NetScaler SD-WAN 9.2

Jun 14, 2017

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

CloudBridge

CloudBridge 9.0  CloudBridge 8.1  CloudBridge 8.0  CloudBridge 7.4  CloudBridge 7.4  CloudBridge 7.3

For information on NetScaler SD-WAN WO 9.2 installation, deployment, and feature configuration, please refer CloudBridge 7.4 documentation.

Overview

What's New

Release Notes

NetScaler SD-WAN 9.2 Release Notes
NetScaler SD-WAN 9.1.2 Release Notes
NetScaler SD-WAN 9.1.1 Release Notes
NetScaler SD-WAN 9.2.1 Release Notes

Before You Begin

System Requirements
Acquiring the NetScaler SD-WAN Software Packages
NetScaler SD-WAN Software Packages and Appliance Models
NetScaler SD-WAN Appliance Packages
Preparing for Your Deployment
Installation and Configuration Information Checklist

Deployment

Installing and Deploying a SD-WAN VPX Standard Edition on VMware ESXi
Setting up the Master Control Node (MCN) Site
Adding and Configuring the Branch Sites

Configuration
Configuring Virtual WAN Service
Configuring the Virtual Path Service Between the MCN and Client Sites
Enabling and Configuring WAN Optimization

Monitoring
Viewing Statistical Information
Viewing Flow Information
Viewing Reports
Viewing Firewall Statistics

How-To-Articles
Virtual Routing and Forwarding
How To Configure Routing Domain
How To Configure Routes
How To Select Routing Domain for Intranet Service
How To Configure Interface Groups
How To Configure Virtual IP Addresses
How To Configure Virtual IP Address Identity
How To Configure GRE Tunnels
How To Configure Access Interface
How to Customize Classes
How to Add Custom Applications and Enable MOS
How to Create Rules
How To Configure Firewall Segmentation

Dynamic Routing
OSPF
BGP
iBGP
eBGP

Standby WAN Links

Secure Web Gateway

Use Cases - Virtual Route Forwarding
Deploying SD-WAN in Gateway Mode
Deploying SD-WAN in PBR mode (Virtual Inline Mode)
Building a SD-WAN Network
Dynamic Paths for Branch to Branch Communication
Configuring Static WAN Paths
Routing Support for LAN Segmentation
Utilizing Enterprise Edition Appliance to Provide WAN Optimization Services Only
SD-WAN SE/EE Appliance in Hairpin Deployment Mode
Two Box Mode

Zero Touch Deployment

Licensing
Provisioning Licensing
License Procedure

Upgrade
Upgrade to 9.2 With Working Virtual WAN Configuration
Upgrade to 9.2 Without Virtual WAN Configuration
Convert SD-WAN 1000 / 2000 WANOP Appliances to Enterprise Edition With USB
Converting Existing Appliance to Enterprise Edition Appliance

About SD-WAN VPX Standard Edition
NetScaler SD-WAN VPX-SE Installation Requirements and Prerequisites
Differences Between a VPX-SE and a WANOP VPX Installation
Overview of VPX Installation and Deployment Procedures
NetScaler SD-WAN VPX-SE Installation and Configuration Information Checklist

Getting Started
NetScaler SD-WAN Management Web Interface
Installing the SD-WAN Appliance Packages on the Clients
Preparing the SD-WAN Appliance Packages on the MCN
Connecting the Client Appliances to Your Network
Setting up the SD-WAN Appliances
Route Filtering

IPSec Tunnel Termination and Monitoring

How to Configure IPSec Tunnels for Virtual and Dynamic Paths
How To Configure IPSec Tunnel Between SD-WAN and Third-Party Devices
How To Add IKE Certificates
How To View IPSec Tunnel Configuration
IPSec Monitoring and Logging
Eligibility for IPSec Non-Virtual Path Routes
IPSec Null Encryption

DHCP Client and Server Management

Link State Propagation

Multiple Net Flow Collectors

Network Objects

QoS Fairness With RED

SNMP MIBs

MPLS QoS Queues

Statefull Firewall and NAT Support

Auto Secure Peering and Manual Secure Peering

Active Bandwidth Testing

Adaptive Bandwidth Detection

Diagnostic Tool

NetScaler SD-WAN Center 9.2
Overview

Mar 30, 2017

The NetScaler SD-WAN product was formerly called "CloudBridge". Similar to the previous product portfolio, NetScaler SD-WAN is available in three different editions, allowing you to deploy the features you need at each location with easy upgrades, configuration, and monitoring.

All references to the term “CloudBridge” is applicable to the new product term “NetScaler SD-WAN”.


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

- **NetScaler SD-WAN Enterprise Edition (EE)** – This Edition includes both Standard Edition and WAN Optimization features. Enterprise Edition Integrates WAN virtualization with WAN optimization capabilities to optimize branch and mobile user experience and to achieve fully resilient applications regardless of network quality. For release 9.1, Enterprise Edition is available for the 1000-VW and 2000-VW branch hardware appliances, only.

- **NetScaler SD-WAN Standard Edition (VW/SE)** – This Edition includes Standard Edition Virtual WAN features, only. It supports software-defined WAN capability to create a highly reliable network from multiple network links and to ensure that each application takes the best path to achieve the highest application performance.

- **NetScaler SD-WAN Optimization Edition (WANOP)** – This Edition includes WAN Optimization features, only. It supports application acceleration, data reduction and protocol control to optimize applications across the WAN. Optionally, it can include virtual Windows Server to simplify branch infrastructure and mobile PC plug-in capability.

**Note**

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

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

See the Licensing section, for more information about the license options available for using NetScaler SD-WAN platform editions.
Release Notes

Oct 09, 2016

This release notes describes the new features, enhancements, known issues, and fixed issues applicable to Citrix NetScaler SD-WAN software releases 9.1 and later for the SD-WAN Standard Edition and Enterprise Edition appliances.

For information about the previous product called CloudBridge Virtual WAN and CloudBridge Enterprise Editions, see the CloudBridge Virtual WAN Administration Guide.

For information about WAN OP edition, refer to the CloudBridge 7.4.x documentation.

- Enterprise Edition appliances cannot be joined to Active Directory Domains. To accelerate file or Microsoft Exchange servers in a branch, a standalone WAN Optimization deployment is required.
- Secure peering is required for WAN optimization of signed SMB or encrypted MAPI traffic. This is only supported on data path IPs and is not supported over the management IPs.
- Automatic Secure peering of an Enterprise Edition appliance from a standalone WAN Optimization appliance requires that the datacenter side WAN Optimization appliance is running release 7.4.x or later.
- Virtual WAN Enterprise Edition does not support WAN optimization of SSL traffic.

Web Management Interface

- Issue ID 636005: Single bundle upgrade of NetScaler SD-WAN from release 8.1 or 9.0 to 9.1 fails if using Internet Explorer version 11.0

  If you use Internet Explorer version 11.0 to connect to the web management interface and navigate to Configuration > System Maintenance > Update Software, the following error message appears when you attempt to perform a single bundle Virtual WAN or SD-WAN upgrade from release 8.1.x or 9.0.x to release 9.1.x:

  An error occurred while transfer of software to change management system. No space file = C:\Users\Administrator.NSLB1\Downloads\ CB-VW-PKG-9.1.0.114.upg

  Workaround: Use a different web browser, such as Mozilla Firefox or Google Chrome.

- Issue ID 659515: NetScaler SD-WAN web interface freezes at the Quick Install Wizard page.

  Description: The Quick Install Wizard page appears instead of the admin login page when a NetScaler SD-WAN VPX WANOPT instance deployed on VMware (OVA template) or HyperV (XVA template) with the 9.1 software image is restarted. After the restart, the SD-WAN web interface freezes at the Quick Installation page, and clicking the Skip Install button does not work. Also, the Install button on the Quick Installation page is not enabled. The web interface stays frozen on the Quick Installation page.

  Workaround: Skip the Quick Installation wizard by clicking the Dashboard tab, then the Monitoring tab, and then the Configuration tab in the web interface. Configuration otherwise available through the quick install wizard has to
be performed manually through the web interface options available on the Configuration page.

ICA Connectivity and Client Session

• Issue ID 658696: LINUX VDA version field for ICA Session information on WAN OPT appliance is blank or empty

  Description: In a LINUX VDA session on a WAN OPT appliance, the VDA version field in the session information table at ICA Advanced > Session/Conn is empty.

• Issue ID 660501: Session Reconnection of NetScaler SD-WAN WAN OPT client fails with HTML5 Receiver version 2.1

  Description: When you attempt to reconnect to a NetScaler SD-WAN WAN OPT client session through XenDesktop or XenServer with HTML5 Receiver version 2.1, the session reconnect fails.

  Steps:
  1. In XenDesktop, click Launch application through the HTML5 Receiver.
  2. In the storefront setting, select Always use HTML5 receiver.
  3. Disrupt the connection for more than a minute, and then try to reconnect. The session reconnect fails and the XenDesktop session closes with an error.

Licensing

• Issue ID 659809: DBV check support for Remote Licensing Server configuration on Virtual-WAN and SD-WAN appliances

  Description: The DBV check fails and the appliance becomes unlicensed after an upgrade, if the Maintenance date is expired, and when the customer has Remote License configured on the SD-WAN.

  Workaround: Ensure that the Maintenance date in the license file is more recent than the Built date of the SD-WAN or Virtual-WAN software image that is being upgraded.

Networking and Security

• Issue ID 653039: IPsec Rekey based on Data (KB) not working properly

  Description: In this release, NetScaler SDWAN does not support IPsec tunnel Rekey based on the assigned data (Kilo Bytes). After the available data KB is exhausted, the IPsec tunnel is not brought down and rekeying does not work. No data loss is observed.

  Configure an IPsec Tunnel between the SD-WAN appliance Intranet and third-party appliance in the SD-WAN network and set IKE and IPsec Lifetime in seconds to 3600 seconds, set IPsec Lifetime in KB to 500 KB. Use the ping command to send basic ICMP traffic (for example, ping 6.2.1.1 -I 5.2.1.1 -s 1000 –i 0.001). Generate enough traffic so that the IPsec SA lifetime in KB uses 500KB.

  During this phase, the IPsec Rekey has to happen before expiration of Lifetime in KB, but the IPsec Tunnel is deleted after data expiration and packets are dropped. The new IPsec tunnel is established after a few seconds.

  Root Cause: All IKE/IPsec generated events are placed in an event queue with a timestamp attached to each entry within the queue. When the queue timestamp expires, the queued event is processed, and the entry is removed from the queue. In the case of data expiry, a duplicate entry already present in the event queue does not allow the rekey
SNMP

- Issue ID 655068: The SNMP MIB table entry query for the management interface returns incorrect values.

  Description: In the management interface, the values of the SNMP query table fields for Bytes Sent, Packets Sent, Bytes Received, Packets Received, and Bytes Dropped fields are zero (0). Only the Packets Dropped field has a larger value.

  Workaround: Use the following command to obtain the table output:

  ```
  snmptable -v2c -c public <ip> -Cb CITRIX-NetScaler-SD-WAN-MIB::sdWANStatsEthernetInterfaceTable
  ```

- Issue ID 660821: The SNMP MIB table entry query for Dynamic WAN paths displays “0” instead of no entries when Dynamic WAN Paths are not configured.

  Description: Each field of the Dynamic WAN Path snmptable -v2c -c public -Cb <ip> CITRIX-NetScaler-SD-WAN-MIB::sdWANStatsDynamicWANClassTable displays a zero (0) instead of no entry.

Platform

- Issue: On the 4000 Standard Edition appliances, the link state for 10G interface is not propagated when the 10G link becomes inactive. The link states for all other 1G interfaces are propagated correctly.

SD-WAN Center

- Issue ID 580103: E-Mail and Syslog event notifications not displayed for the PATH event type in SD-WAN Center.

  Description: In the SD-WAN Center web interface, events raised for WAN PATH objects from the MCN are visible in the Event Viewer, but the email or syslog notifications are not available.

- Issue: Direct upgrade from previous releases to 9.1 is not supported for SD-WAN Center

  Description: Upgrading SD-WAN Center from release 8.x or 9.0.x to 9.1 requires an intermediate upgrade to Release 9.0.1 build 1000.

  Workaround: The intermediate upgrade is not required if you use a new software image of Release 9.1 SD-WAN center.

- Issue ID 640507: Auto secure peering feature will not work over TLS1.2 until support is added to Data Path Access. Currently TLS1.2 support is limited to Management Path Access only.
- Workaround: Auto secure peering has to be performed over HTTPS configuration using the default "Any Protocol" and then the configuration can be moved to "TLS1.2".

- Issue ID 641505: Direct upgrade of MCN from version 8.1 to 9.0.1 on VPX on a VMware ESXi server fails.
  - Workaround: Upgrade to version 9.0 first and then to 9.0.1.

- Issue ID 608355: When Citrix XenServer private networks are deployed for CloudBridge VW VPX along with CloudBridge WAN Optimization VPX, the 'ChecksumSendForceSW' parameter available through the support.html page on the WAN OPT web interface must be turned off.

- Issue ID 580103: In Virtual WAN Center, events raised for WAN PATH objects are visible in the Event Viewer, but are not available for email or syslog notifications.
NetScaler SD-WAN 9.2 Release Notes

May 10, 2017

This release notes describes the fixed issues, known issues, and limitations applicable to Citrix NetScaler SD-WAN software release 9.2 for the SD-WAN Standard Edition, WANOP, and Enterprise Edition appliances.

Note

- This release note document does not include security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin.
- The [# XXXXXX] labels for issue descriptions are internal tracking IDs used by the SD-WAN support team.

Fixed Issues

Software Downgrade

- Issue ID 662369: NetScaler SD-WAN VPX software downgrade from release 9.1.2 to 9.1.0 fails
  - Downgrading software version from 9.1.2 to 9.1.0 on NetScaler SD-WAN VPX appliances in XenServer, VMWare ESXi, and AWS environments fails. All SD-WAN services are disabled and both GUI and CLI become unresponsive.

Routing-OSPF Link-State Advertisement (LSA) ID Collision

- Issue ID 671213: LSA ID collisions are observed in OSPF Type-1 deployment
  - A NetScaler SD-WAN appliance does not support OSPF Type-1 LSAs when deployed as an Area Border Router (ABR) in OSPF Type-1 Intra Area stub-networks.

SSL Secure Peering not established between 4000/5000 appliances configured at the branch site and data center

- Issue ID 665823: After you provision SSL secure tunnel configuration and instances on the 4000 and 5000 appliances with factory image version 9.1.2, the following message is displayed on the appliances configured at the branch site: unable to activate signaling listener for the following IP/TCP ports.

Licensing

- Issue ID 666146: SD-WAN WANOP License page might not refresh when Local License file is uploaded.

Incorrect CLI output for Connection Idle Timeout

- Issue ID 671169: Discrepancy between CLI output and GUI display for Connection Idle Timeout parameter. The show-config-script command output displays the Connection Idle Timeout parameter as disabled even when it is enabled in the GUI and vice-versa.
Known Issues

**SD-WAN 4100 SE**
- Issue ID 675452: NetScaler SD-WAN WANOP client info displays OS version as Windows 8 even when plugin is installed in Windows 10 OS.
- Issue ID 675715: On a NetScaler SD-WAN 4100-SE appliance, changing Interface settings for 1G interface does not work and causes link to become inactive. For example; changing the speed to 100MB does not work. The interface settings change option is disabled for all 1G ports similar to the 10G ports as it is not supported on the 4100-SE bare metal platform.

**SD-WAN 4000 WANOP and 4000 SE**
- Issue ID 679121: While upgrading SD-WAN 4000 appliance from old releases to 9.2 release, the SD-WAN GUI appears before the upgrade process is completed. The old image is listed in the GUI.
- Issue ID 680825: On a NetScaler SD-WAN 4000 appliance with release version 9.2, the HTTP service does not work for one of the SD-WAN instances and fails to start or restart the https service.
- Issue ID 681550: On a NetScaler SD-WAN 4000 WANOP appliance, uploading DER encoded certificate for the SSL profile is ignored and no error message is displayed in the web GUI. Only PEM encoded certificates are accepted.
- Issue ID 680778: A configuration audit error occurs in two-box mode deployment when a NetScaler SD-WAN 4000 SE appliance with two interface groups is configured with first interface group having bridged pair with two ethernet interfaces selected, and second interface group is connected to the WANOP appliance. The error occurs when the first interface group is enabled with WCCP listener indicating that multiple ethernet interfaces cannot be enabled with WCCP. When you revert configuration by disabling WCCP on the first interface group and enabling it on the second interface group, the same configuration audit error is displayed even though only one ethernet interface is enabled on the interface group.
  - Workaround: Delete the interface groups and reconfigure them. Do not enable WCCP listener on the bridge pair, enable it on the interface group that has single one-arm interface with the external WANOP appliance in the WCCP mode.

**Two Box Mode**
- Issue ID 680110: WCCP convergence fails after the SD-WAN SE appliance is restarted in a two box deployment mode. On the SD-WAN WANOP appliance, the following status is displayed - *No response from router.*
  - Workaround: Re-enable Virtual WAN service on the SD-WAN SE appliance.
- Issue ID 681680: After a factory reset on the SD-WAN SE appliance in a two box mode, configuration sync between SD-WAN WANOP and SD-WAN SE appliances fails due to stale SSL certificates.
  - Workaround: Disable and re-enable two box mode on the SD-WAN WANOP appliance.

**SD-WAN 2000**
- Issue ID 681663: When you upgrade SD-WAN 2000 appliance from release build version 9.2.1.26 to 9.2.0.147, a warning is displayed in the browser.
  - Workaround: Perform the upgrade in an in-cognitive window of the browser.

**TCP Fragmented traffic**
- Issue ID 681472: Virtual WAN drops TCP Fragmented traffic when firewall connection tracking is enabled.
WAN GRE Tunnel

- Issue ID 681171: The GRE tunnel packets are not reassembled if they get fragmented on a NetScaler SD-WAN 2000 appliance.

NTP Server Time Settings

- Issue ID 680987: On NetScaler SD-WAN 2000 appliances, when you change the NTP server settings, the Standard Edition appliance time settings sync up with the new NTP server time settings and the correct time zone format is displayed. However, the new NTP server time settings on a WANOP appliance are not synchronized with the new NTP server time settings.
  - Workaround: Restart the appliance.

SSL Profile Name

- Issue ID 681482: In a NetScaler SD-WAN VPX appliance setup, when you create an SSL profile and try to edit the profile and save it, the following error message is displayed: “No object with profile name exists”.

IPSec Tunnel Configuration

- Issue ID 681121: On a NetScaler SD-WAN VPX appliance, a web GUI error is displayed and configuration fails when you try to add and configure IPSec tunnel through the SD-WAN configuration editor.
  - Workaround: Configure IKE and IPsec parameters except protected networks and save the configuration. Edit the configuration to add protected networks.

Enterprise Edition as MCN – SSL Profile

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

Simplified Configuration

- Issue ID 678342: In the SD-WAN configuration editor, secondary level confirmation is not provided when deleting a WAN Link, Interface Group, or Static Route from the Basics view.

SSL Profile page

- Issue ID 681443: When creating or editing an SSL profile, the settings are saved but the application does not redirect to the SSL Profile home page.
  - Workaround: After creating or editing an SSL profile, click the CLOSE or the BACK tab.

Ethernet Interfaces Configuration

- Issue ID 680585: In a NetScaler SD-WAN Standard Edition appliance web GUI, the Basic View under Configuration Editor allows you to create Interface without selecting ethernet interfaces. The created interface is displayed in the Advanced View as VLAN 0 instead of displaying in the Basic View.

Diagnostic tool

- Issue ID 680251: In a NetScaler SD-WAN VPX appliance setup, multiple IPREF client TCP sessions are initiated while
server session is still on causing the server to display additional entries even when the client has stopped sending any further traffic.

Rules Group Tab

- Issue ID 681562: The Rule group tab in SD-WAN Center report page does not show any data for the configured applications.

DPI - ICMP Functionality

- Issue ID 677356: A firewall policy for blocking ICMP as an application blocks only pings (echo requests). All other ICMP types are allowed to pass through.
  - Workaround: Instead of blocking ICMP as an application, block IP-protocol > ICMP.

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

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

DPI- No audit error on disabling DPI

- Issue ID 681175: If an application object created with DPI application is associated to a firewall policy template, and is used in firewall and then if the DPI is disabled, there is no audit error message displayed indicating that there are rules still associated with firewall as the firewall is still functional.

DPI - Traffic classified as unknown when the traffic flows through EE appliances

- Issue ID 677504: Applications are classified as Unknown protocol when the traffic flows through EE appliances, because the compressed traffic is not classified. Therefore, the Firewall rules do not work on EE appliance with DPI enabled when rules are configured with Application, Application Family or Application Object firewall policies. This issue occurs only when a WANOP Service Class Compression policy is configured on a Standard Edition/Enterprise Edition or Standard Edition/Standard Edition appliance with a WANOP deployment mode.

DPI – GRE Keepalive classification

- Issue ID 680994: On a NetScaler SD-WAN 2000 appliance, configure GRE tunnel through Internet service, enable Keepalive option for the GRE Tunnel, and activate the configuration. When you check the GRE Tunnel configuration, the GRE Keepalive packets are not classified properly by DPI. The application is not classified and the family is classified as WEB.

DPI – XenDesktop 7.12/EDT VDAs sessions shows traffic for Top App Family as “Standard” and Top App as “Unknown Virtual protocol” for a Standard Edition appliance

- Issue IDs – 678373, 678339, 678545, 675063, 676017

On a NetScaler SD-WAN Standard Edition appliance, enable EDT policy for MSI+MP for Win7 and Win2K12 XD 7.12 VDAs on ports 2598, 2599, 2600, 2601 and subsequently disable Session Reliability policy for Win7 VDA. Start sending internet traffic and check the monitoring flows in the Standard-Edition web management interface for Classes, Rule groups – ICAUDP and ICACGPUDP, and Firewall. Check the Dashboard and Reporting page in SD-WAN
Center web management interface. The results display Top Application Family as Standard and Top Applications as Unknown Virtual Protocol.

**GUI**

- Issue ID 681649: Unable to enable DHCP Server and Relay for management from the UI. On selecting **Enable DHCP Server**, the fields **Lease Time, Domain Name, Start IP Address** and **End IP Address** should be editable, but these fields are not editable.

---

**Limitations**

**DPI Classification**

- DPI Classification will not classify compressed traffic. This happens on any deployment which has two box (SD-WAN SE/WANOP) solution or an Enterprise Edition appliance where WANOP is optimizing the traffic through MBC/DBC as acceleration policy and the traffic is received as compressed traffic.
- Enabling DPI functionality may affect the system performance.

**SD-WAN Center and Diagnostic Tool**

- SD-WAN web GUI Diagnostic tool will not be supported on UNTRUSTED links and Dynamic Virtual Paths.
- In the SD-WAN Center Reporting page, the Application name, Application Family, and Site filter do not contain scrollable search drop-down menu.

**Microsoft Azure**

- A VM in Azure can have Public IP on only one interface. This VM needs to be on the WAN link to establish Virtual Path. Management is accessed over Private network. While configuring SD-WAN SE-VPX, network interfaces have to added in following order:
  
  a) WAN interface (Private IP, Public IP)
  
  b) LAN interface (Private IP)
  
  c) Management interface (Private IP)

- After a VM is created and booted in Azure, the interfaces cannot be added or deleted. The VM profile (RAM/HD/CPUs) can be changed.
- Azure does not allow two network interfaces NIC on a VM to have IP address on same subnet. There is no L2 Support and bridging is not allowed. SE-VPX on Azure has to be deployed in Gateway mode.
- There is no concept of MAC address spoofing in Azure Cloud. The LAN subnet of the SE-VPX and the LAN subnet of the Client/Server Host have to be different. This will require additional routing configuration to be done in two places.
  
  – User Defined Routes (UDR) have to be added in Azure directing all Virtual WAN Data traffic from the Client/Server LAN Subnet to the LAN interface of the SE-VPX in Azure.
  
  – Routes have to be added in the Virtual WAN Configuration File directing all Virtual WAN Data traffic coming from the WAN to the Client/Server LAN Subnet.

- PCI Enumeration causes the order of NICs in an Azure VM to get switched on reboots. This might cause Management Subnet unreachable.
NetScaler SD-WAN 9.1.2 Release Notes

Jan 17, 2017

These release notes describe the new features, enhancements, known issues, and fixed issues applicable to Citrix NetScaler SD-WAN software release 9.1.2. The list of known issues is cumulative, that is, it includes issues that are newly found in this release and also issues from previous releases.

### Note
- This release note document does not include security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin.
- The [# XXXXXX] labels for issue descriptions are internal tracking IDs used by the SD-WAN support team.

### Enhancements

- **OSPF routing enhancements**
  - SD-WAN OSPF routes can now be advertised as Intra-area routes (Type 5 or Type 1) to participate in OSPF path selection as per it's route cost set. This prevents complex PBR configurations when deploying SD-WAN in one-arm and non-Citrix networks.
- **Support for WAN Edge HA (Serial HA)**

### Fixed Issues

#### New Hardware Platform - Configuration

- **Issue ID 667650**: Configuration of 410-SE appliance through default management IP address is not supported.
  - When you reset a new factory-shipped 410-SE appliance to the factory configuration, it acquires a default DHCP IP address. If you connect the appliance's management port to another device for example; laptop and attempt to use the default static IP address (192.168.100.1) to configure the appliance, the IP address of the appliance is lost.
- **Issue ID 668128**: Default IP address is lost when applying local change management with no assigned DHCP IP address on the 410-SE appliance.
  - If you reset a factory-shipped 410-SE appliance to it's factory configuration, the appliance acquires a default DHCP IP address. If you then remove the appliance from the DHCP network and restart it, it acquires the default IP address (192.168.100.1). Typically, you connect the appliance's management port to another device for example; laptop and use the default static IP address (192.168.100.1) to access the web management interface and install the license. When you then apply Local Change Management, click Activate and click Done, the appliance's default IP address is lost. It also no longer has the DHCP IP address because it was removed from DHCP network.

#### Licensing

- **Issue ID 666146**: SD-WAN WANOP License page might not refresh when Local License file is uploaded.

#### Diagnostics - NetScaler SD-WAN WANOP 4000 and 5000

- **Issue ID 668321**: On NetScaler SD-WAN WANOP 4000 or 5000 appliances, the Erase All Files option on the Diagnostics page of the GUI does not work.
  - In the SD-WAN WANOP GUI, under Configuration > Diagnostics > Diagnostics Files, the Erase All Files option does not erase/delete/remove all the Diagnostics files.

#### Incorrect CLI output for Connection Idle Timeout

- **Issue ID 671169**: Discrepancy between CLI output and GUI display for Connection Idle Timeout parameter.
  - The show-config-script command output displays the Connection Idle Timeout parameter as disabled even when it is Enabled in the GUI and vice-versa.
  - **Workaround**: None

### Known Issues

#### NetScaler SD-WAN VPX software downgrade failure from release 9.1.2 to 9.1.0

- **Issue ID 662369**: Software downgrade from release 9.1.2 to 9.1.0 fails on SD-WAN VPX appliances.
  - Downgrading software version from 9.1.2 to 9.1.0 on NetScaler SD-WAN VPX appliances in XenServer, VMWare ESXi, and AWS environments fail. All SD-WAN services are disabled and both GUI and CLI become unresponsive.
  - **Workaround**: None

#### NetScaler SD-WAN WANOP VPX web management interface

- **Issue ID 629687**: Unable to access the GUI on SD-WAN WANOP VPX appliance
  - After you import and configure the two apx NetScaler SD-WAN WANOP VPX adapters with DHCP IP address from the VPX console, and then shut down and restart the VPX, the NetScaler SD-WAN WANOP VPX appliance is restarted and you can navigate to the Network adapters page in the GUI. Configure the primary adapter IP address in the GUI and reboot the appliance as prompted. Now, you cannot access the GUI using the primary adapter configuration.
  - **Workaround**: Configure the primary adapter IP address in the CLI and enable web management. Reboot the appliance as prompted. You can access the GUI without any issues.

Routing-OSPF Link-State Advertisement (LSA) ID Collision
Issue ID 671213: LSA ID collisions are observed in OSPF Type-1 deployment

A NetScaler SD-WAN appliance does not support OSPF Type-1 LSAs when deployed as an Area Border Router (ABR) in OSPF Type-1 Intra Area stub-networks.

NetScaler SD-WAN 2000 Enterprise Edition (WANOP service) - DHCP and Static IP address warning message

Issue ID 671528: When a NetScaler SD-WAN 2000 EE appliance is in factory default state, the appliance acquires both DHCP IP address and static IP address. The following warning message is displayed when you access the web management interface with the default static IP address (192.168.100.1). This appliance has both DHCP IP address (162.198.10.10/24) and factory default IP address (192.168.100.1/24). If you want to use static IP address, it is required to update your management network IP address settings before proceeding with any other configuration steps. If you disable WAN Optimization on this SD-WAN 2000 EE appliance and apply configuration from the Local Change Management and Activate it, the web management interface displays the previous warning message instead of the following warning message: Failed to apply configuration on for WAN OP service. This warning message is overwritten by the previous warning message.

Workaround: None

NetScaler SD-WAN 5100 SE and 2000 SE gateway IP address is not updated even after moving the appliance to another DHCP network

Issue 671131: The NetScaler SD-WAN 5100 SE and 2000 SE appliances acquire DHCP IP address from the DHCP server in which they are configured. When you configure the appliances in another network with a different DHCP server, the appliances acquire the DHCP IP address from the newly configured DHCP server. However, the gateway IP address of the appliances is not changed and still shows the gateway IP address from the previously configured DHCP network. This issue does not occur with DNS configuration.

Workaround: Reboot the appliances to obtain the correct gateway IP address and DHCP IP address from the configured DHCP network.

SSL Secure Peering not established between 4000/5000 appliances configured at the branch site and data center

Issue 665823: After you provision SSL secure tunnel configuration and instances on the 4000 and 5000 appliances with factory image version 9.1.2, the following message is displayed on the appliances configured at the branch site: unable to activate signalling listener for the following IP/TCP ports.

Workaround: Reboot the appliance for secure peering functionality to work.
NetScaler SD-WAN 9.1.1 Release Notes

Dec 19, 2016

These release notes describe the new features, enhancements, known issues, and fixed issues applicable to Citrix NetScaler SD-WAN software release 9.1.1. The list of known issues is cumulative, that is, it includes issues that are newly found in this release and also issues from previous releases.

Note

- This release note document does not include security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin.
- The [# XXXXXX] labels for issue descriptions are internal tracking IDs used by the SD-WAN support team.

What's New

The following new features and enhancements were introduced in NetScaler SD-WAN for Release 9.1.1.

Support for new Standard Edition appliance; 410-SE. 410-SE is a small, affordable 1U appliance suitable for smaller branch offices. It supports WAN speeds of up to 150 Mbps.

For more information, see the SD-WAN 400 and 410 Standard Edition hardware documentation.

Support for 300 Mbps SKU on 2000-SE appliance.

SNMP MIBs

ENH0655072 - Support for adding enterprise MIB object to provide Service Uptime and Appliance Uptime information (values).

Fixed Issues

**OSPF Neighbor relationship traffic does not pass through the NetScaler SD-WAN 4000 appliance**

- Issue ID: 604657 - The multicast packets used for creating OSPF neighbor relationship between routers are not observed when Virtual WAN service is enabled on SD-WAN 4000 appliance, but is working fine on the 2000 and VPX appliances.

  Workaround: None
Known Issues

New Hardware Platform - Configuration

- Issue ID 667650: Configuration of 410-SE appliance through default management IP address is not supported.

  When you reset a new factory-shipped 410-SE appliance to the factory configuration, it acquires a default DHCP IP address. If you connect the appliance's management port to another device for example; laptop and attempt to use the default static IP address (192.168.100.1) to configure the appliance, the IP address of the appliance is lost.

  Workaround: Use the acquired default DHCP IP address for configuration or use the serial console.

- Issue ID 668128: Default IP address is lost when applying local change management with no assigned DHCP IP address on the 410-SE appliance.

  If you reset a factory-shipped 410-SE appliance to its factory configuration, the appliance acquires a default DHCP IP address. If you then remove the appliance from the DHCP network and restart it, it acquires the default IP address (192.168.100.1). Typically, you connect the appliance's management port to another device for example; laptop and use the default static IP address (192.168.100.1) to access the web management interface and install the license. When you then apply Local Change Management, click **Activate** and click **Done**, the appliance's default IP address is lost. It also no longer has the DHCP IP address because it was removed from DHCP network.

  Workaround: Reboot the appliance or use the serial console.

Licensing

- Issue ID 666146: SD-WAN WANOP License page might not refresh when Local License file is uploaded.

  Workaround: Wait for a few seconds, and then refresh the page or navigate to a different node and then click on the Licensing page again.

Diagnostics - NetScaler SD-WAN WANOP 4000 and 5000

- Issue ID 668321: On NetScaler SD-WAN WANOP 4000 or 5000 appliances, the Erase All Files option on the Diagnostics page of the GUI does not work.

  In the SD-WAN WANOP GUI, under **Configuration > Diagnostics > Diagnostics Files**, the **Erase All Files** option does not erase/delete/remove all the Diagnostics files.

  Expected Behavior: All diagnostic files should be removed when you click **Erase All Files**.

  Workaround: Use the **Erase** button to delete individual files.
NetScaler SD-WAN 9.2.1 Release Notes

Sep 25, 2017

This release notes describes the fixed issues, known issues, and limitations applicable to Citrix NetScaler SD-WAN software release 9.2.1 for the SD-WAN Standard Edition, WANOP, and Enterprise Edition appliances.

Note

- This release note document includes a security related fix (CTX225990). For complete list of security related fixes and advisories, see the Citrix security bulletin.
- The [# XXXXX] labels for issue descriptions are internal tracking IDs used by the SD-WAN support team.

What’s New in Release 9.2.1 (build 1002)

The following new features and enhancements were introduced in NetScaler SD-WAN Release 9.2.1 build 1002:

NetScaler SD-WAN release 9.2.1, build 1002 has new images with security fix for CVE-2017-14602.

This vulnerability is only present when the above versions are used on the following appliance models:

- Citrix NetScaler SD-WAN model 5100 WAN Optimization appliances
- Citrix NetScaler SD-WAN (CloudBridge) model 5000 WAN Optimization appliances
- Citrix NetScaler SD-WAN model 4100 WAN Optimization appliances
- Citrix NetScaler SD-WAN (CloudBridge) model 4000 WAN Optimization appliances

For additional information related to this security fix, impacted editions, and platforms, refer to the security bulletin posted at https://support.citrix.com/article/CTX228091.

Best practices for use of WAN Optimization products are now available at: Read more

Fixed Issues

SD-WAN 4000 WANOP and 4000 SE

- Issue ID 680778: A configuration audit error occurs in two-box mode deployment when a NetScaler SD-WAN 4000 SE appliance with two interface groups is configured with first interface group having bridged pair with two ethernet interfaces selected, and second interface group is connected to the WANOP appliance. The error occurs when the first interface group is enabled with WCCP listener indicating that multiple ethernet interfaces cannot be enabled with WCCP. When you revert configuration by disabling WCCP on the first interface group and enabling it on the second interface group, the same configuration audit error is displayed even though only one ethernet interface is enabled on the interface group.

- Issue ID 680825: On a NetScaler SD-WAN 4000 appliance with release version 9.2, the HTTP service does not work for one of the SD-WAN instances and fails to start or restart the HTTPS service.

- Issue ID 679121: While upgrading SD-WAN 4000 appliance from old releases to 9.2 release, the SD-WAN GUI appears before the upgrade process is completed. The old image is listed in the GUI.
SD-WAN 4100 SE

- Issue ID 675715: On a NetScaler SD-WAN 4100 SE appliance, changing interface settings for 1G interface does not work and causes link to become inactive. For example; changing the speed to 100MB does not work. The interface settings change option is disabled for all 1G ports similar to the 10G ports as it is not supported on the 4100-SE bare metal platform.

TCP Fragmented traffic

- Issue ID 681472: Virtual WAN drops TCP Fragmented traffic when firewall connection tracking is enabled.

NTP Server Time Settings

- Issue ID 680987: On NetScaler SD-WAN 2000 appliances, when you change the NTP server settings, the Enterprise Edition appliance time settings sync up with the new NTP server time settings and the correct time zone format is displayed. However, the new NTP server time settings on a WANOP appliance are not synchronized with the new NTP server time settings.

Diagnostic tool

- Issue ID 680251: In a NetScaler SD-WAN VPX appliance setup, multiple IPREF client TCP sessions are initiated while server session is still on causing the server to display additional entries even when the client has stopped sending any further traffic.

Rules Group Tab

- Issue ID 681562: The Rule group tab in SD-WAN Center report page does not show any data for the configured applications.

DPI- No audit error on disabling DPI

- Issue ID 681175: If an application object created with DPI application is associated to a firewall policy template, and is used in firewall and then if the DPI is disabled, there is no audit error message displayed indicating that there are rules still associated with firewall as the firewall is still functional.

SSL Profile Name

- Issue ID 681482: In a NetScaler SD-WAN VPX appliance setup, when you create an SSL profile and try to edit the profile and save it, the following error message is displayed: “No object with profile name exists”.

SSL Profile Page

- Issue ID 681443: When creating or editing an SSL profile, the settings are saved but the application does not redirected to the SSL Profile home page.

GUI

- Issue ID 681649: Unable to enable DHCP Server and Relay for management from the UI. On selecting Enable DHCP Server, the fields Lease Time, Domain Name, Start IP Address and End IP Address should be editable, but these fields are not editable.

Security Vulnerability

- Issue ID 690709: Unauthenticated remote code execution on the NetScaler SD-WAN Enterprise Edition and Standard
Known Issues

SD-WAN 4000 WANOP and 4000 SE

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

Two Box Mode

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

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

SD-WAN 1000 / 2000

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

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

SD-WAN WANOP

- Issue ID 675452: NetScaler SD-WAN WANOP client info displays OS version as Windows 8 even when plugin is installed in Windows 10 OS.

SD-WAN GUI

- Issue ID 683520: In the SD-WAN GUI, changing the interface settings for interface under Configuration > Appliance Settings > Network adapters > Ethernet does not work for the SD-WAN 1000-EE, 2000-EE and 400-SE platforms.

WAN GRE Tunnel

- Issue ID 681171: Fragmented GRE tunnel packets are not reassembled properly by a NetScaler SD-WAN appliance.

IPSec Tunnel Configuration

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

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

Enterprise Edition as MCN – SSL Profile

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

### Simplified Configuration

- **Issue ID 678342:** In the SD-WAN configuration editor, secondary level confirmation is not provided when deleting a WAN Link, Interface Group, or Static Route from the Basics view.

### Ethernet Interfaces Configuration

- **Issue ID 680585:** In a NetScaler SD-WAN Standard Edition appliance web GUI, the Basic View under Configuration Editor allows you to create Interface without selecting ethernet interfaces. The created interface is displayed in the Advanced View as VLAN 0 instead of displaying in the Basic View.

### Configuration and Reporting

- **Issue ID 683882:** Audit errors are reported when you create more than one Service Class on an SD-WAN appliance with override options. This issue occurs only when you perform override for service class and create more than one service class. It is not observed when you create only one Service Class under the default section.

### DPI - ICMP Functionality

- **Issue ID 677356:** A firewall policy for blocking ICMP as an application blocks only pings (echo requests). All other ICMP types are allowed to pass through.
  
  **Workaround:** Instead of blocking ICMP as an application, block IP-protocol > ICMP.

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

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

### DPI - Traffic classified as unknown when the traffic flows through EE appliances

- **Issue ID 677504:** Applications are classified as Unknown protocol when the traffic flows through EE appliances, because the compressed traffic is not classified. Therefore, the Firewall rules do not work on EE appliance with DPI enabled when rules are configured with Application, Application Family or Application Object firewall policies. This issue occurs only when a WANOP Service Class Compression policy is configured on a Standard Edition/Enterprise Edition or Standard Edition/Standard Edition appliance with a WANOP deployment mode.

### DPI – Any application traffic sent via GRE Tunnel is reported as GRE in SD-WAN Center

- **Issue ID 680994:** Ideally, any application traffic (example HTTP) sent through the GRE tunnel should be classified by DPI reported as both GRE and the real application traffic (example HTTP) in the Application section of Reporting page in SD-WAN Center. Due to this bug, the real application (example HTTP) is also reported as GRE traffic. This bug is only a reporting issue and the real classification has no issues in the site level DPI. Both the classification and firewall actions after DPI will have no impact in any site.

### DPI – Traffic for Top App Family as "Standard" and Top App as "Unknown Virtual protocol" for a Standard Edition appliance
• Issue IDs 678373, 678339, 678545, 675063, 676017: On a NetScaler SD-WAN Standard Edition appliance, enable EDT policy for MSI+MP for Win7 and Win2K12 XD 7.12 VDAs on ports 2598, 2599, 2600, 2601 and subsequently disable Session Reliability policy for Win7 VDA.

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

SD-WAN Center – GUI Error
• Issue ID 683419: In the SD-WAN Center, read-only user login access generates the following GUI error:
  Error in retrieving top applications.

Limitations

DPI Classification
• DPI Classification will not classify compressed traffic. This happens on any deployment which has two box (SD-WAN SE/WANOP) solution or an Enterprise Edition appliance where WANOP is optimizing the traffic through MBC/DBC as acceleration policy and the traffic is received as compressed traffic.
• Enabling DPI functionality may affect the system performance.

SD-WAN Center and Diagnostic Tool
• SD-WAN web GUI Diagnostic tool will not be supported on UNTRUSTED links and Dynamic Virtual Paths.
• In the SD-WAN Center Reporting page, the Application name, Application Family, and Site filter do not contain scrollable search drop-down menu.

Microsoft Azure
• A VM in Azure can have Public IP on only one interface. This VM needs to be on the WAN link to establish Virtual Path. Management is accessed over Private network. While configuring SD-WAN SE-VPX, network interfaces have to added in following order:
  a)    WAN interface (Private IP, Public IP)
  b)    LAN interface (Private IP)
  c)     Management interface (Private IP)
• After a VM is created and booted in Azure, the interfaces cannot be added or deleted. The VM profile (RAM/HD/CPUs) can be changed.
• Azure does not allow two network interfaces NIC on a VM to have IP address on same subnet. There is no L2 Support and bridging is not allowed. SE-VPX on Azure has to be deployed in Gateway mode.
• There is no concept of MAC address spoofing in Azure Cloud. The LAN subnet of the SE-VPX and the LAN subnet of the Client/Server Host have to be different. This will require additional routing configuration to be done in two places.
  – User Defined Routes (UDR) have to be added in Azure directing all Virtual WAN Data traffic from the Client/Server LAN Subnet to the LAN interface of the SD-WAN SE-VPX in Azure.
- Routes have to be added in the Virtual WAN Configuration File directing all Virtual WAN Data traffic coming from the WAN to the Client/Server LAN Subnet.

- PCI Enumeration causes the order of NICs in an Azure VM to get switched on reboots. This might cause Management Subnet unreachability.
What's New

Oct 27, 2016

Release 9.2

The following new features and enhancements were introduced in NetScaler SD-WAN Standard Edition, WANOP, and Enterprise Edition appliances for Release 9.2.

Application classification usage for firewall

- Support for an integrated DPI library that provides Deep Packet Inspection (DPI) technology for real-time classification of packets. Using the DPI technology, the SD-WAN appliance analyzes the incoming packet and classifies it as belonging to a particular application or application family.

- Once a packet is classified, the application identifier can be used either on the rule or firewall filter as a possible match criterion to handle this type of traffic.

Application visibility in SD-WAN Center

- You can now view the top applications and top application families used at the different sites in your network in the SD-WAN Center dashboard. You can view details about incoming traffic, outgoing traffic and total traffic of the top applications, sites, and application families as reports. This provides a holistic view of your network bandwidth usage.

- Deep packet inspection (DPI) allows the SD-WAN appliance to parse the traffic passing through it and identify the application and application family types. The number of bytes of incoming and outgoing traffic of every application is recorded and is stored in the SD-WAN appliance. The SD-WAN Center polls the SD-WAN appliance as per the defined polling interval, obtains this data, and displays it in the dashboard and as reports.

Diagnostic tool - A new inbuilt traffic generator is introduced in SD-WAN 9.2. This diagnostic tool is used to generate test traffic which allows you to troubleshoot network issues that may result in:

- Frequent change in path state from Good to Bad.
- Poor application performance.
- Higher packet loss

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 you to generate the following two types of traffic:

- Control: Eliminates SD-WAN processing such as SD-WAN QoS/ Schedulers, optimization and so on, on the diagnostic traffic. This is used to identify SD-WAN related issues.

- Data: Simulates the traffic generated from the host with SD-WAN traffic processing. This is used to identify issues
related to ISP/ customer gateway devices and so on.

**Virtual Routing and Forwarding (VRF)**

- Firewall segmentation

Introduces VRF Firewall segmentation to allow multiple routing domains each having access to the Internet. Each routing domain is associated with a different user group, for example, employee or guests, while keeping the traffic from each isolated group. This feature allows each Routing Domain (user group) access to the Internet through a common Access Interface.

This provides the following capability:

- 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 per Routing Domain, if required.
- When enabled, this feature applies to all Routing Domains.

**Dynamic Routing - BGP Enhancements**

- Configure neighbour/peer router AS number (iBGP / eBGP).
- Create BGP Policies to be applied selectively to a set of networks per neighbour in either direction (import/export). SD-WAN appliances will support eight policies per site and total of 8 network objects (or 8 networks) tied to a policy.
- For each policy, users can configure multiple community strings, prepend AS path, MED attribute. Users can configure up to 10 attributes for each policy.

**Non-Virtual Path route eligibility for IPSec**

- IPsec non-virtual path Routes are now considered ineligible when the IPsec tunnel is no longer available.

**Adaptive Bandwidth Detection**

- Allows the NetScaler SD-WAN appliances to adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range (minimum and maximum WAN link rate) to use the maximum amount of available bandwidth without marking the paths bad.
  - Greater bandwidth reliability (Over VSAT, Microwave, 3G/4G, and LTE)
  - Greater predictability of adaptive bandwidth over user configured settings
  - 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.

**SD-WAN EE and SE appliance in hair pin deployment mode**
With the hairpin deployment, you can implement use of Remote Hub site for Internet Access through backhaul or hairpin when local internet services are unavailable or are experiencing a slow traffic. You can leverage high bandwidth routing between client sites by allowing for selected backhauling (from specific sites).

Stateful Firewall and NAT Support

- This features 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.

DHCP Relay and Server management

Devices on the same network as the SD-WAN appliance's LAN/WAN interface can now use the SD-WAN DHCP Relay & DHCP Server features to provide those devices with their IP configuration. These features help to simplify the client site network by reducing the amount of equipment necessary.

- Reduce equipment at client site
- Replace router at client site (Easy deployment of edge router services)
- Simplify the client site network
- Configuration of Router without CLI commands
- Use of Dynamic Host Configuration Protocol (DHCP) on Internet Protocol (IP) networks to request IP addresses and networking parameters automatically reducing manual configuration needs by network admin on simple client sites

WAN Link configuration with templates

- In NetScaler SD-WAN 9.2, new customers with five or more basic sites configuring for the first time will save time when setting up new sites and WAN Links. With the use of templates, you can configure certain settings one-time and then duplicate the settings across more than one site as required. This functionality is implemented in two ways. First, the ability to create and administer WAN Link templates. Second a tab, which simplifies the setup of basic sites. Each of these is accessed through the Basic tab. Under the Basic tab, you have the Network option used for WAN Link templates and the Site option, which simplifies the configuration process for a site.

MCN scalability for up to 550 nodes

- NetScaler SD-WAN supports the ability for SD-WAN appliance functioning as an MCN to create up to 550 static virtual paths with full support for all previously existing features, including up to 16,000 Routes. You can now configure up to 23,000 WAN Paths, 11,000 WAN Links, 512,000 Flows, and 200,000 Rules. This feature is for users with SAML knowledge, and fundamental authentication proficiency is required to use this information.

SNMPv3 polling and trap

- SD-WAN only supports a single user account for each SNMPv3 capability. This capability provides the following advantages:
  - Ensure SNMPv3 compliance for network devices
  - Verification of SNMPv3 capability
  - Easy configuration of SNMPv3

Easy 1st Install – Simplified Appliance Installation
NetScaler SD-WAN appliances deployed into new sites and RMA replacement appliances deployed into existing site can now be configured with ease. A new SD-WAN network can now be connected and powered on by a non-technical person. A Network Administrator can add a new site, configure it at the MCN, and upload the software and configuration package to a Citrix Support and Cloud registration server (https://support.citrix.com). This registration server will reside in the cloud. The client appliance is then installed and acquires an IP address from DHCP. Once the client appliance has a valid IP address it will contact the registration server, and based on its serial number, download the corresponding package. Once the package is downloaded, it is activated automatically and the site becomes operational.

Configuring Service Class Association with SSL Profile

All SSL related configuration is available through the new configuration editor of the appliance for security and usability. On the SD-WAN Enterprise Edition and two-box deployments, service classes are configured from the configuration editor and hence you cannot attach any SSL profiles. To accommodate the expression of SSL profile mapping to a service class, the workflow for SSL profiles is changed to allow for attaching Service classes in the profile node. One of the limitations is that the SSL profile will get attached to all rules in a service class. If you need to attach the SSL profile selectively to a particular rule, the service class configuration is split into detailed rules for further selection.

Virtual WAN IPsec for FIPS Compliant Operation

IPSec security setting enhancements are introduced with addition of DH groups and random number generator functionality for compliance with Federal Standards.

IPSec Null Encryption

In SD-WAN 9.2 release, the tunnel type ESP+NULL is introduced. When using IPsec ESP protocol, traffic is typically encrypted and authenticated. However, you can choose not to use encryption by using Null encryption. In ESP + NULL tunnel type the packets are authenticated but not encrypted.

SD-WAN-SE VPX in Microsoft Azure

NetScaler SD-WAN Standard Edition for Microsoft Azure logically bonds multiple network links into a single secure virtual path. The solution enables organizations to leverage variety of connections from different service providers including Broadband, MPLS, 4G/LTE, Satellite, and point-to-point links to get high resiliency virtual WAN paths. These virtual paths seamlessly aggregate bandwidth capacities across multiple links and deliver consistent user experience even if some of the member links go down or suffer degradation. This is enabled by the per-packet load balancing and monitoring capabilities of NetScaler SD-WAN. NetScaler SD-WAN for Azure enables organizations to have direct high quality secure connection from each branch to the applications hosted in Azure eliminating the need to backhaul cloud-bound traffic through a data center.

Higher capacity (200Mbps/1Gbps) VPX for Azure, AWS, and ESXi

This feature describes the support for a virtualized appliance to bond multiple WAN links at the branch office. This is required in the case where virtualized appliances can be supported on existing branch routers or other open compute environments. To address this need, the following NetScaler SD-WAN VPX (WANOP and SE) appliances are supported on: Azure, AWS, XenServer, ESXi, and Hyper-V.
Introducing SD-WAN 2100-SE edition appliance with ZTD

Introducing SD-WAN 4100-SE edition appliance

Auto Secure Peering – Enterprise Edition appliance as MCN

- Enterprise Edition appliance can be installed at the data center and now has the capability to join the appliance to a Windows Domain Controller for allowing users/administrator to make use of the extended rich feature of standalone WANOP appliance.

For more information about each of these supported features, refer to the topics listed on the left navigation panel.
There are three NetScaler SD-WAN Editions each with a different set or subset of NetScaler SD-WAN features. The type of license you install determines the NetScaler SD-WAN Standard Edition, WANOP, and Enterprise Edition appliances.

**Note**
When installing and applying a license, make sure that your specific appliance supports the NetScaler SD-WAN Edition you want to enable, and that you have the correct software version in place.

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>R.7.X</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>R.8.X</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>R.9.0</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>R.9.1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>R.9.2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

NetScaler SD-WAN 9.2 introduced a new set of licenses specific to the SD-WAN solution. Earlier versions of licenses, including those compatible with release 7.x, are not supported with the NetScaler SD-WAN release. The existing process to obtain NetScaler SD-WAN licenses remains consistent with the CloudBridge 8.0.x, and 9.0.x releases. Once obtained, the licenses can be activated through the appliance’s management web interface.

The following table lists all the appliance models supported in NetScaler SD-WAN 9.2 release:

<table>
<thead>
<tr>
<th>Platform Edition</th>
<th>License Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Edition VPX</td>
<td>VPX-020-SE, 050-SE, 100-SE, 200-SE, 500-SE, 1000-SE</td>
</tr>
<tr>
<td>Standard Edition 1000</td>
<td>1000-020-SE, 1000-050-SE, 1000-100-SE</td>
</tr>
<tr>
<td>WANOP Edition VPX</td>
<td>VPX-2, 6, 10, 20, 50, 100, 200</td>
</tr>
<tr>
<td>WANOP Edition 800</td>
<td>800-002, 800-006, 800-010</td>
</tr>
<tr>
<td>WANOP Edition 1000 Windows Server</td>
<td>1000WS-006, 1000WS-010, 1000WS-020</td>
</tr>
<tr>
<td>WANOP Edition 1000</td>
<td>1000-006, 1000-010, 1000-020</td>
</tr>
<tr>
<td>WANOP Edition 3000</td>
<td>3000-050, 3000-100, 3000-155</td>
</tr>
<tr>
<td>WANOP Edition 4000</td>
<td>4000-310, 4000-500, 4000-1000</td>
</tr>
<tr>
<td>WANOP Edition 5000</td>
<td>5000-1500, 5000-2000</td>
</tr>
<tr>
<td>Enterprise Edition 1000</td>
<td>1000-010-EE, 1000-020-EE, 1000-050-EE, 1000-100-EE</td>
</tr>
</tbody>
</table>

1000-006, 1000-010, 1000-020
1000-006, 1000-010, 1000-020
VPX models allow 2, 6, 10, 20, 50, 100, and 200 Mbps bandwidth licenses. At least two 2.1 GHz CPUs are required in order to support the VPX instances.

Before you can download the software, you must obtain and register a NetScaler SD-WAN software license. For instructions on obtaining a NetScaler SD-WAN software license, please contact Citrix NetScaler SD-WAN Customer Support. Instructions for uploading and installing the license file on your appliances are provided in the section, "Uploading and Installing the SD-WAN Software License File." However, before installing the license, you must first set up the appliance hardware, and set the date and time for the appliance.

To return or reallocate a license, you must use the Citrix NetScaler SD-WAN Licensing Portal. You also have the option to use the Licensing Portal for license allocation. For instructions, see the Knowledge Base article entitled, "My Account All Licensing Tools User Guide," at this location:

http://support.citrix.com/article/ctx131110
Provisioning Licensing

Sep 15, 2016
The license procedure for provisioning licensing for SD-WAN platform editions covers the following topics:

- Supported SD-WAN license model for 9.0, 9.1, and 9.2
- Remote License Server support for SD-WAN VPX-SE appliances
- Pre-requisites for using Remote License Server
- Use Cases
  - Deployment scenarios supported for 9.1 and 9.2
    - Remote License server reachable in Management network (without using data/apA Ports)
    - Remote License server in the Branch network
    - SD-WAN VPX-SE - PBR Deployment in the Branch Office
    - SD-WAN SE - Microsoft Azure
    - Two Box Deployment
    - Hairpin Mode
  - Deployment scenarios not supported for 9.2
    - Remote License server deployed in Data Center (data/apA Ports)
- Import SD-WAN VPX-SE license on XenServer/ESXi 9.2
  - Local License
  - Remote License
License Procedure

Oct 06, 2016
Pre-requisites for using Remote License Server for SD-WAN appliances.

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

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

- Release 9.2: 11.13.1 LS
- Release 9.1: 11.13.1 LS
- Release 9.0: 11.13.1 LS
- Release 8.1: 11.12.1 LS

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

2. Remote license server in the Branch network.

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

Deployment scenarios not supported for 9.2

4. Remote license server deployed in Data Center reachable through the data/apA Ports.
Importing SD-WAN VPX-SE license deployed on XenServer/ESXi:

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

1. In the SD-WAN web management interface, navigate to Configuration > Appliance Settings > Licensing.
2. Select Remote and enter the Remote Server-IP address details.
There are two main upgrade scenarios:

1. Upgrade existing appliances with working Virtual WAN configuration from a previous release version, 8.1, 9.0, 9.1 to the current version 9.2.0.x.

2. Upgrade appliances to release 9.2.0.x without existing Virtual WAN configuration.

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

**Note**

Upgrading to 9.2 release is a multi-step process. Virtual WAN software is upgraded centrally from the MCN appliance using .tar.gz files. Additionally, operating system software needs to be upgraded locally on every hardware appliance in the network using .upg software package file. It is important to complete the second upgrade step locally on every appliance, otherwise some functionality will be missing. Refer to the upgrade instructions in the following sections.
Upgrade to 9.2 With Working Virtual WAN Configuration

May 23, 2017

Note
Upgrading to 9.2 release is a multi-step process. Virtual WAN software is upgraded centrally from the MCN appliance using tar.gz files. Additionally, operating system software needs to be upgraded locally on every hardware appliance in the network using .upg software package file. It is important to complete the second upgrade step locally on every appliance, otherwise some functionality will be missing. Refer to the upgrade instructions in the following sections.

Important
Operating system upgrade process (.upg) is not applicable to the following platform editions:

- 410-SE
- 2100-SE
- 4100-SE

1. Targeted appliances for upgrade to Enterprise Edition (1000-EE or 2000-EE) are required to have:
   - factory image of 9.0.0.x RTM build, if your appliance is WANOP edition which has been converted to Enterprise Edition using USB. See, Convert SD-WAN 1000 or 2000 WANOP to Enterprise Edition with USB.
   - factory image of 8.1.0.x RTM build
2. Have a valid SD-WAN license.
3. Have a working Virtual WAN configuration running 8.1.x or 9.0.x build with virtual paths established from MCN to the branch sites.

1. On the MCN appliance, navigate to Configuration > Virtual WAN > Change Management.
3. Upload the tar.gz file to the Change Management page in SD-WAN web interface for the MCN appliance and complete the change management process.
   a. Click Begin.
b. Click **Choose File** to provide the cb-wv_<APPLIANCE-MODEL>_9.2.0.X.tar.gz file.

c. Click **Upload**. The .tar.gz file is uploaded.

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

e. Once complete, in Appliance Staging, click on **Stage Appliances**.

f. In the Activation page, click on **Activate Staged** and then click **Done**.

---


   a. Navigate to **Configuration > System Maintenance > Update Software > Update Operating System Software**.

   b. Click **Choose File** to provide the **CB-VW-PKG- 9.2.0.X.UPG** file.
c. Click **Upload** and **Upgrade**.

5. Perform operating system software update on the MCN appliance and all other appliances in the network using the **CB-VW-PKG-9.2.0.x.upg** file.

This step may take about 20 minutes to complete. Do not unplug the appliance during this process. Run a continuous ping to the management IP to identify when the box has completed the reboot.

6. Verify that the release version changed to 9.2.0.X on both MCN and branch site, and the Virtual path is established. It might take about few minutes for the licenses to get activated. Refresh the browser, and validate for proper licensing, if you see any anomalies.

### Warning

- On the 1000/2000 appliances, the following warning message appears.

  **Failed to apply configuration on WAN Optimization service. WAN Optimization service could be down or on older software version.** Check whether Update Software Operation is performed with latest software version and WAN Optimization service is up. Re-apply Configuration once these prerequisites are met using Change Management from MCN or Local Change Management on this appliance.

**Workaround:** Check **Configuration > Appliance Settings > Licensing** to verify if license file is present. If the license file is present, reapply the same configuration using the Change Management on the MCN by navigating to **Configuration > Virtual WAN > Change Management > Begin > Next > Stage Appliances > Activate Staged > Done**.

If the license file is not present or available, re-upload the license file to the appliance and then re-apply it.

### Note

- Intermittent SSO session might be timed out, when accessing the **WAN Optimization** node.

  **- Workaround:** Please re-login and continue.
Upgrade to 9.2 Without Virtual WAN Configuration

May 15, 2017

Note
Upgrading to 9.2 release is a multi-step process. Virtual WAN software is upgraded centrally from the MCN appliance using tar.gz files. Additionally, operating system software needs to be upgraded locally on every hardware appliance in the network using .upg software package file. It is important to complete the second upgrade step locally on every appliance, otherwise some functionality will be missing. Refer to the upgrade instructions in the following sections.

Important
Operating system upgrade process (.upg) is not applicable for the following platform editions:

- 410-SE
- 2100-SE
- 4100-SE

Targeted appliances for upgrade to Enterprise Edition (1000-EE or 2000-EE) are required to have:

- factory image of 9.0.0.x RTM build, if your appliance is WANOP edition which has been converted to Enterprise Edition using USB. See, Convert WANOP 1000 or 2000 appliance to Enterprise Edition with USB.
- factory image of 8.10.x RTM build

1. Decide which appliance needs to be MCN.
   a. Promote the appliance as MCN. Navigate to Configuration -> Appliance Settings -> Administrator Interface -> Miscellaneous -> Switch Console.
b. Obtain applicable `cb-vw_<APPLIANCE-MODEL>_9.2.0.X.tar.gz` file for the MCN device. For example, if NetScaler SD-WAN 1000 EE is chosen to be MCN, obtain the `cb-vw_CB1000_9.2.0.X.tar.gz` from the Citrix download page for NetScaler SD-WAN 9.2.0 release.

c. Upgrade this appliance using the `.tar.gz` file through Configuration > System Maintenance > Update Software > Re-image Virtual WAN Appliance software > Click Choose File to provide the `cb-vw_CB1000_9.2.0.X.tar.gz` file.

d. Click Upload. Select Accept, and click Install to proceed.

3. Create a new Virtual WAN Network Configuration file through Configuration > Virtual WAN > Configuration Editor. Export the configuration to Change Management.


5. Obtain applicable cb-vv_<APPLIANCE-MODEL>_9.2.0.X.tar.gz file from Citrix product downloads page at: https://www.citrix.com/downloads/netscaler-sd-wan.html for all sites in the Virtual WAN network defined in the configuration. Upload the tar.gz files to the change management, and complete the Appliance Staging process, but do not Activate the configuration yet.

6. Download the staged package for all the sites from the MCN Change Management. Upload each package to the respective site appliance through Local Change Management, Configuration > System Maintenance > Local Change Management. Activate staged configuration on each site appliance and MCN appliance.

7. Perform operating system software update on the MCN appliance and all other appliances. For non-MCN (branch) appliance, if the appliance model is VPX, then skip this step.
   b. Install the .upg file. Go to System Maintenance > Update Software > Update Operating System Software on both MCN and non-MCN device.
   c. On MCN and non-MCN (branch) appliance, the Update software web interface displays the upgrade status. Do not unplug the appliance during this process. Run a continuous ping to the management IP to identify whether the appliance has completed reboot (ping should fail initially and after 20 minutes, it should succeed).

8. Install the Standard Edition or Enterprise Edition license for each site appliance through Configuration > Appliance Settings > Licensing.


**Warning**

- On the 1000/2000 appliances, the following warning message appears.

  Failed to apply configuration on WAN Optimization service. WAN Optimization service could be down or on older software version. Check whether Update Software Operation is performed with latest software version and WAN Optimization service is up. Re-apply Configuration once these prerequisites are met using Change Management from MCN or Local Change Management on this appliance.

  - workaround: Please reapply the same configuration using the Change Management on the MCN by navigating to Configuration > Virtual WAN > Change Management > Begin > Next > Stage Appliances > Activate Staged > Done.
Convert SD-WAN 1000 / 2000 WANOP Appliances to Enterprise Edition With USB

May 15, 2017

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

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

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

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

How To Convert With USB Stick

To upgrade the appliance with USB stick:

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

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

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

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

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

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

- For licensing about the NetScaler and NetScaler SD-WAN products, see the support link at: http://support.citrix.com/article/ctx1311110
- For Documentation and Release Notes information about NetScaler SD-WAN, see; http://support.citrix.com/proddocs and docs.citrix.com
Converting Existing Appliance to Enterprise Edition Appliance

Jan 03, 2017

You can convert your existing appliance to Standard Edition if the Enterprise Edition license installation fails on the Enterprise Edition 1000 and 2000 appliances:

To perform platform conversion from Standard Edition to Enterprise Edition:

1. Export the Configuration locally.
2. Download the Active Package from the Change Management page.
3. Upgrade the appliance using the downloaded package from System Maintenance -> Update Software -> Re-image Virtual WAN Appliance software.
4. Click Choose File to provide the cb-ww_CB1000_9.10.x.tar.gz file.
5. Click Upload. Select Accept and click on Install to proceed.
7. Perform Local Change Management on the appliance using the downloaded active package in step 2 above.
Before You Begin

This section outlines the hardware and software requirements for deploying Citrix NetScaler SD-WAN Standard and Enterprise Editions, and defines the platform dependencies. Also provided is a summary and overview of the SD-WAN appliance installation and deployment procedures.

For more information, refer to the following topics:

- System Requirements
- Acquiring the Netscaler SD-WAN Software Packages
- NetScaler SD-WAN Software Packages and Appliance Models
- NetScaler SD-WAN Appliance Packages
- Preparing for Your Deployment
- Installation and Configuration Information checklist
System Requirements

Apr 04, 2017

Important

Before proceeding with installing and configuring NetScaler SD-WAN appliances, refer to the product datasheet on the Citrix.com product site at:


Instructions for installing your NetScaler SD-WAN Appliances are provided in Setting up the SD-WAN Appliances.

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

The SD-WAN release requires all appliances on the SD-WAN network to install the same software release. Appliances running earlier CloudBridge software versions will not be able to establish a Virtual Path connection to the appliance running SD-WAN release 9.2.

For details regarding license requirements, see Licensing.

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

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

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

Supported browsers must have cookies enabled, and JavaScript installed and enabled.
Acquiring the NetScaler SD-WAN Software Packages

Apr 04, 2017
This section provides information about downloading the NetScaler SD-WAN software packages.

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

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

To download the NetScaler SD-WAN software packages, go to the following URL:

http://www.citrix.com/downloads.html

Instructions for downloading the software are provided on this site.
NetScaler SD-WAN Software Packages and Appliance Models

May 28, 2017

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

There are two main categories of SD-WAN Appliances:

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

Note

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

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


Citrix NetScaler SD-WAN 9.2 supports the following SD-WAN standard edition hardware appliance models:

<table>
<thead>
<tr>
<th>SD-WAN SE MODEL</th>
<th>ROLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD-WAN 410-SE</td>
<td>Small branch node appliance</td>
</tr>
<tr>
<td>SD-WAN 1000-SE</td>
<td>Large branch node appliance</td>
</tr>
<tr>
<td>SD-WAN 2000-SE</td>
<td>Large branch node appliance</td>
</tr>
<tr>
<td>SD-WAN 2100-SE</td>
<td>Large branch node appliance</td>
</tr>
<tr>
<td>SD-WAN 4100-SE</td>
<td>Data Center Master Control Node (MCN) appliance</td>
</tr>
<tr>
<td>SD-WAN 5100-SE</td>
<td>Data Center Master Control Node (MCN) appliance</td>
</tr>
</tbody>
</table>
Citrix NetScaler SD-WAN 9.2 supports the following SD-WAN WAN Optimization (WANOP) appliance models:

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

Citrix NetScaler SD-WAN 9.2 supports the following SD-WAN VPX Virtual Appliance (VPX-SE) models:
### SD-WAN VPX-SE Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD-WAN VPX 20-SE</td>
<td>MCN or client node, small branch</td>
</tr>
<tr>
<td>SD-WAN VPX 50-SE</td>
<td>MCN or client node, small branch</td>
</tr>
<tr>
<td>SD-WAN VPX 100-SE</td>
<td>MCN or client node, small branch</td>
</tr>
<tr>
<td>SD-WAN VPX 200-SE</td>
<td>MCN or client node, small branch</td>
</tr>
<tr>
<td>SD-WAN VPX 500-SE</td>
<td>MCN or client node, small branch</td>
</tr>
<tr>
<td>SD-WAN VPX 1000-SE</td>
<td>MCN or client node, small branch</td>
</tr>
</tbody>
</table>

For more information, see [About SD-WAN Virtual VPX](https://docs.citrix.com).

Citrix NetScaler SD-WAN 9.2 supports the following SD-WAN WANOP Virtual Appliance (VPX-WANOP) models:

<table>
<thead>
<tr>
<th>Model</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD-WAN WANOP VPX-2</td>
<td>Small branch node</td>
</tr>
<tr>
<td>SD-WAN WANOP VPX-6</td>
<td>Small branch node</td>
</tr>
<tr>
<td>SD-WAN WANOP VPX-10</td>
<td>Small branch node</td>
</tr>
<tr>
<td>SD-WAN WANOP VPX-20</td>
<td>Small branch node</td>
</tr>
<tr>
<td>SD-WAN WANOP VPX-50</td>
<td>Large branch node</td>
</tr>
<tr>
<td>SD-WAN WANOP VPX-100</td>
<td>Large branch node</td>
</tr>
<tr>
<td>SD-WAN WANOP VPX-200</td>
<td>Large branch node</td>
</tr>
</tbody>
</table>

Citrix NetScaler SD-WAN 9.2 supports the following SD-WAN Enterprise Edition appliance (SD-WAN EE) models:

<table>
<thead>
<tr>
<th>Model</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD-WAN 1000-EE</td>
<td>Large branch, Data Center appliance</td>
</tr>
<tr>
<td>SD-WAN 2000-EE</td>
<td>Large branch, Data Center appliance</td>
</tr>
</tbody>
</table>
NetScaler SD-WAN Appliance Packages

Oct 04, 2016

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

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

Oct 04, 2016

It is strongly recommended that before beginning the installation, you first read through the Citrix CloudBridge Virtual WAN Deployment Planning Guide. This article discusses the essential Virtual WAN concepts and features, and provides guidelines for planning your deployment. You can find this document in the CloudBridge documentation section on the Citrix Documentation Portal (http://docs.citrix.com/).

The following list outlines the steps and procedures involved in deploying the NetScaler SD-WAN Standard and Enterprise Editions.

1. Gather your NetScaler SD-WAN deployment information.

2. Set up the NetScaler SD-WAN Appliances.
   
   For each hardware appliance you want to add to your SD-WAN deployment, you must complete the following tasks:
   
   a. Set up the appliance hardware.
   
   b. Set the Management IP Address for the appliance and verify the connection.
   
   c. Set the date and time on the appliance.
   
   d. (Optional) Set the console session **Timeout** interval to a high or the maximum value.
   
   e. Upload and install the software license file on the appliance.

3. Set up the Master Control Node (MCN) site.
   
   a. Switch the Management Web Interface to MCN Console mode.
   
   b. Add and configure the MCN site.
   
   c. Configure the Virtual Interface Groups for the MCN site.
   
   d. Configure the Virtual IP Addresses for the MCN site.
   
   e. (Optional) Configure the GRE Tunnels for the MCN site.
   
   f. Configure the WAN Links for the MCN site.
   
   g. Configure the Routes for the MCN site.
   
   h. (Optional) Configure High Availability (HA) for the MCN site.
   
   i. (Optional) Configure Virtual WAN security and encryption.
   
   j. Name and save the MCN site configuration.

4. Set up the branch sites.
   
   a. Add the branch site.
b. Configure the Virtual Interface Groups for the branch site.

c. Configure the Virtual IP Addresses for the branch site.

d. (Optional) Configure the GRE Tunnels for the branch site.

e. Configure the WAN Links for the branch site.

f. Configure the Routes for the branch site.

g. (Optional) Configure High Availability (HA) for the branch site.

h. (Optional) Clone the new branch site to create and configure additional sites.

**Note**

Cloning the branch site is optional. The SD-WAN appliance models must be the same for both the original and the cloned sites. You cannot change the specified appliance model for a clone. If the appliance model is different for a site, you must manually add the site, by repeating steps (a) through (f).

i. Resolve any configuration Audit Alerts.

j. Save the new configuration.

5. Configure the Virtual Paths and Virtual Path Service between the MCN and the client sites.

6. (Optional/provisional) If your license includes WAN Optimization, enable and configure WAN Optimization.
   a. Enable WAN Optimization and configure the default Features settings.
   b. Configure the default Tuning Settings.
   c. Configure the default Application Classifiers.
   d. Configure the default Service Classes.
   e. Configure WAN Optimization for the branch sites.

7. Prepare the SD-WAN Appliance Packages on the MCN.
   a. Export the new configuration package to Change Management on the MCN.
   b. Generate and stage the Appliance Packages on the MCN.

8. Connect the client appliances to your network.

9. Install the SD-WAN Appliance Packages on the clients.

10. Enable the SD-WAN Service on each of the SD-WAN appliances in your network.

11. Use the Monitoring pages to verify the activation and check for any existing or potential configuration issues.
Installation and Configuration Information Checklist

Oct 04, 2016
Gather the following information for each NetScaler SD-WAN site you want to deploy:

- The licensing information for your product

- Required Network IP Addresses for each appliance to be deployed:

  * Management IP Address
  * Virtual IP Addresses

- Site Name

- Appliance Name (one per site)

- SD-WAN Appliance Model (for each appliance to be deployed)

- Deployment Mode (MCN or Client)

- Topology

- Gateway MPLS

- GRE Tunnel information

- Routes

- VLANs

- Bandwidth at each site for each circuit
Getting Started With NetScaler SD-WAN

Mar 30, 2017
Refer to the following sections to help you get familiarized with using NetScaler SD-WAN web interface, installing required appliance packages, connecting appliances, and setting up the SD-WAN network.

- NetScaler SD-WAN Management Web Interface
- Installing the Virtual WAN Appliance Packages
- Preparing the Virtual WAN Appliance Packages
- Connecting the Client Appliances to Your Network
- Setting up the SD-WAN Appliances
NetScaler SD-WAN Management Web Interface

Oct 04, 2016

This section provides basic navigation instructions, and a navigation roadmap of the Management Web Interface page hierarchy. Also provided are specific navigation instructions for the Configuration Editor and Change Management wizard.

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

The basic navigation elements are as follows:

- **Title bar** – This is the dark grey bar at the top of all Management Web Interface screens. 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 light blue 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 blue main menu bar at the top of the page. These are the top-level categories for the Management Web 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 blue and grey pane, below the main menu bar. This displays the navigation tree for a section. Click a section tab to display the navigation tree for that section. The navigation tree offers the following display and navigation options:
  - Click a section tab to display the navigation tree and page hierarchy for that section.
  - Click + (plus sign) next to a branch in the tree to reveal the available pages for that branch topic.
  - Click a page name to display that page in the page area.
- Click – (minus sign) next to a branch item to close the branch.

- **Breadcrumbs** – This displays the navigation path to the current page. The breadcrumbs are located at the top of the page area, just below the main menu bar. Active navigation links display in blue font. The name of the current page is displayed in black bold font.

- **Page area** – This is the page display and work area for the selected page. Select an item in the navigation tree to display the default page for that item.

- **Page tabs** – Some pages contain tabs for displaying additional child pages for that topic or configuration form. These are usually located at the top of the page area, just below the breadcrumbs display. In some cases (as for the Change Management wizard), tabs are located in the left pane of the page area, between the navigation tree and the work area of the page.

- **Page area resizing** – For some pages, you can grow or shrink the width of the page area (or sections of it) to reveal additional fields in a table or form. Where this is the case, there will be a grey, vertical resize bar on the right border of a page area pane, form, or table. Roll your cursor over the resize bar until the cursor changes to a bi-directional arrow. Then click and drag the bar to the right or left to grow or shrink the area width.

If the resize bar is not available for a page, you can click and drag the right edge of your browser to display the full page.
Click the Dashboard section tab to display basic information for the local appliance.

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

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

The below figure shows a sample Master Control Node (MCN) appliance Dashboard display.
The below figure shows a sample client appliance Dashboard display.
The **Configuration Editor** enables you to add and configure CloudBridge Virtual WAN Appliance sites, connections, optimization, and provisioning, and to create and define the Virtual WAN Configuration.

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

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

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

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

   ![Configuration Editor Diagram](image)

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

   - **Configuration Editor menu bar** – This is located at the top of the page area, just below the breadcrumbs links. The menu bar contains the primary activity buttons for **Configuration Editor** operations. In addition, at the far right edge of the menu bar is the **View Tutorial** link button for initiating the **Configuration Editor** tutorial. The tutorial steps you
through a series of bubble descriptions for each element of the Configuration Editor display.

- **Configuration Editor sections tree** – This is the stack of dark grey bars located in the left pane of the Configuration Editor page area. Each grey bar represents a top-level section. Click + at the left of a section name to reveal the sub-branches for that section.

- **Sections tree branches** – Click + (plus sign) at the left of a section name in the sections tree to open a section branch. Click – (minus sign) to close a branch. Each section branch contains one or more sub-branches of configuration categories and forms, which in turn may contain additional child branches and forms.

- **Sites tree** – This lists the site nodes that have been added to the configuration currently opened in the Configuration Editor. In the section tree, click + at the left of Sites to open the Sites tree. Click + to the left of a site name to open the branch for that site. Click – (minus sign) to close a branch. For detailed instructions on navigating and using the Sites tree and configuration forms, see the following sections:
  - Setting up the Master Control Node (MCN) Site.
  - Adding and Configuring the Branch Sites.

- **Audits status bar** – This is the dark grey bar at the bottom of the Configuration Editor page, and spanning the entire width of the Management Web Interface screen. The Audits status bar is available only when the Configuration Editor is open. An Audit Alert icon (red dot or goldenrod delta) at the far left of the status bar indicates one or more errors present in the currently-opened configuration. Click the status bar to display a complete list of all unresolved Audit Alerts for that configuration.

- **Resize bar** – The resize bar is the thin, grey, vertical bar located on the right border of the main page area pane, and is available in most of the Configuration Editor pages. You can use the resize bar to grow or shrink the width of the page area to reveal or truncate content in a table, tree, or form. 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 area, you can click and drag the right edge of your browser to display the full page.

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

- **MCN (Global) Change Management wizard** – The MCN Global Change Management wizard is the primary (main) version, and is available in the MCN Management Web Interface, only. Use this to generate the Virtual WAN Appliance Packages to be deployed for each type of Virtual WAN Appliance in your network. You can also use the wizard to automatically propagate configuration changes to Virtual Appliances already deployed in your Virtual WAN. Basic navigation instructions are provided in the section, “Using the MCN Global Change Management Wizard” below. Instructions for using the MCN global Change Management wizard to create the Appliance Packages are provided in the section Preparing the Virtual WAN Appliance Packages on the MCN.

- **Local Change Management wizard** – The Local Change Management wizard is available in the Management Web Interface running on both the MCN and on all client node appliances. Use this to upload, stage, and activate the appropriate Virtual WAN Appliance Package on a local appliance to be added to your Virtual WAN. You can also use this
wizard to upload an updated Appliance Package specifically to the local MCN, or to an individual, local Virtual WAN Appliance already deployed in your network. Instructions for navigating and using the Local Change Management wizard are provided in the section Installing the Virtual WAN Appliance Packages on the Clients.

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

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

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

5. To start the wizard, click Begin.

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

- Preparing the Virtual WAN Appliance Packages on the MCN
- Installing the Virtual WAN Appliance Packages on the Clients

The Change Management wizard contains the following navigation elements:

- **Page area** – This displays the forms, tables, and activity buttons for each page of the Change Management wizard.
• **Change Management wizard page tabs** – The page tabs are located in the left pane of the page area on each page of the wizard. Tabs are listed in the order that the corresponding steps occur in the wizard process. When a tab is active, you can click it to return to a previous page in the wizard. If a tab is active, the name displays in blue font. Grey font indicates an inactive tab. Tabs are inactive until all dependencies (previous steps) have been fulfilled without error.

• **Appliance-Site table** – This is located at the bottom of the wizard page area, on most wizard pages. The table contains information about each configured appliance site, and links for downloading the active or staged Appliance Packages for that appliance model and site. A package in this context is a Zip file bundle containing the appropriate NetScaler SD-WAN software package for that appliance model, and the specified configuration package. The **Configuration Filenames** section above the table shows the package name for the current active and staged packages on the local appliance.

• **Active/Staged download links** – These are located in the **Download Package** field (far right column) of each entry in the **Appliance-Site** table. Click a link in an entry to download the active or staged package for that appliance site.

• **Begin button** – Click **Begin** to initiate the **Change Management** wizard process and proceed to the **Change Preparation** tab page.

• **Activate Staged button** – If this is not an initial deployment, and you want to activate the currently staged configuration, you have the option of proceeding directly to the **Activation** step. Click **Activate Staged** to proceed directly to the Activation page and initiate activation of the currently staged configuration.
Installing the SD-WAN Appliance Packages on the Clients

Oct 04, 2016

After you have prepared the Appliance Packages and connected the MCN, and the branch Site Administrators have connected their respective client appliances to the LAN and WAN, the next step is to upload and activate the appropriate SD-WAN Appliance Package on each client. The Change Management wizard guides you through this process.

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

1. On a connected PC, open a browser and log onto the MCN appliance Management Web Interface.

   Enter the Management IP Address for the MCN in the browser address field. This displays the Management Web Interface Dashboard page for the MCN appliance.

2. Select the Configuration tab.

3. In the navigation pane on the left, select Virtual WAN and then select Change Management.

   This displays the Change Process Overview page (the first page of the Change Management wizard).

At the bottom of this page, you will see a table listing the individual sites and appliances. At the far right of the table in the Download Package column, are links for the Active (if available) and Staged Appliance Packages.
4. Click the **Staged** link for the package you want to download.

   In the **Site-Appliance** table, locate the entry for your site appliance, and click the **Staged** link in the **Download Package** column of that entry. A file browser for selecting the download location (on the local PC) displays.

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

6. (Optional.) After the download completes, log out of the MCN Management Web Interface.

7. Open a browser, and enter the IP Address for the client to which you want to upload the Appliance Package Zip file.

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

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

8. Enter the Administrator user name and password and click **Login**.

   The default Administrator user name is **admin**; the default password is **password**.
This displays the Management Web Interface **Dashboard** page for the client appliance.

![Citrix NetScaler SD-WAN VPX 50-SE Dashboard](image)

**Note**

If this is an initial installation, or if you have temporarily disabled the Virtual WAN Service on this appliance, you will see a goldenrod Audit Alert icon with a status message indicating that the Virtual WAN Service is currently inactive or disabled. You can ignore this alert for now. The alert will remain on the **Dashboard** page until you manually start the service, after completing the installation.

9. Select the **Configuration** tab.

10. Open the System Maintenance branch in the navigation tree (left pane), and select Local Change Management.

    This displays the **Local Appliance Change Process Upload** page for uploading an Appliance Package.
11. Click Choose File next to the Upload Item label.

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

12. Navigate to the SD-WAN Appliance Package Zip file you just downloaded from the MCN, select it, and click OK.

13. Click Upload.

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

14. Click Next.

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

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

   The page at https://10.199.81.236 says: ✗

   This will switch the Active software/configuration image on this appliance to the
   one in the Staged area.
   Are you sure you want to perform the Activate
   Process?

   ![OK Cancel](image)

16. Click **OK**.

   This activates the newly-installed package and, if this is not an initial deployment, starts the Virtual WAN Service on
   the client appliance. This process takes several seconds, during which a progress status message displays.
When the activation completes, a status message displays stating **Activation complete**, and the **Done** button becomes available.

After the activation completes, click **Done** on the **Activation** page to return to the Management Web Interface **Dashboard** page.

If this is not an initial deployment, this page should now display updated information for the currently active version of the software package, the OS partition, and the status of the CloudBridge Virtual Path. If this is an initial installation, there will be a goldenrod Audit Alert icon, along with a status message indicating that the Virtual WAN Service is currently inactive or disabled. In this case, you must manually enable the service, as described in **Enabling the Virtual WAN Service**.
The below figure shows a sample client Dashboard page displaying the alert icon and status message.

![Dashboard page](image)

The final step to complete an initial SD-WAN deployment, is to enable the Virtual WAN Service. Instructions are provided in the section Enabling the Virtual WAN Service.
Preparing the SD-WAN Appliance Packages on the MCN

Oct 04, 2016

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

1. Export the Configuration Package to Change Management.

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

2. Generate and stage the Appliance Packages.

   After you have added the new configuration package to the Change Management inbox, you can generate and stage the Appliance Packages. To do this, you will use the Change Management wizard in the Management Web Interface on the MCN. Instructions are provided in the section Generating and Staging the SD-WAN Appliance Packages.
Exporting the Configuration Package to Change Management

Oct 04, 2016

Before you can generate the Appliance Packages, you must first export the completed configuration package to the Management Web Interface \textit{Change Management} system.

To export the configuration package to \textit{Change Management}, do the following:

1. In the \textit{Configuration Editor} page, click \textit{Export} (at the top of the page).

This opens the \textit{Export Configuration} dialog box.
2. Select **Change Management** Inbox as the export destination.

   Use the drop-down menu in the **Destination: field to make your selection**.

3. Click **Export**.

   When the export operation completes, a green success status message displays at the top of the page.

   ![The Configuration has been exported to Change Management](image)

   - **Sites**
   - **Virtual WAN Network Settings**
   - **MCN_DC-01_K**
   - **BR-01_K**

   **Tip**

   You can click the blue **Change Management** link in the success message to go directly to the **Change Preparation -- Upload and Verify Files** page (second page) of the **Change Management** wizard. You will need to navigate to this page to perform the next step in the configuration process. However, the success message displays for only a few seconds, after which you must use the navigation tree to open the wizard and then step through to this page. Instructions are provided in the next section.

You are now ready to upload the SD-WAN software packages to the MCN Appliance, and prepare the Appliance Packages for distribution to the client nodes.
Generating and Staging the SD-WAN Appliance Packages

Oct 04, 2016
The next step is to prepare the SD-WAN Appliance Packages for distribution to the client nodes. To do this, you will use the Change Management wizard in the Management Web Interface on the MCN.

There is a different SD-WAN software package for each SD-WAN Appliance model. An Appliance Package consists of the software package for a specific model, bundled with the configuration package you want to deploy. Consequently, a different Appliance Package must be prepared and generated for each appliance model in your network.

Note

If you have not already downloaded the required SD-WAN software packages to a PC connected to your network, you will need to do so now. For information on acquiring and downloading the software, see the section Acquiring the SD-WAN Software Packages.

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

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

   Note

   You will be uploading the software packages you previously downloaded to the connected PC. For convenience, you might want to use this same PC to connect to the MCN again.

2. Select the Configuration tab.

3. In the left pane, open the Virtual WAN section, and select Change Management.

   This displays the first page of the Change Management wizard, the Change Process Overview page.
4. Click **Begin**.

This displays the **Change Preparation** page for uploading and verifying the specified configuration and software package(s).
5. Upload each of the SD-WAN software packages required for your network.

**Note**

There is a different software package for each SD-WAN Appliance model. Before proceeding with this step, make sure you have downloaded a copy of the appropriate Virtual WAN software package for each of the different appliance models in your network. For information on downloading the software packages, see the section [Acquiring the SD-WAN Software Packages](#).

For each SD-WAN software package you want to deploy, do the following:

- a. Click **Choose File** next to the **Upload Item** field.
  
  This opens a file browser for selecting a SD-WAN software package to upload.
  
- b. Select a SD-WAN software package, and click **OK**.
  
  Navigate to the SD-WAN software packages you downloaded earlier to the local PC, and select the package to upload.
  
  c. Click **Upload**.
  
  d. Repeat steps (a) through (c) for each of the SD-WAN software packages required for your network.

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

7. Click **Next**.

   The selected configuration is submitted for verification, and the **Verification** results page displays.
8. Click OK.

This dismisses the Verification page and proceeds to the License page.

9. Select I accept the End User License Agreement and click OK.
This dismisses the License page and proceeds to Appliance Staging page.

10. If this is an initial deployment, check the Ignore Incomplete box.

This indicates that the client sites should be ignored for this staging operation, and only the MCN should be updated and staged at this time.

Note

In the future, if you need to update this configuration after it has been deployed and Virtual Path communication is in effect, you can skip this step.

In such a case, the configuration will be automatically distributed from the MCN to all active remote clients, by means of the existing Virtual Path.

11. Click Stage Appliances.

This initiates the following actions:

- Transfers the selected software package and configuration to the MCN.
- Generates an Appliance Package for each appliance model identified in the selected configuration.
- Adds the new Appliance Packages to the list of available packages in the Site-Appliance table.
- Stages the new configuration and appropriate software package on the MCN.

**Note**

If this is an initial deployment, only the MCN is updated and staged at this time. If you are updating an existing deployment and the Virtual Paths are already functioning between the deployed sites, this also distributes the appropriate Appliance Packages to the deployed client nodes, and initiates staging on those nodes. However, if you are adding new client nodes to an existing Virtual WAN deployment, you still must manually upload, stage, and activate the appropriate Appliance Package on each new client, as outlined in the remaining steps in this manual.

A goldenrod Transfer Progress status bar displays as the transfer proceeds. When the staging operation completes, the Site-Appliance table is populated with the newly-staged Appliance Packages information.

12. Click **Next**.

This proceeds to the Activation tab Activate page.
13. Click **Activate Staged**.

A dialog box displays, prompting you to confirm the activation operation.

The page at https://10.199.81.236 says:  

![Image of dialog box](https://docs.citrix.com)

This will switch the Currently Active software/configuration on the network to the version in the Currently Staged area.
Are you sure you want to begin Activation?

The results and next steps will differ at this point, depending on whether this is an initial configuration or you are updating or replacing an existing configuration, as follows:

- **If you are updating or changing the configuration on an existing deployment:**
  
  To complete the activation, do the following:

  a. Click **OK**.

  If this is not an initial configuration, this activates the new configuration and the appropriate Appliance Package on the MCN appliance. The appropriate Appliance Package is then distributed to and automatically activated on each client in
your SD-WAN. (This may take several seconds to complete.)

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

The below figure shows the **Activation Complete** page and status message, and active **Done** button.

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

This returns you to the Management Web Interface Dashboard page, where you can view the activation results.

c. Proceed to one of the following:

* If you are not adding any new nodes to your SD-WAN, this completes the preparation, distribution, and activation of the new Appliance Packages in your SD-WAN. You can proceed directly to [Enabling the Virtual WAN Service](https://docs.citrix.com).

* If you want to add new client nodes to your SD-WAN, please proceed to [Connecting the Client Appliances to Your Network](https://docs.citrix.com).

- **If you are activating an initial configuration:**

  If this is an initial configuration, the new configuration package will not be activated at this point, and there are some extra steps you must perform. The next step is to copy the configuration package to the Local Appliance Staging area, in preparation for staging and activating the configuration package on the MCN.

  Do the following:
a. Click OK.

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

b. Click OK.

This copies the package to the local **Appliance Staging** area, and displays a progress status message.

After a few seconds, the copy operation completes, and the **Local Change Management Activation** screen displays.
c. Click **Activate Staged**.

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

The page at https://10.199.81.236 says:

```
This will switch the Currently Active software/configuration on the network to the version in the Currently Staged area.
Are you sure you want to begin Activation?
```

- Click **OK**.

