5           5/5           4           Hop Count           50	Int	Hop IP/RT 172.16.3 172.16.1 172.16.2 172.16.2	RTT 2.354ms 2.2286ms T 1.1/0.737 1/1.136 1.1/0.623 2/1.072	
Ping Result Direction LAN to WAN WAN to LAN Traceroute Result Direction LAN to WAN WAN to LAN	Statu Succ Succ	Status pass pass s ess	Ping Cou           5/5           5/5           4           Hop Count           50	int	Hop IP/R1	RTT 2.354ms 2.2286ms T 1.1/0.737 1/1.136	
ing Result Direction LAN to WAN WAN to LAN Graceroute Result Direction LAN to WAN WAN to LAN WAN to LAN	Statu Succ	S Status pass pass s ess ess	Ping Cou           5/5           5/5           4           50	int	Hop IP/R1 172.16.3 172.16.1 172.16.1	RTT 2.354ms 2.2286ms T 1.1/0.737 1/1.136 1.1/0.623 2/1.072	
ring Result Direction LAN to WAN WAN to LAN Graceroute Result Direction LAN to WAN WAN to LAN WAN to LAN Candwidth Result	Statu Succ Succ	S Status pass pass s ess s s s s s s s s s s s s	Hop Count           50	unt UI	Hop IP/RT	RTT         2.354ms         2.2286ms           1.1/0.737         1.1/0.623         2.21.072	
Ping Result Direction LAN to WAN WAN to LAN Fraceroute Result Direction LAN to WAN WAN to LAN WAN to LAN Upload (overlay)	Statu Succ Succ TCP Statu Success	s Status Pass Pass Pass Pass Pass Pass Pass Pa	Hop Count           5/5           5/5           5/5	unt UI S	Hop IP/R1 172.16.1 172.16.1 172.16.1 DP Status success	RTT       2.354ms       2.2286ms         T         1.1/0.623       2.2/1.072         UDP Bandwidth kbps/Loss       100000/0%	

# Improved Path Mapping and Bandwidth Usage

#### August 24, 2022

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.

Statistics	Monitoring >	Flows															
Flows																	
outing Protocols	Select Flow	s															
all	Flow Type:	LAN to	WAN 🗹 W	AN to LA	AN 🗆	Intern	et Load B	alancing	Table 🔲 '	TCP Term	ination Ta	able					
ec	Max Flows to Dis (Per Flow Type):	50 V															
	Filter (Optional):	er (Optional): Help															
ance Reports	Refresh																
rts	Flows Data																
orts																	
ity Reports	Both LAN to WA	N and WAN to L	AN Flows						1							Toggle Co	olumns
eports	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtua Path Overhe
iver/neidy	172.16.14.99	172.16.19.167	LAN to WAN	80	2189	тср	default	41572	Virtual Path	DC-BR	LOCAL	758	41571	14527110	2.072	6.337	0.8
mization	172.16.14.99	172.16.19.162	LAN to WAN	80	3161	ТСР	Override =	NO				261	41525	14427708	2.099	6.488	0.9
	172.16.14.99	172.16.19.161	LAN to WAN	80	6310	ТСР	Separate T	CP ACK C	lass = NO			60	41827	14468200	2.115	6.341	0.9
	172.16.14.99	172.16.19.170	LAN to WAN	80	10844	тср	Inorder H	loldtime: 9	100			560	41863	14393387	2.110	6.285	0.9
			برينيد بيندين			7.00		t Action =	DISCARD				44300		0.070	C 201	
ilability Paparts	Both LAN to WA	N and WAN to L	AN Flows													Toggle C	olumns
bliance Reports	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtu; Path Overhe kbps
Optimization	172.16.14.99	172.16.19.167	LAN to WAN	80	2189	тср	default	41572	Virtual Path	DC-BR	LOCAL	758	41571	14527110	2.072	6.337	3.0
	172.16.14.99	172.16.19.162	LAN to WAN	80	3161	тср	Override = Demote o	= NO n Large Pa	ickets = NO			261	41525	14427708	2.099	6.488	0.9
	172.16.14.99	172.16.19.161	LAN to WAN	80	6310	тср	Separate 1 Packet Sec	ICP ACK C quence Inc	lass = NO order = YES			60	41827	14468200	2.115	6.341	0.9
	172.16.14.99	172.16.19.170	LAN to WAN	80	10844	тср	Inorder H Late Packe	loldtime: 9 et Action =	900 : DISCARD			560	41863	14393387	2.110	6.285	0.9
	172.16.14.99	172.16.19.164	LAN to WAN	80	3387	тср	Packet Du Persistent	plication = Paths = N	NO O			58	41798	14472656	2.070	6.284	3.0
	172.16.14.215	172.16.19.99	LAN to WAN	9321	80	тср	Reliable = TCP Stand	YES alone ACk	- (s = NO			14	43483	2592802	2.145	1.022	0.9
	172.16.14.99	172.16.19.167	LAN to WAN	80	4200	тср	Check Flor	w TOS = N	IO ion = NO			312	41705	14426227	2.114	6.348	0.9
	172.16.14.99	172.16.19.169	LAN to WAN	80	3161	тср	IP,TCP,UD	P Header (	Compression =	NO		)56	40970	14508376	2.054	6.299	0.8
	172.16.14.218	172.16.19.99	LAN to WAN	3371	80	тср	Packet Ag	gregation	= NO			107	42980	2552820	2.043	0.967	3.0
	172.16.14.99	172.16.19.166	LAN to WAN	80	1116	тср	Rule ID =	1 0				313	41286	14568312	2.047	6.220	3.0
	172.16.14.213	172.16.19.99	LAN to WAN	17082	80	TCP	App Rule 1	D = N/A	_			361	42915	2556999	2.114	1.006	0.9
	172.16.14.217	172.16.19.99	LAN to WAN	4090	80	TCP	UPI Applic	ation = ht	tp			564	42530	2540882	2.059	0.983	3.0

# 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.** 

Select Flows																
Flow Type:	🗹 LA	N to W	AN 🗹	WAN to I	AN 🗌	Internet	Load Baland	ing Table	П	CP Ter	ninatio	on Table				
Aax Flows to Display Per Flow Type):																
Filter (Optional):	ilter (Optional): Help															
Refresh	Refresh															
Flows Data																
									Tog	gle Colu	mns					
Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
DC-MCN-BR1-VPX	LOCAL	3	291	435918	85.373	1023.106	36.881	0.000	52	N/A	15	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

The following figure illustrates when traffic is flowing, and the WAN attributes of the path are degraded, you notice that a new path is chosen for processing traffic without disruption. In this case, the path mapping feature allows you to indicate that the current best path processing the traffic is **DC-MCN-Internet2** -> **BR1-VPX-Internet** and the last best path that processed the traffic is **DC-MCN-Internet** -> **BR1-VPX-Internet**.

The last best path in this example is an indicator of which path served the connection earlier.

Sel	ect Flows												
Flow Ty	/pe:	۷ ۲	AN to WAN	🗹 WAI	N to LAN	🗆 In	ternet	Load Ba	alancing	Table 🔲 TCP Termination Table			
Max Fl (Per Flo	ows to Displa ow Type):	<sup>y</sup> 50	•										
Filter (0	Optional):			Help									
Refre	sh												
Flo	ws Data												
						Tog	gle Colu	mns					
ckets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
728	1090544	0.983	11.778	0.425	0.000	52	N/A	15	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

The following figure illustrates that when traffic is ongoing and more than one path is chosen for traffic processing due to demand in bandwidth, as shown below, more than one path is chosen when the traffic is being sent. Unlike in the case above, here there may be more than two paths also serving the traffic but in the GUI only the two best paths that is currently serving the traffic is displayed.

Observe **DC-MCN-Internet->BR1-VPX-Internet**, **DC-MCN-Internet2->BR1-VPX-Internet** being the two paths shown in the **Flows Data** table.

### Note

As indicated, only max two paths in the flows table are displayed.

s	elect Flow	s											
Flow Max (Per	Type: Flows to Dis Flow Type):	₽ LI Play 50	AN to WAN	VAN 🖻	l to LAN	🗆 In	ternet l	Load Ba	alancing	Table 🛛 TCP Termination Table			
Filter	(Optional):			Help									
Ret	resh												
F	lows Data							_					
					l	Toggle	Columr	ns					
ets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
355	1280790	318.598	3818.082	137.634	0.000	52	N/A	15	BULK	DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

The following figure illustrates that when traffic is still flowing, if the current best path which is **DC-MCN-Internet->BR1-VPX-Internet** is unavailable/inactive/degraded in WAN attributes, the current best path chosen will appear first in the path section of **Flows Data** table followed by the last best path which 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.

Selec	t Flows												
low Type	e:	🗹 LAN t	o WAN	WAN to	LAN 🗆	Intern	et Load	l Balan	cing Tab	le 🔲 TCP Termination Table			
Aax Flow Per Flow	s to Display Type):	50 <b>v</b>											
ilter (Op	tional):			Help									
Refresh													
Flow	s Data												
					[	Toggle	Column	ns					
ackets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
2764	4140472	170.434	2042.476	73.627	0.000	52	N/A	15	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

# **Duplicate Transmit Mode**

General packet duplication mode ensures that two paths are initially taken for processing packets of the same connection to ensure reliable delivery by duplicating packets across two separate paths.

For Path Mapping, you notice that two paths being taken in the path section of the flow table as long as two paths exist to process flows by duplicating.

The following figure illustrates that wen traffic is flowing, it can be noticed that two paths are shown to be processing the traffic. Unlike any other mode, even if traffic demands less bandwidth that can

be provided by just one path, this mode will always duplicate traffic across two paths for reliable application delivery.

You notice in the figure below, two paths in the path section of the **Flows Data** table; **DC-MCN-Internet2->BR-VPX-Internet**, **DC-MCN-MPLS->BR1-VPX-MPLS**.

1	Select Flo	ows												
Flov	v Туре:	•	LAN to W	AN 🗹 V	AN to LAN	🗆 Inte	rnet L	oad Bal	ancing	Table	TCP Termination Table			
Ma: (Per	Flows to I Flow Type	Display 50	۲											
Filte	er (Optiona	l):		He	lp									
R	efresh													
	Flows Da	ta					Toggle	Column	5					
e S)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
3	551	32640	88.836	42.100	38.377	0.000	0	N/A	9	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Duplicate, Reliable	iperf
4	1651	2362062	262.860	3008.560	113.555	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable	iperf

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.

Se	elect F	lows												
Flow Max F	Type: Tows to	Display 5	LAN to W	AN 🗹	WAN to LA	AN 🗆 Int	ternet Load	Balan	cing Ta	ble	🗏 ТСР 1	Fermination Table		
Filter	(Option	ial):		ł	Help									
Ref	resh													
FI	ows D	ata												
							Тс	ggle C	olumns					
IN I IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
CAL	10	9692	530732	75.025	32.705	32.411	0.000	0	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Duplicate, Reliable
CAL	0	34213	49055970	267.264	3066.058	115.458	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable

### **Persistent Path Transmit Mode**

Persistent path transmit mode helps to retain packets of a flow based on path latency impedance.

The following figure illustrates only one path which is the best path currently handling the flows and its packets. There is no demand of bandwidth and one path serves it all. Currently there is only one best path which is **DC-MCN-Internet->BR1-VPX-Internet.** 

Flows [	Data																
										1	Toggle (	Columns					
rvice ype	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
ual Path	DC-MCN-BR1-VPX	LOCAL	662	3	4494	1.127	13.511	0.487	0.000	4	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

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**.

Flow	s Data														
								То	oggle Co	olumns					
AN V IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
CAL	950	41	61418	0.992	11.894	0.429	0.000	4	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

In persistent mode, there can be more than one path chosen to process traffic. In that case, the GUI displays both the paths with best and next best in the path section of the flow table from the beginning of the traffic flow.

The following figure illustrates that the flow initially only needs more than two paths and they stay persistent as long as there is no path latency impedance crossing (50 ms). The two paths taken are shown as; **DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS.** 

	Flows	Data													
							Т	oggle C	olumns						
,	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
L	51	6368	367504	128.449	59.303	55.490	0.000	2	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Persistent	iperf
L	1	9694	13894396	195.491	2241.576	84.452	0.000	74	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

Assume that one of the best paths **DC-MCN-Internet** goes into high latency or is disabled. This makes a new path appear and the new path may be the best path or could be the second best path based on the decision of path selection at that instant of time.

Flo	ws Data													
						Togg	le Colui	mns						
Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
2	79540	4709572	147.475	73.223	63.709	0.000	2	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Persistent	iperf
0	119720	171655210	195.634	2233.531	84.514	0.000	74	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

# **Troubleshooting Management IP**

### August 24, 2022

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 - 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**

#### August 24, 2022

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**.

<ul> <li>Appliance Settings</li> </ul>	Configuration > Ap	opliance Settings (> 1	ogging/Monitoring			
- Administrator Interface						
Logging/Monitoring	Log Options	Alert Options	Alarm Options	Syslog Server	HTTP Server	
<ul> <li>Network Adapters</li> <li>Net Flow</li> <li>App Flow</li> </ul>	нттр					
- SNMP - NETRO APE	Server URL:	essages Send Test Me	ssage			
Licensing	Server UserName: Server Password:					

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**.