This initiates activation of the staged configuration package. This process takes several seconds, during which a progress status message displays.
When the activation completes, a status message displays stating Activation complete, and the Done button is enabled.

e. Click Done.

This proceeds to the Management Web Interface Dashboard page, where you can view the activation results.
If this is an initial deployment, the Dashboard page displays an Audit Alert icon (goldenrod delta) and a status message stating that the Virtual WAN Service is currently disabled. You can ignore this Audit Alert for now. This alert will be resolved when you complete the final step, enabling the Virtual WAN Service.

You have now completed the preparation of the SD-WAN Appliance Packages on the MCN. Proceed to Connecting the Client Appliances to Your Network.
Connecting the Client Appliances to Your Network

Oct 04, 2016

If this is an initial deployment, or you are adding client nodes to an existing SD-WAN, the next step is for the branch Site Administrators to connect the client appliances to the network at their respective branch sites. This is in preparation for uploading and activating the appropriate SD-WAN Appliance Packages to the clients. You will need to contact each branch Site Administrator to initiate and coordinate these procedures.

To connect the site appliances to the SD-WAN, Site Administrators should do the following:

1. If you have not already done so, set up the client appliances.

   For each appliance you want to add to your SD-WAN, you will need to do the following:

   **Note**

   Instructions for each of these tasks are provided in Setting up the SD-WAN Appliances.

   a. Set up the SD-WAN Appliance hardware and any SD-WAN VPX Virtual Appliances (SD-WAN VPX-SE) you will be deploying.
   b. Set the Management IP Address for the appliance and verify the connection.
   c. Set the date and time on the appliance.
   d. Upload and install the software license file on the appliance.

2. Connect the appliance to the branch site LAN.

   Connect one end of an Ethernet cable to a port configured for LAN on the SD-WAN Appliance, and the other end of the cable to the LAN switch.

3. Connect the appliance to the WAN.

   Connect one end of an Ethernet cable to a port configured for WAN on the SD-WAN Appliance, and the other end of the cable to the WAN router.

   The next step is for the branch Site Administrators to install and activate the appropriate SD-WAN Appliance Package on their respective clients.
Setting up the SD-WAN Appliances

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-VW on ESXi.
- Differences Between a SD-WAN VPX-SE and SD-WAN WANOP VPX Installation.
Setting up the Appliance Hardware

Oct 04, 2016
To set up your NetScaler SD-WAN Appliance hardware, do the following:

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

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

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

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

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

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

The below figure shows the location of the NetScaler SD-WAN 400-SE Management Port.
The NetScaler SD-WAN 2000-SE Management Port is the bottom-left port labeled 0/1, on the front of the chassis. The default IP Address for the Management Port is 192.168.100.1.

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

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

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

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

The below figure shows the location of the NetScaler SD-WAN 5100-SE Management Port.
The NetScaler SD-WAN VPX-SE Virtual Appliance is a Virtual Machine, so there is no physical Management Port. However, if you did not configure the Management IP Address for the SD-WAN VPX-SE when you created the VPX Virtual Machine, you will need to do so now, as outlined in the section, Configuring the Management IP Address for the SD-WAN VPX-SE.

Also see the section Setting the Management IP Addresses for the Appliances.
Setting the Management IP Addresses for the Appliances

Oct 04, 2016
To enable remote access to a NetScaler SD-WAN appliance, you must specify a unique Management IP Address for the appliance. To do so, you must first connect the appliance to a personal computer. You can then open a browser on the PC and connect directly to the Management Web Interface on the appliance, where you can set the Management IP Address for that appliance. The Management IP Address must be unique for each appliance.

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

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

- **SD-WAN hardware appliance** – See the section Setting the Management IP Address for a Hardware SD-WAN Appliance.
Setting the Management IP Address for a SD-WAN Appliance

Oct 04, 2016
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
Make sure the Ethernet port is enabled on the PC you are using to connect to the appliance.

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

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

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

5. On the PC, open a browser and enter the default IP Address for the appliance.

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

Enter the following IP Address in the address line of the browser:
192.168.100.1
Note
Please ignore any browser certificate warnings for the CloudBridge Management Web Interface.

This opens the NetScaler SD-WAN Management Web Interface Login screen on the connected appliance, as shown in the below figure.

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

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

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

After you have logged into the Management Web Interface, the **Dashboard** page displays, as shown below.
The first time you log into the Management Web Interface on an appliance, the Dashboard displays an Alert icon (goldenrod delta) and alert message indicating that the Virtual WAN Service is disabled, and the license has not been installed. For now, you can ignore this alert. The alert will be resolved after you have installed the license, and completed the configuration and deployment process for the appliance.

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

7. In the main menu bar, select the Configuration section tab.
   This displays the Configuration navigation tree in the left pane of the screen. The Configuration navigation tree contains the following three primary branches:
   - Appliance Settings
   - Virtual WAN
   - System Maintenance

   When you select the Configuration tab, the Appliance Settings branch automatically opens, with the Administrator Interface page preselected by default, as shown in the below figure.
8. In the Appliance Settings branch of the navigation tree, select Network Adaptors.

This displays the Network Adaptors settings page with the IP Address tab preselected by default, as shown in the below figure.
9. In the **IP Address** tab page, enter the following information for the CloudBridge Virtual WAN Appliance you want to configure.

   - IP Address
   - Subnet Mask
   - Gateway IP Address

**Note**
The Management IP Address must be unique for each appliance.

10. Click **Change Settings**.
    A confirmation dialog box displays, prompting you to verify that you want to change these settings.
11. Click **OK**.
12. Change the network interface settings on your PC back to the original settings.

**Note**
Changing the IP Address for your PC automatically closes the connection to the appliance, and terminates your login session on the Management Web Interface.
13. Disconnect the appliance from the PC and connect the appliance to your network router or switch. Disconnect the Ethernet cable from the PC, but do not disconnect it from your appliance. Connect the free end of the cable to your network router or switch.

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

14. Test the connection.

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

If the connection is successful, this displays the Login screen for the NetScaler SD-WAN Management Web Interface on the appliance you just configured.

Tip

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

You have now set the Management IP Address of your SD-WAN Appliance, and can connect to the appliance from any location in your network.
Setting the Date and Time on an SD-WAN Appliance

Oct 04, 2016

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

**Note**

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

To set the date and time, do the following:

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

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

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

6. Click Change Timezone.
   This updates the time zone and recalculates the current date and time setting, accordingly. If you set the correct date and time before this step, then your settings will no longer be correct.
   When the time zone update completes, a success Alert icon (green check mark) and status message displays in the top section of the page.

7. (Optional) Enable NTP Server service.
   a) Select Use NTP Server.
   b) Enter the server address in the Server Address field.
   c) Click Change Settings.
      A success Alert icon (green checkmark) and status message displays when the update completes.
8. Select the month, day, and year from the Date field drop-down menus.
9. Select the hour, minutes, and seconds from the Time field drop-down menus.
10. Click Change Date.

Note

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

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

Warning

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

Oct 04, 2016

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

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

1. Select the Configuration tab, and then select the Appliance Settings branch in the navigation tree.
   
   This displays the Appliance Settings page, with the User Accounts tab preselected by default.

   ![Configuration Tab](image)

2. Select the Miscellaneous tab (far right corner).
   
   This displays the Miscellaneous tab page.
3. Enter the console **Timeout** value.

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

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

4. Click **Change Timeout**.

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

   After a brief interval (a few seconds), the session is terminated and you are automatically logged out of the Management Web Interface. The Login page page appears.
5. Enter the Administrator user name (admin) and password (password), and click Login.

The next step is to upload and install the SD-WAN software license file on the appliance.
Uploading and Installing the SD-WAN Software License File

Oct 04, 2016

This section provides instructions for uploading and installing the SD-WAN software license files to the appliances. You must do this for each appliance you want to add to your SD-WAN deployment.

If this is an initial deployment, you have the option of completing this task now, or when you manually upload and install the Appliance Packages on each of the appliances. However, installing the Appliance Packages occurs much later in the deployment process, and involves several other procedures. In general, it is recommended that you complete the licensing procedure now, as it will simplify both tasks.

For each appliance you want to add to your network, do the following:

1. If you have not already done so, download the license file to the PC you will be using to log into the appliance.
   For information about obtaining licenses, see the section Licensing.

2. Log into the Management Web Interface on the appliance you are licensing.
   Open a browser and enter the Management IP Address for the appliance in the address field of the browser, and press Return. A successful login opens the Management Web Interface and displays the Dashboard page.

3. In the main menu bar, select the Configuration tab.
   This displays the Configuration navigation tree in the left pane, and automatically opens the Appliance Settings branch in the tree.
4. In the **Appliance Settings** branch, select **Licensing**.

This displays the Licensing page.

5. Click **Choose File**.
This displays a file browser for selecting the license file. Navigate to the license file you downloaded earlier, and select it.

6. Click **Upload**.

When the upload completes, the name of the file displays in the Filename: field at the bottom of the page.

7. Click **Apply Settings**.

When the operation completes, the Licensing page refreshes and the new license information displays in the License Status section.

You have now completed the process of setting up the appliance. Repeat these steps for each appliance you want to add to your SD-WAN.

**Note**

If you have not already downloaded the NetScaler SD-WAN software packages to a PC connected to your network, please do so now. For information on acquiring and downloading the software packages, see [Acquiring the SD-WAN Software Packages](https://docs.citrix.com).
Troubleshooting DHCP Management IP Address Configuration

Dec 20, 2016

The following are the possible scenarios that you might encounter when configuring DHCP IP address. It also includes best practices and recommendations for configuring DHCP Management IP address when deploying SD-WAN appliances.

These recommendations are applicable to all platform models of SD-WAN; Standard Edition, WANOP, and Enterprise Edition - Physical and Virtual appliances.

Note

All hardware models of SD-WAN appliances are shipped with a factory default management IP address. Ensure that you configure the required DHCP IP address for the appliance during the setup process.

All Virtual models of SD-WAN appliances (VPX models) and appliances which can be deployed in AWS environment do not have a factory default IP address assigned.

Appliances power on without DHCP server(s) reachable

- Causes:
  - Ethernet management cable is disconnected
  - DHCP service is down for the connected network
- Expected behavior
  - Appliances with DHCP service enabled will retry DHCP request every 300 seconds (default value). The actual interval is approximately 7 minutes
  - Therefore, appliances with DHCP service enabled will acquire DHCP addresses within 7 minutes after DHCP server(s) become available. The delay ranges from 0 to 7 minutes

Assigned DHCP address expires

- Expected behavior:
  - Appliances with DHCP service enabled will try to renew the lease before the address expires
  - Appliances start with new DHCP discovery, if the renew fails

Appliances with DHCP service enabled move from one DHCP enabled subnet to another subnet:

- Causes: Appliances move from an assigned DHCP subnet to a different DHCP subnet
- Expected behavior:
  - A permanent lease DHCP IP address assignment might require the appliances to be rebooted to acquire an IP address from the new DHCP server.
  - Upon DHCP lease expiration, appliances might re-initiate DHCP discovery protocol, if current DHCP server is not reachable.
  - Appliances will acquire new IP addresses with a delay of 8 minutes. The gateway IP address is not modified in the GUI
and CLI. It is updated after the reboot process is completed.

Recommendation

- Always assign permanent lease for DHCP addresses assigned to SD-WAN appliances (physical/virtual). This will allow appliances to have predictable management IP address.
About SD-WAN VPX Standard Edition

Mar 30, 2017
This section outlines the requirements and prerequisites for installing a NetScaler SD-WAN VPX Virtual Appliance (SD-WAN VPX-SE). It also includes an overview and summary of the installation procedures, and a checklist of information you will need to complete for installation.

For step-by-step instructions on installing and deploying a NetScaler SD-WAN VPX-SE, see the following:

- Installing VPX-SE on VMware ESXi – See Installing and Deploying a SD-WAN VPX-SE on ESXi.

- Installing SD-WAN VPX-SE on XenServer – The procedures for installing a NetScaler SD-WAN Virtual WAN VPX (SD-WAN VPX-SE) and a NetScaler SD-WAN WAN Optimization appliance (WANOP VPX) are very similar. However, there are some critical differences, as outlined in Differences Between a SD-WAN VPX-VW and WAN OP VPX Installation. For instructions on installing a SD-WAN VPX on XenServer, see NetScaler SD-WAN VPX in the document entitled, Citrix CloudBridge 7.4 Product Documentation, available on the Citrix Documentation Portal at this location: [http://docs.citrix.com/](http://docs.citrix.com/).

The following section outlines the requirements and prerequisites for installing a NetScaler SD-WAN VPX-SE and deploying it in your SD-WAN environment.
NetScaler SD-WAN VPX-SE Installation Requirements and Prerequisites

Oct 04, 2016

This section outlines the hardware and software requirements for NetScaler SD-WAN Virtual Appliance (SD-WAN VPX-SE), and defines the platform dependencies.

The SD-WAN VPX-SE hardware requirements for the hosting platform are as follows:

- **Processor requirements**: 4 Core, 2.7 GHz (or equivalent) processor or better.
- **Disk space requirements**: 40 GB of disk space

This section outlines the software requirements for the SD-WAN VPX-SE, and basic information on acquiring and downloading the SD-WAN VPX-SE software.

SD-WAN VPX-SE Virtual Appliance supports the following server platforms:

- XenServer Hypervisor 6.5 SP1
- VMware Hypervisor ESXi server, version 5.5.0 or higher

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

The SD-WAN VPX-SE Management Web Interface supports the following browsers:

- Google Chrome 49.0.2623112 m+
- Mozilla Firefox 43.0.4+
- Microsoft Internet Explorer 11.0.9600.18163+

Before you can install and deploy a SD-WAN VPX-SE 9.1 as a client appliance, the SD-WAN Master Control Node (MCN) and existing client nodes must be upgraded to Virtual WAN version 8.1 or above. For information on updating and upgrading your CloudBridge (SD-WAN) deployment, please refer to the Citrix CloudBridge 9.0.0 Release Notes, available on the Citrix Documentation Portal (http://docs.citrix.com/).

The following section provides instructions for downloading the SD-WAN VPX-SE installation files.

Before beginning the installation, you must download or copy the SD-WAN VPX-SE OVF template (.ova file) to the local PC you will be using to connect to the ESXi server that will host your SD-WAN VPX-SE.
To download the SD-WAN VPX-SE installation files, go to the following URL:

http://www.citrix.com/downloads.html

Instructions for downloading the software are provided on this site.

Download the appropriate file, as follows:

- To install SD-WAN VPX-SE on XenServer, download this file:
  cb-vw-vpx-<version>.xva

- To install SD-WAN VPX-SE on VMware ESXi Server, download this file:
  cb-vw-vpx-<version>_vmware.ova

Where <version> is the current SD-WAN SE version number.

The following section provides a summary of the steps and procedures involved in installing and configuring a SD-WAN VPX-SE Virtual Appliance.

The minimum configuration requirements for the SD-WAN VPX-SE Virtual Machine are as follows:

- Virtual CPUs: 4
- Memory: 4GB RAM
- Virtual Datastore: 40 GB disk
- Management Interface: 1 (default)

The SD-WAN VPX-SE interface specifications are as follows:

- SD-WAN VPX-SE supports a maximum number of five interfaces.
- The first interface is reserved for use as the Management IP Address for the Virtual Appliance.
- Before powering up the new VM for the SD-WAN VPX-SE Virtual Appliance, you must configure and assign additional interfaces (one each) for the LAN and WAN.
- For SD-WAN VPX-SE, bridges are not created by default for the data interface (for example, eth1 and eth2).

Deployments that are supported for hardware SD-WAN Appliances are also supported for SD-WAN VPX-SE. SD-WAN VPX-
SE supports both 1-arm and In-line deployments. WCCP is not supported.
Differences Between a VPX-SE and a WANOP VPX Installation

Oct 04, 2016

This section outlines the essential differences between installing a SD-WAN VPX (VPX-SE) for deployment in your SD-WAN network, as compared to a SD-WAN VPX for WAN Optimization.

The primary differences when installing and configuring a SD-WAN VPX-SE virtual appliance from SD-WAN WANOP VPX, are as follows:

- Download the following installation files from the Citrix NetScaler downloads site (http://www.citrix.com/downloads.html).

  Note
  Remote licenses are supported for SD-WANVPX-SE.

  - To install SD-WAN VPX-SE on XenServer, download this file:
    cb-vw-vpx-<version>.xva

  - To install SD-WAN VPX-SE on VMware ESXi Server, download this file:
    cb-vw-vpx-<version>_vmware.ova

    Where <version> is the current SD-WAN version number.

  Note
  For additional information on licensing and downloading SD-WAN software, see the sections, Licensing and Acquiring the SD-WAN Software Packages.

- SD-WAN VPX-SE Virtual Appliance supports the following server platforms:
  - XenServer Hypervisor 6.5 SP1
  - VMware Hypervisor ESXi server, version 5.5.0 or higher

- SD-WAN VPX-SE supports both Inline and PBR deployments; however, WCCP deployments are not supported for VPX-SE.

- The Virtual Machine for the SD-WAN VPX-SE Virtual Appliance must be installed manually, on either the XenServer or VMware ESXi Server platform. Currently, there is no installation wizard for this procedure.

- The minimum configuration requirements for the Virtual Machine are as follows:
  - Virtual CPUs: 4
- **Memory**: 4GB RAM
- **Virtual Datastore**: 40 GB disk
- **Management Interface**: 1 (default)

- SD-WAN VPX-SE interface specifications are as follows:
  - SD-WAN VPX-SE supports a maximum number of five interfaces.
  - The first interface is reserved for use as the Management IP Address for the Virtual Appliance.
  - Before powering up the new VM for the SD-WAN VPX-SE Virtual Appliance, you must configure and assign additional interfaces (one each) for the LAN and WAN.
  - For VPX-SE, bridges are not created by default for the data interface (for example, eth1 and eth2).

- If you are not using DHCP, you must configure a static Management IP Address for the SD-WAN VPX-SE Virtual Appliance.

### Note

DHCP is enabled by default for the SD-WAN VPX-SE Management IP Address.

To configure a static Management IP Address for a SD-WAN VPX-SE Virtual Appliance, do the following:

1. Open the vSphere Client or XenServer Client where you created the SD-WAN VPX-SE Virtual Machine (VM).
2. Open the vSphere or XenServer Console for the new SD-WAN VPX-SE, and log into the Administrator account for the VM.
   - Default Administrator user name: `admin`
   - Default Administrator password: `password`
3. Enter the following command lines at the console CLI prompt:
   ```
   management_ip
   set_management_ip set interface <ip> <subnetmask> <gateway>
   ```
   Where:
   - `<ip>` is the Management IP Address for the SD-WAN VPX-SE Virtual Appliance.
   - `<subnetmask>` is the subnet mask used to define the network in which the SD-WAN VPX-SE Virtual Appliance resides.
   - `<gateway>` is the Gateway IP Address of the SD-WAN VPX-SE Virtual Appliance will use to communicate with external networks.
4. Restart the SD-WAN VPX-SE Virtual Appliance VM.
Note
See also the section, Setting the Management IP Addresses for the Appliances.
Overview of VPX Installation and Deployment Procedures

Oct 04, 2016

This section provides a summary of the steps involved for installing and deploying a SD-WAN VPX-SE Virtual Appliance.

You can install SD-WAN VPX-SE on the following platforms:

- **VMware ESXi** – For instructions, see Installing and Deploying a SD-WAN VPX-SE on ESXi.

- **XenServer** – The procedures for installing a SD-WAN VPX (VPX-SE) and a SD-WAN (WAN Optimization) VPX are very similar. For instructions on installing a SD-WAN WANOP VPX on XenServer, see the chapter entitled, “CloudBridge VPX,” in the document entitled, Citrix CloudBridge 7.4 Product Documentation, available on the Citrix Documentation Portal (http://docs.citrix.com/). See also, Differences Between a SD-WAN VPX-SE and WANOP VPX Installation.

The following list summarizes the steps and procedures involved in deploying a SD-WAN VPX-SE on a VMware ESXi server.

1. Gather your SD-WAN VPX-SE installation and configuration information.
   
   For instructions, see SD-WAN VPX-SE Installation and Configuration Checklist.

2. Install the VMware vSphere Client.
   
   For instructions, see Installing the VMware vSphere Client.

3. Install and deploy the SD-WAN VPX-SE OVF Template.
   
   For instructions, see Installing and Deploying the SD-WAN VPX-SE OVF Template.

4. Configure the SD-WAN VPX-SE Management IP Address.
   
   For instructions, see Configuring the Management IP Address for the SD-WAN VPX-SE.

5. Connect to the SD-WAN VPX-SE and test the deployment.
   
   For instructions, see Connecting to the SD-WAN VPX-SE and Testing the Deployment.
NetScaler SD-WAN VPX-SE Installation and Configuration Information Checklist

Oct 04, 2016
Gather the following information:

- Note the IP Address of the ESXi server that will host the SD-WAN VPX-SE Virtual Machine (VM).
- Select a unique name to assign to the SD-WAN VPX-SE VM.
- Determine the amount of memory to allocate for the SD-WAN VPX-SE VM.
- Determine the amount of disk capacity to allocate for the virtual disk for the VM (default disk space requirement is 39.1 GB).
- If you are not using DHCP, note the IP Address you intend to assign as the static Management IP Address for the SD-WAN VPX-SE. (By default, SD-WAN VPX-SE uses DHCP).
- Determine the Gateway IP Address the SD-WAN VPX-SE will use to communicate with external networks.
- Note the subnet mask for the network in which the SD-WAN VPX-SE will reside.
Deployment

Mar 30, 2017
Refer to the following topics for SD-WAN VPX deployment related information:

- Installing and Deploying SD-WAN VPX on ESxi
- Configuring Management IP Address
Installing and Deploying a SD-WAN VPX Standard Edition on VMware ESXi

Oct 04, 2016

This chapter provides step-by-step instructions for installing, configuring, and deploying the SD-WAN VPX-SE. This includes basic instructions for installing the VMware vSphere Client, which you will use to create and deploy the SD-WAN VPX-SE Virtual Machine.

Note

VMware vSphere Client operation details might change with new releases of the vSphere software. For the most complete and current vSphere Client installation and operation instructions, please refer to your VMware documentation. The instructions in this chapter are intended to provide the most basic and essential guidelines, only, for installing a SD-WAN VPX-SE Virtual Machine on the ESXi platform.

The following summarizes the top-level steps for installing and deploying a SD-WAN VPX-SE. You must perform these procedures in the exact order listed.

1. Install the VMware vSphere Client.
2. Install and deploy the SD-WAN VPX-SE OVF Template.
3. Configure the SD-WAN VPX-SE Management IP Address.
4. Connect and test the deployment.
Installing the VMware vSphere Client

Oct 04, 2016

This section provides basic instructions for downloading and installing the VMware vSphere client you will use to create and deploy the SD-WAN VPX-SE Virtual Machine.

**Note**

Please refer to your VMware vSphere Client documentation for additional information. NetScaler SD-WAN can be deployed in vSphere Client version 5.5 or later.

1. Open a browser and navigate to the ESXi server that will host your vSphere Client and VPX-SE Virtual Machine (VM) instance at: https://my.vmware.com/group/vmware/evalcenter?p=free-esxi6

   The VMware ESXi downloads page displays,

   **Download Packages**

   ![Download Packages](attachment:image)

   2. Click the **Download vSphere Client** link to download the vSphere Client installation file.

   3. Install the vSphere Client.

      Run the vSphere Client installer file that you just downloaded, and accept each of the default options when prompted.

   4. After the installation completes, start the vSphere Client program.

      The VMware vSphere Client login page displays, prompting you for the ESXi server login credentials.
5. Enter the ESXi server login credentials.

Enter the following:

- **IP address / Name**: Enter the IP Address or Fully Qualified Domain Name (FQDN) for the ESXi server that will host your SD-WAN VPX-SE VM instance.

- **User name**: Enter the server Administrator account name. The default is root.

- **Password**: Enter the password associated with this Administrator account.

6. Click **Login**.

This displays the **vSphere Client** main page.
The next step is to install and deploy the SD-WAN VPX-SE OVF template and set up the Virtual Machine. The following section provides instructions for these procedures.
Installing and Deploying the SD-WAN VPX OVF Template

Oct 04, 2016
This section provides instructions for installing the SD-WAN VPX OVF template and creating the SD-WAN VPX Virtual Machine.

1. If you have not already done so, download the SD-WAN VPX OVF template file (.ova file) to the local PC.

   Download or copy the SD-WAN VPX OVF template to the local PC you will be using to connect to the ESXi server that will host your SD-WAN VPX. The OVF template file has a file name using the following naming convention:

   \textit{cb-wv-vpx-version\_number-vmware.ova}

   where:

   \textit{version\_number} is the SD-WAN VPX release version number.

   .\textit{ova} is the file name suffix indicating that this is an OVF template file.

   \textbf{Note}

   For additional information, please see downloading the Software Packages in System Requirements section.

2. Continuing in the vSphere Client, click \textbf{File} and then select \textbf{Deploy OVF Template}... from the drop-down menu.

   This displays the first page of the \textbf{Deploy OVF Template} wizard, the \textbf{Source} page.
3. Select the CB VPX-VW OVF template (.ova file) you want to install.

   Browse to the location of the .ova file you downloaded earlier to the local PC, and select it.

4. Click **Next**.

   This imports the selected .ova file and displays the **OVF Template Details** page.
5. This page displays some basic information regarding the OVF template you just imported.

6. Click **Next**.

   This proceeds to the **End User License Agreement** page.
7. Click **Accept**, and then click **Next**.

This proceeds to the **Name and Location** page.
8. Enter a unique name for the new VM (or accept the default).

The name must be unique within the current Inventory folder, and can be up to 80 characters in length.

9. Click Next.

This displays the Disk Format page. The SD-WAN VPX-VW Virtual Machine requires 39.1 GB of disk space.
12. Accept the default settings, and click Next.

This proceeds to the **Network Mapping** page.
13. Accept the default (VM Network) and click Next.

This proceeds to the Ready to Complete page.
14. Click **Finish** to create the VM.

**Note**

Decompressing the disk image onto the server could take several minutes.

This displays the **Deploying Citrix NetScaler SD-WAN VPX** status dialog box.

Depending on the conditions present on your server, the deployment can take from several minutes to a few hours to complete. When the SD-WAN VPX Virtual Machine has been successfully created, a success message displays.
15. Click Close.

This closes the Deploy OVF Template wizard and returns to the vSphere Client main window. If this is the first VM you have created using this vSphere Client, the vSphere Client Home page displays. If you have previously created one or more VMs, the Inventory page displays.

The next step is to configure the SD-WAN VPX Management IP Address. The following section provides instructions for this procedure.
Configuring the Management IP Address for the SD-WAN VPX

October 04, 2016

There are two methods for assigning the Management IP Address to the SD-WAN VPX Virtual Machine:

- If you are not using DHCP: If you are not using DHCP, you must manually assign a static Management IP Address for the SD-WAN VPX Virtual Appliance. For instructions, see Manually Configuring a Static Management IP Address for the VPX.

- If you are using DHCP: By default, all SD-WAN VPX Virtual appliances use DHCP to acquire the Management IP Address. To use DHCP, the DHCP server must be present and available in the SD-WAN. For instructions on identifying the acquired Management IP Address, see Displaying the DHCP-assigned Management IP Address for the VPX.
Manually Configuring a Static Management IP Address for the VPX

Oct 04, 2016

If you are not using DHCP, or want to set a static Management IP Address for the SD-WAN VPX Virtual Appliance VM, you must do this manually. To do so, you will use the console for the Virtual Machine you just created, in the vSphere Client.

Also see, Setting up the SD-WAN Appliances.

To set the Management IP Address manually, do the following:

**Note**

DHCP is enabled by default for the SD-WAN VPX Management IP Address.

1. Continuing in the vSphere client **Inventory** page, select the new SD-WAN VPX VM in the Inventory tree (left pane).

   This displays the **Inventory** page for the new VM, with the **Getting Started** tab preselected.

2. **Power on the new Virtual Machine.**

   In the **Basic Tasks** section of the **Getting Started** tab page, click **Power on the virtual machine** (green play
button) to power on the new SD-WAN VPX-SE VM.

3. Select the **Console** tab in the **Inventory** page tab bar.

The Console tab is located in **Inventory** page tab bar at the top of the main page area. Selecting this tab displays and enables access to the CLI console for the VM.

![Console tab in vSphere Client](image)

As the new VM starts up, a series of status messages display in the console.
When the startup process completes, the console login prompt displays.

4. Click anywhere inside the console area to enter console mode.

   This turns control of your mouse cursor over to the VM console, and enables console mode.

**Note**

To release console control of your cursor, press the Ctrl and Alt keys simultaneously.

5. Log into the VM console.
The default login credentials for the new SD-WAN VPX-SE VM are as follows:

**Login:** admin  
**Password:** password

This displays the console **Welcome** screen.

6. Enter the following command line at the console prompt:

```
management_ip
```

This switches to the `management_ip` CLI in the console, and displays the `set_management_ip` prompt.
7. Configure the interface settings for the VM.

Enter the following command line at the `set_management_ip` prompt:

```
set interface <ipaddress> <subnetmask> <gateway>
```

Where:

- `<ip>` is the Management IP Address for the SD-WAN VPX-SE Virtual Appliance.
- `<subnetmask>` is the subnet mask used to define the network in which the CB VPX-VW Virtual Appliance resides.
- `<gateway>` is the Gateway IP Address the SD-WAN VPX-SE Virtual Appliance will use to communicate with external networks.

This stages but does not apply the interface settings.
8. Apply the staged settings for the VM interface.

Do the following:

a. Enter the following command at the `set_management_ip` prompt:

   `apply`

b. When prompted to confirm the `apply` operation, enter `Y`.

   This applies the staged interface settings for the VM, and displays the results.

9. Enter exit and press Return at the prompt to exit the management_ip CLI.

10. Exit the console.

   Enter **exit and press Return** at the console prompt, and then press **Ctrl+Alt** to regain control of the cursor.
11. Shut down and restart the VM.

   Do the following:

   a. Select the **Getting Started** tab to display the **Basic Tasks** options.

   ![Getting Started Tab](image1)

   b. In the **Basic Tasks** section, click **Shut down the virtual machine** (red box icon).

      You are prompted to confirm that you want to shut down the guest operating system for the VM.

   ![Confirm Shutdown](image2)

   c. Click **Yes** to confirm.

      This shuts down the guest operating system and powers off the VM. When the shutdown completes, the **Power on the virtual machine** option (green play button) becomes available.
12. Restart the Virtual Machine.

Click **Power on the virtual machine** (green right-arrow) to restart the VM. You can view the progress of the startup process in the **Console** tab page for the VM.

When the startup process completes, the login prompt displays.
You can now proceed to the final step, Connecting to the SD-WAN VPX-SE and Testing the Deployment.
Displaying the DHCP-assigned Management IP Address for the VPX

Oct 04, 2016
This section provides instructions for displaying and recording the DHCP-assigned Management IP Address for the new SD-WAN VPX-SE Virtual Appliance VM.

Note
By default, all SD-WAN VPX-SE Virtual Appliances use DHCP. If you are not using DHCP, or have assigned a static IP Address for the Virtual Appliance, you can skip this step. If you are using DHCP, the DHCP server must be present and available in the SD-WAN before you can complete this step.

To display the DHCP-assigned Management IP Address for the Virtual Appliance, do the following:

1. Continuing in the vSphere client Inventory page, select the new SD-WAN VPX-SE VM in the Inventory tree (left pane).

   This displays the Inventory page for the SD-WAN VPX-SE VM.

2. If you have not already done so, power on the new Virtual Machine.
In the **Basic Tasks** section, click the Play icon (green arrow) to power on the new SD-WAN VPX-SE VM.

3. Select the **Console** tab in the **Inventory** page tab bar.

   The **Console** tab is located in **Inventory** page tab bar at the top of the main page area. Selecting this tab displays and enables access to the CLI console for the VM.

4. Click anywhere inside the console area to enter console mode.

   This turns control of your mouse cursor over to the VM console, and enables console mode.

   **Note**

   To release console control of your cursor, press the **Ctrl** and **Alt** keys simultaneously.

5. Press **Enter** to display the console **login** prompt.

   Press **Enter** once or twice to display the console **login** prompt.
6. Log into the VM console.

The default login credentials for the new SD-WAN VPX-SE VM are as follows:

   **Login**: admin
   **Password**: password

This displays the console **Welcome** message, which includes the **Host IP Address**.

7. Record the Management IP Address for the SD-WAN VPX-SE VM.

---

**Note**

The DHCP server must be present and available in the SD-WAN, or this step cannot be completed.
After logging into the console, the Welcome message displays the *Last login* information and the *Host IP Address*. This IP Address is the Management IP Address for this new SD-WAN VPX-SE VM.

This completes the deployment of the SD-WAN VPX-SE Virtual Machine. The final step is to connect to the new SD-WAN VPX-SE and test the deployment. Instructions are provided in the next section.
Connecting to the SD-WAN VPX and Testing the Deployment

Oct 04, 2016
The next step is to connect to the new SD-WAN VPX-SE Virtual Appliance, to confirm that the deployment was successful.

To test the deployment, do the following:

1. On a connected PC, open a browser and enter the Management IP Address for the SD-WAN VPX-SE Virtual Appliance.

   You can use any PC connected to your network (for example, the local PC you used to deploy the SD-WAN VPX-SE Virtual Machine in the vSphere Client).

   If you have successfully assigned the Management IP Address for the SD-WAN VPX-SE, the Management Web Interface Login page displays.

2. Enter the Administrator user name and password, and click Login.

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

   **Note**
   It is strongly recommended that you change the default password as soon as possible. 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.

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 Virtual WAN Service is disabled, and the license has not been installed. For now, you can ignore this alert. The alert will be resolved automatically after you have installed the license, and completed the configuration and deployment process for the appliance.

You have now completed the initial installation and deployment of the SD-WAN VPX-SE Virtual Appliance. However, there are some remaining steps to complete the set-up process for the Virtual Appliance before adding it to your SD-WAN network. For instructions on completing the next step, please proceed to the section, Setting the Date and Time on an Appliance.
Setting up the Master Control Node (MCN) Site

Oct 04, 2016

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

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

The following CloudBridge Knowledge Base support articles are recommended:

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

- CloudBridge Virtual WAN Gateway Mode Deployment Steps (CTX201576)
  
  http://support.citrix.com/article/CTX201576

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

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

Instructions for each of these tasks are provided in the following sections.
Master Control Node (MCN)

Oct 04, 2016

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

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

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

![Diagram](https://docs.citrix.com)
How to Switch the Management Web Interface to MCN Console Mode

Oct 04, 2016

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

**Note**

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

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

1. Log into the Management Web Interface on the appliance you want to configure as the MCN.

2. Click **Configuration** in the main menu bar of the Management Web Interface main screen (blue bar at the top of the page).

3. In the navigation tree (left pane), open the **Appliance Settings** branch and click **Administrator Interface**.

   This displays the Administrator Interface page in the middle pane.

4. Select the **Miscellaneous** tab.

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

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

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

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

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

**Note**

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

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

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

![Image of confirmation dialog box](https://example.com)

6. Click OK.

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

Configuration ➤ Appliance Settings

**Switch Console Success**

- Your console has been switched.
- You will be automatically logged out in 2 seconds.

After the countdown completes, the session is terminated and the login page appears.
7. Enter the Administrator user name and password, and click Login.

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

After logging in, the Dashboard displays, now indicating that the appliance is in MCN mode.
The next step is to open a new configuration and add the MCN site to the Sites table, and begin configuring the new MCN site.
How to Add the MCN Site

Oct 04, 2016
The first step is to open a new configuration package, and add the MCN site to the new configuration.

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

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

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

1. In the navigation tree, open the Virtual WAN branch and select Configuration Editor.

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

This displays the Configuration Editor main page (middle pane).
2. Click **New** to start defining a new configuration.

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

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

This displays the **Add Site** dialog box.
4. Enter the site information.

Do the following:

a. Enter the **Site Name**, **Appliance Name**, and **Secure Key**.

b. Select the appliance **Model**.

**Note**

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

c. Select **primary MCN** as the mode.

**Note**

Entries cannot contain spaces and must be in Linux format.

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

This adds the new site to the **Sites** tree, and displays the **Basic Settings** configuration form for the new site.
6. Enter the basic settings for the new site, or accept the defaults.

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

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

**Note**

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

To save the current configuration package, do the following:

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

2. Enter the configuration package name.

   ![Save As dialog box](image)

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

3. Click **Save**.
How to Configure Virtual Interface Groups for the MCN Site

Oct 04, 2016
After adding the new MCN site, the next step is to create and configure the Virtual Interface Groups for the site.

The following are some guidelines for configuring Virtual Interface groups:

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

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

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

1. Continuing in the Sites tree of the Configuration Editor, click + next to the name of the site you just added.
   This opens the configuration branches for the new site.

2. Click + to the left of the Interface Groups branch.
   This displays the Interface Groups table for the site.

3. Click + to the right of Interface Groups.
   This adds a new blank group entry to the table and opens it for editing.
4. Select the Ethernet Interfaces to include in the group.

Under **Ethernet Interfaces**, click a box to include/exclude that interface. You can select any number of interfaces to include in the group. A goldenrod highlight indicates an included interface.

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

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

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

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

7. Click + at the left edge of the new blank entry.

This displays the **Virtual Interfaces** and **Bridge Pairs** tables.

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

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

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

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

10. Click + to the right of **Bridge Pairs**.

    This adds a new **Bridge Pairs** entry and opens it for editing.

11. Select the Ethernet interfaces to be paired from the drop-down menus.

    To add more pairs, click + next to **Bridge Pairs** again.

12. Click **Apply**.

    This applies your settings and adds the new Virtual Interface Group to the table.
Note

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

13. To add more Virtual Interface Groups, click + to the right of the Interface Groups branch, and proceed as above.
How to Configure Virtual IP Addresses for the MCN Site

Oct 04, 2016

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

1. Continuing in the Sites tree for the new MCN site, click + to the left of the Virtual IP Addresses branch.

   This displays the Virtual IP Addresses table for the new site.

2. Click + to the right of Virtual IP Addresses to add an address.

   This opens the form for adding and configuring a new Virtual IP Address.

3. Enter the Virtual IP Address / Prefix information, and select the Virtual Interface with which the address is associated.

   The Virtual IP Address must include the full host address and netmask.

   **Note**

   You can click + again to add more Virtual IP Address entries before applying your settings.
4. Click Apply.

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

5. To add more Virtual IP Addresses, click + to the right of the **Virtual IP Addresses** branch, and proceed as above.
How to Configure GRE Tunnels for the MCN Site (Optional)

Oct 04, 2016

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

To configure a GRE Tunnel, do the following:

1. Continuing in the site tree for the new MCN site, click $+$ to the left of the GRE Tunnels branch label.

   This opens the GRE Tunnels table for the new site.

2. Click $+$ to the right of the GRE Tunnels.

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

3. Configure the GRE Tunnel settings.

   Enter the following:

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

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

- **Source IP** – Select a source IP Address for the tunnel from the drop-down menu for this field. The menu options will be the list of Virtual Interfaces configured for this site. You must configure at least one Virtual Interface before you can configure a GRE Tunnel. For instructions, see Configuring the Virtual Interface Groups for the MCN Site and Configuring the Virtual IP Addresses for the MCN Site.

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

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

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

- **Keepalive Period(s)** – Enter the wait time interval (in seconds) between keepalive messages. If configured to 0, no keepalive packets will be sent, but the tunnel will remain up. The default is 10.

- **Keepalive Retries** – Enter the number of keepalive retries the Virtual WAN Appliance should attempt before it brings down the tunnel. The default is 3.

4. Click **Apply**.

   This submits your settings and adds the new GRE Tunnel to the table.

5. To configure additional GRE Tunnels, click **+** to the right of the **GRE Tunnels** branch label, and proceed as above.

   The next step is to configure the WAN links for the MCN site.
How to Configure WAN Links for the MCN Site

Oct 04, 2016
The next step is to configure the WAN links for the site.

1. Continuing in the site tree for the new MCN site, click the WAN Links branch label.

   **Note**
   At this point in a new configuration, there are no WAN links to form a table, and therefore no Open (+) icon to the left of the WAN Links branch. However, if links exist, the + active icon is available. If so, click + to the left of the WAN Links branch to display the table. This also reveals the Add (+), Edit (pencil), Delete (trashcan), and Help (?) active icons to the right of the WAN Links branch.

   This reveals the Add (+) and Help (?) active icons to the right of the WAN Links label.

2. Click + to the right of the WAN Links branch to add a new WAN link.

   This opens the Add WAN Link dialog box.
3. [Optional] Enter a name for the WAN Link if you do not want to use the default.

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

   -WL-<number>

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

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

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

5. Click Add.

   This displays the WAN Links table, adds the new unconfigured link to the table, and opens the Basic Settings configuration form for the link.
6. Click the Edit (pencil) icon to the right of the **Settings** branch label.

   This enables editing for the form, and reveals the **Apply** and **Close** buttons.

7. Enter the link details for the new WAN link.

   Some guidelines are as follows:

   - Some Internet links might be asymmetrical.
   - Misconfiguring the permitted speed can adversely affect performance for that link.
   - Avoid using burst speeds that surpass the Committed Rate.
   - For Internet WAN links, be sure to add the Public IP Address.

8. Click the grey **Advanced Settings** section bar.

   This opens the **Advanced Settings** form for the link.
9. Enter the Advanced Settings for the link.

Enter the following:

- **Provider ID** – (Optional) Enter a unique ID number from 1-100 to designate WAN Links connected to the same service provider. Virtual WAN uses the Provider ID to differentiate paths when sending duplicate packets.

- **Frame Cost (bytes)** – Enter the size (in bytes) of the header/trailer added to each packet; for example, the size in bytes of added Ethernet IPG or AAL5 trailers.

- **Congestion Threshold** – Enter the congestion threshold (in microseconds) after which the WAN link will throttle packet transmission to avoid further congestion.

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

10. Click the grey **Eligibility** section bar.

This opens the Eligibility settings form for the link.
11. Select the Eligibility settings for the link.

12. Click the grey Metered Link section bar.

This opens the Metered Link settings form for the link.

13. (Optional) Select Enable Metering to enable metering for this link.

This displays the Enable Metering settings fields.
14. Configure the metering settings for the link.

Enter the following:

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

15. Click **Apply**.

This applies your specified settings to the new WAN link.

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

16. Click + next to the **Access Interfaces** branch in the configuration tree for the link.

This opens the **Access Interfaces** table for the site.

17. Click + next to the **Access Interfaces** to add an interface.

This adds a blank entry to the table and opens it for editing.
18. Enter the **Access Interfaces** settings for the link.

**Note**

Each WAN link must have at least one Access Interface.

Enter the following:

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

  
  \[WAN\_link\_name-AI-number\]

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

**Note**

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

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

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

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

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

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

19. Click **Apply**.
This applies your settings and adds the new Access Interface entry to the **Access Interfaces** table.

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

The next step is to add and configure the routes for the site.
How to Configure Routes for the MCN Site

Oct 04, 2016
To add and configure the routes for the site, do the following:

1. Continuing in the Connections tree for the new MCN site, click + to the left of Routes.

   This displays the Routes table for the site.

   ![Routes Table](image)

2. Click + to the right of the Routes branch to add a route.

   This opens the Routes table for editing and adds a blank route entry to the table (top entry).

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

   Enter the following:

   - **Network IP Address** – Enter the Network IP Address.

   - **Cost** – Enter a weight from 1 to 15 for determining the route priority for this route. Lower-cost routes take precedence over higher-cost routes. The default value is 5.

   - **Service Type** – Select the service type for the route from the drop-down menu for this field. The options are as follows:
Virtual Path – This service manages traffic across the Virtual Paths. A Virtual Path is a logical link between two WAN links. It comprises a collection of WAN Paths combined to provide high service-level communication between two SD-WAN nodes. This is accomplished by constantly measuring and adapting to changing application demand and WAN conditions. SD-WAN Appliances measure the network on a per-path basis. A Virtual Path can be static (always exists) or dynamic (exists only when traffic between two SD-WAN Appliances reaches a configured threshold).

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

Intranet – This service manages Enterprise Intranet traffic that has not been defined for transmission across a Virtual Path. As with Internet traffic, it remains unencapsulated, and the SD-WAN manages bandwidth by rate-limiting this traffic relative to other service types during times of congestion. Note that under certain conditions, and if configured for Intranet Fallback on the Virtual Path, traffic that ordinarily travels by means of a Virtual Path may instead be treated as Intranet traffic, in order to maintain network reliability.

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

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

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

- Gateway IP Address – Enter the Gateway IP Address for this route.

4. Click + to the left of the new entry.

This opens the Eligibility Settings form for the route.
5. Enter the route **Eligibility** settings.

   The settings are as follows:

   - **Next Hop Site** – This indicates the remote site to which Virtual Path packets will be directed.

   - **Eligibility Based on Path** (checkbox) – (Optional) If enabled, the route will not receive traffic when the selected path is down.

   - **Path** – This specifies the path to be used for determining route eligibility.

9. Click **Apply**.

**Note**

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

10. To add more routes for the site, click + to the right of the **Routes** branch, and proceed as above.

You have now finished entering the primary configuration information for the new MCN site. The following two sections provide instructions for additional optional steps:

- **Configuring High Availability (HA) for the MCN Site (Optional).**

- **Enabling and Configuring Virtual WAN Security and Encryption (Optional).**

If you do not want to configure these features at this time, you can proceed directly to the section **Naming, Saving, and Backing Up the MCN Site Configuration.**
How to Configure High Availability (HA) for the MCN Site (Optional)

Dec 06, 2016

A SD-WAN High Availability (HA) configuration is a configuration in which two SD-WAN Appliances at a site serve in an Active/Standby partnership, for redundancy purposes.

Note
Before configuring High Availability for the primary MCN site, it is first best to add and configure the site that will act as the secondary MCN.

Important
Both appliances in an HA pair must be the same appliance model.

To configure High Availability for the MCN site, do the following:

1. Continuing in the Sites tree for the new MCN site, click + to the left of the High Availability branch for the site.

   This displays the High Availability configuration form.

   ![High Availability Configuration Form]

2. Click Edit (pencil icon) to the right of the High Availability branch to enable editing of the form.

3. Select the Enable High Availability check box.

   This enables High Availability for the site, and enables the first level of fields for configuring. A red asterisk ( * ) indicates a required field where you must enter a
4. Enter the basic **High Availability** parameter values for the HA pair.

Enter or select the following:

- **HA Appliance Name** – This is the name of the HA (secondary) appliance.

**Note**

To change or specify the mode for a site, open the Basic Settings branch for the site, and select the mode from the **Mode** drop-down menu. The options are: client, primary MCN, or secondary MCN.

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

- **Shared Base MAC** – This is the shared MAC Address for the HA pair appliances.

- **Swap Primary/Secondary** (checkbox) – When this is selected, if both appliances in the HA pair come up simultaneously, the secondary MCN appliance becomes the primary MCN appliance, and takes precedence.

- **Primary Reclaim** (checkbox) – When this is selected, the designated primary MCN appliance recovers control upon restart after a failover event.

5. Click + to the right of **HA IP Interfaces**.

This adds a new blank entry in the **HA IP Interfaces** table, and enables the entry for editing.
6. Enter the **HA IP Interfaces** information for the MCN site.

   Select or enter the following:
   
   - **Virtual Interface** – This is the Virtual Interface to be used for communication between the appliances in the MCN HA pair.
   
   - **Primary** – This is the unique Virtual IP Address for the primary MCN appliance. The secondary MCN uses this for communication with the primary MCN.
   
   - **Secondary** – This is the unique Virtual IP Address for the secondary MCN appliance. The primary MCN uses this for communication with the secondary MCN.

7. Click + to the left of the new **HA IP Interfaces** entry.

   This displays the **External Tracking** table, as shown in.
8. Click + to the right of **External Tracking**.

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

9. Enter the **External Tracker IP Address**.

   Enter the IP Address of the external device that will respond to ARP requests regarding the state of the primary MCN appliance.

10. Click **Apply**.

   This adds the new **High Availability** configuration settings to the MCN site configuration.
How to Enable and Configure Virtual WAN Security and Encryption (Optional)

Oct 04, 2016
To enable and configure Virtual WAN security and encryption, do the following:

**Note**

Enabling Virtual WAN security and encryption is optional.

1. At the top of the **Global** tree of the **Configuration Editor**, click + to the left of the **Virtual WAN Network Settings** branch.

   This opens the branch and displays the **Global Security Settings** configuration form.

2. Click Edit (pencil icon) to enable editing for the form.

3. Enter your global security settings.
The options are as follows:

- **Network Encryption Mode** – This is the encryption algorithm used for encrypted paths. Select one of the following from the drop-down menu: **AES 128-Bit** or **AES 256-Bit**.

- **Enable Encryption Key Rotation** – When enabled, encryption keys are rotated at intervals of 10 to 15 minutes.

- **Enable Extended Packet Encryption Header** – When enabled, a 16 byte encrypted counter is prepended to encrypted traffic to serve as an initialization vector, and randomize packet encryption.

- **Enable Extended Packet Authentication Trailer** – When enabled, an authentication code is appended to the contents of the encrypted traffic to verify that the message is delivered unaltered.

- **Extended Packet Authentication Trailer Type** – This is the type of trailer used to validate packet contents. Select one of the following from the drop-down menu: **32-Bit Checksum** or **SHA-256**.

4. Click **Apply** to apply your settings to the configuration.

This completes the configuration of the MCN site. The next step is to name and save the new MCN site configuration (optional, but strongly recommended), as described in the following section.

**Warning**
If your console session times out or you log out of the Management Web Interface before saving your configuration, any unsaved configuration changes will be lost. You must then log back into the system, and repeat the configuration procedure from the beginning. For that reason, it is strongly recommended that you save the configuration package often, or at key points in the configuration.
Naming, Saving, and Backing Up the MCN Site Configuration

Oct 04, 2016

The next step is to name and save the new configuration, referred to as a configuration package. This step is optional at this point in the configuration, but strongly recommended. The configuration package will be saved to your workspace on the local appliance. You then have the option to log out of the Management Web Interface and continue the configuration process at a later time. However, if you log out, you will need to reopen the saved configuration when you resume. Instructions for opening a saved configuration are provided in the section Loading a Saved Configuration Package into the Configuration Editor.

Warning

If the Console session times out or you log out of the Management Web Interface before saving your configuration, any unsaved configuration changes will be lost. You must then log back into the system, and repeat the configuration procedure from the beginning. For that reason, it is strongly recommended that you save the configuration package often, or at key points in the configuration.

Tip

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

1. Click Save As (at the top of the Configuration Editor middle pane).

   This opens the Save As dialog box.
2. Enter the configuration package name.

**Note**

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

3. Click **Save**.

**Note**

After saving the configuration file, you have the option to log out of the Management Web Interface and continue the configuration process at a later time. However, if you log out, you will need to reopen the saved configuration when you resume. Instructions are provided in the section, **Loading a Saved Configuration Package into the Configuration Editor**.

You have now completed the MCN site configuration, and created a new SD-WAN configuration package. You are now ready to add and configure the branch sites. Instructions are provided in **Adding and Configuring the Branch Sites**.
How to Export Backup Copy of the Configuration Package (Optional)

Jul 18, 2016

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

To export the current configuration package to your PC, do the following:

1. Click **Export**.

   This displays the **Export Configuration** dialog box.

2. Select **File Download** from the **Destination:** drop-down menu.

   This reveals the **Include Network Map** option, which is selected by default.

3. Accept the default, and click **Export**.

   This includes the **Network Map** information in the configuration package, and opens a file browser for specifying the name and location for saving the configuration.
4. Navigate to the save location on your PC and click **Save**.

This saves the configuration package to your PC.

**Note**

To recover a backed-up configuration package, you can use an **Import** operation to import the package from your PC and load it into the **Configuration Editor**. You can then save the imported package to your Management Web Interface workspace for future use. Instructions are provided in the section **Importing a Backed up Configuration Package into the Configuration Editor**.
How to Load Saved Configuration Package into the Configuration Editor

Jul 18, 2016
To resume work on a saved configuration package, you must first open the package and load it into the Configuration Editor.

To load a saved configuration package, do the following:

1. Log back into the Management Web Interface, and navigate to the Configuration Editor.

To open the Configuration Editor, do the following:

a. Select the Configuration tab at the top of the page to open the Configuration navigation tree (left pane).

b. In the navigation tree, click + to the left of the Virtual WAN branch to open that branch.

c. In the Virtual WAN branch, select Configuration Editor.

This opens the Configuration Editor main page for a new session.

If you have just logged back into the Management Web Interface, the Configuration Editor initially opens for a new session, with no configuration package loaded. You have the option of starting a new configuration (New), opening an existing saved configuration (Open), or importing (Import) and then opening (Open) a configuration previously backed up to your local PC.

2. Click Open.

This displays the Open Configuration Package dialog box.
3. Select the package to open from the **Saved Packages** drop-down menu.

**Note**

If you have just opened the **Configuration Editor**, it might take a few seconds or a minute or two for the **Saved Packages** menu to be populated, depending on the number of configurations you have saved to your workspace. If so, in the interim, the **Saved Packages** menu field might display the message **No saved packages**. If this occurs, click **Cancel** to close the dialog box, wait a few moments, and click **Open** again to reopen the dialog box.

4. Click **Open**.

**Note**

This opens the specified Configuration Package and loads it into the **Configuration Editor** for editing, only. This does not stage or activate the selected configuration to the local appliance.
How to Import Backed up Configuration Package into the Configuration Editor

Jul 18, 2016

In some cases, you might want to revert to an earlier version of a Configuration Package. If you have saved a copy of the earlier version to your local PC, you can import it back into the Configuration Editor, and then open it for editing. If this is not an initial deployment, you can also import an existing Configuration Package from the global Change Management inbox on the current MCN. Instructions for both of these procedures are provided below.

To import a Configuration Package, do the following:

1. Open the Configuration Editor.
   - To open the editor, do the following:
     a. Select the Configuration tab at the top of the page to open the Configuration navigation tree (left pane).
     b. In the navigation tree, click + to the left of the Virtual WAN branch to open that branch.
     c. In the Virtual WAN branch, select Configuration Editor.

2. In the Configuration Editor menu bar, click Import.

   A Virtual WAN Master Configuration consists of an Virtual WAN Configuration and one or more optional Network Maps. To get started, click New or Import an existing configuration (CFG) file.

   The Import Virtual WAN Configuration dialog box appears.
3. Select the location from which to import the package.

   - **To import a Configuration Package from Change Management:** Select the package from the From Change Management drop down menu (top left corner).

   - **To import a Configuration Package from your local PC:** Click Browse to open a file browser on your local PC. Select the file and click OK.

4. Select the import destination (if applicable).

   If a Configuration Package is already open in the Configuration Editor, then the Import to: drop down menu will be available.

   Select one of the following options:

   - **Current Package** - Select this to replace the contents of the currently opened Configuration Package with the contents of the imported package, and retain the name of the opened package. However, the contents of the saved version of the current package will not be overwritten until you explicitly save the modified package. If you use Save As to
save the package, select **Allow Overwrite** to enable overwriting of the previous version.

- **New Package** – Select this to open a new, blank Configuration Package, and populate it with the contents of the imported package. The new package automatically takes the same name as the imported package.

5. Specify which network maps to include (if applicable).

   If a Configuration Package is already open in the **Configuration Editor**, then the **Use Network Maps** drop-down menu will be available.

   Select one of the following options:

   - **Current Package** – This retains the network maps currently configured in the package currently open in the Configuration Editor, and discards any network maps from the imported package.
   
   - **New Package** – This replaces the network maps currently configured in the currently open package with the network maps (if any) from the imported package.
   
   - **Both Packages** – This includes all network maps from both the current and the imported package.

6. Click **Import**.

   This loads the imported file into the **Configuration Editor**, according to your specifications.

**Note**

If a package of the same name already exists in your workspace, then the **Name Conflict** dialog box displays.
To specify the name to use for the imported package, do one of the following:

- Enter a different name in the **Package Name** field to rename the new package and enable the **Import** button. The imported package is loaded into the **Configuration Editor** with the specified name. The package name is saved to your workspace at this time, but the package contents will not be saved to your workspace until you explicitly save the package.

- Select **Allow Overwrite** to confirm that you want to retain the existing name and enable overwriting of the contents of the saved package. However, the contents of the saved version of the current package will not be overwritten until you explicitly save the modified package.

This also enables the **Import** button in the **Name Conflict** dialog box. Click **Import** to complete the import operation.
Adding and Configuring the Branch Sites

Oct 04, 2016

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

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

Supplemental Branch Site Deployment Information

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

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

- CloudBridge Virtual WAN Gateway Mode Deployment Steps (CTX201576)
  http://support.citrix.com/article/CTX201576

Overview of Branch Site Configuration Procedures

The steps to complete this process are as follows:

1. Add the branch site.
2. Configure the Virtual Interface Groups for the branch site.
3. Configure the Virtual IP Addresses for the branch site.
4. (Optional) Configure the LAN GRE Tunnels for the branch site.
5. Configure the WAN Links for the branch site.
6. Configure the Routes for the branch site.
7. (Optional) Configure High Availability for the branch site.
8. (Optional) Clone the new branch site to create and configure additional sites.

Note

Cloning the site is optional. The Virtual WAN appliance models must be the same for both the original and the cloned sites. You cannot change the specified appliance model for a clone. If the appliance model is different for a site, you must manually add the site.
9. Resolve any configuration Audit Alerts.

10. Save the completed configuration.
How to Add the Branch Site

Oct 04, 2016
To add a new branch site to the Sites table and begin configuring the site, do the following:

Note
If you logged out of the MCN after creating and saving the new configuration package, you will need to log back in and reopen the configuration before you can continue. To do so, click Open in the Configuration Editor menu bar (top of page area). This displays a dialog box for selecting the configuration you want to modify.

1. Continuing in the Configuration Editor, click Add in the Sites bar to begin adding and configuring the new branch site.

   This displays the Add Site dialog box.

2. Enter the following site information.

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

- **Site Name** – Enter a name for the site.

- **Appliance Name** – Enter the name you want to assign to the appliance.

- **Secure Key** – This is a hexadecimal key of 8 to 32 digits used for encryption and membership verification in the SD-WAN Appliance. By default, this field is prefilled with an automatically generated security key. Accept the default or enter a custom key in hexadecimal format.
- **Model** – Select the appliance model from the drop-down menu.

- **Mode** – Select client as the mode.

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

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

![Basic Settings form](image)

4. Click the Edit (pencil) icon to enable editing for the form.

5. Enter the basic settings for the site, and click **Apply**.

   The next step is to add and configure the Virtual Interface Groups for the new site.
How to Configure Virtual Interface Groups for the Branch Site

Oct 04, 2016

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

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

1. In the **Sites** navigation tree, click + next to the name of the site you just added.
   
   This opens the configuration branches for the new site.

2. Click + to the left of the **Interface Groups** branch.
   
   This displays the **Interface Groups** table for the site.

3. Click + to the right of **Interface Groups**.
   
   This adds a new blank group entry to the table and opens it for editing.
4. Select the **Ethernet Interfaces** to include.

   Under **Ethernet Interfaces**, click a box to include/exclude that interface. You can select any number of interfaces to include in the group. A goldenrod highlight indicates an included interface.

5. Select the **Bypass Mode** and **Security level** from the drop-down menus.

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

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

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

7. Click + at the left edge of the new blank entry.

   This reveals the **Virtual Interfaces** and **Bridge Pairs** fields.
Tip
You can resize the tree pane to reveal any truncated contents. To do so, roll your cursor over the resize bar at the right edge of the tree area. When the cursor changes to a bi-directional arrow, click and drag the bar to the right or left to grow or shrink the pane width.

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

   This opens the **Name** and **VLAN ID** fields for editing.

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

10. Click + to the right of **Bridge Pairs**.

    This adds a new **Bridge Pairs** entry and opens it for editing.
11. Select the interfaces to be paired from the drop-down menus.

To add more pairs, click + next to the Bridge Pairs field again.

12. Click Apply.

This applies your settings and adds the new Virtual Interface Group to the table.

**Note**

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

13. To add more Virtual Interface groups, click + to the right of the Interface Groups branch, and proceed as above.
How to Configure Virtual IP Addresses for the Branch Site

Oct 04, 2016
The next step is to configure the Virtual IP Addresses for the site, and assign them to the appropriate group.

1. Continuing in the site tree for the new site, click + to the left of the Virtual IP Addresses branch.

   This displays the Virtual IP Addresses table for the new site.

   ![Virtual IP Addresses Table](image)

2. Click + to the right of the Virtual IP Addresses branch to add an address.

   This opens the form for adding and configuring a new Virtual IP Address.
3. Enter the **Virtual IP Address / Prefix** information, and select the **Virtual Interface** (Virtual Interface Group) with which the address is associated.

The Virtual IP Address must include the full host address and netmask.

**Note**

You can click + again to add more Virtual IP Address entries before applying your settings.

4. Click **Apply**.

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

5. To add more Virtual IP Addresses, click + to the right of the **Virtual IP Addresses** branch, and proceed as above.
How to Configure GRE Tunnels for the Branch Site

Oct 04, 2016

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

To configure a LAN GRE Tunnel for the branch site, do the following:

1. Continuing in the site tree for the new branch site, click + to the left of the LAN GRE Tunnels branch label.

   This opens the LAN GRE Tunnels table for the new site.

   ![LAN GRE Tunnels Table](image)

2. Click + to the right of the LAN GRE Tunnels.

   This adds a new blank LAN GRE Tunnel entry to the table and opens it for editing.

   ![Add LAN GRE Tunnel](image)

3. Configure the LAN GRE Tunnel settings.
Enter the following:

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

\[\text{Appliance-Tunnel-<number>}\]

Where `<number>` is the number of LAN GRE Tunnels configured for this site, incremented by one.

- **Source IP** – Select a Source IP Address for the tunnel from the drop-down menu for this field. The menu options will be the list of Virtual IP Addresses that you configured for this site. You must configure at least one Virtual Interface and one Virtual IP Address before you can configure a LAN GRE Tunnel. For instructions, see the sections, Configuring the Virtual Interface Groups for the Branch Site and Configuring the Virtual IP Addresses for the Branch Site.

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

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

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

- **Keepalive Period(s)** – Enter the wait time interval (in seconds) between keepalive messages. If configured to 0, no keepalive packets will be sent, but the tunnel will remain up. The default is 10.

- **Keepalive Retries** – Enter the number of keepalive retries the Virtual WAN Appliance should attempt before it brings down the tunnel. The default is 3.

4. Click **Apply**.

This submits your settings and adds the new LAN GRE Tunnel entry to the table.

5. To configure additional LAN GRE Tunnels, click + to the right of the **LAN GRE Tunnels** branch label, and proceed as above.

The next step is to configure the WAN links for the branch site.
How to Configure WAN Links for the Branch Site

Oct 04, 2016

1. Continuing in the site tree for the new site, click the **WAN Links** branch label.

   This reveals the Add (+) and Help (?) active icons to the right of the **WAN Links** branch.

2. Click + to the right of the **WAN Links** branch to add a new WAN link.

   This opens the **Add WAN Link** dialog box.

---

**Note**

At this point in a new configuration, there are no WAN links to form a table, and therefore no Open (+) icon to the left of the **WAN Links** branch label. However, if links exist, the + icon is available. If so, you can click + to the left of the **WAN Links** branch to display the table. This also reveals the Add (+), Edit (pencil), Delete (trashcan), and Help (?) active icons to the right of the **WAN Links** branch.
3. (Optional) Enter a name for the WAN Link if you do not want to use the default.

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

   \(-WL-\langle\text{number}\rangle\)

   Where \(<\text{number}\rangle\) is the number of WAN Links for this site, incremented by one.

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

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

5. Click **Add**.

   This displays the **WAN Links** table, adds the new un-configured link to the table, and opens the **Basic Settings** configuration form for the link.
Note

At this point, you will see some additional Audit Alerts (red dot icons) display in various sections of the WAN Links configuration form. This is because you have not yet configured the settings for the new WAN link. You can ignore these for now, as these will be resolved automatically as you complete the configuration of the new WAN link.

6. Click the Edit (pencil) icon to the right of the Settings branch to enable editing of the form.

   This enables editing for the form, and reveals the Apply and Close buttons.

7. Enter the path information for the new WAN link.

   Some guidelines are as follows:
   - Some Internet links might be asymmetrical.
   - Misconfiguring the permitted speed can adversely affect performance for that path.
   - Avoid using burst speeds that surpass the Committed Rate.
   - For Internet WAN link paths, be sure to add the Public IP Address.

8. Click the grey Advanced Settings section bar.
9. Enter the **Advanced Settings** for the link.

10. Click the grey **Eligibility** section bar.

This opens the **Eligibility** settings form for the link.
11. Select the **Eligibility** settings for the link.

12. Click the grey **Metered Link** section bar. This opens the **Metered Link** settings form for the link.

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

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

   - **Data Cap (MB)** – Enter the data cap allocation for the link, in megabytes.
- **Billing Cycle** – Select either **Monthly** or **Weekly** from the drop-down menu.

- **Starting From** – Enter the start date of the billing cycle.

- **Set Last Resort** – Select this to enable this link as a link of last resort in the event of a failure of all other available links. Under normal WAN conditions, Virtual WAN sends only minimal traffic over metered links, for the purpose of checking link status. However, in the event of a failure, Virtual WAN can use active metered links as a last resort for forwarding production traffic.

15. Click **Apply**.

This applies your specified settings to the new WAN link.

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

16. Click + next to the **Access Interfaces** branch in the configuration tree for the link.

This opens the **Access Interfaces** table for the site.

17. Click + to the right of the **Access Interfaces** branch to add an interface.

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

18. Enter the **Access Interfaces** settings for the link.
Enter the following:

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

  \[WAN\_link\_name-AI-number\]

  Where \(WAN\_link\_name\) is the name of the WAN link you are associating with this interface, and number is the number of Access Interfaces currently configured for this link, incremented by 1.

**Note**

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

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

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

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

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

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

19. Click **Apply**.

This applies your settings and adds the new Access Interface entry to the **Access Interfaces** table.

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

The next step is to add and configure the routes for the site.
How to Configure Routes for the Branch Site

Oct 04, 2016

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

1. Continuing in the site tree for the new site, click + to the left of the Routes branch.

   This displays the Routes table for the site.

```
<table>
<thead>
<tr>
<th>Network IP Address</th>
<th>Cost</th>
<th>Service Type</th>
<th>Gateway IP Address</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.105.32.8/20</td>
<td>5</td>
<td>Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>172.104.192.2/18</td>
<td>5</td>
<td>Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>16</td>
<td>Passthrough</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

2. Click + to the right of the Routes branch to add a route.

   This opens the Routes table for editing and adds a blank route entry to the table.

3. Enter the route configuration information and click Apply.
4. To add more routes for the site, click + to the right of the Routes branch, and proceed as above.

5. (Recommended.) Save your changes to the configuration.

Note

As an extra precaution, it is recommended that you use Save As, rather than Save, to avoid overwriting the wrong configuration package. Be sure to select Allow Overwrite before saving to an existing configuration, or your changes will not be saved.

You have now completed the required steps for configuring a client site. There are also some additional, optional steps you can choose to complete, before proceeding with the next phase of the deployment. A list of these steps and links to instructions are provided below. If you do not want to configure these features at this time, you can proceed directly to Preparing the Virtual WAN Appliance Packages on the MCN.

The optional steps are as follows:

- **Configure High Availability** – High Availability refers to a configuration in which two Virtual WAN Appliances at a site serve in an Active/Standby partnership capacity for redundancy purposes. If you are not implementing High Availability for this site, you can skip this step. For instructions, see Configuring High Availability (HA) for the Branch Site (Optional).

- **Clone the new branch site** – You have the option of cloning the branch site you just configured, and using that as a template for adding another site. The appliance models for the original site and the clone must be the same. For instructions, see Cloning the Branch Site (Optional).

- **Configure WAN Optimization** – If your CloudBridge Virtual WAN license includes WAN Optimization features, you have the option of enabling and adding these features to your configuration. To do so, you must complete the Optimization section in the Configuration Editor, and save the modified configuration. For instructions, proceed to Enabling and Configuring WAN Optimization.
How to Configure High Availability (HA) for the Branch Site (Optional)

Oct 04, 2016
To configure High Availability for the branch site, do the following:

1. Continuing in the Sites tree, click + to the left of the High Availability branch for the new site.

   This displays the High Availability configuration form.

   ![High Availability Configuration Form]

2. Click Edit (pencil icon) to the right of the High Availability branch to enable editing of the form.

3. Select the Enable High Availability check box.

   This enables High Availability for the site, and enables the first level of fields for configuring. A red asterisk (*) indicates a required field where you must enter a non-default value.
4. Enter the basic **High Availability** parameter values for the HA pair.

   Enter or select the following:

   - **HA Appliance Name** – This is the name of the HA (secondary) client appliance.

   **Note**

   To change or specify the mode for a site, open the **Basic Settings** branch for the site, and select the mode from the **Mode** drop-down menu. The options are: **client**, **primary MCN**, or **secondary MCN**. For a branch site appliance, select **client** as the mode.

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

   - **Shared Base MAC** – This is the shared MAC Address for the HA pair appliances.

   - **Swap Primary/Secondary** (checkbox) – When this is selected, if both appliances in the HA pair come up simultaneously, the secondary client appliance becomes the primary client appliance for the site, and takes precedence.

   - **Primary Reclaim** (checkbox) – When this is selected, the designated primary client appliance recovers control upon restart after a failover event.

5. Click + to the right of **HA IP Interfaces**.

   This adds a new blank entry in the **HA IP Interfaces** table, and enables the entry for editing.
6. Enter the HA IP Interfaces information for the branch site.

Select or enter the following:

- **Virtual Interface** – This is the Virtual Interface to be used for communication between the appliances in the HA appliance pair.

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

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

7. Click + to the left of the new **HA IP Interfaces** entry.

This displays the **External Tracking** table.
8. Click + to the right of External Tracking.

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

9. Enter the External Tracker IP Address.

Enter the IP Address of the external device that will respond to ARP requests regarding the state of the primary client.
appliance.

10. Click **Apply**.

This adds the new **High Availability** configuration settings to the branch site configuration.
How to Clone the Branch Site (Optional)

Oct 04, 2016

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

**Note**

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

Cloning a site streamlines the process of adding and configuring additional branch nodes. When a site is cloned, the entire set of configuration settings for the site are copied and displayed in a single form page. You can then modify the settings according to the requirements of the new site. Some of the original settings can be retained, where applicable. However, most of the settings must be unique for each site.

To clone a site, do the following:

1. In the Sites tree (middle pane) of the Configuration Editor, click + to the left of the branch site you want to duplicate.

   This opens that site branch in the Sites tree, and reveals the Clone button (double page icon) and Delete button (trashcan icon).

2. Click the **Clone** icon to the right of the branch site name in the tree.

   This opens the **Clone Site** configuration page.
3. Enter the configuration parameter settings for the new site.

A pink field with an Audit Alert icon (red dot) indicates a required parameter setting that must have a value different than the setting for the original cloned site. In most cases, this value must be unique.

**Tip**

To further streamline the cloning process, use a consistent, pre-defined naming convention when naming the clones.

4. Resolve any Audit Alerts.

To diagnose an error, roll your cursor over the Audit Alert icon (red dot or goldenrod delta) to reveal bubble help for that specific alert.

5. Click **Clone** (far right corner) to create the new site and add it to the **Sites** table.

**Note**

The **Clone** button remains unavailable until you have entered all of the required values, and the new site configuration is error-free.

6. (Optional) Save your changes to the configuration.
Note

As an extra precaution, it is recommended that you use **Save As**, rather than **Save**, to avoid overwriting the wrong configuration package. Be sure to select **Allow Overwrite** before saving to an existing configuration, or your changes will not be saved.

Repeat the steps up to this point for each branch site you want to add.

After you have finished adding all of the sites, the next step is to check the configuration for Audit Alerts, and make corrections or additions as needed.
How to Resolve Configuration Audit Alerts

Oct 04, 2016

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

Resolving all of the Audit Alerts (if any), completes the Sites phase of the configuration. The next step is to save the completed Sites configuration.
How to Save the Completed Sites Configuration

Oct 04, 2016

The next step is to save the completed Sites configuration. The configuration will be saved to your workspace on the local appliance.

Warning

If the console session times out or you log out of the Management Web Interface before saving your configuration, any unsaved configuration changes will be lost. You must then log back into the system, and repeat the configuration procedure from the beginning. For that reason, it is strongly recommended that you save the configuration package often, or at key points in the configuration.

Note

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

To save the current configuration package, do the following:

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

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

3. Click **Save**.

Note
After saving the configuration file, you have the option to log out of the Management Web Interface and continue the configuration process at a later time. However, if you log out, you will need to reopen the saved configuration when you resume. Instructions are provided in the section **Loading a Saved Configuration Package into the Configuration Editor**.

The next step is to configure the Virtual Paths and Virtual Path Service between the MCN and the client sites. Instructions are provided in the Configuring the Virtual Path Service Between the MCN and Client Sites.
Deployment Use Cases

Mar 30, 2017
Following are some of the use case scenarios implemented by using NetScaler SD-WAN appliances:

- Deploying SD-WAN in Gateway Mode
- Deploying SD-WAN in PBR mode (Virtual Inline Mode)
- Dynamic Paths for Branch to Branch Communication
- Static WAN Paths
- Building an SD-WAN Network
- Routing for LAN Segmentation
- Utilizing Enterprise Edition Appliance to Provide WAN Optimization Services Only
Deploying SD-WAN in Gateway Mode

Nov 24, 2016

To deploy SD-WAN in a Gateway Mode:

This article provides step-by-step procedure to configure a SD-WAN appliance in Gateway mode in a sample network setup. Inline deployment is also described for the branch side to complete the configuration.

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

Note

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

Topology

DataCenter in Gateway Deployment

Branch in Inline Deployment
Deployment Requirements

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

<table>
<thead>
<tr>
<th>Site Name</th>
<th>DataCenter Site</th>
<th>Branch Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Name</td>
<td>A_DC1</td>
<td>A_BR1</td>
</tr>
<tr>
<td>Management IP</td>
<td>172.30.2.10/24</td>
<td>172.30.2.20/24</td>
</tr>
<tr>
<td>Security Key</td>
<td>If any</td>
<td>If any</td>
</tr>
<tr>
<td>Model/Edition</td>
<td>4000</td>
<td>2000</td>
</tr>
<tr>
<td>Mode</td>
<td>Gateway</td>
<td>Inline</td>
</tr>
<tr>
<td>Topology</td>
<td>2 x WAN Path</td>
<td>2 x WAN Path</td>
</tr>
</tbody>
</table>
| VIP Address     | 192.168.10.9/24 – MPLS  
10.0.10.9/24 – Internet (Public IP – A.B.C.D)  
192.168.30.1/24 - LAN | 192.168.20.9/24 - MPLS  
10.0.20.9/24 – Internet (Public IP – W.X.Y.Z) |
| Gateway MPLS    | 192.168.10.1    | 192.168.20.1 |
| Gateway Internet| 10.0.10.1       | 10.0.20.1   |
| Link Speed      | MPLS – 100 Mbps  
Internet – 20 Mbps | MPLS – 10 Mbps  
Internet – 2 Mbps |
| Route           | Network IP Address - 192.168.31.0/24  
Service Type - Local  
Gateway IP Address - 192.168.30.2 | If any |
| VLANs           | If any          | If any      |

Configuration Pre-requisites
Enable SD-WAN appliance as a Master Control Node
Configuration is done only on the Master Control Node (MCN) of the SD-WAN appliance.

To enable an appliance as a Master Control Node:

1. In the NetScaler SD-WAN web management interface, navigate to **Configuration > Appliance Settings > Administrator Interface > Miscellaneous tab > Switch Console**.

   **Note**

   If "Switch to Client Console" is displayed, then the appliance is already in MCN mode. There should only be one active MCN in a SD-WAN network.

2. Start Configuration by navigating to **Configuration > Virtual WAN > Configuration Editor**. Click the **New** to begin configuration.

   **Datacenter Site Gateway Mode Configuration**

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

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

   **To create a new DC site**

   1. Navigate to **Configuration Editor - > Sites**, and click the "+" **Add** button.
   2. Populate the fields as shown below.
   3. Keep default settings unless instructed to change.
To configure interface groups based on connected Ethernet interfaces

1. In the Configuration Editor, navigate to Sites → [Site Name] → Interface Groups. Click “+” to add interfaces intended to be used. For Gateway Mode, each Interface Group is assigned a single Ethernet interface.
2. Bypass mode is set to fail-to-block since only one Ethernet/physical interface is used per virtual interface. There are also no Bridge Pairs.
3. In this example three Interfaces Groups are created, one facing the LAN and two others facing each respective WAN Link. Refer to the sample “DC Gateway Mode” topology above and populate the Interface Groups fields as shown below.

To create Virtual IP (VIP) address for each virtual interface

1. Create a VIP on the appropriate subnet for each WAN Link. VIPs are used for communication between two SD-WAN appliances in the Virtual WAN environment.
2. Create a Virtual IP Address to be used as the Gateway address for the LAN network

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

1. Navigate to WAN Links, click the “+” button to add a WAN Link for the Internet link.
2. Populate Internet link details, including the supplied Public IP address as shown below. Note that **AutoDetect Public IP** cannot be selected for SD-WAN appliance configured as MCN.

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

4. Populate Access Interface for IP and gateway addresses as shown below.

---

To create MPLS Link

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

2. Populate MPLS link details as shown below.

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

4. Populate Access Interface for IP and gateway addresses as shown below.
To populate Routes

Routes are auto-created based on the above configuration. The DC LAN sample topology shown above has an additional LAN subnet which is 192.168.31.0/24. A route needs to be created for this subnet. Gateway IP address must be in the same subnet as the DC LAN VIP as shown below.

Branch Site Inline Deployment Configuration

Following are the high-level configuration steps to configure Branch site for Inline deployment:

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

To create a new Branch site

1. Navigate to Configuration Editor - > Sites, and click the “+” Add button.
2. Populate the fields as shown below.
3. Keep default settings unless instructed to change.
To populate interface groups based on connected Ethernet interfaces

1. In the Configuration Editor, navigate to Sites → [Client Site Name] → Interface Groups. Click “+” to add interfaces intended to be used. For Inline Mode, each Interface Group is assigned two Ethernet interfaces.
2. Bypass mode is set to fail-to-wire and Bridge Pair is created using the two Ethernet interfaces.
3. Refer to the sample “Remote Site Inline Mode” topology above and populate the Interface Groups fields as shown below.

To create Virtual IP (VIP) address for each virtual interface

1. Create a Virtual IP address on the appropriate subnet for each WAN Link. VIPs are used for communication between two SD-WAN appliances in the Virtual WAN environment.
To populate WAN links based on physical rate and not on burst speeds using Internet link

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

To create MPLS Link

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

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

Resolving Audit Errors

After completing configuration for DC and Branch sites, you will be alerted to resolve audit error on both DC and BR sites.

By default, the system will generate paths for WAN Links defined as access type Public Internet. You would be required to use the auto-path group function or enable paths manually for WAN Links with an access type of Private Internet. Paths
for MPLS links can be enabled by clicking on the Add operator (in the green rectangle).

After completing all the above steps, proceed to Preparing the SD-WAN Appliance Packages on the MCN topic.
Deploying SD-WAN in PBR mode (Virtual Inline Mode)

Aug 17, 2017

In virtual inline mode, the router uses policy based routing rules to redirect incoming and outgoing WAN traffic to the appliance, and the appliance forwards the processed packets back to the router.

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

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

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

Gathering Information for Configuration

- Accurate network diagram (example diagram show below) of your local and remote site(s) including:
  - Local and Remote WAN links and their bandwidths in both directions, their subnets, Virtual IP Addresses and Gateways from each link, Routes, and VLANs.
- Deployment Table (example diagram shown below)

Data Center Topology – PBR mode (Virtual Inline Mode)

Branch Topology – Inline Mode
<table>
<thead>
<tr>
<th>Site Name</th>
<th>DataCenter Site</th>
<th>Branch Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Name</td>
<td>A_DC1</td>
<td>A_BR1</td>
</tr>
<tr>
<td>Management IP</td>
<td>172.30.2.10/24</td>
<td>172.30.2.20/24</td>
</tr>
<tr>
<td>Security Key</td>
<td>If any</td>
<td>If any</td>
</tr>
<tr>
<td>Model/Edition</td>
<td>4000</td>
<td>2000</td>
</tr>
<tr>
<td>Mode</td>
<td>PBR mode (Virtual Inline Mode)</td>
<td>Inline</td>
</tr>
<tr>
<td>Topology</td>
<td>2 x WAN Path</td>
<td>2 x WAN Path</td>
</tr>
<tr>
<td>VIP Address</td>
<td>192.168.1.10/24 – MPLS</td>
<td>10.17.0.9/24 – MPLS</td>
</tr>
<tr>
<td></td>
<td>192.168.1.11/24 – Internet *Public IP w.x.y.z</td>
<td>10.18.0.9/24 – Internet *Public IP a.b.c.d</td>
</tr>
<tr>
<td>Gateway MPLS</td>
<td>10.20.0.1</td>
<td>10.17.0.1</td>
</tr>
<tr>
<td>Gateway Internet</td>
<td>10.19.0.1</td>
<td>10.18.0.1</td>
</tr>
<tr>
<td>Link Speed</td>
<td>MPLS – 100 Mbps</td>
<td>MPLS – 10 Mbps</td>
</tr>
<tr>
<td></td>
<td>Internet – 20 Mbps</td>
<td>Internet – 2 Mbps</td>
</tr>
<tr>
<td>Route</td>
<td>Need to add a route on the SD-WAN SE Appliance on how to reach the LAN Subnets (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, etc) through any of the physical interfaces: Gi0/1 – 192.168.1.1</td>
<td>No additional routes were added</td>
</tr>
<tr>
<td></td>
<td>Configuration &gt; Virtual WAN &gt; Configuration Editor &gt; SJC_DC &gt; Routes. In this example interface 192.168.1.1 was used:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n/w address: 10.10.13.0/24, 10.10.12.0/24, 10.10.11.0/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• service type: local</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• gateway IP address: 192.168.1.1</td>
<td></td>
</tr>
</tbody>
</table>
Steps to configure a site in Virtual Inline Mode:

<table>
<thead>
<tr>
<th>Site Name</th>
<th>Branch Site</th>
</tr>
</thead>
</table>

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

Configuration Pre-requisites

- Enable SD-WAN appliance as a Master Control Node.
- Configuration is done only on the Master Control Node (MCN) of the SD-WAN appliance.

To enable an appliance as a Master Control Node:

1. In the NetScaler SD-WAN web management interface, navigate to Configuration > Appliance Settings > Administrator Interface > Miscellaneous tab > Switch Console.

Note

If "Switch to Client Console" is displayed, then the appliance is already in MCN mode. There should only be one active MCN in a SD-WAN network.

2. Enable Virtual WAN Service.

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

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

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

Datacenter Site PBR Mode Configuration

To create a new DC site

1. Navigate to Configuration Editor - > Sites, and click the "+" Add button.
2. Populate the fields as shown below.
3. Keep default settings unless instructed to change.

To configure interface groups based on connected Ethernet interfaces

1. In the Configuration Editor, navigate to Sites -> [Site Name] -> Interface Groups. Click "+" to add interfaces intended to be used. In PBR mode, configuration on only a single Ethernet interface is used i.e. interface connecting the upstream router providing PBR policy implications (Example- Interface 1/1).
2. Bypass mode is set to fail-to-block since only one Ethernet/physical interface is used per virtual interface. There are also no Bridge Pairs.
3. In this example, expand Virtual Interfaces + option and configure the Virtual Interfaces.
To create Virtual IP (VIP) address for each virtual interface

1. Create a **Virtual IP Address** on the appropriate subnet for each WAN Link. VIPs are used for communication between two SD-WAN appliances in the Virtual WAN environment.
To populate WAN links based on physical rate and not on burst speeds using Internet and MPLS link:

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

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

The Proxy ARP is not checked for less than two Ethernet interfaces.

To populate Routes

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

0/1/0.1 – 192.168.1.1 on VLAN 10

0/1/0.2 – 192.168.2.1 on VLAN 20
Following are the high-level configuration steps to configure Branch site for Inline deployment:
1. Create a new Branch site.

2. Populate Interface Groups based on connected Ethernet interfaces.

3. Create Virtual IP address for each virtual interface.

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

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

To populate interface groups based on connected Ethernet interfaces

1. In the Configuration Editor, navigate to Sites → [Client Site Name] → Interface Groups. Click “+” to add interfaces intended to be used. For Inline mode configuration, four Ethernet interface are used; interface pair 1/3, 1/4 and interface pair 1/1 and 1/2.

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

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

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

4. Refer to the sample “Remote Site Inline Mode” topology above and populate the Interface Groups fields as shown below.
To create Virtual IP (VIP) address for each virtual interface

1. Create a Virtual IP address on the appropriate subnet for each WAN Link. VIPs are used for communication between two SD-WAN appliances in the Virtual WAN environment.

To populate WAN links based on physical rate and not on burst speeds using Internet link
1. Navigate to **WAN Links**, click the “+” button to add a WAN Link for the Internet link.
2. Populate Internet link details, including the **AutoDetect Public IP address** as shown below.
3. Navigate to **Access Interfaces**, click the “+” button to add interface details specific for the Internet link.
4. Populate Access Interface for Virtual IP address and gateway as shown below.

---

To create MPLS Link

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

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

Resolving Audit Errors

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

Note: By default the system will generate paths for WAN Links defined as access type Public Internet (highlighted).
By default, the system will generate paths for WAN Links defined as access type Public Internet. You would be required to use the auto-path group function or enable paths manually for WAN Links with an access type of Private Internet. Paths for MPLS links can be enabled by clicking on the Add operator (in the green rectangle).

Create an Autopath Group

1. Click on the [+] sign next to Autopath Groups.
2. Configure the Autopath Group created as per requirement and click Apply.
3. Rename the Autopath Group [Optional].

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

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

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

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

After manually adding the virtual paths for WAN links with access type Private Intranet, it gets populated under Paths (highlighted).
After completing all the above steps, proceed to Preparing the SD-WAN Appliance Packages on the MCN topic.

**Policy Based Routing configuration on the PBR Router**

**Interface connected to the LAN**

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

**Interface connect to the MPLS WAN Link**

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

**Interface connected to the INET WAN Link**

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

Note: Interface GigabitEthernet0/1 on the PBR router is connected to the SD-WAN port 1/1, it is in 1-arm mode and this one port will serve traffic for MPLS and INET links.
Router# configure terminal
Router(config)# interface GigabitEthernet0/1
Router(config-if)# description To-SDWAN-link
Router(config-if)# ip address 192.168.1.1 255.255.255.0

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

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

Router# configure terminal
Router(config)# ip route 10.17.0.0 255.255.255.0 10.20.0.1
Router(config)# ip route 10.18.0.0 255.255.255.0 10.19.0.1

Route Map Definition

Access Control List Configuration:

Configure ACL's to define the traffic to be sent to and from the SD-WAN appliance.

1- From LAN to SD-WAN Appliance

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

- Router# configure terminal
  Router(config)# ip access-list extended server_side
  Router(config)# permit ip 10.10.0.0 0.0.255.255 any

2- From SD-WAN Appliance to physical WAN Links

- Router# configure terminal
  Router(config)# ip access-list extended MPLS_Link
  Router(config)# permit ip 192.168.1.10 0.0.0.0 any
  Router# configure terminal
  Router(config)# ip access-list extended INET_Link
  Router(config)# permit ip 192.168.1.11 0.0.0.0 any

Route Map Configuration:

Define the route-map matching the ACL's.

Route map for LAN traffic:

Next hop will be any of SD-WAN Virtual IP's (VIP).

MPLS VIP 192.168.1.10
INET VIP 192.168.1.11
In this case, we chose MPLS VIP 192.168.1.10 as next hop and also added a health check to make sure if the SD-WAN fails, traffic is not routed to it.