Configuration > A	ppliance Settings >	Logging/Monitoring			
Log Options	Alert Options	Alarm Options	Syslog Server	HTTP Server	
нттр	·	· · · · · · · · · · · · · · · · · · ·	·		
Enable HTTP M	lessages Send Test Me	essage			
Server URL:	https://sdwar	n/nitro/v1/conf			
Server UserName:	admin				
Server Password:					
	L				

#### Apply Settings

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.

	opliance Settings	Logging/Monitoring								
Log Options	Alert Options	Alarm Options	Syslog S	Server	HTTP Server					
Alarm Configura	ation									
Add Alarm										
Event Type		Trigger State	Trigger Duration (sec)	Clear Sta	ate	Clear Duration (sec)	Severity	E	imail	Syslo
	•	•			•			•		

3. Select an **Event Type** from the drop-down list.

Dashboard Monitoring	Con	DYNAMIC_VIRTUAL_PATH										
- Appliance Settings	G	WAN_LINK_CONGESTION		ogging/Monitoring								
Administrator Interface     Logging/Monitoring		USAGE_CONGESTION		Alarm Options	Syslog 9	Server	HTTP Server					
· Network Adapters		PROXY_ARP										
Net Flow App Flow	-	ETHERNET										
- SNMP		DISCOVERED_MTU										
- NITRO API Licensing		GRE_TUNNEL	Ŧ	gger State	Trigger Duration (sec)	Clear Sta	te	Clear Duration (sec)	Severity		Email	Syslog
+ Virtual WAN		•		•			•			۲		
+ System Maintenance												
	Ар	oly Settings										
												Þ

- 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

<ul> <li>Appliance Settings</li> </ul>	Configuration >	Appliance Settings	> Logging/Monitoring					
- Administrator Interface								
Logging/Monitoring	Log Options	Alert Options		Syslog Ser	ver HTTP Server			
·· Network Adapters			GOOD					
- Net Flow	Alarm Configu	ration						
- App Flow	Add Alarm		DISABLED					
- SNMP	Add Alarm		BAD					
- NITRO API	Event Type		DEAD	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Severity	Ema
+ Virtual WAN	VIRTUAL_PATH	<del>،</del> ۲		▼ 0		▼ 0		•
System Maintenance								
Dashboard Monitoring	Apply Settings						DEBUG	
Dashboard Monitoring	Apply Settings						DEBUG	
Dashboard Monitoring Appliance Settings	Apply Settings   Configuration  Configuration > A	opliance Settings >	Logging/Monitoring				DEBUG INFO NOTICE	
Dashboard Monitoring Appliance Settings - Administrator Interface	Apply Settings  Configuration  Configuration > Apply Settings	opliance Settings >	Logging/Monitoring				DEBUG INFO NOTICE WARNING	
Dashboard Monitoring Appliance Settings - Administrator Interface - Logging/Monitoring	Apply Settings  Configuration  Configuration > Apply Settings  Log Options	opliance Settings > Alert Options	Logging/Monitoring	Syslog Serve	r HTTP Server		DEBUG INFO NOTICE WARNING	
Dashboard Monitoring Appliance Settings - Administrator Interface - Logging/Monitoring - Network Adapters	Apply Settings	opliance Settings > Alert Options	Logging/Monitoring Alarm Options	Syslog Serve	r HTTP Server		DEBUG INFO NOTICE WARNING ERROR	
Dashboard Monitoring Appliance Settings - Administrator Interface - Logging/Monitoring - Network Adapters - Net Flow	Apply Settings	opliance Settings > Alert Options ation	Logging/Monitoring Alarm Options	Syslog Serve	r HTTP Server	]	DEBUG INFO NOTICE WARNING ERROR - CRITICAL	
Dashboard     Monitoring       Appliance Settings     -       - Administrator Interface     -       - Logging/Monitoring     -       - NetWork Adapters     -       - Net Flow     -       - App Flow     -	Apply Settings	opliance Settings > Alert Options ation	Logging/Monitoring     Alarm Options	Syslog Serve	r HTTP Server	]	DEBUG INFO NOTICE WARNING ERROR - CRITICAL	
Dashboard Monitoring Appliance Settings   Administrator Interface  Logging/Monitoring  Network Adapters  Net Flow  App Flow  SNMP NITEO APF	Apply Settings	opliance Settings > Alert Options ation	Logging/Monitoring     Alarm Options	Syslog Serve	tr HTTP Server	Clear	DEBUG INFO NOTICE WARNING ERROR CRITICAL ALERT	
Dashboard Monitoring Appliance Settings    Administrator Interface  Logging/Monitoring  Network Adapters  Net Flow  App Flow  SNMP  NTRO API Ucensing	Apply Settings  Configuration  Configuration > A  Log Options  Alarm Configur  Add Alarm  Event Type	opliance Settings > Alert Options ation	Logging/Monitoring     Alarm Options     Trigger State	Syslog Serve Trigger Duration	tr HTTP Server	Clear Duration freed	DEBUG INFO NOTICE WARNING ERROR CRITICAL ALERT EMERGENCY	Email
Dashboard Monitoring Appliance Settings  - Administrator Interface - Logging/Monitoring - Network Adapters - Net Flow - App Flow - SNMP - NITRO API - Licensing Virtual WAN	Apply Settings  Configuration  Configuration > A  Log Options  Alarm Configur  Add Alarm  Event Type  VIRTUAL_PATH	opliance Settings > Alert Options ation	Logging/Monitoring Alarm Options Trigger State	Syslog Serve Trigger Duration (sec) \$50	tr HTTP Server	Clear Duration (sec)	DEBUG INFO WARNING ERROR CRITICAL ALERT EMERGENCY	Email

5. Select the **Syslog** and **HTTP** checkboxes to receive notifications specific to the Syslog and HTTP server events. Click **Apply Settings**.

Log Options	Alert Options	Alarm Options	Syslog Serv	er HTTP Server							
arm Configura	ation										
dd Alarm											
vent Type		Trigger State	Trigger Duration (sec)	Clear State	Clear Duration (sec)	Severity		Email	Syslog	SNMP	нттр
IRTUAL PATH	•	DEAD 🔻	80	BAD V	80	NOTICE	•		<b>V</b>		

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
#### Citrix SD-WAN 11.5

- Administrator Interface		art Options	Alarm Ontions	System Server	н	TD Serve						
Network Adapters	Log options Re	Tr Options	Harmoptions	Systog Server		TP Serve	1			_		
Net Flow	Email Alerts											
App Flow												
SNMP	Enable Email Alerts	Send	J Test Email									
NITRO API	Destination Email Address(e	es):										
Licensing	SMTP Server Hostname or I	P Address:										
tual WAN	SMTP Server Port:	25										
tem Maintenance	Source Email Address:											
	You may enter multiple desi separated with semicolons (	tination email ac	idresses									
	Enable SMTP Authentic	ation										
	SMTP User Name:											
	SMTP Password:											
	Verify SMTP Password:											
	General Event Configu	ration								-		
										- 1		
	Event Type	Persists	te Email	Filter		Syslog	Filter	Filter		HTTP	Filter	
	SERVICE	0		Warning	٣		Warning	▼ Warning	*		Warning	
	VIRTUAL PATH	0		Warning	٣		Warning	▼ Warning	Ψ.		Warning	
	WAN LINK	D		Warning	Ŧ		Warning	▼ Warning	*		Warning	
	PATH	D		Warning	Ψ.		Warning	▼ Warning	*		Warning	
	DYNAMIC VIRTUAL PATH	D		Warning	٣		Warning	▼ Warning	٣		Warning	
	WAN_LINK_CONGESTION	D		Warning	Ŧ		Warning	▼ Warning	Ŧ		Warning	
	USAGE_CONGESTION	D		Warning	Ŧ		Warning	▼ Warning			Warning	
	HARD_DISK			Warning	Ŧ		Warning	▼ Warning	Ŧ		Warning	_
	APPLIANCE			Warning	Ŧ		Warning	▼ Warning	Ŧ		Warning	
	USER EVENT			Warning	Ŧ		Warning	▼ Warning			Warning	_
				Worning			Warning	▼ Warning			Warning	-
	CONFIG UPDATE			TTCI III U			· · ·				Warning	
	CONFIG_UPDATE			Warning	* *		Warning	▼ Warning	*			_
	CONFIG_UPDATE SOFTWARE_UPDATE PROXY_ARP			Warning	* *		Warning	Warning     Warning	<b>v</b>		Warning	
	CONFIG_UPDATE SOFTWARE_UPDATE PROXY_ARP ETHERNET			Warning Warning Warning	* * *		Warning Warning	Warning     Warning     Warning	* *		Warning	_
	CONFIG_UPDATE SOFTWARE_UPDATE PROXY_ARP ETHERNET WATCHTOG			Warning Warning Warning Warning	7 7 7 7		Warning Warning Warning	Warning     Warning     Warning     Warning     Warning	Υ Υ Υ		Warning Warning	_
	CONFIG_UPDATE SOFTWARE, UPDATE PROXY_ARP ETHERNET WATCHDOG APPLIANCE SETTINGS LIPDJ	ATE		Warning Warning Warning Warning Warning	* * * * *		Warning Warning Warning Warning Warning	Warning     Warning     Warning     Warning     Warning     Warning     Warning	<b>v</b> <b>v</b> <b>v</b> <b>v</b>		Warning Warning Warning	
	CONFIG_UPDATE SOFTWARE_UPDATE PROXY_ARP ETHERNET WATCHDOG APPLIANCE_SETTINGS_UPD/ DISCOVERD_MTU	ATE		Warning Warning Warning Warning Warning Warning	* * * * *		Warning Warning Warning Warning Warning	Warning     Warning     Warning     Warning     Warning     Warning     Warning     Warning	V           V           V           V           V           V           V           V           V           V           V		Warning Warning Warning Warning Warning	
	CONFIG_UPDATE SOFTWARE_UPDATE PROXY_ARP ETHERNET WATCHOOG APPLANCE_SETTINGS_UPDA DISCOVERED_MTU GRET INNIE	ATE		Warning Warning Warning Warning Warning Warning Warning	v           v           v           v           v           v           v           v           v           v           v           v           v           v           v           v           v		Warning Warning Warning Warning Warning Warning	Warning     Warning     Warning     Warning     Warning     Warning     Warning     Warning     Warning	<b>V</b> <b>V</b> <b>V</b> <b>V</b> <b>V</b> <b>V</b>		Warning Warning Warning Warning Warning	
	CONFIG_UPDATE SOFTWARE_UPDATE PROXY_ARP ETHERNET WATCHDOG APPLIANCE_SETTINGS_UPD/ DISCOVERED_MTU GRE_TUNNEL	ATE		Warning Warning Warning Warning Warning Warning Warning Warning Warning	v           v           v           v           v           v           v           v           v           v           v           v           v           v           v           v           v           v           v		Warning Warning Warning Warning Warning Warning Warning	Warning	<b>V</b> <b>V</b> <b>V</b> <b>V</b> <b>V</b> <b>V</b> <b>V</b> <b>V</b>		Warning Warning Warning Warning Warning Warning	
	CONFIG_UPDATE SOFTWARE_UPDATE PROXY_ARP ETHERNET WATCHOOG APPLANCE_SETTINGS_UPDA DISCOVERED_MTU GRE_TUNNEL IPSEC_TUNNEL	ATE		Warning	v           v           v           v           v           v           v           v           v           v           v           v           v           v           v           v           v           v           v           v		Warning Warning Warning Warning Warning Warning Warning Warning	Warning     Warning	<b>V</b> <b>V</b> <b>V</b> <b>V</b> <b>V</b> <b>V</b> <b>V</b> <b>V</b> <b>V</b>		Warning Warning Warning Warning Warning Warning Warning	
	CONFIG_UPDATE SOFTWARE_UPDATE PROXY_ARP ETHERNET WATCHDOG APPLIANCE_SETTINGS_UPDA DISCOVERED_NTU GRE_TUNNEL IPSEC_TUNNEL VISTUAL_INTERFACE	ATE		Warning Warning Warning Warning Warning Warning Warning Warning Warning	* * * * * * * * * * * * * * * * * * *		Werning	Warning			Warning Warning Warning Warning Warning Warning Warning	

# **Configure HTTP Notifications in Citrix SD-WAN Center**

To configure HTTP notifications:

1. Navigate to Fault > Notification Settings > HTTP.

Dashboard	Fault	Monitoring	Configuration	ı Report	ing Adr	ninistration	Nitro API
< Event Viewer		Fault / Notification	1 Settings / HTTP				
Notification Setting	s	Email Alerts	SNMP Traps	Syslog	нттр		
Severity Settings		HTTP Enable HTTP Me Server Url: https://10.102.78.15 Apply Send Test Ma	ssages Server Userr i4/tes admin essage	iame:	Server Password:		

- 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.