```
Router# configure terminal
Router(config)# route-map server_side_VW_PBR permit 10
Router(config-route-map)# match ip address server_side
Router(config-route-map)# set ip next-hop verify-availability 192.168.1.10 10 track 123
```

Note: The above command configures the route map to verify the reachability of the tracked object. The tracking process provides the ability to track individual objects, such as ICMP ping reachability, routing adjacency, an application running on a remote device, a route in the Routing Information Base (RIB) or to track the state of an interface line protocol.

**Route map for WAN traffic:**

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

```
Router# configure terminal
Router(config)# route-map WAN_VW_PBR permit 20
Router(config-route-map)# match ip address MPLS_Link
Router(config-route-map)# set ip next-hop verify-availability 10.20.0.1 20 track 124
Router# configure terminal
Router(config)# route-map WAN_VW_PBR permit 30
Router(config-route-map)# match ip address INET_Link
Router(config-route-map)# set ip next-hop verify-availability 10.19.0.1 30 track 125
```

**Apply the Route Map to the interface:**

```
Router# configure terminal
Router(config)# interface FastEthernet0/1
Router(config-if)# ip policy route-map server_side_VW_PBR
Router(config-if)# duplex auto
Router(config-if)# speed auto
Router# configure terminal
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip policy route-map WAN_VW_PBR
Router(config-if)# duplex auto
Router(config-if)# speed auto
```

**MPLS Router Configuration (Gateway 10.20.0.1)**

- Add route on MPLS router to reach MPLS VWAN VIP on the Data Center.
- MPLS VIP subnet 192.168.1.0/24 via next hop PBR router MPLS link 10.20.0.2
- Router# configure terminal
- Router(config)# ip route 192.168.1.0 255.255.255.0 10.20.0.2

**Firewall Configuration (Gateway 10.19.0.1)**

Add route on Firewall to reach INET VWAN VIP on the Data Center.

INET VIP subnet 192.168.10/24 via next hop PBR router INET link 10.19.0.2
• Router# configure terminal
• Router(config)# ip route 192.168.1.0 255.255.255.0 10.19.0.2
To build an SD-WAN overlay network without the need to statically build SD-WAN overlay route tables:

1. Create a WAN Path tunnel across each WAN link between two SD-WAN appliances.

2. Configure Virtual IP to represent the endpoint for each WAN link. You can establish encrypted WAN paths through the current L3 Network.

3. Aggregate 2, 3, and 4 WAN paths (physical links) into a single Virtual Path allowing packets to traverse the WAN utilizing the SD-WAN overlay network instead of the existing underlay which is least intelligent and cost inefficient.

**SD-WAN Routing Components and Network Topology**

- Local – subnet resides at this site (advertised to SD-WAN environment)
- Virtual Path – sent through Virtualized Path to the selected site appliance
- Intranet – sites with no SD-WAN appliance
- Internet – internet bound traffic
- Pass-through – untouched traffic, in one bridge interface out the other
- Default route (0.0.0.0/0) defined. Used for pass-through traffic not captured by the SD-WAN overlay route table, or utilized at the MCN to instruct clients sites to forward all traffic back to MCN node for back-haul of internet traffic.
Dynamic Paths for Branch to Branch Communication

Aug 25, 2017

With demand for VoIP and video conferencing, the traffic is increasingly moving between offices. It is inefficient to set up full mesh connections through datacenters which can be time consuming.

With NetScaler SD-WAN, you do not need to configure paths between every office. You can enable the Dynamic Path feature and the SD-WAN solution automatically creates paths between offices on demand. The session initially uses an existing fixed path. And as bandwidth and time threshold is met, a path is created dynamically if that new path has better performance characteristics than the fixed path. Session traffic is transmitted through the new path. This results in efficient usage of resources. Paths exist only when they are needed and reduce the amount of traffic getting transmitted to and from the datacenter.

Additional benefits of SD-WAN network include:

- Bandwidth and PPS thresholds to allow branch to branch connections
- Reduce bandwidth requirements in and out of data center while minimizing latency
- Paths created on demand depend on set thresholds
- Dynamically release network resources when not required
- Reduce load on the Master Control Node and latency

Branch to Branch Communication Using Dynamic Paths

SD-WAN Network with Dynamic Path

- Dynamic virtual paths are used for large scale deployments, such as Enterprises
● Smaller deployments use Static virtual paths and any-to-any virtual paths
● Always use Static virtual paths between two Data Centers (DC to DC)
● Not all WAN paths need to be configured for using Dynamic virtual path
● Each SD-WAN appliance has limited number of Dynamic virtual paths (8 dynamic lowest limit, 8 static lowest limit = total 16) that can be configured.

How to Enable Dynamic Virtual Path in the SD-WAN GUI

To enable dynamic virtual paths:

1. In the NetScaler SD-WAN GUI, go to Configuration > Virtual WAN > Configuration Editor.
   a) Enable WAN to WAN Forwarding to enable the site to serve as a proxy for multi-hop site to site.
   b) Enable Site as Intermediate Node
3. Navigate to Connections > Remote Site > WAN to WAN Forwarding.
   a) Enable WAN to WAN Forwarding to enable the site to serve as a proxy for multi-hop site to site.
   a) Enable Dynamic Virtual Paths.
   b) Set the maximum number of dynamic paths.
How to Create a Dynamic Virtual Path

- Configuration determines when a Dynamic Virtual Path is active or down.
- Configure sample packet count (pps) or bandwidth (kbps) within a timeframe.
- Can be set Globally or with WAN Link configured at the Intermediate Node.
Configuring Static WAN Paths

Nov 24, 2016

With WAN to WAN enabled on the MCN, remote site routes are advertised by MCN.

- Clients are aware of MCN local routes as well as other client site routes
- From client perspective, all routes are considered as MCN routes

When WAN-to-WAN forwarding is not enabled on the MCN, Branch to Branch communication issues are encountered in the customer network.

SD-WAN appliances running in client mode are not aware of other branches subnets until WAN-to-WAN forwarding is enabled on MCN. Once this option is enabled, branch SD-WAN nodes become aware of other branch subnets and all the traffic destined to other branches is forwarded to MCN. MCN routes it to the correct destination.
Routing Support for LAN Segmentation

Nov 24, 2016

The SD-WAN Standard and Enterprise Edition appliances implement LAN segmentation across distinct sites where either appliance is deployed. The appliances recognize and maintain a record of the LAN side VLANs available, and configure rules around what other LAN segments (VLANs) can connect to at a remote location with another SD-WAN Standard or Enterprise Edition appliance.

The above capability is implemented through the use of a Virtual Routing and Forwarding (VRF) table that is maintained in the SD-WAN Standard or Enterprise Edition appliance, which keeps track of the remote IP address ranges accessible to a local LAN segment. This VLAN-to-VLAN traffic would still traverse the WAN through the same pre-established Virtual Path between the two appliances (no new paths need to be created).

An example use case for this functionality is that a WAN administrator may be able to segment local branch networking environment through a VLAN, and provide some of those segments (VLANs) access to DC-side LAN segments that have access to the internet, while others may not obtain such access. The configuration of the VLAN-to-VLAN associations is achieved through the MCN's Configuration Editor in the SD-WAN management web interface.
Utilizing Enterprise Edition Appliance to Provide WAN Optimization Services Only

Nov 24, 2016

The SD-WAN Enterprise Edition appliances contain fully featured WAN Optimization functionality in addition to WAN Virtualization. Some customers prefer to implement WAN Optimization functionality before migrating to SD-WAN services. This deployment use case provides the steps to utilize Enterprise Edition appliances to utilize WAN optimization services.

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

- SD-WAN: SD-WAN Standard Edition appliance
- Enterprise: SD-WAN Enterprise Edition appliance
- WANOP: SD-WAN WANOP Edition appliance

To integrate Enterprise Edition appliances into an existing distributed WANOP network, you need to configure SD-WAN (Physical or Virtual) appliance at the DC site as the MCN. The SD-WAN appliance manages all configuration of the network. A Virtual Path is established between the Branch site and MCN at the DC site. This Virtual Path is only used for sending control traffic between the appliances. At the branch appliance, the data traffic is processed as an intranet service. The intranet traffic is not encapsulated and traverses over existing WAN link to reach the DC site. A WANOP appliance at the DC site needs to be in the traffic path to provide end-to-end traffic optimization.

For customer sites that do not have SD-WAN hardware appliance at the head-end, VPX appliances in a HA pair (two Virtual WAN VPXs) can be used as MCN in one-arm mode. For the one-arm mode, PBR rules on the third-party router are required to redirect traffic to the SD-WAN appliance.

This document assumes that the DC site appliances are deployed in HA mode for redundancy. However, note that HA mode is not mandatory for this deployment.

Prerequisites

- A pair of WANOP appliances and a pair of SD-WAN appliances deployed in HA mode at the DC site.
- An Enterprise Edition appliance at the Branch site.

Network Topology

SD-WAN Standard Edition and WANOP Appliances in PBR Deployment

In the below illustration, both the SD-WAN SE and WAN OP appliances at the DC site are deployed in one-arm mode. The SD-WAN appliance supports PBR deployment while the WANOP appliance supports both PBR and WCCP. The control traffic (Virtual Path traffic) received from WAN at the DC site will be redirected to the SD-WAN appliance by the PBR Router. The data traffic will be redirected to WAN Optimization appliance by the PBR Router.

Traffic flow for WAN to DC LAN:

- CE (Customer Edge) Router -> PBR Router -> SD-WAN -> PBR Router -> LAN
- CE (Customer Edge) Router -> PBR Router - > WAN OPT - > PBR Router -> LAN
The same traffic flow will be followed in the reverse direction.

SD-WAN Standard Edition in PBR mode and WANOP in Inline Deployment

In the below illustration, the SD-WAN appliance at the DC site is deployed in one-arm mode while the WANOP appliance is deployed in inline mode.

The control traffic (Virtual Path traffic) received from WAN at the DC site will be redirected to the SD-WAN appliance by the PBR Router. The data traffic will be forwarded to WAN Optimization appliance (inline) by the PBR Router.

Traffic flow for WAN to DC LAN:
- CE (Customer Edge) Router - > PBR Router - > SD-WAN -> PBR Router - > LAN
- CE (Customer Edge) Router - > PBR Router ->  WAN OPT - > LAN

The same traffic flow will be followed in the reverse direction.

Configuration Steps

1. Configure the SD-WAN Appliance at DC [MCN] to establish Virtual Paths between DC and Branch sites.

2. Configure Intranet Service at the DC site.
   a) On the MCN (DC site), go to Configuration > Virtual WAN > Configuration Editor > Connections > Site (DC) > Intranet Services. Click the [+ ] sign to add an Intranet Service.
   b) Select the WAN Link(s) for Intranet Service, and then click Apply.
c) Navigate to Routes under the same Site (DC), click [+] sign to add the remote network with cost lower than 5, and select click Add.

For example - Enter 192.168.1.0/24 in the Network IP address field with cost 4 and select Service Type as Intranet.

Note
Cost at each site should be less than 5 for the intranet route to take precedence.

3. Configure Intranet Service at the Branch site.
   
a) Repeat sub-steps a to c from step 2 above on the Branch site.

For example - Enter 172.16.1.0/24 in the Network IP address field with cost 4 and select Service Type as Intranet.

4. Perform Change Management to upload and distribute configuration to the Branch site.

See, Exporting configuration package and change management

By default, the traffic is sent from Branch to DC through the Virtual Path.

Note
The PBR router needs to be configured to redirect traffic as per the deployment steps provided.

For more information about configuring WAN Optimization, refer to the CloudBridge 9.1 documentation at: Enabling-configuring-wan-optimization
SD-WAN SE/EE Appliance in Hairpin Deployment Mode

Mar 20, 2017

With a hairpin deployment, you can implement use of a Remote Hub site for internet access through backhaul or hairpin when local internet services are unavailable or are experiencing a slow traffic. You can leverage high bandwidth routing between client sites by allowing backhauling from specific sites.

The purpose of a hairpin deployment from a non-WAN to a WAN forwarding site is to provide customers with a more efficient deployment process and more streamlined technical implementation. Customers will have the ability to use a remote hub site for internet access when needs arise, and can route flows through the virtual path to the SD-WAN network.

For example, consider an administrator with multiple SD-WAN Sites, A and B. Site A has poor internet service. Site B has usable internet service, with which you want to backhaul traffic from site A to site B only. You can try to accomplish this without the complexity of strategically weighted route costs and propagation to sites that should not receive the traffic.

Also, the route table is not shared across all sites in a Hairpin deployment. For example, if traffic is hairpin'ned between Site A and Site B through Site C, then only Site C would be aware of site A's and B's routes. Site A and Site B will not share each other's route table unlike in WAN-to-WAN forwarding.

When traffic is Hairpin'ned between Site A and Site B through Site C, the static routes are required to be added in Site A and Site B indicating that the next hop for both the sites is the intermediate Site C.

WAN-to-WAN Forwarding and Hairpin deployment have certain differences, namely:

a. Dynamic Virtual Paths are not configured. At all times, the intermediate site will see all the traffic between the two sites.

b. Does not participate in WAN-to-WAN Forwarding groups.

WAN-to-WAN Forwarding and Hairpin deployment are mutually exclusive. Only one of them can be configured at any given point in time.

NetScaler SD-WAN SE/EE and VPX (virtual) appliances support hairpin deployment. You can now configure a 0.0.0.0/0 route to hairpin traffic between two locations without affecting any additional locations. If hairpinning used for intranet traffic, specific Intranet routes are added to the client site to forward intranet traffic through the virtual path to the hairpin site. Enabling WAN-to-WAN forwarding to accomplish hairpin functionality is no longer required.

You can configure hairpin deployment through the SD-WAN web management interface from the configuration editor.
When enabled, this Site may serve as a mediator for the creation and destruction of Dynamic Virtual Paths between two or more Sites connected to this Site.

### Edit Route

<table>
<thead>
<tr>
<th>Order</th>
<th>Network IP Address</th>
<th>Routing Domain</th>
<th>Cost</th>
<th>Service Type</th>
<th>Gateway IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.16.1.95/24</td>
<td>Default_RoutingDomain</td>
<td>5</td>
<td>Virtual Path</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>172.16.2.85/24</td>
<td>Green</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0.0.0.0/0</td>
<td>Default_RoutingDomain</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0.0.0.0/0</td>
<td>Green</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Eligibility Based On Path:
Path: 

Apply | Cancel
Two Box Mode

Two box mode is a WCCP one-arm based deployment where the SD-WAN SE appliance acts as a WCCP router and the SDWAN-WANOP (4000/5000) appliances act as WCCP clients and help establish WCCP convergence. This way all the virtual path/Intranet service oriented TCP packets reaching the SD-WAN SE appliance get redirected to the SDWAN-WANOP appliance for optimization benefits thereby providing both SD-WAN SE and WANOP benefits for the customer traffic.

Two Box mode is supported only on the following appliance models:

- SD-WAN SE appliances – 4000, 4100, and 5100
- SDWAN-WANOP appliances – 4000 and 5000

**Note**

High Availability and WCCP deployment modes are not accessible when Two Box mode is enabled. However, these deployment modes will be available for the user to administer.

**Important**

- Although the legacy WCCP deployment is disabled when Two Box Mode is enabled, the Service Group convergence can only be verified from the WCCP monitoring page. There is no separate GUI page under the monitoring section for the Two Box Mode.
- If WCCP process running on the Standard Edition appliance reboots multiple times within a short interval of time, for example, 3 times in a minute then Service Group shuts down automatically. In such scenario, to get the WCCP convergence on the WANOP appliance, re-enable the WCCP feature in the WANOP appliance web GUI.
- When there is a change in the WCCP configuration or WAN optimization related to configuration on the Standard Edition appliance, the external WANOP appliance reboots. For example, enabling/disabling the WCCP checkbox in the Interface Group of config editor followed by Change Management process, restarts the WANOP appliance as well.
Note

Also, note the following points to consider when implementing the two box mode:

- When a routing domain is selected to be redirected to the WANOP appliance from the Configuration Editor, it should be added in the Interface Group for which WCCP is enabled.
- The same routing domain’s traffic should be selected on the partner site as well. For example; MCN > Branch01 to observe WAN optimization benefits.
- If a routing domain is selected in the interface group on which WCCP is enabled, another interface group which contains the bridged interfaces should have the same routing domain configured. Only if WCCP enabled interface group has the routing domain configured it is not enough to transmit the end-to-end traffic flowing with WAN optimization benefits.

NetScaler SD-WAN Standard Edition

To configure two-box mode solution in the Standard Edition appliance at the DC or Branch site:

1. In the NetScaler SD-WAN SE web management interface, go to Configuration > Virtual WAN > Configuration Editor. Open an existing configuration package or create a new package.

2. In the chosen configuration package, go to the Advanced tab to view the configuration details.

3. Open Global settings and expand Routing Domains to view that the Redirect to WANOP checkbox is enabled.

4. Expand DC to enable WCCP for the Virtual Interface under Interface Group settings that will signify which virtual network interface the appliance will be enabled for.
5. Expand Sites > Add to view the Branch routing domain and interface group settings. Under the Branch site, the Redirect to WANOP checkbox is enabled for Routing Domains.

**Note**

The WCCP listener should be enabled only for those virtual network interfaces which have only ONE Ethernet Interface configured. This indicates that WCCP Listener should not be enabled on a BRIDGED Pair. It is intended to be enabled on the ONE-ARM interface between the SD-WAN SE and SD-WAN WANOP appliances.

**NetScaler SD-WAN WANOP Configuration**

To configure two-box deployment mode in the SD-WAN WANOP appliance web GUI:

1. In the NetScaler SD-WAN WANOP web management interface, go to **Configuration > Appliance Settings > Advanced Deployments > Two Box Solution.**
2. Click the Edit icon to edit the two box mode settings. Information dialog about Cache IPs is displayed. Click OK.

3. Enable the Two Box Enabled checkbox.

4. Enter the Peer IP. Peer IP is the Netscaler SD-WAN Standard Edition appliance IP address.

5. Enter the user credentials and click Apply.

Two Box Mode Configuration and Manageability

Following are some of the two box mode configuration and manageability points to consider for deployment:

* SD-WAN WANOP configurations mentioned below can be configured from SD-WAN SE configuration editor as a unified pane
- SERVICE CLASS
- APPLICATION CLASSIFIER
- FEATURES
- SYSTEM TUNING

Monitoring

You can monitor SD-WAN WANOP traffic directly using the Monitoring page of the SD-WAN SE appliance’s web UI. This allows for a single pane monitoring of both the SDWAN-SE and SDWAN-WO appliances while processing data traffic. You can view the connection details, secure partner details and so on under the WAN Optimization node in the SDWAN-SE UI.

Configuration

You can configure APPFLOW directly from the SDWAN-SE Configuration page under APPFLOW node. This enables SDWAN-SE to act as a single pane for configuration of APPFLOW and other data processing configuration attributes such as Service Class, Application Classifiers and so on. The configuration done on the SDWAN-SE reflects on the SDWAN-WO configuration, maintaining seamless APPFLOW functionality support.
SD-WAN WANOP already discovered by an insight center, if used in Two Box Mode should be isolated and not configured using MAS/Insight until this mode is turned off. This is because the configuration of WANOP for traffic processing is governed by the SD-WAN SE appliance in the Two Box Mode.

Advanced Optimizations or Secure Acceleration should be directly configured on the SDWAN-SE appliance like we would configure on the SDWAN-WO appliance. This helps maintain a single pane of configuration of configurations like Domain Join or Secure Acceleration/SSL Profile creation for Advanced optimizations or SSL Proxy.

* Licensing should be separately managed for each of SD-WAN SE and SD-WAN WANOP appliances.

* Software Upgrade should be separately managed for each of SD-WAN SE and SD-WAN WANOP appliances with the respective software packages. For example, tar.gz for SD-WAN SE and upgrade upg for SD-WAN WANOP.

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

Unified Configuration and Monitoring

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

a. Go to Configuration > Virtual WAN > WAN Optimization
b. Appflow node under Configuration > Appliance Settings
c. WAN Optimization node under Configuration.

This information is redirected from the SD-WAN WANOP appliance which is in Two box mode with the SD-WAN SE appliance.

Configuration related to WANOP, such as SSL Acceleration and AppFlow can now be performed from SD-WAN SE web GUI.

Traffic related statistics, such as Connections, Compression, CIFS/SMB, ICA Advanced, MAPI and partners can now be monitored from SD-WAN SE web GUI under Monitoring > WAN Optimization similar to the SD-WAN Enterprise edition appliance.
Management IP Address Change for SD-WAN WANOP Appliance in Two Box Mode

To change the management IP address of SDWAN-WANOP appliance in Two box mode:

1. Execute command `clear_wo_sync` on the SD-WAN SE appliance. This ensures that the SD-WAN WANOP IP address information is cleared for GUI redirection.

2. Disable and enable Two box mode config on the SD-WAN WANOP appliance. The new IP address (changed IP) of SD-WAN WANOP appliance is sent to SD-WAN SE. The new changed IP address is displayed in the URL redirection pages.

Disable Two Box mode on SD-WAN WANOP Appliance

To disable or decouple the SD-WAN WANOP and SD-WAN SE appliances from the Two Box mode:

a. Disable the Two Box mode from SD-WAN WANOP appliance.

b. It is expected to still see the SD-WAN WANOP appliance two box mode pages in the SD-WAN SE web GUI. To clear these pages, execute the command: `clear_wo_sync`. 

### Diagram

[Image of Citrix NetScaler SD-WAN 5100-4000-SE configuration interface]
High-Availability Deployment Modes

May 31, 2017
This topic covers the High Availability (HA) deployments and configurations supported by SD-WAN appliances (Standard Edition and Enterprise Edition).

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

- Parallel Inline HA
- Fail-to-Wire HA
- One-Arm HA

These HA deployment modes are similar to Virtual Router Redundancy Protocol (VRRP) and use a proprietary SD-WAN protocol. Both Client Nodes (Clients) and Master Control Nodes (MCNs) within a SD-WAN network can be deployed in an HA configuration as long as the selected SD-WAN platform model supports HA.

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

Note
For MCNs, secondary MCN redundancy is supported. In this mode, one of the Clients is also designated as a Secondary MCN. It will continuously monitor the health of the Primary MCN and, if a catastrophic event occurs, it will assume the role of the MCN.

Configuring High Availability

To configure HA:

1. Navigate to the SD-WAN web management interface at: Configuration > Virtual WAN > Configuration Editor > Sites (MCN) > DC. Click Enable High Availability.
2. After a site is configured, the HA appliance and interface groups are configured.
Primary Reclaim: In the event that the Active appliance fails and then comes back up, it can be configured to reclaim the Active status after it is rebooted. This feature is disabled by default. To enable it, select the check box for Primary Reclaim in the HA section of the configuration for the site. The Active/Standby states of a HA pair can be manually switched from the web console of either appliance during run-time operation.

Fail-to-Wire: Select the Fail-to-Wire check box.

3. Configure interface groups by clicking the + next to HA IP Interfaces. From the Virtual Interface drop-down menu, select the desired interface. This interface monitors the Active appliance for reachability. For One-Arm HA mode, only one interface group is required.

4. Select the Primary and Secondary IP address.

5. For Inline HA mode, additional interface groups are required for External Tracking to monitor the upstream or downstream network infrastructure. For example; switch port failure, to detect if HA change state is required.

Monitoring

To monitor HA configuration:

Login to the SD-WAN web management interface for the Active and Standby MCN appliance's for which high-availability is implemented. View high-availability status under the Dashboard tab.
For Network Adapter details of Active and Standby HA appliances, navigate to Configuration > Appliance Settings > Network Adapters > Ethernet tab.
Selecting a High Availability Mode

**One-Arm mode:**

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

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

**IP SLA Monitoring for Fall Back**

The active traffic will flow 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 will try to redirect traffic to the appliances. IP SLA monitoring can be configured at the router to disable PBR, if the next appliance is not reachable. This allows the router to fall back to perform a route lookup and forward packets appropriately.
Parallel Inline HA mode:

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

The HA 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 HA 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 HA mode is very quick and nearly hitless, as no physical state change occurs. Fallback to the tertiary path is not hitless and can block traffic for 5-30 seconds depending on the spanning tree configuration. If there are out of path connections to other WAN Links, both appliances must be connected to them.

![Higher Spanning Tree Cost Fallback Connection](image)

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

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

**Note**

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

- Due to a physical state change when the SD-WAN appliances switch over from Active to Standby, failover can cause partial loss of connectivity depending on how long the auto-negotiation takes on the Ethernet ports.
- It is recommended that Fail-to-Wire mode be used on ports that are auto-negotiated, as this will increase failover time.

The following illustration shows an example of the Fail-to-Wire deployment.
The One-Arm HA configuration or Parallel Inline HA configuration is recommended for Datacenters 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 HA mode is a better solution. The Fail-to-Wire HA mode protects against appliance failure and parallel inline HA protects against all failures. In all scenarios, HA is valuable to preserve the continuity of SD-WAN network during a system failure.
Configuration

Mar 30, 2017
The following topics provide information about how to configure Virtual path service between MCN and branch sites, and enabling WAN optimization.

Configuring Virtual WAN service

Configuring virtual path between MCN and branch sites

Enabling and configuring WAN optimization
Configuring Virtual WAN Service

Oct 04, 2016

The SD-WAN configuration describes and defines the topology of your SD-WAN network. Before you can deploy a SD-WAN network, you must define the Virtual WAN configuration. To do this, use Configuration Editor in the SD-WAN Management Web Interface on the MCN appliance.

Security and Encryption

Enabling encryption for SD-WAN (for the Virtual Paths) is optional. Instructions for configuring this feature are provided in the section, Enabling and Configuring Virtual WAN Security and Encryption (Optional).

When encryption is enabled, SD-WAN uses the Advanced Encryption Standard (AES) to secure traffic across the Virtual Path. Both AES 128 and 256 bit ciphers (key sizes) are supported by the SD-WAN Appliances, and are configurable options. You can select, enable, and configure these and the other encryption options by using the Configuration Editor in the Management Web Interface on the Management Control Node (MCN). You must have administrative access on the MCN to modify the configuration, and to distribute your changes across the SD-WAN network. Once the MCN is secured, the encryption settings and their distribution are also secure.

Authentication between sites functions by means of the Virtual WAN Configuration. The network configuration has a secret key for each site. For each Virtual Path, the network configuration generates a key by combining the secret keys from the sites at each end of the Virtual Path. The initial key exchange that occurs after a Virtual Path is first set up, is dependent upon the ability to encrypt and decrypt packets by means of that combined key.

Enabling Virtual WAN Service

If this is an initial installation and configuration, as a final step you will need to manually enable the Virtual WAN Service on each SD-WAN appliance in your network. Enabling the service enables and starts the Virtual WAN daemon.

Note

If you are reconfiguring an existing deployment, the MCN automatically enables the service when it distributes the updated Appliance Packages to the client sites. In this case, you can skip this final step.

To manually enable the Virtual WAN Service on an appliance, do the following:

1. Log into the Management Web Interface on the appliance you want to activate.
2. Select Configuration tab.
3. In the navigation pane, open the Virtual WAN branch and select Enable/Disable/Purge Flows.

   If the Virtual WAN Service is currently disabled, this displays the Enable Virtual WAN Service page, as shown below. If the service is already enabled, this displays the Enable/Disable/Purge Flows page.
4. Click Enable.

This enables the service, and displays the **Enable/Disable/Purge Flows** page.

When the Virtual WAN Service is enabled, a status message to that effect displays in the top section of the page.

**Note**

This page also presents options for enabling/disabling specific paths and Virtual Paths in your network, as well as an option to purge all flows.

This completes the installation and activation of the SD-WAN on the MCN and branch site client appliances. You can now
use the Monitoring pages to verify the activation and diagnose any existing or potential configuration issues.
Configuring the Virtual Path Service Between the MCN and Client Sites

Oct 04, 2016

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

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

1. Continuing in the Configuration Editor, click the Connections section heading.

   This reveals the Connections section configuration tree.

2. Click + to the left of the MCN site name in the Connections section tree.

   This opens the MCN site branch in the Connections configuration tree.

3. Click + next to the Virtual Paths branch label.

   This opens the Virtual Paths configuration section (child branch) for the MCN site branch in the tree. This section
provides settings and forms for configuring the Virtual Path Service between the MCN and each of the Virtual WAN client sites. The below figure shows an example **Virtual Paths** section for an MCN site.

The Virtual Paths section contains the following child branches:

- **Dynamic Virtual Paths** – (Optional) The settings in this section allow you to enable and disable Dynamic Virtual Paths, and set the maximum allowable Dynamic Virtual Paths for the site. Dynamic Virtual Paths are Virtual Paths that are established directly between sites, based on a configured threshold. The threshold is typically based on the amount of traffic occurring between those sites. Dynamic Virtual Paths are operational only after the specified threshold is reached. Dynamic Virtual Paths are not required for normal operation, so configuring this section is optional.

- **<MCN_Site_Name>_<Client_Site_Name>** – The system initially automatically adds a static Virtual Path between the MCN and a client site, as this Virtual Path is required. The name for the path uses the following form:

  `<MCN_Site_Name>_<Client_Site_Name>`

Where:

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

* **Client_Site_Name** is the name of a client site identified in the current configuration package.

User-configurable default settings are initially applied to the static Virtual Path, as defined in the **Default Sets > Virtual Path Default Sets** section of the **Connections** configuration tree. However, you can customize or add to the defined **Default Sets**, and also customize the configuration for a specific site and Virtual Path.

**Note**

To add more static Virtual Paths for a site, you must do so manually. Instructions for manually adding a static Virtual Path are included in the steps below.
4. Click + next to the name of the static Virtual Path in the Virtual Paths tree.

This reveals additional child branches (configuration sets) for the static Virtual Path, as follows:

- **Local Site** – This section enables you to view and configure the Virtual Path settings from the perspective of a local site. You can also view, customize, and add Classes or Rules as required for this specific Virtual Path. You can also add Virtual Paths to the local site, as needed.

- **Remote Site** – This section enables you to view and configure the Virtual Path settings from the perspective of a remote site. As for the Local Site section, you can also view, customize, and add Class or Rules as required for this specific Virtual Path. You can also add Virtual Paths to the remote site, as needed.

- **Paths** – This section provides settings and forms for configuring the Virtual Paths and Virtual Path Service between the MCN and the client site.

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

5. Click + next to the Paths branch label, or click Paths if no + icon is present.

The system is able to automatically generate Virtual Paths for some WAN Links. If so, there will be a plus sign (+) to the left of the Paths child branch label. If the + icon is not present, click the Paths label directly. This reveals the Add (+) button for adding a Virtual Path. The Add icon is located to the right of the Paths branch label.
6. Click + (Add) to the right of the **Paths** branch label.

This displays the **Add Path** dialog box (configuration form).

7. Specify the source and destination site information for the new Virtual Path.

Specify the following from the available drop-down menus:

**Note**

Depending on how the WAN links are configured for the sites, some fields will be read-only. Fields that are configurable provide a
- **From Site** – This is the source site for the Virtual Path. For the required static Virtual Path, this is configured as the MCN site by default.

- **From WAN Link** – This is the originating WAN Link for the Virtual Path.

- **To Site** – This is the destination site for the Virtual Path.

- **To WAN Link** – This is the destination WAN link for the Virtual Path.

8. **Click Add**.

This adds the configured Virtual Path to both the MCN and the associated client site in the **Connections** tree. This also automatically opens the **Paths** settings configuration form for the **From Site** for the Virtual Path (in this case, the MCN).

9. **Click Edit** (pencil icon), to the right of the MCN-to-client Virtual Path label.

This opens the Virtual Path Service configuration form for editing.

10. **Configure the settings for the Virtual Path, or accept the defaults.**
The Paths configuration form contains the following settings:

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

- **To Site** section:
  - *Site* – This is the destination site for the Virtual Path.
  - *WAN Link* – This is the destination WAN link for the Virtual Path.

- **Reverse Also** – Select this checkbox to enable Reverse Also for this Virtual Path. If enabled, the system automatically builds a Virtual Path in the opposite direction of the configured path, using the same WAN links as configured for the original path.

- **IP DSCP Tagging** – Select a tag from the drop-down menu. This specifies the DSCP tag to set in the IP header for traffic traveling over this Virtual Path.

- **Enable Encryption** – Select this checkbox to enable encryption of packets sent along this Virtual Path.

- **Bad Loss Sensitive** – Select a setting from the drop-down menu. The options are:
  - *Enable* – (Default) If enabled, paths will be marked BAD due to loss, and will incur a path scoring penalty.
  - *Disable* – Disabling Bad Loss Sensitive can be useful when the loss of bandwidth is intolerable.
  - *Custom* – Select Custom to specify the percentage of loss over time required to mark a path as BAD. Selecting this option reveals the following additional settings:
    - **Percent Loss (%)** – This specifies the percentage of loss threshold before a path is marked BAD, as measured over the specified time. By default, the percentage is based on the last 200 packets received.
    - **Over Time (ms)** – Specify the time period (in milliseconds) over which to measure packet loss. Select an option between 100 and 2000 from the drop-down menu for this field.

- **Silence Period (ms)** – This specifies the duration (in milliseconds) before the path state transitions from GOOD to BAD. The default is 150 milliseconds. Select an option between 150 and 1000 from the drop-down menu for this field.

- **Path Probation Period (ms)** – This specifies the wait time (in milliseconds) before a path transitions from BAD to GOOD. Select an option between 500 and 60000 from the drop-down menu for this field. The default is 10000 milliseconds.

- **Instability Sensitive** – Select this checkbox to enable. If enabled, latency penalties due to a path state of BAD and other latency spikes are considered in the path scoring algorithm.

- **Tracking IP Address** – Enter a Virtual IP Address on the Virtual Path that can be pinged to determine the state of the path.

- **Reverse Tracking IP Address** – If Reverse Also is enabled for the Virtual Path, enter a Virtual IP Address on the path.
that can be pinged to determine the state of the reverse path.

11. Click the minus sign (−) to the left of the path label to close the settings form.

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

12. Repeat the steps above for each branch you want to connect to the MCN.

13. (Optional) When you finish adding and configuring all of the Virtual Paths to and from the MCN, click the minus sign (−) to the left of the MCN branch label to close the branch.

Next, you have the option of customizing the Virtual Paths configurations for the client sites, as well as adding and configuring additional paths between clients. Instructions are provided in the remaining steps, below.

14. Click + to the left of the client site branch label in the tree.

This opens the client site branch in the **Connections** tree.

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

To navigate to the Paths settings form for the client site, do the following:
a. Click + to the left of the branch label for the client site.

b. Click + to the left of the **Virtual Paths**.

c. Click + to the left of the branch label for the Virtual Path you want to configure.

d. Click + to the left **Paths**.

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

16. Configure the settings for each path you want to customize.

   Follow the same steps as you did to configure the Virtual Paths for the MCN site.

17. (Optional) Click the minus sign (–) to the left of the client site branch label.

   This closes the configured client site branch in the tree.
This completes the basic configuration of the Virtual Paths between the client sites and the MCN.

**Note**

For information on configuring additional settings in the Connections or Provisioning sections of the Configuration Editor, please refer to the Management Web Interface online help for those sections. If you do not want to configure these settings at this time, you can proceed to the appropriate step indicated below.

The next step depends on the SD-WAN Edition license you have activated for your deployment, as follows:

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

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

Oct 04, 2016

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

Note

You must have a SD-WAN Enterprise Edition license installed to access, enable, configure, and activate WAN Optimization features in your Virtual WAN. SD-WAN Standard Edition does not support these features.

There are two top-level steps for configuring the Optimization section sets and parameters. These are as follows, listed in order of dependency:

1. Enable WAN Optimization and customize the Defaults configuration, or accept the defaults.

   The Defaults configuration is used as the base Optimization configuration for all sites eligible for WAN Optimization. The Defaults configuration comes pre-configured, and can be customized.

   Note

   For instructions, see Enabling Optimization and Configuring Default Settings.

2. (Optional) Customize the WAN Optimization configuration for each of the individual branch sites, or accept the Defaults sets and settings for each.

   By default, the Defaults configuration is initially applied to each branch site that is eligible for WAN Optimization. WAN Optimization is supported for 1000-EE and 2000-EE hardware appliances, only. For each supported branch site, you can elect to accept or modify any combination of the Defaults sets and settings, or any subset of these. For instructions, see Configuring Optimization for a Branch Site.

   To complete these steps, you will use the configuration forms the Optimization section of the Configuration Editor. The Optimization section is organized as follows:

   - Defaults – The Defaults branch contains the following child branches, which in turn contain one or more forms for configuring their respective sets and settings:

     * Defaults Features
     * Defaults Tuning Settings
     * Defaults Application Classifiers (set)
     * Defaults Service Classes (set)
- *Client Site Name* – The **Optimization** section configuration tree contains a branch for each client node (branch site) that supports WAN Optimization. If a client node is an unsupported appliance model, the site will not be included in the **Optimization** section configuration tree. Each branch in the tree contains the following child branches, which in turn contain one or more forms for configuring their respective sets and settings:

* **Defaults Features**

* **Defaults Tuning Settings**

* **Defaults Application Classifiers** (set)

* **Defaults Service Classes** (set)

The below figure shows a simple example of the top and second levels of the **Optimization** section configuration tree. In this example, the branch site **BR-01_K** is included, because the site is configured for a 1000-EE appliance.

![Configuration Tree Example](image)

The following section provides instructions for enabling WAN Optimization for your Virtual WAN, and configuring the **Defaults** sets and settings.
Enabling Optimization and Configuring Default Settings

Oct 04, 2016
The first step is to enable WAN Optimization in the new configuration package, and configure the defaults sets and settings.

The Optimization section defaults sets and settings are categorized as follows:

- Defaults Features
- Defaults Tuning Settings
- Defaults Application Classifiers (set)
- Defaults Service Classes (set)

The following sections provide instructions for enabling WAN Optimization and configuring each of these defaults sets and settings.
Enabling Optimization and Configuring the Default Feature Settings

Dec 12, 2016

Enabling WAN Optimization in your Virtual WAN entails the following procedures:

1. Enable WAN Optimization in the Features settings of the Optimization section.
   
   Instructions for this part of the process are provided in this section.

2. Configure the Acceleration policy setting for each applicable Service Class in the Service Classes table.

   This procedure occurs further on, after you have completed the rest of the Optimization configuration. Instructions are provided in the section, Configuring Optimization Default Service Classes. At this point, WAN Optimization has been enabled in your configuration, but not yet enabled and activated in your Virtual WAN. To enable and activate WAN Optimization in your Virtual WAN, you must complete the Virtual WAN configuration, and then generate, stage, and activate the Virtual WAN Appliance Packages on the eligible sites in your deployment, as outlined in the subsequent chapters of this guide.

To enable WAN Optimization and configure the Defaults section Features settings, do the following:

1. If necessary, log back into the Management Web Interface, and open the Configuration Editor.

   To open the Configuration Editor, do the following:

   a. Select the Configuration tab at the top of the page to open the Configuration navigation tree (left pane).
   
   b. In the navigation tree, click + to the left of the Virtual WAN branch to open that branch.

   C. In the Virtual WAN branch, select Configuration Editor.

2. Open the configuration package you want to modify.

   Click Open to display the Open Configuration Package dialog box, and select the package from the Saved Packages drop-down menu.

   This loads the selected package into the Configuration Editor and opens it for editing.

If you have a valid and current license that includes WAN Optimization features, the Optimization section will be available in the Configuration Editor.
Note

If the **Optimization** section is not available, please check that you have installed a CloudBridge Enterprise Edition license in your Virtual WAN. CloudBridge Virtual WAN Edition does not support WAN Optimization features.

For details and instructions, see the following sections:

- **The SD-WAN Editions**
- **Licensing**
- **Uploading and Installing the Virtual WAN Software License File**

3. Click the **Optimization** section heading.

This opens the **Configuration Editor Optimization** section tree.

The **Optimization** section tree contains a branch for the **Defaults** settings, and a branch for each eligible client node (branch site) in the current configuration. Optimization is supported for 1000-EE and 2000-EE clients, only. Consequently,
the client node must be a 1000-EE or 2000-EE hardware Virtual WAN Appliance for that site to be included in the tree.

4. Click + to the left of the **Defaults** branch label.

   This opens the **Defaults** settings tree.

5. Click + to the left of the **Features** branch label.

   This opens the default **Features** configuration form.

6. Click Edit (pencil icon) to the right of the **Features** branch label to enable editing of the form.

7. Select the **WAN Optimization** checkbox.

   The **WAN Optimization** checkbox is in the upper left corner of the **WAN Optimization** Features section at the top of the form. Select the checkbox to select **WAN Optimization** for enabling. This also opens the other options in the form for editing, and reveals the **Apply** and **Revert** buttons.

---

**Note**

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved.
This selects this feature for enabling only. WAN Optimization will not be enabled in the Optimization section or the configuration package until you click Apply, after completing the Features configuration. In addition, you must also configure the Acceleration setting for each applicable Service Class in the Service Classes table, as instructed further on in the Optimization configuration process. (Instructions are provided in the section Configuring Optimization Default Service Classes) Finally, WAN Optimization will not be enabled and activated in your Virtual WAN until you have completed the entire Virtual WAN configuration, and then generated, staged, distributed, and activated the Virtual WAN Appliance Packages on the eligible sites in your Virtual WAN.

The below figure shows the Defaults section Features configuration form, with WAN Optimization enabled, and the Apply and Revert buttons revealed.

8. Configure the Features settings.

Click a checkbox to select or deselect an option. You can accept the default settings pre-selected in the form, or customize the settings.

**Note**

By default, the settings you configure in the Defaults section forms are automatically applied to each branch site included in the tree. However, you can customize the Optimization configuration for a specific branch, as outlined in the section, Configuring Optimization for a Branch Site.

The Features configuration form contains two sections:

- **WAN Optimization Features**
- **CIFS Optimization Protocols**

  The **WAN Optimization Features** settings are as follows:

  - **WAN Optimization** – Select this to enable WAN Optimization for this configuration. This also enables compression, deduplication, and TCP Protocol Optimization.

  **Note**

  The WAN Optimization option must be selected for the other Optimization section options to be available.

  - **ICA Multi Stream** – Select this to enable CloudBridge to negotiate the use of multi-stream for ICA traffic for improved Quality of Service.
  
  - **SCPS** – Select this to enable TCP Protocol optimization for Satellite Links.
  
  - **HDX QoS Priorities** – Select this to enable optimization of ICA traffic based on prioritization of HDX sub-channels.
  
  - **MAPI Cross Protocol Optimization** – Select this to enable cross-protocol optimization of Microsoft Outlook (MAPI) traffic.
  
  - **SSL Optimization** – Select this to enable optimization for traffic streams with SSL encryption.
  
  - **RPC Over HTTP** – Select this to enable optimization of Microsoft Exchange traffic that uses RPC over HTTP.
  
  - **User Data Store Encryption** – Select this to enable enhanced security of data through the encryption of WAN Optimization compression history.
  
  - **Native MAPI** – Select this to enable optimization of Microsoft Exchange traffic.

  The **CIFS Optimization Protocols** options are as follows:

  - **SMB1** – Select this to enable Optimization of Windows File Sharing (SMB1)
  
  - **SMB2** – Select this to enable Optimization of Windows File Sharing (SMB2)
  
  - **SMB3** – Select this to enable Optimization of Windows File Sharing (SMB3). You must first select the **SMB2** option before you can select **SMB3**.

  9. Click **Apply**.

  This enables and adds the selected **Default Features** to the configuration package.

  The next step is to configure the **Optimization default Tuning Settings**.
Configuring Optimization Default Tuning Settings

Oct 04, 2016

To configure the WAN Optimization default Tuning Settings, do the following:

1. Open the Tuning Settings configuration form.

   Continuing in the Defaults branch of the Optimization section of the Configuration Editor, click + to the left of the Tuning Settings branch label.

2. Click Edit (pencil icon) to enable editing of the form.

3. Select and configure the Tuning Settings.

   The Tuning Settings options are as follows:

   - **Maximum MSS** – Enter the maximum size (in bytes) for the Maximum Segment Size (MSS) for a TCP segment.
   - **Default MSS** – Enter the default size (in octets) for the MSS for TCP segments.
   - **Enable Connection Timeout** – Select this to enable automatic termination of a connection when the idle
threshold is exceeded.

- **Idle Timeout** – Enter a threshold value (in seconds) to specify the amount of idle time permitted before an idle connection is terminated. You must first select **Enable Connection Timeout** before this field can be configured.

4. Click **Apply**.

   This applies the modified **Tuning Settings** to the **Defaults** configuration.

   The next step is to configure the default set of WAN Optimization Application Classifiers.
Configuring Optimization Default Application Classifiers

Oct 04, 2016
To configure the default set of WAN Optimization Application Classifiers, do the following:

1. Open the **Application Classifiers** table.

   Continuing in the **Defaults** branch of the **Optimization** section of the **Configuration Editor**, click + next to the **Application Classifiers** branch.

   ![Application Classifiers Table](image)

   This opens the **Application Classifiers** table, displaying the default set of Application Classifiers.
This table is also a configuration form. You can use this form to configure (edit), delete, and add Application Classifiers to create a customized default set. The modified default Application Classifiers set and individual Application Classifier settings you configure are automatically applied as the defaults to any branch site included in the Optimization section tree.

**Note**

You can also customize the Application Classifiers set and settings for each specific branch site. For instructions, see the section Configuring Optimization for a Branch Site.

2. To configure an existing Application Classifier, click Edit (pencil icon), in the Edit column of that classifier entry.

   This opens a pop-up Edit settings form for configuring the selected Application Classifier.
3. In the **Port** field, enter the port number for the Application Classifier, or accept the default.

4. Add or remove Application Groups in the **Configured** list, or accept the defaults.
   
   - **To add an Application Group to the list:** Select it in the **Application Groups** list on the left, and then click the Add right-arrow (>) to add the group to the **Configured** list on the right. To add all of the **Application Groups** to the list at once, click the Add All double right-arrow (>>).
   
   - **To remove an Application Group from the list:** Select it in the **Configured** list on the right, and then click the Remove left-arrow (<). To remove all of the **Application Groups** from the list at once, click the Remove All double left-arrow (<<).

5. Click **Apply**.

   This applies your changes to the Application Classifier, and dismisses the **Edit** configuration form.

6. (Optional) Customize the default **Application Classifiers** set.

   You can add or delete Application Classifiers to customize the default set, as follows:

   - **To remove an Application Classifier from the set:**
     
     Click the trashcan icon in the **Delete** column of an **Application Classifier** entry to remove that entry from the table.

   - **To add an Application Classifier to the set:**
     
     a. Click + to the right of the **Application Classifier** branch label.

     This displays the **Add** configuration form.
b. Enter the name and port number for the Application Classifier in the **Name** and **Port** fields, respectively.

c. Add or remove Application Groups in the **Configured** list.

   **To add an Application Group to the list:** Select it in the **Application Groups** list on the left, and then click the Add right-arrow (>) to add the group to the **Configured** list on the right. To add all of the **Application Groups** to the list at once, click the Add All double right-arrow (>>).

   **To remove an Application Group from the list:** Select it in the **Configured** list on the right, and then click the Remove left-arrow (<). To remove all of the **Application Groups** from the list at once, click the Remove All double left-arrow (<<).

d. Click **Apply**.

   This adds the new Application Classifier to the set, and dismisses the **Add** configuration form.

The next step is to configure the default set of WAN Optimization Service Classes.
Configuring Optimization Default Service Classes

Dec 12, 2016

To configure the default set of WAN Optimization Service Classes, do the following:

1. Open the Service Classes table.

   Continuing in the Defaults branch of the Optimization section of the Configuration Editor, click + to the left of the Service Classes branch label.

   ![Service Classes Table]

   This opens the Service Classes table, displaying the default set of Service Classes.

   ![Modified Service Classes Table]

   This table is also a configuration form. You can use this form to configure (edit), delete, and add Service Classes to create a customized default set. The modified default Service Classes set and individual Service Class settings you configure are automatically applied as the defaults to any branch site included in the Optimization section tree.
Note

You can also customize the Service Classes set and settings for each specific branch site. For instructions on customizing the Optimization configuration for a branch site, see the section, Configuring Optimization for a Branch Site.

2. To configure an existing Service Class, click Edit (pencil icon), in the Edit column of that class entry in the Service Classes table.

This opens a pop-up Edit settings form for configuring the selected Service Class.

3. Configure the basic settings for the Service Class.

The basic settings are as follows:

- **Enabled** – Select this to enable the new Service Class. The class is enabled by default.

- **Acceleration Policy** – Select a policy from the Acceleration Policy drop-down menu. The options are:
  
  * **disk** – Select this policy to specify the appliance disk as the location for storing the traffic history used for compression. This enables Disk Based Compression (DBC) policy for this Service Class. Generally speaking, a policy of disk is usually the best choice, as the appliance automatically selects disk or memory as the storage location, depending on which is more appropriate for the traffic.

  * **none** – Select this if you do not want to enable an Acceleration Policy for this Service Class. A policy of none is generally used only for uncompressible encrypted traffic and real-time video.

  * **flow control only** – Select this policy to disable compression but enable flow-control acceleration. Select this for services that are always encrypted, and for the FTP control channel.

  * **memory** – Select this policy to specify memory as the location for storing the traffic history used for compression.
- **Enable AppFlow Reporting** – Select this to enable AppFlow reporting for this Service Class. AppFlow is an industry standard for unlocking application transactional data processed by the network infrastructure. The WAN Optimization AppFlow interface works with any AppFlow collector to generate reports. The collector receives detailed information from the appliance, using the AppFlow open standard (http://www.appflow.org).

For more information on AppFlow, please see the Citrix CloudBridge 7.4 Product documentation available on the citrix documentation portal http://docs.citrix.com/.

---

**Note**

To view WAN Optimization AppFlow reports, select the Monitoring tab, and then in the navigation tree (left pane), open the **WAN Optimization** branch, and select **AppFlow**. See also, Monitoring Your SD-WAN Virtual WAN.

---

- **Exclude from the SSL Tunnel** – Select this to exclude traffic associated with the Service Class from SSL Tunneling.

4. Configure the **Filter Rules** for the Service Class.

To edit an existing rule, do the following:

a. In the Filter Rules table (bottom of form), click Edit (pencil icon) in the Edit column of the rule you want to edit. This reveals the Filter Rules settings for the selected Filter Rule.

b. Select the filter direction from the Direction drop-down menu.
Select one of the following options:

* **BIDIRECTIONAL**

* **UNIDIRECTIONAL**

c. Add or remove Applications in the **Configured** list.

**To add an Application to the list:** Select it in the **Applications** list on the left, and then click the Add right-arrow (> to add the group to the **Configured** list on the right. To add all of the **Applications** to the list at once, click the Add All double right-arrow (>>).

**To remove an Application from the list:** Select it in the **Configured** list on the right, and then click the Remove left-arrow (<). To remove all of the **Applications** from the list at once, click the Remove All double left-arrow (<<).

d. Scroll down to reveal the truncated portion of the form.

The **Filter Rules** settings section is somewhat long, so you will need to use the scroll bars to reveal the truncated portion of the form.

e. Enter the Source IP Address in the **Source IP Address** field.

f. Click + to the right of the Source IP Address you just entered.

This adds the specified IP Address to the **Source IP Address** table.
g. Specify whether to include or exclude the Source IP Address for this Filter Rule.

Select the **Exclude** checkbox to exclude the specified Source IP Address from this Filter Rule. Deselect the checkbox to include the address.

h. Enter the Destination IP Address in the **Destination IP Address** field.

i. Click + to the right of the Destination IP Address you just entered.

This adds the specified IP Address to the **Source IP Address** table.

j. Specify whether to include or exclude the Destination IP Address for this Filter Rule.

Select the **Exclude** checkbox to exclude the specified Destination IP Address from this Filter Rule. Deselect the checkbox to include the address.

k. Click **Apply**.

This applies your modifications to the rule and hides the **Filter Rules** settings section.

5. (Optional) Customize the default **Service Classes** set.

You can add or delete Service Classes to customize the default set, as follows:

- **To remove an Service Class from the set:**

  Click the trashcan icon in the **Delete** column of a Service Class entry in the table to remove that entry.

- **To add an Service Class to the set:**

  a. Click + to the right of the **Service Class** branch label.

  This displays the **Add** configuration form.
b. Enter the name for the new Service Class in the **Name field**.

c. Configure the new Service Class.

   The steps for configuring a new Service Class are the same as for modifying an existing Service Class. For instructions, see the following steps, earlier in this section:

   "3. Configure the basic settings for the Service Class."

   "4. Configure the Filter Rules for the Service Class."

d. Click **Add** to add the new Service Class to the default set and dismiss the **Add** configuration form.

6. (Optional, recommended) **Save** the configuration package.

For instructions on saving and loading a configuration package, see Naming, Saving, and Backing Up the MCN Site Configuration.

You have now completed the **Defaults** section configuration, and can begin configuring the **Optimization** sets and settings for the branch sites.
Configuring Optimization for a Branch Site

Oct 04, 2016

After you have completed the Defaults configuration, you have the option of customizing the sets and settings for each of the branch sites.

The Defaults sets and settings you just configured are automatically applied to each branch site included in the Optimization section. You can elect to accept the defaults, or customize the configuration for any given branch. The procedures for configuring the Optimization sets and settings for a branch site are the same as for configuring the Defaults, with a few minor differences.

To customize the Optimization configuration for a branch site, do the following:

1. If you have not done so, open the Optimization section in the Configuration Editor.
   
   Click the Optimization section heading to open that section.
   
   ![Optimization Section](image)

   The Optimization section tree contains a branch for the Defaults settings, and a branch for each eligible client site in the current configuration. Optimization is supported for CB 1000-VW and CB 2000-VW clients, only. Consequently, the appliance for a site must be a CB 1000-VW or CB 2000-VW hardware Virtual WAN Appliance for that site to be included in the tree.

2. Click + to the left of the branch label for the branch site you want to configure.
   
   This opens the Optimization settings tree for the branch site.
   
   ![Optimization Settings Tree](image)

3. Click + to the left of the branch label for the Optimization settings you want to configure.

   For example, click + next to the Features branch label to open that configuration category. Opening a category displays the Override Defaults option for that category.
4. Click Edit (pencil icon) to the right of the set label to enable editing.

5. Select the **Override Defaults** checkbox.

   This reveals the top-level configuration form for that configuration category, and opens it for editing.

   The below image shows an example top-level settings configuration form, in this case for the **Features** set.

6. Enter your configuration changes.

   From this point on, the configuration process for each branch site **Optimization** category is the same as for the corresponding **Defaults** section category. For instructions on configuring a particular category of sets or settings, see the appropriate section listed below:
Enabling Optimization and Configuring the Defaults Features Settings.

Configuring Optimization Default Tuning Settings.

Configuring Optimization Default Application Classifiers.

Configuring Optimization Default Service Classes.

7. (Optional, recommended) **Save** the configuration package.

For instructions on saving and loading a configuration package, see [Naming, Saving, and Backing Up the MCN Site Configuration](https://docs.citrix.com).

You have now completed configuring the **Optimization** section sets and settings for your Virtual WAN. The next step is to prepare the Virtual WAN Appliance Packages for distribution to the client nodes.
Basic Configuration - WAN Link Templates

Mar 30, 2017
In NetScaler SD-WAN 9.2, a user configuring five or more basic sites for the first time can save time when setting up new sites and WAN Links. Using templates, you can configure certain settings one time and then duplicate them on more than one site. On the Basic tab, you can use the Network option to create and administer WAN Link templates, and the Site option to configure a site.

Basic Configuration Mode

NetScaler SD-WAN 9.2 introduces the Basic configuration mode for ease of use. Network administrators with basic sites can now reduce repetitive tasks and configure new sites with minimal clicks. Combined with WAN Link Templates Basic configuration mode is a powerful tool that involves minimal manual configuration.

The Basic > Sites view simplifies the configuration process by enabling you to create a configuration file that generates a virtual path between the defined sites. The required configuration properties for a virtual path between sites include:

- Appliance
- Interface
- WAN Links
- Static Routes

Existing users can observe that one configuration change on the Basic mode view might modify or change more than one setting in Advance mode. Basic mode does allow Importing of existing configurations, and allows you to move between Basic and Advanced modes.

The following figure shows the top-level screen of the Basic configuration mode. To display this screen, navigate to Configuration Editor > New > Basic.

Click the +Site button. The Site dialog presents the basic site details in the site list at the left-hand side and displays a Site Summary at the right-hand side. The Site Summary provides the ability to add, view, and edit site details for interfaces, WAN Links, and Static Routes.

WAN Link Templates

The WAN Link Templates functionality provides a way to set up a basic configuration for WAN Links and reuse these links
across the network to save time. The WAN Link Templates feature in both the Basic configuration mode and the advanced configuration mode, with minimal differences between the two modes.

To configure WAN Link templates by using the Basic configuration mode:

1. In the SD-WAN web management interface, navigate to Configuration Editor > New > Basic. Click Network to change from the (default) Sites view to the Network view.

2. Click + WAN Link Template to create a blank WAN Link Template.

3. After a WAN Link Template is added, it appears as one of the WAN Link Templates in the Network view in the Basic mode.
4. Existing WAN Link Template value can be used while adding new WAN Link from the existing WAN Link properties.

5. At this point, you can edit Appliance information entered in the previous step by clicking the Edit icon to the right of the Appliance settings in the summary view.
6. Clicking the **Add / Edit** Icon to the right of the **Interfaces** summary view shown for the site provides the ability to add, edit, and delete Interfaces.

The Interface option allows you to define the physical topology of the site, such as the ports, logical VLANs and security level for the physical ports. At this level, you can also define if the WAN interface uses DHCP for an IP address, or they may statically assign an IP address. This allows you to configure multiple options under the same panel.

7. Clicking the **Edit** Icon to the right of the WAN Links summary view shown for the site provides the ability to add, edit, and delete WAN Links.

While Adding or Editing a WAN Link, the option to use a WAN Link Template is provided. After selecting a WAN Link Template, the WAN Link can be configured using the WAN Link Template values. You have an option to overwrite the Template values if desired. Additionally once the Virtual Interface is selected, the IP address is automatically provided from the interface configuration.
8. Clicking the **Add / Edit** icon to the right of the **Static Routes** area will take you to the **Add / Edit Static Routes** dialog. Currently you only add local routes within the Basic configuration view.

After configuration, the summary view will display the site information configured and provide the ability to edit all items, as well as add more Interfaces, WAN Links, or Static Routes as needed.

The Basic view is intended to simplify the configuration process and provide you the ability to create a configuration file.
quickly and easily. For more complicated configurations, you can create a Basic configuration using this mode and then proceed to the advanced mode to complete the configuration.
How-To-Articles

Mar 30, 2017

NetScaler SD-WAN "How-to Articles" describe the procedure to configure the features supported by NetScaler SD-WAN. These articles contain information about some of the following important features:

Click a feature name in the table below to view the list of how-to articles for that feature.

| Virtual Routing and Forwarding | Enabling RED for QoS Fairness | Deployment |
| Dynamic Routing                | DHCP Client and Server Management | Route Filters |
| IPsec Termination and Monitoring | Secure Web Gateway | Configuration |
| FIPS Compliant Operation - IPSec Tunnels | Dynamic NAT Configuration | Adaptive Bandwidth Detection |
| Active Bandwidth Testing       | BGP Enhancements               | Service Class Association with SSL Profiles |
| WAN Link Templates - Basic Mode Configuration | Auto Secure Peering and Manual Secure Peering | Zero Touch Deployment |
| Two Box Mode Deployment        | IPSec Null Encryption          | SD-WAN SE/EE Hairpin Mode Deployment |
Virtual Routing and Forwarding

Oct 04, 2016

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

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

NetScaler SD-WAN appliances implement OSPF and BGP routing protocols for the routing domains to control and segment network traffic.

Following are the list of points to consider when configuring the VRF functionality:

- By default, routing domains are enabled on an MCN.
- Routing domains have to be enabled on the Branch sites.
- Each enabled routing domain should have a virtual interface and virtual IP associated with it.
- Routing selection is part of all the following configurations:
  - Interface group
  - Virtual IP
  - GRE
  - WAN Link -> Access Interface
  - IPSec tunnels
  - Routes
  - Rules

- Routing domains are exposed in the web interface configuration only when multiple domains are created.
- For a Public Internet link, only one primary and secondary access interfaces can be created.
- For a Private Intranet/MPLS link, one primary and secondary access interface can be created per routing domain.
How To Configure Routing Domain

Dec 14, 2016

NetScaler SD-WAN appliances enable configuring routing protocols providing single point of administration to manage a corporate network, or a branch office network, or a data center network.

To configure routing domain:

1. In the SD-WAN web interface, navigate to Configuration → Virtual WAN → Configuration Editor. In the Configuration Editor, navigate to Global → Routing Domains, click Add (+) and enter a Name for your new Routing Domain.

2. If you want to default to this Routing Domain, click the Default checkbox. Click Apply to save the changes. If you plan to implement a single Routing Domain, no explicit configuration is required.

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

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

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

Note

Unchecking Enable for a Routing Domain will make it unavailable for use at the Site.
To configure routes:

1. In the Configuration Editor, navigate to Connections → [Site Name] → Routes.

2. Choose a Routing Domain from the drop-down menu. New Routes are automatically associated with the default Routing Domain.

For detailed instructions, see configuring routes.

3. After you configure routes, validate the route tables for the configured routing domain by navigating to Configuration → Virtual WAN → View → Routes.
How To Select Routing Domain for Intranet Service

Oct 04, 2016
To select routing domain for intranet service:

1. In the Configuration Editor, navigate to Connections → [Site Name] → Intranet Services → [Intranet Service Name] → Basic Settings click the Edit () icon.

2. Choose a Routing Domain from the drop-down menu.
How To Configure Interface Groups

Dec 14, 2016

To configure interface groups:

1. In the **Configuration Editor**, navigate to Sites → [Client Site Name] → Interface Groups, choose a **Routing Domain** from the drop-down menu when configuring Virtual Interfaces.

For detailed instructions, see [configuring interface groups](https://docs.citrix.com).

**Note**

After Virtual Interfaces are associated with a specific Routing Domain, only those interfaces will be available when using that Routing Domain.

![Interface Groups configuration interface](image-url)
How To Configure Virtual IP Addresses

Dec 14, 2016
To configure Virtual IP Addresses:

1. In the Configuration Editor, navigate to Sites → [Client Site Name] → Virtual IP Addresses.

2. Choose a Routing Domain from the dropdown menu when configuring Virtual IP Addresses.

For detailed instructions, see configuring Virtual IP addresses.

The Routing Domain you choose determines which Virtual Interfaces are available from the drop-down menu.
How To Configure Virtual IP Address Identity

Oct 04, 2016
To configure Virtual IP Address identity:

1. In the Configuration Editor, navigate to Sites → [Site Name] → Virtual IP Addresses.

2. Click the Identity checkbox for a Virtual IP Address to use it for IP services.
How To Configure GRE Tunnels

Dec 14, 2016

To configure GRE Tunnels:

1. In the configuration editor, navigate to Connections > Site > GRE Tunnels. The source IP address can only be chosen from the Virtual network interface on trusted links.

2. Enter a name for the GRE Tunnel.

3. Select the Source IP address available from the drop-down menu. The Routing Domain determines which Source IP Addresses are available from the drop-down menu.

4. (Optional) Select the Public Source IP. This field can be empty if this address is the same as Source IP.

5. Enter the Destination IP address of the GRE Tunnel.

6. Enter the Tunnel IP/Prefix address of the GRE Tunnel.

7. Click Checksum, if you want to use checksum in the GRE Tunnel Header.

8. Enter a value for the Keepalive Period in seconds. If you configure 0, no keepalive packet are transmitted, but the GRE Tunnel will be active.

9. Enter a value for the Keepalive Retries. This value determines the number of times the keepalive retries are attempted before the SD-WAN appliance deactivates the GRE Tunnel.

Refer to the configuring GRE tunnels on the MCN site for more information.

For more information about securing web gateway using GRE tunnels, see; Secure Web Gateway
How To Configure Access Interface

Dec 14, 2016
To configure Access Interface:

1. In the Configuration Editor, navigate to Sites → [Client Site Name] → WAN Links → [WAN Link Name] → Access Interfaces.

2. Choose a Routing Domain from the drop-down menu when configuring an Access Interface.

For detailed instructions, see configuring WAN links and Access Interfaces.
How to Customize Classes

Jan 05, 2017

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

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

For more information about creating rules, see How to Create Rules.

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

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

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

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

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

**To customize classes:**

1. In the SD-WAN Configuration Editor, click **Global > Default Sets > Virtual Path Default Sets > New_Virtual_Path_Default_Set > Classes**.
2. Click the pencil icon.

3. In the Name field, either leave the default name or enter a name of your choice.

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

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

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

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

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

   * **Initial Period**: The time period, in milliseconds, during which to apply initial percentage of the available bandwidth before switching to the sustained percentage. Typically, 20 ms.

   * **Initial Share %**: The maximum share of virtual-path bandwidth during the initial period.

   * **Sustained Share %**: The maximum share of virtual-path bandwidth after the initial period.

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

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

8. Click Apply.

**Note**

Save the configuration, export it to the change management inbox, and initiate the change management process.
How to Add Custom Applications and Enable MOS

Jan 05, 2017

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

For more information about rules, see How to Create Rules.

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

SD-WAN Center calculates and displays the MOS for existing traffic that passes through the virtual path. For more information about viewing MOS in SD-WAN Center, see How to View MOS for Applications.

To add a custom application:

1. In the Configuration Editor, navigate to Global > Applications.

   The default list of applications appears.

2. Click the add (+) icon.

3. Enter the application name.
4. Click the pencil icon and select **Estimate MOS**.

5. Click **Apply**.

**Note**

You can also enable MOS estimation for the default applications, by clicking the pencil icon and selecting **Estimate MOS**.

**Note**

Enable the Track Performance option under Rules to estimate MOS for applications and display it in SD-WAN Center. For more information about rules, see How to Create Rules.
How to Create Rules

Jan 06, 2017

Using the configuration editor, you can create rules for traffic flow and associate the rules with applications and classes. You can specify criteria to filter traffic for a flow, and can apply general behavior, LAN to WAN behavior, WAN to LAN behavior, and packet inspection rules.

To create rules:

1. In the Configuration Editor, navigate to Default Set > Virtual Path Default Set > New_Virtual_Path_Default_Sets > Rules and click the plus (+) icon to add a new custom rule.

2. In the Order field, enter the order value to define when the rule is applied in relation to other rules.

3. In the Application field, select an application. The statistics for rules with the same application name will be grouped together as a rule group and can be viewed together.

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

   You can also add custom applications. For more information, see How to add Custom Applications and Enable MOS.

4. In the Routing Domain field, choose one of the configured routing domains.

5. You can define rule matching criteria to filter services on the basis of the parameters listed below. After the filtering, the rule settings are applied to the services matching these criteria.

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

   * **Protocol:** Protocol to match against the traffic.
   
   * **Source Port:** Source port number or port range to match against the traffic.
   
   * **Destination Port:** Destination port number or port range to match against the traffic.
   
   * **DSCP:** The DSCP tag in the IP header to match against the traffic.
   
   * **VLAN:** The VLAN ID to match against the traffic.

   **Note**

   Select Dest=Src, if the source and destination IP address are the same.
6. Click the add (+) icon next to the new rule.

7. Click Initialize Properties Using Protocol to initialize the rule properties by applying the rule defaults and recommended settings for the protocol. This will populate the default rule settings. You can also customize the settings manually, as shown in the following steps.

8. Click the WAN General tile to configure the following properties.

   * **Transmit Mode**: Select one of the following transmit modes.
     - **Load Balance Path**: Traffic for the flow will be balanced across multiple paths for the service. Traffic will be sent through the best path until that path is completely used. Leftover packets will be sent through the next best path.
     - **Persistent Path**: Traffic for the flow will remain on the same path until the path is no longer available.
     - **Duplicate Path**: Traffic for the flow is duplicated across multiple paths, increasing reliability.
     - **Override Service**: Traffic for the flow will override to a different service. In the Override Service field, select the service type to which the service will override. For example, a virtual path service could override to an intranet, internet, or pass-through service.

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

   * **Enable TCP Termination**: Enable TCP termination of traffic for this flow. This reduces the round-trip time for acknowledgement packets and therefore improves throughput.

   * **Enable IP, TCP and UDP**: Compress headers in IP, TCP and UDP packets.

   * **Enable GRE**: Compress headers in GRE packets.

   * **Enable Packet Aggregation**: Aggregate small packets into larger packets.

   * **Track Performance**: Records performance attributes of this rule in a session data base (for example, loss, jitter, latency and bandwidth).

9. Click the LAN to WAN tile, to configure LAN to WAN behavior for this rule.

   * **Class**: Select a class with which to associate this rule.
**Note**
You can also customize classes before applying rules, for more information, see [How to Customize Classes](#).

* **Large Packet Size**: Packets smaller than or equal to this size are assigned the **Drop Limit** and **Drop Depth** values specified in the fields to the right of the **Class** field.

* **Drop Limit**: Length of time after which packets waiting in the class scheduler are dropped. Not applicable for a bulk class.
* **Drop Depth**: Queue depth threshold after which packets are dropped.

* **Enable RED**: Random Early Detection (RED) ensures fair sharing of class resources by discarding packets when congestion occurs.

* **Reassign Size**: Packet length that, when exceeded, causes the packet to be reassigned to the class specified in the Reassign Class field.

* **Reassign Class**: Class used when the packet length exceeds the packet length specified in the Reassign Size field.

* **Disable Limit**: Time for which duplication can be disabled to prevent duplicate packets from consuming bandwidth.

* **Disable Depth**: The queue depth of the class scheduler, at which point the duplicate packets will not be generated.

* **TCP Standalone ACK class**: High priority class to which TCP standalone acknowledgements are mapped during large file transfers.

10. Click the **WAN to LAN** tile to configure WAN to LAN behavior for this rule.

* **Enable Packets Resequencing**: Sequences the packets into the correct order at the destination.

* **Hold Time**: Time interval for which the packets are held for resequencing, after which the packets are sent to the
LAN.

* **DiscardLateResequencing Packets:** Discard out-of-order packets that arrived after the packets needed for resequencing have been sent to the LAN.

* **DSCP Tag:** DSCP tag applied to the packets that match this rule, before sending them to the LAN.

11. Click **Deep Packet Inspection** tile and select **Enable Passive FTP Detection** to allow the rule to detect the port used for FTP data transfer and automatically apply the rule settings to the detected port.

12. Click **Apply**.

**Note**

Save the configuration, export it to the change management inbox, and initiate the change management process.
How To Configure Firewall Segmentation

Mar 20, 2017

NetScaler SD-WAN 9.2 introduces VRF firewall segmentation to give multiple routing domains access to the internet through a common interface, with each domain's traffic isolated from that of the others. For example, employees and guests can access the internet through the same interface, without any access to each other's traffic.

- Local guest-user Internet access
- Employee-user Internet access for defined applications
- Employee-users may continue hairpin all other traffic to the MCN
- Allow the user to add specific routes for specific routing domains.
- When enabled, this feature applies to all routing domains.

You can also create multiple access interfaces to accommodate separate public facing IP addresses. Either option provides the required security necessary for each user group.

Note
For more information, see how to configure VRFs.

To configure internet services for all Routing Domains:

1. Create Internet Service for a Site. Navigate to Connections > [Site Name] > Internet Services and and, under WAN Links, select the Use check box.

2. Navigate to Sites > [Site Name] > WAN Links > [WAN Link Name] > Access Interfaces and select the Internet Access for All Routing Domains check box.

Selecting this check box allows SD-WAN to use this access interface for internet service on all configured routing domains. The check box is grayed out if two or more access interfaces are configured for the same WAN link. You can configure
either a shared access interface or one access interface for each group (separate public-facing IP addresses).

**Note**

After completing the following steps you should see 0.0.0.0/0 routes added, one per routing domain, under **Connections > [Site Name] > Routes**.

It is no longer required to have all routing domains enabled at the MCN.

If you disable routing domains at the MCN, the following message appears if the domains are in use at a branch site:
You can confirm that each routing domain is using the internet service by checking the Routing Domain column in the Flows table of the web management interface under Monitor > Flows.

You can also check the routing table for each routing domain under Monitor > Statistics > Routes.

Use Cases

In previous NetScaler SD-WAN releases, virtual routing and forwarding have the following issues:

- 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.

Release 9.2 introduces the following enhancements to address the above concerns:

- 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 required
- Routing domains are VLAN based
- Removes the requirement for the RD to have to reside at the MCN
- Routing Domain can now be configured at a branch site only
- Allows you to assign multiple RD to an access interface (once enabled)
- Each RD will be assigned a 0.0.0.0 route
- Allows specific routes to be added for a RD
- Allows traffic from different RD to exit to the internet using the same access interface
- Allows you to configure a different access interface for each RD
- Must be unique subnets (RD are assigned to a VLAN)
- Each RD can use the same FW default Zone
- The traffic is isolated through the Routing Domain
- Outbound flows have the RD as a component of the flow header. Allows SD-WAN to map return flows to correct Routing domain.

Prerequisites to configure multiple routing domains:

- Internet access is configured and assigned to a WAN Link.
- Firewall configured for NAT and correct policies applied.
- Second routing domain added globally.
- Each routing domain added to a site.
- At Sites > Site Name > WAN Links > WL [name] > Access Interface, make sure that the check box is available and internet service has been defined correctly. If you cannot select the check box, the internet service is not defined or assigned to a WAN link for the site.

Deployment Scenarios
The internet service must be added to the WAN link before you can enable Internet access for all Routing Domains. (Until you do, the check box for enabling this option is grayed out).

After enabling internet access for all routing domains, auto add a dynamic-NAT rule.

- Up to 16 Routing Domains per site.
- Access Interface (AI): Single AI per subnet.
  - Multiple AIs require a separate VLAN for each AI.
  - If you have two routing domains at a site and have a single WAN Link, both domains use the same public IP address.
- If Internet access for all routing domains is enabled, all sites can route to Internet. (If one routing domain does not require internet access, you can use the firewall to block its traffic.)
- No support for the same subnet in multiple routing domains.
- There is no audit functionality

- The WAN links are shared for Internet access.
- No QOS per routing domain; first come first serve.
Dynamic Routing

Mar 30, 2017

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

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

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

You can now configure NetScaler SD-WAN appliances (Standard and Enterprise Editions) to learn routes and advertise routes using OSPF.

Note
- NetScaler SD-WAN appliances do not participate as Designated Router (DR) and BDR (Backup Designated Router) on each multi-access network since the default DR priority is set to “0”.
- NetScaler SD-WAN appliances do not support summarization as an Area Border Router (ABR).

To configure OSPF:

1. In the Configuration Editor, navigate to Connections → [Site Name] → Route Learning → OSPF → Basic Settings and click the Edit () icon.
2. Click the Enable checkbox, enter an optional Router ID.

Note
If the Router ID is not specified, it will be auto-selected as the lowest Virtual IP hosted in the SD-WAN network.

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

4. Expand **OSPF -> Area**, and click **Edit**.

5. Enter an **area ID** to learn routes from and advertise to.

6. For sites with multiple Routing Domains, from the **Virtual Interfaces** panel, choose a **Routing Domain** from the drop-down menu as illustrated in the figure. The Routing Domain determines which Virtual Interfaces are available.

**Note**

If there is only one Routing Domain configured, the Routing Domain column will not appear. If Identity is not checked for a specific Virtual IP Address, the associated Virtual Interface will not be available for IP services. For more information, see the Virtual IP Address Identity section.

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

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

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

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

11. In the **Hello Interval** field, enter the amount of time to wait between sending Hello protocol packets to directly connected neighbors (10 seconds is the default).
12. In the **Dead Interval** field, enter the amount of time to wait to receive a Hello protocol packet before marking a router as dead (40 seconds is the default).

13. Click **Apply** to save your changes.

**Stub Area**

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

Enable the **Stub Area** check box.

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

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

**To configure BGP:**

1. In the **Configuration Editor**, navigate to **Connections** → [Site Name] → **Route Learning** → **BGP** → **Basic Settings** and click the **Edit** icon.

2. Click the **Enable** checkbox and the **Advertise NetScaler SD-WAN Routes** checkbox if you want to advertise NetScaler SD-WAN Routes. Enter an optional **Router ID**, and enter the number of the Local Autonomous System to learn routes from and advertise routes to in the **Local Autonomous System** field. The routes advertise or redistribute the SD-WAN virtual path routes to peer routes with whom adjacency or peering is established so that the peer routes are aware of being able to reach those network prefixes through the SD-WAN network.

3. Click **Apply** to enable BGP.
4. Expand BGP → Basic Settings → Neighbors and click the Add (+) icon.

**Note**

If there is only one Routing Domain configured, the Routing Domain column will not appear. If Identity is not checked for a specific Virtual IP Address (see the Virtual IP Address Identity section for more details), the associated Virtual Interface will not be available for IP services.

5. For Sites with multiple Routing Domains, choose a Routing Domain from the drop-down.

The Routing Domain determines which Virtual Interfaces are available.

6. Choose a Virtual Interface from the drop-down menu. The Virtual Interface will determine the Source IP Address.

7. Enter the IP Address of the IBGP Neighbor router in the Neighbor IP field.

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

9. In the Local Preference (s) field, enter the Local Preference value, in seconds, which is used for selection from multiple BGP routes (the default is 100).

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

11. Click the Multi Hop checkbox to enable multiple hops for the route.

12. In the Password field, enter a password for MD5 authentication of BGP sessions (authentication is not required).

**Note**

Configuring Route Reflectors and Confederations for iBGP is not supported in a NetScaler SD-WAN network.
1. Navigate to **Monitor → Statistics**. Select **Routes** from the **Show** drop-down menu.

All functions for applicable Routes are supported in NetScaler SD-WAN regardless of whether a Route is Dynamic or Static.

NetScaler SD-WAN appliances connect to a switch on the LAN side and a Router on the WAN side. As SD-WAN technology starts becoming more integral to Enterprise network deployments, SD-WAN appliances will replace the Routers. SD-WAN implements eBGP dynamic routing protocol to function as a dedicated routing device.

SD-WAN appliance establishes neighbourship with peer routers using eBGP towards WAN side and is able to learn, advertise routes from and to peers. You can select importing and exporting eBGP learned routes on peer devices. Also, SD-WAN static, virtual path learned routes can be configured to advertise to eBGP peers.

For more information, refer to the following use cases:
- SD-WAN site Communicating with non SD-WAN site over eBGP
- Communication Between SD-WAN sites Using Virtual Path and eBGP
- Implementing OSPF in one-arm topology
- OSPF Type5 to Type1 deployment in MPLS Network
- SD-WAN and non SD-WAN (third-party) appliance OSPF deployment
- Implementing OSPF using SD-WAN network with high-availability setup
OSPF

Dec 27, 2016

OSPF running on the LAN port of Netscaler SD-WAN appliance deployed in Gateway Mode

SD-WAN appliances perform route discovery of Layer 3 routing advertisements within a local customer network (both branch and data center) for each of the desired routing protocols (OSPF and BGP). The routes that are learnt are dynamically captured and displayed.

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

NetScaler SD-WAN appliance having an AREA defined as a STUB area by limiting the learning of Type 5 AS-external LSA.

SD-WAN appliances can advertise the locally learned dynamic routes with the MCN. The MCN can then relay these routes to other SD-WAN appliances in the network. This exchange of information dynamically allows for maintaining connectivity between sites across the changing network.

In previous releases, OSPF instance learned routes from SD-WAN were treated as external routes with Type 5 LSA only. These routes were advertised to its neighbor routers in Type 5 External LSA. This resulted in SD-WAN routes to be less preferred routes according to the OSPF path selection algorithm.

With the latest release, SD-WAN can now advertise routes as intra-area routes (LSA Type 1) to get preference as per its route cost using the OSPF path selection algorithm. The route cost can be configured and advertised to the neighbor router. This allows for deploying SD-WAN appliance in one-arm mode described below.

Implementing OSPF in One-Arm Topology

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

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

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

You should be able to see following route types under Export OSPF Route Type
- Type 5 AS External
- Type 1 Intra Area

You should be able to configure Type 5 AS External route.

After activation of the changed configuration, you should see the Route Type changes under Configuration->[Virtual WAN]->View Configuration->[Dynamic Routing].

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

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

OSPF Type5 to Type1 Deployment in MPLS Network

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

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

**Recommended Configuration:**

a. DC VW and **ME-DC_Router** on area0

b. **ME-BR1_Router** and **ME-DC_Router** on area0

c. **BR1 VW** and **ME-BR1_Router** on area0

On the **ME-DC_Router**:

a. Add, static route for 172.58.3.10/32 (Virtual IP of BR1 for MPLS Link) through 172.58.6.1

b. Add, static route for 172.58.4.10/32 (Virtual IP of BR1 for INET) through 172.58.5.1

Adding static routes prevents loop formation between the **ME-DC_Router** and **DC SD-WAN appliance**. If you do not add static routes, the MCN forwards traffic to the **ME-DC Router**, and back from router to the MCN and this creates a loop continuously.

The static routes which are not PBR routes but the destination Host IP based routes will traverse towards the right link to be chosen from the DC side based on the path chosen and the encapsulation performed thereafter. Therefore, with these static routes configured, the encapsulated packets with any destination Virtual IP of BR1 SD-WAN appliance would use these links as per the best path selected by the DC MCN.

Add ACL to avoid loop formation when IPHOST routes are installed (if no static Virtual IPs configured):

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

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

**On the ME-BR1_Router:**

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

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

b. If the ME-BR1_Router is also advertising 172.58.3.0/24 as an internal OSPF type 1 route alongside DC (SD-WAN) which also advertises the same prefix as interal ospf Type 1 route, then according to cost computation, by default the ME-BR1_Router's route will be configured, as the cost is lesser than SD-WAN's default cost of 5. To avoid this and make SD-WAN appliance chosen as preferred route initially, the interface cost of (172.58.3.1) needs to be manipulated to make it higher on the ME-BR1_Router so that DC SD-WAN route is configured in the routing table of the ME-DC_Router.

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

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

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

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

1. Configure Virtual Interfaces and WAN links on both DC and Branch sites to create Virtual Path between them.
2. Under Connections->[MCN]-->Route Learning-->OSPF-->Basic Settings, select Export OSPF Route Type to be Type 1 Intra Area.
3. Save the configuration, stage and activate the same.
4. You should be able to see following two route types under Export OSPF Route Type
   - Type 5 AS External
   - Type 1 Intra Area

5. After activation of the changed config, you can see the Route Type changes under Configuration-->Virtual WAN-->View Configuration-->Dynamic Routing.

6. Routes should be advertised as Type5 External AS by the SD-WAN appliance. Routes learnt through SD-WAN should be displayed in the neighboring routers as Type5 AS External routes.

**To configure OSPF exported route weight under Basic OSPF Settings**
1. Configure Virtual Interfaces and WAN links on both DC and Branch sites to create Virtual Path between them.

2. Under Connections->[MCN]->Route Learning->OSPF->Basic Settings, configure Export OSPF Route Weight.

3. Save the configuration, stage and activate the same.

4. Now, configure Export OSPF Route Weight to any numeric value between 1 to 65529.

5. After activation of the changed config, you can see the Route Weight under Configuration->Virtual WAN->View Configuration->Dynamic Routing.

6. The default route weight exported should be 0. Actual cost of the route should only be the cost of SD-WAN.

To configure OSPF exported routes as Type1 under Export Filter settings

1. Configure Virtual Interfaces and WAN links on both DC and Branch so that we can create Virtual Path between them.

2. Under Connections->[MCN]->Route Learning->OSPF->Export Filters configure an export filter.

3. Expand the filter. Configure Export OSPF Route Type to Type 1 Intra Area route.

4. Save the configuration, stage and activate the same.

5. You should be able to see following two route types under Export OSPF Route Type

   - Type 5 AS External
   - Type 1 Intra Area

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

To configure OSPF exported route weight under Export Filter settings

1. Configure Virtual Interfaces and WAN links on both DC and Branch so that we can create Virtual Path between them.

2. Under Connections->[MCN]->Route Learning->OSPF->Export Filters configure an export filter.

3. Expand the filter. Configure Export OSPF Route Weight to any numeric value between 1 to 65529.

4. Save the configuration, stage and activate the same.

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

6. Route Weight configured under Export Filter should override the Weight configured under Basic OSPF Settings.

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

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

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

Verifying Configuration

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

Traffic flow can be observed in the SD-WAN GUI under **Monitoring->Flows**.
**OSPF Type5 to Type1 with high-availability sites during failover to standby appliance and deployed in high-availability setup**

To configure OSPF in HA deployment:

1. Configure **Virtual Interfaces** and **WAN links** on both DC and Branch to create Virtual Path between them.
2. Setup High-Availability.
3. Export **Route Type** configured as **Type 1** and **Route Weight** as 50.
4. Save the configuration, stage and activate the same.
5. Start traffic flow.
6. Observe that under **Monitor->Statistics->Routes**, the hit count increases for OSPF routes with least costs.
7. Bring the Active MCN down and observe the behavior.
8. Bring the original Active MCN back up.
9. The **Dashboard->High Availability Status** shows correctly for HA Local Appliance and Peer Appliance for Active and Standby.
10. Under **Configuration->View Configuration->Dynamic Routing**, OSPF is enabled and **export_ospf_route_type** shows **Type1** and **export_ospf_route_weight** as 50.
11. Even after failover the High Availability Status shows correct OSPF configuration for Local and Peer Appliance.
12. View **Monitor->Statistics->Routes**. The hit count increases for OSPF routes with least costs.
13. After failback, the High Availability Status shows correct OSPF configuration for Local and Peer Appliance.
14. Verify that the hit count increases for OSPF routes with low cost under view **Monitor->Statistics->Routes**.
BGP enhancements in release 9.2 enable users to:

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

**Note**
Configuring eBGP with a different neighbour AS is not supported. Also, only local preference and IGP metric for path selection and manipulation is allowed.

In the SD-WAN web management interface, the configuration editor has a new section, BGP policy, under **Route Learning > BGP**. In this section, users can add BGP attributes that constitute a policy. Adding community strings, prepending AS path prepend, and configuring MED are supported.

You can manually configure each community string or select no advertise or no export community string from a drop-down menu. For manual configuration, you can enter an AS number and community. You can select Insert/Remove to tag the routes or remove the community from the routes.

You can configure the number of times you want to prepend the local AS to the AS Path before advertising outside the local network. You can configure MED for matching routes.

To configure BGP policy:

1. In the NetScaler SD-WAN web management interface, go to **Configuration > Virtual WAN > Configuration Editor**. Open an existing configuration package. Go to **Sites > DC or Branch settings**.
2. Expand BGP and click Enable under Basic Settings. Enter Router ID and Local Autonomous System value and click Apply.

3. Click + sign next to the Community String Lists. Configure each community string manually or by selecting no advertise or no export community string from the drop-down menu. For manual configuration, you can enter an AS number and community. You can select Insert/Remove tag the routes with the community string or remove the community string from the routes received from the peers.
4. Configure BGP policy by expanding **BGP Policies**. Add BGP attributes to the **New Route Policy**.

5. Click the + sign next to **Attributes** to edit BGP attributes. The **Edit Attributes** window is displayed. Select the desired BGP attribute from the drop-down menu. Enter the desired value for **MED**, **AS Prepend Length**, or **Community String** as per your selection. Click **Apply**.
Note

Any policy can have only one occurrence of an attribute and cannot take multiple occurrence of the same attribute. You cannot have 2 MED or 2 AS Path Prepend. It can have either MED/AS-PATH Prepend/Community String or a combination.

To configure eBGP, an additional column to the existing BGP neighbors section is added to configure neighbor AS number. The existing configurations are pre-populated to this field with the local AS number when you import previous configuration using the SD-WAN 9.2 configuration editor.

The neighbor configuration also has an optional advanced section (expandable row) where you can add Policies for each neighbor.

With this option, you can add network objects and add a configured BGP policy for that network object. This is similar to creating a route map and ACL to match certain routes and configuring BGP attributes for that neighbor. You can specify the direction to indicate if this policy is applied for incoming or outgoing routes.

The default policy is to <accept> all routes. Note that accept and reject policies are defaults and cannot be modified.

You have the ability to match routes based on Network address (destination address), AS Path, Community string and assign a policy and select direction for the policy to be applied.

To configure neighbors:

1. Configure neighbors by clicking Add as shown below.

2. Click the + sign. Select a Virtual Interface. Enter the Neighbor IP address.
3. Add policies. Select **Network Address**, **BGP Community**, and **AS Path** details as desired. Click **Apply**.
4. Go to Monitoring > Routing Protocols > Dynamic Routing Protocols to monitor the configured BGP policies and neighbors for the DC or Branch site appliance.

You can enable debug logging and to view log files for routing from the Monitor > Routing Protocol page. The logs for the routing daemon are split into separate log files. The standard routing information is stored in `dynamic_routing.log` while dynamic routing issues are captured in `dynamic_routing_diagnostics.log` which can be viewed from monitoring of routing protocols.
**iBGP**

Dec 14, 2016

**Netscaler SD-WAN appliance with iBGP on the LAN side and eBGP on the WAN side**

Netscaler SD-WAN appliances advertise all the eBGP routes learnt into the IGP domain with NEXT HOP SELF when deployed with iBGP on the LAN side and eBGP on the WAN side.

**Multiple iBGP LAN Routers in a Linear Network Topology with Direct Peering and meshed with NetScaler SD-WAN**

Limitations:

- AS-Path prepend, Med, and Community attributes are not supported.
- Route filtering between OSPF and BGP during redistribution is not supported. Either all (or) none of the routes learned from OSPF are advertised to BGP peers and vice-versa.
- Route aggregation is not supported.
- Only a Max of 16 BGP peers (including iBGP and eBGP) can be configured.
**eBGP**

Dec 14, 2016

**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.
Route Filtering

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

1. In the Configuration Editor, navigate to Connections → [Site Name] → Route Learning.
2. Expand Import Filters and Export Filters to view the existing route filters. Import Filters are separate and distinct from Export Filters. You can configure up to 32 Export Filters.

Note
If there is only one Routing Domain configured, the Routing Domain column will not appear.

![Configuration Editor](image)

Use the following criteria to construct each Export Filter that you want to create.

<table>
<thead>
<tr>
<th>Field Criteria</th>
<th>Description</th>
<th>Value(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>The Order in which filters are prioritized. The first filter that a route matches to will be applied to that route.</td>
<td>100, 200, 300, 400, 500, 600</td>
</tr>
<tr>
<td>Field Criteria</td>
<td>Description</td>
<td>Value(s)</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>Network Address</td>
<td>Enter the IP Address and Netmask or configured Network Object that describes the route's network.</td>
<td>IP address, eq: Equal to, lt: Less than, le: Less than or equal to, gt: Greater than, ge: Greater than or equal to</td>
</tr>
<tr>
<td>Prefix</td>
<td>To match routes by prefix, choose a match predicate from the drop-down menu and enter a Route prefix in the adjacent field.</td>
<td></td>
</tr>
<tr>
<td>NetScaler SD-WAN Cost</td>
<td>The method (predicate) and the SD-WAN Route Cost that are used to narrow the selection of routes exported.</td>
<td>Numeric value</td>
</tr>
<tr>
<td>Service Type</td>
<td>Select the Service types that will be assigned to matching routes from a list of the existing, supported NetScaler SD-WAN Services.</td>
<td>Service Types: Any, Local, Virtual Path, Internet, Intranet, LAN GRE Tunnel, LAN IPsec Tunnel</td>
</tr>
<tr>
<td>Site/Service Name</td>
<td>For Intranet, LAN GRE Tunnel, and LAN IPsec Tunnel, specify the name of the configured Service Type to use.</td>
<td>Text string</td>
</tr>
<tr>
<td>Gateway IP Address</td>
<td>If you choose LAN GRE Tunnel as the Service Type, enter the Gateway IP for the tunnel.</td>
<td>IP address</td>
</tr>
<tr>
<td>Include</td>
<td>Click the checkbox to Include routes that match this filter. Otherwise matching routes are ignored.</td>
<td>None</td>
</tr>
<tr>
<td>Enabled</td>
<td>Click the checkbox to Enable this filter. Otherwise the filter is ignored</td>
<td>None</td>
</tr>
<tr>
<td>Clone</td>
<td>Click the Clone icon to make copy of an existing Filter.</td>
<td>None</td>
</tr>
</tbody>
</table>
IPSec Tunnel Termination

Mar 30, 2017
NetScaler SD-WAN supports IPsec virtual paths, enabling third-party devices to terminate IPsec VPN Tunnels on the LAN or WAN side of a NetScaler SD-WAN appliance. You can secure site-to-site IPsec Tunnels terminating on an SD-WAN appliance by using a 140-2 Level 1 FIPS certified IPsec cryptographic binary.

SD-WAN also supports resilient IPsec tunneling using a differentiated virtual path tunneling mechanism.
How to Configure IPSec Tunnels for Virtual and Dynamic Paths

Oct 04, 2016
To configure IPSec Tunnels for Virtual and Dynamic Virtual Paths between SD-WAN branch sites:

1. Navigate to Global → Virtual Path Default Sets or Dynamic Virtual Path Default Sets.

2. Create new default set (virtual or dynamic virtual path), and enable Secure Virtual Path User Data with IPsec.

3. Choose one of the available options for IPsec encryption:
   * Encapsulation types: ESP, AH, or ESP+AH
   * Encryption Modes: AES 128, or 256-Bit
   * Hash Algorithm: SHA1 or SHA-256

4. Apply the created Virtual Path Default Set to the MCN node. This automatically applies the same default set to all Client nodes that have Virtual Path to the MCN.
How To Configure IPsec Tunnel Between SD-WAN and Third-Party Devices

Oct 04, 2016
To configure IPsec Tunnel for Intranet or LAN service:

1. In the Configuration Editor, navigate to Connections → [Site Name] → IPsec Tunnels. Choose a Service Type (LAN or Intranet).

2. Enter a Name for the service type. For Intranet service type, the configured Intranet Server will determine which Local IP addresses are available.

3. Select the available Local IP address and enter the Peer IP address for the virtual path to peer with.

Note
If the Service Type is Intranet, the IP address is pre-determined by the chosen Intranet Service.

4. Configure IPsec settings by applying the criteria described in the following tables. When finished, click Apply to save your settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Type</td>
<td>Choose a service type from the drop-down menu.</td>
<td>• Intranet • LAN</td>
</tr>
<tr>
<td>Name</td>
<td>If the service type is Intranet, choose from the list of configured Intranet services in the drop-down menu. If the service type is LAN,</td>
<td>• Text string</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Values (s)</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Local IP</td>
<td>Description: the IP address of the IPsec Tunnel from the drop-down menu of</td>
<td>IP address</td>
</tr>
<tr>
<td></td>
<td>available virtual IP addresses configured at this Site.</td>
<td></td>
</tr>
<tr>
<td>Peer IP</td>
<td>Enter the peer IP address of the IPsec Tunnel.</td>
<td>IP address</td>
</tr>
<tr>
<td>MTU</td>
<td>Enter the MTU for fragmenting IKE and IPSec fragments</td>
<td>Default: 1500</td>
</tr>
<tr>
<td>IKEv1 Settings</td>
<td><strong>Version</strong>: Choose an IKE version from the drop-down menu.</td>
<td>IKEv1, IKEv2</td>
</tr>
<tr>
<td></td>
<td><strong>Mode</strong>: Choose a mode from the drop-down menu.</td>
<td>Main, Aggressive</td>
</tr>
<tr>
<td></td>
<td><strong>Identity</strong>: Choose an Identity from the drop-down menu.</td>
<td>Auto, IP Address</td>
</tr>
<tr>
<td></td>
<td><strong>Authentication</strong>: Choose the authentication type from the drop-down menu.</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td></td>
<td>If you are using a pre-shared key, copy and paste it into this field. Click</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on the Eyeball ( ) icon to view the Pre-Shared Key.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Validate Peer Identity</strong>: Click this checkbox to validate the IKE's peer.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>If the peer's ID type is not supported, do not enable this feature.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>DH Group</strong>: Choose the Diffie–Hellman group to use for IKE key generation</td>
<td>Group 1, Group 2, Group 5</td>
</tr>
<tr>
<td></td>
<td>from the drop-down menu.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Hash Algorithm</strong>: Choose an algorithm from the drop-down menu to</td>
<td>MD5, SHA1, SHA-254</td>
</tr>
<tr>
<td></td>
<td>authenticate IKE messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Encryption Mode</strong>: Choose the Encryption Mode for IKE messages from the</td>
<td>AES 128-bit, AES 192-bit, AES 256-bit</td>
</tr>
<tr>
<td></td>
<td>drop-down menu.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Lifetime (s)</strong>: Enter the preferred duration, in seconds, for an IKE</td>
<td>3600 seconds (default)</td>
</tr>
<tr>
<td></td>
<td>security association to exist.</td>
<td></td>
</tr>
</tbody>
</table>
### IPsec and IPsec Protected Network Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Values (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lifetime Max (s)</strong></td>
<td>Enter the maximum preferred duration, in seconds, to allow an IKE security association to exist.</td>
<td>86400 seconds (default)</td>
</tr>
<tr>
<td><strong>DPD Timeout (s)</strong></td>
<td>Enter the Dead Peer Detection timeout, in seconds, for VPN connections.</td>
<td></td>
</tr>
<tr>
<td><strong>Peer Authentication</strong></td>
<td>Choose Peer Authentication from the drop-down menu.</td>
<td>Mirrored, Pre-Shared Key, Certificate</td>
</tr>
<tr>
<td><strong>Peer Pre-Shared Key</strong></td>
<td>Paste the IKEv2 Peer Pre-Shared Key into this field for authentication.</td>
<td>Text string</td>
</tr>
<tr>
<td><strong>Integrity Algorithm</strong></td>
<td>Choose an algorithm as the hashing algorithm to use for HMAC verification from the drop-down menu.</td>
<td>MD5, SHA, SHA-256</td>
</tr>
</tbody>
</table>

---

IPsec and IPsec Protected Network Settings
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Value (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tunnel Type</strong></td>
<td>Choose the Tunnel Type from the drop-down menu.</td>
<td>• ESP&lt;br&gt;• ESP+Auth&lt;br&gt;• ESP + NULL&lt;br&gt;• AH</td>
</tr>
<tr>
<td><strong>PFS Group</strong></td>
<td>Choose the Diffie–Hellman group to use for perfect forward secrecy key generation from the drop-down menu.</td>
<td>• Group 1&lt;br&gt;• Group 2&lt;br&gt;• Group 5&lt;br&gt;• If you chose ESP or ESP+ Auth, select either one of the following:&lt;br&gt;• AES 128-bit&lt;br&gt;• AES 192-bit&lt;br&gt;• AES 256-bit</td>
</tr>
<tr>
<td><strong>Encryption Mode</strong></td>
<td>Choose the Encryption Mode for IPsec messages from the drop-down menu.</td>
<td>If you chose ESP or ESP+ Auth, select either one of the following:&lt;br&gt;• AES 128-bit&lt;br&gt;• AES 192-bit&lt;br&gt;• AES 256-bit</td>
</tr>
<tr>
<td><strong>Lifetime (s)</strong></td>
<td>Enter the amount of time, in seconds to allow an IPsec security association to exist.</td>
<td>• 28800 seconds (default)</td>
</tr>
<tr>
<td><strong>Lifetime Max (s)</strong></td>
<td>Enter the maximum amount of time, in seconds to allow an IPsec security association to exist.</td>
<td>• 86400 seconds (default)</td>
</tr>
<tr>
<td><strong>Lifetime (KB)</strong></td>
<td>Enter the amount of data, in kilobytes, for an IPsec security association to exist.</td>
<td>• Kilobytes</td>
</tr>
<tr>
<td><strong>Lifetime (KB) Max</strong></td>
<td>Enter the maximum amount of data, in kilobytes, to allow an IPsec security association to exist.</td>
<td>• Kilobytes</td>
</tr>
<tr>
<td><strong>Network Mismatch Behavior</strong></td>
<td>Choose the action to take if a packet does not match the IPsec Tunnel's Protected Networks from the drop-down menu.</td>
<td>• Drop&lt;br&gt;• Send Unencrypted&lt;br&gt;• Use Non-IPsec Route</td>
</tr>
<tr>
<td><strong>Source IP/Prefix</strong></td>
<td>After clicking the Add (+ Add) button, enter the Source IP and Prefix of the network traffic the IPsec Tunnel will protect.</td>
<td>• IP address</td>
</tr>
<tr>
<td><strong>Destination IP/Prefix</strong></td>
<td>Enter the Destination IP and Prefix of the network traffic the IPsec Tunnel will protect.</td>
<td>• IP address</td>
</tr>
</tbody>
</table>
IPsec Settings

Tunnel Type:
ESP

PFS Group:
<None>

Encryption Mode:
AH+ESP

Hash Algorithm:
SHA1

Lifetime (s) ESP:
20000

Lifetime (KB) ESP:
0

Network Mismatch Behavior:
Drop

IPsec Protected Networks

<table>
<thead>
<tr>
<th>Source IP/Prefix</th>
<th>Destination IP/Prefix</th>
<th>Delete</th>
</tr>
</thead>
</table>

Apply Revert
How To Add IKE Certificates

Oct 04, 2016
To implement certificates for IKE negotiation:

1. Navigate to Sites → Certificates and add any necessary certificates.
How To View IPSec Tunnel Configuration

Oct 04, 2016

To view IPSec tunnel configuration:

1. Navigate to **Configuration → Virtual WAN → View Configuration**.

2. Select **Virtual Path Service** from the drop-down menu. The IPsec settings are displayed only if IPsec is enabled in the configuration editor.

3. Select **IPsec Tunnels** from the drop-down menu to view the IPsec Tunnel configuration.

4. Each virtual path will show its own IPsec tunnel status as shown below.
### System Status

<table>
<thead>
<tr>
<th>Name</th>
<th>MCN1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>VPN</td>
</tr>
<tr>
<td>Appliance Mode</td>
<td>MCN</td>
</tr>
<tr>
<td>Management IP Address</td>
<td>10.105.184.82</td>
</tr>
<tr>
<td>Appliance Uptime</td>
<td>6 hours, 19 minutes, 6.0 seconds</td>
</tr>
<tr>
<td>Service Uptime</td>
<td>6 hours, 17 minutes, 48.0 seconds</td>
</tr>
</tbody>
</table>

### Virtual Path Service Status

<table>
<thead>
<tr>
<th>Virtual Path</th>
<th>Uptime</th>
<th>Proc state</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCN1-BR1</td>
<td>6 hours, 17 minutes, 34.0 seconds</td>
<td>GOOD</td>
</tr>
<tr>
<td>MCN1-BUC02</td>
<td>6 hours, 14 minutes, 58.0 seconds</td>
<td>GOOD</td>
</tr>
</tbody>
</table>
IPSec Monitoring and Logging

Oct 04, 2016

How To Monitor IPSec Tunnel Statistics

To monitor IPSec tunnel statistics:

1. Navigate to Monitor → Statistics. Choose IPsec Tunnel from the Show drop-down menu as shown below:

2. Navigate to Monitor → IKE/IPsec. Observe the configured IPsec tunnels, the IKE and IPsec service associations between two or more VPN endpoints configured within the SD-WAN network.

How To Monitor IPSec Logs

1. Navigate to Configuration → Appliance Settings → Logging/Monitoring. Select Filename from the drop-down menu and click View Log. You can view the following log details for the IPsec tunnel:

   * Creation and Deletion of IPsec tunnel
   * IPsec tunnel status change

How To View IPSec Tunnel Alerts

1. Navigate to Configuration → Appliance Settings → Logging/Monitoring → Alert Options.
2. Create Email and Syslog alerts for IPsec tunnel state reporting.

   * Supports IPSEC_TUNNEL as one of the Event types which allows you to configure Email and Syslog Severity Filters.

How To Monitor IPSec Tunnel Events
1. Navigate to Configuration → System Maintenance → Diagnostics → Events.

2. Add events based on the "IPSEC_TUNNEL" object type. Create filters for all IPsec related events.
Eligibility for IPsec Non-Virtual Path Routes

Mar 20, 2017

Before to release 9.2, IPsec tunnel routes would remain in the route table even if the tunnel became unavailable.

Using the Keepalive option under Connections > [Site Name] > IPsec Tunnels enhances this behavior so that the IPsec non-virtual path Routes are now considered ineligible when the IPsec tunnel is no longer available. When the keepalive option is enabled, the SAs get created automatically without any traffic being sent through Tunnel.
IPSec Null Encryption

Mar 29, 2017

In SD-WAN 9.2 release, the tunnel type ESP+NULL is introduced. When using IPsec ESP protocol, traffic is typically encrypted and authenticated. However, you can choose not to use encryption by using Null encryption. In ESP + NULL tunnel type the packets are authenticated but not encrypted.

You can configure the IPsec tunnel with ESP+NULL tunnel type in the Configuration editor, under IPsec Settings section.
Secure Web Gateway Using GRE Tunnels

Oct 28, 2016

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

An alternative to backhauling is to add security appliances at the branch. However, the cost and complexity increases as you install multiple appliances to maintain consistent policies across the sites. And if you have a large number of branch offices, it becomes impractical to manage costs.

The ideal solution to enforce security without adding cost, complexity, or latency is to route all branch Internet traffic from the Citrix NetScaler SD-WAN appliance to the Zscaler Cloud Security Platform.

With the addition of Zscaler to your SD-WAN network, you can create granular security policies for users using a central Zscaler console, and the policies are applied consistently whether the user is at the data center site or branch site. Because the Zscaler security solution is cloud based, no new security appliances need to be added in the network.

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 instantly 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.

SD-WAN appliances can connect to Zscaler cloud network through GRE tunnels at the customer's site. When implementing Zscaler using SD-WAN appliances, the following functionality is supported:

- GRE traffic forwarding mode only to Zscaler, enabling direct Internet breakout.
- Support for direct internet access (DIA) using Zscaler on a per customer site basis.
  - On some sites, you may want to provide DIA with on-premises security equipment and not use Zscaler.
  - On some sites, you may choose to backhaul all traffic another customer site and provide internet access.
- Virtual Routing and Forwarding deployment.
- One WAN link as part of internet services.

Zscaler is a cloud service and needs to be setup as a service with underlying WAN links defined for the Internet Service that it uses.

- Configure an internet service at the data center and branch through GRE events.
- Create a trusted Public internet link configured at the data center and branch sites.

Topology
GRE Traffic Forwarding

To use GRE 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 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.

Configuring GRE Events in SD-WAN Web Interface

To configure internet service:

Configure GRE Tunnel

a) Source IP address is the Tunnel Source IP address, and if the Tunnel Source IP address is NATted, then Public Source IP address is the public IP address of the Tunnel Source IP address, even if it is NATted on a different intermediate device.

b) Destination IP address is the ZEN IP address which Zscaler provides.

c) The Source IP address and the Destination IP address are the router GRE headers when the original payload is encapsulated.

d) Tunnel IP address and Prefix is the IP addressing on the GRE tunnel itself. This is useful for routing traffic that needs to be sent over the GRE tunnel and needs this IP address as gateway address.

To configure GRE

1. In the configuration editor, navigate to Connections > Site > GRE Tunnels. The source IP address can only be chosen from the Virtual network interface on trusted links. See, How to Configure GRE Tunnel.

Configure Routes

Configure routes to forward internet prefix services to the Zscaler GRE Tunnels.

a) The ZEN IP address (Tunnel destination IP, 199.168.148.131 shown below) must be configured with Service-Type Internet. This is required so that traffic destined towards Zscaler is accounted from the Internet service.
b) All traffic destined towards Zscaler matches the default route 0/0 and be transmitted over the GRE tunnel. Ensure that the 0/0 under the GRE tunnel has a lower Cost than Passthrough or any other Service type.

c) Similarly, the backup GRE tunnel towards Zscaler needs to be set up with a higher cost as compared to the Primary GRE tunnel.

d) Ensure that non-recursive routes exist for the ZEN IP address.

To configure routes:

Navigate to Connections > Site > Routes.

Refer to the How-To article; Configuring Routes for instructions about creating routes.

Note

If you do not have specific routes for the Zscaler IP then the route prefix 0.0.0.0/0 would match the ZEN IP and route it in a GRE tunnel encapsulation loop. This particular configuration utilizes the tunnels in an active-backup mode; traffic automatically switches over to the tunnel with gateway IP address 172.61.2.2 when the tunnel with gateway IP address 172.61.2.2 fails. 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 fails.

Limitations

- Multiple VRF deployments are not supported.
- Primary backup GRE tunnels are supported for a high-availability design mode only.
- GRE keep alive messages are supported. A new field called Public Source IP that provides the NAT address of the GRE Source address is added to the NetScaler SD-WAN GUI interface (in the case when SD-WAN appliance Tunnel Source is NATted by an intermediate device).
Stateful Firewall and NAT Support

Mar 21, 2017

This feature provides a firewall built into the SD-WAN application. The firewall allows policies between services and zones, and supports Static NAT, Dynamic NAT (PAT), and Dynamic NAT with Port Forwarding. Additional firewall capabilities include:

- Provide security for user traffic within SD-WAN network (Enterprise and Service Providers)
- (Potential) Reduction of External Equipment (Enterprise and Service Providers)
- Using the same IP address space for Multiple customers: NAT Capability (Service Providers)
- Apply multiple firewalls from a global perspective (Service Providers)
- Filtering traffic flows between Zones
- Filtering traffic between services within a Zone
- Filtering traffic between services that reside in different Zones
- Filtering traffic between services at a site
- Defining Filter Policies to Allow, Deny, or Reject flows
- Tracking flow state for selected flows
- Applying Global Policy Templates
- Support for Port Address Translation for traffic to the Internet on an untrusted port, as well as port forwarding inbound and outbound
- Provide Static Network Address Translation (Static NAT)
- Provide Dynamic Network Address Translation (Dynamic NAT)
- Port Address Translation (PAT)
- Port-Forwarding

To simplify the configuration process, firewall policies are created at the Global Configuration level. This Global configuration consists of Pre-Appliance and Post-Appliance site Policy Templates that can be applied to all sites within the SD-WAN network.

Note

It is not recommended to use firewall in Fail-to-Wire inline mode due to security reasons.
Zones

Mar 22, 2017

You can configure zones in the network and define policies to control how traffic enters and leaves zones. By default, the following zones are created:

* Internet_Zone
  - Applies to traffic to or from an Internet service using a Trusted interface.

* Untrusted_Internet_Zone
  - Applies to traffic to or from an Internet service using an Untrusted interface.

* Default_LAN_Zone
  - Applies to traffic to or from an object with a configurable zone, where the zone has not been set.

You can create your own zones and assign them to the following types of objects:

* Virtual Network Interfaces (VNI)
* Intranet Services
* GRE Tunnels
* LAN IPsec Tunnels

The following illustration displays the three zones pre-configured. Additionally, you can create your own zones as required. In this example, the zone “ZoneA_Intranet” is a user created zone. It is assigned to the Virtual Interface of the bypass segment (ports 1 and 2) of the SD-WAN appliance.

The source zone of a packet is determined by the service or virtual network interface a packet is received on. The exception to this is virtual path traffic. When traffic enters a virtual path, packets are marked with the zone that originated the traffic and that source zone is carried through the virtual path. This allows the receiving end of the virtual path to make a policy decision based on the original source zone before it entered the virtual path.

For example, a network administrator may want to define policies so that only traffic from VLAN 30 at Site A is allowed to
enter VLAN 10 at Site B. The administrator can assign a zone for each VLAN and create policies that permit traffic between these zones and blocks traffic from other zones. The screenshot below shows how a user would assign the "ZoneA_Intranet" zone to VLAN 10. In this example, the "ZoneA_Intranet" zone was previously defined by the user in order to assign it to Virtual Interface "VirtualInterface-2".

The destination zone of a packet is determined based on the destination route match. When a SD-WAN appliance looks up the destination subnet in the route table, the packet will match a route, which has a zone assigned to it.

* Source zone
  - Non-Virtual Path: Determined through the Virtual Network Interface packet was received on.
  - Virtual Path: Determined through source zone field in packet flow header.
  - Virtual network interface - the packet was received on at source site.

* Destination zone
  - Determined through destination route lookup of packet.

Routes shared with remote sites in the SD-WAN maintain information about the destination zone, including routes learned through dynamic routing protocol (BGP, OSPF). Using this mechanism, zones gain global significance in SD-WAN network and allow end-to-end filtering within the network. The use of zones provides a network administrator an efficient way to segment network traffic based on customer, business unit, or department.

The capability of SD-WAN firewall allows the user to filter traffic between services within a single zone, or to create policies that can be applied between services in different zones, as shown in figure below. In the example below, we have Zone_A and Zone_B, each of which has a LAN Virtual network interface.
Screenshot below displays the inheritance of zone for a VIP from its assigned VNI.
Policies

Policies provide the ability to allow, deny, reject, or count and continue specific traffic flows. Applying these policies individually to each site would be difficult as the SD-WAN networks grows. To resolve this issue, groups of firewall filters can be created with a Firewall Policy Template. A Firewall Policy Template can be applied to all sites in the network or only to specific sites. These policies are ordered as either Pre-Appliance Template Policies or Post- Appliance Template Policies. Both network-wide Pre-Appliance and Post-Appliance Template Policies are configured at the Global level. Local policies are configured at the site level under Connections and apply only to that specific site.

Pre-Appliance Template Policies are applied before any local site policies. Local site policies are applied next, followed by Post-Appliance Template Policies. The goal is to simplify the configuration process by allowing you to apply global policies while still maintaining the flexibility to apply site-specific policies.

Filter Policy Evaluation Order

1. Pre-Templates – compiled policies from all template “PRE” sections.
2. Pre-Global – compiled policies from Global “PRE” section.
3. Local – appliance-level policies.
4. Local Auto Generated – automatically local generated policies.
5. Post-Templates – compiled policies from all template “POST” sections.
6. Post-Global – compiled policies from Global “POST” section.

Policy definitions - Global and Local (site)

You can configure Pre-Appliance and Post-Appliance Template Policies at a global level. Local policies are applied at the site level of an appliance.
The above screenshot shows the policy template that would apply to the SD-WAN network globally. To apply a template to all sites in the network, navigate to Settings > Global Policy Template and select a specific policy. At the site level, you can add more policy templates, as well as create site specific policies.

The specific configurable attributes for a policy are displayed in the below screen shot, these are the same for all the policies.

**Policy Attributes**

* **Priority** – order in which the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority policies.
* Zone – flows have a source zone and destination zone.
  - From Zone – source zone for the policy.
  - To Zone – destination zone for the policy.

* Action – action to perform on a matched flow.
  - Allow – permit the flow through the Firewall.
  - Drop – deny the flow through the firewall by dropping the packets.
  - Reject – deny the flow through the firewall and send a protocol specific response. TCP will send a reset, ICMP will send an error message.
  - Count and Continue – count the number of packets and bytes for this flow, then continue down the policy list.

* Log Interval – time in seconds between logging the number of packets matching the policy to the firewall log file or the syslog server, if it is configured.
  - Log Start – if selected, a log entry is created for the new flow.
  - Log End – log the data for a flow when the flow is deleted.

Note
The default Log Interval value of 0 means no logging.

* Track – allows the firewall to track the state of a flow and display this information in the Monitoring > Firewall > Connections table. If the flow is not tracked, the state will show NOT_TRACKED. See the table for the state tracking based on protocol below. Use the setting defined at the site level under Firewall > Settings > Advanced > Default Tracking.
  - No Track – flow state is not enabled.
  - Track – displays the current state of the flow (which matched this policy).

* Match Type – select one of the following match types –
  - IP Protocol – If this match type is selected, select an IP protocol that the filter will match with. Options include ANY, TCP, UDP, ICMP and so
  - Application – If this match type is selected, specify the application that is used as a match criteria for this filter.
  - Application Family – If this match type is selected, select an application family that is used as a match criteria for this filter.
  - Application Object – If this match type is selected, select an application family that is used as a match criteria for this filter.

For more information on application, application family and application object, see Application Classification.
* DSCP – allow the user to match on a DSCP tag setting.

* Allow Fragments – allow IP fragments that match this filter policy.

**Note**
The firewall does not reassemble fragmented frames.

* Reverse Also – automatically add a copy of this filter policy with source and destination settings reversed.

* Match Established – match incoming packets for a connection to which outgoing packets were allowed.

* Source Service Type – in reference to a SD-WAN service – Local (to the appliance), Virtual Path, Intranet, IPhost, or Internet are examples of Service Types.

* IPhost Option - This is a new service type for the Firewall and is used for packets that are generated by the SD-WAN application. For example, running a ping from the Web UI of the SD-WAN results in a packet sourced from a SD-WAN Virtual IP address. Creating a policy for this IP address would require the user to select the IPhost option.

* Source Service Name – name of a service tied to the service type. For example, if virtual path is selected for Service Type, this would be the name of the specific virtual path. This is not always required and depends on the service type selected.

* Source IP address – typical IP address and subnet mask the filter will use to match.

* Source Port – source port the specific application will use.

* Destination Service Type - in reference to a SD-WAN service – Local (to the appliance), Virtual Path, Intranet, IPhost, or Internet are examples of service types.

* Destination Service Name - name of a service tied to the service type. This is not always required and depends on the service type selected.

* Destination IP Address - typical IP address and subnet mask the filter will use to match.

* Destination Port – destination port the specific application will use (i.e. HTTP destination port 80 for the TCP protocol).

The track option provides much more detail about a flow. The state information tracked in the state tables is included below.

**State Table for The Track Option**

There are only a few states that are consistent:

* INIT - connection created, but the initial packet was invalid.

* O_DENIED- packets that created the connection are denied by a filter policy.

* R_DENIED- packets from the responder are denied by a filter policy.

* NOT_TRACKED- the connection is not statefully tracked but is otherwise allowed.
* **CLOSED**- the connection has timed out or otherwise been closed by the protocol.

* **DELETED**- the connection is in the process of being removed. The DELETED state will almost never be seen.

All other states are protocol specific and require stateful tracking be enabled.

TCP can report the following states:

* **SYN_SENT**- first TCP SYN message seen.

* **SYN_SENT2**- SYN message seen in both directions, no SYN+ACK (AKA simultaneous open).

* **SYN_ACK_RCVD**- SYN+ACK received.

* **ESTABLISHED**- second ACK received, connection is fully established.

* **FIN_WAIT** - first FIN message seen.

* **CLOSE_WAIT**- FIN message seen in both directions.

* **TIME_WAIT** - last ACK seen in both directions. Connection is now closed waiting for reopen.

All other IP protocols (notably ICMP and UDP) have the following states:

* **NEW**- packets seen in one direction.

* **ESTABLISHED**- packets seen in both directions.
Network Address Translation (NAT)

Mar 22, 2017
The SD-WAN firewall allows the user to configure static NAT and dynamic NAT for different use cases. The following configurations are supported for NAT:

* Static one-to-one NAT
* Dynamic NAT (PAT - Port Address Translation)
* Dynamic NAT with Port Forwarding rules

Note
At this time, the NAT capability can only be configured at the site level; there is no global configuration (templates) for NAT. All NAT policies are defined from a Source-NAT ("SNAT") translation. Corresponding Destination-NAT ("DNAT") rules are created automatically for the user.
Static NAT Configuration

Aug 29, 2017

Static NAT allows the user to configure one-to-one NAT, where an inside IP address will match a public IP address. The configuration options are shown below. You must also define the filter policies to allow traffic back in for the static NAT configuration. In the NetScaler SD-WAN GUI, navigate to Configuration > Virtual WAN > Configuration Editor. Open an existing configuration file. Go to Connections > Site (Branch/MCN) > Firewall > Static NAT Policies.

### Configuration Options

* **Priority** - the order the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority polices.

* **Direction** – the direction, from the perspective of the virtual interface or service, that the translation will operate.

* **Outbound** – the destination address for a packet will be translated for packets received on the service. The source address will be translated for packets transmitted on the service.

For example, LAN service to Internet service – for packets outbound, (LAN to Internet) the source IP address is translated. For packets inbound or received (Internet to LAN) the destination IP address are translated.

* **Inbound** - the source address for a packet will be translated for packets received on the service. The destination address will be translated for packets transmitted on the service.

For example, Internet service to LAN service – For packets received on the Internet service, the source IP address is translated. For packets transmitted on the Internet service, the destination IP address is translated.

* **Service Type** – in reference to a SD-WAN service. For static NAT, these include Local (to the appliance), Intranet, and Internet.

* **Service Name** – specific service name that corresponds to the defined Service Type above.

* **Inside Zone** – one of the existing inside zones configured on the appliance.

* **Inside IP address** – source IP address and mask of the direction selected above.

* **Outside IP address** – the outside IP address and mask of packets that are translated to.
Dynamic NAT Configuration

Aug 29, 2017

Dynamic NAT is used when the user wants to forward traffic from a LAN segment to the Internet on an untrusted port. In this case, the user would configure the NAT in an outbound direction, as well as make sure the corresponding filter policies are defined to allow traffic back in. By default, once the dynamic NAT has been configured the system will add in three filter policies.

In the NetScaler SD-WAN GUI, navigate to Configuration > Virtual WAN > Configuration Editor. Open an existing configuration file.

Go to Connections > Site (Branch/MCN) > Firewall > Dynamic NAT Policies.

These policies will:

* allow Any IPhost route, Any zone, Any source and destination.
* allow match established rule, for reverse traffic of sessions initiated from the inside network.
* drop all other traffic from the source zone to the destination zone (zone specific).

The following screenshot displays the configuration options for the dynamic NAT configuration.

**Configuration Options**

* **Priority** – the order the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority policies.

* **Direction** – the direction from the virtual interface or service perspective the translation will operate.

* **Outbound** – the destination address for a packet will be translated for packets received on the service. The source address will be translated for packets transmitted on the service.
For example, LAN service to Internet service – for packets outbound, (LAN to Internet) the source IP address is translated. For packets inbound or received (Internet to LAN) the destination IP address are translated.

* **Inbound** - the source address for a packet will be translated for packets received on the service. The destination address will be translated for packets transmitted on the service.

For example, Internet service to LAN service – for packets received on the Internet service the source IP address is translated. For packets transmitted on the Internet service, the destination IP address is translated.

* **Type** – the type of dynamic NAT to perform.

  - **Port-Restricted** - Port-Restricted NAT is what most consumer grade gateway routers use. Inbound connections are generally disallowed unless a port is specifically forwarded to an inside address. Outbound connections allow return traffic from the same remote IP and port (this is known as endpoint independent mapping). This requirement limits a Port-Restricted NAT firewall to 65535 simultaneous sessions, but facilitates an often used internet technology known as hole punching.

  - **Symmetric** – Symmetric NAT is sometimes known as enterprise NAT because it allows for a much larger NAT space and enhances security by making translations less predictable. Inbound connections are generally disallowed unless a port is specifically forwarded to an inside address. Outbound connections allow return traffic from the same remote IP and port. Connections from the same inside IP and port need to map to the same outside IP and port (this is known as endpoint dependent mapping). This mode explicitly prevents hole punching.

* **Service Type** – in reference to a SD-WAN service. For static NAT these include Local (to the appliance), Intranet, Internet.

* **Service Name** – the specific service name that corresponds to the defined Service Type above.

* **Inside Zone** – select the inside zone for the packets that require NAT.

* **Inside IP address** - define an IP host address or a subnet based on traffic that requires NAT. This should be an IP address that resides in the Inside Zone.

* **Allow Related** – allow traffic related to the flow matching the rule. For example, ICMP redirection related to the specific flow that matched the policy, if there was some type of error related to the flow.

* **IPsec Passthrough** – allow IPsec traffic to pass through unchanged.

* **GRE/PPTP Passthrough** – allow GRE or IPsec to pass through unchanged.

* **Port Parity** - allows parity for NAT connections.
Dynamic NAT with Port Forwarding Configuration

Dynamic NAT with port forwarding allows the user to port forward specific traffic to a defined IP address. This is typically used for inside hosts like web servers. Once the dynamic NAT is configured the user would define the port forwarding policy. From the example in figure below, we can see that dynamic NAT is configured for a specific IP host address. The NAT example will map an inside IP host to an outside IP host. Port forwarding can then be configured which will define a specific inside and outside port mapped to an inside IP address. In this example, HTTP port 80 is defined for port forwarding.

**Configuration Options**

* **Protocol** – TCP, UDP, or both.

* **Outside Port** – outside port the user will port forward into the inside port.

* **Inside IP address** – inside address to forward matching packets.

* **Inside Port** – map the packet to the same, or a different, outside port.

* **Fragments** – allow the forwarding of fragmented packets.

* **Log Interval** – time in second between logging the number of packets matching the policy to a syslog server.

* **Log Start** – If selected, a new log entry is created for the new flow.

* **Log End** – log the data for a flow when the flow is deleted.

**Note**

The default Log Interval value of 0 means no logging.
**Track** – allows the firewall to track the state of a flow and display this information in the Monitor > Firewall > Connections. If the flow is not tracked, the state will show NOT_TRACKED. See the table for the state tracking based on protocol below. Use the setting defined at the site level under Firewall > Settings > Advanced > Default Tracking.

- **No Track** – flow state is not enabled.
- **Track** – displays the current state of the flow (which matched this policy).
Global Firewall Settings

Mar 30, 2017

Once you have created the firewall policy templates you can use this policy to configure firewall settings for NetScaler SD-WAN Network. Using the Global firewall settings, you can configure the global firewall parameters, these settings are applied to all the sites on the virtual WAN network.

To configure global firewall settings:

1. In the Configuration Editor, navigate to Advanced > Global > Virtual WAN Network Settings and click the edit icon.

2. In the Global Firewall Settings section, select values for the following options:

   * **Global Policy Template**: Select a firewall policy template to be applied to all the appliances in the SD-WAN network.

   * **Default Firewall Actions**: Select Allow to allow packets not matching the filter policy. Select Drop, to drop the packets not matching the filter policy.

   * **Default Connection State Tracking**: This enables directional connection state tracking for TCP, UDP and ICMP flows that do not match a filter policy or NAT rule. This blocks asymmetric flow, even when there are no firewall policies defined.

   **Note**
You can also configure these settings at the site level, this will override the global setting.

3. Click **Apply**.
Advanced Firewall Settings

Mar 30, 2017
You can configure the advanced firewall settings for every site individually. This will override the global settings.

To configure advanced firewall settings:

1. In the **Configuration Editor**, navigate to **Advanced > Connections > Site > Firewall > Settings**.

2. In the **Policy Template** section, click **Add**. Enter values for the following parameters.

   * **Priority** - The order in which the policy is applied at the site.
   
   * **Name** - The name of the Policy Template to use at the Site.

3. Click Advanced. Enter values for the following parameters:

   * **Default Firewall Action** - Select one of the following options.

     - **Use Global Setting** - Use the Global setting configured in NetScaler SD-WAN settings
- **Allow** - Packets not matching any filter policy is permitted.
- **Drop** - Packets not matching any filter policy is dropped.

* **Default Connection State Tracking** – Select one of the following options.
  - **Use Global Setting** - Use the Global setting configured in NetScaler SD-WAN settings
  - **No Tracking** - Bidirectional connection state tracking will not be performed on packets not matching any filter policy
  - **Track** - Bidirectional connection state tracking will be performed on TCP, UDP and ICMP packets not matching any filter policy or NAT rule. This blocks asymmetric flow, even when there are no firewall policies defined.

* **Source Route Validation**: If enabled, packets will be dropped when received on an interface that differs from the packet's route, as determined by the Source IP Address. Only the route the packet would currently match is considered.

* **Max New Connections per Source**: The maximum number of non-established Connections to allow per Source IP Address. 0 means unlimited. Use this setting to help prevent Denial of Service Attacks on the firewall.

* **Max Connections per Source**: The maximum number of connections to allow per Source IP Address. 0 means unlimited. Use this setting to help prevent Denial of Service Attacks on the firewall.

4. Configure the various timeout settings and click **Apply**.
Configuring Virtual WAN IPsec for FIPS Compliant Operation

Mar 30, 2017
In release 9.2, IPSec security setting enhancements are introduced with addition of DH groups and random number generator functionality for compliance with Federal Standards.

To configure Virtual Path IPsec Settings:

- Enable Virtual Path IPsec Tunnels for all Virtual Paths where FIPS compliance is required. IPsec settings for Virtual Paths are controlled via Default Sets.
- Configure message authentication by changing the IPsec Mode to AH or ESP+Auth and use a FIPS approved hashing function. SHA1 is currently accepted by FIPS, but SHA256 is highly recommended.
- IPsec lifetime should be configured for no more than 8 hours (28800 seconds).

The Virtual WAN uses IKE version 2 with pre-shared-keys to negotiate IPsec tunnels through the Virtual Path using the following settings:

- DH Group Group 19: ECP256 (256-bit Elliptic Curve) for key negotiation
- 256-bit AES-CBC Encryption
- SHA256 hashing for message authentication
- SHA256 hashing for message integrity
- DH Group 2: MODP-1024 for Perfect Forward Secrecy

To configure IPsec Tunnel for a third party, use the following settings:

a) Configure FIPS approved DH Group. Groups 2 and 5 are permissible under FIPS, however groups 14 and above are highly recommended.

b) Configure FIPS approved hash function. SHA1 is currently accepted by FIPS, however SHA256 is highly recommended.

c) If using IKEv2, configure a FIPS approved integrity function. SHA1 is currently accepted by FIPS, however SHA256 is highly recommended.

d) Configure an IKE lifetime, and max lifetime, of no more than 24 hours (86400 seconds).

e) Configure IPsec message authentication by changing the IPsec Mode to AH or ESP+Auth and use a FIPS approved hashing function. SHA1 is currently accepted by FIPS, but SHA256 is highly recommended.

f) Configure an IPsec lifetime, and max lifetime, of no more than 8 hours (28800 seconds).

To configure IPsec tunnels:

1. On the MCN appliance, go to Configuration -> Virtual WAN -> Configuration Editor. Open an existing configuration package. Click the Advanced tab. Go to Connections > IPSec Tunnels.

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.420
2. Expand **IKE Settings**. Configure groups in the **DH Group** drop-down list.

3. Expand **IPsec Settings**. Configure groups in the **PFS Group** drop-down list.
Network Objects

Mar 30, 2017
NetScaler SD-WAN introduces the option of adding Network Objects under the Global panel in the Configuration Editor. You can group multiple subnets together and reference a single Network Object when defining a Route Filter rather than creating a filter for each subnet.

To configure Network Objects:

1. In the Configuration Editor, navigate to Global → Network Objects, click Add (+).
2. Click Add (+) under Networks.
3. Enter the IP Address and Subnet of the new Network Object.
4. Click Apply to save the settings.

To edit the Network Object’s name, double-click on the name of the Network Object and enter a new name.
Application Classification

May 29, 2017

The SD-WAN 9.2 release has an integrated Deep Packet Inspection (DPI) library, that enables real-time discovery and classification of applications. Using the DPI technology, the SD-WAN appliance analyzes the incoming packet and classifies it as belonging to a particular application or application family.

Once a packet is classified, the application identifier can be used on firewall filter as a match criterion to identify this type of traffic.

Classifying Encrypted Traffic

NetScaler SD-WAN detects and reports encrypted traffic, as part of application reporting, in the following two methods:

- For HTTPS traffic, the DPI engine inspects the SSL certificate to read the common name, which carries the name of the service (for example - Facebook, Twitter). Depending on the application architecture only one certificate may be used for several service types (for example - email, news and so on). If different services utilize different certificates, the DPI engine would be able to differentiate between services.
- For applications that utilize their own encryption protocol, the DPI engine looks for binary patterns in the flows, for instance in case of Skype the DPI engine looks for a binary pattern inside the certificate and determines the application.

To enable Application Classification on an SD-WAN appliance:

1. In the Configuration Editor, click Advanced > Global > Applications > Settings.

2. Select Enable Deep Packet Inspection. Click Apply. Enabling deep packet inspection will turn on statistics and when disabled will turn off statistics collection of classified data. For more information, see SD-WAN Center – App Visibility feature.

Note

By default, Enable Deep Packet Inspection will collect statistics for classified data.

Note
You can view application statistics in SD-WAN Center. For more information, see How to View Application Statistics.

3. You can enable DPI at each site individually. Click Connections, select a site, click Applications Settings, and select Enable Deep Packet Inspection. You can also choose to use the global application settings.

Search Applications

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

To search for an application:

1. In the Configuration Editor, click Advanced > Global > Application > Search.
2. Click Add and in the Search field type the name of the application.
3. Click Revert.

A brief description of the Application and the Application Family name appear.
Application Objects

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

To create an application object:

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

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

3. Click + in the Application Match Criteria section.

4. Select one of the following match types:
   - **IP Protocol**: Specify the protocol, network IP address, port number, and DSCP tag.
   - **Application**: Specify the application name, network IP address, port number, and DSCP tag.

Note

For information on applications that the SD-WAN appliance can identify using Deep Packet Inspection, see Application Signature Library.
- **Application Family**: Select an application family and specify the network IP address, port number, and DSCP tag.

5. Click + to add more application match criteria.

6. Click **Apply**.

Using Application Classification with a Firewall

The classification of traffic as applications and application families enables you to use the application, application families and application objects as match types to filter traffic and apply firewall policy and rules. This applies for all Pre, Post and local policies. For more information about firewall, see [Stateful Firewall and NAT Support](https://docs.citrix.com).
Link State Propagation

Mar 30, 2017

Link State Propagation feature allows network administrators to keep the link state of a bypass pair synchronized allowing attached devices on the other side of the link to view when links are inactive. When one port of a bypass pair becomes inactive, the coupled link is de-activated administratively. If your network architecture includes a parallel failover network, this forces traffic to transition to that network. Once the disrupted link is restored, its corresponding link will automatically become active.

How To Configure Link State Propagation

To configure Link State Propagation:

1. Navigate to Configuration Editor → Sites → [Site Name] → Interface Groups.

2. Expand Virtual Interfaces and under Bridge Pairs, click the LSP checkbox to enable Link State Propagation for a Bridge Pair. Click Apply to save the settings.

Monitoring Link Statistics

To monitor Link statistics:

1. In the Monitor → Statistics page, choose Ethernet from the Show drop-down menu to view the status of the bypass port pair with Link State Propagation enabled. Observe that the LAN side link is down and subsequently the WAN side link of the bypass pair is administratively DISABLED.

2. Navigate to Configuration→ Appliance Settings → Network Adapters → Ethernet tab. The ports that are administratively down are indicated by a red asterisk (*) in the Ethernet Interface Settings list.
<table>
<thead>
<tr>
<th>Port</th>
<th>MAC Address</th>
<th>Autonegotiate</th>
<th>Speed</th>
<th>Duplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:44:7e:12:bc:11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>00:44:7e:12:bc:12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>00:44:7e:12:bc:13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>00:44:7e:12:bc:14</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>00:44:7e:12:bc:15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGT</td>
<td>00:44:7e:12:bc:16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X1</td>
<td>00:25:90:ed:22:9a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X2</td>
<td>00:25:90:ed:22:9b</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X3</td>
<td>00:25:90:ed:22:9c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X4</td>
<td>00:25:90:ed:22:9d</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Interface disabled by Port State Reflection

[Change Settings]
Multiple Net Flow collectors

Mar 30, 2017

Net Flow Collectors provide the ability to collect IP network traffic as it enters or exits an SD-WAN interface. By analyzing the data provided by Net Flow, you can determine the source and destination of traffic, class of service, and the causes for traffic congestion.

To configure Net Flow Hosts:

1. Navigate to Configuration → Appliance Settings → Net Flow → Netflow Host Settings page. Click the Enable Netflow checkbox, and enter the IP Address, and Port numbers for up to three Net flow Hosts, then click Apply Settings to save the changes.
Metered Links

May 14, 2017

NetScaler SD-WAN supports enabling metered links, which can be configured such that user traffic is only transmitted on a specific Internet WAN Link when all other available WAN Links are disabled.

Metered links conserve bandwidth on links that are billed based on usage. With the metered links you can configure the links as the Last Resort link, which disallows the usage of the link until all other non-metered links are down or degraded. Set Last Resort is typically enabled when there are three WAN Links to a site (i.e. MPLS, Broadband Internet, 4G/LTE) and one of the WAN links is 4G/LTE and might be too costly for a business to allow usage unless it is necessary.

**Note**

This feature can only be configured for Private Intranet and Public Internet Access Types.

To configure Metered links

1. In the SD-WAN web management interface, under **Configuration > Virtual WAN > Configuration Editor**, Import your last saved configuration file from the Change Management.

2. Save the newly imported configuration and then make further configuration changes.

Navigate to the **DC_vWAN > WAN Links > DC_INET > Settings** node and notice that the WAN Links settings has a new option called Metered Links.
3. Click the pen icon to enable Metering for the DC_INET WAN link. Let us assume that this is a 4G/LTE link, which is charged based on $/Mbps of usage.

4. After enabling the metered links capability, you will be allowed to provide a Data Cap in MB, billing cycle, and starting date specific to this WAN link. Let’s set some low values so that we can more easily trigger these settings. Set the **Data Cap** to **1MB**, **Cycle** to **Monthly** and **start date** **03/01/2016**, then click **Apply**.

5. **Save** and **Export** the new configuration to the **Change Management Inbox**.
6. Run through the **Change Management** process.
How To Monitor Metered WAN Links

From the NetScaler SD-WAN appliance web access home page, Routing Domain names are displayed in the System Status area of the screen.

1. After **Activating the Staged** appliances that have the new configuration changes running, navigate to the **Monitoring > Usage Reports** page to get a report on your metered link usage.

The top banner appears on every page alerting when threshold is reached at 50, 75, 90 and 100% usage (always updating with the latest).

The **WAN Link Metering Report** on the **Usage Reports** page provides mode granular detail of usage.
Note that the configuration change is pushed though the Virtual Paths, which has the INET WAN link enabled. Therefore, the usage shows 10Mbps of usage even though you recently enabled this meter feature.

2. Navigate to the **Monitoring > Statistics** page, you can observe that the usage of the WAN Links is lowered compared to the other WAN link (MPLS) even when there is no traffic across and the system itself is forced to send heartbeat packets between sites to determine the state (latency, loss, jitter) of the links in each direction.

3. Navigate to **Monitoring → Statistics**. Click **Show → WAN Link** to view WAN Links and results filtered by the Routing Domain.

4. Navigate to **Configuration → Virtual WAN → View Configuration**. Notice that wherever configuration information for the following attributes is displayed, the Routing Domain is also displayed:
How To Monitor WAN Links

1. Navigate to Monitoring → Statistics. Click Show → Paths (Summary) to monitor standby WAN links.

A Path that has at least one Standby WAN Link as an endpoint is considered a backup Path. All functions for Paths are supported regardless of whether or not a Path is configured as a backup Path.
DHCP Client for Data Port (WAN Link IP Address Learning)

Mar 30, 2017

NetScaler SD-WAN appliances support WAN Link IP address learning through DHCP Clients. This functionality reduces the amount of manual configuration to deploy SD-WAN appliances and reduces ISP costs by eliminating the need to purchase static IP addresses. SD-WAN appliances can obtain dynamic IP addresses for WAN Links on untrusted interfaces eliminating the need for an intermediary WAN router to perform this function.

**Note**
- DHCP Client can only be configured for untrusted non-bridged interfaces configured as Client Nodes.
- DHCP Client for Data Port can be enabled only on non-MCN sites.
- One-Arm or Policy Based Routing (PBR) deployment is not supported on the site with DHCP Client configuration.
- DHCP events are logged from the client's perspective only and no DHCP server logs are generated.

**How To Configure DCHP Client**

To configure DHCP for an untrusted virtual interface:

1. In the Configuration Editor, choose **Client** from the **DHCP** drop-down menu under **[Site Name] → Interface Groups → Virtual Interfaces**.

**Note**

The physical interface in the interface group should be a non-bridged pair on a single interface.
2. Navigate to WAN Links → [WAN Link Name] → Settings → Basic Settings.

3. Click the Autodetect Public IP checkbox to enable the MCN to detect the Public IP Address used by the Client. This is required when DHCP Client mode is configured for the WAN Link.
NetScaler SD-WAN introduces the ability to use Standard or Enterprise Edition appliances as either DHCP Servers or DHCP Relay agents. You can configure your appliance to issue IP addresses using DHCP or forward DHCP packets between clients and servers.

Note
- DHCP Server supports only IP Pool based address assignment
- DHCP Relay does not support multiple DHCP Server IP address assignment

How To Enable DHCP Server

NetScaler SD-WAN appliances can be configured as DHCP server that assigns and manages IP addresses from specified address pools within the network to DHCP clients. The DHCP server can be configured to assign additional parameters such as the IP address of the Domain Name System (DNS) server and the default router. DHCP server accepts address assignment requests and renewals. The DHCP server also accepts broadcasts from locally attached LAN segments or from DHCP requests that have been forwarded by other DHCP relay agents within the network.

To enable DHCP server:

1. Navigate to Configuration → Appliance Settings → Network Adapters. In the Network Adapters page, look for the Management Interface DHCP Server pane.

2. Click the Enable DHCP Server checkbox to start the server, then enter the Lease Time (in minutes), the Domain Name, and define the IP Address range by entering a Start IP Address and an End IP Address.

Note
- The server IP address pool should be within the management network.
### Management Interface DHCP Server

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable DHCP Server</td>
<td>☑</td>
</tr>
<tr>
<td>Lease Time (minutes)</td>
<td>1440</td>
</tr>
<tr>
<td>Domain Name</td>
<td>as-cx</td>
</tr>
<tr>
<td>Start IP Address</td>
<td>10.3.1.1</td>
</tr>
<tr>
<td>End IP Address</td>
<td>10.3.1.254</td>
</tr>
</tbody>
</table>

3. Click the **Change Settings** button to finish configuring the DHCP Server.

**Note**

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

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

### How To Enable DHCP Relay

A DHCP relay agent is a host or router that forwards DHCP packets between clients and servers. Network administrators can use the DHCP Relay service on the management port of the SD-WAN (Standard or Enterprise Editions) appliances to relay requests and replies between local DHCP Clients and a remote DHCP Server. This allows local hosts to acquire dynamic IP addresses from the remote DHCP Server. Relay agent receives DHCP messages and generates a new DHCP message to send out on another interface.

To enable DHCP relay service:

1. Navigate to **Configuration → Appliance Settings → Network Adapters**. In the Network Adapters page, look for the **Management Interface DHCP Relay** pane.

2. Click the **Enable DHCP Relay** checkbox to enable the service. Enter the **DHCP Server IP Address** and click the **Change Settings** button to begin using your appliance as a DHCP Relay Agent.

**Note**

If you plan to use DHCP Relay service on an appliance configured for High Availability (HA), do not configure the service on both the Active and Standby appliances. Doing so will lead to duplicate IP addresses on the defined management network.
How To Monitor DHCP Client WAN Links

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

To monitor DHCP client WAN links:

1. In the Virtual WAN→ Enable/Disable/Purge Flows page, the DHCP Client WAN Links table provides the status of learned IPs.

2. You can request to renew the IP, which refreshes the lease time. You can also choose to Release Renew, which will issue a new IP address with a new lease.
DHCP Management

Mar 30, 2017

Devices on the same network as the SD-WAN appliance's LAN/WAN interface can now use the SD-WAN DHCP Relay & DHCP Server features to provide those devices with their IP configuration. These features help to simplify the client site network by reducing the amount of equipment necessary.

- Reduce equipment at client site
- Replace router at client site (Easy deployment of edge router services)
- Simplify the client site network
- Configuration of Router without CLI commands
- Use of Dynamic Host Configuration Protocol (DHCP) on Internet Protocol (IP) networks to request IP addresses and networking parameters automatically reducing manual configuration needs by network admin on simple client sites

DHCP Relay

Network administrators can now use the DHCP Relay service of the SD-WAN appliance to relay requests and replies between local DHCP clients and a remote DHCP Server. This allows local hosts to acquire dynamic IP addresses from the remote DHCP Server.

To configure DHCP Relay:

1. In the SD-WAN web management interface, navigate to Configuration Editor > Sites > [Site Name] > DHCP > Relays. Expand Relays, and then specify the server IP address.
2. Select the Virtual Interface to be used.
3. Configure a static route to reach the DHCP Server.
Network administrators can use the DHCP Server feature on data ports of an SD-WAN appliance to allow local hosts to acquire dynamic or static IP addressing directly from the SD-WAN appliance.

To configure DHCP Server:

1. In the SD-WAN web management interface, navigate to **Configuration Editor > Sites > [Site Name] > DHCP > Server Subnets**.

2. Select the Virtual Interface to be used and specify the range of IP addresses allowed to be dynamically assigned to local hosts.

3. Optionally, specify settings for configuring the hosts, such as gateway IP address, DNS address, and an Option Set (described below).

The Hosts option of this drop-down gives users an option to manually associate specific IP addresses with specific hosts through the host MAC addresses.
Note

The following feature is optional, not required.

DHCP Option Sets are groups of DHCP settings that can be applied to individual IP address ranges. To create DHCP Option Sets, navigate to the Global section of the configuration and expand DHCP Options Sets. Enter the settings that you would like to include in the set, and then click Apply.

Your DHCP Option Set must then be assigned to a DHCP range. Do this in the Sites section where the IP address range was defined. The DHCP Option Set defined globally takes precedence over local configuration for same parameters.
To view a list of Clients from the DHCP Server Database, in the web management interface, navigate to Monitor > DHCP Server/Relay.
QoS Fairness With Random Early Detection (RED)

Mar 30, 2017
The QoS fairness feature improves the fairness of multiple virtual path flows by using QoS classes and Random Early Detection (RED). A virtual path can be assigned to one of 16 different classes. A class can be one of three basic types:

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

Users specify different bandwidth requirements for different classes, which enables the virtual path scheduler to arbitrate competing bandwidth requests from multiple classes of the same type. The scheduler uses the Hierarchical Fair Service Curve (HFSC) algorithm to achieve fairness among the classes.

HFSC services classes in first-in, first-out (FIFO) order. Before scheduling packets, NetScaler SD-WAN examines the amount of traffic pending for the packets' class. When excessive traffic is pending, the packets are dropped instead of being put into the queue (tail dropping).

Why Does TCP Cause Queuing?
TCP cannot control how quickly the network can transmit data. To control bandwidth, TCP implements the concept of a bandwidth window, which is the amount of unacknowledged traffic that it will allow in the network. It initially starts with a small window and doubles the size of that window whenever acknowledgments are received. This is called the slow start or exponential growth phase.

TCP identifies network congestion by detecting dropped packets. If the TCP stack sends a burst of packets that introduce a 250 ms delay, TCP does not detect congestion if none of the packets are discarded, so it continues to increase the size of the window. It might continue to do so until the wait time reaches 600-800 ms.

When TCP is not in the slow start mode, it reduces the bandwidth by half when packet loss is detected, and increases the allowed bandwidth by one packet for each acknowledgment received. TCP therefore alternates between putting upward pressure on the bandwidth and backing off. Unfortunately, if the wait time reaches 800ms by the time packet loss is detected, the bandwidth reduction causes a transmission delay.

Impact on QoS Fairness
When TCP transmission delay occurs, providing any kind of fairness guarantee within a virtual-path class is difficult. The virtual path scheduler must apply tail-drop behavior to avoid holding enormous amounts of traffic. The nature of TCP connections is such that a small number of traffic flows to fill the virtual path, making it difficult for a new TCP connection to achieve a fair share of the bandwidth. Sharing bandwidth fairly requires making sure that bandwidth is available for new packets to be transmitted.

Random Early Detection
Random Early Detection (RED) prevents traffic queues from filling up and causing tail-drop actions. It prevents needless queuing by the virtual path scheduler, without affecting the throughput that a TCP connection can achieve.

How To Use RED
1. Start a TCP session to create the virtual path. Verify that with RED enabled, the wait time on that class stays at around 50 ms in the steady state.

2. Start a second TCP session and verify that the both TCP sessions share the virtual path bandwidth evenly. Verify that the wait time on the class stays at the steady state.

3. Verify that the Configuration Editor can be used to enable and disable RED and that it displays the correct value for the parameter.

4. Verify that the View Configuration in the SD-WAN GUI page displays whether RED is enabled for a rule.

How To Enable RED

1. Navigate to Configuration editor → Connections → Virtual Paths → [Select Virtual Path] → [Local/Remote Site] → Rules → Select Rule, for example: (VOIP).

2. Expand the LAN to WAN pane. Under LAN to WAN section, click the Enable RED checkbox to enable it for TCP based rules.
### WAN General

#### LAN to WAN

<table>
<thead>
<tr>
<th>Source</th>
<th>Class</th>
<th>Drop Limit (ms)</th>
<th>Drop Depth (bytes)</th>
<th>Enable RED</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>realtime_class</td>
<td>100</td>
<td>5000</td>
<td>X</td>
</tr>
<tr>
<td>Large Packet Size (bytes)</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Large Packets</th>
<th>Drop Limit (ms)</th>
<th>Drop Depth (bytes)</th>
<th>Enable RED</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**Random Early Detection (RED)**: Random Early Detection (RED) will discard packets uniformly when congestion is detected.
MPLS QoS Queues

May 31, 2017

This feature simplifies creating SD-WAN configurations when adding a Multiprotocol Label Switching (MPLS) WAN Link. Previously, each MPLS queue required one WAN Link to be created. Each WAN Link required a unique Virtual IP Address (VIP) to create the WAN Link and a unique Differentiated Services Code Point (DSCP) tag corresponding to the provider's queuing scheme. After defining a WAN Link for each MPLS queue, the Intranet Service to map to a specific queue is defined.

Currently, a new MPLS specific WAN Link definition (i.e., Access Type) is available. When a new Private MPLS Access Type is selected, you can define MPLS queues associated with the WAN Link. This allows a single VIP with multiple DSCP tags that correspond to the provider’s queuing implementation for the MPLS WAN Link. This maps the Intranet Service to multiple MPLS Queues on a single MPLS WAN Link.

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

**Note**

If you have existing MPLS configurations and would like to implement the Private MPLS Access Type, please contact Citrix Support for assistance.

### Configuring Private MPLS WAN Links

1. Define the WAN Link Access Type as Private MPLS.
2. Define the MPLS Queues corresponding to the Service Provider MPLS queues.
3. Enable the WAN Link for virtual path service (enabled by default for Private MPLS WAN Links).
4. From the virtual path on a WAN Link, assign an Autopath group.

**Note**

If the Autopath Group is assigned from the WAN Link level, SD-WAN creates paths automatically between the MCN and Client MPLS Queues based on matching DSCP tags. If the Autopath Group is assigned from the MPLS Queue level, SD-WAN creates paths automatically regardless of whether or not the DSCP tags match.

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

**Note**

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

To configure new WAN Link Access Type for Private MPLS

1. In the Configuration Editor, click + (Add) under Sites > [Site Name] > WAN Links, the Add WAN Link pop-up appears.

2. Under the Basic Settings, there is now a new MPLS Queues tab. Click + Add to add specific MPLS Queues. These should correspond with the queues defined by the Service Provider.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Queue Name</td>
<td>The MPLS queue name</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DSCP Tag</td>
<td>Service Provider's DSCP tag setting for the queue.</td>
</tr>
<tr>
<td>Unmatched</td>
<td>When enabled, any frames arriving that do not match defined tags within the configuration file are mapped to this queue and the bandwidth defined for this queue.</td>
</tr>
<tr>
<td>LAN to WAN Permitted Rate (kbps)</td>
<td>The amount of bandwidth that SD-WAN devices are permitted to use for upload, which cannot exceed the defined physical upload rate of the WAN Link.</td>
</tr>
<tr>
<td>WAN to WAN Permitted Rate (kbps)</td>
<td>The amount of bandwidth that SD-WAN devices are permitted to use for download, which cannot exceed the defined physical download rate of the WAN Link.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking IP Address</td>
<td>WAN Link tracking address</td>
</tr>
<tr>
<td>Congestion Threshold</td>
<td>The defined amount of time for congestion (in microseconds) after which the MPLS Queue will throttle packet transmission to avoid additional congestion. When congestion exceeds the set Threshold, SD-WAN backs off the sending rate.</td>
</tr>
<tr>
<td>Eligibility</td>
<td>The MPLS Queue’s eligibility to process specific classes of traffic. When eligibility is disabled for a specific class of traffic, that class of traffic is unlikely to route through the MPLS Queue unless network conditions require it.</td>
</tr>
</tbody>
</table>

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

**Note**

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

**Define WAN Link Properties for Private MPLS**

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

**To assign autopath group**

1. Go to Connections > [Site Name] > WAN Links >[MPLS WAN Link Name] > Virtual Paths > [Virtual Path Name] > [Local Site] > WAN Links and click Edit ( ).

2. Click the Autopath Group drop-down menu and choose from the available groups. By default, MPLS Queues inherit the Autopath Group assigned to the MPLS WAN Link. You may choose to set the individual MPLS Queues to Inherit the chosen Autopath Group or choose an alternate from the Autopath Group drop-down menu for each MPLS Queue.
Note

If there is no one-to-one mapping, based on DSCP tag, between queues at the local site and the remote site, you must map MPLS Queues to specific Autopath Groups. Inheriting an Autopath Group from the MPLS WAN Link will only automatically generate paths between queues with matching DSCP tags.

Assign Autopath Group to Virtual Path-WAN Link

The Autopath Group defined is the same for the MCN and Client appliance. This allows the system to build the Paths automatically. At the MCN site you can also expand the WAN Link associated with the virtual path.
The SD-WAN web interface now allows you to view the permitted rate for WAN Links and WAN Link Usages and whether a WAN Link, Path, or Virtual Path may be in a congested state. In the previous releases, this information was only available in SD-WAN log files and through the CLI. These options are now available in the web interface to assist in troubleshooting.

**View Permitted Rate**

Permitted Rate is the amount of bandwidth that a particular WAN Link, Virtual Path Service, Intranet Service, or Internet Service is permitted to use at a given point in time. The permitted rate for a WAN Link is static, and is defined explicitly in the SD-WAN configuration. The permitted rate for a Virtual Path Service, Intranet Service, or Internet Service will fluctuate over time, in response to congestion, user demand, and Fair Shares, but will always be greater than or equal to the Minimum Reserved Bandwidth for the Service.

**Monitor WAN Link**

Go to Monitor > Statistics, and select WAN Link from the Show drop-down menu.

![WAN Link Statistics](image)

**Monitor MPLS Queues**

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

![MPLS Queue Statistics](image)
Monitoring Your Virtual WAN

Mar 30, 2017

Viewing Basic Information for an Appliance

Use a browser to connect to the Management Web Interface of the appliance you want to monitor, and click the Dashboard tab to display basic information for that appliance.

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

**System Status:**

- **Name** – This is the name you assigned to the appliance when you added it to the system.
- **Model** – This is the Virtual WAN appliance model number.
- **Appliance Mode** – This indicates whether this appliance has been configured as the primary or secondary MCN, or as a client appliance.
- **Management IP Address** – This is the Management IP Address for the appliance.
- **Appliance Uptime** – This specifies the duration for which the appliance has been running since the last reboot.
- **Service Uptime** – This specifies the duration for which the Virtual WAN Service has been running since the last restart.

**Virtual Path Service Status:**

- **Virtual Path [site name]** – This displays the current status of all the Virtual Paths associated with this appliance. If the Virtual WAN Service is enabled, this section is included on the page. If the Virtual WAN Service is disabled, an Alert icon (goldenrod delta) and Alert message to that effect displays in place of this section.

**Local Version Information:**

- **Software version** – This is the version of the CloudBridge Virtual Path software package currently activated on the appliance.
- **Build on** – This is the build date for the product version currently running on the local appliance.
- **Hardware version** – This is the hardware model number and version of the appliance.
- **OS Partition Version** – This is the version of the OS partition currently active on the appliance.

The below figure shows a sample Dashboard page for the MCN, and MCN Appliance information.
The below figure shows a sample Dashboard page and information for a client appliance.

### System Status

<table>
<thead>
<tr>
<th>Name:</th>
<th>BR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model:</td>
<td>2000</td>
</tr>
<tr>
<td>Appliance Mode:</td>
<td>Client</td>
</tr>
<tr>
<td>Management IP Address:</td>
<td>10.199.106.222</td>
</tr>
<tr>
<td>Appliance Uptime:</td>
<td>1 weeks, 5 days, 10 hours, 43 minutes, 7.2 seconds</td>
</tr>
<tr>
<td>Service Uptime:</td>
<td>4 days, 5 hours, 31 minutes, 45.0 seconds</td>
</tr>
</tbody>
</table>

### Virtual Path Service Status

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

### Local Versions

<table>
<thead>
<tr>
<th>Software Version:</th>
<th>9.0.0.271.505202</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built On:</td>
<td>Mar 31 2016 at 12:41:53</td>
</tr>
<tr>
<td>Hardware Version:</td>
<td>2000</td>
</tr>
<tr>
<td>OS Partition Version:</td>
<td>4.5</td>
</tr>
</tbody>
</table>
Viewing Statistical Information

Oct 04, 2016
This section provides basic instructions for viewing Virtual WAN statistics information.

1. Log onto the Management Web Interface for the MCN.

2. Select the Monitoring tab.

   This opens the Monitoring navigation tree in the left pane. By default, this also displays the Statistics page with Paths preselected in the Show field. This contains a detailed table of path statistics.

Note

If you navigate to another Monitoring page (for example, Flows), you can return to this page by selecting Statistics in the Monitoring navigation tree (left pane).

3. Open the Show drop-down menu next to the Show field.

   In addition to the Paths statistics, the Show menu also offers several additional options for filtering and viewing statistical information.
4. Select a filter from the **Show** menu to view a table of statistical information for that topic.
Viewing Flow Information

Oct 04, 2016

This section provides basic instructions for viewing Virtual WAN flow information.

To view flow information, do the following:

1. Log onto the Management Web Interface for the MCN, and select the Monitoring tab.

   This opens the Monitoring navigation tree in the left pane.

2. Select the Flows branch in the navigation tree.

   This displays the Flows page with LAN to WAN preselected in the Flow Type field.

3. Select the Flow Type.

   The Flow Type field is located in the Select Flows section at the top of the Flows page. Next to the Flow Type field is a row of checkbox options for selecting the flow information you want to view. You can check one or more boxes to filter the information to be displayed.

4. Select the Max Flows to Display from the drop-down menu next to that field.

   This determines the number of entries to display in the Flows table. The options are: 50, 100, 1000.

5. (Optional) Enter search text in the Filter field.

   This filters the table results so that only entries containing the search text display in the table.
To see detailed instructions for using filters to refine Flow table results, click Help to the right of the Filter field. To close the help display, click Refresh in the bottom left corner of the Select Flows section.

6. Click Refresh to display the filter results.

The below figure shows a sample Flows page filtered display with all flow types selected.

7. (Optional) Select the columns to include in the table.

Do the following:

a. Click Toggle Columns.

The Toggle Columns button is just above the top right corner of the Flows table. This reveals any deselected columns, and opens a checkbox above each column for selecting or deselecting that column. Deselected columns display greyed out, as shown in the below figure.

Note

By default, all of the columns are selected, which can cause the table to be truncated in the display, obscuring the Toggle Columns button. If so, a horizontal scroll bar displays beneath the table. Slide the scroll bar to the right to view the truncated section of the table and reveal the Toggle Columns button. If the scroll bar is not available, try resizing the width of your browser window until the scroll bar is revealed.
b. Click a checkbox to select or deselect a column.

c. Click **Apply** (above the top right corner of the table).

This dismisses the selection options, and refreshes the table to include only the selected columns.
Viewing Reports

Oct 04, 2016
This section provides basic instructions for generating and viewing CloudBridge Virtual WAN reports about the local appliance using the Management Web Interface.

Note
Reports generated on the Management Web Interface apply to the local appliance, only. To generate and view reports for the Virtual WAN, use the Virtual WAN Center Web Interface.

To generate and view CloudBridge Virtual WAN reports, do the following:

1. Log onto the Management Web Interface for the MCN, and select the Monitoring tab.
   
   This opens the Monitoring navigation tree in the left pane.

2. Select a report type from the navigation tree.
   
   The report types are listed as branches in the navigation tree, just below the Flows branch.

   ![Monitoring Navigation Tree]

   The available report types are as follows:
   - Performance Reports
   - QoS Reports
   - Usage Reports
   - Availability Reports
   - Appliance Reports

3. Select the report options.
In addition to the various types of reports, for each report type there are numerous options and filters for refining report results.
Viewing Firewall Statistics

Mar 23, 2017

Once you have configured firewall and NAT policies you can view the statistics of the connections, firewall policies and NAT policies as reports. You can filter the reports using the various filtering parameters.

For information on configuring firewall and NAT policies, see Stateful Firewall and NAT Support.

Connections

You can check the statistics for Applications for the Firewall Policy. This enables you to see all connections that match to the selected Application, where they are coming from, where they are going to, and how much traffic they are generating. You can see how the firewall policies are acting on the traffic for each Application.

You can filter the connections statistics using the following parameters:

- **Application** - The application used as filter criteria for the connection.
- **Family** - The application family 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.
subnet mask.

- **Source Port** - The port or range of ports from which the connection originated. A single port or a range of ports using the "-" character is accepted.
- **Destination Service Type** - The service to which responding traffic is destined.
- **Destination Service Name** - When applicable, the service to which responding traffic is destined.
- **Destination IP** - The IP address of the responding device, input in dotted decimal notation with an optional subnet mask.
- **Destination Port** - The port or range of ports used by the responding device. A single port or a range of ports using the "." character is accepted.
- **Source Zone** - The origination zone matched by the filter policy.
- **Destination Zone** - The responding zone matched by the filter policy.

**NAT Policies**

You can view the statistics of all the Network Address Translation (NAT) policies and filter the report using the following parameters.

- **IP Protocol** - The IP protocol that the NAT policy matches.
- **NAT Type** - The type of NAT in use by the NAT policy.
- **Dynamic NAT Type** - The type of Dynamic NAT in use by the NAT policy.
- **Service Type** - The service type used by the NAT policy.
- **Service Name** - The instance of the service used by the NAT policy.
- **Inside IP** - The inside IP address, input in dotted decimal notation with an optional subnet mask.
- **Inside Port** - The inside port range used by the NAT policy. A single port or a range of ports using the "-" character is accepted.
- **Outside IP** - The outside IP address, input in dotted decimal notation with an optional subnet mask.
- **Outside Port** - The outside port range used by the NAT policy. A single port or a range of ports using the "-" character is accepted.

To view Firewall Statistics:

1. Navigate to **Monitoring > Firewall**.
2. In the Statistics field select, **Connections, Filter Policies** or **NAT Policies** as required.
3. Set the filtering criteria as required.
4. Click **Refresh**.
Adaptive Bandwidth Detection

Mar 30, 2017
This feature is applicable to networks with VSAT, LOS, Microwave, 3G/4G/LTE WAN Links, for which the available bandwidth varies based on weather and atmosphere conditions, location, and line of site obstructions. It allows the NetScaler SD-WAN appliances to adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range (minimum and maximum WAN link rate) to use the maximum amount of available bandwidth without marking the paths BAD.

- Greater bandwidth reliability (Over VSAT, Microwave, 3G/4G, and LTE)
- Greater predictability of adaptive bandwidth over user configured settings

To enable adaptive bandwidth detection:

This feature needs Bad loss sensitivity option to be enabled (default/custom) as a prerequisite. You can enable it under Global > Autopath Groups > [Autopath Group Name] > Bad Loss Sensitive.


2. Navigate to Configuration Editor > Sites > [Site Name] > WAN Links > [WAN Link Name] > Settings > Advanced Settings.
3. Check the **Adaptive Bandwidth Detection** box and enter a value in the **Minimum Acceptable Bandwidth** field.

4. View the **Usage and Permitted Rates** table by navigating to **Monitor > Statistics > WAN Link Usage > Usage and Permitted Rates**.
Active Bandwidth Testing

Mar 30, 2017

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

To use the active bandwidth testing feature:

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

The output displays average bandwidth used as value to set as the permitted rate for the WAN Link minimum and maximum bandwidth results of the test. Along with the ability to test the bandwidth, you can now change the configuration file to use the learned bandwidth. This is accomplished through the Auto Learn option is under Site > [Site Name] > WAN Links > [WAN Link Name] > Settings and if enabled, the system will use the learned bandwidth.

You can also schedule recurring tests of path bandwidth in weekly, daily, or hourly intervals.

Note
A history of the path bandwidth testing results is displayed at the bottom of this page and results are archived every 7 days.
Schedule Path Bandwidth Testing

<table>
<thead>
<tr>
<th>Path Name</th>
<th>Frequency</th>
<th>Day of Week</th>
<th>Hour</th>
<th>Minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Apply Settings

History Path Bandwidth Testing Result

<table>
<thead>
<tr>
<th>Num</th>
<th>From Link</th>
<th>To Link</th>
<th>Test Time</th>
<th>Min Bandwidth (Mbps)</th>
<th>Max Bandwidth (Mbps)</th>
<th>Avg Bandwidth (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BR_1-NET-1</td>
<td>DC_MCN-NET-1</td>
<td>3/28/2017, 1:29:54 AM</td>
<td>363140</td>
<td>78016</td>
<td>515927</td>
</tr>
<tr>
<td>2</td>
<td>BR_1-NET-1</td>
<td>DC_MCN-NET-1</td>
<td>3/29/2017, 1:30:00 AM</td>
<td>281095</td>
<td>573073</td>
<td>410345</td>
</tr>
<tr>
<td>3</td>
<td>BR_1-NET-1</td>
<td>DC_MCN-NET-1</td>
<td>3/29/2017, 1:30:06 AM</td>
<td>317568</td>
<td>636640</td>
<td>498018</td>
</tr>
<tr>
<td>4</td>
<td>BR_1-MPLS-1</td>
<td>DC_MCN-MPLS-1</td>
<td>3/29/2017, 1:34:00 AM</td>
<td>460016</td>
<td>103357</td>
<td>725514</td>
</tr>
<tr>
<td>5</td>
<td>DC_MCN-NET-1</td>
<td>BR_1-NET-1</td>
<td>3/28/2017, 1:34:10 AM</td>
<td>290708</td>
<td>781704</td>
<td>639873</td>
</tr>
<tr>
<td>6</td>
<td>DC_MCN-NET-1</td>
<td>BR_1-NET-1</td>
<td>3/29/2017, 1:34:18 AM</td>
<td>462368</td>
<td>1388712</td>
<td>669232</td>
</tr>
<tr>
<td>7</td>
<td>DC_MCN-NET-1</td>
<td>BR_1-WL-1</td>
<td>3/29/2017, 1:34:27 AM</td>
<td>380670</td>
<td>772609</td>
<td>533286</td>
</tr>
<tr>
<td>8</td>
<td>DC_MCN-MPLS-1</td>
<td>BR_1-MPLS-1</td>
<td>3/29/2017, 1:35:12 AM</td>
<td>26623</td>
<td>35495</td>
<td>30578</td>
</tr>
<tr>
<td>9</td>
<td>DC_MCN-NET-1</td>
<td>BR_1-NET-1</td>
<td>3/29/2017, 1:36:09 AM</td>
<td>350097</td>
<td>739329</td>
<td>591542</td>
</tr>
<tr>
<td>10</td>
<td>DC_MCN-NET-1</td>
<td>BR_1-NET-1</td>
<td>3/29/2017, 1:35:47 AM</td>
<td>473024</td>
<td>789756</td>
<td>639548</td>
</tr>
<tr>
<td>11</td>
<td>DC_MCN-NET-1</td>
<td>BR_1-WL-1</td>
<td>3/29/2017, 1:35:56 AM</td>
<td>446260</td>
<td>777674</td>
<td>608533</td>
</tr>
</tbody>
</table>
Diagnostic Tool

Jul 26, 2017
A new inbuilt traffic generator is introduced in SD-WAN 9.2. This diagnostic tool is used to generate test traffic which allows you to troubleshoot network issues that may result in:

- Frequent change in path state from Good to Bad.
- Poor application performance.
- Higher packet loss

Most often, these problems arise due to rate limiting configured on firewall/router, incorrect bandwidth settings, low link speed, priority queue set by network provider and so on. The diagnostic tool allows you to identify the root cause of such issues and troubleshoot it.

The diagnostic tool removes the dependency on third party tools such as iPerf which has to be manually installed on the Data Center and Branch hosts. It provides more control over the type of diagnostic traffic sent, the direction in which the diagnostic traffic flows, and the path on which the diagnostic traffic flows.

The diagnostic tool allows to generate the following two types of traffic:

- Control: Generates traffic with no QoS/scheduling applied to the packets. As a result, the packets are sent over the path selected in the UI, even if the path is not the best at the time. This traffic is used to test specific paths and helps to identify ISP related issues. You can also use this to determine the bandwidth of the selected path.
- Data: Simulates the traffic generated from the host with SD-WAN traffic processing. Since QoS/scheduling is applied to the packets, the packets are sent over the best path available at that time. Traffic will be sent over multiple paths if load balancing is enabled. This traffic is used to troubleshoot QoS/scheduler related issues.

**Note**

To run a diagnostic test on a path, you have to start the test on the appliances at both ends of the path. Start the diagnostic test as a server on one appliance and as a client on the other appliance.

To use diagnostics tool:

1. On both the appliances, click **Configuration > System Maintenance > Diagnostics > Diagnostics Tool**.
2. In the Tool Mode field, select Server on one appliance and select Client on the other appliance.

3. In the Traffic Type field, select the type of diagnostic traffic, either Control or Data. Select the same traffic type on both the appliances.

4. In the Port field, specify the TCP / UDP port number on which the diagnostic traffic will be sent. Specify the same port number on both the appliances.

5. In the iperf field, specify IPERF command line options, if any.

Note
You need not specify the following IPERF command line options:
- -c: Client mode option is added by the diagnostic tool.
- -s: Server mode option is added by the diagnostic tool.
- -B: Binding IPERF to specific IP/interface is done by the diagnostic tool depending on the path selected.
- -p: Port number is provided in the diagnostics tool.

6. Select the path on which you want to send the diagnostic traffic. Select the same path on both the appliances.

7. Click Start on both the appliances.
Zero Touch Deployment

Note
The Zero Touch Deployment service is supported only on select NetScaler SD-WAN appliances:
- NetScaler SD-WAN 410 Standard Edition
- NetScaler SD-WAN 2100 Standard Edition
- NetScaler SD-WAN 1000 Standard Edition (reimage required)
- NetScaler SD-WAN 1000 Enterprise Edition (reimage required)
- NetScaler SD-WAN 2000 Standard Edition (reimage required)
- NetScaler SD-WAN 2000 Enterprise Edition (reimage required)

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

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

ZTD High-Level Architecture and Workflow

Data Center Site:
NetScaler SD-WAN Administrator – A user with Administration rights of the NetScaler SD-WAN environment with the following primary responsibilities:
- Configuration creation using NetScaler SD-WAN Center Network Configuration tool, or import of configuration from the Master Control Node (MCN) SD-WAN appliance
- Citrix Cloud Login to initiate the Zero Touch Deployment Service for new remote site deployment

Network Administrator – A user responsible for Enterprise network management (DHCP, DNS, internet, firewall, etc.)
- If required, configure firewalls for outbound communication to FQDN sdwanzt.citrixnetworkapi.net from SD-WAN Center

Remote Site:
Onsite Installer – A local contact or hired installer for on-site activity with the following primary responsibilities:
- Physically unpack the NetScaler SD-WAN appliance
- Reimage non-ZTD ready appliances
  
  - Required for: NetScaler SD-WAN 1000-SE, 2000-SE, 1000-EE, 2000-EE
  
  - Not required for: NetScaler SD-WAN 410-SE, 2100-SE

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

**Note**

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

---

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

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

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

Zero Touch Deployment Service Overview

The Zero Touch Deployment Service works in tandem with the NetScaler SD-WAN Center to provide an easier deployment of branch office SD-WAN appliances. SD-WAN Center is configured and used as the central management tool for the SD-WAN Standard and Enterprise Edition appliances. In order to utilize the Zero Touch Deployment Service (or ZTD Cloud Service), an Administrator must begin by deploying the first NetScaler SD-WAN device in the environment, then configure and deploy the SD-WAN Center as the central point of management. When the SD-WAN Center, release 9.1 or later, is installed with connectivity to the public internet on port 443, SD-WAN Center will automatically call home to the Cloud Service and install necessary components to unlock the Zero Touch Deployment features and to make the Zero Touch Deployment option available in the GUI of SD-WAN Center. Zero Touch Deployment is not available by default in the SD-WAN Center software. This is purposely designed to make sure the proper preliminary components on the underlay network are present before allowing an Administrator to initiate any on-site activity involving Zero Touch Deployment.

After a working SD-WAN environment is up and running registration into the Zero Touch Deployment Service is accomplished through creating a Citrix Cloud account login. With SD-WAN Center able to communicate with the ZTD service, the GUI will expose the Zero Touch Deployment options under the Configuration tab. Logging into the Zero Touch Service authenticates the Customer ID associated with the particular NetScaler SD-WAN environment and registers the SD-WAN Center, in addition to unlocking the account for further authentication of ZTD appliance deployments.

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

The Onsite Installer will receive email communication that the site is ready for Zero Touch Deployment and can begin the installation procedure of powering on and cabling the appliance for DHCP IP address assignment and internet access on the MGMT port. Also, cabling in any LAN and WAN ports. Everything else will be automated by the ZTD Service and progress can be monitored by the utilizing the activation URL.

The Zero Touch Deployment Cloud Service will automate the following actions:
Download and Update the ZTD Agent if new features are available on the branch appliance

- Authenticate the branch appliance by validating the serial number
- Authenticate that the SD-WAN Administrator accepted the site for ZTD using the SD-WAN Center
- Pull the configuration file specific for the targeted appliance from the SD-WAN Center
- Push the configuration file specific for the targeted appliance to the branch appliance
- Install the configuration file on the branch appliance
- Push any missing SD-WAN software components or required updates to the branch appliance
- Push a temporary 10Mbps license file for confirmation of Virtual Path establishment to the branch appliance
- Enable the SD-WAN Service on the branch appliance

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

Zero Touch Deployment Service Procedure

The following procedure detail the steps required to successfully deploy a new site using the Zero Touch Deployment Service. It is recommended to have a running MCN and one client node already working with proper communication to NetScaler SD-WAN Center, as well as established Virtual Paths confirming connectivity across the underlay network.

The following steps are required of the SD-WAN Administrator to initiate the deployment of zero touch:

How to Configure Zero Touch Deployment Service

The SD-WAN Center has the functionality to accept requests from newly connected appliances to join the SD-WAN Enterprise network. The request is forwarded to the web interface through the zero touch deployment service. Once the appliance connects to the service, configuration and software upgrade packages are downloaded.

Configuration workflow:

- Access SD-WAN Center > Create New site configuration or Import existing configuration and save it.
- Login to Citrix Workspace Cloud to enable ZTD service. The Zero Touch Deployment menu option is now displayed in the SD-WAN center web management interface.
- In SD-WAN Center, navigate to Configuration > Zero Touch Deployment > Deploy New Site.
- Select an appliance, click Enable and click Deploy.
To configure Zero Touch Deployment service:

1. Install SD-WAN Center with enabled Zero Touch Deployment capabilities:
   a) Install NetScaler SD-WAN Center with DHCP assigned IP address
   b) Verify SD-WAN Center is assignment a proper management IP address and network DNS address with connectivity to the public internet across the management network
   c) Upgrade the NetScaler SD-WAN Center to the latest 9.2 firmware
   d) With proper internet connectivity, the SD-WAN Center will call home to the Zero Touch Deployment (ZTD) Cloud Service and automatically download and install any firmware updates specific to ZTD, if this call home procedure fails the following Zero Touch Deployment option will not be available in the GUI.
   e) Read the Terms and Conditions, and then select “I acknowledge that I have read and agree to the above Terms and Conditions.”
   f) Click the “Login to Citrix Workspace Cloud” button if a Citrix Cloud account has leady been created.
   g) Login into the Citrix Cloud account, and upon receiving the following message of successful login, PLEASE DO NOT CLOSE THIS WINDOW UP, THE PROCESS REQUIRES ANOTHER ~20 SECONDS FOR THE SD-WAN CENTER GUI TO BE REFRESHED. The window should close on its own when it is complete.
   h) In order to create a Cloud Login account follow the below procedure:
      - Open a web browser to https://onboarding.cloud.com
      - Click on the link for "Wait, I have a Citrix.com account".
· Sign in with an existing Citrix account.

Sign in with an existing Citrix account.

- Once logged into SD-WAN Center Zero Touch Deployment page, you may notice no sites are available for ZTD deployment, this could be because of the following reasons:
  - The active configuration has not been selected from the Configuration drop-down menu
  - All the sites for the current active configuration have already been deployed
  - The configuration was not built using the SD-WAN Center, but rather the Configuration Editor available on the MCN
  - Sites were not built in the configuration referencing zero touch capable appliances (e.g. 410-SE, 2100-SE)

2. Update the configuration to add a new site using SD-WAN Center Network Configuration

   If the SD-WAN configuration was not built using the SD-WAN Center Network Configuration, import the active configuration from the MCN and begin modifying the configuration using SD-WAN Center. For Zero Touch Deployment capability, the SD-WAN Administrator must build the configuration using SD-WAN Center. The following procedure should be used to add a new site targeted for zero touch deployment.

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

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

Branch Office Topology with NetScaler SD-WAN

This is an example deployment of a branch office site, the NetScaler SD-WAN appliance is deployed physically in path of the existing MPLS WAN link across a 172.16.30.0/24 network, and leveraging an existing backup link by enabling it into an active state and terminating that second WAN link directly into the NetScaler SD-WAN appliance on a different subnet 172.16.31.0/24.

Note

The NetScaler SD-WAN appliances automatically assign a default IP address of 192.168.100.1/16. With DHCP enabled by default, the DHCP Server in the network may provide the appliance a second IP address in a subnet that overlaps the default. This can possibly result in a routing issue on the appliance where the appliance may fail to connect to the ZTD Cloud Service. It is recommended to configure the DHCP server to assign IP addresses outside of the range of 192.168.0.0/16.

There are various different deployment modes available for NetScaler SD-WAN product placement in a network. In the above example, SD-WAN is being deployed as an overlay on top of existing networking infrastructure. For new sites, SD-WAN Administrators may choose to deploy the NetScaler SD-WAN in Edge or Gateway Mode deployment, eliminating the need for a WAN edge router and firewall, and consolidating the network needs of edge routing and firewall onto the NetScaler SD-WAN solution.

b) Open the SD-WAN Center web management interface and navigate to the Configuration > Network Configuration page.
c) Make sure a working configuration is already in place, or import the configuration from the MCN.

d) Navigate to the Advanced tab to create a new site.

e) Open the Sites tile to display the currently configurated sites.

f) Quickly built the configuration for the new site by utilizing the clone feature of any existing site.

g) Populate all the required fields from the topology designed for this new branch site.
h) After cloning a new site, navigate to the site’s Basic Settings, and verify that the Model of SD-WAN is correctly selected which would support the zero touch service.

i) The SD-WAN model for the site can be updated, but do be aware that the Interface Groups may have to be redefined since the updated appliance may have a new interface layout then what was used to clone.

j) Save the new configuration on SD-WAN Center, and use the export to the “Change Management inbox” option to push the configuration using Change Management.

k) Follow the Change Management procedure to properly stage the new configuration, which makes the existing SD-WAN devices aware of the new site to be deployed via zero touch, you will need to utilize the “Ignore Incomplete” option to skip attempting to push the configuration to the new site that still needs to go through the ZTD workflow.
3. Navigate back to the SD-WAN Center Zero Touch Deployment page, and with the new active configuration running, the new site will be available for deployment.

   a) In the Zero Touch Deployment page, under the **Deploy New Site** tab, select the running network configuration file

   b) After the running configuration file is selected, the list of all the branch sites with undeployed NetScaler SD-WAN devices that are supported for zero touch will be displayed

   c) Select the branch sites you want to configure for Zero Touch service, click **Enable**, and then **Deploy**.

   d) A Deploy New Site pop-up window will appear, where the Admin can provide the Serial Number, branch site Street Address, Installer Email address, and Additional Notes, if required.
Note
The Serial Number entry field is optional and depending if it is populated or not, will result in a change in on-site activity the Installer is responsible for.

- If Serial Number field is populated – The installer is not required to enter serial number into the activation URL generated with the deploy site command
- If Serial Number field is left blank – The installer will be responsible for entering in the correct serial number of the appliance into the activation URL generated with the deploy site command

e) After clicking the Deploy button, a message will appear indicating that “The Site configuration has been deployed”.

f) This action triggers the SD-WAN Center, which was previously registered with the ZTD Cloud Service, to share the configuration of this particular site to be temporality stored in the ZTD Cloud Service.

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

Note
A zero touch deployment in the Pending Activation state can optionally be chosen to Delete or Modify if information is seen to be incorrect. If a Site is deleted from the pending activation page, it will become available to be deployed in the Deploy New Site tab page. Once you choose to delete the branch site from Pending activation, the activation link sent to the installer will become invalid.

If the Serial Number field was not populated by the SD-WAN Administrator, the Status Field will indicate “Waiting for Installer” instead of “Connecting”.

4. The next series of activities will be conducted by the On-site Installer.

a) The Installer will need to check the mailbox of the email address the SD-WAN Administrator used when deploying the site.
b) Open the zero touch deployment Activation URL in an internet browser window (e.g. https://sdwanzt.citrixnetworkapi.net).

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

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

e) The installer must physically be on-site to perform the following actions:

- Cable all WAN and LAN interfaces to match the topology and configuration built in earlier steps.
- Cable the management interface (MGMT, 0/1) in the segment of the network that will provide DHCP IP address and connectivity to the Internet with DNS and FQDN to IP address resolution.
- Power cable the SD-WAN appliance.
- Turn on the power switch of the appliance.

**Note**

Most appliances will automatically power on as soon as the power cable is attached. Some appliance may have to be powered on...
using the power switch on the front of the appliance, others may have the power switch on the rear of the appliance. Some power switches require holding the power button until the unit powers up.

5. The next series of steps are automated with the help of the Zero Touch Deployment service, but requires that the following pre-requisites are available.

- The branch appliance should be powered up
- DHCP must be available in the existing network to assign management and DNS IP address
- Any DHCP assigned IP address will require connectivity to the internet with ability to resolve FQDNs
- IP assignment can be configured manually, as long as the other pre-requisites are meet

a) The appliance obtains an IP address from the networks DHCP Server, in this example topology this is achieved through the bypassed data interfaces of a factory default state appliance.

b) As the appliance obtains the web management and DNS IP addresses from the underlay network DHCP Server, the appliance will call home to the Zero Touch Deployment Service and download any ZTD related software updates.

c) With successful connectivity to the ZTD Cloud Service, the deployment process will automatically perform the following:

- Download the Configuration File that was stored earlier by the SD-WAN Center
- Applying the Configuration to the local appliance
- Download and Install a temporary 10 MB license file
- Download and Install any software updates if needed
- Activate the SD-WAN Service

d) Further confirmation can be done in the SD-WAN Center web management interface, the Zero Touch Deployment menu will display successfully activated appliances in the Activation History tab.
e) The Virtual Paths may not immediately show in a connected state, this is because the MCN may not trust the configuration handed down from the ZTD Cloud Service, and will report “Configuration version mismatch” in the MCN Dashboard.

f) The configuration will automatically be redelivered to the newly installed branch office appliance, the status of this can be monitoring on the MCN > Configuration > Virtual WAN > Change Management page (this process can take several minutes to complete).

g) The SD-WAN Administrator can monitor the head-end MCN web management page for the established Virtual Paths of the remote site.
h) SD-WAN Center can also be utilized to identify the DHCP assigned IP address of the on-site appliance from the Configuration > Network Discovery > Inventory and Status page.

![Network Discovery Page](image)

i) At this point the SD-WAN Network Administrator can gain web management access to on-site appliance utilizing the SD-WAN overlay network.

![Remote GUI access through Virtual Path](image)

j) Web management access to the remote site appliance will indicate that the appliance has been installed with a temporary Grace License at 10Mbps, which enables the ability for the Virtual Path Service Status to report as active.
k) The appliance configuration can be validated using the **Configuration > Virtual WAN > View Configuration** page.

l) The appliance license file can be updated to a permanent license using the **Configuration > Appliance Settings > Licensing** page.
m) After uploading and installing the permanent license file, the Grace License warning banner is will disappear, and during the license install process no loss in connectivity to the remote site will occur (zero pings are dropped).
# Hardware platforms

May 02, 2017

The following sections describe the hardware specifications, installation, and initial configuration for all NetScaler SD-WAN hardware platforms:

<table>
<thead>
<tr>
<th>Hardware Platforms</th>
<th>Describes the NetScaler hardware platforms and provides detailed information about each platform and its components.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparing for Installation</td>
<td>Describes how to unpack the NetScaler appliance and prepare the site and rack for installing the appliance. Lists the cautions and warnings that you should review before you install the appliance.</td>
</tr>
<tr>
<td>Installing the Hardware</td>
<td>Describes the steps to install the rails, mount the hardware, connect the cables, and turn on the appliance.</td>
</tr>
<tr>
<td>Initial Configuration</td>
<td>Describes how to perform initial configuration of your NetScaler appliance and assign management and network IP addresses.</td>
</tr>
</tbody>
</table>

## Citrix NetScaler SD-WAN hardware platforms:

- SD-WAN WANOP 400, 800, 1000, 2000, and 3000
- SD-WAN WANOP 1000 WS and 2000 WS
- SD-WAN WANOP 4000 and 5000
- SD-WAN Standard Edition 400 and 5000
- SD-WAN Standard Edition 1000, 2000, and 2100
- SD-WAN Standard Edition 4000, 4100, and 5100
- SD-WAN Enterprise Edition 1000 and 2000
- SD-WAN VPX Models

The Citrix compliance regulatory models for the appliance editions are:

- SD-WAN 400, 800, 1000: CB 504-2
- SD-WAN 410 Standard Edition: 512-2
- SD-WAN 2000 (all editions): NS 6xCu
- SD-WAN 2100 Standard Edition: 1U1P1A
- SD-WAN 3000 (all editions): NS 6xCu 6xSFP
- SD-WAN 4000 (all editions): 4x10GE SFP+ 8xSFP
- SD-WAN 5000 (all editions): 8x10GE SFP+ 96GB
- SD-WAN 4100 (all editions): 2U1P1B
- SD-WAN 5100 (all editions): 2U1P1D
Common Hardware Components

Nov 30, 2016

Each platform has front panel and back panel hardware components. The various hardware components on the front panel and back panel vary by hardware platform.

On some platforms, the front panel has an LCD display and an RS232 serial console port. The number, type, and location of ports—copper Ethernet, copper and fiber 1G SFP, 10G SFP+, and XFP—vary by hardware platform. The back panel provides access to the fan and the field replaceable units (power supplies, solid-state and hard-disk drives).

This document includes the following details:

- LCD Display and LED Status Indicators
- Ports

LCD Display and LED Status Indicators

The LCD display on the front of every appliance displays messages about the current operating status of the appliance. These messages communicate whether your appliance has started properly and is operating normally. If the appliance is not operating normally, the LCD displays troubleshooting messages.

The LCD displays real-time statistics, diagnostic information, and active alerts. The dimensions of the LCD limit the display to two lines of 16 characters each, causing the displayed information to flow through a sequence of screens. Each screen shows information about a specific function.

The LCD has a neon backlight. Normally, the backlight glows steadily. When there is an active alert, it blinks rapidly. If the alert information exceeds the LCD screen size, the backlight blinks at the beginning of each display screen. When the appliance shuts down, the backlight remains on for one minute and then automatically turns off.

On the appliance's back panel, system status LEDs indicate the overall status of the appliance. The following table describes the indicators of the system status LED.

<table>
<thead>
<tr>
<th>LED Color</th>
<th>LED Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFF</td>
<td>No power</td>
</tr>
<tr>
<td>Green</td>
<td>Appliance is receiving power</td>
</tr>
<tr>
<td>Red</td>
<td>Appliance has detected an error</td>
</tr>
</tbody>
</table>

The port LEDs show whether a link is established and traffic is flowing through the port. The following table describes the LED indicators for each port. There are two LED indicators for each port type.

Note: This section applies to the following appliances:

NetScaler SD-WAN WANOP 400, 800, 1000, 2000, and 3000, 4000, 5000, 1000 WS, 2000 WS, VPX 2, 6, 10, 20, 50, 100, 200,

Table 1. LED port-status indicators

<table>
<thead>
<tr>
<th>Port Type</th>
<th>LED Location</th>
<th>LED Function</th>
<th>LED Color</th>
<th>LED Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet (RJ45)</td>
<td>Left</td>
<td>Speed</td>
<td>Off</td>
<td>No connection, or a traffic rate of 10 megabits per second (Mbps).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Green</td>
<td>Traffic rate of 100 Mbps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>Traffic rate of 1 gigabit per second.</td>
</tr>
<tr>
<td></td>
<td>Right</td>
<td>Link/Activity</td>
<td>Off</td>
<td>No link.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solid green</td>
<td>Link is established but no traffic is passing through the port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Blinking green</td>
<td>Traffic is passing through the port.</td>
</tr>
<tr>
<td>Management (RJ45)</td>
<td>Left</td>
<td>Speed</td>
<td>Off</td>
<td>No connection, or a traffic rate of 10 megabits per second (Mbps).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Green</td>
<td>Traffic rate of 100 Mbps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Amber</td>
<td>Traffic rate of 1 gigabit per second.</td>
</tr>
<tr>
<td></td>
<td>Right</td>
<td>Link/Activity</td>
<td>Off</td>
<td>No link.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Solid yellow</td>
<td>Link is established but no traffic is passing through the port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Blinking yellow</td>
<td>Traffic is passing through the port.</td>
</tr>
</tbody>
</table>

On each power supply, a bicolor LED indicator shows the condition of the power supply. The LEDs of the AC power supplies for each appliance are different from the LEDs of the other appliances.

Table 2. LED Power Supply Indicators
<table>
<thead>
<tr>
<th>Power Supply Type</th>
<th>LED Color</th>
<th>LED Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>OFF</td>
<td>No power to any power supply.</td>
</tr>
<tr>
<td></td>
<td>Flashing RED</td>
<td>No power to this power supply.</td>
</tr>
<tr>
<td></td>
<td>Flashing GREEN</td>
<td>Power supply is in standby mode.</td>
</tr>
<tr>
<td></td>
<td>GREEN</td>
<td>Power supply is functional.</td>
</tr>
<tr>
<td></td>
<td>RED</td>
<td>Power supply failure.</td>
</tr>
<tr>
<td>DC</td>
<td>OFF</td>
<td>No power to any power supply.</td>
</tr>
<tr>
<td></td>
<td>Flashing RED</td>
<td>No power to this power supply.</td>
</tr>
<tr>
<td></td>
<td>Flashing BLUE</td>
<td>Power supply is in standby mode.</td>
</tr>
<tr>
<td></td>
<td>BLUE</td>
<td>Power supply is functional.</td>
</tr>
<tr>
<td></td>
<td>RED</td>
<td>Power supply failure.</td>
</tr>
</tbody>
</table>
Ports

Note: Some SD-WAN appliances do not require SFP transceivers.

Ports are used to connect the appliance to external devices. Citrix NetScaler SD-WAN appliances support RS232 serial ports, 10/100/1000Base-T copper Ethernet ports, fiber 1G SFP ports and 10-gigabit fiber SFP+ ports. All Citrix NetScaler SD-WAN appliances have a combination of some or all of these ports. For details on the type and number of ports available on your appliance, see the section describing that platform.

RS232 Serial Port

The RS232 serial console port provides a connection between the appliance and a computer, allowing direct access to the appliance for initial configuration or troubleshooting.

All hardware platforms ship with an appropriate serial cable used to connect your computer to the appliance. For instructions on connecting your computer to the appliance, see Installing the Hardware.

Copper Ethernet Ports

The copper Ethernet ports installed on many models of the appliance are standard RJ45 ports.

There are two types of copper Ethernet ports that may be installed on your appliance:

10/100BASE-T port The 10/100BASE-T port has a maximum transmission speed of 100 megabits per second (Mbps). Most platforms have at least one 10/100BASE-T port.

10/100/1000BASE-T port The 10/100/1000BASE-T port has a maximum transmission speed of 1 gigabit per second, ten times faster than the other type of copper Ethernet port. Most platforms have at least one 10/100/1000Base-T port.

To connect any of these ports to your network, you plug one end of a standard Ethernet cable into the port and plug the other end into the appropriate network connector.

Management Ports

Management ports are standard copper Ethernet ports (RJ45), which are used for direct access to the appliance for system administration functions.

1G SFP and 10G SFP+ Ports

A 1G SFP port can operate at a speed of 1 Gbps. It accepts either a copper 1G SFP transceiver, for operation as a copper Ethernet port, or a fiber 1G SFP transceiver for operation as a fiber optic port.

The 10G SFP+ ports are high-speed ports that can operate at speeds of up to 10 Gbps. You need a fiber optic cable to connect to a 10G SFP+ port. If the other end of the fiber optic cable is attached to a 1G SFP port, the 10G SFP+ port automatically negotiates to match the speed of the 1G SFP port.

This Netscaler SD-WAN 410-SE appliance can be used as a WAN Optimization device, then the first port pair should have a PA labeled as well.

The motherboard port should be labeled MGMT for port Eth0.
Field Replaceable Units

Nov 30, 2016

Citrix NetScaler SD-WAN field replaceable units (FRU) are SD-WAN components that can be quickly and easily removed from the appliance and replaced by the user or a technician at the user's site. The FRUs in a SD-WAN appliance can include an AC power supply and a solid-state drive. The solid-state drive stores your configuration information used to restore from a backup after replacing the unit.

Note

SD-WAN Standard Edition 400 and 410 appliances do not have field replaceable units. The field replaceable SSD and power supplies are not required.

SD-WAN WANOP/SE 4000 and WANOP 5000 field replaceable units (FRU) are components that can be quickly and easily removed from the appliance and replaced by the user or a technician at the user's site. The FRUs in a SD-WAN WANOP/SE 4000 and WANOP 5000 appliance can include DC or AC power supplies, and solid-state and hard-disk drives.
Power Supply

Nov 30, 2016

SD-WAN appliances are configured with a single power supply. For a SD-WAN 3000 WANOP appliance, you can order a second power supply.

SD-WAN 4000/5000 WANOP and 5100 SE appliances are configured with dual power supplies but can operate with only one power supply. The second power supply serves as a backup.

For a SD-WAN Standard Edition 410 appliance, a single chassis power switch is supplied. The device has an external power brick instead of an internal power supply if a desktop form factor is chosen.

The appliances are shipped with a standard power cord that plugs into the appliance’s power supply. The other end of the cord has a NEMA 5-15 plug on the other end for connecting to the power outlet on the rack or in the wall.

For power-supply specifications, see Common Hardware Components, which describes the various hardware components, hardware platforms and includes a table summarizing the hardware specifications.

Note: If you suspect that a power-supply fan is not working, see the description of your platform. On some platforms, what appears to be the fan does not turn, and the actual fan turns only when necessary.

Table 1. LED Power Supply Indicators

<table>
<thead>
<tr>
<th>Power Supply Type</th>
<th>LED Color</th>
<th>LED Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>OFF</td>
<td>No power to any power supply.</td>
</tr>
<tr>
<td></td>
<td>Flashing RED</td>
<td>No power to this power supply.</td>
</tr>
<tr>
<td></td>
<td>Flashing GREEN</td>
<td>Power supply is in standby mode.</td>
</tr>
<tr>
<td></td>
<td>GREEN</td>
<td>Power supply is functional.</td>
</tr>
<tr>
<td></td>
<td>RED</td>
<td>Power supply failure.</td>
</tr>
<tr>
<td>DC</td>
<td>OFF</td>
<td>No power to any power supply.</td>
</tr>
<tr>
<td></td>
<td>Flashing RED</td>
<td>No power to this power supply.</td>
</tr>
<tr>
<td></td>
<td>Flashing BLUE</td>
<td>Power supply is in standby mode.</td>
</tr>
<tr>
<td></td>
<td>BLUE</td>
<td>Power supply is functional.</td>
</tr>
<tr>
<td></td>
<td>RED</td>
<td>Power supply failure.</td>
</tr>
</tbody>
</table>

Electrical Safety Precautions for Power Supply Replacement

- Make sure that the appliance has a direct physical connection to earth ground during normal use. When installing or repairing an appliance, always connect the ground circuit first and disconnect it last.
Always unplug any appliance before performing repairs or upgrades.

Never touch a power supply when the power cord is plugged in. As long as the power cord is plugged in, line voltages are present in the power supply even if the power switch is turned off.

Replacing an AC Power Supply

A NetScaler SD-WAN 2000 appliance can accommodate only one power supply, which is not field replaceable. A NetScaler 3000 appliance has only one power supply, but you can order and install a second power supply.

Note: Shut down the appliance before replacing the power supply.

To install or replace an AC power supply in a SD-WAN 3000 appliance

1. If replacing an existing power supply, align the semicircular handle, so that it is perpendicular to the power supply, loosen the thumbscrew, press the lever toward the handle and pull out the existing power supply, as shown in the following figure.

   Note: The illustration in the following figures might not represent the actual SD-WAN appliance.

   Figure 1. Removing the Existing AC Power Supply

2. Carefully remove the new power supply from its box.

3. On the back of the appliance, align the power supply with the power supply slot.

4. Insert the power supply into the slot and press against the semicircular handle until you hear the power supply snap into place.

   Figure 2. Inserting the Replacement AC Power Supply

5. Connect the power supply to a power source.

Replacing AC Power Supply on SD-WAN 4000/5000 appliance

Replace an AC power supply with another AC power supply. All power supplies must be of the same type (AC or DC).

Note: You can replace one power supply without shutting down the appliance, provided the other power supply is working.

To install or replace an AC power supply on a SD-WAN 4000/5000 appliance

1. Align the semicircular handle perpendicular to the power supply. Loosen the thumbscrew and press the lever toward the handle and pull out the existing power supply, as shown in the following figure.

   Figure 1. Removing the Existing AC Power Supply

2. Carefully remove the new power supply from its box.

3. On the back of the appliance, align the power supply with the power supply slot.
4. Insert the power supply into the slot and press against the semicircular handle until you hear the power supply snap into place.

Figure 2. Inserting the Replacement AC Power Supply

5. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Note: SD-WAN 4000/5000 appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.

Replacing DC Power Support on SD-WAN 4000/5000 appliance

Replace a DC power supply with another DC power supply. All power supplies must be of the same type (AC or DC).

Note: You can replace one power supply without shutting down the appliance, provided the other power supply is working.

To install or replace a DC power supply on a SD-WAN 4000/5000 appliance

1. Loosen the thumbscrew and press the lever towards the handle and pull out the existing power supply, as shown in the following figure.

Figure 3. Removing the Existing DC Power Supply

- Carefully remove the new power supply from its box.
- On the back of the appliance, align the power supply with the power supply slot.
- Insert the power supply into the slot while pressing the lever towards the handle. Apply firm pressure to insert the power supply firmly into the slot.

Figure 4. Inserting the Replacement DC Power Supply

- When the power supply is completely inserted into its slot, release the lever.
- Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Note: SD-WAN 4000/5000 appliances emit a high-pitched alert if one power supply fails or if you connect only one power supply.
cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.
Solid-State Drive

Mar 22, 2018

A solid-state drive (SSD) is a high-performance data storage device that stores data in solid-state flash memory. It stores the SD-WAN software and user data.

For SD-WAN 410 appliance, the on-board SATA disk controller must support at least two devices. Support for SATAv3 (6 Gbps) is available.

Replacing a Solid-State Drive

Replacement solid-state drives (SSDs) contain a pre-installed version of the SD-WAN software.

To replace a Solid-State Drive

1. Shut down the appliance.
2. Locate the SSD on the back panel of the appliance. Push the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.
3. Verify that the replacement SSD is the correct type for the platform.
4. Pick up the new SSD, open the drive handle fully to the left, and insert the drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the drive locks securely into the slot.
5. Turn on the appliance.
6. Perform the initial configuration of the appliance.

When you insert the drive, make sure that the Citrix product label is at the top if the drive is inserted horizontally or at the right if the drive is inserted vertically.
Hard Disk Drive

Nov 30, 2016

The NetScaler SD-WAN virtual machines are hosted on the hard-disk drive.

Replacing a Hard Disk Drive

Verify that the replacement hard disk drive is the correct type for the NetScaler SD-WAN WANOP/SE 4000, WANOP 5000, and 5100 SE platforms.

To install a hard disk drive

1. Shut down the appliance.
2. Locate the hard disk drive on the back panel of the appliance.
3. Disengage the hard disk drive by pushing the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.

Figure 1. Removing the Existing Hard Disk Drive

4. Pick up the new disk drive, open the drive handle fully to the left, and insert the new drive into the slot as far as possible.
   To seat the drive, close the handle flush with the rear of the appliance so that the hard drive locks securely into the slot.
   Important: When you insert the drive, make sure that the Citrix product label is at the top.

Figure 2. Inserting the Replacement Hard Disk Drive

5. Turn on the appliance.
NetScaler SD-WAN 400, 800, 1000, 2000 and 3000 WANOP Appliances

Apr 14, 2017

The SD-WAN 400, 800, 1000, 2000 and 3000 appliances are 1U accelerators for use in datacenters and larger branch offices.

The SD-WAN 2000 can be thought of as a faster Repeater 8500 appliance with two accelerated bridges, while the SD-WAN WANOP 3000 can be thought of as a faster Repeater 8800 with three accelerated bridges. The configuration process, however, is not the same. Like the high-end Repeater SDX appliance, SD-WAN 2000 and WANOP 3000 appliances use virtual machines for acceleration and management, running under a XenServer hypervisor.

The SD-WAN 400, 800, 1000, 2000, and 3000 Series have the following general characteristics:
- **SD-WAN 400 Series.** An small, affordable 1U appliance suitable for smaller branch offices, the 400 Series has two accelerated bridges and supports WAN speeds of up to 6 Mbps.
- **SD-WAN 800 Series.** A small 1U appliance suitable for medium-sized branch offices, the 800 Series has two accelerated bridges and supports WAN speed of up to 10 Mbps.
- **SD-WAN 2000 Series.** A full-sized 1U appliance suitable for large branch offices and smaller datacenters, the 2000 Series has two accelerated bridges and supports WAN speed of 10-50Mbps.
- **SD-WAN 3000 Series.** A full-sized 1U appliance suitable for the largest branch offices and medium-sized datacenters, the 3000 Series has three accelerated bridges and supports WAN speed of 50-155 Mbps.

The Citrix Compliance Regulatory Models are as follows:
- **SD-WAN 400 WANOP:** CB 504-2
- **SD-WAN 800 WANOP:** CB 504-2
- **SD-WAN 1000 WANOP:** CB 504-2
- **SD-WAN 2000 WANOP:** NS 6xCu
- **SD-WAN 3000 WANOP:** NS 6xCu 6xSFP

All SD-WAN platforms have similar components and hardware platforms offer a wide range of features, communication ports, and processing capacities. All platforms support the SD-WAN software and have multicore processors. These appliances have similar architectures, run the same release binaries and are fully supported with release 9.2.
The Citrix NetScaler SD-WAN 400 and 800 platforms each have a dual-core processor and 8GB of memory. These platforms have a bandwidth of up to 6 Mbps and up to 10 Mbps, respectively.

The following figure shows the front panel of a SD-WAN 400/800 appliance.

Figure 1. Citrix NetScaler SD-WAN 400/800, front panel

The front panel of the NetScaler SD-WAN 400/800 appliance has a power button and five LEDs. The power button switches main power (the power to the power supply) on or off. The reset button restarts the appliance.

The LEDs provide critical information about different parts of the appliance.

- **Power Fail**—Indicates that a power supply unit has failed.
- **Information LED**—Indicates the following:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuously on and red</td>
<td>The appliance is overheated. (This might be a result of cable congestion.)</td>
</tr>
<tr>
<td>Blinking red (1Hz)</td>
<td>Fan failure.</td>
</tr>
<tr>
<td>Blinking red (0.25Hz)</td>
<td>Power failure.</td>
</tr>
<tr>
<td>Solid blue</td>
<td>Local UID has been activated. Use this function to locate the server in a rack mount environment.</td>
</tr>
<tr>
<td>Blinking blue (300 m/s)</td>
<td>Remote UID is on. Use this function to identify the server from a remote location.</td>
</tr>
</tbody>
</table>

- **NIC1 and NIC2**—Indicate network activity on the LAN1 and WAN1 ports.
- **HDD**—Indicates the status of the hard disk drive.
• Power—When blinking, indicates that the power supply unit is receiving power and operating normally.

The following figure shows the back panel of a SD-WAN 400/800 appliance.

Figure 2. Citrix NetScaler SD-WAN 400/800 appliance, back panel

The following components are visible on the back panel of a SD-WAN 400/800 appliance:

• Cooling fan
• Single power supply, rated at 200 watts, 110-240 volts
• Accelerated pairs of Ethernet ports (apA and apB) which function as accelerated bridges. Individual port assignments:
  - LAN1 is apA.1, WAN1 is apA.2, LAN2 is apB.1, LAN2 is apB.2.
• RS-232 serial console port
• One Aux Ethernet port and one management port
• Two USB ports
• One Solid State Drive (SSD)
  • SD-WAN 400 - 160 GB SSD
  • SD-WAN 800 - 240 GB SSD
NetScaler SD-WAN 1000

Mar 19, 2018

The Citrix NetScaler SD-WAN 1000 platform has 3 models: SD-WAN 1000-06, SD-WAN 1000-010, and SD-WAN 1000-020, with bandwidths of 6Mbps, 10Mbps, and 20Mbps, respectively. Each model is a 1U appliance with one quad-core processor and 24 gigabytes (GB) of memory.

The following figure shows the front panel of the SD-WAN 1000 appliance.

The front panel of the NetScaler SD-WAN 1000 appliance has a power button and five LEDs.

- The power button switches main power (the power to the power supply) on or off.
- The reset button restarts the appliance.
- The LEDs provide critical information about different parts of the appliance.

Figure 1. Citrix NetScaler SD-WAN 1000, front panel

The appliance has the following ports:

- An RS232 serial console port.
- A copper Ethernet (RJ45) management port. The management port is used to connect directly to the appliance for system administration functions.
- Four 10/100/1000 Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right. The four ports form two accelerated pairs, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA), and 1/3 and 1/4 are accelerated pair B (apB).

The following figure shows the back panel of the SD-WAN 1000 appliance.

Figure 2. Citrix SD-WAN 1000 appliance, back panel

The following components are visible on the back panel of the SD-WAN 1000 appliance:

- 600 GB removable solid-state drive, which stores the appliance's software and user data.
- USB port (reserved for a future release).
Single power supply, rated at 300 watts, 100-240 volts.

Power on Appliance After Graceful Shut Down

To power on the appliance after a graceful shut down:

1. Connect a Serial console cable to the rear of the appliance and to the serial port on a management laptop.

2. On the management laptop, restart a putty session using the following configuration settings:
   - Serial line: COM1
   - Speed: 9600

3. Power on the appliance and as it is booting, press the following key in the Putty session to enter the BIOS configuration screen.
   
   Keypress: **DEL**

4. When in the BIOS, navigate to,
   - Advanced Tab > Select
   - Boot Feature > Enter
5. When in the Boot Feature screen, change the value of the parameter **Restore on AC Power Loss**; from **Last State > Power ON**.

6. Navigate to Save and Exit.

   - Select **Save changes** and **Reset**
   - Select **Yes**

   Allow the system to restart. This takes approximately five minutes.

7. After the appliance is powered on, login to the appliance management instance (SVM). The default IP address for the appliance is: 192.168.100.1, user name is: admin/password.
8. In the SD-WAN appliance GUI, navigate to **Configuration > Maintenance > Reboot Appliance**. Allow the appliance to fully shut down. Ensure that there are no power lights on the appliance when the shut down process has completed.

9. Power on the appliance to confirm that the BIOS configuration change has been applied successfully. This can be either done through the APC intelligent PDU Web Management console or by physically pulling the power cable out of the shut down SD-WAN appliance, waiting for 10 seconds and then plugging it back in again. The appliance power ups automatically from all shut down scenarios.
NetScaler SD-WAN 2000

Apr 06, 2017

The Citrix NetScaler SD-WAN 2000 platform has 3 models: SD-WAN 2000-010, SD-WAN 2000-020, and SD-WAN 2000-050, with bandwidths of 10Mbps, 20Mbps, and 50Mbps, respectively. Each model is a 1U appliance with one quad-core processor and 24 gigabytes (GB) of memory.

The following figure shows the front panel of the SD-WAN 2000 appliance.

Figure 1. Citrix NetScaler SD-WAN 2000, front panel