									0		
		-	Email	-	Syslog	-	SNMP	-	HTTP		
Event Type	Alert If State Persists	Enable	Severity Filter	Enable	Severity Filter	Enable	Severity Filter	Enable	Severity Filter		
SERVICE	Alert Immediately V		WARNING	r 🗆	WARNING <b>V</b>		WARNING V		WARNING <b>V</b>		
VIRTUAL PATH	Alert Immediately 🔻		WARNING	r 🗆	WARNING <b>T</b>		WARNING <b>V</b>	Ena	ble sending event ifications via		
WANLINK	Alert Immediately		WARNING	-	WARNING <b>T</b>		WARNING <b>V</b>	for	P Notifications the current Event e.		
PATH	Alert Immediately		WARNING	7	WARNING <b>T</b>		WARNING V		WARNING *		
DYNAMIC VIRTUAL PATH	Alert Immediately		WARNING	r 🗆	WARNING •		WARNING V		WARNING <b>V</b>		
WAN LINK CONGESTION	Alert Immediately		WARNING	r 🗆	WARNING •		WARNING V		WARNING <b>V</b>		
USAGE CONGESTION	Alert Immediately		WARNING	7	WARNING •		WARNING V		WARNING <b>T</b>		

2. You can choose to monitor Email, Syslog, SNMP, and HTTP event notifications for the following Event Types. Click **Apply**.

ashboard	Fault	Monitoring	Configuration		Reporting		Adı	ninistration	Ni	tro API		
ent Viewer		Fault / Severity Settin	gs									
tification Settings	5											
verity Settings				-	Email	-	-	Syslog	-	SNMP	-	HTTP
		Event Type	Alert If State Persists	Enable	SeverIty Fil	ter	Enable	Severity Filter	Enable	Severity Filter	Enable	Severity Filt
		SERVICE	Alert Immediately		WARNING	Ŧ		WARNING •		WARNING <b>V</b>		WARNING
		VIRTUAL PATH	Alert Immediately		WARNING	Ŧ		WARNING •		WARNING •		WARNING
		WANLINK	Alert Immediately		WARNING	Ŧ		WARNING .		WARNING .		WARNING
		PATH	Alert Immediately		WARNING	Ŧ		WARNING V		WARNING V		WARNING
		DYNAMIC VIRTUAL PATH	Alert Immediately		WARNING	Ŧ		WARNING V		WARNING V	0	WARNING
		WAN LINK CONGESTION	Alert Immediately		WARNING	Ŧ		WARNING V		WARNING V		WARNING
		USAGE CONGESTION	Alert Immediately		WARNING	V		WARNING V		WARNING V		WARNING
					WARNING	v						WARNING
	-				WARNING		-					WARNING
					MADNING							
					WARNING	•		WARNING *		WARNING *		WARNING
		CONFIG UPDATE			WARNING	V		WARNING V		WARNING V		WARNING
		SOFTWARE UPDATE			WARNING	Ŧ		WARNING V		WARNING <b>T</b>		WARNING
		PROXY ARP			WARNING	Ŧ		WARNING <b>T</b>		WARNING <b>T</b>		WARNING
		ETHERNET			WARNING	Ŧ		WARNING <b>V</b>		WARNING V		WARNING
		WATCHDOG			WARNING	Ŧ		WARNING •		WARNING <b>V</b>		WARNING
		SD WAN CENTER SYSTEM			WARNING	Ŧ		WARNING •		WARNING .		WARNING
		APPLIANCE SETTINGS			WARNING	Ŧ		WARNING .		WARNING .		WARNING
		SD WAN CENTER USER			WARNING	Ŧ		WARNING V		WARNING V		WARNING
		SD WAN CENTER			WARNING	v	-					MARNING
		STORAGE			Waxining	,	-	**************************************				(WHICHING)
		DATABASE			WARNING	Ŧ		WARNING <b>T</b>		WARNING <b>T</b>		WARNING
		CONNECTION TO VIRTUAL WAN			WARNING	Ŧ		WARNING •		WARNING V		WARNING
		DISCOVERED MTU			WARNING	Ŧ		WARNING •		WARNING V		WARNING
		GRE TUNNEL			WARNING	Ŧ		WARNING V		WARNING T		WARNING
		IPSEC TUNNEL			WARNING	v		WARNING V		WARNING T		WARNING
		VIRTUAL INTERFACE			WARNING	Ŧ		WARNING V		WARNING T		WARNING
		LICENSE EVENT			WARNING	Ŧ		WARNING V		WARNING V		WARNING
							_				_	

# Active bandwidth testing

#### August 24, 2022

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

To use the active bandwidth testing feature:

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

Dashboard Monitoring	Configurat	tion							
+ Appliance Settings	Configura	ation > System Maintenance	> Diagnostics						
+ Virtual WAN							1		
- System Maintenance	Ping	Traceroute Pa	cket Capture Path Bandy	vidth System Info	Diagnostic Data	Events	Alarms	Diagnostics Tool	
- Delete Files Restart Sustan	Instan	t Path Bandwidth Testing							
- Nestart System - Date/Time Settings - Local Change Management - Diagnostics - Undate Software	Path: Tes	t	MCN-5100-WL-2->BR572-	~					
Configuration Reset	Result	ts							
Factory Reset	Minimum B Maximum B Average B	andwidth:936564 kbps andwidth:1213863 kbps andwidth:1109045 kbps ule Path Bandwidth Testin	a						
	Adi		e.						
	Add	*	F		Dev of Work			11	
	Apply	settings	Frequency		Day of Week			Hour	Minute
	Histor	ry Path Bandwidth Testing	Result						
	Show 50	<ul> <li>entries</li> </ul>	Showing 1 to 27 of 27 entries	Search					First Previous 1 Next Last
	Num	From Link	To Link	Test Time	Min Bandwi	idth (kbps)	Ma	x Bandwidth (kbps)	Avg Bandwidth (kbps)
	1	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 2:01:03 PM	2883972		50	99707	4357330
	2	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 4:01:03 PM	3109115		38	72000	3616157
	з	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 6:01:04 PM	3041280		41	19960	3518949
	4	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 8:01:04 PM	2769377		37	00672	3276124
	5	RCN1-5100-WL-1	MCN-5100-WL-1	2/17/2018, 10:01:04 PM	409245		35	74153	2489269
	6	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 12:01:04 AM	2481756		40	01684	3198214
	7	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 2:01:04 AM	2549853		38	72000	3236546
	8	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 4:01:03 AM	3204413		39	82628	3642643
	9	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 6:01:03 AM	2997677		46	72357	3664018
	10	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 8:01:04 AM	2248258		62	88360	3612666
	11	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018. 10:01:04 AM	2410236		33	72387	2816032
	12	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 12:01:03 PM	2613600		44	01852	3563752
	13	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018. 2:01:04 PM	2324266		40	59961	3101910
	14	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 4:01:03 PM	2173340		36	84370	2929146
	15	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018. 6:01:03 PM	2613600		35	89493	3021890
	16	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018 8:01:03 PM	1676056		34	99380	2655280
	17	RCN1-5100-WL-1	MCN-5100-WL-1	2/18/2018, 10:01:03 PM	1954093		35	58944	2975884
	18	RCN1-5100-WI-1	MCN-5100-WI-1	2/19/2018 12:01:03 AM	2161116		37	84398	2902068
	19	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018. 2:01:04 AM	2986971		40	79765	3821158
	20	RCN1-5100-WI-1	MCN-5100-WL-1	2/19/2018 4:01:04 AM	3514084		41	81760	3893381
	20	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2018 6:01:03 AM	3358843		40	59961	3756691
	22	RCN1-5100-WI-1	MCN-5100-WI-1	2/19/2018 8:01:03 AM	3216728		40	45441	3716351
	23	RCN1-5100-WI-1	MCN-5100-WI-1	2/19/2018 10:01:04 AM	3558944		42	02773	3932908
	24	RCN1-5100-WL-1	MCN-5100-WL-1	2/19/2010, 10:01:07 AM	3437672		42	67102	2828557
	25	PCN1 E100 WE 1	MCN 5100 WL 1	2/19/2010, 12:01:05 PM	2974051		42	24000	2606052
	20	NCH1-5100-WL-1	MCN-5100-WL-1	2/10/2010, 2:01:04 PM	2074001		42	27000	416527
	20	NCN1-5100-WL-1	MCR-5100-WL-1	2/15/2018, 4/01/05 PM	2010000		62	12062	410535/
	2/	WCW-5100-WL-2	6A5/2-WL-1	2/19/2018, 5:23:04 PM	930504		12	12002	1103040
	Showing 1	to 27 of 27 entries							First Previous 1 Next Last ~

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.

Schedule Path Bandwidth Testing								
Add								
Path Name	Frequency		Day of Week		Hour		Minute	
DC_MPLS2->Branch_ ▼	every day 🔻		Sunday	*	0	•	0 •	×
v	every day 🔻		Sunday	Ŧ	0	Ŧ	0 •	'n
Apply Settings								

#### Note

A history of the path bandwidth testing results is displayed at the bottom of this page and results are archived every seven days.

Schedi	scnedule Path Bandwidth Testing								
Add	1								
Pa	th Name	Frequency		Day of	Week	Hour	Minute		
Apply	Settings								
Histor	y Path Bandwidth Testing	J Result							
show 50	▼ entries	Showing 1 to 14 of 14 entrie	Search		]		First Previous 1 Next Last		
Num	From Link	To Link	Test Time		Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)		
1	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:29:54 AM		363140	780616	525927		
2	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:00 AM		281995	573073	430345		
3	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:06 AM		317568	636640	480818		
4	BR_1-MPLS-1	DC_MCN-MPLS-1	3/29/2017, 1:34:00 AM		440056	1083357	725514		
5	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:10 AM		506768	786784	638673		
6	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:18 AM		462584	1388712	669232		
7	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:34:27 AM		380679	727895	533286		
8	DC_MCN-MPLS-1	BR_1-MPLS-1	3/29/2017, 1:35:12 AM		26823	35495	30578		
9	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:09 AM		350097	733929	591542		
10	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:47 AM		476024	789756	639048		
11	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:36:56 AM		446292	777674	608533		

# Adaptive bandwidth detection

#### August 24, 2022

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. From SD-WAN 11.5 release onwards, you can enable it on Citrix SD-WAN Orchestrator service. For more information, see Adaptive bandwidth detection.

View the Usage and Permitted Rates table by navigating to Monitor > Statistics > WAN Link Usage > Usage and Permitted Rates.

B Delta Packets Delta KB	Kbps	First Previous 1 Permitted Kbps	Next Last Congestion
0 0	0	25	NO
118 8.39	12.69	5905	N/A
6562 5203.86	7872.71	8105	NO
229 17.25	26.1	5880	N/A
3	Delta Packets         Delta KB           0         0           118         8.39           6562         5203.86           229         17.25	Delta Packets         Delta KB         Kbps           0         0         0           118         8.39         12.69           6562         5203.86         7872.71           229         17.25         26.1	Delta Packets         Delta KB         Kbps         Permitted Kbps           0         0         0         25           118         8.39         12.69         5905           6562         5203.86         7872.71         8105           229         17.25         26.1         5880

# **Best practices**

August 24, 2022

The following topics provide the best practices to be followed when the Citrix SD-WAN solution is being designed, planned, and executed in your network.

Security

Routing

QoS

WAN links

# Security

August 24, 2022

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, the 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.

## **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 the following secure lifecycle management practices:

• Secure the Operating System of the Server Hosting a Citrix SD-WAN VPX Appliance - A Citrix SD-WAN VPX appliance runs as a virtual appliance on a standard server. Access to the standard

server should be protected with role based access control and strong password management. Also, Citrix recommends periodic updates to the server with the latest security patches for the operating system, and update-to-date antivirus software on the server.

- Perform Remote Software Updates Install all security updates to resolve any known issues. Refer to the Security Bulletins webpage 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.
- Deploy the management interface of the appliance behind the DMZ to ensure that there is no direct Internet Access to the Management interface. For added protection, ensure that the management network is isolated from the Internet, and only authorized users with approved management applications are running in the network.

## **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 RA-DIUS 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 > Appliance Settings > Administrator Interface								
Administrator Interface									
<ul> <li>Logging/Monitoring</li> </ul>	User Accounts RADIUS TACACS+ HTTPS Cert HTTPS Settings Miscellaneous								
Network Adapters	Installed Certificate								
Net Flow	Instancy Ce uncare								
App Flow	Irrund to:								
SNMP	ISUEL IC. ISUEL								
NITKU API	Country: US Country: US								
Licensing	State/Province: California State/Province: California								
+ Virtual WAN	Locality: San Jose Locality: San Jose     Organization: Citrix Systems. Inc.     Organization: Citrix Systems. Inc.								
+ System Maintenance	Organizational Unit: Engineering Organizational Unit: Engineering								
	Common Name: Citrix Common Name: Citrix								
	сные. зарросуссиясан								
	Certificate Details:								
	Certificate Fingerorint: 24-BE-11-86-0E-22-AE-K&-Da-86-22-E2-E7-C3-D3-98-20-51-42-D5								
	Certimate imperptint 24tiet-1118600F32AE36ABAU2080632E35F74C5103398F30f511A22105 Start Date: Mar 20 0335515 2017 GMT								
	End Date: Mar 18 03:35:15 2027 GMT								
	Serial Number: C5586E258899CFF6								
	Upload HTTPS Certificate Files								
	Upload the certificate that secures the Management HTTPS connection to this Virtual WAN appliance. Uploading and installing the HTTPS Certificate will cause the HTTP server to restart, invalidating all connected sets NOTE: For best results: when the operation is complete close the browser window and reconnect to the appliance.								
	Certificate Filename: Choose File No file chosen								
	Key Filename: Choose File No file chosen								
	Upload HTTPS Certificate Files.								
	Regenerate HTTPS Certificate								

#### Consider using the Citrix Web App Firewall

Citrix ADC licensed appliance provides a built-in Citrix Web App Firewall that uses a positive security model and automatically learns the proper application behavior for protection against threats such as command injection, SQL injection, and Cross Site Scripting.