```
<table>
<thead>
<tr>
<th>LCD Keypad</th>
<th>LCD</th>
<th>Management/Aux1 Port</th>
<th>Ethernet Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>1/1, 1/2 = apA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1/3, 1/4 = apB</td>
</tr>
</tbody>
</table>
```

The appliance has the following ports:

- An RS232 serial console port.
- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.
- A copper Ethernet (RJ45) management port, numbered 0/1. The management port is used to connect directly to the appliance for system administration functions.
  
  Note: The LOM port also operates as a management port.

- Four 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right. The four ports form two accelerated pairs, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA), and 1/3 and 1/4 are accelerated pair B (apB).

The following figure shows the back panel of the SD-WAN 2000 appliance.

Figure 2. Citrix SD-WAN 2000 appliance, back panel

```
<table>
<thead>
<tr>
<th>Solid State Drive</th>
<th>Power Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>U80 port NMI Button (Recessed)</td>
<td>Solid State Drives (Reserved for future use)</td>
</tr>
<tr>
<td>Solid State Drives (Reserved for future use)</td>
<td>Disable Alarm Button</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Power Supply</td>
</tr>
</tbody>
</table>
```

The following components are visible on the back panel of the SD-WAN 2000 appliance:

- 600 GB removable solid-state drive, which stores the appliance's software and user data.
- Power switch, which turns off power to the appliance. Press the switch for five seconds to turn off the power.
- USB port (reserved for a future release).
- Non-maskable interrupt (NMI) button, for use at the request of Technical Support to produce a core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Single power supply, rated at 300 watts, 100-240 volts.
NetScaler SD-WAN 3000

Apr 06, 2017

The Citrix NetScaler SD-WAN 3000 platform has 3 models: SD-WAN 3000-050, SD-WAN 3000-100, and SD-WAN 3000-155, with bandwidths of 50M bps, 100 Mbps, and 155 Mbps, respectively. Each model is a 1U appliance with one quad-core processor and 32 gigabytes (GB) of memory.

The Citrix NetScaler SD-WAN 3000 appliance is available in two port configurations:

- Six 10/100/1000 Base-T copper Ethernet ports
- Four 1G SX Fiber ports

The following figure shows the front panel of a SD-WAN 3000 with six 10/100/1000 Base-T copper Ethernet ports.

Figure 1. Citrix NetScaler SD-WAN 3000 (6×10/100/1000 Base-T copper Ethernet ports), front panel

The following figure shows the front panel of a SD-WAN 3000 appliance with four 1G SX fiber ports.

Figure 2. Citrix NetScaler SD-WAN 3000 (4×1G SX Fiber ports), front panel

The appliance has the following ports:

- An RS232 serial console port.
- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.
- A copper Ethernet (RJ45) management port, numbered 0/1. The management port is used to connect directly to the appliance for system administration functions.
  
  Note: The LOM port also operates as a management port.

- Network Ports, in one of the following configurations:
  - SD-WAN 3000 (6x10/100/1000 Base-T copper Ethernet ports). Six 10/100/1000 Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, 1/4, 1/5, and 1/6 from left to right. The six ports form three accelerated pairs, which function
as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA), 1/3 and 1/4 are accelerated pair B (apB), and 1/5 and 1/6 are accelerated pair C (apC).

- SD-WAN 3000 (4x 1G SX Fiber ports). Four 1G SX fiber ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right. The four ports form two accelerated pairs, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA) and 1/3 and 1/4 are accelerated pair B (apB).

The following figure shows the back panel of the SD-WAN 3000 appliance.

Figure 3. Citrix NetScaler SD-WAN 3000 appliance, back panel

The following components are visible on the back panel of the SD-WAN 3000 appliance:

- Four 600 GB removable solid-state drives. The top left solid-state drive stores both the appliance's software and the user data. The other three store only user data.
- Power switch, which turns power to the appliance on or off. To turn off the power, press the switch for five seconds.
- USB port (reserved for a future release).
- Non-maskable interrupt (NMI) button, for use at the request of Technical Support to produce a core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Disable alarm button, which is nonfunctional unless you install a second power supply. In that case, it disables the alarm that sounds if the appliance is plugged into only one power outlet or one of the power supplies fails.
- Single power supply, rated at 450 watts, 100-240 volts.
Summary of Hardware Specifications

The following table summarizes the specifications of the NetScaler SD-WAN 400, 800, 1000, 2000, and 3000 hardware platforms.

Table 1. Citrix NetScaler SD-WAN 400, 800, 2000, 1000, and 3000 Platforms Summary

<table>
<thead>
<tr>
<th>H/W Specifications</th>
<th>SD-WAN 400</th>
<th>SD-WAN 800</th>
<th>SD-WAN 1000</th>
<th>SD-WAN 2000</th>
<th>SD-WAN 3000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Up to 6 Mbps</td>
<td>Up to 10 Mbps</td>
<td>Model 1000-006: 6 Mbps</td>
<td>Model 2000-010: 10 Mbps</td>
<td>Model 3000-050: 50 Mbps</td>
</tr>
<tr>
<td></td>
<td>Model 400-002: 2 Mbps</td>
<td></td>
<td>Model 1000-010: 10 Mbps</td>
<td>Model 2000-010: 10 Mbps</td>
<td>Model 3000-155: 155 Mbps</td>
</tr>
<tr>
<td>Maximum HDX sessions</td>
<td>Up to 60</td>
<td>Up to 100</td>
<td>200</td>
<td>300</td>
<td>500</td>
</tr>
<tr>
<td>Total sessions</td>
<td>500</td>
<td>10,000</td>
<td>10,000</td>
<td>20,000</td>
<td>50,000</td>
</tr>
<tr>
<td>Acceleration Plug-in CCUs</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>750</td>
<td>1,000</td>
</tr>
</tbody>
</table>

Hardware Specifications

<table>
<thead>
<tr>
<th></th>
<th>SD-WAN 400</th>
<th>SD-WAN 800</th>
<th>SD-WAN 1000</th>
<th>SD-WAN 2000</th>
<th>SD-WAN 3000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>2 Cores</td>
<td>2 Cores</td>
<td>2 Cores</td>
<td>4 Cores</td>
<td>4 Cores</td>
</tr>
<tr>
<td>Total disk space</td>
<td>1 x 160 GB SSD</td>
<td>1 x 240 GB SSD</td>
<td>1 x 600 GB SSD</td>
<td>4 x 600 GB SSD</td>
<td></td>
</tr>
<tr>
<td>SSD (dedicated Compression history)</td>
<td>40 GB</td>
<td>80 GB</td>
<td>275 GB</td>
<td>1.5 TB</td>
<td></td>
</tr>
<tr>
<td>H/W Specifications</td>
<td>SD-WAN 400</td>
<td>SD-WAN 800</td>
<td>SD-WAN 1000</td>
<td>SD-WAN 2000</td>
<td>SD-WAN 3000</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>2 pair with bypass 10/100/1000</td>
<td>2 pair with bypass 10/100/1000</td>
<td>4 x 10/100/1000 Base-T copper Ethernet</td>
<td>6 x 10/100/1000 Base-T copper Ethernet</td>
<td></td>
</tr>
<tr>
<td>Transceiver support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Power supplies</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

**Physical Dimensions**

<table>
<thead>
<tr>
<th>Rack Units</th>
<th>1U</th>
<th>1U</th>
<th>1U</th>
<th>1U</th>
</tr>
</thead>
<tbody>
<tr>
<td>System width</td>
<td>EIA 310-D for 19-inch racks</td>
<td>EIA 310-D for 19-inch racks</td>
<td>EIA 310-D for 19-inch racks</td>
<td>EIA 310-D for 19-inch racks</td>
</tr>
<tr>
<td>System depth</td>
<td>10.5&quot; (26.7 cm)</td>
<td>10.5&quot; (26.7 cm)</td>
<td>25.4&quot; (64.5 cm)</td>
<td>25.4&quot; (64.5 cm)</td>
</tr>
<tr>
<td>System weight</td>
<td>8 lbs (3.5 kg)</td>
<td>8 lbs (3.5 kg)</td>
<td>32 lbs (14.5 kg)</td>
<td>32 lbs (14.5 kg)</td>
</tr>
<tr>
<td>Shipping dimensions and weight</td>
<td>26L x 18.5W x 6.5&quot; H</td>
<td>26L x 18.5W x 6.5&quot; H</td>
<td>32L x 23.5W x 7.5&quot; H</td>
<td>32L x 23.5W x 7.5&quot; H</td>
</tr>
</tbody>
</table>

**Environmental and Regulatory**

<table>
<thead>
<tr>
<th>Voltage</th>
<th>100/240 VAC, 50-60 Hz</th>
<th>100/240 VAC, 50-60 Hz</th>
<th>100/240 VAC, 50-60 Hz</th>
<th>100/240 VAC, 50-60 Hz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power consumption (Max.)</td>
<td>200W</td>
<td>200W</td>
<td>300 W</td>
<td>450 W</td>
</tr>
<tr>
<td>Operating Temperature (degree Celsius)</td>
<td>10–35</td>
<td>10–35</td>
<td>0–40</td>
<td>0–40</td>
</tr>
<tr>
<td>Non-operating Temperature (degree Celsius)</td>
<td>SD-WAN 400</td>
<td>SD-WAN 800</td>
<td>SD-WAN 1000</td>
<td>SD-WAN 2000</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------</td>
<td>------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Allowed Relative Humidity</td>
<td>8%–90%</td>
<td>8%–90%</td>
<td>5%–95%</td>
<td>5%–95%</td>
</tr>
<tr>
<td>Safety certifications</td>
<td>CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)</td>
<td>CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)</td>
<td>CSA</td>
<td>TUV</td>
</tr>
<tr>
<td>Electromagnetic and susceptibility certifications</td>
<td>FCC (Part 15 Class A), EN 55022 Class A, EN 61000-3-2/-3-3, CISPR 22 Class A</td>
<td>FCC (Part 15 Class A), EN 55022 Class A, EN 61000-3-2/-3-3, CISPR 22 Class A</td>
<td>FCC (Part 15 Class A), CE, C-Tick, VCCI-A, CCC, KCC, NOM, SASO, SABS, PCT</td>
<td>FCC (Part 15 Class A), CE, C-Tick, VCCI-A, CCC, KCC, NOM, SASO, SABS, PCT</td>
</tr>
<tr>
<td>Environmental certifications</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
</tr>
</tbody>
</table>
## Supported Features

Oct 14, 2014

The following table lists various features supported on NetScaler SD-WAN 400, 800, 2000, 1000, and 3000 appliances.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Citrix NetScaler SD-WAN 400 series</th>
<th>Citrix NetScaler SD-WAN 800 series</th>
<th>Citrix NetScaler SD-WAN 1000 series</th>
<th>Citrix NetScaler SD-WAN 2000 series</th>
<th>Citrix NetScaler SD-WAN 3000 series</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoConfiguration</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>SD-WAN Plug-In</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Compression</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RPC over HTTPS</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>SSL Compression</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>TCP Acceleration</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Traffic Shaping</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Video Caching</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Windows File System Acceleration</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Windows Outlook Acceleration</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>XenApp/XenDesktop Acceleration</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Group Mode</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>High Availability Mode</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Inline Mode</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Virtual Inline Mode</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>WCCP Mode</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>VLANs</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Feature</td>
<td>Citrix NetScaler SD-WAN 400 series</td>
<td>Citrix NetScaler SD-WAN 800 series</td>
<td>Citrix NetScaler SD-WAN 1000 series</td>
<td>Citrix NetScaler SD-WAN 2000 series</td>
<td>Citrix NetScaler SD-WAN 3000 series</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------</td>
</tr>
</tbody>
</table>

Installation

Jan 28, 2011

Within a given series, all models use the same hardware, and the different WAN speed ratings are obtained through different licensing options. For example, both SD-WAN 400 models (the 400-002 and 400-006) use the same hardware, and a given appliance can be licensed either as a 2 Mbps appliance or a 6 Mbps appliance, but a SD-WAN 400 can not be upgraded to a SD-WAN 800, 1000, 2000, or 3000. The same is true of the other series.

The licensed bandwidth applies only to the sending direction, so a SD-WAN 400-002, rated at 2 Mbps in the sending direction, is appropriate for an ADSL link with a 12 Mbps/2 Mbps download/upload bandwidth.

In addition to differences in WAN bandwidth capabilities, the different series vary in CPU power, installed RAM, and installed disk capacity.

All models use solid-state drives instead of conventional hard drives for increased speed and reliability.
Preparing for Installation

Mar 16, 2012

Before you install your new appliance, carefully unpack your appliance and make sure that all parts were delivered. Once you are satisfied that your appliance has been delivered to your expectations, verify that the location where the appliance will be installed meets temperature and power requirements and that the server cabinet or floor-to-ceiling cabinet is securely bolted to the floor and has sufficient airflow.

Only trained and qualified personnel should install, maintain, or replace the appliance, and efforts should be taken to ensure that all cautions and warnings are followed.
Unpacking the SD-WAN Appliance

Apr 09, 2014

The hardware accessories for your particular appliance, such as cables, adapters, and rail kit, vary depending on the hardware platform you ordered. Unpack the box that contains your new appliance on a sturdy table with plenty of space and inspect the contents.

If you ordered a SD-WAN 400 or 800 appliance, the box should contain:

- The appliance you ordered
- One DB9 female to DB9 female console port cable
- One 6 ft CAT5 network cable
- One power cable

If you ordered a SD-WAN 1000, 2000 or 3000 appliance, the box should contain:

- The appliance you ordered
- One RJ-45 to DB-9 adapter
- One 6 ft RJ-45/DB-9 cable
- One power cable
- One standard 4-post rail kit

Note: If the kit that you received does not fit your rack, contact your Citrix sales representative to order the appropriate kit.

In addition to the items included in the box with your new appliance, you will need the following items to complete the installation and initial configuration process.

- Ethernet cables for each additional Ethernet port that you will connect to your network
- One available Ethernet port on your network switch or hub for each Ethernet port you want to connect to your network
- A computer to serve as a management workstation
Preparing the Site and Rack

Apr 09, 2014

A SD-WAN appliance has specific site and rack requirements. You must make sure that adequate environmental control and power density are available. Racks must be bolted to the ground, have sufficient airflow, and have adequate power and network connections. Preparing the site and rack are important steps in the installation process and will help ensure a smooth installation.

Site Requirements

The appliance should be installed in a server room or server cabinet with the following features:

Environment control
An air conditioner, preferably a dedicated computer room air conditioner (CRAC), capable of maintaining the cabinet or server room at a temperature of no more than 27 degrees C/80.6 degrees F at altitudes of up to 2100 m/7000 ft, or 18 degrees C/64.4 degrees F at higher altitudes, a humidity level no greater than 45 percent, and a dust-free environment.

Power density
Wiring capable of handling at least 4,000 watts per rack unit in addition to power needs for the CRAC.

Rack Requirements

The rack on which you install your appliance should meet the following criteria:

Rack characteristics
Racks should be either integrated into a purpose-designed server cabinet or be the floor-to-ceiling type, bolted down at both top and bottom to ensure stability. If you have a cabinet, it should be installed perpendicular to a load-bearing wall for stability and sufficient airflow. If you have a server room, your racks should be installed in rows spaced at least 1 meter/3 feet apart for sufficient airflow. Your rack must allow your IT personnel unfettered access to the front and back of each server and to all power and network connections.

Power connections
At minimum, two standard power outlets per unit.

Network connections
At minimum, four Ethernet connections per rack unit.

Space requirements
One empty rack unit for each SD-WAN 400, 800, 1000, 2000 and 3000 appliances.

Note: You can order the following rail kits separately.
- Compact 4-post rail kit, which fits racks of 23 to 33 inches.
- 2-post rail kit, which fits 2-post racks.
Cautions and Warnings

Oct 18, 2017
Electrical Safety Precautions

Warning

During installation or maintenance procedures, wear a grounding wrist strap to avoid ESD damage to the electronics of the appliance. Use a conductive wrist strap attached to a good earth ground or to the appliance. You can attach it to the connector beside the ESD symbol on the back.

Follow basic electrical safety precautions to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch, so that you can quickly remove power to the appliance if an electrical accident occurs.
- Remove all jewelry and other metal objects that might come into contact with power sources or wires before installing or repairing the appliance. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and may cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.
- Use a regulating, uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Never stack the appliance on top of any other server or electronic equipment.
- All appliances are designed to be installed on power systems that use TN earthing. Do not install your device on a power system that uses either TT or IT earthing.
- Make sure that the appliance has a direct physical connection to the earth during normal use. When installing or repairing an appliance, always make sure that the ground circuit is connected first and disconnected last.
- Make sure that a fuse or circuit breaker no larger than 120 VAC, 15 A U.S. (240 VAC, 16 A international) is used on all current-carrying conductors on the power system to which your appliances are connected.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, first shut down the appliance, and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages can be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power source can handle the appliance’s maximum power consumption rating with no danger of an overload. Always unplug any appliance before performing repairs or upgrades.
- Do not overload the wiring in your server cabinet or on your server room rack.
- During thunderstorms, or anticipated thunderstorms, avoid performing any hardware repairs or upgrades until the danger of lightning has passed.
- When you dispose of an old appliance or any components, follow any local and national laws on disposal of electronic waste.
- To prevent possible explosions, replace expired batteries with the same model or a manufacturer-recommended substitute and follow the manufacturer’s instructions for battery replacement.
- Never remove a power supply cover or any sealed part.
Appliance Precautions

- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest appliance first, at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near an electrical outlet for easy access.
- Mount equipment in a rack with sufficient airflow for safe operation.
- For a closed or multiple-unit rack assembly, the ambient operating temperature of the rack environment might be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously might cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should be used only for extending the appliance out of the rack. Do not use these handles for mounting the appliance on the rack. Use the rack-rail hardware, described later, instead.
Installing the Hardware

Dec 12, 2013

After you have determined that the location where you will install your appliance meets the environmental standards and the server rack is in place according to the instructions, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you will use for initial configuration. To complete the installation, you turn on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.
Rack Mounting the Appliance

Oct 18, 2017

A SD-WAN 400, 800, 1000, 2000 or 3000 appliance requires one rack unit. These appliances are rack-mount devices that can be installed into two-post relay racks or four-post EIA-310 server racks. Verify that the rack is compatible with your appliance.

To mount the appliance, you must first install the rails and then install the appliance in the rack, as follows:

- Remove the inner rails from the rail assembly.
- Attach the inner rails to the appliance.
- Install the rack rails on the rack.
- Install the appliance in the rack.

To remove the inner rails from the rail assembly
1. Place the rail assembly on a flat surface.
2. Slide out the inner rail toward the front of the assembly.
3. Depress the locking tabs until the inner rail comes all the way out of the rail assembly.
4. Repeat steps 1 through 3 to remove the second inner rail.

To attach the inner rails to the appliance
1. Position the right inner rail behind the ear bracket on the right side of the appliance.
2. Align the holes on the rail with the corresponding holes on the side of the appliance.
3. Attach the rail to the appliance with the provided screws.
4. Repeat steps 1 through 3 to install the left inner rail on the left side of the appliance.

To install the rack rails
1. Position the rack rails at the desired location in the rack, keeping the sliding rail guide facing inward.
2. Snap the rails to the rack.
   Note: Make sure that both rack rails are at same height and that the rail guides are facing inward.

To install the appliance in the rack
1. Align the inner rails, attached to the appliance, with the rack rails.
2. Slide the appliance into the rack rails, keeping the pressure even on both sides, and push the appliance into the rack rails until it locks into place.
3. Verify that the appliance is locked in place by pulling it all the way out from the rack.
Note

The illustration above might not represent your actual appliance.
Connecting the Cables

When the appliance is securely mounted on the rack, determine which ports you should use. You are then ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

**Warning**

Remove all jewelry and other metal objects that might come in contact with power sources or wires before installing or repairing the appliance. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly, and may cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.

**Ports**

A typical installation using a single accelerated-bridge uses three Ethernet ports (the Primary port and apA) and five IP addresses (three on the Primary port’s subnet and two on apA’s subnet).

The appliance has two motherboard ports and two (SD-WAN 400/800 and SD-WAN 1000/2000) or three (SD-WAN 3000) accelerated bridges. The Primary port is used for initial configuration.

On the SD-WAN 2000 and 3000 appliances, the motherboard ports are labeled “0/1” and “0/2.” They are equivalent to the Primary and Aux1 ports, respectively.

The SD-WAN 400/800/1000 and 2000 appliances each have two pairs of accelerated bridge ports. The 3000 appliance has three pairs of accelerated-bridge ports. On the appliance, ports 1/1 and 1/2 are the accelerated pair A (apA) bridge ports, ports 1/3 and 1/4 are the apB ports, and ports 1/5 and 1/6 are the apC bridge ports.

**Connecting the Ethernet Cables**

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on a 10/100/1000BASE-T port.

**To connect an Ethernet cable to a 10/100/1000BASE-T port**

1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port of the appliance.
2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.
3. Verify that the LED glows amber when the connection is established.

**Connecting the Console Cable**

You can use the console cable to connect your appliance to a computer or terminal, from which you can configure the appliance. Before connecting the console cable, configure the computer or terminal to support VT100 terminal emulation, 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE. Then connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

**To connect the console cable to a computer or terminal**

1. Insert the DB-9 connector at the end of the cable into the console port.
Note: To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.

2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.

Connecting the Power Cable

The appliances have one power supply, unless you have installed a second. A separate ground cable is not required, because the three-prong plug provides grounding. Provide power to the appliance by installing the power cord.

To connect the appliance to the power source

1. Connect one end of the power cable to the power outlet on the back panel of the appliance, next to the power supply.
2. Connect the other end of the power cable to a standard 110V/220V power outlet.
Switching on the Appliance

Jan 20, 2014

After you have installed the appliance in a rack and connected the cables, verify that the power cable is properly connected. If you have installed a second power supply, make sure the second cable is connected to an outlet for a different circuit than the first. After verifying the connections, you are ready to switch on the appliance.

To switch on the appliance

1. Verify that the appliance is connected through a console or Ethernet port. This will ensure that you can configure the appliance after it is switched on.
2. Depending on the appliance, press the ON/OFF toggle power switch or the power button to switch on the appliance.

Caution: Be aware of the location of the emergency power off (EPO) switch, so that if an electrical accident occurs you can quickly remove power from the appliance.
Initial Configuration

Aug 12, 2014
The appliance shipped from Citrix has default IP addresses configured on it. To deploy the appliance on the network, you must configure the appropriate IP addresses on the appliance to accelerate the network traffic.

To perform initial configuration:
- Identify the prerequisites for the initial configuration.
- Record various values required in the initial configuration procedure.
- Configure the appliance by connecting it to the Ethernet port.
- Perform additional configuration for Windows.
- Assign management IP address through the serial console.
- Troubleshoot initial configuration issues.

By default, the initial configuration deploys the appliance in inline mode.
Prerequisites

Aug 12, 2014

Before you begin configuring the appliance, make sure that the following prerequisites have been met:

- You should have physical access to the appliance.
- You have chosen four IP addresses for management of the appliance.
- In the Worksheet, record all IP addresses and other values you would use to configure the appliance. Preferably, print out the worksheet before you start the configuration process.
- You should already have a SD-WAN license key from Citrix, sent in an email. If you are using remote licensing, you need the IP address of the licensing server.
- WAN Send and Receive Speeds.
The following table lists the default values of network configuration, SD-WAN configuration, Windows configuration, system settings, password, and setup wizard in your traffic subnet and the management subnet. Record the values applicable to your appliance in the third column.

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Value for your Appliance</th>
<th>Description of the Field</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Configuration</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XenServer IP Address (Management Subnet)</td>
<td>192.168.100.2</td>
<td></td>
<td>Management IP address of the XenServer.</td>
</tr>
<tr>
<td>Management Service IP Address (Management Subnet)</td>
<td>192.168.100.1</td>
<td></td>
<td>Management IP address of the Management Service.</td>
</tr>
<tr>
<td>Netmask (Management Subnet)</td>
<td>255.255.0.0</td>
<td></td>
<td>Network mask for the management subnet.</td>
</tr>
<tr>
<td>Gateway (Management Subnet)</td>
<td>None</td>
<td></td>
<td>The default gateway IP address of the appliance.</td>
</tr>
<tr>
<td>Port Model</td>
<td>2-Port</td>
<td></td>
<td>Select 2-port or 4-port, depending on the model. In 4-port mode, Windows Server does not have access to ports 1/3 and 1/4.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>None</td>
<td></td>
<td>IP address of the DNS server. Citrix recommends that you specify a valid DNS server IP address. This is a mandatory parameter.</td>
</tr>
<tr>
<td><strong>SD-WAN Configuration</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address (Management Subnet)</td>
<td>192.168.100.20</td>
<td></td>
<td>Primary SD-WAN IP address at which you manage the SD-WAN instance.</td>
</tr>
<tr>
<td>Netmask (Management Subnet)</td>
<td>255.255.0.0</td>
<td></td>
<td>Network mask for the management IP address of the appliance. Same as previous netmask.</td>
</tr>
<tr>
<td>Gateway (Management Subnet)</td>
<td>None</td>
<td></td>
<td>The default gateway IP address of the appliance. Same as the previous gateway.</td>
</tr>
<tr>
<td><strong>System Settings</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP Server</td>
<td>(none)</td>
<td></td>
<td>IP address of the NTP server. Citrix recommends that you</td>
</tr>
</tbody>
</table>
### Deployment Worksheet

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>UTC</th>
<th>Specify the time zone for your location.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>nsroot</td>
<td>New password for access to the appliance.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>nsroot</td>
<td>New password for access to the appliance.</td>
</tr>
</tbody>
</table>

### Command Center Configuration

<table>
<thead>
<tr>
<th>Command Center IP Address</th>
<th>None</th>
<th>Optional. IP address of the Command Center appliance with which you want to register this appliance. More info.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Center Port</td>
<td>8443</td>
<td>Optional. Port number of the Command Center SD-WAN. More info.</td>
</tr>
<tr>
<td>Registration Password</td>
<td>None</td>
<td>Password you want to use to register the SD-WAN appliance.</td>
</tr>
</tbody>
</table>

### Licensing

<table>
<thead>
<tr>
<th>License Server Address</th>
<th>None</th>
<th>IP address of the licensing server. Required only when you select a remote model license type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing Service Port</td>
<td>27000</td>
<td>Port number of the licensing server. Required only when you select a remote model license type.</td>
</tr>
</tbody>
</table>

### Links

<table>
<thead>
<tr>
<th>Receive (Download) Speed</th>
<th>None</th>
<th>WAN link download speed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send (Upload) Speed</td>
<td>None</td>
<td>WAN link upload speed.</td>
</tr>
</tbody>
</table>
Configuring the Appliance by Connecting a Computer to the Ethernet Port

Aug 12, 2014
For initial configuration of a SD-WAN appliance, perform the following tasks:

- Configure the appliance for use on your site.
- Install the Citrix license.
- Enable acceleration.
- Enable traffic shaping (inline mode only).

With inline deployments, this configuration might be all you need, because most acceleration features are enabled by default and require no additional configuration.

You can configure the appliance connecting the appliance to your computer through either the Ethernet port or the serial console. The following procedure enables you to configure the appliance by connecting it to your computer through the Ethernet port.

If you want to configure the appliance by connecting it to the computer through the serial console, assign the management service IP address from your Worksheet by completing the Assigning a Management IP Address through the Serial Console procedure, and then run steps 4 through 25 of the following procedure.

Note: Make sure that you have physical access to the appliance.

To configure the appliance by connecting a computer to the SD-WAN appliance's Ethernet port 0/1

1. Set the Ethernet port address of a computer (or other browser-equipped device with an Ethernet port), to 192.168.100.50, with a network mask of 255.255.0.0. On a Windows device, this is done by changing the Internet Protocol Version 4 properties of the LAN connection, as shown below. You can leave the gateway and DNS server fields as blank.

2. Using an Ethernet cable, connect this computer to the port labeled MGMT on a SD-WAN 1000 appliance with Windows Server, or to the port labeled PRI on a SD-WAN 2000 appliance with Windows Server.

3. Switch on the appliance. Using the web browser on the computer, access the appliance by using the default management service IP address http://192.168.100.1.

4. On the login page, use the following default credentials to log on to the appliance:
   - Username: nsroot
   - Password: nsroot

5. Start the configuration wizard by clicking Get Started.

6. On the Platform Configuration page, enter the respective values from your worksheet, as shown in the following example:
   - Note: If, for configuration, you want to use the same network mask and gateway as those for Network Configuration, select the Use System Netmask and Gateway option.

7. Click Done. A screen showing the Installation in Progress… message appears. This process takes approximately 2 to 5 minutes, depending on your network speed.

Note: If you are configuring the appliance by connecting it to your computer through the serial console port, skip step 8.
through step 14.

8. A Redirecting to new management IP message appears.
9. Click OK.
10. Unplug your computer from the Ethernet port and connect the port to your management network.
11. Reset the IP address of your computer to its previous setting.
12. From a computer on the management network, log on to the appliance by entering the new Management Service IP address, such as https://<Management_IP_Address>, in a web browser.
13. To continue the configuration, accept the certificate and continue. The option to continue varies according to the web browser you are using.
14. Log on to the appliance by using the nsroot user name and the password from your worksheet.
15. The Configuration wizard starts again. In this wizard, some of the values which you have already provided, appear by default. Specify rest of the values you have recorded in your worksheet.
16. If you want to manage the appliance through Command Center, specify the Command Center IP address, port, and registration password in the Command Center Configuration page. Otherwise, skip this step.
17. In System Services section, update the values if necessary.
18. In the Licensing section, select the appropriate license type. You can either select a local license or a remote license server to apply a license to the appliance.
   1. If you opt for a local license, you must generate a license by using the host ID of the appliance. To generate a local license for the appliance, see http://support.citrix.com/article/ctx131110. To apply the license, you can navigate to the NetScaler SD-WAN appliance; Configuration > Appliance Settings > Licensing page, after completing the Configuration wizard.
   2. If you opt for a remote licensing server, you must select a remote appliance model and provide the IP address of the licensing server in the Licensing Server Address field.
19. In the WAN Link Definition section, specify receive and send speeds for the WAN link in the respective fields. Citrix recommends values 10% lower than the WAN bandwidth, to avoid network congestion.
20. By default, WAN-side adapter settings are configured on the appliance. Accept the default settings.
21. Click Install. After the Installation process is complete, the appliance restarts.
22. As soon as the appliance restarts, the Dashboard page appears.

23. To configure the appliance to accelerate the network traffic, open navigate to the Configuration tab.
   Note: Make sure that you have already applied the appropriate license to the appliance.
24. On the Network Adapters page of the Appliance Settings node, verify and, if necessary, assign IP addresses, subnet masks, and gateways to the accelerated bridges (apA and apB) to be used. Applying these changes restarts the appliance.
   Note: You need to assign IP addresses to apA and apB adapters only if you intended to configure WCCP mode, virtual inline mode, or the Video Caching feature on the appliance.
25. The Initial Configuration is complete. Traffic now flows through the appliance. The Dashboard page shows this traffic.
26. You need additional configuration on the appliance if you intend to use some of the modes and features, such as WCCP mode, virtual inline mode, video caching, secure peering, high availability, encrypted CIFS/MAPI acceleration, AppFlow monitoring, or SNMP monitoring.

Note:
- Inline installations place the appliance between your LAN and WAN routers, using both ports of the accelerated bridge, such as ports LAN1 and WAN1 on a SD-WAN 1000 appliance with Window Server or ports 1/1 and 1/2 on SD-WAN 2000
appliance with Windows Server, for the apA accelerated bridge port.

- WCCP and virtual inline installations connect a single accelerated bridge port to your WAN router.
- Virtual inline installations require that you configure your router to forward WAN traffic to the appliance. See Router Configuration.
- WCCP installations require configuration of your router and the appliance. See WCCP Mode.
Assigning a Management IP Address through the Serial Console

Aug 12, 2014

If you do not want to change the settings of your computer, you can perform initial configuration by connecting the appliance to your computer with a serial null modem cable. Make sure that you have physical access to the appliance.

To configure the appliance through the serial console

1. Connect a serial null modem cable to the appliance's console port.
2. Connect the other end of the cable to the serial COM port of a computer running a terminal emulator, such as Microsoft HyperTerminal, with settings 9600,N,8,1, p.
3. On the HyperTerminal output, press Enter. The terminal screen displays the Logon prompt.
   Note: You might have to press Enter two or three times, depending on the terminal program you are using.
4. At the logon prompt, log on to the appliance with the following default credentials:
   - **Username**: nsroot
   - **Password**: nsroot
5. At the $ prompt, run the following command to switch to the shell prompt of the appliance:
   ```
   $ ssh 169.254.0.10
   ```
6. Enter Yes to continue connecting to the management service.
7. Log on to the shell prompt of the appliance with the following default credentials:
   - **Password**: nsroot
8. At the logon prompt, run the following command to open the Management Service Initial Network Address Configuration menu:
   ```
   # networkconfig
   ```
9. Type 1 and press Enter to select option 1, and specify a new management IP address for the management service.
10. Type 2 and press Enter to select option 2, and specify a new management IP address for the XenServer server.
11. Type 3 and press Enter to select option 3, and then specify the network mask for the management service IP address.
12. Type 4 and press Enter to select option 4, and then specify the default gateway for the management service IP address.
13. Type 8 and press Enter to save the settings and exit.
14. Access the SD-WAN appliance by entering the new management service IP address of the appliance, such as `https://<Management_Service_IP_Address>`, in a web browser of a computer on the management network.
15. To continue the configuration, accept the certificate and continue. The option to continue varies according to the web browser you are using.
16. Run steps 4 through 25 of the Configuring the Appliance by Connecting a Computer to the Ethernet Port procedure to complete the configuration process.
Deployment Modes

Jan 28, 2011

A SD-WAN appliance acts as a virtual gateway. It is neither a TCP endpoint nor a router. Like any gateway, its job is to buffer incoming packets and put them onto the outgoing link at the right speed. This packet forwarding can be done in different ways, such as inline mode, virtual inline mode, and WCCP mode. Although these methods are called modes, you do not have to disable one forwarding mode to enable another. If your deployment supports more than one mode, the mode that the appliance uses is determined automatically by the Ethernet and IP format of each packet.

Because the appliance supports different forwarding modes and different kinds of non-forwarded connections, it needs a way of distinguishing one kind of traffic from another. It does so by examining the destination IP address and destination Ethernet address (MAC address), as shown in table below. For example, in inline mode, the appliance is acting as a bridge. Unlike other traffic, bridged packets are addressed to a system beyond the appliance, not to the appliance itself. The address fields contain neither the appliance's IP address nor the appliance's Ethernet MAC address.

In addition to pure forwarding modes, the appliance has to account for additional types of connections, including management connections to the GUI and the heartbeat signal that passes between members of a high-availability pair. For completeness, these additional traffic modes are also listed in table below.

Table 1. How Ethernet and IP Addresses Determine the Mode

<table>
<thead>
<tr>
<th>Destination IP Address</th>
<th>Destination Ethernet Address</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not appliance</td>
<td>Not appliance</td>
<td>Inline or Pass-through</td>
</tr>
<tr>
<td>Not appliance</td>
<td>Appliance</td>
<td>Virtual Inline or L2 WCCP</td>
</tr>
<tr>
<td>Appliance</td>
<td>Appliance</td>
<td>Direct (UI access)</td>
</tr>
<tr>
<td>Appliance (VIP)</td>
<td>Appliance</td>
<td>High-Availability. Proxy mode</td>
</tr>
<tr>
<td>Appliance (WCCP GRE Packet)</td>
<td>Appliance</td>
<td>WCCP GRE Mode</td>
</tr>
<tr>
<td>Appliance (Signaling IP)</td>
<td>Appliance</td>
<td>Signaling Connection (SD-WAN plugin Signaling Connection (SD-WAN plugin, Secure Peer) or Redirector Mode Connection (SD-WAN plugin)</td>
</tr>
</tbody>
</table>

All modes can be active simultaneously. The mode used for a given packet is determined by the Ethernet and IP headers.

The forwarding modes are:

- **Inline mode**, in which the appliance transparently accelerates traffic flowing between its two Ethernet ports. In this mode, the appliance appears (to the rest of the network) to be an Ethernet bridge. Inline mode is recommended, because it requires the least configuration.

- **WCCP mode**, which uses the WCCP v. 2.0 protocol to communicate with the router. This mode is easy to configure on most routers. WCCP has two variants: WCCP-GRE and WCCP-L2. WCCP-GRE encapsulates the WCCP traffic within
generic routing encapsulation (GRE) tunnels. WCCP-L2 uses un-encapsulated network Layer 2 (Ethernet) transport.

- **Virtual inline mode**, in which a router sends WAN traffic to the appliance and the appliance returns it to the router. In this mode, the appliance appears to be a router, but it uses no routing tables. It sends the return traffic to the real router. Virtual inline mode is recommended when inline mode and high-speed WCCP operation are not practical.
- **Group mode**, which allows two appliances to operate together to accelerate a pair of widely separated WAN links.
- **High availability mode**, which allows two appliances to operate as an active/standby high availability pair. If the primary appliance fails, the secondary appliance takes over.

Additional traffic types are listed here for completeness:

- **Pass-through traffic** refers to any traffic that the appliance does not attempt to accelerate. It is a traffic category, not a forwarding mode.
- **Direct access**, where the appliance acts as an ordinary server or client. The GUI and CLI are examples of direct access, using the HTTP, HTTPS, SSH, or SFTP protocols. Direct access traffic can also include the NTP and SNMP protocols.
- **Appliance-to-appliance communication**, which can include signaling connections (used in secure peering and by the SD-WAN plugin), VRRP heartbeats (used in high-availability mode), and encrypted GRE tunnels (used by group mode).
- **Deprecated modes**. Proxy mode and redirector mode are legacy forwarding modes that should not be used in new installations.
Customizing the Ethernet ports

Dec 26, 2012

A typical appliance has four Ethernet ports: two accelerated bridged ports, called *accelerated pair A* (apA.1 and apA.2), with a bypass (fail-to-wire) relay, and two unaccelerated motherboard ports, called Primary and Aux1. The bridged ports provide acceleration, while the motherboard ports are sometimes used for secondary purposes. Most installations use only the bridged ports.

Some SD-WAN units have only the motherboard ports. In this case, the two motherboard ports are bridged.

The appliance's user interface can be accessed by a VLAN or non-VLAN network. You can assign a VLAN to any of the appliance's bridged ports or motherboard ports for management purposes.

Figure 1. Ethernet Ports

![Diagram of Ethernet Ports](https://docs.citrix.com)

The ports are named as follows:

<table>
<thead>
<tr>
<th>Table 1. Ethernet Port Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motherboard port 1</td>
</tr>
<tr>
<td>Motherboard port 2</td>
</tr>
<tr>
<td>Bridge #1</td>
</tr>
<tr>
<td>Bridge #2</td>
</tr>
</tbody>
</table>
Port Parameters

May 24, 2013
Each bridge and motherboard port can be:
- Enabled or disabled
- Assigned an IP address and subnet mask
- Assigned a default gateway
- Assigned to a VLAN
- Set to 1000 Mbps, 100 Mbps, or 10 Mbps
- Set to full duplex, half-duplex, or auto (on SD-WAN WANOP 4000/5000 appliances, some ports can be set to 10 Gbps)

All of these parameters except the speed/duplex setting are set on the Configuration: IP Address page. The speed/duplex settings are set on the Configuration: Interface page.

Notes about parameters:
- Disabled ports do not respond to any traffic.
- The browser-based UI can be enabled or disabled independently on all ports.
- To secure the UI on ports with IP addresses, select HTTPS instead of HTTP on the Configuration: Administrator Interface: Web Access page.
- Inline mode works even if a bridge has no IP address. All other modes require that an IP address be assigned to the port.
- Traffic is not routed between interfaces. For example, a connection on bridge apA does not cross over to the Primary or Aux1 ports, but remains on bridge apA. All routing issues are left to your routers.
Accelerated Bridges (apA and apB)

Dec 07, 2012

Every appliance has at least one pair of Ethernet ports that function as an accelerated bridge, called apA (for accelerated pair A). A bridge can act in inline mode, functioning as a transparent bridge, as if it were an Ethernet switch. Packets flow in one port and out the other. Bridges can also act in one arm mode, in which packets flow in one port and back out the same port.

An appliance that has a bypass card maintains network continuity if a bridge or appliance malfunctions.

Some units have more than one accelerated pair, and these additional accelerated pairs are named apB, apC, and so on.

If the appliance loses power or fails in some other way, an internal relay closes and the two bridged ports are electrically connected. This connection maintains network continuity but makes the bridge ports inaccessible. Therefore you might want to use one of the motherboard ports for management access.

Caution: Do not enable the Primary port if it is not connected to your network. Otherwise, you cannot access the appliance, as explained in Ethernet Bypass and Link-Down Propagation. Bypass cards are standard on some models and optional on others. Citrix recommends that you purchase appliances with bypass cards for all inline deployments.

The bypass feature is wired as if a cross-over cable connected the two ports, which is the correct behavior in properly wired installations.

Important: Bypass installations must be tested - Improper cabling might work in normal operation but not in bypass mode. The Ethernet ports are tolerant of improper cabling and often silently adjust to it. Bypass mode is hard-wired and has no such adaptability. Test inline installations with the appliance turned off to verify that the cabling is correct for bypass mode.

If the appliance is equipped with two accelerated bridges, they can be used to accelerate two different links. These links can either be fully independent or they can be redundant links connecting to the same site. Redundant links can be either load-balanced or used as a main link and a failover link.

Figure 1. Using dual bridges

When it is time for the appliance to send a packet for a given connection, the packet is sent over the same bridge from which the appliance received the most recent input packet for that connection. Thus, the appliance honors whatever link decisions are made by the router, and automatically tracks the prevailing load-balancing or main-link/failover-link algorithm in real time. For non-load-balanced links, the latter algorithm also ensures that packets always use the correct bridge.

Multiple bridges are supported in both WCCP mode and virtual inline mode. Usage is the same as in the single-bridge case, except that WCCP has the additional limitation that all traffic for a given WCCP service group must arrive on the same bridge.
Two units with multiple bridges can be used in a high-availability pair. Simply match up the bridges so that all links pass through both appliances.
Motherboard Ports

Dec 05, 2012

Although the Ethernet ports on a bypass card are inaccessible when the bypass relay is closed, the motherboard ports remain active. You can sometimes access a failed appliance through the motherboard ports if the bridged ports are inaccessible.

The Primary Port

If the Primary port is enabled and has an IP address assigned to it, the appliance uses that IP address to identify itself to other acceleration units. This address is used internally for a variety of purposes, and is most visible to users as the Partner Unit field on the Monitoring: Optimization: Connections page. If no motherboard port is enabled, the appliance uses the IP address of Accelerated Pair A.

The Primary port is used for:
- Administration through the web based UI
- A back channel for group mode
- A back channel for high-availability mode

The Aux1 Port

The Aux1 port is identical to the Primary port. If the Aux1 port is enabled and the Primary port is not, the appliance takes its identity from the Aux1 port's IP address. If both are enabled, the Primary port’s IP address is the unit's identity.
VLAN Support

Dec 05, 2012

A virtual local area network (VLAN) uses part of the Ethernet header to indicate which virtual network a given Ethernet frame belongs to. SD-WAN appliances support VLAN trunking in all forwarding modes (inline, WCCP, virtual inline, and group mode). Traffic with any combination of VLAN tags is handled and accelerated correctly.

For example, if one traffic stream passing through the accelerated bridge is addressed to 10.0.0.1, VLAN 100, and another is addressed to 10.0.0.1, VLAN 111, the appliance knows that these are two distinct destinations, even though the two VLANs have the same IP address.

You can assign a VLAN to all, some, or none of the appliance's Ethernet ports. If a VLAN is assigned to a port, the management interfaces (GUI and CLI) listen only to traffic on that VLAN. If no VLAN is assigned, the management interfaces listen only to traffic without a VLAN. This selection is made on the Configuration: Appliance Settings: Network Adapters: IP Addresses tab.
Inline Mode

Dec 26, 2012
In inline mode, traffic passes into one of the appliance's Ethernet ports and out of the other. When two sites with inline appliances communicate, every TCP connection passing between them is accelerated. All other traffic is passed through transparently, as if the appliance were not there.

Figure 1. Inline mode, Accelerating All Traffic on a WAN

Note: Any TCP-based traffic passing through both units is accelerated. No address translation, proxying, or per-site setup is required. Inline mode is auto-detecting and auto-configuring.
Configuration is minimized with inline mode, because your WAN router need not be aware of the appliance's existence.

Depending on your configuration, inline mode's link-down propagation can affect management access to the appliance if a link goes down.

Inline mode is most effective when applied to all traffic flowing into and out of a site, but it can be used for only some of the site's traffic.
Ethernet Bypass and Link-Down Propagation

Oct 30, 2013

Note: Link-Down propagation was added to the SD-WAN (formerly SD-WAN) 1000, 2000, 3000, 4000, and 5000 appliances with the 7.2.1 release.

Most 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 the other as if the appliance were not there. In fail-to-wire mode, the appliance looks like a cross-over cable connecting the two ports.

Any failure of the appliance hardware or software also closes the relay. When the appliance is restarted, the bypass relay remains closed until the appliance is fully initialized, maintaining network continuity at all times. This feature is automatic and requires no user configuration.

When the bypass relay is closed, the appliance’s bridge ports are inaccessible.

If carrier is lost on one of the bridge ports, the carrier is dropped on the other bridge port to ensure that the link-down condition is propagated to the device on the other side of the appliance. Units that monitor link state (such as routers) are thus notified of conditions on the other side of the bridge.

Link-down propagation has two operating modes:
- If the Primary port is not enabled, the link-down state on one bridge port is mirrored briefly on the other bridge port, and then the port is re-enabled. This allows the appliance to be reached through the still-connected port for management, HA heartbeat, and other tasks.
- If the Primary port is enabled, the appliance assumes (without checking) that the Primary port is used for management, HA heartbeat, and other tasks. The link-down condition on one bridge port is mirrored persistently on the other port, until carrier is restored or the unit is rebooted. This is true even if the Primary port is enabled in the GUI but not connected to a network, so the Primary port should be disabled (the default) when not in use.
Accelerating an Entire Site

Dec 05, 2012

Inline mode, Accelerating All Traffic on a WAN shows a typical configuration for inline mode. For both sites, the appliances are placed between the LAN and the WAN, so all WAN traffic that can be accelerated is accelerated. This is the simplest method for implementing acceleration, and it should be used when practical.

Because all the link traffic is flowing through the appliances, the benefits of fair queuing and flow control prevent the link from being overrun.

In IP networks, the bottleneck gateway determines the queuing behavior for the entire link. By becoming the bottleneck gateway, the appliance gains control of the link and can manage it intelligently. This is done by setting the bandwidth limit slightly lower than the link speed. When this is done, link performance is ideal, with minimal latency and loss even at full link utilization.
To reserve the appliance's accelerated bandwidth for a particular group of systems, such as remote backup servers, you can install the appliance on a branch network that includes only those systems. This is shown in the following figure.

**Figure 1. Inline Mode, Accelerating Selected Systems Only**

SD-WAN traffic shaping relies on controlling the entire link, so traffic shaping is not effective with this topology, because the appliance sees only a portion of link traffic. Latency control is up to the bottleneck gateway, and interactive responsiveness can suffer.
Configuring and Troubleshooting Inline Mode

Dec 26, 2012
Inline mode requires only basic configuration, because it is applied automatically to any packets passing through the accelerated bridge. Troubleshooting is described under.
WCCP Mode

Sep 11, 2014

Web Cache Communication Protocol (WCCP) is a dynamic routing protocol introduced by Cisco. Originally intended only for web caching, WCCP version 2 became a more general-purpose protocol, suitable for use by accelerators such as Citrix NetScaler SD-WAN appliances.

WCCP mode is the simplest way of installing a SD-WAN appliance when inline operation is impractical. It is also useful where asymmetric routing occurs, that is, when packets from the same connection arrive over different WAN links. In WCCP mode, the routers use the WCCP 2.0 protocol to divert traffic through the appliance. Once received by the appliance, the traffic is treated by the acceleration engine and traffic shaper as if it were received in inline mode.

Note:
- For the purposes of this discussion, WCCP version 1 is considered obsolete and only WCCP version 2 is presented.
- The standard WCCP documentation calls WCCP clients “caches.” To avoid confusion with actual caches, Citrix generally avoids calling a WCCP client a “cache.” Instead, WCCP clients are typically called “appliances.”
- This discussion uses the term “router” to indicate WCCP-capable routers and WCCP-capable switches. Though the term “router” is used here, some high-end switches also support WCCP, and can be used with SD-WAN appliances.

The SD-WAN appliances support two WCCP modes:
- WCCP is the original SD-WAN WCCP offering supported since release 3.x. It supports a single appliance service group (no clustering).
- WCCP clustering, introduced in release 7.2, allows your router to load-balance traffic between multiple appliances.

The physical mode for WCCP deployment of a SD-WAN appliance is one-arm mode in which the appliance is connected directly to a dedicated port on the WAN router. The WCCP standard includes a protocol negotiation in which the appliance registers itself with the router, and the two negotiate the use of features they support in common. Once this negotiation is successful, traffic is routed between the router and the appliance according to the WCCP router and redirection rules defined on the router.

A WCCP-mode appliance requires only a single Ethernet port. The appliance should either be deployed on a dedicated router port (or WCCP-capable switch port) or isolated from other traffic through a VLAN. Do not mix inline and WCCP modes.

The following figure shows how a router is configured to intercept traffic on selected interfaces and forward it to the WCCP-enabled appliance. Whenever the WCCP-enabled appliance is not available, the traffic is not intercepted, and is forwarded normally.

Figure 1. WCCP Traffic Flow

WCCP allows traffic to be forwarded between the router and the appliance in either of the following modes:
- L2 Mode—Requires that the router and appliance be on the same L2 segment (typically an Ethernet segment). The IP packet is unmodified, and only the L2 addressing is altered to forward the packet. In many devices, L2 forwarding is
performed at the hardware layer, giving it the maximum performance. Because of its performance advantage, L2 forwarding is the preferred mode, but not all WCCP-capable devices support it.

- **GRE Mode**—Generic Routing Encapsulation (GRE) is a routed protocol and the appliance can in theory be placed anywhere, but for performance it should be placed close to the router, on a fast, uncongested path that traverses as few switches and routers as possible. GRE is the original WCCP mode. A GRE header is created and the data packet is appended to it. The receiving device removes the GRE header. With encapsulation, the appliance can be on a subnet that is not directly attached to the router. However, both the encapsulation process and the subsequent routing add CPU overhead to the router, and the addition of the 28-byte GRE header can lead to packet fragmentation, which adds additional overhead.

WCCP mode supports multiple routers and both GRE vs. L2 forwarding. Each router can have multiple WAN links. Each link can have its own WCCP service group.

Traffic shaping is not effective unless the appliance manages UDP traffic as well as TCP traffic. A second service group, with a UDP service group for each WAN link, is recommended if traffic shaping is desired.

A WCCP client (an appliance) uses UDP port 2048 to register itself with the router and to negotiate which traffic should be sent to it, and also which WCCP features should be used for this traffic. The appliance operates on this traffic and forwards the resulting traffic to the original endpoint. The status of an appliance is tracked through the WCCP registration process and a heartbeat protocol. The appliance first contacts the router over the WCCP control channel (UDP port 2048), and the appliance and router exchange information with packets named “Here_I_Am” and “I_See_You,” respectively. By default, this process is repeated every ten seconds. If the router fails to receive a message from the appliance for three of these intervals, it considers the appliance to have failed and stops forwarding traffic to it until contact is reestablished.

Different appliances using the same router can provide different services. To keep track of which services are assigned to which appliances, the WCCP protocol uses a service group identifier, a one-byte integer. When an appliance registers itself with a router, it includes service group numbers as well.

- A single appliance can support more than one service group.
- A single router can support more than one service group.
- A single appliance can use the same service group with more than one router.
- A single router can use the same service group with more than one appliance. For SD-WAN appliances, multiple appliances are supported in WCCP cluster mode, and a single appliance is supported in WCCP mode.
- Each appliance specifies a “return type” (L2 or GRE) independently for each direction and each service group. SD-WAN 4000/5000 appliances always specify the same return type for both directions. Other SD-WAN appliances allow the return type to be different.

**Multiple service groups** can be used with WCCP on the same appliance. For example, the appliance can receive service-group 51 traffic from one WAN link and service-group 62 traffic from another WAN link. The appliance also supports multiple routers. It is indifferent to whether all the routers use the same service group or different routers use different service groups.

**Service Group Tracking.** If a packet arrives on one service group, output packets for the same connection are sent on
the same service group. If packets arrive for the same connection on multiple service groups, output packets track the most recently seen service group for that connection.

When WCCP is used with high-availability mode, the primary appliance sends its own apA or apB management IP address, not the virtual address of the HA pair, when it contacts the router. If failover occurs, the new primary appliance contacts the router automatically, reestablishing the WCCP channel. In most cases the WCCP timeout period and the HA failover time overlap. As a result, the network outage is less than the sum of the two delays.

Standard WCCP allows only a single appliance in a WCCP service group. If a new appliance attempts to contact the router, it discovers that the other appliance is handling the service group, and the new appliance sets an Alert. It periodically checks to determine whether the service group is still active with the other appliance, and the new appliance handles the service group when the other appliance becomes inactive. WCCP clustering allows multiple appliances per service group.

The following figure shows a simple WCCP deployment, suitable for either L2 or GRE. The traffic port (1/1) is connected directly to a dedicated router port (Gig 4/12).

Figure 3. Simple WCCP deployment

In this example, the SD-WAN 4000/5000 is deployed in one-arm mode, with the traffic port (1/1) and the management port (0/1) each connecting to its own dedicated router port.

On the router, WCCP is configured with identical ip wccp redirect in statements on the WAN and LAN ports. Two service groups are used, 71 and 72. Service group 71 is used for TCP traffic and service group 72 is used for UDP traffic. The appliance does not accelerate UDP traffic, but can apply traffic shaping policies to it.

Note: The WCCP specification does not allow protocols other than TCP and UDP to be forwarded, so protocols such as ICMP and GRE always bypass the appliance.

SD-WAN appliances support WCCP clustering, which enables your router to load-balance your traffic between multiple appliances. For more information about deploying SD-WAN appliances as a cluster, see WCCP Clustering.


Note

When deploying SD-WAN in WCCP for switch redundancy, we can connect switch 2 to apB. Create a different SG for apB, give it a lower priority than the SG for apA. If apA higher SG is up, that will be used for redirection. If that is down, apB SG will be used. Please note that apA and apB need to be on different subnet.
WCCP Mode (Non-Clustered)

Sep 11, 2014

WCCP mode allows only a single appliance in a WCCP service group. If a new appliance attempts to contact the router, it discovers that the other appliance is handling the service group, and the new appliance sets an Alert. It periodically checks to determine whether the service group is still active with the other appliance, and the new appliance handles the service group when the other appliance becomes inactive.

Note: WCCP clustering allows multiple appliances per service group.

Following are limitations and best practices for (non-clustered) WCCP mode:

- On appliances with more than one accelerated pair, all the traffic for a given WCCP service group must arrive on the same accelerated pair.
- Do not mix inline and WCCP traffic on the same appliance. The appliance does not enforce this guideline, but violating it can cause difficulties with acceleration. (WCCP and virtual inline modes can be mixed, but only if the WCCP and virtual inline traffic are coming from different routers.)
- For sites with a single WAN router, use WCCP whenever inline mode is not practical.
- Only one appliance is supported per service group. If more than one appliance attempts to connect to the same router with the same service group, the negotiation will succeed only for the first appliance.
- For sites with multiple WAN routers serviced by the same appliance, WCCP can be used to support one, some, or all of your WAN routers. Other routers can use virtual inline mode.
Router Support for WCCP

Jan 31, 2014

Configuring the router for WCCP is very simple. WCCP version 2 support is included in all modern routers, having been added to the Cisco IOS at release 12.0(11)S and 12.1(3)T. The best router-configuration strategy is determined by the characteristics of your router and switches. Traffic shaping requires two service groups.

If your router supports Reverse Path Forwarding, you must disable it on all ports, because it can confuse WCCP traffic with spoofed traffic. This feature is found in newer Cisco routers such as the Cisco 7600.

There are two basic approaches to redirecting traffic from the router to the appliance:
- **On the WAN port only**, add a “WCCP redirect in” statement and a “WCCP redirect out” statement.
- **On every port on the router, except the port attached to the appliance**, add a “WCCP redirect in” statement.

The first method redirects only WAN traffic to the appliance, while the second method redirects all router traffic to the appliance, whether it is WAN related or not. On a router with several LAN ports and substantial LAN-to-LAN traffic, sending all traffic to the appliance can overload its LAN segment and burden the appliance with this unnecessary load. If GRE is used, the unnecessary traffic can load down the router as well.

On some routers, the "redirect in" path is faster and puts less of a load on the router's CPU than does the "redirect out" path. If necessary, this can be determined by direct experiment on your router. Try both redirection methods under full network load to see which delivers the highest transfer rates.

Some routers and WCCP-capable switches do not support "WCCP redirect out," so the second method must be used. To avoid overloading the router, the best practice to avoid redirecting large numbers of router ports through the appliance, perhaps by using two routers, one for WAN routing and one for LAN-to-LAN routing.

In general, method 1 is simpler, while method 2 may provide greater performance.

A service group can be either TCP or UDP, but not both. For the traffic shaper to be effective, both kinds of WAN traffic must pass through the appliance. Therefore:
- Acceleration requires one service group, for TCP traffic.
- Traffic shaping requires two service groups, one for TCP traffic and one for UDP traffic.
- The difference between the two is configured on the appliance, and the router accepts this configuration.
Configuring the Router

Dec 18, 2013

The appliance negotiates WCCP-GRE or WCCP-L2 automatically. The main choice is between *unicast operation* (in which the appliance is configured with the IP address of each router), or *multicast operation* (in which both the appliance and the routers are configured with the multicast address.)

**Normal (Unicast) operation**—For normal operation, the procedure is to declare WCCP version 2 and the WCCP group ID for the router as a whole, then enable redirection on each WAN interface. Following is a Cisco IOS example:

```
config term
ip wccp version 2
! We will configure the appliance to use group 51 for TCP and 52 for UDP.
ip wccp 51
ip wccp 52

! Repeat the following three lines for each WAN interface
! you wish to accelerate:
interface your_wan_interface
! If Reverse Path Forwarding is enabled (with an ip verify unicast
! source reachable" statement), delete or comment out the statement:
! ip verify unicast source reachable-via any
! Repeat on all ports.
ip wccp 51 redirect out
ip wccp 51 redirect in
ip wccp 52 redirect out
ip wccp 52 redirect in

! If the appliance is inline with one of the router interfaces
! (NOT SUPPORTED), add the following line for that interface
! to prevent loops:
ip wccp redirect exclude in
^Z
```

If multiple routers are to use the same appliance, each is configured as shown above, using either the same service groups or different ones.

**Multicast operation**—When giving the appliance and each router a multicast address, the configuration is slightly different than for normal operation. Following is a Cisco IOS example:

```
config term
ip wccp version 2
ip wccp 51 group-address 225.0.0.1

! Repeat the following three lines for each WAN interface
! you wish to accelerate:
interface your_wan_interface
! If Reverse Path Forwarding is enabled (with an ip verify unicast
! source reachable" statement), delete or comment out the statement:
```
! ip verify unicast source reachable-via any

ip wccp 51 redirect out
ip wccp 51 redirect in
!
! The following line is needed only on the interface facing the other router,
! if there is another router participating in this service group.
ip wccp 51 group-listen

! If the appliance is inline with one of the router interfaces,
! (which is supported but not recommended), add
! the following line for that interface to prevent loops:
ip wccp redirect exclude in
^Z
Basic Configuration Procedure for WCCP Mode on the SD-WAN Appliance

Jan 31, 2014

For most sites, you can use the following procedure to configure the WCCP mode on the appliance. The procedure has you set several parameters to sensible default values. Advanced deployments might require that you set these parameters to other values. For example, if WCCP service group 51 is already used by your router, you need to use a different value for the appliance.

To configure WCCP mode on the appliance

2. If no service groups have been defined, the Select Mode page appears. The options are Single SD-WAN and Cluster (Multiple SD-WAN). Select Single SD-WAN. You are taken to the WCCP page.
   Note: The mode labels are misleading. “Single SD-WAN” mode is also used for high-availability pairs.
3. If WCCP mode is not enabled, click Enable.
4. Click Add Service Group.
5. The default interface (apA), Protocol (TCP), WCCP Priority (0), Router Communication (Unicast), (Password blank) and Time to Live (1) values usually do not have to be changed for the first service group that you create, but if they do, type new values in the fields provided.
6. In the Router Addressing field (if you are using unicast) or the Multicast Address field (if you are using multicast), type the router's IP address. Use the IP for the router port used for WCCP communication with the appliance.
7. If more than one router is using WCCP to communicate with this appliance, add additional routers now.
8. If your routers have special requirements, set the Router Forwarding (Auto/GRE/Level-2), Router Packet Return (Auto/GRE/Level-2), and Router Assignment (Mask/Hash) fields accordingly. The defaults produce optimal results with most routers.
9. Click Add.
10. Repeat the preceding steps to create another service group, for UDP traffic (for example, service group Id 52 and Protocol UDP).
11. Go to the Monitoring: Appliance Performance: WCCP page. The Status field should change to Connected within 60 seconds.
12. Send traffic over the link and, on the Connections page, verify that connections are arriving and being accelerated.
WCCP Service Group Configuration Details

In a service group, a WCCP router and a SD-WAN appliance ("WCCP Cache" in WCCP terminology) negotiate communication attributes (capabilities). The router advertises its capabilities in the "I See You" message. The communication attributes are:

- Forwarding Method: GRE or Level-2
- Packet Return Method (multicast only): GRE or Level-2
- Assignment Method: Hash or Mask
- Password (defaults to none)

The appliance triggers an alert if it detects an incompatibility between its attributes and those of the router. The appliance might be incompatible because of a specific attribute of a service group (such as GRE or Level-2). More rarely, in a multicast service group, an alert can be triggered when the "Auto" selection chooses a particular attribute with a particular router connected, but the attribute is incompatible with a subsequent router.

Following are the basic rules for the communication attributes within a SD-WAN Appliance.

For Router Forwarding:
- When "Auto" is selected, the preference is for Level-2, because it is more efficient for both router and appliance. Level-2 is negotiated if the router supports it and the router is on the same subnet as the appliance.
- Routers in a unicast service group can negotiate different methods if "Auto" is selected.
- Routers in a multicast service group must all use the same method, whether forced with "GRE" or "Level-2", or, with "Auto," as determined by the first router in the service group to connect.
- For an incompatibility, an alert announces that the router "has incompatible router forwarding."

For Router Assignment:
- The default is Hash.
- When "Auto" is selected, the mode is negotiated with the router.
- All routers in a service group must support the same assignment method (Hash or Mask).
- For any service group, if this attribute is configured as "Auto," the appliance selects "Hash" or "Mask" when the first router is connected. "Hash" is chosen if the router supports it. Otherwise, "Mask" is selected. The problem of subsequent routers being incompatible with the automatically selected method can be minimized by manually selecting a method common to all routers in the service group.
- For an incompatibility, an alert announces that the router "has incompatible router assignment method."
- With either method, the single appliance in the service group instructs all the routers in the service group to direct all TCP or UDP packets to the appliance. Routers can modify this behavior with access lists or by selecting which interfaces to redirect to the service group.

For the Mask method, the appliance negotiates the "source IP address" mask. The appliance provides no mechanism to select "destination IP address" or the ports for either source or destination. The "source IP address" mask does not specifically identify any specific IP address or range. The protocol does not provide a means to specify a specific IP address. By default, because there is only a single appliance in the service group, a one-bit mask is used, to conserve router resources. (Release 6.0 used a larger mask.)

For Password:
- If the router requires a password, the password defined on the appliance must match. If the router does not require a password, the password field on the appliance must be blank.
WCCP Testing and Troubleshooting

Jan 31, 2014

When working with WCCP, the appliance provides different ways of monitoring the status of the WCCP interface, and your router should also provide information.

**Monitoring: Appliance Performance: WCCP Page**—The WCCP page reports the current state of the WCCP link, and reports most problems.

**Log Entries**—The Monitoring: Appliance Performance: Logging page shows a new entry each time WCCP mode is established or lost.

Figure 1. WCCP Log Entries (format varies somewhat with release)

**Router Status**—On the router, the “show ip wccp” command shows the status of the WCCP link:

```
Router>enable
Password:
Router#show ip wccp
Global WCCP information:
   Router information:
     Router Identifier:                   172.16.2.4
     Protocol Version:                    2.0