When you use the Citrix Web App Firewall, users can add extra security to the web application without code changes and with little change in configuration. For more information, see Introduction to Citrix Web Application Firewall.

## **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 a 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 the 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 the 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.

Riewall Policy Templates Rule Groups Network Objects Route Learning Import Template Route Learning Export Template Virual Path Default Sets	Add Priority: 100			? ×	Port Service Port List
Dynamic Virtual Path Default Sets Internet Default Sets	From Zones		To Zones		urce Destination
Intranet Default Sets DHCP Option Sets	Zone	Enable 🔺	Zone	Enable 🔺	IP Idress Port Service IP Address Port Est
Autopath Groups	Any Defects LAN Zeres		Any Default LAN Zene	×	
Service Providers WAN-to-WAN Forwarding Groups	Internet Zene		Jerault_LAN_Zone		
WAN Optimization Features	Untrusted Internet Zone		Untrusted Internet Zone		
WAN Optimization Application Classifiers WAN Optimization Service Classes	Action: Allow • Match Type: IP Protocol • IP Protocol: Any	Log Interval (s): 0 Application Objects: Applic Any * DSCP: Any *	Log Start Log End ation:     Applicat Allow Fragments Reverse Also	Connection State Tracking: Use Site Setting v tion Family: v Match Established	
	Source Service Type: Any • Dest Service Type: Any •	Source Service Name: Source Any	IP: Source I	Port	
Audits: 0 Audit Now				Add Cancel	?

#### 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.

#### **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 the 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 the 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

August 24, 2022

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

August 24, 2022

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

#### August 24, 2022

Citrix SD-WAN platforms support upto 8 public internet connections and 32 Private MPLS connections. This article outlines WAN link configuration best practices for the Citrix SD-WAN solution.

Points to remember while configuring WAN links:

- Configure the **Permitted and Physical** rate as the actual WAN link bandwidth. In cases where the entire WAN link capacity is not supposed to be used by the SD-WAN appliance, change the **Permitted** rate accordingly.
- When you are unsure of the bandwidth and if the links are non-reliable, you can enable the **Auto Learn** feature. The **Auto Learn** feature learns the underlying link capacity only, and uses the same value in the future.
- If the underlying link is not stable and does not guarantee fixed bandwidth (for example; 4G links), use the **Adaptive Bandwidth Detection** feature.

- It is not recommended to enable **Auto Learn** and **Adaptive Bandwidth Detection** on the same WAN link.
- Manually configure the MCN/RCN with the Ingress/Egress physical rate for all the WAN links since it is the central point of bandwidth distribution among multiple branches.
- For increased reliability of important datacenter workloads/services, when auto-learn is not used, use reliable links with SLA's that does not have random variation of capacity.
- If the underlying link is not stable, change the following Path settings:
  - Loss Settings
  - Disable Instability Sensitive
  - Silence time
- Use **Diagnostic tool** to check the link health/capacity.
- If SD-WAN is deployed in **one-arm** mode, ensure that you do not overrun the physical capacity of the underlying link.

#### Verifying ISP link Health

For new deployments, earlier than SD-WAN deployment and when adding new ISP link to the existing SD-WAN deployment:

- Verify the link type. For example; MPLS, ADSL, 4G.
- Network characteristics. For example bandwidth, loss, latency, and jitter.

This information helps in configuring the SD-WAN network as per your requirements.

## **Network topology**

It is commonly observed that specific network traffic bypasses the Citrix SD-WAN appliances, and uses the same underlying link configured in the SD-WAN network. Because SD-WAN does not have complete visibility over link utilization, there are chances that SD-WAN oversubscribes the link leading to performance and PATH issues.

## Provisioning

Points to consider while provisioning SD-WAN:

• By default, all branches and WAN services (Virtual Path/Internet/Intranet) receive equal share of the bandwidth.

- Provisioning sites needs to be changed, when there is high disparity in terms of bandwidth requirement or availability between the connecting sites.
- When dynamic virtual paths are enabled between maximum available sites, the WAN link capacity is shared between the static virtual path to DC and the dynamic virtual paths.

# FAQs

August 24, 2022

## **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 MC-N/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 Set-tings** 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.

So	heduling Information			
		Saust		?
Show	100 • entri	Edit Selected	Refres	h
	Site Name 🔺	Scheduling Information	Status	Edit
O	GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		0
O	MCNVPXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	$\bigcirc$	0
O	MCNVPXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	$\bigcirc$	0
O	RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		0
O	RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		0
Ο	RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		0
Ο	RCN2BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		0
Ο	RCN2BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		0
Ο	RCN2BR3VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		0
0	RCN2RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		0
0	RCN2RCN(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		0
Ο	RCN3BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		0
Ο	RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		0
Ο	RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	8	0
Ο	RCN3RCN2100	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		0
Ο	RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	•	0
Ο	RCNDefaultBR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)	0	0
Showi	ng 1 to 17 of 17 entries	Previous	1	Next

Can I use *tar.gz* file to upgrade to next release, when single step upgrade was used for previous software upgrade?

You can use *tar.gz* file to upgrade, but it is not recommended because you can perform software upgrade by using the.*upg* file. Upload to upgrade operating system (OS) component software by logging into each applicable appliance. From release 9.3 version 1, the **Update Operating System Software** page is depreciated. As a result, you can perform change management by using the *.zip* package to upgrade OS components.

How can we validate the current running versions of OS Components?

Now you cannot validate the current running versions of OS components from the UI. You can log in from each console or get STS to view this information.

What difference it would make if I have bare metal appliances in my network? Does scheduling impact bare metal / Virtual appliances?

Bare Metal appliances like **SD-WAN** –**410,2100,4100,5100 SD-WAN** run only SD-WAN software. Bare metal appliances do not need OS components packages. These platforms are treated on par with SD-WAN VPX-SE appliances in terms of software need. The MCN will not transfer OS components packages to these appliances. Setting scheduling information will not take effect for these appliances, because they do not have any OS components that need upgrade.

How does SSU work in high availability environment / deployment?

In high availability deployment at MCN, we have a limitation, where the active MCN switch's/toggles the role of primary MCN during Change Management and Standby/Secondary MCN takes over. In this case, you can perform Change Management once again with the *.zip* package on the active MCN for the packages or you can switch back to primary MCN by toggling the role of active MCN so that original primary MCN can take up the role for the OS components packages to be staged to other branches.

How does single step upgrade work in high availability environment / deployment?

While performing single step upgrade in high availability deployment, the role of the primary MCN and the Standby MCN is toggled. This is a limitation. If this happens, perform Change Management again with the *.zip* package on the active MCN. Alternatively, you can switch back to the primary MCN by toggling the role of the active MCN so that the original primary MCN can stage OS components packages to the branches.

Is single step upgrade support for zero-touch deployment to restart strap the appliances?

Yes, it can be used.

Can I use single step upgrade to upgrade my standalone WANOP appliance?

No.

Can I use single step upgrade to upgrade standalone WANOP appliance deployed in two box mode?

No. Only SD-WAN appliance which is part of two box mode would be upgraded and not the WANOP standalone appliance.

Which package should I use to upgrade to multi-tier network?

Use the single step upgrade package *ns-sdw-sw-<release-version>.zip* file when the current software version is 9.3.x or above. MCN takes care of staging package to RCN and RCNs stage software package to its respective branches.

After uploading the *ns-sdw-sw-<release-version>.zip* file, I am seeing only one platform model under current software?

From release 10.0, support for scale architecture is introduced to speed up processing of single step upgrade. You can see only the MCN platform model under current software. Other appliance packages are listed/displayed/processed when you choose the **Verify** or **Stage Appliance** button.

For VPX/VPXL/bare metal appliances, which packages are staged for RCN?

Package is staged to RCNs because RCNs Branches can be of any platform model. Hence they need all packages.

How does my branch site behind the RCN obtain OS component packages if RCN is a VPX appliance, and branch is an appliance that needs these packages?

RCN stages the relevant package to the branch that needs the OS component packages after activation of SD-WAN VW software package.

Can I choose Ignore Incomplete during staging and proceed to next stage of change Management? What impact does it have for sites that have not completed staging when this button is selected?

Yes, you can click **Ignore Incomplete.** This enables **Next** button and the Progress bar is displayed. This option is provided for scenarios where the site is not reachable and change management is still waiting for staging to complete for those site, so users can proceed to next stage by ignoring the stage state and proceed to activation. After the site comes up, MCN stages the package after completion of activation.

#### Partial software upgrade

What is partial site upgrade and how can I use it?

Partial site software upgrade is a new feature introduced in release 10.0. You can stage newer version of release 10.x from the MCN and activate staged software version from **Local Change Management** page on selected sites/branches. Before activating staged software on site/branch, ensure that check box is enabled from MCN.

- This feature is disabled by default. The existing correction mechanism keeps the network in sync. The user has to choose to allow partial site upgrades by enabling a check box on the Configuration > Change Management Settings page.
- Partial Software Upgrade can be done only on a Branch or RCNs and not at the MCN.

Below is the usecase/scenario when partial site software upgrade can be used:

Validate if a software patch with relevant changes is compatible and working for a specific site (where partial site upgrade is done). Validate that the upgraded software is working as expected. This helps validate the new software and fix at a specific site before upgrading entire network with the new software.

Can I use this feature to upgrade from:

- 10.0 to 10.x
- 10.0.x to 10.0.y
- 11.0 to 11.y
- 11.0.x to 11.0.y
- All of the above

Partial Site Software Upgrade is applicable only when appliance is running software release 10.x and newer, and can be used within the same major version of software. It can be used between releases 10.0 to 10.0.x/10.x. Only as part of partial site software upgrade, configuration cannot be changed.

Can I test new feature to test as part of partial software upgrade by enabling them from the config?

No, partial software upgrade requires that now Active and Staged config to be identical. Only software version can change.

Can I disable Partial Software Upgrade for RCN?

No, Partial Software Upgrade can be enabled or disabled from MCN only. At RCN the feature is in readonly mode.

Can I use Partial Software Upgrade when I have active as 9.3.x and 10.0.x as staged?

No, the appliance should be running on release 10.0 as active software.

What happens when Partial Software Upgrade option is disabled from MCN, while some branches are already upgraded through this feature?

MCN sends notification to all appliances in the network that Partial Software Upgrade feature is disabled, and then all appliances in the network are auto-corrected by MCN to match to its active and staged version. However, note that MCN is expecting for Activate Staged option to be clicked from Activation page of **Change Management**. You can choose to activate the network by clicking **Activate Staged** button or click **Change Preparation** to cancel state by accepting the confirmation.

## **Change Management Roll Back**

What is rolled back feature in Change management process?

From release 9.3, the Change management rollback feature enables roll back to the Working Configuration when unexpected events such as, t2-app crash or Virtual path state becomes inactive after a configuration update. The network and the appliances are monitored for 10 mins after the Configuration update and during that interval if the following conditions are met (provided user has enabled the feature), the Staged configuration will be activated. The Active software is rolled back to Staged.

What is the criteria for the configuration roll back to restart?

The rollback occurs, if the following scenarios are encountered:

- 1. MCN After config/software change, if t2\_app service gets disabled due to crash within 30 min interval.
- 2. MCN After config/software change, if Virtual Path service is down for 30 minutes or longer after activation. The Rollback feature is initiated at the sites.
- 3. Site After config/software change, if the Site loses its communication with MCN, then the rollback feature is initiated.
- 4. Site After config/software change t2\_app service gets disabled due to crash within 30 min interval.

What happens after rollback?

After configuration rollback, the faulty config/software is presented as Staged software.

How are users notified that roll back occurred?

A yellow banner at the top in the GUI saying Config is rolled back due to respective errors is displayed. Also, you can see it is change management status table. It shows **Configuration Error** or **Software error** corresponding to the site for which roll back occurred.

Does config and software both get rolled back?

Yes, if software upgrade is also performed along with configuration, and roll back scenario is encountered then Software also gets rolled back.

What happens if there is an issue in MCN and it crashes or loses connectivity with all the sites?

The entire network is rolled back except MCN. Notification is displayed, and all the sites show roll back status in the change management section. You can resolve the issue on MCN manually.

Can we disable this feature?

Yes, we can disable this feature just before activation. However, by default this feature is enabled.

How does roll back interact with Partial Software Upgrade when I have multi-tier network?

- If partial software upgrade is disabled, and if a site in a region (or the RCN) rolls back, the region with the problem is rolled back and once completed the rollback propagates up to the MCN. As a result, the MCN and the rest of the network to rolled back. Both the RCN in the region that rolled back, and the MCN display the rollback banner that the MCN cannot auto-dismiss the rollback banner at the RCN.
- If partial software upgrade is enabled, and if a site in a region (or the RCN) rolls back, only that region is rolled back. The rollback event does not propagate back to the MCN. As a result, the MCN leaves the region. The MCN does not show rollback banner and does not roll back itself or the network.

In both these scenarios, the RCN displays the rollback banner until it is dismissed. Because, it cannot be auto-dismissed by MCN.

# **Reference material**

August 24, 2022

Application Signature Library

A list of applications that the Citrix SD-WAN appliances can identify using Deep Packet Inspection.

# net>scaler

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.