   Service Identifier: 51
     Number of Cache Engines:             0
     Number of routers:                   0
     Total Packets Redirected:            19951
     Redirect access-list:                -none-
     Total Packets Denied Redirect:       0
     Total Packets Unassigned:            0
     Group access-list:                   -none-
     Total Messages Denied to Group:      0
     Total Authentication failures:       0
```
The WCCP clustering feature enables you to multiply your acceleration capacity by assigning more than one SD-WAN appliance to the same links. You can cluster up to 32 identical appliances, for up to 32 times the capacity. Because it uses the WCCP 2.0 standard, WCCP clustering works on most routers and some smart switches, most likely including those you are already using.

Because it uses a decentralized protocol, WCCP clustering allows SD-WAN appliances to be added or removed at will. If an appliance fails, its traffic is rerouted to the surviving appliances.

Unlike SD-WAN high-availability, an active/passive pair that uses two appliances to provide the performance of a single appliance, the same appliances deployed as a WCCP cluster has twice the performance of a single appliance, delivering both redundancy and improved performance.

In addition to adding more appliances as your site’s needs increase, you can use Citrix’s “Pay as You Grow” feature to increase your appliances’ capabilities through license upgrades.

Citrix Command Center is recommended for managing WCCP clusters. The following figure shows a basic network of a cluster of SD-WAN appliances in WCCP mode, administered by using Citrix Command Center.

![Figure 1. SD-WAN Cluster Administered by Using Citrix Command Center](https://www.citrix.com)

The WCCP protocol supports up to 32 appliances in a fault-tolerant, load balanced array called a cluster. In the example below, three identical appliances (same model, same software version) are cabled identically and configured identically except for their IP addresses. Appliances using the same service groups with the same router can become a load balanced WCCP cluster. When a new appliance registers itself with the router, it can join the existing pool of appliances and receive its share of traffic. If an appliance leaves the network (as indicated by the absence of heartbeat signals), the cluster is rebalanced so that only the remaining appliances are used.

![Figure 2. A load-balanced WCCP cluster with three appliances](https://www.citrix.com)

One appliance in the cluster is selected as the designated cache, and controls the load-balancing behavior of the appliances in the cluster. The designated cache is the appliance with the lowest IP address. Because the appliances have identical configurations, it doesn't matter which one is the designated cache. If the current designated cache goes offline, a different appliance becomes the designated cache.

The designated cache determines how the load-balanced traffic is allocated and informs the router of these decisions. The router shares information with all members of the cluster, so the cluster can operate even if the designated cache goes offline.

Note: As normally configured, a SD-WAN 4000/5000 appliance appears as two WCCP caches to the router.

### Load-Balancing Algorithm

Load balancing in WCCP is static, except when an appliance enters or leaves the cluster, which causes the cluster to be rebalanced among its current members.
The WCCP standard supports load balancing based on a mask or a hash. For example, SD-WAN WCCP clustering uses the mask method only, using a mask of 1-6 bits of the 32-bit IP address. These address bits can be non-consecutive. All addresses yielding the same result when masked are sent to the same appliance. Load balancing effectiveness depends on choosing an appropriate mask value: a poor mask choice can result in poor load-balancing or even none, with all traffic sent to a single appliance.
Deployment Topology

Sep 11, 2014

Depending on your network topology, you can deploy WCCP cluster either with a single router or with multiple routers. Whether connected to a single router or multiple routers, each appliance in the cluster must be connected identically to all routers in use.

In the following diagram, three SD-WAN appliances accelerate the datacenter’s 200 Mbps WAN. The site supports 750 XenApp users.

As shown on the Datasheet, a SD-WAN 3000-100 can support 100 Mbps and 400 users, so a pair of these appliances supports 200 Mbps and 800 users, which satisfies the datacenter’s requirements of a 200 Mbps link and 750 users.

For fault tolerance, however, the WCCP cluster should continue to operate without becoming overloaded if one appliance fails. That can be accomplished by using three appliances when the calculations call for two. This is called the N+1 rule.

Failure is an unusual event, so usually all three appliances are in operation. In this case, each appliance is supporting only 67 Mbps and 250 users, leaving plenty of headroom, and making good use of the fact that the cluster has three times the CPU power and three times the compression history of a single appliance.

Without WCCP clustering, the same level of capacity and fault-tolerance would require a pair of SD-WAN 4000-500 appliances in high availability mode. Only one of these appliances is active at a time.

Using multiple WAN routers is very similar to using a single WAN router. If the previous example is changed to include two 100 Mbps links instead of one 200 Mbps link, the topology changes, but the calculations do not.
Limitations

Sep 08, 2014

Configuring appliances in a WCCP cluster has the following limitations:

- All appliances within a cluster must be the same model and use the same software release.
- Parameter synchronization between appliances within the cluster is not automatic. Use Command Center to manage the appliances as a group.
- SD-WAN traffic shaping is not effective, because it relies on controlling the entire link as a unit, and none of the appliances are in a position to do this. Router QoS can be used instead.
- The WCCP-based load-balancing algorithms do not vary dynamically with load, so achieving a good load balance can require some tuning.
- The hash method of cache assignment is not supported. Mask assignment is the supported method.
- While the WCCP standard allows mask lengths of 1-7 bits, the appliance supports masks of 1-6 bits.
- Multicast service groups are not supported; only unicast service groups are supported.
- All routers using the same service group pair must support the same forwarding method (GRE or L2).
- The forwarding and return method negotiated with the router must match: both must be GRE or both must be L2. Some routers do not support L2 in both directions, resulting in an error of "Router's forward or return or assignment capability mismatch." In this case, the service group must be configured as GRE.
- SD-WAN VPX does not support WCCP clustering.
- The appliance supports (and negotiates) only unweighted (equal) cache assignments. Weighted assignments are not supported.
- Some older appliances, such as the SD-WAN 700, do not support WCCP clustering.
- (SD-WAN 4000/5000 only) Two accelerator instances are required per interface in L2 mode. No more than three interfaces are supported per appliance (and then only on appliances with six or more accelerator instances.)
- (SD-WAN 4000/5000 only) WCCP control packets from the router must match one of the router IP addresses configured on the appliance for the service group. In practice, the router's IP address for the interface that connects it to the appliance should be used. The router's loopback IP should not be used.
Planning Your Deployment

Jan 30, 2014

Deploying appliances in a WCCP cluster requires more planning than does deploying a single appliance. Read the following sections carefully before proceeding.
Selecting Appliances

Jan 30, 2014

The appliances you select for the deployment must all be the same model, running the same software version. Otherwise, management and troubleshooting can become impractical.

Your appliance choice is generally made by comparing your site’s WAN bandwidth and number of WAN users to the capacities of the different appliances in the SD-WAN Data Sheet. For fault tolerance, always order one more appliance than is absolutely required according to the data sheet.

The number of appliances you need is found as follows, rounding up all fractions:

\[
\text{appliances} = \max( \text{appliances}_\text{bw}, \text{appliances}_\text{users} ) ,
\]

where

\[
\text{appliances}_\text{bw} = \left( \frac{\text{WAN bandwidth}}{\text{Optimized WAN capacity}} \right) + 1
\]
\[
\text{appliances}_\text{users} = \left( \frac{\text{WAN users}}{\text{Maximum HDX sessions}} \right) + 1
\]

Note that if \( \text{appliances} = 2 \), you can use just a single appliance instead of WCCP clustering, or an HA pair instead of WCCP clustering, since the equation builds in a spare appliance. In other words, WCCP clustering is not necessary (from a capacity perspective) unless appliances is 3 or more.

**Example.** Suppose you have 700 users and a 100 Mbps link. Some appliances you might consider are the SD-WAN 2000-050, the SD-WAN 3000-100, and the SD-WAN 4000-310.

<table>
<thead>
<tr>
<th>Model</th>
<th>Optimized WAN Capacity</th>
<th>Maximum HDX Sessions</th>
<th>Appliances_bw</th>
<th>Appliances_users</th>
<th>Appliances</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000-050</td>
<td>50 Mbps</td>
<td>300</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3000-100</td>
<td>100 Mbps</td>
<td>400</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4000-310</td>
<td>310 Mbps</td>
<td>750</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

As you can see from the above table, the higher-performance platforms require fewer appliances to get the job done, as you would expect. The SD-WAN 4000-310 meets the requirements with a single appliance, and evaluates to two appliances only because the equations build in a spare.

You can always add more capacity by adding more appliances, but that is not always necessary. The bandwidth limits of two of the three choices, the SD-WAN 3000-100 and the SD-WAN 4000-310, can be increased through a license upgrade. The SD-WAN 2000-050 however, is already at the high end of the range for SD-WAN 2000 appliances.
Load-Balancing in the WCCP Cluster

Sep 12, 2014
Traffic is distributed among the appliances in the WCCP cluster. If an appliance leaves the cluster (through failure, overload, or being manually disabled), its traffic is rebalanced by distributing it among the surviving members. If an appliance joins the cluster, traffic is rebalanced once more to give the new appliance its fair share.

The Address Mask
Traffic is distributed on the basis of an address mask that is applied to the source and destination addresses of WAN traffic. You must select an appropriate mask field for efficient load-balancing. An inappropriate mask can result in load-balancing that is poor to nonexistent. For example, if the mask matches an address field that is identical at all your remote sites, all your WAN traffic is sent to a single appliance, overloading it. For example, if all of your remote sites have an address in the form of 10.0.x.x, and your mask bits are within the 10.0 portion of the address all traffic is sent to a single appliance.

The address bits extracted by the address mask are used as an index that is used (indirectly) to select one of the WCCP caches (appliances). For example, an address mask with two “one” bits results in four possible values, depending on the address. Each of these values can be thought of as a bucket. With two mask bits, you have four buckets, numbered 0-3. The buckets are assigned to WCCP caches. To be effective, there must be at least as many buckets as caches. If you use a two-bit mask and have five or more caches, some caches are idle, because each bucket is assigned to only one cache, and there are not enough buckets to cover all five caches:

<table>
<thead>
<tr>
<th>Cache</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Buckets</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>-</td>
</tr>
</tbody>
</table>

If there are more buckets than caches, some caches are assigned multiple buckets. For example, if you set three mask bits, creating eight buckets, and you have four caches, two buckets are assigned to each cache. If you have five caches, three caches are assigned two buckets each, and two caches are assigned just one. If each bucket represents the same number of users, you have a 2:1 load imbalance across caches:

<table>
<thead>
<tr>
<th>Cache</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Buckets</td>
<td>0-1</td>
<td>2-3</td>
<td>4-5</td>
<td>6</td>
<td>7</td>
</tr>
</tbody>
</table>

Increasing the number of set mask bits reduces this imbalance. With four mask bits (16 index values) and five caches, four caches receive three buckets and one cache receives four buckets, resulting in only a 4:3 imbalance. With six set mask bits (the largest number supported), four caches receive 13 buckets and one receives 12, which is only a 13:12 load imbalance.

<table>
<thead>
<tr>
<th>Cache</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Buckets</td>
<td>0-12</td>
<td>13-25</td>
<td>26-38</td>
<td>39-51</td>
<td>52-63</td>
</tr>
</tbody>
</table>

Ideally, you would like each remote site to be directed to a single appliance in the WCCP cluster, so that all traffic to and from a given site is stored in the same compression history. With this arrangement, any traffic from one user at the site can be used to compress similar traffic from any other user at that site. In other words, for compressibility, load-balancing works best if it the address mask selects the bits that differentiate one remote site from another. These are often the least-significant bits of the subnet portion of the IP address. Using these bits tends to allocate the same number of remote sites (not users) per local appliance. A mask that aligns with the host portion of the address instead of the subnet results in a
more equal number of remote users (not sites) per appliance, but at the expense of compression effectiveness. (Compression is only effective when connections flow through the same appliances, and splitting traffic from the same remote site between two or more local appliances interferes with this.)

Finally, for good load-balancing, each "one" bit in the address mask must be set to one on 50% of the remote addresses, and set to zero on 50% of the remote addresses. This is not the case on all address bits, since in most WANs, the highest-order network bits never change at all (such as the 10 in 10.x.x.x). Such bits must never be selected by the address mask.

In addition, many subnets are only sparsely populated. For example, if only 50 addresses are used in the subnet 10.1.2.0/24, and they are assigned sequentially, the two higher-order host bits (representing the unused range of 10.1.2.64-10.1.2.255) for this subnet never change, and if these two bits are included in the address mask, three-fourths of the buckets receive no traffic.

Useful compromises between these two extremes can generally be found.

Follow these rules:
- The number of "one" bits in the address mask must allow at least as many combinations as there are WCCP caches in the cluster. That is, if you have eight appliances, the address mask must contain at least three "one" bits.
- The "one" bits in the address mask must each be inside the active address range for most of your remote subnets, or they skew the load-balancing distribution.
- The mask should split the address range of individual remote sites into as few pieces as possible, for best compression performance.
- If a remote appliance is faster than the local members of the WCCP cluster, the mask should be designed to divide its traffic between multiple local appliances. For example, a 100 Mbps remote appliance should have its traffic split between two 50 Mbps local appliances by setting a bit inside the remote appliance's active address range.
- The "one" bits in the mask are typically contiguous, but this is not required. They can be in any pattern.

**Example:** Suppose you set an address mask of 0x0000 0f00, which has four "one" bits. This defines a four-bit field that is extracted from the IP address, yielding 16 possible results (16 buckets). These buckets are in turn assigned to the actual WCCP caches in the WCCP cluster.

<table>
<thead>
<tr>
<th>Address</th>
<th>Masked Address (mask = 0x0000 0f00)</th>
<th>Bucket</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.5</td>
<td>0.0.0</td>
<td>0</td>
</tr>
<tr>
<td>10.0.1128</td>
<td>0.0.1.0</td>
<td>1</td>
</tr>
<tr>
<td>155.0.2.55</td>
<td>0.0.2.0</td>
<td>2</td>
</tr>
<tr>
<td>253.100.255.2</td>
<td>0.0.15.0</td>
<td>15</td>
</tr>
<tr>
<td>10.0.15.1</td>
<td>0.0.15.0</td>
<td>15</td>
</tr>
</tbody>
</table>

Zero bits in the mask are ignored, and the "one" bits are used to define the extracted field. So if the mask is 0x10 10 10 10, these widely separated "one" bits are extracted into a four-bit field, declaring 16 buckets and a bucket numbers in the range of 0-15.

If the mask value is set to zero, a default value of 0x00 00 0f 00 is used.
Assigning Buckets to Appliances

Sep 08, 2014

The mapping of bucket to appliances is subject to several variables:

- Which appliances are available: If an appliance is down, its share of buckets are given to the available appliance. If a new appliance is added to the cluster, it is given its fair share of buckets.
- The mapping algorithm used (deterministic or least-disruptive).
- The order in which appliances come online (least-disruptive mapping only).
- The IP addresses of the appliances. WCCP algorithms can use a sorted list of appliance IP addresses; for example, assigning buckets to appliances in the same order as the appliance IP addresses.

The most important of these factors, from an administrator's point of view, is the mapping algorithm.

**Deterministic mapping.** The deterministic mapping algorithm is less graceful than the least-disruptive algorithm, but it supports Hot Standby Router Protocol (HSRP) and Global Server Load Balancing (GSLB) routing, and is required when multiple routers using such protocols share the WCCP cluster.

Deterministic mapping is also the preferred method when the cluster has only two appliances.

Assignments are based on the IP addresses of the active appliances. Each appliance gets its fair share of bucket, with the lowest-numbered bucket being assigned to the appliance with the lowest IP address. If there are more appliances than buckets, the leftover appliances (with no bucket assigned to them) are the ones with the highest-numbered IP addresses. This deterministic assignment allows traffic to arrive for a single connection through any of the routers in the service group and be forwarded to the same appliance.

Reassignment can be disruptive to accelerated connections, which are reset if they migrate to a different appliance. With deterministic mapping, the number of buckets that are reassigned to new appliances can be quite high if there are three or more appliances.

**Least-disruptive mapping.** When a bucket is assigned to a different appliance, any open accelerated connections that used the old appliance is reset. The least-disruptive algorithm keeps the reassignment to a minimum. For example, if you have three appliances, and one appliance fails, the new mapping preserves roughly two-thirds of the assignments and remaps the remaining third (which fails anyway, because their appliance failed). The least-disruptive algorithm does not support HSRP or GSLB routing, because it is not guaranteed to result in identical mappings on all the routers in the service group, and therefore, packets from a single connection might be sent to two different appliances by two different routers, which causes accelerated connections to fail.
Startup and Failover Behavior

Each appliance registers itself with the routers specified in its service class definitions. The first appliance to register itself, becomes the designated cache, and works with the routers to apportion traffic between itself and the other caches (called subordinate caches). Because your appliances use identical WCCP algorithms, it does not matter which one becomes the designated cache.

As additional appliances come online, they are added to the WCCP cluster, and the traffic is reapportioned among the active appliances. This happens at ten-second increments. After a cold start of the routers or appliances, all of the appliances might come online within the same ten-second window, or they might arrive over multiple ten-second windows, causing traffic to be reapportioned multiple times before it stabilizes. In the latter case, the appliances that come online first may can become overloaded until additional appliances come online.

An accelerated connection fails when allocated to a different appliance, making reallocation disruptive. This is not true of non-accelerated connections, which generally experience a delay of thirty seconds or more, and then continue. The least disruptive mapping option minimizes the amount of reallocation when an appliance fails.

If an appliance fails or otherwise goes offline, its absence is noted, and the designated cache reapportions its traffic to the remaining appliances. If the designated cache itself goes offline, the role of designated cache is also reapportioned. It takes about thirty seconds for the cluster to react to the loss of a cache.
### Deployment Worksheet

Sep 12, 2014

On the following worksheet, you can calculate the number of appliances needed for your installation and the recommended mask field size. The recommended mask size is 1-2 bits larger than the minimum mask size for your installation.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Model Used</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Supported XenApp and XenDesktop Users Per Appliance</td>
<td>Uspec =</td>
<td>From data sheet</td>
</tr>
<tr>
<td>XenApp and XenDesktop Users on WAN Link</td>
<td>Uwan =</td>
<td>—</td>
</tr>
<tr>
<td>User overload Factor</td>
<td>Uoverload = Uwan/Uspec =</td>
<td>—</td>
</tr>
<tr>
<td>Supported BW Per Appliance</td>
<td>BWspec =</td>
<td>From data sheet</td>
</tr>
<tr>
<td>WAN Link BW</td>
<td>BWwan =</td>
<td>—</td>
</tr>
<tr>
<td>BW Overload Factor</td>
<td>BWoverload = BWwan/BWspec =</td>
<td>—</td>
</tr>
<tr>
<td>Number of appliances required</td>
<td>N = max(Uoverload, BWoverload) + 1 =</td>
<td>Includes one spare</td>
</tr>
<tr>
<td>Min number of buckets</td>
<td>Bmin = N, rounded up a power of 2 =</td>
<td>—</td>
</tr>
<tr>
<td>If SD-WAN 4000 or 5000,</td>
<td>Bmin = 2*N, rounded up to a power of 2 =</td>
<td>—</td>
</tr>
<tr>
<td>Recommended value</td>
<td>B = 4 * Bmin if Bmin &lt;= 16, else 2 * Bmin =</td>
<td>—</td>
</tr>
<tr>
<td>Number of &quot;one&quot; bits in address mask</td>
<td>M = log2(B)</td>
<td>If B=16, M=4.</td>
</tr>
</tbody>
</table>

Mask value: The mask value is a 32-bit address mask with a number of “one” bits equal to M in the above worksheet. Often
these bits can be the least-significant bits in the WAN subnet mask used by your remote sites. If the masks at your remote sites vary, use the median mask. (Example: With /24 subnets, the least significant bits of the subnet are 0x00 00 nn 00. The number of bits to set to one is log2(mask size); if mask size is 16, set four bits to one. So with a mask size of 16 and a /24 subnet, set the mask value to 0x00 00 0f 00: ______

The above guidelines work only if the selected subnet field is evenly distributed in your traffic, that is, that each address bit selected by the mask is a one for half the remote hosts, and a zero for the other half. Otherwise, load-balancing is impaired. This even distribution might be true for only a small number of bits in the network field (perhaps only two or three bits). If this is the case with your network, instead of masking bits in the offending area of the subnet field, displace those bits to a portion of the host address field that has the 50/50 property. For example, if only three subnet bits in a /24 subnet have the 50/50 property, and you are using four mask bits, a mask of 0x00 00 07 10 avoids the offending bit at 0x00 00 0800 and displaces it to 0x00 00 00 10, a portion of the address field that is likely to have the 50/50 property if your remote subnets generally use at least 32 IP addresses each.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final Mask Value</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Accelerated Bridge</td>
<td>Usually apA</td>
<td></td>
</tr>
<tr>
<td>WAN Service Group</td>
<td>A service group not already in use on your router (51-255)</td>
<td></td>
</tr>
<tr>
<td>LAN Service Group</td>
<td>Another unused service group</td>
<td></td>
</tr>
<tr>
<td>Router IP address</td>
<td>IP address of router interface on port facing the appliance</td>
<td></td>
</tr>
<tr>
<td>WCCP Protocol (usually &quot;Auto&quot;)</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>DC Algorithm</td>
<td>Use “Deterministic” if you have only two appliances or are using dynamic load balancing like HSRP or GSLB. Otherwise, use “Least Disruptive.”</td>
<td></td>
</tr>
</tbody>
</table>
Configuring WCCP Clustering

Sep 11, 2014
After you have finalized the deployment topology, considered all limitations, and filled in the deployment worksheet, you are ready to deploy your appliances in a WCCP cluster. To configure the WCCP cluster, you need to perform the following tasks:

- Configuring the NetScaler Instances
- Configuring the Router
- Configuring the Appliance
Configuring the Router

Sep 12, 2014

WCCP configuration on the router is simple, because most WCCP parameters are set by the appliances.

Unlike legacy SD-WAN WCCP support, WCCP clustering uses two service groups for TCP traffic. One service group is used on the router’s WAN interface, and the other is used on the router’s LAN interfaces (except for the LAN interface used by the SD-WAN appliances themselves, when deployed in L2-mode WCCP cluster).

As shown in the following figure, you need to configure two service groups because WCCP allows the mask to be applied to either the source IP or the destination IP address, which is not quite what is required. To keep connections between two endpoints together, regardless of which endpoint initiates the connection, the appliance applies the address mask to the source IP address of incoming WAN traffic, and to the destination IP address of incoming LAN traffic. This requires two service groups.

The WAN service group uses WCCP source-ip address masking, while the LAN service group uses dest-ip masking. In some deployments, it may be necessary to reverse the assignments, using the “WAN” service group for your LAN interface and vice versa. This might occur if the number of local IP addresses greatly exceeds the number of remote IP addresses.

Figure 1. SD-WAN WCCP Cluster

To configure WCCP clustering on the router

This procedure assumes Cisco routers, but is similar on other routers. It uses the first of the two methods, discussed above, of redirecting WCCP traffic with an ip wccp redirect in statement on both LAN and WAN ports.

1. Fill in the WCCP clustering Deployment Worksheet.
2. Log on to your router
3. In the global declarations section, declare each service group on the WCCP clustering worksheet, listed as **WAN service group** and **LAN Service group**. For example, `ip wccp 61` and `ip wccp 62`.
   Note: The `ip wccp` command allows, but does not require, a more elaborate syntax than this, and can specify an ACL name or a password. Both service groups must have the same password, if one is used. The ACLs can be different.
4. Inside the interface declarations for each WAN interface that connects to remote SD-WAN appliances, add an `ip wccp x redirect in` statement, where `x` is the WAN service group from the WCCP clustering worksheet.
5. Inside the interface declarations for each LAN interface (except the one connecting to the WCCP cluster, if you are using L2 mode), add an `ip wccp y redirect in` statement, where `y` is the LAN service group from the WCCP clustering worksheet.
6. Save your configuration.

**Example.** The following example uses service group 61 for the WAN service group and service group 62 for the LAN service group. Three router interfaces are used. One is connected to the WAN, one is connected to the LAN, and one is connected to the WCCP cluster.

```
! Example is for WCCP clustering using WCCP redirect in statements
! on LAN and WAN interfaces.
! This definition is appropriate for modern Cisco routers.
! Global declarations
ip wccp 61
ip wccp 62
```

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.573
interface GigabitEthernet1/1
description LAN interface. SG 62 is used for LAN
ip address 172.80.1.56 255.255.255.0
ip wccp 62 redirect in
!
interface GigabitEthernet1/2
description LAN interface attaching SD-WAN L2-WCCP appliances
description (No wccp redirect statements are used on this interface)
ip address 172.80.21.56 255.255.255.0
!
interface GigabitEthernet1/3
description WAN interface. SG 61 is used for WAN
ip address 172.80.22.56 255.255.255.0
ip wccp 61 redirect in

Note: If the router used multiple ports for LAN traffic, each port is configured with an ip wccp 62 redirect in statement. Similarly, if the router used multiple ports for WAN traffic, each port is configured with an ip wccp 61 redirect in statement.

- If the router used multiple ports for LAN traffic, each port is configured with an ip wccp 62 redirect in statement. Similarly, if the router used multiple ports for WAN traffic, each port is configured with an ip wccp 61 redirect in statement.
- If multiple routers shared the same WCCP cluster, they use the same service groups.

It is also possible to use ip wccp redirect statements on only the WAN interfaces:

- Example for WCCP clustering using WCCP redirect in/out statements on
- WAN interface only

  This definition is appropriate for modern Cisco routers.

  interface GigabitEthernet1/3
description WAN interface. SG 61 is used for WAN. SG 62 is used for LAN.
ip address 172.80.22.56 255.255.255.0
ip wccp 61 redirect in
ip wccp 62 redirect out
!
In many routers, the ip wccp redirect out path is not optimized in hardware, but uses the CPU. If the router's capabilities along this path exceeds the WAN speed, this method is practical, and is simpler than using redirect statements on every interface.

Router ACLs can be used to limit redirection. For example, for initial testing, perhaps only a single remote IP address might be allowed to be redirected through WCCP.
Configuring the Appliance

Sep 09, 2014
Repeat the following procedure for each appliance in the cluster:
1. Fill in the WCCP clustering Deployment Worksheet.
2. Navigate to Configuration > Appliance Settings > WCCP page.
3. Click Enable to enable WCCP mode on the appliance.
4. Select Cluster (Multiple Caches) option.
5. Fill in parameters in the Select SD-WAN Cluster section.
6. Enter T5 from your worksheet as the Cache 1 IP, T6 as the Cache 2 IP, T2 as the Subnet Mask, and T1 as the Gateway. Click Save. The Configure Service Group section appears.
7. In the Service Group Details section, specify the WAN and LAN service groups (T11 and T12 from your worksheet).
8. In the Priority field, select 100 (in practice this value is somewhat arbitrary).
9. From the Protocol list, select TCP.
10. In the DC Algorithm field, select Deterministic or Least Disruptive. “Deterministic” is always safe to use, and should be used if you are using only two appliances, or are using multiple routers. “Least Disruptive” disrupts fewer user sessions on failover when used with clusters of three or more appliances, but has restrictions on its use.
11. Set Service Group Pair Status to On.
12. If your router is configured to require a password, enter the password in the Service Group Password field. Otherwise, leave the field blank.
13. In the Router Communications Details section, enter the IP address of the router (T8 on your worksheet: often identical to T1 as well). This is the IP address of the appliance-facing router interface. If you use multiple routers to communicate with the appliance, list them all here.
14. From the Router Forwarding list, select Level 2 or GRE, according to the capabilities of your router. Use Level 2 if you can, and GRE if you must.
15. For the Mask Value, enter the value you determined from the WCCP Clustering worksheet. This is a critical value: a poor choice will result in poor load-balancing or none at all.
16. Click Create. This creates the WAN and LAN service groups.
17. On the Configuration > Optimization Rules > Link Definitions page, change the bandwidth limits on each defined WAN to 95% of the aggregate speed of all your WANs. This prevents the link from being under-utilized when load-balancing is imperfect. If ICA (XenApp/XenDesktop) is the dominant use, set each appliance to (95% of WAN bandwidth)/N, where N is the number of appliances (or twice the number of appliances if they are SD-WAN 4000 or 5000 units), to divide the bandwidth equally among the appliances. This latter method is most appropriate for applications with large numbers of active connections that have relatively low bandwidth requirements.
The Monitoring > Appliance > Application Performance > WCCP page shows the current state of not only the local appliance but of all other appliances that have joined the cluster. Select a WCCP cache and click Get Info.

The Cache Status tab shows the local appliance's status. When all is well, the status is “25: has assignment.” You must refresh the page manually to monitor changes in status. If the appliance does not reach the status of “25: has assignment” within a timeout period, other informative status messages are displayed.

Additional information is displayed when you click on the Service Group or the Routers tabs.

The Cluster Summary tab displays information about the WCCP cluster as a whole. As a side effect of the WCCP protocol, each member of the cluster has information about all the others, so this information can be monitored from any appliance in the cluster.

Your router can also provide status information. See your router documentation.
Virtual Inline Mode

Dec 28, 2012

Note: Use virtual inline mode only when both inline mode and WCCP mode are impractical. Do not mix inline and virtual inline modes within the same appliance. However, you can mix virtual inline and WCCP modes within the same appliance. Citrix does not recommend virtual inline mode with routers that do not support health monitoring.

In virtual inline mode, the router uses policy based routing (PBR) rules to redirect incoming and outgoing WAN traffic to the appliance for acceleration, and the appliance forwards the processed packets back to the router. Almost all of the configuration tasks are performed on the router. The only thing to be configured on the appliance is the forwarding method, and the default method is recommended.

Like WCCP, Virtual inline deployment requires no rewiring and no downtime, and it provides a solution for asymmetric routing issues faced in a deployment with two or more WAN links. Unlike WCCP, it contains no built-in status monitoring or health checking, making troubleshooting difficult. WCCP is thus the recommended mode, and virtual inline is recommended only when inline and WCCP modes are both impractical.

The following figure shows a simple network in which all traffic destined for or received from the remote site is redirected to the appliance. In this example, both the local site and remote site use virtual inline mode.

Figure 1. Virtual Inline Example

Following are some configuration details for the network in this example:

- Endpoint systems have their gateways set to the local router (which is not unique to virtual inline mode).
- Each router is configured to redirect both incoming and outgoing WAN traffic to the local appliance.
- Each appliance processes the traffic received from its local router and forwards it back to the router.
- PBR rules configured on the router prevent routing loops by allowing packets to make only one trip to and from the appliance. The packets that the appliance forwards back to the router are sent to their original (local or remote) destination.
- Each appliance has its default gateway set to the address of the local router, as usual (on the Configuration: Network Adapters page). The options for forwarding packets back to the router are Return to Ethernet Sender and Send to Gateway.
Virtual inline mode offers two packet-forwarding options:

**Return to Ethernet Sender (default)**—This mode allows multiple routers to share an appliance. The appliance forwards virtual inline output packets back to where they came from, as indicated by the Ethernet address of the incoming packet. If two routers share a single appliance, each gets its own traffic back, but not the traffic from the other router. This mode also works with a single router.

**Send to Gateway (not recommended)**—In this mode, virtual inline output packets are forwarded to the default gateway for delivery, even if they are destined for hosts on the local subnet. This option is usually less desirable than the Return to Ethernet Sender option, because it adds an easily forgotten element of complexity to the routing structure.

**To specify the packet-forwarding option**—On the Configuration: Optimization Rules: Tuning page, next to Virtual Inline, select Return to Ethernet Sender or Send to Gateway.
Router Configuration

May 23, 2013

The router has three tasks when supporting virtual inline mode:
1. It must forward both incoming and outgoing WAN traffic to the SD-WAN appliance.
2. It must forward SD-WAN traffic to its destination (WAN or LAN).
3. It must monitor the health of the appliance so that the appliance can be bypassed if it fails.

In virtual inline mode, the packet forwarding methods can create routing loops if the routing rules do not distinguish between a packet that has been forwarded by the appliance and one that has not. You can use any method that makes that distinction.

A typical method involves dedicating one of the router's Ethernet ports to the appliance and creating routing rules that are based on the Ethernet port on which packets arrive. Packets that arrive on the interface dedicated to the appliance are never forwarded back to the appliance, but packets arriving on any other interface can be.

The basic routing algorithm is:
- Do not forward packets from the appliance back to the appliance.
- If the packet arrives from the WAN, forward it to the appliance.
- If the packet is destined for the WAN, forward to the appliance.
- Do not forward LAN-to-LAN traffic to the appliance.
- Traffic shaping is not effective unless all WAN traffic passes through the appliance.

Note: When considering routing options, keep in mind that returning data, not just outgoing data, must flow through the appliance. For example, placing the appliance on the local subnet and designating it as the default router for local systems does not work in a virtual inline deployment. Outgoing data would flow through the appliance, but incoming data would bypass it. To force data through the appliance without router reconfiguration, use inline mode.

If the appliance fails, data should not be routed to it. By default, Cisco policy based routing does no health monitoring. To enable health monitoring, define a rule to monitor the appliance's availability, and specify the "verify-availability" option for the "set ip next-hop" command. With this configuration, if the appliance is not available, the route is not applied, and the appliance is bypassed.

Important: Citrix recommends virtual inline mode only when used with health monitoring. Many routers that support policy-based routing do not support health-checking. The health-monitoring feature is relatively new. It became available in Cisco IOS release 12.3(4)T.

Following is an example of a rule for monitoring the availability of the appliance:

```
!- Use a ping (ICMP echo) to see if appliance is connected
track 123 rtr 1 reachability
! rtr 1 type echo protocol IcmpEcho 192.168.1.200 schedule 1 life forever start-time now
```
This rule pings the appliance at 192.168.1.200 periodically. You can test against 123 to see if the unit is up.
Routing Examples

Feb 06, 2014
The following examples illustrate configuring Cisco routers for the local and remote sites shown in Virtual inline example. To illustrate health monitoring, the configuration for the local site includes health monitoring, but the configuration for the remote site does not.

Note: The configuration for the local site assumes that a ping monitor has already been configured. The examples conform to the Cisco IOS CLI. They might not be applicable to routers from other vendors.

Local Site, Health-Checking Enabled

! For health-checking to work, do not forget to start
! the monitoring process.
!
! Original configuration is in normal type.
! appliance-specific configuration is in bold.
!
ip cef
!
interface FastEthernet0/0
ip address 10.10.10.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 172.68.1.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.1.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.1.1
!
ip access-list extended client_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
! Now set the appliance as the next hop, if it's up.
set ip next-hop verify-availability 192.168.1.200 20 track 123
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop verify-availability 192.168.1.200 10 track 123
Remote Site (No Health Checking)

! This example does not use health-checking.
! Remember, health-checking is always recommended,
! so this is a configuration of last resort.
!

ip cef
!
interface FastEthernet0/0
ip address 20.20.20.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 171.68.2.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.2.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.2.1
!
ip access-list extended client_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
set ip next-hop 192.168.2.200
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop 192.168.2.200
!

Each of the above examples applies an access list to a route map and attaches the route map to an interface. The access lists identify all traffic originating at one accelerated site and terminating at the other (A source IP of 10.10.10.0/24 and destination of 20.20.20.0/24 or vice versa). See your router's documentation for the details of access lists and route-maps.

This configuration redirects all matching IP traffic to the appliances. If you want to redirect only TCP traffic, you can change the access-list configuration as follows (only the remote side's configuration is shown here):
!
ip access-list extended client_side
permit tcp 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit tcp 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
Note that, for access lists, ordinary masks are not used. Wildcard masks are used instead. Note that when reading a
wildcard mask in binary, "1" is considered a "don't care" bit.
Virtual Inline for Multiple-WAN Environments

Dec 27, 2012
Enterprises with multiple WAN links often have asymmetric routing policies, which seem to require that an inline appliance be in two places at once. Virtual inline mode solves the asymmetric routing problem by using the router configuration to send all WAN traffic through the appliance, regardless of the WAN link used. The below figure shows a simple multiple-WAN link deployment example.

The two local-side routers redirect traffic to the local appliance. The FE 0/0 ports for both routers are in the same broadcast domain as the appliance. The local appliance must use the default virtual inline configuration (Return to Ethernet Sender).

Figure 1. Virtual Inline Mode With Two WAN Routers
Virtual Inline Mode and High-Availability

Sep 10, 2017
Virtual Inline mode can be used in a high availability (HA) configuration. The below figure shows a simple HA deployment. In virtual inline mode, a pair of appliances acts as one virtual appliance. Router configuration is the same for an HA pair as with a single appliance, except that the Virtual IP address of the HA pair, not the IP address of an individual appliance, is used in the router configuration tables. In this example, the local appliances must use default virtual inline configuration (Return to Ethernet Sender).

Figure 1. High-availability Example
Monitoring and Troubleshooting

Dec 17, 2012

In virtual inline mode, unlike WCCP mode, the appliance provides no virtual inline-specific monitoring. To troubleshoot a virtual inline deployment, log into the appliance and use the Dashboard page to verify that traffic is flowing into and out of the appliance. Traffic forwarding failures are typically caused by errors in router configuration.

If the Monitoring: Usage or Monitoring: Connections pages show that traffic is being forwarded but no acceleration is taking place (assuming that an appliance is already installed on the other end of the WAN link), check to make sure that both incoming WAN traffic and outgoing WAN traffic are being forwarded to the appliance. If only one direction is forwarded, acceleration cannot take place.

To test health-checking, power down the appliance. The router should stop forwarding traffic after the health-checking algorithm times out.
Group Mode

May 09, 2013

In group mode, two or more appliances become a single virtual appliance. This mode is one solution to the problem of asymmetric routing, which is defined as any case in which some packets in a given connection pass through a given appliance but others do not. A limitation of the appliance architecture is that acceleration cannot take place unless all packets in a given connection pass through the same two appliances. Group mode overcomes this limitation.

Group mode can be used with multiple or redundant links without reconfiguring your routers.

Note: Group mode is not supported on the SD-WAN 4000 or 5000 appliances.

Group mode applies only to the appliances on one side of the WAN link; the local appliances neither know nor care whether the remote appliances are using group mode.

Group mode uses a heartbeat mechanism to verify that other members of the group are active. Packets are forwarded to active group members only.

Avoiding asymmetric routing is the main reason to use group mode, but group mode is not the only method available for that purpose. If you decide that it is the best method for your environment, you can enable it by setting a few parameters. If the default mechanism for determining which appliance is responsible for a particular connection does not provide optimal acceleration, you can change the forwarding rules.

Figure 1. Group Mode With Redundant Links

Figure 2. Group Mode With Non-Redundant Links with Possible Asymmetric Routing

Figure 3. Group Mode On Nearby Campuses
When to Use Group Mode

Jul 03, 2013

Use group mode in the following set of circumstances:

- You have multiple WAN links.
- There is a chance of asymmetric routing (a packet on a given connection might travel over either link).
- Group mode seems simpler and more practical than alternatives that use a single appliance.

The alternatives are:

- WCCP mode, in which traffic from two or more links is sent to the same appliance by WAN routers, by means of the WCCP protocol.
- Virtual inline mode, in which your routers send traffic from two or more links through the same appliance (or high-availability pair).
- Multiple bridges, where each link passes through a different accelerated bridge in the same appliance.
- LAN-level aggregation, which places an appliance (or high-availability pair) closer to the LAN, before the point where WAN traffic is split into two or more paths.
How Group Mode Works

Dec 06, 2012
In group mode, the appliances that are part of the group each take ownership for a portion of the group's connections. If a given appliance is the owner of a connection, it makes all the acceleration decisions about that connection and is responsible for compression, flow control, packet retransmission, and so on.

If an appliance receives a packet for a connection for which it is not the owner, it forwards the packet to the appliance that is the owner. The owner examines the packet, makes the appropriate acceleration decisions, and forwards any output packets back to the non-owning appliance. This process preserves the link selection made by the router, while allowing all packets in the connection to be managed by the owning appliance. For the routers, the introduction of the appliances has no consequences. The routers do not need to be reconfigured in any way, and the appliances do not need to understand the routing mechanism. They simply accept the routers' forwarding decisions.

Figure 1. Sending-side Traffic in Group Mode

Figure 2. Receiving-side traffic flow in group mode

Group mode has two, user-selectable failure modes, which control how the group members interact with each other if one of them fails. The failure mode also determines whether the failed appliance's bypass card opens (blocking traffic through the appliance) or remains closed (allowing traffic to pass through). The failure modes are:

**Continue to accelerate** - If a group member fails, its bypass card is opened and no traffic passes through the failed appliance. The result is presumably a fail-over if redundant links are used. Otherwise, the link is simply inaccessible. The other appliances in the group continue to accelerate. The usual hashing algorithm handles the changed conditions. (That is, the old hashing algorithm is used, and if the failed unit is indicated as the owner, a hashing algorithm based on the new, smaller group is applied. This preserves as many older connections as possible.)

**Do not accelerate** - If a group member fails, its bypass card closes, allowing traffic to pass through without acceleration. Because an unaccelerated path introduces asymmetric routing, the other members of the group also go into pass-through mode when they detect the failure.
Enabling Group Mode

May 09, 2013
To enable group mode, create a group of two or more appliances. An appliance can be a member of only one group. Group members are identified by IP address and the SSL common name in the appliance license.

All group mode parameters are on the Settings: Group Mode page, in the Configure Settings: Group Mode table.

Figure 1. Group Mode Page

To enable group mode

1. Select the address to use for group communication. At the top of the Group Mode Configuration table on the Configuration: Advanced Deployments: Group Mode tab, the table cell under Member VIP contains the management address of the port used to communicate with other group members. Use the (unlabeled) drop-down menu to select the correct address (for example, to use the Aux1 port, select the IP address you assigned to the Aux1 port). Then, click Change VIP.

2. Add at least one more group member to the list. (Groups of three or more are supported but are rarely used.) In the next cell of the Member VIP column, type the IP address of the port used by the other appliance for group-mode communication.

3. Type the other group member's SSL common name in the SSL Common Name column. The SSL common name is listed on the other appliance's Configure: Advanced Deployments: High Availability tab. If the other group member is a high-availability pair, the name listed is the SSL common name of the primary appliance.

   Note: If the local appliance is not part of a high-availability pair, the first cell in the HA Secondary SSL Common Name is blank.

   If the other group member is a high-availability pair, specify the SSL Common Name of the HA secondary appliance in the HA Secondary SSL Common Name column.

4. Click Add.

5. Repeat steps 2-4 for any additional appliances or high-availability pairs in the group.

6. The three buttons under the list of group members are toggles, so each is labeled as the opposite of its current setting:

   1. The top button reads either, Do not accelerate when member failure is detected or Continue to accelerate when member failure is detected. The “Do not accelerate…” setting always works and does not block traffic, but if any member fails, the other group members go into bypass mode, which causes a complete loss of acceleration. With the “Continue to accelerate” option, the failing appliance’s bridge becomes an open circuit, and the link fails. This option is appropriate if the WAN router responds by causing a failover. New connections, and open connections belonging to the surviving appliances, are accelerated.

   2. The bottom button should now be labeled Disable Group Mode. If it is not, enable group mode by clicking the button.

7. Refresh the screen. The top of the page should list the group mode partners, but display warnings about their status, because they haven’t been configured for group mode yet. For example, it might indicate that the partner cannot be found or is running a different software release.

8. Repeat this procedure with the other members of the group. Within 20 seconds after enabling the last member of the group, the Group Mode Status line should show NORMAL, and the other group mode members should be listed with Status: On-Line and Configuration: OK.
Forwarding Rules

Dec 27, 2012

By default, the owner of a group-mode connection is set by a hash of the source and destination IP addresses. Each appliance in the group uses the same algorithm to determine which group member owns a given connection. This method requires no configuration. The owner can optionally be specified through user-settable rules.

Because the group-mode hash is not identical to that used by load balancers, about half of the traffic tends to be forwarded to the owning appliance in a two-Appliance group. In the worst case, forwarding causes the load on the LAN-side interface to be doubled, which halves the appliance’s peak forwarding rate for actual WAN traffic.

This speed penalty can be reduced if the Primary or Aux1 Ethernet ports are used for traffic between group members. For example, if you have a group of two appliances, you can use an Ethernet cable to connect the two units’ Primary ports, then specify the Primary port on the Group Mode page on each unit. However, maximum performance is achieved if the amount of traffic forwarded between the group-mode members is minimized.

The owner can optionally be set according to specific IP/port-based rules. These rules must be identical on all appliances in the group. Each member of the group verifies that its group-mode configuration is identical to the others. If not all of the configurations are identical, none of the member appliances enter group mode.

If traffic arrives first at the appliance that owns the connection, it is accelerated and forwarded normally. If it arrives first at a different appliance in the group, it is forwarded to its owner over a GRE tunnel, which accelerates it and returns it to the original appliance for forwarding. Thus, group mode leaves the router’s link selection unchanged.

Using explicit IP-based forwarding rules can reduce the amount of group-mode forwarding. This is especially useful in primary-link/backup-link scenarios, where each link handles a particular range of IP addresses, but can act as a backup when the other link is down.

Figure 1. IP-Based Owner Selection

Forwarding rules can ensure that group members handle only their “natural” traffic. In many installations, where traffic is usually routed over its normal link and only rarely crosses the other one, these rules can reduce overhead substantially.

Rules are evaluated in order, from top to bottom, and the first matching rule is used. Rules are matched against an optional IP address/mask pair (which is compared against both source and destination addresses), and against an optional port range.

Regardless of the ordering of rules, if the partner appliance is not available, traffic is not forwarded to it, whether a rule matches or not.

For example, in the figure below, member 172.16.1.102 is the owner of all traffic to or from its own subnet (172.16.1.0/24), while member 172.16.0.184 is the owner of all other traffic.

If a packet arrives at unit 172.16.1.102, and it is not addressed to/from net 172.16.1.0/24, it is forwarded to 172.16.0.184.

If unit 172.16.0.184 fails, however, unit 172.16.1.102 no longer forwards packets. It attempts to handle the traffic itself. This behavior can be inhibited by clicking Do NOT Accelerate When Member Failure Detected on the Group Mode tab.
In a setup with a primary WAN link and a backup WAN link, write the forwarding rules to send all traffic to the appliance on the primary link. If the primary WAN link fails, but the primary appliance does not, the WAN router fails over and sends traffic over the secondary link. The appliance on the secondary link forwards traffic to the primary-link appliance, and acceleration continues undisturbed. This configuration maintains accelerated connections after the link failover.

Figure 2. Forwarding Rules
Monitoring and Troubleshooting Group Mode

Two things should be checked in a group-mode installation:

- That the two appliances have entered group mode, which can be determined on either appliance's Configuration: Advanced Deployments: Group Mode page.
- That the behavior of the group-mode pair is as desired when the other member fails, and when one of the links fail, as determined by disabling the other appliance and temporarily disconnecting one of the links, respectively.
High-Availability Mode

Dec 11, 2013
Two identical appliances on the same subnet can be combined as a high-availability pair. The appliances each monitor the other's status by using the standard Virtual Router Redundancy Protocol (VRRP) heartbeat mechanism. The pair has a common virtual IP address for management, in addition to each appliance's management IP address. If the primary appliance fails, the secondary appliance takes over. Failover takes approximately five seconds.

High availability mode is a standard feature.
How High-Availability Mode Works

Dec 06, 2012

In a high availability (HA) pair, one appliance is primary, and the other is secondary. The primary monitors its own and the secondary's status. If it detects a problem, traffic processing fails over to the secondary appliance. Existing TCP connections are terminated. To ensure successful failover, the two appliances keep their configurations synchronized. In a WCCP mode high availability configuration, the appliance that is processing traffic maintains communication with the upstream router.

Status monitoring—When high availability is enabled, the primary appliance uses the VRRP protocol to send a heartbeat signal to the secondary appliance once per second. In addition, the primary appliance monitors the carrier status of its Ethernet ports. The loss of carrier on a previously active port implies a loss of connectivity.

Failover If the heartbeat signal of the primary appliance should fail, or if the primary appliance loses carrier for five seconds on any previously active Ethernet port, the secondary appliance takes over, becoming the primary. When the failed appliance restarts, it becomes the secondary. The new primary announces itself on the network with an ARP broadcast. MAC spoofing is not used. Ethernet bridging is disabled on the secondary appliance, leaving the primary appliance as the only path for inline traffic. Fail-to-wire is inhibited on both appliances to prevent loops.

Warning
The Ethernet bypass function is disabled in HA mode. If both appliances in an inline HA pair lose power, connectivity is lost. If WAN connectivity is needed during power outages, at least one appliance must be attached to a backup power source.

Note
The secondary appliance in the HA pair has one of its bridge ports, port apA.1, disabled to prevent forwarding loops. If the appliance has dual bridges, apB.1 is also disabled. In a one-arm installation, use port apA.2. Otherwise, the secondary appliance becomes inaccessible when HA is enabled.

Primary/secondary assignment—If both appliances are restarted, the first one to fully initialize itself becomes the primary. That is, the appliances have no assigned roles, and the first one to become available takes over as the primary. The appliance with the highest IP address on the interface used for the VRRP heartbeat is used as a tie-breaker if both become available at the same time.

Connection termination during failover—Both accelerated and unaccelerated TCP connections are terminated as a side effect of failover. Non-TCP sessions are not affected, except for the delay caused by the brief period (several seconds) between the failure of the primary appliance and the failover to the secondary appliance. Users experience the closing of open connections, but they can open new connections.

Configuration synchronization—The two appliances synchronize their settings to ensure that the secondary is ready to take over for the primary. If the configuration of the pair is changed through the browser based interface, the primary appliance updates the secondary appliance immediately.
HA cannot be enabled unless both appliances are running the same software release.

**HA in WCCP mode**—When WCCP is used with an HA pair, the primary appliance establishes communication with the router. The appliance uses its management IP address on apA or apB, not its virtual IP address, to communicate with the router. Upon failover, the new primary appliance establishes WCCP communication with the router.
Cabling Requirements

The two appliances in the high availability pair are installed onto the same subnet in either a parallel arrangement or a one-arm arrangement, both of which are shown in the following figure. In a one-arm arrangement, use the apA.2 port (and, optionally, the apB.2 port), not the apA.1 port. Some models require a separate management LAN, whether deployed in inline or one-armed mode. This is depicted only in the middle diagram.

Figure 1. Cabling for High-Availability Pairs

Do not break the above topology with more switches. Random switch arrangements are not supported. Each of the switches must be either a single, monolithic switch, a single logical switch, or part of the same chassis.

If the spanning-tree protocol (STP) is enabled on the router or switch ports attached to the appliances, failover works, but the failover time may increase to roughly 30 seconds. Without STP, failover time is roughly five seconds. Thus, to achieve the briefest possible failover interval, disable STP on the ports connecting to the appliances.
Figure 2: Ethernet Port Locations (Older Models)

Rear of Appliance, Branch Repeater

Primary Aux1

Rear of Appliance, Repeater 8500 Series

Primary Aux1

Rear of Appliance, Repeater 8800 Series

Primary Aux1

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.597
Other Requirements

Dec 06, 2012

Both appliances in an HA pair must meet the following criteria:

- Have identical hardware, as shown by on the System Hardware entry on the Dashboard page.
- Run exactly the same software release.
- Be equipped with Ethernet bypass cards. To determine what is installed in your appliances, see the Dashboard page.

Appliances that do not support HA display a warning on the Configuration: High Availability page.
Management Access to the High-Availability Pair

Jan 03, 2013

When configuring a high-availability (HA) pair, you assign the pair a virtual IP (VIP) address, which enables you to manage the two appliances as if they were a single unit. After you enable high-availability mode, managing the secondary appliance through its IP address is mostly disabled, with most parameters grayed out. A warning message displays the reason on every page. Use the HA VIP for all management tasks. You can, however, disable the secondary appliance's HA state from its management UI.
You can configure two newly installed appliances as a high-availability pair, or you can create an HA pair by adding a second appliance to an existing installation.

**Prerequisites:** Physical installation and basic configuration procedures

**To configure high availability**

1. Make sure that no more than one appliance is connected to the traffic networks (on the accelerated bridges). If both are connected, disconnect one bridge cable from the active bridges on the second appliance. This will prevent forwarding loops.

2. On the Features page of the first appliance, disable Traffic Processing. This disables acceleration until the HA pair is configured.

3. Repeat for the second appliance.

4. On the first appliance, go to the Configuration: Advanced Deployments: High Availability tab, show below.

5. Select the Enabled Check box.

6. Click the Configure HA Virtual IP Address link and assign a virtual IP address to the apA interface. This address will be used later to control both appliances as a unit.

7. Return to the High Availability page and, in the VRRP VRID field, assign a VRRP ID to the pair. Although the value defaults to zero, the valid range of VRRP ID numbers is 1 through 255. Within this range, you can specify any value that does not belong to another VRRP device on your network.

8. In the Partner SSL Common Name field, type the other appliance’s SSL Common Name, which is displayed on that appliance’s Configuration: Advanced Deployments: High Availability tab, in the Partner SSL Common Name field. The SSL credentials used here are factory-installed.

9. Click Update.

10. Repeat steps 3-8 on the second appliance. If you are managing the appliance via an accelerated bridge (such as apA), you may have to reconnect the Ethernet cable that you removed in step 1 to connect to the second appliance. If so, plug this cable in and disconnect the corresponding cable on the first appliance.

11. With your browser, navigate to the virtual IP address of the HA pair. Enable Traffic Processing on the Features page. Any further configuration will be performed from this virtual address.

12. Plug in the cable that was left disconnected.

13. On each appliance, the Configuration: Advanced Deployments: High Availability page should now show that high availability is active and that one appliance is the primary and the other is the secondary. If this is not the case, a warning banner appears at the top of the screen, indicating the nature of the problem.

![High-availability configuration page](https://docs.citrix.com)
Updating Software on a High-Availability Pair

Dec 06, 2012

Updating the SD-WAN software on an HA pair causes a failover at one point during the update.

Note: Clicking the Update button terminates all open TCP connections.

To update the software on an HA pair

1. Log on to both appliances.
2. On the secondary appliance, update the software and reboot. After the reboot, the appliance is still the secondary. Verify that the installation succeeded. The primary appliance should show that the secondary appliance exists but that automatic parameter synchronization is not working, due to a version mismatch.
3. On the primary appliance, update the software, and then reboot. The reboot causes a failover, and the secondary appliance becomes the primary. When the reboot is completed, HA should become fully established, because both appliances are running the same software.
Saving/Restoring Parameters of an HA Pair

Dec 06, 2012

The System Maintenance: Backup/Restore function can be used to save and restore parameters of an HA pair as follows:

**To back up the parameters**

Use the backup feature as usual. That is, log on to the GUI through the HA VIP address (as is normal when managing the HA pair) and, on the System Management: Backup/Restore page, click Download Settings.

**To restore the parameters**

1. Disable HA on both appliances by clearing the **Enabled** check box on the Configuration: Advanced Deployments: High Availability (HA) tab.
2. Unplug a network cable from the bridge of one appliance. (Call it “Appliance A.”)
3. Unplug the power cord from Appliance A.
4. Restore the parameters on the other appliance (Appliance B), by uploading a previously saved set of parameters on the System Maintenance: Backup/Restore page and clicking Restore Settings. (Completing this operation requires a restart, which reenables HA.)
5. Wait for Appliance B to restart. It becomes the primary.
6. Restart Appliance A.
7. Log on to Appliance A’s GUI and reenable HA on the Configuration: Advanced Deployments: High Availability (HA) tab. The appliance get its parameters from the primary.

Both appliances are now restored and synchronized.
Troubleshooting High Availability Pairs

Dec 26, 2012

If the appliances report any failure to enter high-availability mode, the error message will also note the cause. Some issues that can interfere with high-availability mode are:

- The other appliance is not running.
- The HA parameters on the two appliances are not identical.
- The two appliances are not running the same software release.
- The two appliances do not have the same model number.
- Incorrect or incomplete cabling between the appliances does not allow the HA heartbeat to pass between them.
- The HA/Group Mode SSL Certificates on one or both appliances are damaged or missing.
NetScaler SD-WAN 1000 and 2000 WANOP Appliances with Windows Server

Nov 30, 2016

SD-WAN supports Windows Server on two hardware platforms – 1000WS and 2000WS. Whereas 2000WS has better performance capacity as compared to the 1000WS, the latter has more RAM and hard disk space.


The SD-WAN 1000 and 2000 WANOP appliances with Windows Servers are based on the Citrix branch architecture, which supports multiple virtual machines. All branch appliances contain a SD-WAN instance, a management service instance, and a Xen hypervisor. In addition, the SD-WAN 1000 and 2000 appliances with Windows Server include a Windows Server instance, which runs independently of the SD-WAN WANOP instance.

As shown in the below figure, the Windows Server and the WANOP instance are partly isolated from one another, because the accelerated bridges are accessible only to the accelerator. This allows the accelerator and the Windows Server to be placed at different points in your LAN topology.

Figure 1. Architecture of the SD-WAN WANOP 1000 and 2000 Appliances with Windows Server

The SD-WAN WANOP instance is typically used in inline mode, with the SD-WAN instance interposed between the WAN
router and the LAN, so WAN traffic flows through the accelerated bridge. The SD-WAN WANOP instance can also be deployed in WCCP or virtual inline modes, using a single accelerated bridge port.

The Windows server is deployed in a one-armed configuration in the same local LAN in which you would deploy any other server.

In addition to the accelerated bridges and the Windows LAN port, a management port connects to all virtual machines (instances) and the hypervisor.

The appliance has two modes, two-port mode and four-port mode, which determine how ports 1/3 and 1/4 are used.

The Citrix Compliance Regulatory Models are:

- SD-WAN 1000WS WANOP: CB 504-2
- SD-WAN 2000WS WANOP: NS 6xCu
SD-WAN 1000 Appliance with Windows Server

Apr 07, 2017

The Citrix SD-WAN 1000 with Windows Server platform has a quad-core processor and 32 GB of memory. This platform has a bandwidth of up to 20 Mbps.

The following figure shows the front panel of a SD-WAN 1000 appliance with Windows Server.

Figure 1. Citrix SD-WAN 1000 with Windows Server, front panel

The front panel of the SD-WAN 1000 with Windows Server appliance has a power button and five LEDs.

The power button is used to switch the appliance on or off.

The reset button restarts the appliance.

The LEDs provide critical information related to different parts of the appliance.

- **Power Fail** – Indicates the power supply unit has failed.
- **Information LED** – Indicates the following:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuously ON and red</td>
<td>The appliance is overheated.</td>
</tr>
<tr>
<td></td>
<td>(This might be a result of cable congestion.)</td>
</tr>
<tr>
<td>Blinking red (1Hz)</td>
<td>Fan failure, check for an inoperative fan.</td>
</tr>
<tr>
<td>Blinking red (0.25Hz)</td>
<td>Power failure, check for the non-operational power supply.</td>
</tr>
<tr>
<td>Solid blue</td>
<td>Local UID has been activated. Use this function to locate the server in a rack mount environment.</td>
</tr>
<tr>
<td>Blinking blue (300 m/s)</td>
<td>Remote UID is on. Use this function to identify the server from a remote location.</td>
</tr>
</tbody>
</table>

- **NIC1 and NIC2** – Indicate network activity on the LAN1 and WAN1 ports.
- **HDD** – Indicates the status of the hard disk drive.
- **Power** – Indicates that the power supply units are receiving power and operating normally.
The following figure shows the back panel of a SD-WAN 1000 appliance with Windows Server.

Figure 2. Citrix SD-WAN 1000 appliance with Windows Server, back panel

The following components are visible on the back panel of a SD-WAN 1000 appliance with Windows Server:

- Cooling fan
- Single power supply, rated at 200 watts, 110-240 volts
- Accelerated pairs of Ethernet ports (apA and apB) which function as accelerated bridges
- RS-232 serial console port
- One AUX Ethernet port and one management port
- Two USB ports
SD-WAN 2000 Appliance with Windows Server

The Citrix NetScaler SD-WAN 2000 with Windows Server platform is a 1U appliance with one quad-core processor and 24 gigabytes (GB) of memory.

The following figure shows the front panel of the NetScaler SD-WAN 2000 appliance with Windows Server.

Figure 1. Citrix NetScaler SD-WAN 2000 appliance with Windows Server, front panel

Note: You cannot assign apA ports to Windows Server. However, you can assign AUX port to Windows Server.

SD-WAN 2000 appliance with Windows Server has the following ports:
- An RS232 serial console port.
- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.
- A copper Ethernet (RJ45) management port, numbered 0/1, and named PRI (primary). The management port is used to connect directly to the appliance for system administration functions. You can use this port for initial provisioning of WAN optimization and Windows Server.
  Note: The LOM port also operates as a management port.
- Four 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right. The four ports form two accelerated pairs, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA), and 1/3 and 1/4 are accelerated pair B (apB).

The following figure shows the back panel of the NetScaler SD-WAN 2000 appliance with Windows Server.

Figure 2. Citrix NetScaler SD-WAN 2000 appliance with Windows Server, back panel

The following components are visible on the back panel of the NetScaler SD-WAN 2000 appliance with Windows Server:
- 600 GB removable solid-state drive, which stores the appliance's software and user data, and 1 TB hard disk drive.
- Power switch, which switches power to the appliance on or off. Press the switch for five seconds to switch off the
power.

- USB port (reserved for a future release).
- Non-maskable interrupt (NMI) button, for use at the request of Technical Support to produce a core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Single power supply, rated at 300 watts, 100-240 volts.
# Ethernet Port Names

When configuring the appliance, you have to specify IP addresses for various Ethernet ports of the appliance. The Ethernet ports are named differently on the front panel of NetScaler SD-WAN 1000 and 2000 appliances with Windows Server, in the NetScaler SD-WAN instance, and in the Windows Server, as shown in the following table:

<table>
<thead>
<tr>
<th>Front Panel</th>
<th>SD-WAN 1000WS</th>
<th>SD-WAN 2000WS</th>
<th>SD-WAN Instance</th>
<th>Windows Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGMT (Blue)</td>
<td>0/1 (LOM/PRI)</td>
<td>Primary</td>
<td>Citrix PV Ethernet Adapter #0: 0/1</td>
<td></td>
</tr>
<tr>
<td>AUX</td>
<td>0/2 (AUX)</td>
<td>Aux</td>
<td>Citrix PV Ethernet Adapter #1: 0/2</td>
<td></td>
</tr>
<tr>
<td>apA LAN1/WCCP (Green)</td>
<td>1/1</td>
<td>apA.1</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>apA WAN1</td>
<td>1/2</td>
<td>apA.2</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>apB LAN2</td>
<td>1/3</td>
<td>apB.1*</td>
<td>Double-click the Desktop icon nic_mapping.vbs to display the mapping**</td>
<td></td>
</tr>
<tr>
<td>apB WAN2</td>
<td>1/4</td>
<td>apB.2*</td>
<td>Double-click the Desktop icon nic_mapping.vbs to display the mapping**</td>
<td></td>
</tr>
</tbody>
</table>

* Available to the SD-WAN instance only in four-port mode.

** Available to the Windows Server only in two-port mode.
Supported Features

The following table lists various features supported on SD-WAN 1000 and 2000 appliances with Windows Server.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Citrix NetScaler SD-WAN 1000 with Windows Server series</th>
<th>Citrix NetScaler SD-WAN 2000 with Windows Server series</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoConfiguration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>SD-WAN Plug-In</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Compression</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RPC over HTTPS</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>SSL Compression</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>TCP Acceleration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Traffic Shaping</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Video Caching</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Windows File System Acceleration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Windows Outlook Acceleration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>XenApp/ XenDesktop Acceleration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Group Mode</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>High Availability Mode</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Inline Mode</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Virtual Inline Mode</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>WCCP Mode</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>VLANs</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
Summary of Hardware Specifications

Jun 12, 2014

The following tables summarize the specifications of the SD-WAN 1000 and 2000 with Windows Server hardware platforms.

<table>
<thead>
<tr>
<th>H/W Specification</th>
<th>SD-WAN 1000 with Windows Server</th>
<th>SD-WAN 2000 with Windows Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows Server version</strong></td>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td><strong>Platform Performance</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Up to 20 Mbps</td>
<td>Up to 50 Mbps</td>
</tr>
<tr>
<td>Maximum HDX sessions</td>
<td>Up to 100</td>
<td>300</td>
</tr>
<tr>
<td>Total sessions</td>
<td>10,000</td>
<td>20,000</td>
</tr>
<tr>
<td>Acceleration Plug-in CCUs</td>
<td>N/A</td>
<td>750</td>
</tr>
<tr>
<td><strong>Hardware Specifications</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td>4 Cores</td>
<td>4 Cores</td>
</tr>
<tr>
<td>Total disk space</td>
<td>1x300 GB SSD and 1x1 TB HDD</td>
<td>1 x 600 GB SSD and 1X1 TB HDD</td>
</tr>
<tr>
<td>SSD (dedicated Compression history)</td>
<td>123 GB for Disk-Based Compression (DBC)</td>
<td>225 GB for Disk-Based Compression (DBC)</td>
</tr>
<tr>
<td></td>
<td>25 GB for video caching</td>
<td>50 GB for video caching</td>
</tr>
<tr>
<td>RAM</td>
<td>32 GB</td>
<td>24 GB</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>2 pair with bypass 10/100/1000</td>
<td>4 x 10/100/1000 Base-T copper Ethernet</td>
</tr>
<tr>
<td></td>
<td>2 GigE ports for Management and AUX ports</td>
<td>2 GigE ports for Management and AUX ports</td>
</tr>
<tr>
<td>Power supplies</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Physical Dimensions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rack Units</td>
<td>1U</td>
<td>1U</td>
</tr>
<tr>
<td>System width</td>
<td>EIA 310-D for 19-inch racks</td>
<td>EIA 310-D for 19-inch racks</td>
</tr>
<tr>
<td>System depth</td>
<td>10&quot; (25.4 cm)</td>
<td>25.4&quot; (64.5 cm)</td>
</tr>
<tr>
<td>System weight</td>
<td>8.5 lbs (3.9 kg)</td>
<td>32 lbs (14.5 kg)</td>
</tr>
<tr>
<td>H/W Specification</td>
<td>SD-WAN 1000 with Windows Server</td>
<td>SD-WAN 2000 with Windows Server</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Shipping dimensions and weight</td>
<td>26 L x 18.5 W x 6.5&quot; H 14.5 lbs</td>
<td>32 L x 23.5 W x 7.5&quot; H 39 lbs</td>
</tr>
</tbody>
</table>

**Environmental and Regulatory**

<table>
<thead>
<tr>
<th>Voltage</th>
<th>100/240 VAC, 50-60 Hz</th>
<th>100/240 VAC, 50-60 Hz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power consumption (Max.)</td>
<td>200 W</td>
<td>300 W</td>
</tr>
<tr>
<td>Operating Temperature (degree Celsius)</td>
<td>10–35</td>
<td>0–40</td>
</tr>
<tr>
<td>Non-operating Temperature (degree Celsius)</td>
<td>-40 – +70</td>
<td>-40 – +70</td>
</tr>
<tr>
<td>Allowed Relative Humidity</td>
<td>8% – 90% non-condensing</td>
<td>5%–95%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Safety certifications</th>
<th>CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)</th>
<th>CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electromagnetic and susceptibility certifications</td>
<td>FCC (Part 15 Class A), CCC, KCC, NOM, SASO, CITC, EAC, DoC, CE, VCCI, RCM</td>
<td>FCC (Part 15 Class A), CCC, KCC, NOM, SASO, CITC, EAC, DoC, CE, VCCI, RCM</td>
</tr>
</tbody>
</table>

| Environmental certifications | RoHS, WEEE | RoHS, WEEE |
Installing the Appliance

Jun 12, 2014

After you have determined that the location where you will install your appliance meets the environmental standards and the server rack is in place according to the instructions, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you will use for initial configuration. You can also connect the appliance to a computer through Ethernet port for initial configuration. On SD-WAN 1000 appliance with Windows Server, this port is labeled as MGMT (management) port and on SD-WAN 2000 appliance with Windows Server, the port is labeled as PRI (primary) port. To complete the installation, you switch on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.
A SD-WAN 1000 or 2000 appliance with Windows Server requires one rack unit. Both are rack-mount devices that can be installed into two-post relay racks or four-post EIA-310 server racks. Verify that the rack is compatible with your appliance.
Rack Mounting an SD-WAN 1000 Appliance with Windows Server

Apr 09, 2014

SD-WAN 1000 appliance with Windows Server is not shipped with rails. You can mount the appliance to the rack by using the front mounting ports.
Rack Mounting an SD-WAN 2000 Appliance with Windows Server

Apr 09, 2014
A SD-WAN 2000 appliance with Windows Server requires one rack unit. Both are rack-mount devices that can be installed into two-post relay racks or four-post EIA-310 server racks. Verify that the rack is compatible with your appliance.

To mount a SD-WAN appliance, you must first install the rails and then install the appliance in the rack, as follows:

- Remove the inner rails from the rail assembly.
- Attach the inner rails to the appliance.
- Install the rack rails on the rack.
- Install the appliance in the rack.

To remove the inner rails from the rail assembly
1. Place the rail assembly on a flat surface.
2. Slide out the inner rail toward the front of the assembly.
3. Depress the locking tabs until the inner rail comes all the way out of the rail assembly.
4. Repeat steps 1 through 3 to remove the second inner rail.

To attach the inner rails to the appliance
1. Position the right inner rail behind the ear bracket on the right side of the appliance.
2. Align the holes on the rail with the corresponding holes on the side of the appliance.
3. Attach the rail to the appliance with the provided screws.
4. Repeat steps 1 through 3 to install the left inner rail on the left side of the appliance.

To install the rack rails
1. Position the rack rails at the desired location in the rack, keeping the sliding rail guide facing inward.
2. Snap the rails to the rack.
   Note: Make sure that both rack rails are at same height and that the rail guides are facing inward.

To install the appliance in the rack
1. Align the inner rails, attached to the appliance, with the rack rails.
2. Slide the appliance into the rack rails, keeping the pressure even on both sides, and push the appliance into the rack rails until it locks into place.
3. Verify that the appliance is locked in place by pulling it all the way out from the rack.
   Note: The illustration in the following figure might not represent your actual appliance.

Figure 1. Rack Mounting the Appliance
Connecting the Cables

Jun 12, 2014

When the appliance is securely mounted on the rack, determine which ports you should use. You are then ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

Warning: Before installing or repairing the appliance, remove all jewelry and other metal objects that might come in contact with power sources or wires. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.

Ports

A typical installation using a single accelerated bridge uses four Ethernet ports (the Primary port and apA) and six IP addresses (four on the Primary port's subnet and two on apA's subnet). The appliance has two motherboard ports and two accelerated bridges.

- The motherboard ports are labeled as MGMT (management) and AUX1 (auxiliary) ports in SD-WAN1000 appliance with Windows Server and PRI (primary) and AUX (auxiliary) in SD-WAN 2000 appliance with Windows Server. You use MGMT port of the SD-WAN 1000 appliance with Windows Server and PRI port of the SD-WAN 2000 appliance with Windows Server for initial configuration.
- Accelerated bridge ports are apA and apB are available on the back panel of SD-WAN 1000 appliance with Windows Server and the front panel of SD-WAN 2000 appliance with Windows Server. On SD-WAN 1000WS appliance with Windows Server, these ports are labeled as LAN1 and WAN1, and LAN2 and WAN2, respectively. However, on SD-WAN 2000WS appliance with Windows Server, these ports are labeled as 1/1 and 1/2, and 1/3 and 1/4, respectively.

Connecting the Ethernet Cables

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on a 10/100/1000BASE-T port.

To connect an Ethernet cable to a 10/100/1000BASE-T port

1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port.
   - On SD-WAN 1000 appliance with Windows Server, the ports are available on the back panel and labeled as LAN1 and WAN1 for apA bridged port for LAN and WAN links, respectively.
   - On SD-WAN 2000 appliance with Windows Server, the ports are available on the front panel. The ports on SD-WAN 2000 with Windows are labeled as 1/1 and 1/2 for the apA bridged port. You can use 1/1 for LAN and 1/2 for WAN link.

2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.
3. Verify that the LED glows amber when the connection is established.

Connecting the Console Cable

You can use the console cable to connect your appliance to a computer or terminal, from which you can configure the appliance. Before connecting the console cable, configure the computer or terminal to support VT100 terminal emulation, 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE. Then connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

To connect the console cable to a computer or terminal

1. Insert the DB-9 connector at the end of the cable into the console port.
   - On SD-WAN 1000 appliance with Windows Server, the port is located on the back panel.
On SD-WAN 2000 appliance with Windows Server, the port is located on the front panel.

Note: To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.

2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.

**Connecting the Power Cable**

A SD-WAN appliance has one power supply. A separate ground cable is not required, because the three-prong plug provides grounding. Provide power to the appliance by installing the power cord. Connect the other end of the power cable to a standard 110V/220V power outlet.
Switching on the Appliance

Jun 12, 2014

After you have installed the appliance in a rack and connected the cables, verify that the power cable is properly connected. After verifying the connections, you are ready to switch on the appliance.

To switch on the appliance

1. Verify that the appliance is connected through a console or Ethernet port, so that you can configure the appliance after it is switched on.
2. Press the ON/OFF toggle power switch on the appliance.
3. On SD-WAN 2000 appliance for Windows Server, verify that the LCD on the front panel is backlit and the start message appears.

Caution: Be aware of the location of the emergency power off (EPO) switch, so that if an electrical accident occurs, you can quickly remove power from the appliance.
Initial Configuration

Aug 12, 2014

After checking the connections, you are ready to deploy the SD-WAN 1000 and 2000 appliances with Windows Server on the network.

The appliance shipped from Citrix has default IP addresses configured on it. To deploy the appliance on the network, you must configure the appropriate IP addresses on the appliance to accelerate the network traffic.

To perform initial configuration:
- Identify the prerequisites for the initial configuration.
- Record various values required in the initial configuration procedure.
- Configure the appliance by connecting it to the Ethernet port.
- Perform additional configuration for Windows.
- Assign management IP address through the serial console.
- Troubleshoot initial configuration issues.

By default, the initial configuration deploys the appliance in inline mode.
Prerequisites

Aug 12, 2014

Before you begin configuring the appliance, make sure that the following prerequisites have been met:

- You should have physical access to the appliance.
- You have chosen four IP addresses for management of the SD-WAN appliance.
- In the Worksheet, record all IP addresses and other values you would use to configure the appliance. Preferably, print out the worksheet before you start the configuration process.
- You should already have a SD-WAN license key from Citrix, sent in an email. If you are using remote licensing, you need the IP address of the licensing server.
- WAN Send and Receive Speeds.
## SD-WAN WANOP 1000 or 2000 Appliance with Windows Server Deployment Worksheet

### Network Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Value for your Appliance</th>
<th>Description of the Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>XenServer IP Address (Management Subnet)</td>
<td>192.168.100.2</td>
<td>Management IP address of the XenServer.</td>
<td></td>
</tr>
<tr>
<td>Management Service IP Address (Management Subnet)</td>
<td>192.168.100.1</td>
<td>Management IP address of the Management Service.</td>
<td></td>
</tr>
<tr>
<td>Netmask (Management Subnet)</td>
<td>255.255.0.0</td>
<td>Network mask for the management subnet.</td>
<td></td>
</tr>
<tr>
<td>Gateway (Management Subnet)</td>
<td>None</td>
<td>The default gateway IP address of the appliance.</td>
<td></td>
</tr>
<tr>
<td>Port Model</td>
<td>2-Port</td>
<td>Select 2-port or 4-port, depending on the model. In 4-port mode, Windows Server does not have access to ports 1/3 and 1/4.</td>
<td></td>
</tr>
<tr>
<td>DNS Server</td>
<td>None</td>
<td>IP address of the DNS server. Citrix recommends that you specify a valid DNS server IP address. This is a mandatory parameter.</td>
<td></td>
</tr>
</tbody>
</table>

### SD-WAN Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Value for your SD-WAN instance.</th>
<th>Description of the Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address (Management Subnet)</td>
<td>192.168.100.20</td>
<td>Primary SD-WAN IP address at which you manage the SD-WAN instance.</td>
<td></td>
</tr>
<tr>
<td>Netmask (Management Subnet)</td>
<td>255.255.0.0</td>
<td>Network mask for the management IP address of the appliance. Same as previous netmask.</td>
<td></td>
</tr>
<tr>
<td>Gateway (Management Subnet)</td>
<td>None</td>
<td>The default gateway IP address of the appliance. Same as the previous gateway.</td>
<td></td>
</tr>
</tbody>
</table>

### Windows Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Value for your Windows Virtual Machine.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.100.40</td>
<td>IP address to manage Windows Virtual Machine.</td>
</tr>
</tbody>
</table>
### SD-WAN WANOP 1000 or 2000 Appliance with Windows Server Deployment Worksheet

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Netmask (Management Subnet)</strong></td>
<td>255.255.0.0</td>
<td>Network mask for the management IP address of the appliance. Same as the previous netmask.</td>
</tr>
<tr>
<td><strong>Gateway (Management Subnet)</strong></td>
<td>None</td>
<td>The default gateway IP address of the appliance. Same as the previous gateway.</td>
</tr>
<tr>
<td><strong>System Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NTP Server</strong></td>
<td>(none)</td>
<td>IP address of the NTP server. Citrix recommends that you specify a valid NTP server IP address. You can either enter the IP address or the server name.</td>
</tr>
<tr>
<td><strong>Time Zone</strong></td>
<td>UTC</td>
<td>Specify the time zone for your location.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>nsroot</td>
<td>New password for access to the appliance.</td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
<td>nsroot</td>
<td>New password for access to the appliance.</td>
</tr>
<tr>
<td><strong>Command Center Configuration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Command Center IP Address</strong></td>
<td>None</td>
<td>Optional. IP address of the Command Center appliance with which you want to register this appliance. More info.</td>
</tr>
<tr>
<td><strong>Command Center Port</strong></td>
<td>8443</td>
<td>Optional. Port number of the Command Center appliance.</td>
</tr>
<tr>
<td><strong>Registration Password</strong></td>
<td>None</td>
<td>Password you want to use to register the SD-WAN appliance.</td>
</tr>
<tr>
<td><strong>Licensing</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>License Server Address</strong></td>
<td>None</td>
<td>IP address of the licensing server. Required only when you select a remote model license type.</td>
</tr>
<tr>
<td><strong>Licensing Service Port</strong></td>
<td>27000</td>
<td>Port number of the licensing server. Required only when you select a remote model license type.</td>
</tr>
<tr>
<td><strong>Links</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Receive (Download) Speed</strong></td>
<td>None</td>
<td>WAN link download speed.</td>
</tr>
<tr>
<td><strong>Send (Upload) Speed</strong></td>
<td>None</td>
<td>WAN link upload speed.</td>
</tr>
</tbody>
</table>
Configuring the Appliance by Connecting a Computer to the Ethernet Port

Aug 12, 2014

For initial configuration of a SD-WAN appliance, perform the following tasks:
- Configure the appliance for use on your site.
- Install the Citrix license.
- Enable acceleration.
- Enable traffic shaping (inline mode only).

With inline deployments, this configuration might be all you need, because most acceleration features are enabled by default and require no additional configuration.

You can configure the appliance connecting the appliance to your computer through either the Ethernet port or the serial console. The following procedure enables you to configure the appliance by connecting it to your computer through the Ethernet port.

Note: On a SD-WAN 1000 appliance with Windows Server, you use the Ethernet port labeled as MGMT. However, on SD-WAN 2000 appliance with Windows Server, you use the Ethernet port labeled as PRI or LOM.

If you want to configure the appliance by connecting it to the computer through the serial console, assign the management service IP address from your Worksheet by completing the Assigning a Management IP Address through the Serial Console procedure, and then run steps 4 through 25 of the following procedure.

Note: Make sure that you have physical access to the appliance.

To configure the appliance by connecting a computer to the SD-WAN appliance’s Ethernet port 0/1

1. Set the Ethernet port address of a computer (or other browser-equipped device with an Ethernet port), to 192.168.100.50, with a network mask of 255.255.0.0. On a Windows device, this is done by changing the Internet Protocol Version 4 properties of the LAN connection, as shown below. You can leave the gateway and DNS server fields as blank.

2. Using an Ethernet cable, connect this computer to the port labeled MGMT on a SD-WAN WANOP 1000 appliance with Windows Server, or to the port labeled PRI on a SD-WAN WANOP 2000 appliance with Windows Server.

3. Switch on the appliance. Using the web browser on the computer, access the appliance by using the default management service IP address http://192.168.100.1.

4. On the login page, use the following default credentials to log on to the appliance:
   - Username: nsroot
   - Password: nsroot.

5. Start the configuration wizard by clicking Get Started.

6. On the Platform Configuration page, enter the respective values from your worksheet, as shown in the following example:

   - Note: If, for SD-WAN configuration, you want to use the same network mask and gateway as those for Network Configuration, select the Use System Netmask and Gateway option.

7. Click Done. A screen showing the Installation in Progress… message appears. This process takes approximately 2 to 5
minutes, depending on your network speed.

Note: If you are configuring the appliance by connecting it to your computer through the serial console port, skip step 8 through step 14.

8. A Redirecting to new management IP message appears.

9. Click OK.

10. Unplug your computer from the Ethernet port and connect the port to your management network.

11. Reset the IP address of your computer to its previous setting.

12. From a computer on the management network, log on to the appliance by entering the new Management Service IP address, such as https://<Management_IP_Address>, in a web browser.

13. To continue the configuration, accept the certificate and continue. The option to continue varies according to the web browser you are using.

14. Log on to the appliance by using the nsroot user name and the password from your worksheet.

15. The Configuration wizard starts again. In this wizard, some of the values which you have already provided, appear by default. Specify rest of the values you have recorded in your worksheet.

16. If you want to manage the appliance through Command Center, specify the Command Center IP address, port, and registration password in the Command Center Configuration page. Otherwise, skip this step.

17. In System Services section, update the values if necessary.

18. In the Licensing section, select the appropriate license type. You can either select a local license or a remote license server to apply a license to the appliance.

1. If you opt for a local license, you must generate a license by using the host ID of the appliance. To generate a local license for the appliance, see http://support.citrix.com/article/ctx131110. To apply the license, you can navigate to the SD-WAN > Configuration > Appliance Settings > Licensing page, after completing the Configuration wizard.

2. If you opt for a remote licensing server, you must select a remote appliance model and provide the IP address of the licensing server in the Licensing Server Address field.

19. In the WAN Link Definition section, specify receive and send speeds for the WAN link in the respective fields. Citrix recommends values 10% lower than the WAN bandwidth, to avoid network congestion.

20. By default, WAN-side adapter settings are configured on the appliance. Accept the default settings.

21. Click Install. After the Installation process is complete, the appliance restarts.

22. As soon as the appliance restarts, the Dashboard page appears.

23. To configure the appliance to accelerate the network traffic, open navigate to the Configuration tab.

Note: Make sure that you have already applied the appropriate license to the appliance.

24. On the Network Adapters page of the Appliance Settings node, verify and, if necessary, assign IP addresses, subnet masks, and gateways to the accelerated bridges (apA and apB) to be used. Applying these changes restarts the appliance.

Note: You need to assign IP addresses to apA and apB adapters only if you intended to configure WCCP mode, virtual inline mode, or the Video Caching feature on the appliance.

25. The Initial Configuration is complete. Traffic now flows through the appliance. The Dashboard page shows this traffic.

26. You need additional configuration on the appliance if you intend to use some of the modes and features, such as WCCP mode, virtual inline mode, video caching, secure peering, high availability, encrypted CIFS/MAPI acceleration, AppFlow monitoring, or SNMP monitoring.

Note:

- Inline installations place the appliance between your LAN and WAN routers, using both ports of the accelerated bridge,
such as ports LAN1 and WAN1 on a SD-WAN 1000 appliance with Window Server or ports 1/1 and 1/2 on SD-WAN 2000 appliance with Windows Server, for the apA accelerated bridge port.

- WCCP and virtual inline installations connect a single accelerated bridge port to your WAN router.
- Virtual inline installations require that you configure your router to forward WAN traffic to the appliance. See Router Configuration.
- WCCP installations require configuration of your router and the appliance. See WCCP Mode.
Additional Configuration for Windows

Aug 12, 2014
You can use the Windows management tools to perform additional configuration, such as configuring ports and other Windows services, on the Windows instance.

To perform additional configurations for Windows
1. Open a remote desktop (RDP) session to the IP address of the Windows instance from your Worksheet.
2. Log on to the Windows instance with the following credentials:
   - **Username**: Administrator
   - **Password**: password
3. Use interface AUX for Windows Server traffic. This port has a Windows Device Description of "Citrix PV Ethernet Adapter #1: 0/2." Set it to use an IP address and network mask in the network that you chose for the Windows adapter.
4. Enable Windows services for access to services, such as domain services, printer definitions, and user rights.
5. Define only a single default gateway. Add non-default routes as appropriate for your installation.
Assigning a Management IP Address through the Serial Console

Aug 12, 2014

If you do not want to change the settings of your computer, you can perform initial configuration by connecting the appliance to your computer with a serial null modem cable. Make sure that you have physical access to the appliance.

To configure the appliance through the serial console

1. Connect a serial null modem cable to the appliance's console port.
2. Connect the other end of the cable to the serial COM port of a computer running a terminal emulator, such as Microsoft HyperTerminal, with settings 9600,N,8,1, p.
3. On the HyperTerminal output, press Enter. The terminal screen displays the Logon prompt.
   Note: You might have to press Enter two or three times, depending on the terminal program you are using.
4. At the logon prompt, log on to the appliance with the following default credentials:
   Username: nsroot
   Password: nsroot.
5. At the $ prompt, run the following command to switch to the shell prompt of the appliance:
   $ ssh 169.254.0.10
6. Enter Yes to continue connecting to the management service.
7. Log on to the shell prompt of the appliance with the following default credentials:
   Password: nsroot.
8. At the logon prompt, run the following command to open the Management Service Initial Network Address Configuration menu:
   # networkconfig
9. Type 1 and press Enter to select option 1, and specify a new management IP address for the management service.
10. Type 2 and press Enter to select option 2, and specify a new management IP address for the XenServer server.
11. Type 3 and press Enter to select option 3, and then specify the network mask for the management service IP address.
12. Type 4 and press Enter to select option 4, and then specify the default gateway for the management service IP address.
13. Type 8 and press Enter to save the settings and exit.
14. Access the SD-WAN appliance by entering the new management service IP address of the appliance, such as https://<Management_Service_IP_Address>, in a web browser of a computer on the management network.
15. To continue the configuration, accept the certificate and continue. The option to continue varies according to the web browser you are using.
16. Run steps 4 through 25 of the Configuring the Appliance by Connecting a Computer to the Ethernet Port procedure to complete the configuration process.
Deployment Modes

A SD-WAN appliance acts as a virtual gateway. It is neither a TCP endpoint nor a router. Like any gateway, its job is to buffer incoming packets and put them onto the outgoing link at the right speed. This packet forwarding can be done in different ways, such as inline mode, virtual inline mode, and WCCP mode. Although these methods are called modes, you do not have to disable one forwarding mode to enable another. If your deployment supports more than one mode, the mode that the appliance uses is determined automatically by the Ethernet and IP format of each packet.

Because the appliance supports different forwarding modes and different kinds of non-forwarded connections, it needs a way of distinguishing one kind of traffic from another. It does so by examining the destination IP address and destination Ethernet address (MAC address), as shown in table below. For example, in inline mode, the appliance is acting as a bridge. Unlike other traffic, bridged packets are addressed to a system beyond the appliance, not to the appliance itself. The address fields contain neither the appliance's IP address nor the appliance's Ethernet MAC address.

In addition to pure forwarding modes, the appliance has to account for additional types of connections, including management connections to the GUI and the heartbeat signal that passes between members of a high-availability pair. For completeness, these additional traffic modes are also listed in table below.

**Table 1. How Ethernet and IP Addresses Determine the Mode**

<table>
<thead>
<tr>
<th>Destination IP Address</th>
<th>Destination Ethernet Address</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not appliance</td>
<td>Not appliance</td>
<td>Inline or Pass-through</td>
</tr>
<tr>
<td>Not appliance</td>
<td>Appliance</td>
<td>Virtual Inline or L2 WCCP</td>
</tr>
<tr>
<td>Appliance</td>
<td>Appliance</td>
<td>Direct (UI access)</td>
</tr>
<tr>
<td>Appliance (VIP)</td>
<td>Appliance</td>
<td>High-Availability. Proxy mode</td>
</tr>
<tr>
<td>Appliance (WCCP GRE Packet)</td>
<td>Appliance</td>
<td>WCCP GRE Mode</td>
</tr>
<tr>
<td>Appliance (Signaling IP)</td>
<td>Appliance</td>
<td>Signaling Connection (SD-WAN plugin, Secure Peer) or Redirector Mode Connection (SD-WAN plugin)</td>
</tr>
</tbody>
</table>

All modes can be active simultaneously. The mode used for a given packet is determined by the Ethernet and IP headers.

The forwarding modes are:
- **Inline mode**, in which the appliance transparently accelerates traffic flowing between its two Ethernet ports. In this mode, the appliance appears (to the rest of the network) to be an Ethernet bridge. Inline mode is recommended, because it requires the least configuration.
- **WCCP mode**, which uses the WCCP v. 2.0 protocol to communicate with the router. This mode is easy to configure on most routers. WCCP has two variants: WCCP-GRE and WCCP-L2. WCCP-GRE encapsulates the WCCP traffic within
generic routing encapsulation (GRE) tunnels. WCCP-L2 uses un-encapsulated network Layer 2 (Ethernet) transport.

- **Virtual inline mode**, in which a router sends WAN traffic to the appliance and the appliance returns it to the router. In this mode, the appliance appears to be a router, but it uses no routing tables. It sends the return traffic to the real router. Virtual inline mode is recommended when inline mode and high-speed WCCP operation are not practical.
- **Group mode**, which allows two appliances to operate together to accelerate a pair of widely separated WAN links.
- **High availability mode**, which allows two appliances to operate as an active/standby high availability pair. If the primary appliance fails, the secondary appliance takes over.

Additional traffic types are listed here for completeness:

- **Pass-through traffic** refers to any traffic that the appliance does not attempt to accelerate. It is a traffic category, not a forwarding mode.
- **Direct access**, where the appliance acts as an ordinary server or client. The GUI and CLI are examples of direct access, using the HTTP, HTTPS, SSH, or SFTP protocols. Direct access traffic can also include the NTP and SNMP protocols.
- **Appliance-to-appliance communication**, which can include signaling connections (used in secure peering and by the SD-WAN plugin), VRRP heartbeats (used in high-availability mode), and encrypted GRE tunnels (used by group mode).
- **Deprecated modes**. Proxy mode and redirector mode are legacy forwarding modes that should not be used in new installations.
Customizing the Ethernet ports

Dec 26, 2012

A typical appliance has four Ethernet ports: two accelerated bridged ports, called *accelerated pair A* (apA.1 and apA.2), with a bypass (fail-to-wire) relay, and two unaccelerated motherboard ports, called Primary and Aux1. The bridged ports provide acceleration, while the motherboard ports are sometimes used for secondary purposes. Most installations use only the bridged ports.

Some SD-WAN units have only the motherboard ports. In this case, the two motherboard ports are bridged.

The appliance's user interface can be accessed by a VLAN or non-VLAN network. You can assign a VLAN to any of the appliance's bridged ports or motherboard ports for management purposes.

Figure 1. Ethernet Ports

The ports are named as follows:

<table>
<thead>
<tr>
<th>Table 1. Ethernet Port Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motherboard port 1</td>
</tr>
<tr>
<td>Motherboard port 2</td>
</tr>
<tr>
<td>Bridge #1</td>
</tr>
<tr>
<td>Bridge #2</td>
</tr>
</tbody>
</table>
Port Parameters

Each bridge and motherboard port can be:
- Enabled or disabled
- Assigned an IP address and subnet mask
- Assigned a default gateway
- Assigned to a VLAN
- Set to 1000 Mbps, 100 Mbps, or 10 Mbps
- Set to full duplex, half-duplex, or auto (on SD-WAN 4000/5000 appliances, some ports can be set to 10 Gbps)

All of these parameters except the speed/duplex setting are set on the Configuration: IP Address page. The speed/duplex settings are set on the Configuration: Interface page.

Notes about parameters:
- Disabled ports do not respond to any traffic.
- The browser-based UI can be enabled or disabled independently on all ports.
- To secure the UI on ports with IP addresses, select HTTPS instead of HTTP on the Configuration: Administrator Interface: Web Access page.
- Inline mode works even if a bridge has no IP address. All other modes require that an IP address be assigned to the port.
- Traffic is not routed between interfaces. For example, a connection on bridge apA does not cross over to the Primary or Aux1 ports, but remains on bridge apA. All routing issues are left to your routers.
Accelerated Bridges (apA and apB)

Dec 07, 2012

Every appliance has at least one pair of Ethernet ports that function as an accelerated bridge, called apA (for accelerated pair A). A bridge can act in inline mode, functioning as a transparent bridge, as if it were an Ethernet switch. Packets flow in one port and out the other. Bridges can also act in one arm mode, in which packets flow in one port and back out the same port.

An appliance that has a bypass card maintains network continuity if a bridge or appliance malfunctions.

Some units have more than one accelerated pair, and these additional accelerated pairs are named apB, apC, and so on.

If the appliance loses power or fails in some other way, an internal relay closes and the two bridged ports are electrically connected. This connection maintains network continuity but makes the bridge ports inaccessible. Therefore you might want to use one of the motherboard ports for management access.

Caution: Do not enable the Primary port if it is not connected to your network. Otherwise, you cannot access the appliance, as explained in Ethernet Bypass and Link-Down Propagation.

Bypass cards are standard on some models and optional on others. Citrix recommends that you purchase appliances with bypass cards for all inline deployments.

The bypass feature is wired as if a cross-over cable connected the two ports, which is the correct behavior in properly wired installations.

Important: Bypass installations must be tested - Improper cabling might work in normal operation but not in bypass mode. The Ethernet ports are tolerant of improper cabling and often silently adjust to it. Bypass mode is hard-wired and has no such adaptability. Test inline installations with the appliance turned off to verify that the cabling is correct for bypass mode.

If the appliance is equipped with two accelerated bridges, they can be used to accelerate two different links. These links can either be fully independent or they can be redundant links connecting to the same site. Redundant links can be either load-balanced or used as a main link and a failover link.

Figure 1. Using dual bridges

When it is time for the appliance to send a packet for a given connection, the packet is sent over the same bridge from which the appliance received the most recent input packet for that connection. Thus, the appliance honors whatever link decisions are made by the router, and automatically tracks the prevailing load-balancing or main-link/failover-link algorithm in real time. For non-load-balanced links, the latter algorithm also ensures that packets always use the correct bridge.

Multiple bridges are supported in both WCCP mode and virtual inline mode. Usage is the same as in the single-bridge case, except that WCCP has the additional limitation that all traffic for a given WCCP service group must arrive on the same bridge.
Two units with multiple bridges can be used in a high-availability pair. Simply match up the bridges so that all links pass through both appliances.
Motherboard Ports

Dec 05, 2012

Although the Ethernet ports on a bypass card are inaccessible when the bypass relay is closed, the motherboard ports remain active. You can sometimes access a failed appliance through the motherboard ports if the bridged ports are inaccessible.

The Primary Port

If the Primary port is enabled and has an IP address assigned to it, the appliance uses that IP address to identify itself to other acceleration units. This address is used internally for a variety of purposes, and is most visible to users as the Partner Unit field on the Monitoring: Optimization: Connections page. If no motherboard port is enabled, the appliance uses the IP address of Accelerated Pair A.

The Primary port is used for:
- Administration through the web based UI
- A back channel for group mode
- A back channel for high-availability mode

The Aux1 Port

The Aux1 port is identical to the Primary port. If the Aux1 port is enabled and the Primary port is not, the appliance takes its identity from the Aux1 port's IP address. If both are enabled, the Primary port's IP address is the unit's identity.
VLAN Support

Dec 05, 2012

A virtual local area network (VLAN) uses part of the Ethernet header to indicate which virtual network a given Ethernet frame belongs to. SD-WAN appliances support VLAN trunking in all forwarding modes (inline, WCCP, virtual inline, and group mode). Traffic with any combination of VLAN tags is handled and accelerated correctly.

For example, if one traffic stream passing through the accelerated bridge is addressed to 10.0.0.1, VLAN 100, and another is addressed to 10.0.0.1, VLAN 111, the appliance knows that these are two distinct destinations, even though the two VLANs have the same IP address.

You can assign a VLAN to all, some, or none of the appliance's Ethernet ports. If a VLAN is assigned to a port, the management interfaces (GUI and CLI) listen only to traffic on that VLAN. If no VLAN is assigned, the management interfaces listen only to traffic without a VLAN. This selection is made on the Configuration: Appliance Settings: Network Adapters: IP Addresses tab.
Inline Mode

Dec 26, 2012
In inline mode, traffic passes into one of the appliance's Ethernet ports and out of the other. When two sites with inline appliances communicate, every TCP connection passing between them is accelerated. All other traffic is passed through transparently, as if the appliance were not there.

Figure 1. Inline mode, Accelerating All Traffic on a WAN

Note: Any TCP-based traffic passing through both units is accelerated. No address translation, proxying, or per-site setup is required. Inline mode is auto-detecting and auto-configuring.
Configuration is minimized with inline mode, because your WAN router need not be aware of the appliance's existence.
Depending on your configuration, inline mode's link-down propagation can affect management access to the appliance if a link goes down.

Inline mode is most effective when applied to all traffic flowing into and out of a site, but it can be used for only some of the site's traffic.
Ethernet Bypass and Link-Down Propagation

Oct 30, 2013

Note: Link-Down propagation was added to the SD-WAN 2000, 3000, 4000, and 5000 appliances with the 7.2.1 release. Most 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 the other as if the appliance were not there. In fail-to-wire mode, the appliance looks like a cross-over cable connecting the two ports.

Any failure of the appliance hardware or software also closes the relay. When the appliance is restarted, the bypass relay remains closed until the appliance is fully initialized, maintaining network continuity at all times. This feature is automatic and requires no user configuration.

When the bypass relay is closed, the appliance’s bridge ports are inaccessible.

If carrier is lost on one of the bridge ports, the carrier is dropped on the other bridge port to ensure that the link-down condition is propagated to the device on the other side of the appliance. Units that monitor link state (such as routers) are thus notified of conditions on the other side of the bridge.

Link-down propagation has two operating modes:

- If the Primary port is not enabled, the link-down state on one bridge port is mirrored briefly on the other bridge port, and then the port is re-enabled. This allows the appliance to be reached through the still-connected port for management, HA heartbeat, and other tasks.
- If the Primary port is enabled, the appliance assumes (without checking) that the Primary port is used for management, HA heartbeat, and other tasks. The link-down condition on one bridge port is mirrored persistently on the other port, until carrier is restored or the unit is rebooted. This is true even if the Primary port is enabled in the GUI but not connected to a network, so the Primary port should be disabled (the default) when not in use.
Accelerating an Entire Site

Dec 05, 2012

Inline mode, Accelerating All Traffic on a WAN shows a typical configuration for inline mode. For both sites, the appliances are placed between the LAN and the WAN, so all WAN traffic that can be accelerated is accelerated. This is the simplest method for implementing acceleration, and it should be used when practical.

Because all the link traffic is flowing through the appliances, the benefits of fair queuing and flow control prevent the link from being overrun.

In IP networks, the bottleneck gateway determines the queuing behavior for the entire link. By becoming the bottleneck gateway, the appliance gains control of the link and can manage it intelligently. This is done by setting the bandwidth limit slightly lower than the link speed. When this is done, link performance is ideal, with minimal latency and loss even at full link utilization.
Partial-Site Acceleration

Dec 27, 2012
To reserve the appliance’s accelerated bandwidth for a particular group of systems, such as remote backup servers, you can install the appliance on a branch network that includes only those systems. This is shown in the following figure.
Figure 1: Inline Mode, Accelerating Selected Systems Only

SD-WAN traffic shaping relies on controlling the entire link, so traffic shaping is not effective with this topology, because the appliance sees only a portion of link traffic. Latency control is up to the bottleneck gateway, and interactive responsiveness can suffer.
Configuring and Troubleshooting Inline Mode

Dec 26, 2012
Inline mode requires only basic configuration, because it is applied automatically to any packets passing through the accelerated bridge. Troubleshooting is described under.
WCCP Mode

Web Cache Communication Protocol (WCCP) is a dynamic routing protocol introduced by Cisco. Originally intended only for web caching, WCCP version 2 became a more general-purpose protocol, suitable for use by accelerators such as Citrix NetScaler SD-WAN appliances.

WCCP mode is the simplest way of installing a SD-WAN appliance when inline operation is impractical. It is also useful where asymmetric routing occurs, that is, when packets from the same connection arrive over different WAN links. In WCCP mode, the routers use the WCCP 2.0 protocol to divert traffic through the appliance. Once received by the appliance, the traffic is treated by the acceleration engine and traffic shaper as if it were received in inline mode.

Note:
- For the purposes of this discussion, WCCP version 1 is considered obsolete and only WCCP version 2 is presented.
- The standard WCCP documentation calls WCCP clients “caches.” To avoid confusion with actual caches, Citrix generally avoids calling a WCCP client a “cache.” Instead, WCCP clients are typically called “appliances.”
- This discussion uses the term “router” to indicate WCCP-capable routers and WCCP-capable switches. Though the term “router” is used here, some high-end switches also support WCCP, and can be used with SD-WAN WANOP appliances.

The SD-WAN WANOP appliances support two WCCP modes:
- WCCP is the original SD-WAN WANOP WCCP offering supported since release 3.x. It supports a single appliance service group (no clustering).
- WCCP clustering, introduced in release 7.2, allows your router to load-balance traffic between multiple appliances.

The physical mode for WCCP deployment of a SD-WAN WANOP appliance is one-arm mode in which the SD-WAN appliance is connected directly to a dedicated port on the WAN router. The WCCP standard includes a protocol negotiation in which the appliance registers itself with the router, and the two negotiate the use of features they support in common. Once this negotiation is successful, traffic is routed between the router and the appliance according to the WCCP router and redirection rules defined on the router.

A WCCP-mode appliance requires only a single Ethernet port. The appliance should either be deployed on a dedicated router port (or WCCP-capable switch port) or isolated from other traffic through a VLAN. Do not mix inline and WCCP modes.

The following figure shows how a router is configured to intercept traffic on selected interfaces and forward it to the WCCP-enabled appliance. Whenever the WCCP-enabled appliance is not available, the traffic is not intercepted, and is forwarded normally.

Figure 1. WCCP Traffic Flow

WCCP allows traffic to be forwarded between the router and the appliance in either of the following modes:
- L2 Mode—Requires that the router and appliance be on the same L2 segment (typically an Ethernet segment). The IP packet is unmodified, and only the L2 addressing is altered to forward the packet. In many devices, L2 forwarding is...
performed at the hardware layer, giving it the maximum performance. Because of its performance advantage, L2 forwarding is the preferred mode, but not all WCCP-capable devices support it.

- GRE Mode—Generic Routing Encapsulation (GRE) is a routed protocol and the appliance can in theory be placed anywhere, but for performance it should be placed close to the router, on a fast, uncongested path that traverses as few switches and routers as possible. GRE is the original WCCP mode. A GRE header is created and the data packet is appended to it. The receiving device removes the GRE header. With encapsulation, the appliance can be on a subnet that is not directly attached to the router. However, both the encapsulation process and the subsequent routing add CPU overhead to the router, and the addition of the 28-byte GRE header can lead to packet fragmentation, which adds additional overhead.

WCCP mode supports multiple routers and both GRE vs. L2 forwarding. Each router can have multiple WAN links. Each link can have its own WCCP service group.

Traffic shaping is not effective unless the appliance manages UDP traffic as well as TCP traffic. A second service group, with a UDP service group for each WAN link, is recommended if traffic shaping is desired.

A WCCP client (an appliance) uses UDP port 2048 to register itself with the router and to negotiate which traffic should be sent to it, and also which WCCP features should be used for this traffic. The appliance operates on this traffic and forwards the resulting traffic to the original endpoint. The status of an appliance is tracked through the WCCP registration process and a heartbeat protocol. The appliance first contacts the router over the WCCP control channel (UDP port 2048), and the appliance and router exchange information with packets named “Here_I_Am” and “I_See_You,” respectively. By default, this process is repeated every ten seconds. If the router fails to receive a message from the appliance for three of these intervals, it considers the appliance to have failed and stops forwarding traffic to it until contact is reestablished.

Different appliances using the same router can provide different services. To keep track of which services are assigned to which appliances, the WCCP protocol uses a service group identifier, a one-byte integer. When an appliance registers itself with a router, it includes service group numbers as well.

- A single appliance can support more than one service group.
- A single router can support more than one service group.
- A single appliance can use the same service group with more than one router.
- A single router can use the same service group with more than one appliance. For SD-WAN appliances, multiple appliances are supported in WCCP cluster mode, and a single appliance is supported in WCCP mode.
- Each appliance specifies a “return type” (L2 or GRE) independently for each direction and each service group. SD-WAN WANOP 4000/5000 appliances always specify the same return type for both directions. Other SD-WAN appliances allow the return type to be different.

Multiple service groups can be used with WCCP on the same appliance. For example, the appliance can receive service-group 51 traffic from one WAN link and service-group 62 traffic from another WAN link. The appliance also supports multiple routers. It is indifferent to whether all the routers use the same service group or different routers use different service groups.

Service Group Tracking. If a packet arrives on one service group, output packets for the same connection are sent on
the same service group. If packets arrive for the same connection on multiple service groups, output packets track the most recently seen service group for that connection.

When WCCP is used with high-availability mode, the primary appliance sends its own apA or apB management IP address, not the virtual address of the HA pair, when it contacts the router. If failover occurs, the new primary appliance contacts the router automatically, reestablishing the WCCP channel. In most cases the WCCP timeout period and the HA failover time overlap. As a result, the network outage is less than the sum of the two delays.

Standard WCCP allows only a single appliance in a WCCP service group. If a new appliance attempts to contact the router, it discovers that the other appliance is handling the service group, and the new appliance sets an Alert. It periodically checks to determine whether the service group is still active with the other appliance, and the new appliance handles the service group when the other appliance becomes inactive. WCCP clustering allows multiple appliances per service group.

The following figure shows a simple WCCP deployment, suitable for either L2 or GRE. The traffic port (1/1) is connected directly to a dedicated router port (Gig 4/12).

Figure 3. Simple WCCP deployment

In this example, the SD-WAN WANOP 4000/5000 is deployed in one-arm mode, with the traffic port (1/1) and the management port (0/1) each connecting to its own dedicated router port.

On the router, WCCP is configured with identical ip wccp redirect in statements on the WAN and LAN ports. Two service groups are used, 71 and 72. Service group 71 is used for TCP traffic and service group 72 is used for UDP traffic. The SD-WAN appliance does not accelerate UDP traffic, but can apply traffic shaping policies to it.

Note: The WCCP specification does not allow protocols other than TCP and UDP to be forwarded, so protocols such as ICMP and GRE always bypass the appliance.

SD-WAN release 7.2 or later supports WCCP clustering, which enables your router to load-balance your traffic between multiple appliances. For more information about deploying SD-WAN appliances as a cluster, see WCCP Clustering.

WCCP Mode (Non-Clustered)

Sep 11, 2014

WCCP mode allows only a single appliance in a WCCP service group. If a new appliance attempts to contact the router, it discovers that the other appliance is handling the service group, and the new appliance sets an Alert. It periodically checks to determine whether the service group is still active with the other appliance, and the new appliance handles the service group when the other appliance becomes inactive.

Note: WCCP clustering allows multiple appliances per service group.

Following are limitations and best practices for (non-clustered) WCCP mode:

- On appliances with more than one accelerated pair, all the traffic for a given WCCP service group must arrive on the same accelerated pair.
- Do not mix inline and WCCP traffic on the same appliance. The appliance does not enforce this guideline, but violating it can cause difficulties with acceleration. (WCCP and virtual inline modes can be mixed, but only if the WCCP and virtual inline traffic are coming from different routers.)
- For sites with a single WAN router, use WCCP whenever inline mode is not practical.
- Only one appliance is supported per service group. If more than one appliance attempts to connect to the same router with the same service group, the negotiation will succeed only for the first appliance.
- For sites with multiple WAN routers serviced by the same appliance, WCCP can be used to support one, some, or all of your WAN routers. Other routers can use virtual inline mode.
Router Support for WCCP

Jan 31, 2014

Configuring the router for WCCP is very simple. WCCP version 2 support is included in all modern routers, having been added to the Cisco IOS at release 12.0(11)S and 12.1(3)T. The best router-configuration strategy is determined by the characteristics of your router and switches. Traffic shaping requires two service groups.

If your router supports Reverse Path Forwarding, you must disable it on all ports, because it can confuse WCCP traffic with spoofed traffic. This feature is found in newer Cisco routers such as the Cisco 7600.

There are two basic approaches to redirecting traffic from the router to the appliance:
- **On the WAN port only**, add a “WCCP redirect in” statement and a “WCCP redirect out” statement.
- **On every port on the router, except the port attached to the appliance**, add a “WCCP redirect in” statement.

The first method redirects only WAN traffic to the appliance, while the second method redirects all router traffic to the appliance, whether it is WAN related or not. On a router with several LAN ports and substantial LAN-to-LAN traffic, sending all traffic to the appliance can overload its LAN segment and burden the appliance with this unnecessary load. If GRE is used, the unnecessary traffic can load down the router as well.

On some routers, the "redirect in" path is faster and puts less of a load on the router's CPU than does the "redirect out" path. If necessary, this can be determined by direct experiment on your router: Try both redirection methods under full network load to see which delivers the highest transfer rates.

Some routers and WCCP-capable switches do not support "WCCP redirect out," so the second method must be used. To avoid overloading the router, the best practice to avoid redirecting large numbers of router ports through the appliance, perhaps by using two routers, one for WAN routing and one for LAN-to-LAN routing.

In general, method 1 is simpler, while method 2 may provide greater performance.

A service group can be either TCP or UDP, but not both. For the traffic shaper to be effective, both kinds of WAN traffic must pass through the appliance. Therefore:
- **Acceleration** requires one service group, for TCP traffic.
- **Traffic shaping** requires two service groups, one for TCP traffic and one for UDP traffic.
- The difference between the two is configured on the appliance, and the router accepts this configuration.
Configuring the Router

Dec 18, 2013

The appliance negotiates WCCP-GRE or WCCP-L2 automatically. The main choice is between *unicast operation* (in which the appliance is configured with the IP address of each router), or *multicast operation* (in which both the appliance and the routers are configured with the multicast address.)

**Normal (Unicast) operation**—For normal operation, the procedure is to declare WCCP version 2 and the WCCP group ID for the router as a whole, then enable redirection on each WAN interface. Following is a Cisco IOS example:

```
config term
ip wccp version 2
! We will configure the appliance to use group 51 for TCP and 52 for UDP.
ip wccp 51
ip wccp 52

! Repeat the following three lines for each WAN interface
! you wish to accelerate:
interface your_wan_interface
! If Reverse Path Forwarding is enabled (with an ip verify unicast
! source reachable” statement), delete or comment out the statement:
! ip verify unicast source reachable-via any
! Repeat on all ports.
ip wccp 51 redirect out
ip wccp 51 redirect in
ip wccp 52 redirect out
ip wccp 52 redirect in

! If the appliance is inline with one of the router interfaces
! (NOT SUPPORTED), add the following line for that interface
! to prevent loops:
ip wccp redirect exclude in
^Z
```

If multiple routers are to use the same appliance, each is configured as shown above, using either the same service groups or different ones.

**Multicast operation**—When giving the appliance and each router a multicast address, the configuration is slightly different than for normal operation. Following is a Cisco IOS example:

```
config term
ip wccp version 2
ip wccp 51 group-address 225.0.0.1

! Repeat the following three lines for each WAN interface
! you wish to accelerate:
interface your_wan_interface
! If Reverse Path Forwarding is enabled (with an ip verify unicast
! source reachable” statement), delete or comment out the statement:
```
ip verify unicast source reachable-via any

ip wccp 51 redirect out
ip wccp 51 redirect in
!
! The following line is needed only on the interface facing the other router,
! if there is another router participating in this service group.
ip wccp 51 group-listen

! If the appliance is inline with one of the router interfaces,
! (which is supported but not recommended), add
! the following line for that interface to prevent loops:
ip wccp redirect exclude in
^Z
Basic Configuration Procedure for WCCP Mode on the SD-WAN Appliance

Jan 31, 2014

For most sites, you can use the following procedure to configure the WCCP mode on the appliance. The procedure has you set several parameters to sensible default values. Advanced deployments might require that you set these parameters to other values. For example, if WCCP service group 51 is already used by your router, you need to use a different value for the appliance.

To configure WCCP mode on the appliance

2. If no service groups have been defined, the Select Mode page appears. The options are Single SD-WAN and Cluster (Multiple SD-WANs). Select Single SD-WAN. You are taken to the WCCP page. Note: The mode labels are misleading. “Single SD-WAN” mode is also used for SD-WAN high-availability pairs.
3. If WCCP mode is not enabled, click Enable.
4. Click Add Service Group.
5. The default interface (apA), Protocol (TCP), WCCP Priority (0), Router Communication (Unicast), (Password blank) and Time to Live (1) values usually do not have to be changed for the first service group that you create, but if they do, type new values in the fields provided.
6. In the Router Addressing field (if you are using unicast) or the Multicast Address field (if you are using multicast), type the router's IP address. Use the IP for the router port used for WCCP communication with the appliance.
7. If more than one router is using WCCP to communicate with this appliance, add additional routers now.
8. If your routers have special requirements, set the Router Forwarding (Auto/GRE/Level-2), Router Packet Return (Auto/GRE/Level-2), and Router Assignment (Mask/Hash) fields accordingly. The defaults produce optimal results with most routers.
9. Click Add.
10. Repeat the preceding steps to create another service group, for UDP traffic (for example, service group Id 52 and Protocol UDP).
11. Go to the Monitoring: Appliance Performance: WCCP page. The Status field should change to Connected within 60 seconds.
12. Send traffic over the link and, on the Connections page, verify that connections are arriving and being accelerated.
In a service group, a WCCP router and a SD-WAN appliance ("WCCP Cache" in WCCP terminology) negotiate communication attributes (capabilities). The router advertises its capabilities in the "I See You" message. The communication attributes are:

- Forwarding Method: GRE or Level-2
- Packet Return Method (multicast only): GRE or Level-2
- Assignment Method: Hash or Mask
- Password (defaults to none)

The appliance triggers an alert if it detects an incompatibility between its attributes and those of the router. The appliance might be incompatible because of a specific attribute of a service group (such as GRE or Level-2). More rarely, in a multicast service group, an alert can be triggered when the "Auto" selection chooses a particular attribute with a particular router connected, but the attribute is incompatible with a subsequent router.

Following are the basic rules for the communication attributes within a SD-WAN Appliance.

For Router Forwarding:
- When "Auto" is selected, the preference is for Level-2, because it is more efficient for both router and appliance. Level-2 is negotiated if the router supports it and the router is on the same subnet as the appliance.
- Routers in a unicast service group can negotiate different methods if "Auto" is selected.
- Routers in a multicast service group must all use the same method, whether forced with "GRE" or "Level-2", or, with "Auto," as determined by the first router in the service group to connect.
- For an incompatibility, an alert announces that the router "has incompatible router forwarding."

For Router Assignment:
- The default is Hash.
- When "Auto" is selected, the mode is negotiated with the router.
- All routers in a service group must support the same assignment method (Hash or Mask).
- For any service group, if this attribute is configured as "Auto," the appliance selects "Hash" or "Mask" when the first router is connected. "Hash" is chosen if the router supports it. Otherwise, "Mask" is selected. The problem of subsequent routers being incompatible with the automatically selected method can be minimized by manually selecting a method common to all routers in the service group.
- For an incompatibility, an alert announces that the router "has incompatible router assignment method."
- With either method, the single appliance in the service group instructs all the routers in the service group to direct all TCP or UDP packets to the appliance. Routers can modify this behavior with access lists or by selecting which interfaces to redirect to the service group.
- For the Mask method, the appliance negotiates the "source IP address" mask. The appliance provides no mechanism to select "destination IP address" or the ports for either source or destination. The "source IP address" mask does not specifically identify any specific IP address or range. The protocol does not provide a means to specify a specific IP address. By default, because there is only a single appliance in the service group, a one-bit mask is used, to conserve router resources. (Release 6.0 used a larger mask.)

For Password:
- If the router requires a password, the password defined on the appliance must match. If the router does not require a password, the password field on the appliance must be blank.
WCCP Testing and Troubleshooting

Jan 31, 2014

When working with WCCP, the appliance provides different ways of monitoring the status of the WCCP interface, and your router should also provide information.

**Monitoring: Appliance Performance: WCCP Page**—The WCCP page reports the current state of the WCCP link, and reports most problems.

**Log Entries**—The Monitoring: Appliance Performance: Logging page shows a new entry each time WCCP mode is established or lost.

Figure 1. WCCP Log Entries (format varies somewhat with release)

---

**Router Status**—On the router, the "show ip wccp" command shows the status of the WCCP link:

```
Router>enable
Password:
Router#show ip wccp

Global WCCP information:
  Router information:
    Router Identifier: 172.16.2.4
    Protocol Version: 2.0

  Service Identifier: 51
    Number of Cache Engines: 0
    Number of routers: 0
    Total Packets Redirected: 19951
    Redirect access-list: -none-
    Total Packets Denied Redirect: 0
    Total Packets Unassigned: 0
    Group access-list: -none-
    Total Messages Denied to Group: 0
    Total Authentication failures: 0
```
WCCP Clustering

Sep 12, 2014

The WCCP clustering feature enables you to multiply your acceleration capacity by assigning more than one SD-WAN appliance to the same links. You can cluster up to 32 identical appliances, for up to 32 times the capacity. Because it uses the WCCP 2.0 standard, WCCP clustering works on most routers and some smart switches, most likely including those you are already using.

Because it uses a decentralized protocol, WCCP clustering allows SD-WAN appliances to be added or removed at will. If an appliance fails, its traffic is rerouted to the surviving appliances.

Unlike SD-WAN high-availability, an active/passive pair that uses two appliances to provide the performance of a single appliance, the same appliances deployed as a WCCP cluster has twice the performance of a single appliance, delivering both redundancy and improved performance.

In addition to adding more appliances as your site’s needs increase, you can use Citrix’s “Pay as You Grow” feature to increase your appliances’ capabilities through license upgrades.

Citrix Command Center is recommended for managing WCCP clusters. The following figure shows a basic network of a cluster of SD-WAN appliances in WCCP mode, administered by using Citrix Command Center.

Figure 1. SD-WAN Cluster Administered by Using Citrix Command Center

The WCCP protocol supports up to 32 appliances in a fault-tolerant, load balanced array called a cluster. In the example below, three identical appliances (same model, same software version) are cabled identically and configured identically except for their IP addresses. Appliances using the same service groups with the same router can become a load balanced WCCP cluster. When a new appliance registers itself with the router, it can join the existing pool of appliances and receive its share of traffic. If an appliance leaves the network (as indicated by the absence of heartbeat signals), the cluster is rebalanced so that only the remaining appliances are used.

Figure 2. A load-balanced WCCP cluster with three appliances

One appliance in the cluster is selected as the designated cache, and controls the load-balancing behavior of the appliances in the cluster. The designated cache is the appliance with the lowest IP address. Because the appliances have identical configurations, it doesn’t matter which one is the designated cache. If the current designated cache goes offline, a different appliance becomes the designated cache.

The designated cache determines how the load-balanced traffic is allocated and informs the router of these decisions. The router shares information with all members of the cluster, so the cluster can operate even if the designated cache goes offline.

Note: As normally configured, a SD-WAN WANOP 4000/5000 appliance appears as two WCCP caches to the router.

Load-Balancing Algorithm

Load balancing in WCCP is static, except when an appliance enters or leaves the cluster, which causes the cluster to be rebalanced among its current members.
The WCCP standard supports load balancing based on a mask or a hash. For example, SD-WAN WANOP WCCP clustering uses the mask method only, using a mask of 1-6 bits of the 32-bit IP address. These address bits can be non-consecutive. All addresses yielding the same result when masked are sent to the same appliance. Load balancing effectiveness depends on choosing an appropriate mask value: a poor mask choice can result in poor load-balancing or even none, with all traffic sent to a single appliance.
Deployment Topology

Sep 11, 2014

Depending on your network topology, you can deploy WCCP cluster either with a single router or with multiple routers. Whether connected to a single router or multiple routers, each appliance in the cluster must be connected identically to all routers in use.

In the following diagram, three SD-WAN appliances accelerate the datacenter's 200 Mbps WAN. The site supports 750 XenApp users.

As shown on the NetScaler SD-WAN Datasheet, a SD-WAN 3000-100 can support 100 Mbps and 400 users, so a pair of these appliances supports 200 Mbps and 800 users, which satisfies the datacenter's requirements of a 200 Mbps link and 750 users.

For fault tolerance, however, the WCCP cluster should continue to operate without becoming overloaded if one appliance fails. That can be accomplished by using three appliances when the calculations call for two. This is called the N+1 rule.

Failure is an unusual event, so usually all three appliances are in operation. In this case, each appliance is supporting only 67 Mbps and 250 users, leaving plenty of headroom, and making good use of the fact that the cluster has three times the CPU power and three times the compression history of a single appliance.

Without WCCP clustering, the same level of capacity and fault-tolerance would require a pair of SD-WAN WANOP 4000-500 appliances in high availability mode. Only one of these appliances is active at a time.

Using multiple WAN routers is very similar to using a single WAN router. If the previous example is changed to include two 100 Mbps links instead of one 200 Mbps link, the topology changes, but the calculations do not.
Limitations

Sep 08, 2014
Configuring appliances in a WCCP cluster has the following limitations:

- All appliances within a cluster must be the same model and use the same software release.
- Parameter synchronization between appliances within the cluster is not automatic. Use Command Center to manage the appliances as a group.
- SD-WAN traffic shaping is not effective, because it relies on controlling the entire link as a unit, and none of the appliances are in a position to do this. Router QoS can be used instead.
- The WCCP-based load-balancing algorithms do not vary dynamically with load, so achieving a good load balance can require some tuning.
- The hash method of cache assignment is not supported. Mask assignment is the supported method.
- While the WCCP standard allows mask lengths of 1-7 bits, the appliance supports masks of 1-6 bits.
- Multicast service groups are not supported; only unicast service groups are supported.
- All routers using the same service group pair must support the same forwarding method (GRE or L2).
- The forwarding and return method negotiated with the router must match: both must be GRE or both must be L2. Some routers do not support L2 in both directions, resulting in an error of "Router's forward or return or assignment capability mismatch." In this case, the service group must be configured as GRE.
- SD-WAN VPX does not support WCCP clustering.
- The appliance supports (and negotiates) only unweighted (equal) cache assignments. Weighted assignments are not supported.
- Some older appliances, such as the SD-WAN 700, do not support WCCP clustering.
- (SD-WAN WANOP 4000/5000 only) Two accelerator instances are required per interface in L2 mode. No more than three interfaces are supported per appliance (and then only on appliances with six or more accelerator instances.)
- (SD-WAN 4000/5000 only) WCCP control packets from the router must match one of the router IP addresses configured on the appliance for the service group. In practice, the router's IP address for the interface that connects it to the appliance should be used. The router's loopback IP should not be used.
Planning Your Deployment

Jan 30, 2014
Deploying appliances in a WCCP cluster requires more planning than does deploying a single appliance. Read the following sections carefully before proceeding.
Selecting Appliances

Jan 30, 2014

The appliances you select for the deployment must all be the same model, running the same software version. Otherwise, management and troubleshooting can become impractical.

Your appliance choice is generally made by comparing your site’s WAN bandwidth and number of WAN users to the capacities of the different appliances in the NetScaler SD-WAN Data Sheet. For fault tolerance, always order one more appliance than is absolutely required according to the data sheet.

The number of appliances you need is found as follows, rounding up all fractions:

\[
\text{appliances} = \max ( \text{appliances}_\text{bw}, \text{appliances}_\text{users} ),
\]

where

\[
\text{appliances}_\text{bw} = \frac{\text{WAN\_bandwidth}}{\text{Optimized\_WAN\_capacity}} + 1
\]

\[
\text{appliances}_\text{users} = \frac{\text{WAN\_users}}{\text{Maximum\_HDX\_sessions}} + 1
\]

Note that if \( \text{appliances} = 2 \), you can use just a single appliance instead of WCCP clustering, or an HA pair instead of WCCP clustering, since the equation builds in a spare appliance. In other words, WCCP clustering is not necessary (from a capacity perspective) unless appliances is 3 or more.

**Example**. Suppose you have 700 users and a 100 Mbps link. Some appliances you might consider are the SD-WAN 2000-050, the SD-WAN 3000-100, and the SD-WAN 4000-310.

<table>
<thead>
<tr>
<th>Model</th>
<th>Optimized WAN Capacity</th>
<th>Maximum HDX Sessions</th>
<th>Appliances_bw</th>
<th>Appliances_users</th>
<th>Appliances</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000-050</td>
<td>50 Mbps</td>
<td>300</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3000-100</td>
<td>100 Mbps</td>
<td>400</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4000-310</td>
<td>310 Mbps</td>
<td>750</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

As you can see from the above table, the higher-performance platforms require fewer appliances to get the job done, as you would expect. The SD-WAN 4000-310 meets the requirements with a single appliance, and evaluates to two appliances only because the equations build in a spare.

You can always add more capacity by adding more appliances, but that is not always necessary. The bandwidth limits of two of the three choices, the SD-WAN 3000-100 and the SD-WAN 4000-310, can be increased through a license upgrade. The SD-WAN 4000-050 however, is already at the high end of the range for NetScaler 2000 appliances.
Load-Balancing in the WCCP Cluster

Sep 12, 2014

Traffic is distributed among the appliances in the WCCP cluster. If an appliance leaves the cluster (through failure, overload, or being manually disabled), its traffic is rebalanced by distributing it among the surviving members. If an appliance joins the cluster, traffic is rebalanced once more to give the new appliance its fair share.

The Address Mask

Traffic is distributed on the basis of an address mask that is applied to the source and destination addresses of WAN traffic. You must select an appropriate mask field for efficient load-balancing. An inappropriate mask can result in load-balancing that is poor to nonexistent. For example, if the mask matches an address field that is identical at all your remote sites, all your WAN traffic is sent to a single appliance, overloading it. For example, if all of your remote sites have an address in the form of 10.0.x.x, and your mask bits are within the 10.0 portion of the address all traffic is sent to a single appliance.

The address bits extracted by the address mask are used as an index that is used (indirectly) to select one of the WCCP caches (appliances). For example, an address mask with two “one” bits results in four possible values, depending on the address. Each of these values can be thought of as a bucket. With two mask bits, you have four buckets, numbered 0-3. The buckets are assigned to WCCP caches. To be effective, there must be at least as many buckets as caches. If you use a two-bit mask and have five or more caches, some caches are idle, because each bucket is assigned to only one cache, and there are not enough buckets to cover all five caches:

<table>
<thead>
<tr>
<th>Cache</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buckets</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>-</td>
</tr>
</tbody>
</table>

If there are more buckets than caches, some caches are assigned multiple buckets. For example, if you set three mask bits, creating eight buckets, and you have four caches, two buckets are assigned to each cache. If you have five caches, three caches are assigned two buckets each, and two caches are assigned just one. If each bucket represents the same number of users, you have a 2:1 load imbalance across caches:

<table>
<thead>
<tr>
<th>Cache</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buckets</td>
<td>0-1</td>
<td>2-3</td>
<td>4-5</td>
<td>6</td>
<td>7</td>
</tr>
</tbody>
</table>

Increasing the number of set mask bits reduces this imbalance. With four mask bits (16 index values) and five caches, four caches receive three buckets and one cache receives four buckets, resulting in only a 4:3 imbalance. With six set mask bits (the largest number supported), four caches receive 13 buckets and one receives 12, which is only a 13:12 load imbalance.

<table>
<thead>
<tr>
<th>Cache</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buckets</td>
<td>0-12</td>
<td>13-25</td>
<td>26-38</td>
<td>39-51</td>
<td>52-63</td>
</tr>
</tbody>
</table>

Ideally, you would like each remote site to be directed to a single appliance in the WCCP cluster, so that all traffic to and from a given site is stored in the same compression history. With this arrangement, any traffic from one user at the site can be used to compress similar traffic from any other user at that site. In other words, for compressibility, load-balancing works best if it the address mask selects the bits that differentiate one remote site from another. These are often the least-significant bits of the subnet portion of the IP address. Using these bits tends to allocate the same number of remote sites (not users) per local appliance. A mask that aligns with the host portion of the address instead of the subnet results in a
more equal number of remote users (not sites) per appliance, but at the expense of compression effectiveness. (Compression is only effective when connections flow through the same appliances, and splitting traffic from the same remote site between two or more local appliances interferes with this.)

Finally, for good load-balancing, each “one” bit in the address mask must be set to one on 50% of the remote addresses, and set to zero on 50% of the remote addresses. This is not the case on all address bits, since in most WANs, the highest-order network bits never change at all (such as the 10 in 10.x.x.x). Such bits must never be selected by the address mask.

In addition, many subnets are only sparsely populated. For example, if only 50 addresses are used in the subnet 10.1.2.0/24, and they are assigned sequentially, the two higher-order host bits (representing the unused range of 10.1.2.64-10.1.2.255) for this subnet never change, and if these two bits are included in the address mask, three-fourths of the buckets receive no traffic.

Useful compromises between these two extremes can generally be found.

Follow these rules:
- The number of “one” bits in the address mask must allow at least as many combinations as there are WCCP caches in the cluster. That is, if you have eight appliances, the address mask must contain at least three “one” bits.
- The “one” bits in the address mask must each be inside the active address range for most of your remote subnets, or they skew the load-balancing distribution.
- The mask should split the address range of individual remote sites into as few pieces as possible, for best compression performance.
- If a remote appliance is faster than the local members of the WCCP cluster, the mask should be designed to divide its traffic between multiple local appliances. For example, a 100 Mbps remote appliance should have its traffic split between two 50 Mbps local appliances by setting a bit inside the remote appliance’s active address range.
- The “one” bits in the mask are typically contiguous, but this is not required. They can be in any pattern.

**Example:** Suppose you set an address mask of 0x0000 0f00, which has four “one” bits. This defines a four-bit field that is extracted from the IP address, yielding 16 possible results (16 buckets). These buckets are in turn assigned to the actual WCCP caches in the WCCP cluster.

<table>
<thead>
<tr>
<th>Address</th>
<th>Masked Address (mask = 0x0000 0f00)</th>
<th>Bucket</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.5</td>
<td>0.0.0.0</td>
<td>0</td>
</tr>
<tr>
<td>10.0.1128</td>
<td>0.0.1.0</td>
<td>1</td>
</tr>
<tr>
<td>155.0.2.55</td>
<td>0.0.2.0</td>
<td>2</td>
</tr>
<tr>
<td>253.100.255.2</td>
<td>0.0.15.0</td>
<td>15</td>
</tr>
<tr>
<td>10.0.15.1</td>
<td>0.0.15.0</td>
<td>15</td>
</tr>
</tbody>
</table>

Zero bits in the mask are ignored, and the “one” bits are used to define the extracted field. So if the mask is 0x10 10 10 10, these widely separated “one” bits are extracted into a four-bit field, declaring 16 buckets and a bucket numbers in the range of 0-15.

If the mask value is set to zero, a default value of 0x00 00 0f 00 is used.
Assigning Buckets to Appliances

Sep 08, 2014

The mapping of bucket to appliances is subject to several variables:

- Which appliances are available: If an appliance is down, its share of buckets are given to the available appliance. If a new appliance is added to the cluster, it is given its fair share of buckets.
- The mapping algorithm used (deterministic or least-disruptive).
- The order in which appliances come online (least-disruptive mapping only).
- The IP addresses of the appliances. WCCP algorithms can use a sorted list of appliance IP addresses; for example, assigning buckets to appliances in the same order as the appliance IP addresses.

The most important of these factors, from an administrator’s point of view, is the mapping algorithm.

**Deterministic mapping.** The deterministic mapping algorithm is less graceful than the least-disruptive algorithm, but it supports Hot Standby Router Protocol (HSRP) and Global Server Load Balancing (GSLB) routing, and is required when multiple routers using such protocols share the WCCP cluster.

Deterministic mapping is also the preferred method when the cluster has only two appliances.

Assignments are based on the IP addresses of the active appliances. Each appliance gets its fair share of bucket, with the lowest-numbered bucket being assigned to the appliance with the lowest IP address. If there are more appliances than buckets, the leftover appliances (with no bucket assigned to them) are the ones with the highest-numbered IP addresses. This deterministic assignment allows traffic to arrive for a single connection through any of the routers in the service group and be forwarded to the same appliance.

Reassignment can be disruptive to accelerated connections, which are reset if they migrate to a different appliance. With deterministic mapping, the number of buckets that are reassigned to new appliances can be quite high if there are three or more appliances.

**Least-disruptive mapping.** When a bucket is assigned to a different appliance, any open accelerated connections that used the old appliance is reset. The least-disruptive algorithm keeps the reassignment to a minimum. For example, if you have three appliances, and one appliance fails, the new mapping preserves roughly two-thirds of the assignments and remaps the remaining third (which fails anyway, because their appliance failed). The least-disruptive algorithm does not support HSRP or GSLB routing, because it is not guaranteed to result in identical mappings on all the routers in the service group, and therefore, packets from a single connection might be sent to two different appliances by two different routers, which causes accelerated connections to fail.
Startup and Failover Behavior

Jan 30, 2014

Each appliance registers itself with the routers specified in its service class definitions. The first appliance to register itself, becomes the designated cache, and works with the routers to apportion traffic between itself and the other caches (called subordinate caches). Because your appliances use identical WCCP algorithms, it does not matter which one becomes the designated cache.

As additional appliances come online, they are added to the WCCP cluster, and the traffic is reapportioned among the active appliances. This happens at ten-second increments. After a cold start of the routers or appliances, all of the appliances might come online within the same ten-second window, or they might arrive over multiple ten-second windows, causing traffic to be reapportioned multiple times before it stabilizes. In the latter case, the appliances that come online first may can become overloaded until additional appliances come online.

An accelerated connection fails when allocated to a different appliance, making reallocation disruptive. This is not true of non-accelerated connections, which generally experience a delay of thirty seconds or more, and then continue. The least-disruptive mapping option minimizes the amount of reallocation when an appliance fails.

If an appliance fails or otherwise goes offline, its absence is noted, and the designated cache reapportions its traffic to the remaining appliances. If the designated cache itself goes offline, the role of designated cache is also reapportioned. It takes about thirty seconds for the cluster to react to the loss of a cache.
# Deployment Worksheet

Sep 12, 2014

On the following worksheet, you can calculate the number of appliances needed for your installation and the recommended mask field size. The recommended mask size is 1-2 bits larger than the minimum mask size for your installation.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Model Used</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Supported XenApp and XenDesktop Users Per Appliance</td>
<td>Uspec =</td>
<td>From data sheet</td>
</tr>
<tr>
<td>XenApp and XenDesktop Users on WAN Link</td>
<td>Uwan =</td>
<td></td>
</tr>
<tr>
<td>User overload Factor</td>
<td>Uoverload = Uwan/Uspec =</td>
<td></td>
</tr>
<tr>
<td>Supported BW Per Appliance</td>
<td>BWspec =</td>
<td>From data sheet</td>
</tr>
<tr>
<td>WAN Link BW</td>
<td>BWwan =</td>
<td></td>
</tr>
<tr>
<td>BW Overload Factor</td>
<td>BWoverload = BWwan/BWspec =</td>
<td></td>
</tr>
<tr>
<td>Number of appliances required</td>
<td>N = max(Uoverload, BWoverload) +1 =</td>
<td>Includes one spare</td>
</tr>
<tr>
<td>Min number of buckets</td>
<td>Bmin = N, rounded up a power of 2 =</td>
<td></td>
</tr>
<tr>
<td>If SD-WAN 4000 or 5000</td>
<td>Bmin = 2*N, rounded up to a power of 2 =</td>
<td></td>
</tr>
<tr>
<td>Recommended value</td>
<td>B = 4 * Bmin if Bmin &lt;= 16, else 2 * Bmin =</td>
<td></td>
</tr>
<tr>
<td>Number of “one” bits in address mask</td>
<td>M = log2(B)</td>
<td>If B=16, M=4.</td>
</tr>
</tbody>
</table>

Mask value: The mask value is a 32-bit address mask with a number of “one” bits equal to M in the above worksheet. Often
these bits can be the least-significant bits in the WAN subnet mask used by your remote sites. If the masks at your remote sites vary, use the median mask. (Example: With /24 subnets, the least significant bits of the subnet are 0x00 00 nn 00. The number of bits to set to one is log2(mask size); if mask size is 16, set four bits to one. So with a mask size of 16 and a /24 subnet, set the mask value to 0x00 00 0f 00.): ______

The above guidelines work only if the selected subnet field is evenly distributed in your traffic, that is, that each address bit selected by the mask is a one for half the remote hosts, and a zero for the other half. Otherwise, load-balancing is impaired. This even distribution might be true for only a small number of bits in the network field (perhaps only two or three bits). If this is the case with your network, instead of masking bits in the offending area of the subnet field, displace those bits to a portion of the host address field that has the 50/50 property. For example, if only three subnet bits in a /24 subnet have the 50/50 property, and you are using four mask bits, a mask of 0x00 00 07 10 avoids the offending bit at 0x00 00 0800 and displaces it to 0x00 00 00 10, a portion of the address field that is likely to have the 50/50 property if your remote subnets generally use at least 32 IP addresses each.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final Mask Value</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Accelerated Bridge</td>
<td>Usually apA</td>
<td></td>
</tr>
<tr>
<td>WAN Service Group</td>
<td>A service group not already in use on your router (51-255)</td>
<td></td>
</tr>
<tr>
<td>LAN Service Group</td>
<td>Another unused service group</td>
<td></td>
</tr>
<tr>
<td>Router IP address</td>
<td>IP address of router interface on port facing the appliance</td>
<td></td>
</tr>
<tr>
<td>WCCP Protocol (usually &quot;Auto&quot;)</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>DC Algorithm</td>
<td>Use “Deterministic” if you have only two appliances or are using dynamic load balancing like HSRP or GSLB. Otherwise, use “Least Disruptive.”</td>
<td></td>
</tr>
</tbody>
</table>
After you have finalized the deployment topology, considered all limitations, and filled in the deployment worksheet, you are ready to deploy your appliances in a WCCP cluster. To configure the WCCP cluster, you need to perform the following tasks:

- Configuring the NetScaler Instances
- Configuring the Router
- Configuring the Appliance
Configuring the Router

Sep 12, 2014

WCCP configuration on the router is simple, because most WCCP parameters are set by the appliances.

Unlike legacy SD-WAN WCCP support, WCCP clustering uses two service groups for TCP traffic. One service group is used on the router’s WAN interface, and the other is used on the router’s LAN interfaces (except for the LAN interface used by the SD-WAN appliances themselves, when deployed in L2-mode WCCP cluster).

As shown in the following figure, you need to configure two service groups because WCCP allows the mask to be applied to either the source IP or the destination IP address, which is not quite what is required. To keep connections between two endpoints together, regardless of which endpoint initiates the connection, the appliance applies the address mask to the source IP address of incoming WAN traffic, and to the destination IP address of incoming LAN traffic. This requires two service groups.

The WAN service group uses WCCP source-ip address masking, while the LAN service group uses dest-ip masking. In some deployments, it may be necessary to reverse the assignments, using the “WAN” service group for your LAN interface and vice versa. This might occur if the number of local IP addresses greatly exceeds the number of remote IP addresses.

Figure 1. SD-WAN WCCP Cluster

To configure WCCP clustering on the router

This procedure assumes Cisco routers, but is similar on other routers. It uses the first of the two methods, discussed above, of redirecting WCCP traffic with an ip wccp redirect in statement on both LAN and WAN ports.

1. Fill in the WCCP clustering Deployment Worksheet.
2. Log on to your router
3. In the global declarations section, declare each service group on the WCCP clustering worksheet, listed as WAN service group and LAN Service group. For example, ip wccp 61 and ip wccp 62.
   Note: The ip wccp command allows, but does not require, a more elaborate syntax than this, and can specify an ACL name or a password. Both service groups must have the same password, if one is used. The ACLs can be different.
4. Inside the interface declarations for each WAN interface that connects to remote SD-WAN appliances, add an ip wccp x redirect in statement, where x is the WAN service group from the WCCP clustering worksheet.
5. Inside the interface declarations for each LAN interface (except the one connecting to the WCCP cluster, if you are using L2 mode), add an ip wccp y redirect in statement, where y is the LAN service group from the WCCP clustering worksheet.
6. Save your configuration.

Example. The following example uses service group 61 for the WAN service group and service group 62 for the LAN service group. Three router interfaces are used. One is connected to the WAN, one is connected to the LAN, and one is connected to the WCCP cluster.

Example is for WCCP clustering using WCCP redirect in statements
   on LAN and WAN interfaces.
   This definition is appropriate for modern Cisco routers.
   Global declarations
   ip wccp 61
   ip wccp 62
interface GigabitEthernet1/1
description LAN interface. SG 62 is used for LAN
ip address 172.80.1.56 255.255.255.0
ip wccp 62 redirect in
!
interface GigabitEthernet1/2
description LAN interface attaching SD-WAN L2-WCCP appliances
description (No wccp redirect statements are used on this interface)
ip address 172.80.21.56 255.255.255.0
!
interface GigabitEthernet1/3
description WAN interface. SG 61 is used for WAN
ip address 172.80.22.56 255.255.255.0
ip wccp 61 redirect in
!
Note: If the router used multiple ports for LAN traffic, each port is configured with an ip wccp 62 redirect in statement. Similarly, if the router used multiple ports for WAN traffic, each port is configured with an ip wccp 61 redirect in statement.
- If the router used multiple ports for LAN traffic, each port is configured with an ip wccp 62 redirect in statement.
  - Similarly, if the router used multiple ports for WAN traffic, each port is configured with an ip wccp 61 redirect in statement.
- If multiple routers shared the same WCCP cluster, they use the same service groups.

It is also possible to use ip wccp redirect statements on only the WAN interfaces:
- Example for WCCP clustering using WCCP redirect in/out statements on
  - WAN interface only
  - This definition is appropriate for modern Cisco routers.
interface GigabitEthernet1/3
description WAN interface. SG 61 is used for WAN. SG 62 is used for LAN.
ip address 172.80.22.56 255.255.255.0
ip wccp 61 redirect in
ip wccp 62 redirect out
!
In many routers, the ip wccp redirect out path is not optimized in hardware, but uses the CPU. If the router's capabilities along this path exceeds the WAN speed, this method is practical, and is simpler than using redirect statements on every interface.

Router ACLs can be used to limit redirection. For example, for initial testing, perhaps only a single remote IP address might be allowed to be redirected through WCCP.
Configuring the Appliance

Sep 09, 2014
Repeat the following procedure for each appliance in the cluster:

1. Fill in the WCCP clustering Deployment Worksheet.
2. Navigate to Configuration > Appliance Settings > WCCP page.
3. Click Enable to enable WCCP mode on the appliance.
4. Select Cluster (Multiple Caches) option.

5. Fill in parameters in the Select SD-WAN Cluster section.

6. Enter T5 from your worksheet as the Cache 1 IP, T6 as the Cache 2 IP, T2 as the Subnet Mask, and T1 as the Gateway. Click Save. The Configure Service Group section appears.
7. In the Service Group Details section, specify the WAN and LAN service groups (T11 and T12 from your worksheet).
8. In the Priority field, select 100 (in practice this value is somewhat arbitrary).
9. From the Protocol list, select TCP.
10. In the DC Algorithm field, select Deterministic or Least Disruptive. “Deterministic” is always safe to use, and should be used if you are using only two appliances, or are using multiple routers. “Least Disruptive” disrupts fewer user sessions on failover when used with clusters of three or more appliances, but has restrictions on its use.
11. Set Service Group Pair Status to On.
12. If your router is configured to require a password, enter the password in the Service Group Password field. Otherwise, leave the field blank.
13. In the Router Communications Details section, enter the IP address of the router (T8 on your worksheet: often identical to T1 as well). This is the IP address of the appliance-facing router interface. If you use multiple routers to communicate with the appliance, list them all here.
14. From the Router Forwarding list, select Level 2 or GRE, according to the capabilities of your router. Use Level 2 if you can, and GRE if you must.
15. For the Mask Value, enter the value you determined from the WCCP Clustering worksheet. This is a critical value: a poor choice will result in poor load-balancing or none at all.
16. Click Create. This creates the WAN and LAN service groups.
17. On the Configuration > Optimization Rules > Link Definitions page, change the bandwidth limits on each defined WAN to 95% of the aggregate speed of all your WANs. This prevents the link from being under-utilized when load-balancing is imperfect. If ICA (XenApp/XenDesktop) is the dominant use, set each appliance to (95% of WAN bandwidth)/N, where N is the number of appliances (or twice the number of appliances if they are SD-WAN 4000 or 5000 units), to divide the bandwidth equally among the appliances. This latter method is most appropriate for applications with large numbers of active connections that have relatively low bandwidth requirements.
Testing and Troubleshooting

Jan 31, 2014

The Monitoring > Appliance > Application Performance > WCCP page shows the current state of not only the local appliance but of all other appliances that have joined the cluster. Select a WCCP cache and click Get Info.

The Cache Status tab shows the local appliance's status. When all is well, the status is “25: has assignment.” You must refresh the page manually to monitor changes in status. If the appliance does not reach the status of “25: has assignment” within a timeout period, other informative status messages are displayed.

Additional information is displayed when you click on the Service Group or the Routers tabs.

The Cluster Summary tab displays information about the WCCP cluster as a whole. As a side effect of the WCCP protocol, each member of the cluster has information about all the others, so this information can be monitored from any appliance in the cluster.

Your router can also provide status information. See your router documentation.
Virtual Inline Mode

Dec 28, 2012

Note: Use virtual inline mode only when both inline mode and WCCP mode are impractical. Do not mix inline and virtual inline modes within the same appliance. However, you can mix virtual inline and WCCP modes within the same appliance. Citrix does not recommend virtual inline mode with routers that do not support health monitoring.

In virtual inline mode, the router uses policy based routing (PBR) rules to redirect incoming and outgoing WAN traffic to the appliance for acceleration, and the appliance forwards the processed packets back to the router. Almost all of the configuration tasks are performed on the router. The only thing to be configured on the appliance is the forwarding method, and the default method is recommended.

Like WCCP, Virtual inline deployment requires no rewiring and no downtime, and it provides a solution for asymmetric routing issues faced in a deployment with two or more WAN links. Unlike WCCP, it contains no built-in status monitoring or health checking, making troubleshooting difficult. WCCP is thus the recommended mode, and virtual inline is recommended only when inline and WCCP modes are both impractical.

The following figure shows a simple network in which all traffic destined for or received from the remote site is redirected to the appliance. In this example, both the local site and remote site use virtual inline mode.

Figure 1. Virtual Inline Example

Following are some configuration details for the network in this example:

- Endpoint systems have their gateways set to the local router (which is not unique to virtual inline mode).
- Each router is configured to redirect both incoming and outgoing WAN traffic to the local appliance.
- Each appliance processes the traffic received from its local router and forwards it back to the router.
- PBR rules configured on the router prevent routing loops by allowing packets to make only one trip to and from the appliance. The packets that the appliance forwards back to the router are sent to their original (local or remote) destination.
- Each appliance has its default gateway set to the address of the local router, as usual (on the Configuration: Network Adapters page). The options for forwarding packets back to the router are Return to Ethernet Sender and Send to Gateway.
Configuring Packet Forwarding on the Appliance

May 12, 2015

Virtual inline mode offers two packet-forwarding options:

**Return to Ethernet Sender (default)**—This mode allows multiple routers to share an appliance. The appliance forwards virtual inline output packets back to where they came from, as indicated by the Ethernet address of the incoming packet. If two routers share a single appliance, each gets its own traffic back, but not the traffic from the other router. This mode also works with a single router.

**Send to Gateway (not recommended)**—In this mode, virtual inline output packets are forwarded to the default gateway for delivery, even if they are destined for hosts on the local subnet. This option is usually less desirable than the Return to Ethernet Sender option, because it adds an easily forgotten element of complexity to the routing structure.

**To specify the packet-forwarding option**—On the Configuration: Optimization Rules: Tuning page, next to Virtual Inline, select Return to Ethernet Sender or Send to Gateway.
Router Configuration

May 23, 2013

The router has three tasks when supporting virtual inline mode:
1. It must forward both incoming and outgoing WAN traffic to the SD-WAN appliance.
2. It must forward traffic to its destination (WAN or LAN).
3. It must monitor the health of the SD-WAN appliance so that the appliance can be bypassed if it fails.

In virtual inline mode, the packet forwarding methods can create routing loops if the routing rules do not distinguish between a packet that has been forwarded by the appliance and one that has not. You can use any method that makes that distinction.

A typical method involves dedicating one of the router's Ethernet ports to the appliance and creating routing rules that are based on the Ethernet port on which packets arrive. Packets that arrive on the interface dedicated to the appliance are never forwarded back to the appliance, but packets arriving on any other interface can be.

The basic routing algorithm is:
- Do not forward packets from the appliance back to the appliance.
- If the packet arrives from the WAN, forward it to the appliance.
- If packet is destined for the WAN, forward to the appliance.
- Do not forward LAN-to-LAN traffic to the appliance.
- Traffic shaping is not effective unless all WAN traffic passes through the appliance.

Note: When considering routing options, keep in mind that returning data, not just outgoing data, must flow through the appliance. For example, placing the appliance on the local subnet and designating it as the default router for local systems does not work in a virtual inline deployment. Outgoing data would flow through the appliance, but incoming data would bypass it. To force data through the appliance without router reconfiguration, use inline mode.

If the appliance fails, data should not be routed to it. By default, Cisco policy based routing does no health monitoring. To enable health monitoring, define a rule to monitor the appliance's availability, and specify the "verify-availability" option for the "set ip next-hop" command. With this configuration, if the appliance is not available, the route is not applied, and the appliance is bypassed.

Important: Citrix recommends virtual inline mode only when used with health monitoring. Many routers that support policy-based routing do not support health-checking. The health-monitoring feature is relatively new. It became available in Cisco IOS release 12.3(4)T.

Following is an example of a rule for monitoring the availability of the appliance:

```
! Use a ping (ICMP echo) to see if appliance is connected track 123 rtr 1 reachability ! rtr 1 type echo protocol IpIcmpecho 192.168.1.200 schedule 1 life forever start-time now
```

This rule pings the appliance at 192.168.1.200 periodically. You can test against 123 to see if the unit is up.
Routing Examples

Feb 06, 2014

The following examples illustrate configuring Cisco routers for the local and remote sites shown in Virtual inline example. To illustrate health monitoring, the configuration for the local site includes health monitoring, but the configuration for the remote site does not.

Note: The configuration for the local site assumes that a ping monitor has already been configured. The examples conform to the Cisco IOS CLI. They might not be applicable to routers from other vendors.

Local Site, Health-Checking Enabled

! For health-checking to work, do not forget to start
! the monitoring process.
!
! Original configuration is in normal type.
! appliance-specific configuration is in bold.
!
ip cef
!
interface FastEthernet0/0
ip address 10.10.10.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 172.68.1.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.1.5 255.255.255.0
!
ip classless
!
ip route 0.0.0.0 0.0.0.0 171.68.1.1
!
ip access-list extended client_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.16.20.0 0.0.0.255 10.10.1.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
! Now set the appliance as the next hop, if it’s up.
set ip next-hop verify-availability 192.168.1.200 20 track 123
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop verify-availability 192.168.1.200 10 track 123

https://docs.citrix.com  © 1999-2017 Citrix Systems, Inc. All rights reserved.  p.673
Remote Site (No Health Checking)

! This example does not use health-checking.
! Remember, health-checking is always recommended,
! so this is a configuration of last resort.
!
ip cef
!
interface FastEthernet0/0
ip address 20.20.20.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 171.68.2.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.2.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.2.1
!
ip access-list extended client_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
set ip next-hop 192.168.2.200
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop 192.168.2.200
!
Each of the above examples applies an access list to a route map and attaches the route map to an interface. The access lists identify all traffic originating at one accelerated site and terminating at the other (A source IP of 10.10.10.0/24 and destination of 20.20.20.0/24 or vice versa). See your router's documentation for the details of access lists and route-maps.

This configuration redirects all matching IP traffic to the appliances. If you want to redirect only TCP traffic, you can change the access-list configuration as follows (only the remote side's configuration is shown here):
!
ip access-list extended client_side
permit tcp 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit tcp 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
Note that, for access lists, ordinary masks are not used. Wildcard masks are used instead. Note that when reading a
wildcard mask in binary, "1" is considered a "don't care" bit.
Virtual Inline for Multiple-WAN Environments

Dec 27, 2012
Enterprises with multiple WAN links often have asymmetric routing policies, which seem to require that an inline appliance be in two places at once. Virtual inline mode solves the asymmetric routing problem by using the router configuration to send all WAN traffic through the appliance, regardless of the WAN link used. The below figure shows a simple multiple-WAN link deployment example.

The two local-side routers redirect traffic to the local appliance. The FE 0/0 ports for both routers are in the same broadcast domain as the appliance. The local appliance must use the default virtual inline configuration (Return to Ethernet Sender).

Figure 1. Virtual Inline Mode With Two WAN Routers
Virtual Inline Mode and High-Availability

Dec 27, 2012

Virtual Inline mode can be used in a high availability (HA) configuration. The below figure shows a simple HA deployment. In virtual inline mode, a pair of appliances acts as one virtual appliance. Router configuration is the same for an HA pair as with a single appliance, except that the Virtual IP address of the HA pair, not the IP address of an individual appliance, is used in the router configuration tables. In this example, the local appliances must use default virtual inline configuration (Return to Ethernet Sender).

Figure 1. High-availability Example
In virtual inline mode, unlike WCCP mode, the appliance provides no virtual inline-specific monitoring. To troubleshoot a virtual inline deployment, log into the appliance and use the Dashboard page to verify that traffic is flowing into and out of the appliance. Traffic forwarding failures are typically caused by errors in router configuration.

If the Monitoring: Usage or Monitoring: Connections pages show that traffic is being forwarded but no acceleration is taking place (assuming that an appliance is already installed on the other end of the WAN link), check to make sure that both incoming WAN traffic and outgoing WAN traffic are being forwarded to the appliance. If only one direction is forwarded, acceleration cannot take place.

To test health-checking, power down the appliance. The router should stop forwarding traffic after the health-checking algorithm times out.
In group mode, two or more appliances become a single virtual appliance. This mode is one solution to the problem of asymmetric routing, which is defined as any case in which some packets in a given connection pass through a given appliance but others do not. A limitation of the appliance architecture is that acceleration cannot take place unless all packets in a given connection pass through the same two appliances. Group mode overcomes this limitation.

Group mode can be used with multiple or redundant links without reconfiguring your routers.

Note: Group mode is not supported on the SD-WAN 4000 or 5000 appliances. Group mode applies only to the appliances on one side of the WAN link; the local appliances neither know nor care whether the remote appliances are using group mode.

Group mode uses a heartbeat mechanism to verify that other members of the group are active. Packets are forwarded to active group members only.

Avoiding asymmetric routing is the main reason to use group mode, but group mode is not the only method available for that purpose. If you decide that it is the best method for your environment, you can enable it by setting a few parameters. If the default mechanism for determining which appliance is responsible for a particular connection does not provide optimal acceleration, you can change the forwarding rules.

Figure 1. Group Mode With Redundant Links

Figure 2. Group Mode With Non-Redundant Links with Possible Asymmetric Routing

Figure 3. Group Mode On Nearby Campuses
When to Use Group Mode

Jul 03, 2013
Use group mode in the following set of circumstances:

- You have multiple WAN links.
- There is a chance of asymmetric routing (a packet on a given connection might travel over either link).
- Group mode seems simpler and more practical than alternatives that use a single appliance.

The alternatives are:

- WCCP mode, in which traffic from two or more links is sent to the same appliance by WAN routers, by means of the WCCP protocol.
- Virtual inline mode, in which your routers send traffic from two or more links through the same appliance (or high-availability pair).
- Multiple bridges, where each link passes through a different accelerated bridge in the same appliance.
- LAN-level aggregation, which places an appliance (or high-availability pair) closer to the LAN, before the point where WAN traffic is split into two or more paths.
How Group Mode Works

Dec 06, 2012

In group mode, the appliances that are part of the group each take ownership for a portion of the group’s connections. If a given appliance is the owner of a connection, it makes all the acceleration decisions about that connection and is responsible for compression, flow control, packet retransmission, and so on.

If an appliance receives a packet for a connection for which it is not the owner, it forwards the packet to the appliance that is the owner. The owner examines the packet, makes the appropriate acceleration decisions, and forwards any output packets back to the non-owning appliance. This process preserves the link selection made by the router, while allowing all packets in the connection to be managed by the owning appliance. For the routers, the introduction of the appliances has no consequences. The routers do not need to be reconfigured in any way, and the appliances do not need to understand the routing mechanism. They simply accept the routers’ forwarding decisions.

Figure 1. Sending-side Traffic in Group Mode

Figure 2. Receiving-side traffic flow in group mode

Group mode has two, user-selectable failure modes, which control how the group members interact with each other if one of them fails. The failure mode also determines whether the failed appliance’s bypass card opens (blocking traffic through the appliance) or remains closed (allowing traffic to pass through). The failure modes are:

**Continue to accelerate** - If a group member fails, its bypass card is opened and no traffic passes through the failed appliance. The result is presumably a fail-over if redundant links are used. Otherwise, the link is simply inaccessible. The other appliances in the group continue to accelerate. The usual hashing algorithm handles the changed conditions. (That is, the old hashing algorithm is used, and if the failed unit is indicated as the owner, a hashing algorithm based on the new, smaller group is applied. This preserves as many older connections as possible.)

**Do not accelerate** - If a group member fails, its bypass card closes, allowing traffic to pass through without acceleration. Because an unaccelerated path introduces asymmetric routing, the other members of the group also go into pass-through mode when they detect the failure.
Enabling Group Mode

May 09, 2013

To enable group mode, create a group of two or more appliances. An appliance can be a member of only one group. Group members are identified by IP address and the SSL common name in the appliance license.

All group mode parameters are on the Settings: Group Mode page, in the Configure Settings: Group Mode table.

Figure 1. Group Mode Page

To enable group mode

1. Select the address to use for group communication. At the top of the Group Mode Configuration table on the Configuration: Advanced Deployments: Group Mode tab, the table cell under Member VIP contains the management address of the port used to communicate with other group members. Use the (unlabeled) drop-down menu to select the correct address (for example, to use the Aux1 port, select the IP address you assigned to the Aux1 port). Then, click Change VIP.

2. Add at least one more group member to the list. (Groups of three or more are supported but are rarely used.) In the next cell of the Member VIP column, type the IP address of the port used by the other appliance for group-mode communication.

3. Type the other group member's SSL common name in the SSL Common Name column. The SSL common name is listed on the other appliance's Configure: Advanced Deployments: High Availability tab. If the other group member is a high-availability pair, the name listed is the SSL common name of the primary appliance.

   Note: If the local appliance is not part of a high-availability pair, the first cell in the HA Secondary SSL Common Name column is blank.

   If the other group member is a high-availability pair, specify the SSL Common Name of the HA secondary appliance in the HA Secondary SSL Common Name column.

4. Click Add.

5. Repeat steps 2-4 for any additional appliances or high-availability pairs in the group.

6. The three buttons under the list of group members are toggles, so each is labeled as the opposite of its current setting:

   1. The top button reads either, Do not accelerate when member failure is detected or Continue to accelerate when member failure is detected. The “Do not accelerate…” setting always works and does not block traffic, but if any member fails, the other group members go into bypass mode, which causes a complete loss of acceleration. With the “Continue to accelerate” option, the failing appliance’s bridge becomes an open circuit, and the link fails. This option is appropriate if the WAN router responds by causing a failover. New connections, and open connections belonging to the surviving appliances, are accelerated.

   2. The bottom button should now be labeled Disable Group Mode. If it is not, enable group mode by clicking the button.

7. Refresh the screen. The top of the page should list the group mode partners, but display warnings about their status, because they haven't been configured for group mode yet. For example, it might indicate that the partner cannot be found or is running a different software release.

8. Repeat this procedure with the other members of the group. Within 20 seconds after enabling the last member of the group, the Group Mode Status line should show NORMAL, and the other group mode members should be listed with Status: On-Line and Configuration: OK.
By default, the owner of a group-mode connection is set by a hash of the source and destination IP addresses. Each appliance in the group uses the same algorithm to determine which group member owns a given connection. This method requires no configuration. The owner can optionally be specified through user-settable rules.

Because the group-mode hash is not identical to that used by load balancers, about half of the traffic tends to be forwarded to the owning appliance in a two-Appliance group. In the worst case, forwarding causes the load on the LAN-side interface to be doubled, which halves the appliance's peak forwarding rate for actual WAN traffic.

This speed penalty can be reduced if the Primary or Aux1 Ethernet ports are used for traffic between group members. For example, if you have a group of two appliances, you can use an Ethernet cable to connect the two units' Primary ports, then specify the Primary port on the Group Mode page on each unit. However, maximum performance is achieved if the amount of traffic forwarded between the group-mode members is minimized.

The owner can optionally be set according to specific IP/port-based rules. These rules must be identical on all appliances in the group. Each member of the group verifies that its group-mode configuration is identical to the others. If not all of the configurations are identical, none of the member appliances enter group mode.

If traffic arrives first at the appliance that owns the connection, it is accelerated and forwarded normally. If it arrives first at a different appliance in the group, it is forwarded to its owner over a GRE tunnel, which accelerates it and returns it to the original appliance for forwarding. Thus, group mode leaves the router's link selection unchanged.

Using explicit IP-based forwarding rules can reduce the amount of group-mode forwarding. This is especially useful in primary-link/backup-link scenarios, where each link handles a particular range of IP addresses, but can act as a backup when the other link is down.

Rules are evaluated in order, from top to bottom, and the first matching rule is used. Rules are matched against an optional IP address/mask pair (which is compared against both source and destination addresses), and against an optional port range.

Regardless of the ordering of rules, if the partner appliance is not available, traffic is not forwarded to it, whether a rule matches or not.

For example, in the figure below, member 172.16.1.102 is the owner of all traffic to or from its own subnet (172.16.1.0/24), while member 172.16.0.184 is the owner of all other traffic.

If a packet arrives at unit 172.16.1.102, and it is not addressed to/from net 172.16.1.0/24, it is forwarded to 172.16.0.184. If unit 172.16.0.184 fails, however, unit 172.16.1.102 no longer forwards packets. It attempts to handle the traffic itself. This behavior can be inhibited by clicking Do NOT Accelerate When Member Failure Detected on the Group Mode tab.
In a setup with a primary WAN link and a backup WAN link, write the forwarding rules to send all traffic to the appliance on the primary link. If the primary WAN link fails, but the primary appliance does not, the WAN router fails over and sends traffic over the secondary link. The appliance on the secondary link forwards traffic to the primary-link appliance, and acceleration continues undisturbed. This configuration maintains accelerated connections after the link failover.

Figure 2. Forwarding Rules
Two things should be checked in a group-mode installation:

- That the two appliances have entered group mode, which can be determined on either appliance's Configuration: Advanced Deployments: Group Mode page.
- That the behavior of the group-mode pair is as desired when the other member fails, and when one of the links fail, as determined by disabling the other appliance and temporarily disconnecting one of the links, respectively.
High-Availability Mode

Dec 11, 2013
Two identical appliances on the same subnet can be combined as a *high-availability pair*. The appliances each monitor the other’s status by using the standard *Virtual Router Redundancy Protocol (VRRP)* heartbeat mechanism. The pair has a common virtual IP address for management, in addition to each appliance’s management IP address. If the primary appliance fails, the secondary appliance takes over. Failover takes approximately five seconds.

High availability mode is a standard feature.
How High-Availability Mode Works

Dec 06, 2012

In a high availability (HA) pair, one appliance is primary, and the other is secondary. The primary monitors its own and the secondary's status. If it detects a problem, traffic processing fails over to the secondary appliance. Existing TCP connections are terminated. To ensure successful failover, the two appliances keep their configurations synchronized. In a WCCP mode high availability configuration, the appliance that is processing traffic maintains communication with the upstream router.

Status monitoring—When high availability is enabled, the primary appliance uses the VRRP protocol to send a heartbeat signal to the secondary appliance once per second. In addition, the primary appliance monitors the carrier status of its Ethernet ports. The loss of carrier on a previously active port implies a loss of connectivity.

Failover If the heartbeat signal of the primary appliance should fail, or if the primary appliance loses carrier for five seconds on any previously active Ethernet port, the secondary appliance takes over, becoming the primary. When the failed appliance restarts, it becomes the secondary. The new primary announces itself on the network with an ARP broadcast. MAC spoofing is not used. Ethernet bridging is disabled on the secondary appliance, leaving the primary appliance as the only path for inline traffic. Fail-to-wire is inhibited on both appliances to prevent loops.

Caution: The Ethernet bypass function is disabled in HA mode. If both appliances in an inline HA pair lose power, connectivity is lost. If WAN connectivity is needed during power outages, at least one appliance must be attached to a backup power source.

Note: The secondary appliance in the HA pair has one of its bridge ports, port apA.1, disabled to prevent forwarding loops. If the appliance has dual bridges, apB.1 is also disabled. In a one-arm installation, use port apA.2. Otherwise, the secondary appliance becomes inaccessible when HA is enabled.

Primary/secondary assignment—If both appliances are restarted, the first one to fully initialize itself becomes the primary. That is, the appliances have no assigned roles, and the first one to become available takes over as the primary. The appliance with the highest IP address on the interface used for the VRRP heartbeat is used as a tie-breaker if both become available at the same time.

Connection termination during failover—Both accelerated and unaccelerated TCP connections are terminated as a side effect of failover. Non-TCP sessions are not affected, except for the delay caused by the brief period (several seconds) between the failure of the primary appliance and the failover to the secondary appliance. Users experience the closing of open connections, but they can open new connections.

Configuration synchronization—The two appliances synchronize their settings to ensure that the secondary is ready to take over for the primary. If the configuration of the pair is changed through the browser based interface, the primary appliance updates the secondary appliance immediately.

HA cannot be enabled unless both appliances are running the same software release.

HA in WCCP mode—When WCCP is used with an HA pair, the primary appliance establishes communication with the router. The appliance uses its management IP address on apA or apB, not its virtual IP address, to communicate with the router. Upon failover, the new primary appliance establishes WCCP communication with the router.
Cabling Requirements

May 24, 2013

The two appliances in the high availability pair are installed onto the same subnet in either a parallel arrangement or a one-arm arrangement, both of which are shown in the following figure. In a one-arm arrangement, use the apA.2 port (and, optionally, the apB.2 port), not the apA.1 port. Some models require a separate management LAN, whether deployed in inline or one-armed mode. This is depicted only in the middle diagram.

Figure 1. Cabling for High-Availability Pairs

Do not break the above topology with additional switches. Random switch arrangements are not supported. Each of the switches must be either a single, monolithic switch, a single logical switch, or part of the same chassis.

If the spanning-tree protocol (STP) is enabled on the router or switch ports attached to the appliances, failover will work, but the failover time may increase to roughly thirty seconds. Without STP, failover time is roughly five seconds. Thus, to achieve the briefest possible failover interval, disable STP on the ports connecting to the appliances.

Figure 2. Ethernet Port Locations (Older Models)
Other Requirements

Dec 06, 2012

Both appliances in an HA pair must meet the following criteria:

- Have identical hardware, as shown by on the System Hardware entry on the Dashboard page.
- Run exactly the same software release.
- Be equipped with Ethernet bypass cards. To determine what is installed in your appliances, see the Dashboard page.

Appliances that do not support HA display a warning on the Configuration: High Availability page.
Management Access to the High-Availability Pair

Jan 03, 2013

When configuring a high-availability (HA) pair, you assign the pair a virtual IP (VIP) address, which enables you to manage the two appliances as if they were a single unit. After you enable high-availability mode, managing the secondary appliance through its IP address is mostly disabled, with most parameters grayed out. A warning message displays the reason on every page. Use the HA VIP for all management tasks. You can, however, disable the secondary appliance's HA state from its management UI.
Configuring the High-Availability Pair

Dec 27, 2012
You can configure two newly installed appliances as a high-availability pair, or you can create an HA pair by adding a second appliance to an existing installation.

Prerequisites: Physical installation and basic configuration procedures

To configure high availability

1. Make sure that no more than one appliance is connected to the traffic networks (on the accelerated bridges). If both are connected, disconnect one bridge cable from the active bridges on the second appliance. This will prevent forwarding loops.
2. On the Features page of the first appliance, disable Traffic Processing. This disables acceleration until the HA pair is configured.
3. Repeat for the second appliance.
4. On the first appliance, go to the Configuration: Advanced Deployments: High Availability tab, show below.
5. Select the Enabled Check box.
6. Click the Configure HA Virtual IP Address link and assign a virtual IP address to the apA interface. This address will be used later to control both appliances as a unit.
7. Return to the High Availability page and, in the VRRP VRID field, assign a VRRP ID to the pair. Although the value defaults to zero, the valid range of VRRP ID numbers is 1 through 255. Within this range, you can specify any value that does not belong to another VRRP device on your network.
8. In the Partner SSL Common Name field, type the other appliance's SSL Common Name, which is displayed on that appliance's Configuration: Advanced Deployments: High Availability tab, in the Partner SSL Common Name field. The SSL credentials used here are factory-installed.
9. Click Update.
10. Repeat steps 3-8 on the second appliance. If you are managing the appliance via an accelerated bridge (such as apA), you may have to reconnect the Ethernet cable that you removed in step 1 to connect to the second appliance. If so, plug this cable in and disconnect the corresponding cable on the first appliance.
11. With your browser, navigate to the virtual IP address of the HA pair. Enable Traffic Processing on the Features page. Any further configuration will be performed from this virtual address.
12. Plug in the cable that was left disconnected.
13. On each appliance, the Configuration: Advanced Deployments: High Availability page should now show that high availability is active and that one appliance is the primary and the other is the secondary. If this is not the case, a warning banner appears at the top of the screen, indicating the nature of the problem.

Figure 1. High-availability configuration page
Updating Software on a High-Availability Pair

Dec 06, 2012

Updating the SD-WAN software on an HA pair causes a failover at one point during the update.

Note: Clicking the Update button terminates all open TCP connections.

To update the software on an HA pair

1. Log on to both appliances.
2. On the secondary appliance, update the software and reboot. After the reboot, the appliance is still the secondary. Verify that the installation succeeded. The primary appliance should show that the secondary appliance exists but that automatic parameter synchronization is not working, due to a version mismatch.
3. On the primary appliance, update the software, and then reboot. The reboot causes a failover, and the secondary appliance becomes the primary. When the reboot is completed, HA should become fully established, because both appliances are running the same software.
Saving/Restoring Parameters of an HA Pair

Dec 06, 2012

The System Maintenance: Backup/Restore function can be used to save and restore parameters of an HA pair as follows:

To back up the parameters

Use the backup feature as usual. That is, log on to the GUI through the HA VIP address (as is normal when managing the HA pair) and, on the System Management: Backup/Restore page, click Download Settings.

To restore the parameters

1. Disable HA on both appliances by clearing the Enabled check box on the Configuration: Advanced Deployments: High Availability (HA) tab.
2. Unplug a network cable from the bridge of one appliance. (Call it “Appliance A.”)
3. Unplug the power cord from Appliance A.
4. Restore the parameters on the other appliance (Appliance B), by uploading a previously saved set of parameters on the System Maintenance: Backup/Restore page and clicking Restore Settings. (Completing this operation requires a restart, which reenables HA).
5. Wait for Appliance B to restart. It becomes the primary.
6. Restart Appliance A.
7. Log on to Appliance A’s GUI and reenable HA on the Configuration: Advanced Deployments: High Availability (HA) tab. The appliance get its parameters from the primary.

Both appliances are now restored and synchronized.
Troubleshooting High Availability Pairs

Dec 26, 2012
If the appliances report any failure to enter high-availability mode, the error message will also note the cause. Some issues that can interfere with high-availability mode are:

- The other appliance is not running.
- The HA parameters on the two appliances are not identical.
- The two appliances are not running the same software release.
- The two appliances do not have the same model number.
- Incorrect or incomplete cabling between the appliances does not allow the HA heartbeat to pass between them.
- The HA/Group Mode SSL Certificates on one or both appliances are damaged or missing.
NetScaler SD-WAN 4000 and 5000 WANOP Appliances

Apr 07, 2017
Citrix NetScaler SD-WAN 4000/5000 WANOP appliances are high-performance WAN accelerators for busy datacenters. These appliances combine multiple virtual accelerator instances with a single virtual instance of the NetScaler load-balancer, providing the performance of multiple SD-WAN WANOP appliances in a single package.

SD-WAN 4000/5000 WANOP WAN accelerators are the high end of the Citrix NetScaler SD-WAN product line. They are designed to accelerate sites with WAN links with speeds in excess of 155 Mbps, especially busy datacenters that communicate with a large number of branch and regional sites.

Figure 1. Typical Use Case

A single SD-WAN WANOP 4000/5000 appliance can support WAN speeds of up to 2 Gbps and up to 5000 XenApp/XenDesktop users.

For datacenters needing even more performance, multiple SD-WAN WANOP 4000/5000 appliances can be deployed as a load-balanced array using the WCCP clustering feature.

Figure 2. Load balancing multiple SD-WAN WANOP 4000/5000 appliances

SD-WAN WANOP 4000/5000 is recommended at the hub of a hub-and-spoke deployment, where smaller appliances are used at the spokes, whenever the link speed or the number of XenApp/XenDesktop users is higher than can be supported
If you require a secondary data center, SD-WAN WANOP 4000/5000 appliances can provide optimization for Data-Center to Data-Center replication. This optimization improves replication time and reduces bandwidth consumption.

For details on how to configure a SD-WAN WANOP appliance for DC-to-DC replication with NetApp SnapMirror, see http://support.citrix.com/article/CTX137181.
Internally, the SD-WAN 4000/5000 appliance contains several virtual machines:

- A Xen hypervisor
- A NetScaler instance
- At least two accelerator instances
- A management server instance that manages the GUI and other tasks
- Internal networking

No WAN traffic enters or leaves the accelerators except as configured in the NetScaler instance. When the appliance is first used, the Provisioning Wizard sets up an initial configuration that provides communication and load balancing between the NetScaler instance and the accelerators.

The management service is the management configuration interface for the appliance, and provides access to key operating and monitoring elements of the appliance. The management service displays SD-WAN parameters as if they were from a single accelerator, and all changes made through this interface are applied to all the accelerator instances.

The Xen hypervisor hosts all the virtual machines. The hypervisor is not user-configurable and should not be accessed except at the request of Citrix.

The external network interfaces are divided into two categories: traffic interfaces and management interfaces.

Traffic Interfaces—The traffic interfaces include all the network interfaces except ports 0/1 and 0/2, which are used only for management. Acceleration takes place only on the traffic interfaces.

Note: You must keep the traffic interfaces isolated from the management interface to prevent ARP flapping and other problems. This isolation can be achieved physically or by tagging management interface and traffic interface packets with...
different VLANs.

**Management subnet**—The virtual machines connect directly to the external management subnet, with different IP addresses for the management service, NetScaler instance, and XenServer.

Note: You must keep the traffic interfaces isolated from the management interface to prevent ARP flapping and other problems. This isolation can be achieved physically or by tagging management interface and traffic interface packets with different VLANs.

**Private Internal traffic subnet**—The accelerators’ accelerated ports are connected to the NetScaler instance internally in a one-arm mode, using an internal traffic subnet. There is no direct connection between the instances’ accelerated ports and the appliance’s external ports. All accelerated traffic to the accelerators is controlled by the NetScaler instance.

Since this internal subnet is not accessible from outside the appliance, it uses non-routable subnets in the 169.254.0.0/16 range. The NetScaler instance provides NAT for features that require routable access to the accelerator. Only the following two features of the accelerators require IP addresses that can be reached from the outside world:

- The signaling IP address, used for secure peering and the SD-WAN Plugin.
- IP addresses, used for communication with the router when the WCCP protocol is used.

In both cases, the number of externally visible IP addresses is independent of the number of accelerators the appliance has.

The internal traffic subnet requires two IP addresses per accelerator, plus an address for the NetScaler, plus one or two WCCP VIP addresses if WCCP is used. Since the internal network is private, it has an abundance of address space for these tasks.

**Data Flow on the Private Traffic Subnet**—The one-arm connection between the NetScaler instance and the accelerators uses the SD-WAN virtual inline mode, in which the NetScaler instance routes packets to the accelerators and the accelerators route them back to the NetScaler instance. Traffic flow over this internal traffic subnet is identical regardless of whether the mode visible to the outside world (on the external interfaces) is inline, virtual inline, or WCCP.

This traffic requires the SD-WAN “Return to Ethernet Sender” option, and the NetScaler MAC Address Forwarding and Use Subnet IP options, which are enabled by the Provisioning Wizard.

**Deployment Mode Summary**

The differences between WCCP mode, inline mode, and virtual inline mode can be summarized as follows:

- **WCCP mode** is a one-arm configuration. The accelerators establish WCCP control channels with the router. In WCCP mode, only one or two accelerators manage the WCCP control channel on behalf of all the accelerators. Data traffic is load-balanced across all the accelerators. When GRE encapsulation is used, the NetScaler instance performs GRE encapsulation/decapsulation on the data stream between itself and the router, allowing the data between the NetScaler and the accelerators to use a decapsulated, Level-2 configuration.

- **Inline mode** operates much the same as WCCP mode internally, but externally the appliance emulates a bridge, and no WCCP control channel is established. A packet that enters the appliance on one bridge port exits through the other bridge port. SD-WAN 4000 and 5000 appliances have multiple bridges to support multiple inline links.

- **In virtual inline mode** (used when WCCP and inline modes are not feasible), the appliance is deployed in a one-arm configuration, much like WCCP, but without the WCCP control channel. Traffic is sent to the appliance from the router, using policy-based routing (PBR) rules. The appliance processes the traffic and returns it to the router.

Figure 3. WCCP and virtual inline cabling
See SD-WAN 4000/5000 virtual machines, internal networks, and external port usage for a diagram of port usage on SD-WAN 4000/5000 appliances. Traffic ports are arranged as a set of accelerated bridges, while the management ports are independent. Typically only one management port is used.

Figure 4. Inline cabling

SD-WAN 4000/5000 appliances have multiple accelerated bridges. Different models have different numbers and types of bridge ports. The two ports making up such a bridge are called an "accelerated pair." All current models include a built-in network bypass function. (Some older SD-WAN 4000-500 and 4000-1000 units do not include network bypass). The network bypass function (also called "fail to wire") connects pairs of ports together if the appliance fails as a result of either power loss or software failure (as determined by an internal watchdog timer).

**Inline deployment.** The bypass function allows SD-WAN 4000/5000 to be deployed in line with your WAN, typically between your LAN and your WAN router, without introducing a point of network failure.

The accelerated bridges support either 1 Gbps or 10 Gbps data rates. Ethernet and SFP+ interfaces are supported, depending on model.

**One-arm deployment.** One-arm deployments are also supported, using WCCP or virtual inline modes. With such deployments, a SD-WAN 4000/5000 traffic port is usually connected directly to a port on the WAN router. The other port on the bridged pair is left unconnected.

**Performance considerations.** Inline deployments provide higher performance than the one-arm deployments, because the use of two ports instead of one doubles the peak throughput of the interfaces.

Peak throughput is important with SD-WAN 4000/5000 appliances, because the compressor provides acceleration in proportion to the compression ratio. That is, a connection that achieves 100:1 compression transfers data one hundred times faster than an uncompressed connection, provided that the rest of the network path can keep up.

For example, take a datacenter with a 500 Mbps WAN link and a 1 Gbps LAN. The small 2:1 speed ratio between the WAN and LAN allows compression to provide only a 2x speedup on a whole-link basis, because there is no way to get data onto or off of the LAN at speeds above 1 Gbps. A 10 Gbps LAN, which allows a tenfold increase in peak data rates, is recommended for use with SD-WAN 4000/5000 deployments.

When a SD-WAN 4000/5000 appliance is deployed in a one-arm mode, the peak transfer rate is cut in half. A SD-WAN
4000/5000 in one-arm mode, connected to the router with a 1 Gbps LAN interface, saturates this interface when the WAN is running at full speed in both directions. For good performance, a SD-WAN 4000/5000 must have a LAN interface that is much faster than the WAN. When the appliance is connected directly to the router in a one-arm mode, use a 10 Gbps router port.

Note: The 10 Gbps ports support 10 Gbps only. They do not negotiate lower speeds. Use the 1 Gbps ports for 1 Gbps networks.

A SD-WAN 4000/5000 appliance has at least two non-accelerated ports. Port 0/1 is typically used for management, Port 0/2 is present but typically not used. A Light Out Management (LOM) port is also provided. An RS-232 port can be used for management.
Citrix SD-WAN 4000 are 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 48 gigabytes (GB) of memory. The Citrix SD-WAN 4000 have a bandwidth of 310Mbps, 500Mbps, and 1Gbps, respectively.

The following figures shows the front panel of the Citrix SD-WAN 4000 appliance.

Figure 1. Citrix SD-WAN 4000, front panel (without FTW cards) and (with FTW cards)

The Citrix SD-WAN 4000 appliances have the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.
  
  Note: The LEDs on the LOM port are not operational by design.

- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports (RJ45). These ports are used to connect directly to the appliance for system administration functions.
- Network Ports
  - SD-WAN 4000 (without FTW cards). Eight 1G SFP ports and four 10G SFP+ ports.
  - SD-WAN 4000 (with FTW cards). Eight 1G copper Ethernet ports and four 10G ports.

The following figure shows the back panel of the Citrix SD-WAN 4000 appliance.

Figure 2. Citrix SD-WAN 4000, back panel
The following components are visible on the back panel of the Citrix SD-WAN 4000 appliance:

- Four 600 GB removable solid-state drives, which store the appliance's compression history. The 256 GB solid-state drive below the hard disk drive stores the appliance's software.
- USB port (reserved for a future release).
- A 1 TB removable hard disk drive.
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Disable alarm button. This button is functional only when the appliance has two power supplies. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies (either AC or DC), each rated at 850 watts, 100-240 volts.
SD-WAN 5000

Apr 06, 2017

Citrix SD-WAN 5000 are 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 96 gigabytes (GB) of memory. The Citrix SD-WAN 5000 have a bandwidth of 1.5Gbps and 2Gbps respectively.

The following figure shows the front panel of the Citrix SD-WAN 5000 appliance.

Figure 1. Citrix SD-WAN 5000, front panel

The Citrix SD-WAN 5000 appliance has the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software. Note: The LEDs on the LOM port are not operational by design.
- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports (RJ45). These ports are used to connect directly to the appliance for system administration functions.
- Eight 10G ports.

The following figure shows the back panel of the Citrix SD-WAN 5000 appliance.

Figure 2. Citrix SD-WAN 5000, back panel

The following components are visible on the back panel of the Citrix SD-WAN 5000 appliance:

- Six 600 GB removable solid-state drives, which store the appliance's compression history. The 256 GB solid-state drive next to the power supplies store the appliance's software.
- USB port (reserved for a future release).
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- A 1 TB removable hard disk drive.
- Disable alarm button. This button is functional only when the appliance has two power supplies. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies (either AC or DC), each rated at 650 watts, 100-240 volts.
Field Replaceable Units

Oct 09, 2013

Citrix SD-WAN 4000/5000 field replaceable units (FRU) are components that can be quickly and easily removed from the appliance and replaced by the user or a technician at the user's site. The FRUs in a Citrix SD-WAN 4000/5000 appliance can include DC or AC power supplies, and solid-state and hard-disk drives.

Note: By default the appliance ships with AC power supplies. DC power supply is orderable.
Power Supply

Oct 23, 2013

Citrix SD-WAN 4000/5000 appliances are configured with dual power supplies but can operate with only one power supply. The second power supply serves as a backup.

For power-supply specifications, see "Hardware Platforms," which describes the various platforms and includes a table summarizing the hardware specifications.

Table 1. LED Power Supply Indicators

<table>
<thead>
<tr>
<th>Power Supply Type</th>
<th>LED Color</th>
<th>LED Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>OFF</td>
<td>No power to any power supply.</td>
</tr>
<tr>
<td></td>
<td>Flashing RED</td>
<td>No power to this power supply.</td>
</tr>
<tr>
<td></td>
<td>Flashing GREEN</td>
<td>Power supply is in standby mode.</td>
</tr>
<tr>
<td></td>
<td>GREEN</td>
<td>Power supply is functional.</td>
</tr>
<tr>
<td></td>
<td>RED</td>
<td>Power supply failure.</td>
</tr>
<tr>
<td>DC</td>
<td>OFF</td>
<td>No power to any power supply.</td>
</tr>
<tr>
<td></td>
<td>Flashing RED</td>
<td>No power to this power supply.</td>
</tr>
<tr>
<td></td>
<td>Flashing BLUE</td>
<td>Power supply is in standby mode.</td>
</tr>
<tr>
<td></td>
<td>BLUE</td>
<td>Power supply is functional.</td>
</tr>
<tr>
<td></td>
<td>RED</td>
<td>Power supply failure.</td>
</tr>
</tbody>
</table>

- Make sure that the appliance has a direct physical connection to earth ground during normal use. When installing or repairing an appliance, always connect the ground circuit first and disconnect it last.
- Always unplug any appliance before performing repairs or upgrades.
- Never touch a power supply when the power cord is plugged in. As long as the power cord is plugged in, line voltages are present in the power supply even if the power switch is turned off.

Replace an AC power supply with another AC power supply. All power supplies must be of the same type (AC or DC).

Note: You can replace one power supply without shutting down the appliance, provided the other power supply is working.

To install or replace an AC power supply on a Citrix SD-WAN 4000/5000 appliance

1. Align the semicircular handle perpendicular to the power supply. Loosen the thumbscrew and press the lever toward the handle and pull out the existing power supply, as shown in the following figure.

Figure 1. Removing the Existing AC Power Supply
2. Carefully remove the new power supply from its box.
3. On the back of the appliance, align the power supply with the power supply slot.
4. Insert the power supply into the slot and press against the semicircular handle until you hear the power supply snap into place.
   Figure 2. Inserting the Replacement AC Power Supply

5. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Note: SD-WAN 4000/5000 appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.

Replace a DC power supply with another DC power supply. All power supplies must be of the same type (AC or DC).

Note: You can replace one power supply without shutting down the appliance, provided the other power supply is working.

To install or replace a DC power supply on a Citrix SD-WAN 4000/5000 appliance
1. Loosen the thumbscrew and press the lever towards the handle and pull out the existing power supply, as shown in the following figure.
   Figure 3. Removing the Existing DC Power Supply

2. Carefully remove the new power supply from its box.
3. On the back of the appliance, align the power supply with the power supply slot.
4. Insert the power supply into the slot while pressing the lever towards the handle. Apply firm pressure to insert the power supply firmly into the slot.
   Figure 4. Inserting the Replacement DC Power Supply

5. When the power supply is completely inserted into its slot, release the lever.
6. Connect the power supply to a power source. If connecting all power supplies, plug separate power cords into the power supplies and connect them to separate wall sockets.

Note: SD-WAN 4000/5000 appliances emit a high-pitched alert if one power supply fails or if you connect only one power cable to an appliance in which two power supplies are installed. To silence the alarm, press the small red button on the back panel of the appliance. The disable alarm button is functional only when the appliance has two power supplies.
Solid-State Drive

May 08, 2014

A solid-state drive (SSD) is a high-performance device that stores data in solid-state flash memory.

The SD-WAN 4000/5000 software is stored on the solid-state drive (SSD).

To replace a solid-state drive

1. Shutdown the appliance.

2. Locate the SSD on the back panel of the appliance. Push the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.

   Figure 1. Removing the Existing Solid-State Drive

3. Verify that the replacement SSD is the correct type for the platform.

4. Pick up the new SSD, open the drive handle fully to the left or up, and insert the drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the drive locks securely into the slot.

   Important: When you insert the drive, make sure that the Citrix product label is at the top if the drive is inserted horizontally or at the right if the drive is inserted vertically.

   Figure 2. Inserting the Replacement Solid-State Drive

5. Turn on the appliance.

6. Log on to the default IP address by using a web browser, or connect to the serial console by using a console cable, to perform the initial configuration.
Hard Disk Drive

Feb 28, 2014
The NetScaler and SD-WAN virtual machines are hosted on the hard-disk drive.

Verify that the replacement hard disk drive is the correct type for the SD-WAN 4000/5000 platform.

To install a hard disk drive
1. Shut down the appliance.
2. Locate the hard disk drive on the back panel of the appliance.
3. Disengage the hard disk drive by pushing the safety latch of the drive cover to the right or down, depending on the platform, while pulling out on the drive handle to disengage. Pull out the faulty drive.
   Figure 1. Removing the Existing Hard Disk Drive

4. Pick up the new disk drive, open the drive handle fully to the left, and insert the new drive into the slot as far as possible. To seat the drive, close the handle flush with the rear of the appliance so that the hard drive locks securely into the slot.
   Important: When you insert the drive, make sure that the Citrix product label is at the top.
   Figure 2. Inserting the Replacement Hard Disk Drive

5. Turn on the appliance.
Supported Features

Table 1. Features Table for Citrix SD-WAN 4000 and 5000 Series Appliances

<table>
<thead>
<tr>
<th>Feature</th>
<th>Citrix SD-WAN 4000 series</th>
<th>Citrix SD-WAN 5000 series</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoConfiguration</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>SD-WAN Connector</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>SD-WAN Plug-In</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Compression</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RPC over HTTPS</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>SSL Compression</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>TCP Acceleration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Traffic Shaping</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Video Caching</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Windows File System Acceleration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Windows Outlook Acceleration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>XenApp/ XenDesktop Acceleration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Group Mode Mode</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>High Availability Mode</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Inline Mode</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Virtual Inline Mode</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>WCCP Mode</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>VLANs</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
## Summary of Hardware Specifications

Sep 12, 2013

The following tables summarize the specifications of the Citrix NetScaler SD-WAN 4000/5000 WANOP hardware platforms.

### Table 1. Citrix NetScaler SD-WAN 4000/5000 WANOP Appliances

<table>
<thead>
<tr>
<th>SD-WAN 4000/5000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform Performance</strong></td>
</tr>
<tr>
<td><strong>Bandwidth</strong></td>
</tr>
<tr>
<td>Maximum HDX sessions</td>
</tr>
<tr>
<td>Total sessions</td>
</tr>
<tr>
<td>Acceleration Plug-in CCUs</td>
</tr>
</tbody>
</table>

| **Hardware Specifications** |
| **Processor** | Dual Intel E5645 | Dual Intel E5645 | Dual Intel E5645 | Dual Intel X5680 | Dual Intel X5680 |
| Total disk space | 3.2 TB | 3.2 TB | 3.2 TB | 4.2 TB | 4.2 TB |
| SSD (dedicated compression history) | 2 TB | 2 TB | 2 TB | 3 TB | 3 TB |
| HDD | 1 TB | 1 TB | 1 TB | 1 TB | 1 TB |
| RAM | 48 GB | 48 GB | 48 GB | 96 GB | 96 GB |
| Network interfaces | 4 x 10GigE SX and 8 x 1GigE TX Bypass | 4 x 10GigE SX and 8 x 1GigE TX Bypass* | 4 x 10GigE SX and 8 x 1GigE TX Bypass* | 8 x10GigE SR Bypass | 8 x10GigE SR Bypass |
### SD-WAN 4000/5000

<table>
<thead>
<tr>
<th>Transceiver support</th>
<th>N/A</th>
<th>N/A</th>
<th>N/A</th>
<th>N/A</th>
<th>N/A</th>
</tr>
</thead>
</table>

*Note: Some non fail-to-wire SD-WAN 4000 appliances require SFP+ transceivers.*

<table>
<thead>
<tr>
<th>Power supplies</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
</tr>
</thead>
</table>

### Physical Dimensions

<table>
<thead>
<tr>
<th>Rack units</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>System width</td>
<td>EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets</td>
<td>EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets</td>
<td>EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets</td>
<td>EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets</td>
<td></td>
</tr>
<tr>
<td>System depth</td>
<td>25.4”/64.5 cm</td>
<td>25.4”/64.5 cm</td>
<td>25.4”/64.5 cm</td>
<td>25.4”/64.5 cm</td>
<td>25.4”/64.5 cm</td>
</tr>
<tr>
<td>System weight</td>
<td>46 lbs (20.9 kg)</td>
<td>46 lbs (20.9 kg)</td>
<td>46 lbs (20.9 kg)</td>
<td>49 lbs (22.2 kg)</td>
<td>49 lbs (22.2 kg)</td>
</tr>
<tr>
<td>Shipping dimensions and weight</td>
<td>37” x 24” by 11” 59 lbs 94 x 61 x 28 cm 26.8 kg</td>
<td>37” x 24” by 11” 59 lbs 94 x 61 x 28 cm 26.8 kg</td>
<td>37” x 24” by 11” 61 lbs 94 x 61 x 28 cm 27.7 kg</td>
<td>37” x 24” by 11” 61 lbs 94 x 61 x 28 cm 27.7 kg</td>
<td></td>
</tr>
</tbody>
</table>

### Environmental and Regulatory

<p>| Input voltage and frequency ranges | 100-240 VAC 47-63 Hz | 100-240 VAC 47-63 Hz | 100-240 VAC 47-63 Hz | 100-240 VAC 47-63 Hz | 100-240 VAC 47-63 Hz |
| Power consumption | 650 watts 2,200 BTU per hour. | 650 watts 2,200 BTU per hour. | 650 watts 2,200 BTU per hour. | 850 watts 2,900 BTU per hour. | 850 watts 2,900 BTU per hour. |
| Operating temperature | 32–104° F | 32–104° F | 32–104° F | 32–104° F | 32–104° F |</p>
<table>
<thead>
<tr>
<th>Operating altitude</th>
<th>SD-WAN 4000/5000</th>
<th>0–40° C</th>
<th>0–4921'</th>
<th>0–40° C</th>
<th>0–4921'</th>
<th>0–40° C</th>
<th>0–4921'</th>
<th>0–40° C</th>
<th>0–4921'</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(1,500 m)</td>
<td>(1,500 m)</td>
<td>(1,500 m)</td>
<td>(1,500 m)</td>
<td>(1,500 m)</td>
<td>(1,500 m)</td>
<td>(1,500 m)</td>
<td>(1,500 m)</td>
</tr>
<tr>
<td>Non-operating temperature</td>
<td>-4–140° F</td>
<td>0–60° C</td>
<td>-4–140° F</td>
<td>0–60° C</td>
<td>-4–140° F</td>
<td>0–60° C</td>
<td>-4–140° F</td>
<td>0–60° C</td>
<td>-4–140° F</td>
</tr>
<tr>
<td>Allowed relative humidity</td>
<td>5%-95%, non-condensing</td>
<td>20–60° C</td>
<td>5%-95%, non-condensing</td>
<td>20–60° C</td>
<td>5%-95%, non-condensing</td>
<td>20–60° C</td>
<td>5%-95%, non-condensing</td>
<td>20–60° C</td>
<td>5%-95%, non-condensing</td>
</tr>
<tr>
<td>Safety certifications</td>
<td>UL, TUV-C</td>
<td>UL, TUV-C</td>
<td>UL, TUV-C</td>
<td>UL, TUV-C</td>
<td>UL, TUV-C</td>
<td>UL, TUV-C</td>
<td>UL, TUV-C</td>
<td>UL, TUV-C</td>
<td>UL, TUV-C</td>
</tr>
<tr>
<td>Environmental compliance</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
</tr>
</tbody>
</table>
Lights Out Management Port of the SD-WAN WAN OP 4000/5000 Appliance

Jul 05, 2013

The SD-WAN 4000/5000 appliances have an Intelligent Platform Management Interface (IPMI), also known as the Lights out Management (LOM), port on the front panel of the appliance. By using the LOM, you can remotely monitor and manage the appliance, independently of the SD-WAN 4000/5000 software. You can remotely change the IP address, perform different power operations, and obtain health monitoring information of the appliance by connecting to the appliance through the LOM port.

By connecting the LOM port over a dedicated channel that is separate from the data channel, you can make sure that connectivity to the appliance is maintained even if the data network is down.

By using a web browser you can remotely log on to the LOM port to obtain information about the appliance and perform different operations on the appliance.

To access the LOM by using a web browser

1. In a web browser, type the IP address of the LOM port. For initial configuration, type the port’s default address: http://192.168.1.3
2. In the User Name box, type nsroot.
3. In the Password box, type nsroot.

You can use the Intelligent Platform Management Interface (IPMI), also known as the Lights Out Management (LOM) port, to remotely monitor and manage the appliance, independently of the NetScaler software. For initial configuration of the lights-out management (LOM) port, connect to the port’s default IP address and change it to the address that you want to use for remote monitoring and management. Also specify the administrator credentials and the network settings.

Note: The LEDs on the LOM port are unoperational by design.

To configure the NetScaler LOM Port

1. Connect the LOM port to a management workstation or network.
   
   Note: The NetScaler LOM port is preconfigured with the IP address 192.168.13 and subnet mask 255.255.255.0.
3. In the User Name box, type nsroot.
4. In the Password box, type nsroot.
5. On the Configuration tab, click Network and type values for the following parameters:
   
   - IP Address—IP address of the LOM port.
   - Subnet Mask—Subnet mask used to define the subnet of the LOM port.
   - Default Gateway—IP address of the router that connects the LOM port to the network.
6. Click Save.

You can remotely turn off the appliance and turn it back on. The result is similar to pressing the power button on the back
To power cycle the appliance

1. In a web browser, type the IP address of the LOM port.
2. In the User Name and Password boxes, type the administrator credentials.
3. In the Menu bar, click Remote Control.
4. Under Options, click Power Control, and then click Power Cycle System.
5. Click Perform Action.

The LOM port allows you to remotely access and manage the appliance by logging on to a redirected console.

To access the appliance by using the access console

1. In a web browser, type the IP address of the LOM port.
2. In the User Name and Password boxes, type the administrator credentials.
3. In the Menu bar, click Remote Control.
4. Under Options, click Console Redirection.
5. Click Launch Console, and then click Yes.
6. Type the administrator credentials for the appliance.

You can log on to the LOM port to view the health information about the appliance. All system sensor information, such as system temperature, CPU temperature, status of fan and power supplies, appears on the sensor readings page.

To obtain health monitoring information

1. In a web browser, type the IP address of the LOM port.
2. In the User Name and Password boxes, type the administrator credentials.
3. In the Menu bar, click System Health.

You can remotely perform different power control operations, such as restarting the appliance, performing a graceful shutdown, and performing a forced shutdown, by using the LOM port.

To perform power control operations

1. In a web browser, log on to the LOM port by using the administrator credentials.
2. In the Menu bar, click Remote Control.
3. Under Options, click Power Control, and then select one of the following options:
   - **Reset System**—Restart the appliance.
   - **Power Off System – Immediate**—Disconnect power to the appliance without shutting down the appliance.
   - **Power On System**—Turn on the appliance.
   - **Power Cycle System**—Turn off the appliance, and then turn it back on.
4. Click Perform Action.
Preparing for Installation

Mar 16, 2012

Before you install your new appliance, carefully unpack your appliance and make sure that all parts were delivered. Once you are satisfied that your appliance has been delivered to your expectations, verify that the location where the appliance will be installed meets temperature and power requirements and that the server cabinet or floor-to-ceiling cabinet is securely bolted to the floor and has sufficient airflow.

Only trained and qualified personnel should install, maintain, or replace the appliance, and efforts should be taken to ensure that all cautions and warnings are followed.
Unpacking the Appliance

May 08, 2014

Unpack the box that contains your new appliance on a sturdy table with plenty of space and inspect the contents.

Use the following list to verify that you received everything that should have been included in the box.

- The appliance you ordered
- One RJ-45 to DB-9 adapter
- One 6 ft RJ-45/DB-9 cable
- Two power cables
- One fiber patch cable
- One standard 4-post rail kit
  Note: If the kit that you received does not fit your rack, contact your Citrix sales representative to order the appropriate kit.

In addition to the items included in the box with your new appliance, you will need the following items to complete the installation and initial configuration process.

- Ethernet cables for each additional Ethernet port that you will connect to your network
- One available Ethernet port on your network switch or hub for each Ethernet port you want to connect to your network
- A computer to serve as a management workstation
Preparing the Site and Rack

Jul 10, 2013

There are specific site and rack requirements for the SD-WAN 4000/5000 appliance. You must make sure that adequate environmental control and power density are available. Racks must be bolted to the ground, have sufficient airflow, and have adequate power and network connections. Preparing the site and rack are important steps in the installation process and help ensure a smooth installation.

Site Requirements

The appliance should be installed in a server room or server cabinet with the following features:

**Environment control**
An air conditioner, preferably a dedicated computer room air conditioner (CRAC), capable of maintaining the cabinet or server room at a temperature of no more than 27 degrees C/80.6 degrees F at altitudes of up to 2100 m/7000 ft, or 18 degrees C/64.4 degrees F at higher altitudes, a humidity level no greater than 45 percent, and a dust-free environment.

**Power density**
Wiring capable of handling at least 4,000 watts per rack unit in addition to power needs for the CRAC.

Rack Requirements

The rack on which you install your appliance should meet the following criteria:

**Rack characteristics**
Racks should be either integrated into a purpose-designed server cabinet or be the floor-to-ceiling type, bolted down at both top and bottom to ensure stability. If you have a cabinet, it should be installed perpendicular to a load-bearing wall for stability and sufficient airflow. If you have a server room, your racks should be installed in rows spaced at least 1 meter/3 feet apart for sufficient airflow. Your rack must allow your IT personnel unfettered access to the front and back of each server and to all power and network connections.

**Power connections**
At minimum, two standard power outlets per unit.

**Network connections**
At minimum, Ethernet connection per rack unit.

**Space requirements**
Two empty rack units for SD-WAN 4000/5000 appliances.

Note: You can order the following rail kits separately.
- Compact 4-post rail kit, which fits racks of 23 to 33 inches.
- 2-post rail kit, which fits 2-post racks.
Cautions and Warnings

Mar 24, 2010
Electrical Safety Precautions

Updated: 2014-02-06

Caution: During installation or maintenance procedures, wear a grounding wrist strap to avoid ESD damage to the electronics of the appliance. Use a conductive wrist strap attached to a good earth ground or to the appliance. You can attach it to the connector beside the ESD symbol on the back. Follow basic electrical safety precautions to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch, so that you can quickly remove power to the appliance if an electrical accident occurs.
- Remove all jewelry and other metal objects that might come into contact with power sources or wires before installing or repairing the appliance. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and may cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.
- Use a regulating, uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Never stack the appliance on top of any other server or electronic equipment.
- All appliances are designed to be installed on power systems that use TN earthing. Do not install your device on a power system that uses either TT or IT earthing.
- Make sure that the appliance has a direct physical connection to the earth during normal use. When installing or repairing an appliance, always make sure that the ground circuit is connected first and disconnected last.
- Make sure that a fuse or circuit breaker no larger than 120 VAC, 15 A U.S. (240 VAC, 16 A international) is used on all current-carrying conductors on the power system to which your appliances are connected.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, first shut down the appliance, and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages can be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload. Always unplug any appliance before performing repairs or upgrades.
- Do not overload the wiring in your server cabinet or on your server room rack.
- During thunderstorms, or anticipated thunderstorms, avoid performing any hardware repairs or upgrades until the danger of lightning has passed.
- When you dispose of an old appliance or any components, follow any local and national laws on disposal of electronic waste.
- To prevent possible explosions, replace expired batteries with the same model or a manufacturer-recommended substitute and follow the manufacturer's instructions for battery replacement.
- Never remove a power supply cover or any sealed part that has the following label.
Appliance Precautions

- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest appliance first, at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near an electrical outlet for easy access.
- Mount equipment in a rack with sufficient airflow for safe operation.
- For a closed or multiple-unit rack assembly, the ambient operating temperature of the rack environment might be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously might cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should be used only for extending the appliance out of the rack. Do not use these handles for mounting the appliance on the rack. Use the rack-rail hardware, described later, instead.
Installing the Hardware

Dec 12, 2013

After you have determined that the location where you will install your appliance meets the environmental standards and the server rack is in place according to the instructions, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you will use for initial configuration. To complete the installation, you turn on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.
Rack Mounting the Appliance

Oct 18, 2017

Most appliances can be installed in standard server racks that conform to EIA-310-D specification. The appliances ship with a set of rails, which you must install before you mount the appliance. The only tools that you need for installing an appliance are a Phillips screwdriver and a flathead screwdriver.

Citrix SD-WAN 4000/5000 appliance requires two rack units. Each appliance ships with a mounting rail kit that contains two rail assemblies, one for the left side and the other for the right side of the appliance, and screws to attach the rails. An assembly consists of an inner rail and a rack rail. The supplied rail kit is 28 inches long (38 inches extended). Contact your Citrix sales representative to order a 23-inch (33 inches extended) rail kit.

To mount the appliance, you must first install the rails and then install the appliance in the rack.

Perform the following tasks to mount the appliance:

- Remove the inner rails from the rail assembly.
- Attach the inner rails to the appliance.
- Install the rack rails on the rack.
- Install the appliance in the rack.

Note

The same rail kit is used for both square-hole and round-hole racks.

If you are installing the appliance as the only unit in the rack, mount it at the bottom. If the rack contains other units, make sure that the heaviest unit is at the bottom. If the rack has stabilizing devices available, install them before mounting the appliance.

To remove the inner rails from the rail assembly

1. Place the rail assembly on a flat surface.
2. Slide out the inner rail toward the front of the assembly.
3. Depress the latch until the inner rail comes all the way out of the rail assembly.
4. Repeat steps 1 through 3 to remove the second inner rail.

To attach the inner rails to the appliance

1. Position the right inner rail behind the handle on the right side of the appliance.
2. Align the holes on the rail with the corresponding holes on the side of the appliance.
3. Attach the rail to the appliance with the provided screws: 5 per side.
4. Repeat steps 1 through 3 to install the left inner rail on the other side of the appliance.
To install the rack rails on the rack

1. If you have a round-hole, threaded rack, skip to step 3.
2. Install square nut retainers into the front post and back post of the rack as shown in the following figures. Before inserting a screw, be sure to align the square nut with the correct hole for your appliance. The three holes are not evenly spaced.

3. Install the adjustable rail assembly into the rack as shown in the following figures. Use a screw to lock the rear rail flange into the rack. With the screw securing the rail in place, you can optionally remove the latching spring.

To install the appliance in the rack

1. Align the inner rails, attached to the appliance, with the rack rails.
2. Slide the appliance into the rack rails, keeping the pressure even on both sides.
3. Verify that the appliance is locked in place by pulling it all the way out from the rack.
Installing and Removing 1G SFP Transceivers

Oct 18, 2017

A Small Form-Factor Pluggable (SFP) is a compact transceiver that can operate at speeds of up to 1 gigabit per second and is available in both copper and fiber types. Inserting a 1G SFP copper transceiver converts the 1G SFP port to a 1000BASE-T port. Inserting a 1G SFP fiber transceiver converts the 1G SFP port to a 1000BASE-X port. Auto-negotiation is enabled by default on the 1G SFP port into which you insert your 1G SFP transceiver. As soon as a link between the port and the network is established, the speed and mode are matched on both ends of the cable.

Insert 1G SFP transceivers into the 1G SFP ports on the front panel of the appliance. Frequent installation and removal of transceivers shortens their life span. Follow the removal procedure carefully to avoid damaging the 1G SFP transceiver or the appliance.

### Warning

SD-WAN 4000/5000 appliances do not support 1G SFP transceivers from vendors other than Citrix Systems. Attempting to install third-party 1G SFP transceivers on your SD-WAN 4000/5000 appliance voids the warranty.

### Note

Some SD-WAN 4000/5000 appliances do not require SFP transceivers.

### Warning

Do not install the transceivers with the cables attached. Doing so can damage the cable, the connector, or the optical interface of the transceiver.

To install a 1G SFP transceiver

1. Remove the 1G SFP transceiver carefully from its box.
   Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.
2. Align the 1G SFP transceiver to the front of the 1G SFP transceiver port on the front panel of the appliance.
3. Hold the 1G SFP transceiver between your thumb and index finger and insert it into the 1G SFP transceiver port, pressing it in until you hear the transceiver snap into place.
4. Lock the transceiver.
5. Verify that the LED is green and blinks twice, which indicates that the transceiver is functioning correctly.
6. If you are using a fiber 1G SFP transceiver, do not remove the dust caps attached to the transceiver and the cable until you are ready to insert the cable.
To remove a 1G SFP transceiver

1. Disconnect the cable from the 1G SFP transceiver. If you are using a fiber optic cable, replace the dust cap on the cable before putting it away.
   Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.
2. Unlock the 1G SFP transceiver.
3. Hold the 1G SFP transceiver between your thumb and index finger and slowly pull it out of the port.
4. If you are removing a fiber 1G SFP transceiver, replace the dust cap before putting it away.
5. Put the 1G SFP transceiver into its original box or another appropriate container.
Installing and Removing 10G SFP+ Transceivers

Oct 18, 2017

A 10-Gigabit Small Form-Factor Pluggable (SFP+) is a compact optical transceiver that can operate at speeds of up to 10 gigabits per second. Autonegotiation is enabled by default on the 10G SFP+ ports into which you insert your 10G SFP+ transceiver. As soon as a link between the port and the network is established, the mode is matched on both ends of the cable and for 10G SFP+ transceivers, the speed is also autonegotiated.

Insert the 10G SFP+ transceivers into the 10G SFP+ ports on the front panel of the appliance. Frequent installation and removal of transceivers shortens their life span. Follow the removal procedure carefully to avoid damaging the transceiver or the appliance.

Warning

SD-WAN 4000/5000 appliances do not support 10G SFP+ transceivers provided by vendors other than Citrix Systems. Attempting to install third-party 10G SFP+ transceivers on your SD-WAN 4000/5000 appliance voids the warranty.

Do not install the transceivers with the cables attached. Doing so can damage the cable, the connector, or the optical interface of the transceiver.

To install a 10G SFP+ transceiver

1. Remove the 10G SFP+ transceiver carefully from its box.
2. Align the 10G SFP+ transceiver to the front of the 10G SFP+ transceiver port on the front panel of the appliance.
3. Hold the 10G SFP+ transceiver between your thumb and index finger and insert it into the 10G SFP+ transceiver port, pressing it in until you hear the transceiver snap into place.
4. Move the locking hinge to the DOWN position.
5. Verify that the LED is green and blinks twice, which indicates that the transceiver is functioning correctly.
6. Do not remove the dust caps attached to the transceiver and cable until you are ready to insert the cable.

Warning

Do not look directly into fiber optic transceivers and cables. They emit laser beams that can damage your eyes.

To remove a 10G SFP+ transceiver

1. Disconnect the cable from the 10G SFP+ transceiver. Replace the dust cap on the cable before putting it away.
   Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.
2. Unlock the 10G SFP+ transceiver by moving the locking hinge to the UP position.
3. Hold the 10G SFP+ transceiver between your thumb and index finger and slowly pull it out of the port.
4. Replace the dust cap on the transceiver before putting it away.
5. Put the 10G SFP+ transceiver into its original box or another appropriate container.
Install Fiber Patch Cable in Ports 10/3 and 10/4

Oct 18, 2017

Through release 7.2.1, on an appliance, SD-WAN ports 10/3 and 10/4 must be connected with the provided cable, as shown in the following figure.

Starting with release 7.2.2, the patch cable is no longer required, and can be omitted if:
- The appliance was shipped from the factory with release 7.2.2 or later, or
- The appliance was shipped from the factory with release 7.2.1 or earlier, but you upgrade it to 7.2.2 or later and change the default loopback in the management service (on System > Configuration > System > Configure Loopback Settings).

To install the patch cable
1. Connect the LC-to-LC cable to the ports as shown in the figures above.
2. Insert one end of the cable into port 10/3.
3. Insert the other end of the cable into port 10/4.

Note

If you decide to eliminate the need to use loopback cable, the ports 10/3 and 10/4 are still reserved. These ports are not available for WAN optimization.
Connecting the Cables

When the appliance is securely mounted on the rack, you are ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

Danger: Before installing or repairing the appliance, remove all jewelry and other metal objects that might come in contact with power sources or wires. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.

Connecting the Appliance to the Network

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on a 10/100/1000BASE-T port.

To connect an Ethernet cable to a 10/100/1000BASE-T port

1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port on the front panel of the appliance, as shown in the following figure.
   Figure 1. Inserting an Ethernet cable
2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.
3. Verify that the LED glows amber when the connection is established.

Connecting the Console Cable

You can use the console cable to connect your appliance to a computer or terminal, from which you can configure the appliance. Before connecting the console cable, configure the computer or terminal to support VT100 terminal emulation, 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE. Then connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

To connect the console cable to a computer or terminal

1. Insert the DB-9 connector at the end of the cable into the console port that is located on the front panel of the appliance, as shown in the following figure.
   Figure 2. Inserting a console cable
2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.

Note: To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.

Connecting the Appliance to a Power Source

The SD-WAN 4000/5000 appliance has two power supplies, with one serving as a backup. A separate ground cable is not required, because the three-prong plug provides grounding. Power up the appliance by installing one or both power cords.

To connect the appliance to the power source
1. Connect one end of the power cable to the power outlet on the back panel of the appliance, next to the power supply, as shown in the following figure.

Figure 3. Inserting a power cable

2. Connect the other end of the power cable to a standard 110V/220V power outlet.

3. Repeat steps 1 and 2 to connect the second power supply.

Note: The appliance emits a high-pitched alert if one power supply fails or if you connect only one power cable to the appliance. To silence the alarm, you can press the small red button located on the back panel of the appliance.
Switching on the Appliance

Oct 09, 2013
After you have installed the appliance in a rack and connected the cables, verify that the power cable is properly connected. If you have installed a second power supply, make sure the second cable is connected to an outlet for a different circuit than the first. After verifying the connections, you are ready to switch on the appliance.

To switch on the appliance

1. Verify that the appliance is connected through a console or Ethernet port. This will ensure that you can configure the appliance after it is switched on.
2. Press the ON/OFF toggle power switch on the back panel of the appliance.

Caution: Be aware of the location of the emergency power off (EPO) switch, so that if an electrical accident occurs you can quickly remove power from the appliance.
Planning the Deployment

Apr 26, 2013
SD-WAN 4000/5000 deployments require adequate planning, especially for units deployed in large datacenters:

- An appropriate appliance or group of appliances must be selected to support both the current and anticipated load.
- A deployment mode must be selected to match the requirements of your site.
- Other aspects must also be considered.
Sizing Guidelines

Jun 26, 2013

For successful deployment of one or more SD-WAN 4000/5000 appliances in your datacenter, keep the following principles in mind:

- You must provide enough SD-WAN 4000/5000 peak-load capacity, in terms of WAN bandwidth and the number of users. See the current specifications sheet for the capacities of different SD-WAN 4000/5000 models: http://www.citrix.com/content/dam/citrix/en_us/documents/products/SD-WAN-branch-repeater-spec-sheet.pdf (In the spec sheet, the number of users is referred to as "HDX sessions"). Ensure adequate peak-load capacity, both for now and for the time until you expect to upgrade. Acceleration is resource intensive, and performance suffers if the appliance runs short of resources. Never overcommit any SD-WAN appliance, especially in the datacenter. Provision your datacenter to easily accommodate peak loads.

- Provide enough capacity for expected expansion over the life of the deployment. SD-WAN 4000/5000 appliances using the same hardware platform can have their capacity upgraded with a new license as part of the Citrix pay-as-you-grow program. SD-WAN 4000/5000 models 310, 500, and 1000 use one hardware platform, and models 1500 and 2000 use another hardware platform. This means that, for example, a SD-WAN 4000/5000 500 can be converted through a license upgrade to a SD-WAN 4000/5000 1000, but not to a SD-WAN 4000/5000 1500.

- For more capacity than can be provided by a single appliance, multiple SD-WAN 4000/5000 appliances can be cascaded behind a stand-alone NetScaler appliance.

- Different models have differing numbers of traffic ports. If you require multiple bridges, make sure your model has at least as many as you need.
Selecting a Deployment Mode

Oct 08, 2013

The SD-WAN 4000/5000 appliance can be deployed inline or in a one-arm mode. Inline deployments do not require router reconfiguration; one-arm modes do. SD-WAN 4000/5000 offers internal port bypassing (fail-to-wire) to allow traffic to continue flowing in inline mode if the appliance fails.

Note: Only the one-arm WCCP mode (with a single router) is documented at this time. Inline mode is not yet documented. Citrix recommends WCCP mode at this time.


Deploying a Single SD-WAN 4000/5000 Appliance (or HA Pair)

A standalone SD-WAN 4000/5000 appliance can be deployed in either of these two recommended modes:
- Inline, bridged (L2 inline). This closely resembles a standard SD-WAN inline deployment. Packets enter one bridge port and exit the other bridge port.
- One-arm, WCCP. This resembles a standard SD-WAN WCCP deployment.

Citrix also supports the following two modes (which are outside the scope of this document):
- Inline, routed. The NetScaler instance uses routing rules instead of bridging rules to determine how to forward packets.
- Virtual inline. This resembles WCCP, but lacks built-in health-checking.

In L2 inline mode, SD-WAN 4000/5000 is placed between your LAN and your WAN router (or other aggregation point at the LAN-WAN boundary). In a one-arm mode, SD-WAN 4000/5000 is generally connected directly to a dedicated port on your WAN router.

In cases where the WAN router ports are not as fast as the LAN (for example, when the WAN router has gigabit Ethernet, but the LAN has 10 gigabit Ethernet), inline mode provides better performance, because its LAN-side traffic is not limited to the speed of the router interface. (Compression allows the LAN-side traffic to be much faster than WAN-bound traffic under favorable conditions.)

Considerations:
- The inline modes require no reconfiguration of your routers, but involves a service disruption when bringing the appliance into service.
- One-arm modes require router reconfiguration but do not require a service disruption.
- Inline mode has higher performance than the other modes.
- One-arm modes are limited to half the speed of the router or switch port they are attached to.
- With WCCP mode, configuring the router to send only a fraction of the WAN traffic to SD-WAN 4000/5000 (as little as the traffic from a single remote site or even a single remote IP address) makes it easy to bring up and test the installation gradually. Inline mode requires that all WAN traffic pass through the appliance.
- WCCP mode requires more configuration of the SD-WAN 4000/5000 appliance than do other modes, but is more standardized and provides more status information on the router.

Recommendation:
- The greater control provided by WCCP, and especially the ability to put the deployment into service in stages, makes WCCP the mode of choice for larger, more complex datacenters, especially if there might be a possibility of overloading.
the SD-WAN 4000/5000 appliance.

- Inline mode is convenient for smaller WAN networks and simpler datacenters. It is most commonly used with the SD-WAN 4000/5000 310 and 500, and more rarely with the larger appliances.
- Cascaded installations should use WCCP.

Note: Only WCCP mode (with a single router) is currently documented.
Selecting a Load Balancing Method

Aug 14, 2013

By default, the SD-WAN 4000/5000 Provisioning Wizard sets up load balancing to handle different kinds of connections appropriately. This default behavior is adequate for most installations.

Sending all the connections from the same remote accelerator to the same local accelerator maximizes the benefits of SD-WAN compression, and the default load balancing method accomplishes this. If an instance becomes overloaded or unavailable, new connections are reallocated.

Default Load Balancing Behavior

By default, the NetScaler instance uses the least-connection method to balance the load across the accelerators. This method applies whether or not the connections are accelerated. Connections are persistent, but persistency is discontinued for an instance that becomes overloaded, and is lost if the local appliance is restarted or when no traffic from a remote appliance is seen for more than 24 hours.

Accelerated connections

For incoming accelerated connections (that is, connections with SD-WAN options in the header of the SYN packet), all connections from a given remote SD-WAN are sent to the same local accelerator.

The identity of the remote SD-WAN is determined by one of the SD-WAN SYN options: the "AgentID" field, which contains the management IP address of the remote SD-WAN.

This method is used for connections from remote SD-WAN appliances and remote SD-WAN Plug-ins.

Other connections

Incoming non-accelerated connections and all outgoing connections are also distributed among the accelerators according to the least-connection method, but since they do not contain an AgentID field, they cannot use AgentID persistence. Instead, they use SRCIPDESTIP persistence, meaning that connections with the same IP addresses use the same accelerator.

Bypassing Overloaded Instances

If an instance is overloaded, the NetScaler instance bypasses it for new connections, sending them through without acceleration. Existing connections continue to be sent to the instance.

This behavior is controlled by the skipPersistency parameter. The default behavior is -skippersistency ReLB. The alternative behavior, -skippersistency bypass, instructs the NetScaler instance to pass the connection through without sending it to an accelerator.

Optional Load Balancing Behavior

The default load balancing behavior is adequate for most installations, but sometimes customization is needed. This is most commonly true when a few remote sites have much more traffic than the rest. In that case, it can be worthwhile to assign these large sites to accelerators explicitly.

Optional load balancing behavior includes the use of static routing (for hand-crafted load balancing) and variations on the least-connection with AgentID and SRCIPDESTIP persistence methods used in the default configuration. The behavior for
dealing with overloaded instances can be changed from assigning connections to a difference instance to passing them through as unaccelerated.
Gathering Information Needed for Configuration

Jun 26, 2013

Accurate information about both the local and the remote sites is essential to troubleshooting. Before installing the SD-WAN 4000/5000 appliance, make sure that you have done the following:

1. Obtained or drawn an accurate network diagram of your local site (the one in which you are installing SD-WAN 4000/5000). The local network topology and the capabilities of your WAN routers determine which deployment modes are appropriate for the site.

2. Chosen the deployment mode of the local SD-WAN 4000/5000 appliance (for example, WCCP or inline, with or without HA and cascading).

3. Compiled a list of critical applications that must be tested to validate the deployment.

4. Obtained or drawn an accurate network diagram of your WAN, including both the local and the remote WAN links, their bandwidths in both directions, their subnets, and whether they are accelerated. In deployments with many remote sites, an aggregate of the different categories (accelerated and non-accelerated) is probably sufficient, and only the largest remote sites need to be considered individually.

5. Determined whether there are multiple datacenters with datacenter-to-datacenter traffic, and whether any remote datacenters have a SD-WAN 4000/5000 appliance.

6. Decided whether you plan to increase WAN capacity, the number of sites, or the number of users in the next 24 months. If so, the corresponding SD-WAN 4000/5000 capacity should be installed now.

7. If possible, formed an idea of the traffic breakdown over the WAN, including TCP traffic to and from SD-WAN-accelerated sites, other TCP traffic, ICA users, HDX sessions, and real-time traffic such as VoIP. SD-WAN 4000/5000 needs to be provisioned for the peak loads in terms of accelerated TCP connections, ICA users, and total WAN link capacity.

8. Determined the number of WAN links in the local site. Are they independent, or are they load balanced? If so, are they active-active or active-standby?

9. Determined the current, unaccelerated RTT of the remote sites during peak periods.

10. Identified any QoS devices or proxies in the path between the local and remote sites. QoS devices should be on the WAN side of SD-WAN 4000/5000. Proxies should be on the LAN side.
Initial Configuration

Jan 28, 2011

After checking the connections, you are ready to deploy the SD-WAN 4000 and 5000 appliances on the network.

The appliance shipped from Citrix has default IP addresses configured on it. To deploy the appliance on the network, you must configure the appropriate IP addresses on the appliance to accelerate the network traffic.

Initial configuration consists of the following tasks:
- Identify the prerequisites for the initial configuration.
- Record various values required in the initial configuration procedure.
- Configure the appliance by connecting it to the Ethernet port.
- Assign management IP address through the serial console.

By default, the initial configuration deploys the appliance in inline mode.
Prerequisites

Mar 21, 2018
To deploy a Citrix SD-WAN 4000 or 5000 appliance, you must complete the following prerequisite setup before configuring the appliance.

Software Versions

This document covers release of the SD-WAN software. See the release notes for the recommended versions of the NetScaler software corresponding to the desired release of the SD-WAN software. Never use any versions other than those recommended for SD-WAN 4000 and 5000 appliances.

License File

The number of accelerator appliances depend on the hardware platform and the type of license you apply to the appliance. The following list displays the number of accelerators that gets provisioned automatically by the Configuration Wizard:

- Model 310: Two
- Model 500: Three
- Models 1000 and 1500: Six
- Model 2000: Eight

Before you start provisioning the appliance, Citrix recommends that you have the license file with you, as it is required early in the configuration process.

Installing the Hardware

To install the SD-WAN 4000/5000 appliance hardware, follow the installation procedure at Installing the Hardware.
Deployment Worksheet

Aug 12, 2014

Note: Use this worksheet only when provisioning a factory-reset appliance with the release 7.1 configuration wizard. If you are simply upgrading a previously configured system to release 7.1, your appliance will retain its previous configuration, which will be different.

The appliance uses at least two ports: the management port (typically 0/1) and the traffic port (such as 10/1). Inline mode uses traffic ports in pairs, such as ports 10/1 and 10/2. Ports must be selected in advance, because the configuration depends on their identity.

The appliance uses three subnets directly: the management subnet, the external traffic subnet, and the internal traffic subnet. Multiple IP addresses are used on each subnet. Each subnet must be specified along with the correct subnet mask.

The following figure is a worksheet for these parameters. It supports inline and WCCP modes, with and without HA. The table below the figure describes what each entry means.

Figure 1. Deployment worksheet

<table>
<thead>
<tr>
<th>Table 1. Deployment Worksheet Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>Management Subnet</td>
</tr>
<tr>
<td>M2.</td>
</tr>
<tr>
<td>M3.</td>
</tr>
<tr>
<td>M4.</td>
</tr>
<tr>
<td>M5.</td>
</tr>
<tr>
<td>M6.</td>
</tr>
<tr>
<td>M7.</td>
</tr>
<tr>
<td>External Traffic Subnet</td>
</tr>
<tr>
<td>T1.</td>
</tr>
<tr>
<td>T2.</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>T3.</td>
</tr>
<tr>
<td>T4.</td>
</tr>
<tr>
<td>T5.</td>
</tr>
<tr>
<td>T6.</td>
</tr>
<tr>
<td>T7.</td>
</tr>
<tr>
<td>T8.</td>
</tr>
<tr>
<td>T9.</td>
</tr>
<tr>
<td>T10+.</td>
</tr>
<tr>
<td>T11, T12</td>
</tr>
<tr>
<td>T13, T14</td>
</tr>
<tr>
<td>T15, T16</td>
</tr>
<tr>
<td>T17, T18</td>
</tr>
<tr>
<td>VLAN1.1, VLAN1.2, VLAN1.3, VLAN1.4</td>
</tr>
<tr>
<td>VLAN2.1, VLAN2.2, VLAN2.3, VLAN2.4</td>
</tr>
<tr>
<td>VLAN3.1, VLAN3.2, VLAN3.3, VLAN3.4</td>
</tr>
</tbody>
</table>
Configuring the Appliance

Aug 12, 2014

Before you start configuring the appliance, you must change the IP address of the management service to the one in your management network, so that you can access the appliance over the network. You can change the management IP address by connecting a computer to the appliance through either the Ethernet port or the serial console.
Assigning a Management IP Address through the Ethernet Port

Aug 25, 2017

Use the following procedure for initial configuration of every SD-WAN 1000 or 2000 appliance with Windows Server. The procedure accomplishes the following tasks:
- Configure the appliance for use on your site.
- Install the Citrix license.
- Enable acceleration.
- Enable traffic shaping (inline mode only).

With inline deployments, this configuration might be all you need, because most acceleration features are enabled by default and require no additional configuration.

If you want to configure the appliance by connecting it to the computer through the serial console, assign the management service IP address from your Worksheet by completing the Assigning a Management IP Address through the Serial Console procedure, and then run steps 4 through 15 of the following procedure.

Note: You must have physical access to the appliance.

**To configure the appliance by connecting a computer to the SD-WAN appliance’s Ethernet port 0/1**

1. Set the Ethernet port address of a computer (or other browser-equipped device with an Ethernet port), to 192.168.100.50, with a network mask of 255.255.0.0. On a Windows device, this is done by changing the Internet Protocol Version 4 properties of the LAN connection. You can leave the gateway and DNS server fields blank.
2. Using an Ethernet cable, connect this computer to the port labeled PRI on the SD-WAN appliance.
3. Switch on the appliance. Using the web browser on the computer, access the appliance by using the default management service IP address, which is http://192.168.1.00.1.
4. On the login page, use the following default credentials to log on to the appliance:
   - **Username:** nsroot
   - **Password:** nsroot.
5. Start the configuration wizard by clicking Get Started.
6. On the Platform Configuration page, enter respective values from your worksheet.
7. Click Done. A screen showing the Installation in Progress… message appears. This process takes approximately 2 to 5 minutes, depending on your network speed.
8. A Redirecting to new management IP message appears.
9. Click OK.
10. Unplug your computer from the Ethernet port and connect the port to your management network.
11. Reset the IP address of your computer to its previous setting.
12. From a computer on the management network, log on to the appliance by entering the new management service IP address, such as https://<Managemnt_IP_Address>, in a web browser.
13. To continue the configuration, accept the certificate and continue. The option to continue varies according to the web browser you are using.
14. Log on to the appliance by using the nsroot user name and the password from your worksheet.
15. To complete the configuration process, see Provisioning the Appliance.
Assigning a Management IP Address through the Serial Port

Aug 12, 2014
If you do not want to change the settings of your computer, you can configure the appliance by connecting it to your computer with a serial null modem cable. You must have physical access to the appliance.

**To configure the appliance through the serial console**
1. Connect a serial null modem cable to the appliance’s console port.
2. Connect the other end of the cable to the serial COM port of a computer running a terminal emulator, such as Microsoft HyperTerminal, with settings 9600,N,8,1, p.
3. In the HyperTerminal output, press **Enter**. The terminal screen displays the logon prompt.
   *Note: You might have to press **Enter** two or three times, depending on the terminal program you are using.*
4. At the logon prompt, log on to the appliance with the following default credentials:
   - **Username**: nsroot
   - **Password**: nsroot
5. At the $ prompt, run the following command to switch to the shell prompt of the appliance:
   ```bash
   $ ssh 169.254.0.10
   ```
6. Enter **Yes** to continue connecting to the management service.
7. Log on to the shell prompt of the appliance with the following default credentials:
   - **Password**: nsroot
8. At the logon prompt, run the following command to open the Management Service Initial Network Address Configuration menu:
   ```bash
   # networkconfig
   ```
9. Type **1** and press **Enter** to select option 1, and specify a new management IP address for the management service.
10. Type **2** and press **Enter** to select option 2, and specify a new management IP address for the XenServer.
11. Type **3** and press **Enter** to select option 3, and specify the network mask for the IP addresses.
12. Type **4** and press **Enter** to select option 4, and specify the default gateway for the management service IP address.
13. Type **8** and press **Enter** to save the settings and exit.
14. Access the SD-WAN appliance by entering the new management service IP address of the appliance, such as https://<Management_Service_IP_Address>, in a web browser of a computer on the management network.
15. To continue the configuration, accept the certificate and continue. The option to continue varies according to the web browser you are using.
16. To complete the configuration process, see Provisioning the Appliance.
Provisioning the Appliance

Aug 12, 2014

After assigning an IP address to the management service, you are ready to provision the NetScaler and accelerator instances. As soon as you log on to the appliance, the configuration wizard appears.

When using the configuration wizard, keep the following points in mind:

- The following procedure assumes that you have already filled out the configuration worksheet.
- If you change the IP addresses of the Management Network, or change the default gateway to an address not on the Management Network, you lose connectivity to the appliance unless you are on the same Ethernet segment as the management port.
- When using the configuration wizard, check your entries carefully. The wizard has no Back button. If you need to modify the previous screen, use the Back button on your browser. This takes you to the logon page, then to the previous screen.
- The configuration wizard is displayed only when you log on to the appliance for the first time to configure the appliance. After you finish configuring the appliance, this wizard becomes inaccessible, and will reappear only after a factory reset. Check your entries carefully.

This wizard walks you through a fresh configuration of the appliance.

Note: If you receive a #SESS_CORRUPTED error at any time during these procedures, click Logout, clear your browser cache, close your browser, and open it again.

To configure the appliance by using the configuration wizard:

1. On the Welcome page, click Get Started.
   
   Note: All pages after the Get Started page have a heading that says, “Deployment Mode: Inline/L2 Mode,” but this wizard is used for all deployment modes.

2. Follow these steps to configure a fully 7.3-compliant system:
   
   - Acquire the following release 7.3 software distributions from the release 7.3 downloads page on My Citrix:
     - Management service (as a .tgz file)
     - NetScaler VM (as an .xva file)
     - Accelerator VM (as an .xva file)
     - Upgrade bundle (as a .upg) file
   
   - Navigate to the System > Configuration > Management Service > Software Images page, and then select Upload from the Action list.
   
   - Upload a release 7.3 Management Service image (distributed as a .tgz file).
   
   - Navigate to the System > Configuration > NetScaler > Software Images page, and then upload a release 7.3 NetScaler XVA image.
   
   - Navigate to the System > Configuration > SD-WAN > Software Images page, and then upload the accelerator XVA image.
   
   - Navigate to the System > Configuration > Management Service page, and then click the Upgrade Management Service link.
   
   - Select the management service image that you recently uploaded and click OK.
   
   - When the lower left-hand corner of the screen displays “Management Service Updated Successfully,” log off and clear your browser cache. Log on after the management service restarts (a few minutes).
   
   - On the Welcome screen, click Get Started.

3. For Management Access Settings, specify values for the various fields according to the network settings. The following
screen shot displays sample values used in this documentation. Enter values as follows:

- **XenServer IP Address**—(Item M4 on your worksheet, or H4 if this is the second appliance in an HA pair.) The management address of the built-in XenServer hypervisor. This must be a valid address on the management network.

- **Management Service IP Address**—(Item M5 on your worksheet, or H5 if this is the second appliance in an HA pair.) The address of the Management Service VM that you use to perform most system management tasks. This must be a valid address on the management network.

- **Netmask**—(Item M3 on your worksheet). The subnet mask of the management network.

- **Gateway**— (Item M2 on your worksheet). The default gateway for the management network.

- **DNS Server**—The IP address of the DNS server. This is a mandatory parameter.

- **NTP Server**—IP or FQDN address of your time server. This will be used by all the virtual machines in the appliance.
  
  Note that if you use advanced CIFS or MAPI acceleration, the system time of the appliance must be close to that of the Windows domain server, so choose an NTP server that maintains a close relationship to the time on your Windows domain server.

  Note: Unless the NTP server is specified as an IP address, it is not used by the accelerator.

- **Time Zone**—Select your time zone from the pull-down menu.

- **Change Password**—Select this check box and type in a new nsroot password, two times, to change the password.
  
  This same password is used on the management service and the NetScaler instance for account nsroot, and on the accelerator for the admin account. If the password is not changed, it remains set to nsroot (the default).

Figure 1. Sample Values for the Fields in Management Access Settings Page of the Configuration Wizard

4. Check your settings and click **Continue**.

5. In the Manage Licenses section, see if an appropriate license is already listed in the Name field. If so, select it and skip to step 8.

6. Click **Upload** in the Update Licenses section.

7. Navigate to the folder that contains the license file and open the file.

8. Click **Add License** and upload the license file provided by Citrix. The license is added to the appliance, as shown in the following figure.

Figure 2. Sample License Added to the Appliance on the Manage License Files Page of the Configuration Wizard

You can also get a license file from the Citrix.com website by clicking the **here** link and using your My Citrix credentials.

9. Select the license in the Name field and click **Continue**. The SD-WAN Setup page appears. Fill in the fields as follows:

1. **Network Settings**—This section informs the accelerators of the management network.
   - **SD-WAN Accelerator IP Address**—Enter the value of M6 from your worksheet. This is the IP address of the accelerator.
   - **NetScaler IP Address**—Enter the value of M7 from your worksheet. This is the IP address of the NetScaler GUI.
   - **Use System Netmask and Gateway**—Select this option if you want to use the network mask and gateway IP addresses you had specified in the Platform Configuration page.
   - **Netmask**—Enter the value of M3 from your worksheet. This is the subnet mask (netmask) of the management network (note that you have entered this already, on a previous page).
   - **Gateway**—Enter the value of M2 from your worksheet again.
   - **Signaling IP Address**—Enter the value of T4 from your worksheet. This is the external signaling IP address of the accelerator, used by SD-WAN Plug-ins to connect to the appliance.
2. **Signaling Netmask**—Enter the value of T2 from your worksheet. This is the subnet mask (netmask) of the external traffic network.

3. **XVA Files**—This section allows you to specify previously uploaded XVA files (Xen virtual machines) for the NetScaler and accelerator instances. Select the XVA images that you uploaded as part of step 2.

   Figure 3. SD-WAN Setup Page

10. Click **Continue**. The wizard starts provisioning the required instances, as shown in the following figure.

    Figure 4. Provisioning Progress Indicator

11. After the instances are provisioned, add one of your local LAN subnets to the Link Configuration section from list T7 in your worksheet, as shown in the following figure. This subnet will be added as a local LAN subnet in the accelerator. If you have more than one LAN subnet, you can add them to the LAN link definition in the Accelerator GUI after the configuration wizard completes. Click Add to add the subnet.

    Figure 5. Link Configuration Is at the Bottom of This Page

12. Log off, and then log back on. If you see a “Version Incompatibility Detected” message, install the upgrade bundle you downloaded in Step 2, using the procedure in Managing the Appliance by using the Management Service.

   Basic configuration is complete. Next, perform deployment-mode-specific configuration (such as for WCCP mode).

   Note: After the wizard completes, the appliance is configured for the basic setup. To configure the appliance for a specific deployment scenario, see Deployment Modes.
Deployment Modes

Aug 08, 2013

SD-WAN 4000/5000 appliances have two recommended deployment modes: WCCP and inline. These modes are commonly used without high availability (HA), and less commonly with HA.

At this time, Citrix recommends WCCP mode, with a single router and without HA, for most deployments. Use inline mode when WCCP is not available.

Although not all of the following modes are recommended at this time, they are all supported:

- WCCP mode with a single router
- WCCP mode with a single router and high availability
- Cascade of two or more appliances in WCCP mode along with a NetScaler MPX Appliance
- Cascade of two or more appliances in WCCP mode along with a NetScaler MPX Appliance in HA
- Inline mode
- Inline mode in HA
- Virtual inline mode
- Virtual inline mode in HA

Note: While modes other than WCCP and inline are supported, they are incompletely documented and are not recommended for typical installations. Please contact your Citrix representative when considering one of these modes.
Virtual Inline Mode

Jan 28, 2011

In virtual inline mode, the router uses policy based routing (PBR) rules to redirect incoming and outgoing WAN traffic to the appliance for acceleration, and the appliance forwards the processed packets back to the router.

Virtual inline mode provides a solution for asymmetric routing issues faced in a deployment with two or more WAN links.

Note: Citrix recommends that you do not deploy SD-WAN appliances in virtual inline mode with routers that do not support health monitoring.

The tasks for configuring virtual inline mode are performed on the router. On the SD-WAN appliance, just verify that the software version supports virtual inline mode and provision the instances with the necessary IP addresses. Do not change the default forwarding method.
Validated Designs

Jan 28, 2011

The physical mode for virtual inline deployment of a SD-WAN appliance is one-arm mode. In a one-arm topology with multiple subnets, the branches, local Repeater instances, and servers can exist on different subnets. For example, you can deploy the appliance in one-arm mode for managing the Repeater instances, with the NetScaler and local Repeater instances connected by the internal private subnet. A NetScaler-owned subnet IP address (SNIP) is used to communicate with an accelerator instance. You must enable MAC Based Forwarding (MBF) Use Subnet IP address (USNIP), and Return To Ethernet Sender options on the NetScaler instance.

This section contains Citrix validated deployment topologies for virtual inline mode.
Single Router and single link

Jan 28, 2011
A SD-WAN appliance deployed in virtual inline mode with one router and one link.

If you are deploying a SD-WAN appliance in virtual inline mode with one router and one link, complete the following procedures:
- Enable Layer 3 Mode
- Enable the Return to Ethernet Sender Mode
- Add a Subnet IP Address
- Bind the Subnet IP Address to VLAN of Data Interface
- Configure a Router
Two routers and a single link

Jan 28, 2011
A SD-WAN appliance deployed in virtual inline mode with two routers and one link.

If you are deploying a SD-WAN appliance in virtual inline mode with two routers and a single link, complete the following procedures:

- Enable Layer 3 Mode
- Enable the Return to Ethernet Sender Mode
- Add a Subnet IP Address
- Bind the Subnet IP Address to VLAN of Data Interface
- Configure a Router (both routers individually)
Two routers and two links

Jan 28, 2011
A SD-WAN appliance deployed in virtual inline mode with two routers and two links.

If you are deploying a SD-WAN appliance in virtual inline mode with two routers and a single link, complete the following procedures:

- Enable Layer 3 Mode
- Enable the Return to Ethernet Sender Mode
- Add a Subnet IP Address
- Bind the Subnet IP Address to VLAN of Data Interface
- Configure Layer 4 Parameters (only if you expect connection migration between routers)
- Configuring VLANs for Connection Migration
- Configure a Router (both routers individually)
Two routers in High Availability setup

Jan 28, 2011
A SD-WAN appliance deployed in virtual inline mode with two routers in high availability setup and one link.

If you are deploying a SD-WAN appliance in virtual inline mode with two routers and a single link, complete the following procedures:

- Enable Layer 3 Mode
- Enable the Return to Ethernet Sender Mode
- Add a Subnet IP Address
- Bind the Subnet IP Address to VLAN of Data Interface
- Configure a Router (both routers individually)
- Configure Routers in High Availability Setup
Deployment Worksheet

Jan 28, 2011

The appliance uses at least two ports: the management port (typically 0/1) and the traffic port (such as 10/1). You must select ports in advance, because the configuration depends on the identity of the ports.

The appliance uses three subnets directly: the management subnet, the external traffic subnet, and the internal traffic subnet. Multiple IP addresses are used on each subnet. Each subnet must be specified along with the correct subnet mask.

The following figure is a worksheet for these parameters. It supports inline and virtual inline modes, with and without HA. The table below the figure describes what each entry means.

### Deployment Worksheet Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Example</th>
<th>Your Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management Subnet</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M2. Gateway IP address</td>
<td>10.199.79.254</td>
<td></td>
<td>Default gateway serving the management subnet.</td>
</tr>
<tr>
<td>M3. Subnet Mask</td>
<td>255.255.255.128</td>
<td></td>
<td>Subnet mask for the management subnet.</td>
</tr>
<tr>
<td>M4. Xen Hypervisor IP address</td>
<td>10.199.79.225</td>
<td></td>
<td>IP address of Xen Hypervisor.</td>
</tr>
<tr>
<td>M5. Service VM IP address</td>
<td>10.199.79.226</td>
<td></td>
<td>IP address of Management Service VM, which controls configuration.</td>
</tr>
<tr>
<td>M6. Accelerator UI</td>
<td>10.199.79.227</td>
<td></td>
<td>Accelerator GUI, also called the Broker UI, which manages the instances as a unit.</td>
</tr>
<tr>
<td>M7. NetScaler Management IP address</td>
<td>10.199.79.245</td>
<td></td>
<td>IP address of the NetScaler instance's GUI and CLI interfaces.</td>
</tr>
<tr>
<td><strong>External Traffic Subnet</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1. Router IP address</td>
<td>172.17.17.1</td>
<td></td>
<td>IP address of the first router on external traffic subnet.</td>
</tr>
<tr>
<td>T2. Router IP address</td>
<td>172.17.18.1</td>
<td></td>
<td>IP address of the second router on external traffic subnet.</td>
</tr>
<tr>
<td>T3. Subnet Mask</td>
<td>255.255.255.0</td>
<td></td>
<td>Subnet mask of external traffic subnet.</td>
</tr>
<tr>
<td>T4. Subnet IP address</td>
<td>172.17.17.2</td>
<td></td>
<td>Subnet IP address for NetScaler on external traffic subnet.</td>
</tr>
<tr>
<td>T5. Subnet IP address</td>
<td>172.17.18.2</td>
<td></td>
<td>Subnet IP address for NetScaler on external traffic subnet.</td>
</tr>
<tr>
<td></td>
<td>Parameter</td>
<td>Example</td>
<td>Your Value</td>
</tr>
<tr>
<td>---</td>
<td>-------------------------------</td>
<td>-----------------</td>
<td>------------</td>
</tr>
<tr>
<td>T6</td>
<td>External Signaling IP address</td>
<td>172.17.17.10</td>
<td></td>
</tr>
<tr>
<td>T7</td>
<td>Local LAN Subnets</td>
<td>10.200.0.0/16</td>
<td></td>
</tr>
<tr>
<td>T8</td>
<td>Traffic Port</td>
<td>10/1</td>
<td></td>
</tr>
<tr>
<td>T9</td>
<td>Traffic Port</td>
<td>10/6</td>
<td></td>
</tr>
</tbody>
</table>

Note: Ports 10/3 and 10/4 are reserved for loopback cable. Do not configure these ports as traffic ports.
Configuring the NetScaler Instance

Jan 28, 2011
By default, the Getting Started wizard configures the appliance in inline mode. To deploy the SD-WAN appliance in virtual inline mode, you must configure the NetScaler instance of the appliance to support this mode.

To configure the NetScaler instance for the virtual inline mode of the appliance:

- Enable L3 Mode
- Enable the Return to Ethernet Sender Mode
- Add a Subnet IP Address
- Bind the Subnet IP Address to VLAN of Data Interface
- Configuring the Instance for Connection Migration
Enable Layer 3 Mode

Jan 31, 2011

In the inline mode, the default deployment mode of the appliance, the appliance uses layer 2 bridging. However, to deploy the appliance in virtual inline mode, you must enable layer 3 mode and disable layer 2 mode on the appliance.

To enable layer 3 mode and disable layer 2 mode by using the configuration utility

1. Access the NetScaler instance by clicking the NetScaler instance’s IP address on the Configuration > Instances > NetScaler page. You are logged on to the NetScaler instance automatically.
2. Navigate to the System > Settings page.
3. Click the Configure modes link.
4. In the Configure Modes dialog box, select Layer 3 Mode (IP Forwarding) option.
5. Clear the Layer 2 Mode option, as shown in following figure.
6. Click OK.

To enable layer 3 mode and disable layer 2 mode by using the command line interface, run the following commands

> enable ns mode L3
> disable ns mode L2
Enable the Return to Ethernet Sender Mode

Jan 31, 2011

This mode allows multiple routers to share an appliance. The appliance forwards virtual inline output packets back to where they came from, as indicated by the Ethernet address of the incoming packet. If two routers share a single appliance, each gets its own traffic back, but not the traffic from the other router. This mode also works with a single router.

**To enable the Return to Ethernet Sender mode by using the configuration utility**

1. Navigate to the System > Network page.
2. Click the Configure Layer 2 Parameter link, as shown in the following figure.
3. In the Configure Layer 2 Parameter dialog box, select the Return to Ethernet Sender option, as shown in the following figure.
4. Click OK.

**To enable the Return to Ethernet Sender mode by using the command line interface, run the following command**

> set L2Param -returnToEthernetSender ENABLED
Add a Subnet IP Address

Jan 31, 2011
You must add a Subnet IP (SNIP) address to the NetScaler instance. You assign this IP address to the NetScaler instance on the external traffic subnet. The NetScaler instance uses this address to communicate with the router.

To add a subnet IP address to the instance by using the configuration utility

1. Navigate to the System > Network > IPs page.
2. Click Add, as shown in the following figure.
3. In the Create IP dialog box, specify a subnet IP address in the IP Address field if the address has not already been created by the configuration wizard. (If it has already been created, it is listed on the IPs page). The subnet IP address declares the external traffic network. In the IP Address field, type the NetScaler traffic IP address (entry T4 in your worksheet).
4. In the Netmask field, specify the network mask (entry T3 in your worksheet).
5. From the IP Type group, make sure that the Subnet IP option is selected, as shown in the following figure.
6. Click Create and then Close.
7. If you are configuring the appliance for two links, repeat this procedure to create another subnet IP address (entry T5 of your worksheet).

To add a Subnet IP address to the instance by using the command line interface, run the following command

> add ns ip 172.17.17.2 255.255.255.0
> add ns ip 172.17.18.2 255.255.255.0

Note: Run the second command only if you are configuring the appliance for two links.
Bind the Subnet IP Address to VLAN of Data Interface

Jan 31, 2011

After adding a subnet IP address to the instance, you must bind the IP address to the VLAN of data interface you are using on the instance. By default, the VLAN 1007 is bound to the 10/1 and 10/2 interfaces.

To bind the subnet IP address to VLAN of data interface from the configuration utility

1. Navigate to the System > Network > VLANs page.
2. Select the VLAN, such as 1007, that was created when provisioning the instances.
3. Click Open, as shown in the following figure.

4. In the Interface Bindings tab of the Configure VLAN dialog box, notice that the VLAN is bound to interfaces 10/1 (entry T9 of your worksheet) and 10/2.

5. In the IP Bindings tab, select the subnet IP address you have created, as shown in the following figure.

6. Click Create and then Close.
7. If you are configuring the appliance for two links, repeat this procedure to bind second subnet IP (entry T5 of your worksheet) to another VLAN, such as 1009.

To bind the subnet IP addresses to VLANs of data interface by using the command line interface, run the following command:

> bind vlan 1007–IPAddress 172.17.17.2 255.255.255.0
> bind vlan 1009–IPAddress 172.17.18.2 255.255.255.0

Note: Run the second command only if you are configuring the appliance for two links.
Configuring the Instance for Connection Migration

Sep 09, 2014
In your network setup, if you expect connection migration between the routers, then you must configure the layer 4 parameters and make changes to the VLAN configurations, appropriately.

Configure Layer 4 Parameters
If you have two routers and expect connection migration between the routers, you must configure layer 4 parameters on the NetScaler instance.

To configure layer 4 parameters from the configuration utility
1. Navigate to the System > Network page.
2. Click the Configure Layer 2 Parameter link, as shown in the following figure.
3. In the Configure Layer 4 Parameter dialog box, select the VLAN from the L2 Connection Method list, as shown in the following figure.
4. Click OK.

To bind the subnet IP address to VLAN of data interface by using the command line interface, run the following command
> set L4Param –l2connMethod vlan

Configuring VLANs for Connection Migration
If the network has two links and connected to interfaces that are bound to different VLANs, then you must bind the interfaces to the same VLAN to enable connection migration. Additionally, you must bind both subnet IP addresses to the same VLAN. Skip this procedure if you are using interfaces that are bound to the same VLAN.

To configure VLANs for connection migration by using the configuration utility
1. Navigate to the System > Network > VLANs page.
2. Select the VLAN, such as 1009, to which interface and subnet IP address of the second link is bound.
3. Click Open.
4. In the Interface Bindings tab of the Configure VLAN dialog box, clear the interface you are using (entry T9 of your worksheet), as shown in the following screen shot.
5. In the IP Bindings tab, clear the entry for subnet IP address bound to the VLAN.
6. Click OK.
7. Open the VLAN, such as 1007, to which you want to bind the data interface.
8. In the Interface Binding tab, select the data interface (entry T9 in your worksheet).
9. In the IP Bindings tab, select the subnet IP address (entry T5 in your worksheet) you just unbound from the other VLAN.
10. Click OK.

To configure VLANs for connection migration by using the command line interface, run the following commands
> unbind vlan 1009 –ifnum 10/6
> unbind vlan 1009 –IPAddress 172.17.18.2 255.255.255.0

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.764
> bind vlan 1007 –ifnum 10/6
> bind vlan 1007 –IPAddress 172.17.18.2 255.255.255.0
Configuring a Router

Jan 28, 2011

To support virtual inline mode, a router must forward incoming as well as outgoing WAN traffic to the SD-WAN appliance. After the appliance processes the traffic, the router must forward the incoming traffic from the appliance to the LAN and the outgoing traffic from the appliance to the WAN. You have to configure policy based rules to avoid routing loops. In addition, the router must monitor the health of the appliance so that the appliance can be bypassed if it fails.

If the router supports the Reverse Path Forwarding feature, you must disable the feature on the interfaces with policies to redirect traffic to a SD-WAN appliance, including the interface that is connected to the appliance. Otherwise, the router intermittently drops traffic. By default, the Reverse Path Forwarding feature is enabled on the router.

Note: If the network has two routers, configure the following procedures for each router using appropriate IP addresses identified in the worksheet.

In the virtual inline mode, the packet forwarding methods can create routing loops if the routing rules do not distinguish between a packet that has been forwarded by the appliance and one that has not. You can use any method that makes that distinction.

A typical method involves dedicating one of the Ethernet ports of the router to the appliance and creating routing rules based on the Ethernet port on which packets arrive. Packets that arrive on the interface dedicated to the appliance are never forwarded back to the appliance, but packets arriving on any other interface can be.

Traffic shaping is not effective unless all WAN traffic passes through the appliance. Following is the basic routing algorithm:

- Do not forward packets from the appliance back to the appliance.
- If the packet arrives from the WAN, forward the packet to the appliance.
- If the packet is destined for the WAN, forward the packet to the appliance.
- Do not forward LAN-to-LAN traffic to the appliance.

If the appliance fails, data should not be routed to it. By default, Cisco policy based routing does not perform health monitoring. To enable health monitoring, define a rule to monitor the availability of the appliance, and specify the "verify-availability" option for the "set ip next-hop" command. With this configuration, if the appliance is not available, the route is not applied, and the appliance is bypassed.

Note: Citrix recommends virtual inline mode only when used with health monitoring. Many routers that support policy based routing do not support health checking. The health-monitoring feature is relatively new. It was first available in Cisco IOS release 12.3(4)T.

Following is an example of a rule for monitoring the availability of the appliance by using Cisco Router model 7600 with IOS Software version:

```
!- Use a ping (ICMP echo) to see if appliance is in the connected track
123 rtr 1 reachability
!
  rtr 1
type echo protocol icmp echo 17.17.17.2 schedule 1 life forever start-time now
This rule pings the appliance at 17.17.17.2 periodically. You can test against 123 to see if the unit is up.
```
Following is an example of configuring a Cisco router for virtual inline mode:

!”
!”For health-checking to work, do not forget to start
!”the monitoring process.
!”
!”Original configuration is in normal type.
!”appliance-specific configuration is in bold.
!”
ip cef
!”
interface FastEthernet0/0
ip address 10.200.51.0 255.255.255.0
ip policy route-map server_side_map
!”
interface FastEthernet0/1
ip address 17.17.17.1 255.255.255.0!
interface FastEthernet1/0
ip address 192.168.1.5 255.255.255.0
ip policy route-map wan_side_map
!”
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.1.1
!”
ip access-list extended server_side
permit ip 10.100.51.0 0.0.0.255 10.20.20.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.20.20.0 0.0.0.255 10.100.51.0 0.0.0.255
!”
route-map wan_side_map permit 20
match ip address wan_side
!- Now set the appliance as the next hop, if it's up.
set ip next-hop verify-availability 17.17.17.1 20 track 123
!”
route-map client_side_map permit 10
match ip address client_side
set ip next-hop verify-availability 17.17.17.1 10 track 123
This example applies an access list to a route map and attaches the route map to an interface. The access lists identify all traffic originating at one accelerated site and terminating at the other (A source IP address of 10.100.51.0/24 and destination IP address of 10.20.20.0/24 or vice versa). See your router's documentation for the details of access lists and route-maps.

This configuration redirects all matching IP traffic to the appliances. If you want to redirect only TCP traffic, you can change the access-list configuration as follows (only the remote side's configuration is shown here):
!”
ip access-list extended server_side
permit tcp 10.200.51.0 0.0.0.255 10.20.20.0 0.0.0.255
ip access-list extended wan_side
permit tcp 10.20.20.0 0.0.0.255 10.200.51.0 0.0.0.255
!

To configure high availability between routers, see the router-specific high availability configuration manual.
Verifying the Virtual Inline Mode

Jan 28, 2011

By default, the HTTP and CIFS acceleration is enabled on the appliance. After you have successfully configured the appliance in the virtual inline deployment mode, the appliance starts accelerating these connections.

Note: To configure application-specific connections, you must configure service classes for the respective applications. To configure a service class, see http://support.citrix.com/proddocs/topic/SD-WAN-72/cb-traffic-classification-con.html.

To verify that you have successfully configure the appliance in the virtual inline mode

1. Send network traffic through the appliance.
2. Navigate to the SD-WAN > Monitoring > Optimization > Connections page.
3. Verify that the Accelerated Connections tab displays entries for the accelerated connections, as shown in the following screen shot. This tab displays an entry each for all accelerated connections.

Figure 1. The Accelerated Connections tab
WCCP Mode

Sep 11, 2014

Web Cache Communication Protocol (WCCP) is a dynamic routing protocol introduced by Cisco. Originally intended only for web caching, WCCP version 2 became a more general-purpose protocol, suitable for use by accelerators such as Citrix SD-WAN appliances.

WCCP mode is the simplest way of installing a SD-WAN appliance when inline operation is impractical. It is also useful where asymmetric routing occurs, that is, when packets from the same connection arrive over different WAN links. In WCCP mode, the routers use the WCCP 2.0 protocol to divert traffic through the appliance. Once received by the appliance, the traffic is treated by the acceleration engine and traffic shaper as if it were received in inline mode.

Note:
- For the purposes of this discussion, WCCP version 1 is considered obsolete and only WCCP version 2 is presented.
- The standard WCCP documentation calls WCCP clients “caches.” To avoid confusion with actual caches, Citrix generally avoids calling a WCCP client a “cache.” Instead, WCCP clients are typically called “appliances.”
- This discussion uses the term “router” to indicate WCCP-capable routers and WCCP-capable switches. Though the term “router” is used here, some high-end switches also support WCCP, and can be used with SD-WAN appliances.

The SD-WAN appliances support two WCCP modes:
- WCCP is the original SD-WAN WCCP offering supported since release 3.x. It supports a single appliance service group (no clustering).
- WCCP clustering, introduced in release 7.2, allows your router to load-balance traffic between multiple appliances.

The physical mode for WCCP deployment of a SD-WAN appliance is one-arm mode in which the SD-WAN appliance is connected directly to a dedicated port on the WAN router. The WCCP standard includes a protocol negotiation in which the appliance registers itself with the router, and the two negotiate the use of features they support in common. Once this negotiation is successful, traffic is routed between the router and the appliance according to the WCCP router and redirection rules defined on the router.

A WCCP-mode appliance requires only a single Ethernet port. The appliance should either be deployed on a dedicated router port (or WCCP-capable switch port) or isolated from other traffic through a VLAN. Do not mix inline and WCCP modes.

The following figure shows how a router is configured to intercept traffic on selected interfaces and forward it to the WCCP-enabled appliance. Whenever the WCCP-enabled appliance is not available, the traffic is not intercepted, and is forwarded normally.

Figure 1. WCCP Traffic Flow

WCCP allows traffic to be forwarded between the router and the appliance in either of the following modes:
- L2 Mode—Requires that the router and appliance be on the same L2 segment (typically an Ethernet segment). The IP packet is unmodified, and only the L2 addressing is altered to forward the packet. In many devices, L2 forwarding is
performed at the hardware layer, giving it the maximum performance. Because of its performance advantage, L2 forwarding is the preferred mode, but not all WCCP-capable devices support it.

- GRE Mode—Generic Routing Encapsulation (GRE) is a routed protocol and the appliance can in theory be placed anywhere, but for performance it should be placed close to the router, on a fast, uncongested path that traverses as few switches and routers as possible. GRE is the original WCCP mode. A GRE header is created and the data packet is appended to it. The receiving device removes the GRE header. With encapsulation, the appliance can be on a subnet that is not directly attached to the router. However, both the encapsulation process and the subsequent routing add CPU overhead to the router, and the addition of the 28-byte GRE header can lead to packet fragmentation, which adds additional overhead.

WCCP mode supports multiple routers and both GRE vs. L2 forwarding. Each router can have multiple WAN links. Each link can have its own WCCP service group.

Traffic shaping is not effective unless the appliance manages UDP traffic as well as TCP traffic. A second service group, with a UDP service group for each WAN link, is recommended if traffic shaping is desired.

A WCCP client (an appliance) uses UDP port 2048 to register itself with the router and to negotiate which traffic should be sent to it, and also which WCCP features should be used for this traffic. The appliance operates on this traffic and forwards the resulting traffic to the original endpoint. The status of an appliance is tracked through the WCCP registration process and a heartbeat protocol. The appliance first contacts the router over the WCCP control channel (UDP port 2048), and the appliance and router exchange information with packets named “Here_I_Am” and “I_See_You,” respectively. By default, this process is repeated every ten seconds. If the router fails to receive a message from the appliance for three of these intervals, it considers the appliance to have failed and stops forwarding traffic to it until contact is reestablished.

Different appliances using the same router can provide different services. To keep track of which services are assigned to which appliances, the WCCP protocol uses a service group identifier, a one-byte integer. When an appliance registers itself with a router, it includes service group numbers as well.

- A single appliance can support more than one service group.
- A single router can support more than one service group.
- A single appliance can use the same service group with more than one router.
- A single router can use the same service group with more than one appliance. For SD-WAN appliances, multiple appliances are supported in WCCP cluster mode, and a single appliance is supported in WCCP mode.
- Each appliance specifies a “return type” (L2 or GRE) independently for each direction and each service group. SD-WAN 4000/5000 appliances always specify the same return type for both directions. Other SD-WAN appliances allow the return type to be different.

Multiple service groups can be used with WCCP on the same appliance. For example, the appliance can receive service-group 51 traffic from one WAN link and service-group 62 traffic from another WAN link. The appliance also supports multiple routers. It is indifferent to whether all the routers use the same service group or different routers use different service groups.

Service Group Tracking. If a packet arrives on one service group, output packets for the same connection are sent on
the same service group. If packets arrive for the same connection on multiple service groups, output packets track the most recently seen service group for that connection.

When WCCP is used with high-availability mode, the primary appliance sends its own apA or apB management IP address, not the virtual address of the HA pair, when it contacts the router. If failover occurs, the new primary appliance contacts the router automatically, reestablishing the WCCP channel. In most cases the WCCP timeout period and the HA failover time overlap. As a result, the network outage is less than the sum of the two delays.

Standard WCCP allows only a single appliance in a WCCP service group. If a new appliance attempts to contact the router, it discovers that the other appliance is handling the service group, and the new appliance sets an Alert. It periodically checks to determine whether the service group is still active with the other appliance, and the new appliance handles the service group when the other appliance becomes inactive. WCCP clustering allows multiple appliances per service group.

The following figure shows a simple WCCP deployment, suitable for either L2 or GRE. The traffic port (1/1) is connected directly to a dedicated router port (Gig 4/12).

Figure 3. Simple WCCP deployment

In this example, the SD-WAN 4000/5000 is deployed in one-arm mode, with the traffic port (1/1) and the management port (0/1) each connecting to its own dedicated router port.

On the router, WCCP is configured with identical ip wccp redirect in statements on the WAN and LAN ports. Two service groups are used, 71 and 72. Service group 71 is used for TCP traffic and service group 72 is used for UDP traffic. The SD-WAN appliance does not accelerate UDP traffic, but can apply traffic shaping policies to it.

Note: The WCCP specification does not allow protocols other than TCP and UDP to be forwarded, so protocols such as ICMP and GRE always bypass the appliance.

SD-WAN release 7.2 or later supports WCCP clustering, which enables your router to load-balance your traffic between multiple appliances. For more information about deploying SD-WAN appliances as a cluster, see WCCP Clustering.

WCCP Mode (Non-Clustered)

Sep 11, 2014

WCCP mode allows only a single appliance in a WCCP service group. If a new appliance attempts to contact the router, it discovers that the other appliance is handling the service group, and the new appliance sets an Alert. It periodically checks to determine whether the service group is still active with the other appliance, and the new appliance handles the service group when the other appliance becomes inactive.

Note: WCCP clustering allows multiple appliances per service group.

Following are limitations and best practices for (non-clustered) WCCP mode:

- On appliances with more than one accelerated pair, all the traffic for a given WCCP service group must arrive on the same accelerated pair.
- Do not mix inline and WCCP traffic on the same appliance. The appliance does not enforce this guideline, but violating it can cause difficulties with acceleration. (WCCP and virtual inline modes can be mixed, but only if the WCCP and virtual inline traffic are coming from different routers.)
- For sites with a single WAN router, use WCCP whenever inline mode is not practical.
- Only one appliance is supported per service group. If more than one appliance attempts to connect to the same router with the same service group, the negotiation will succeed only for the first appliance.
- For sites with multiple WAN routers serviced by the same appliance, WCCP can be used to support one, some, or all of your WAN routers. Other routers can use virtual inline mode.
Configuring WCCP

Sep 12, 2014

A WCCP deployment follows the same initial steps as an inline deployment, but has additional steps beyond the basic inline procedure.

Perform the following tasks if you have not done so already:

- Install the SD-WAN hardware. See Installing the Hardware.
- Fill out the Deployment Worksheet and perform the initial configuration. See .
- If you are using high-availability mode, see the Configuring the High Availability Setup on the Appliances section before proceeding.

The following high-level procedure summarizes the WCCP installation process, which works for both GRE and L2 forwarding and for any number of routers and links.

**To configure WCCP mode**

Note: You must follow the hyperlinks and follow the detailed instructions for each step.

1. **Configuring the Router**.
   1. Enable WCCP globally.
   2. Disable reverse path forwarding if your router supports it.
   3. Configure WCCP service groups.
2. **Configuring Accelerators for WCCP Negotiation**.
   1. Enable WCCP.
   2. For each service group:
      1. Create a service group definition on the SD-WAN appliance.
      2. Verify that this service group establishes WCCP communication with its associated routers.
3. **Verifying WCCP Mode**.
4. If using high-availability mode, configure and test the second appliance, then complete the Configuring the High Availability Setup on the Appliances procedure.

Note: This information is for WCCP mode. For WCCP Clustering, see the SD-WAN WCCP Clustering topics, especially the Configuring the Router subtopic.

For each WCCP router:

1. Enable WCCP in global router configuration.
2. For each WCCP service group on the worksheet for this router, declare ip wccp <sg> in global router configuration.
3. Referring to the configuration examples below, for each WAN interface on this router:
   1. You can either use Method A or Method B to configure the router:
      - Method A: On the WAN interface only, declare ip wccp <sg> redirect in and ip wccp <sg> redirect out for the two service groups associated with the WAN interface.
      - Method B: If there is only one WAN interface, you can alternatively declare ip wccp <sg> redirect in on the WAN interface and on every LAN interface except the appliance's traffic interface.
   2. If your router supports reverse path forwarding, disable it on this interface by changing any ip verify unicast reverse-
path commands to no ip verify unicast reverse-path commands on each interface that has an ip wccp redirect command.

4. Save the configuration.

**Router Configuration Examples**

For normal operation, you must declare WCCP version 2 and the WCCP group ID for the router as a whole, and then enable redirection on each WAN interface.

Either one or two WCCP service groups can be used, but two are recommended, so that both TCP and UDP can be redirected, allowing more accurate traffic shaping. The WCCP standard requires that TCP and UDP traffic use different service groups.

**Method A** is required if the router has multiple WAN interfaces.

Example

Following is an example of configuring a Cisco IOS router:

```plaintext
! This example is for WCCP mode, not WCCP clustering
! (which is covered elsewhere)
config term
ip wccp version 2
! The two service groups are T11 and T12 on the
! configuration worksheet
! We will use group 72 for TCP and 73 for UDP.
ip wccp 72
ip wccp 73

! Repeat the following lines for each WAN interface
! you wish to accelerate:
interface <WAN_Interface>

! If reverse-path forwarding is enabled, change any
! ip verify unicast reverse-path commands to
! no ip verify unicates reverse-path commands:
no ip verify unicast reverse-path
ip wccp 72 redirect out
ip wccp 72 redirect in
ip wccp 73 redirect out
ip wccp 73 redirect in
```

^Z

**Method B** is preferred in circumstances when the routers do not support the `wccp redirect out` statement.

Example

Following is an example of configuring a Cisco IOS router:

```plaintext
! This example is for WCCP mode, not WCCP clustering
```
! (which is covered elsewhere)
config term
ip wccp version 2
!
! The two service groups are T11 and T12 on the
! configuration worksheet
! We will use group 72 for TCP and 73 for UDP.
ip wccp 72
ip wccp 73

! Repeat the following lines for the WAN interface
! you wish to accelerate:
interface <WAN_Interface>
!
! If reverse-path forwarding is enabled, change any
! ip verify unicast reverse-path commands to
! no ip verify unicast reverse-path commands:
no ip verify unicast reverse-path
ip wccp 72 redirect in
ip wccp 73 redirect in

! Repeat the following lines for all the LAN interfaces
! EXCEPT those connected to the SD-WAN appliance:
interface <LAN_Interface>
!
! If reverse-path forwarding is enabled, change any
! ip verify unicast reverse-path commands to
! no ip verify unicast reverse-path commands:
no ip verify unicast reverse-path
ip wccp 72 redirect in
ip wccp 73 redirect in

^Z
Remember to save your router configuration when you are satisfied that it is correct.

One accelerator instance manages WCCP control traffic on behalf of all the instances. The WCCP control traffic is negligible. The actual data traffic is divided among all the accelerators.
Note: The GUI calls WCCP mode “single cache.”
Summary: To configure the accelerators for WCCP mode, first enable WCCP mode. Then, configure service groups and create a WAN link definition, on the SD-WAN appliance, for each WAN link on each WCCP router. (Each link has two service groups, one for TCP and one for UDP.) If a service group is already defined for a given link, add the current router’s IP address to the definition. Test the service group’s WCCP status before creating the WAN link definition, and verify link traffic and acceleration status before configuring the next WAN link.

To configure the accelerators for WCCP mode
1. On the SD-WAN appliance, Navigate to Configuration > Appliance Settings > Advance Deployments > WCCP page.

2. If the **Enable** button is displayed, click it to enable WCCP mode on the appliance. (If the Disable button is displayed, WCCP mode is already enabled.)
   Note: We will actually be configuring two caches.

3. In the Select Mode area, select **Single Cache**.

4. Starting with accelerator instance #1 (labeled “WCCP Cache 1” on the page), configure the SD-WAN IP Details by entering the external VIP you defined for accelerator instance 1 (T5 on your worksheet for instance #1, T6 for instance #2). Set the subnet mask for the external traffic network (T2 on your worksheet). Set the gateway IP for the external traffic network (T1 on your worksheet). Click Save. The Configure Service Group controls appear.

5. In the Configure Service Group section, click Add. An Add Service Group popup appears.

6. In the Service Group Details area, specify a WCCP service group ID in the ID field. This ID must match one of the service groups that you have defined on your router. Start with the lowest-numbered service group in your list (T11 for the TCP service class, T12 for the UDP service class).

7. In the WCCP Priority field, set the WCCP priority to 100 for instance #1, or to 80 for instance #2. (Other values work. Use a priority for instance #1 that is greater than the priority for instance #2, and use a priority for instance #2 that is greater than zero.)

8. From the Protocol list, select a protocol. You will perform this step for both TCP and UDP. Start with TCP.

9. In the Service Group Password field, enter a password if your router is configured to require one. Otherwise, leave the field blank.

10. In the Router Communications Details area, in the Router IP Address field, enter the IP address of the router. This is the router’s address for its appliance-facing interface (T8 on your worksheet). If you use multiple routers to communicate with the appliance, list them all here.

11. From the Router Assignment list, select a router assignment (Hash, Mask, or Auto). Auto is recommended. If Auto is selected, Hash is negotiated if the router supports it. Otherwise Mask is used.

12. From the Router Forwarding list, select **Level 2** or GRE. The same method must be used for both outbound and inbound packets. L2 is recommended whenever possible, as GRE adds overhead to both the router and the appliance. L2 requires that your router support Level 2, and that the router’s IP and the VIP addresses be in the same subnet. Otherwise, use GRE.

13. Click Create.

14. Repeat steps 6-13 with the next service group in sequence, but selecting UDP instead of TCP.

15. Repeat steps 4-14 for instance #2 (called “WCCP Cache 2” in the GUI), except that the Cache IP is T6 from your worksheet (instead of T5), and the WCCP priority value is 80 (instead of 100).

16. If desired, click Advanced Settings on the WCCP page and select a quicker timeout (Responsive or Tolerant, rather than Default). This is a WCCP 2.1 feature and is not supported by all routers. If the appliance has trouble connecting to the router, set this parameter back to Default.

Note: You must consider the following points when configuring a Citrix SD-WAN 4000/5000 appliance:

- Traffic is load balanced across the accelerators on the basis of NetScaler load balancing policies.
- The WCCP service group ID that you assign to the accelerator must match a service group defined on your router, or the WCCP negotiation fails.
Verifying WCCP Mode

Sep 11, 2014
You can monitor the WCCP configuration from the SD-WAN GUI.

To monitor the WCCP configuration
1. Navigate to the Monitoring > Appliance Performance > WCCP page.
2. Select a cache and click Get Info. A Cache Status page displays the WCCP configuration, as shown in the following figure.

3. Start traffic that should be forwarded through the SD-WAN appliance and monitor the connection on the Monitoring > Optimization > Connections page.
   - If the connections are shown on the Accelerated Connections tab, that is an indicator that everything is working.
   - If the connections are on the Unaccelerated Connections tab, look at the Details column. A routing asymmetry detected message implies that one of the ip wccp redirect lines on the router is missing or has an error, or that different paths are taken by client-server and server-client traffic.
   - If no connections are shown, but the appliance reports that it is connected to the router, and the WCCP monitoring page shows no errors, the issue is probably with the router configuration.
WCCP Clustering

Sep 12, 2014

The WCCP clustering feature enables you to multiply your acceleration capacity by assigning more than one SD-WAN appliance to the same links. You can cluster up to 32 identical appliances, for up to 32 times the capacity. Because it uses the WCCP 2.0 standard, WCCP clustering works on most routers and some smart switches, most likely including those you are already using.

Because it uses a decentralized protocol, WCCP clustering allows SD-WAN appliances to be added or removed at will. If an appliance fails, its traffic is rerouted to the surviving appliances.

Unlike SD-WAN high-availability, an active/passive pair that uses two appliances to provide the performance of a single appliance, the same appliances deployed as a WCCP cluster has twice the performance of a single appliance, delivering both redundancy and improved performance.

In addition to adding more appliances as your site’s needs increase, you can use Citrix’s “Pay as You Grow” feature to increase your appliances’ capabilities through license upgrades.

Citrix Command Center is recommended for managing WCCP clusters. The following figure shows a basic network of a cluster of SD-WAN appliances in WCCP mode, administered by using Citrix Command Center.

Figure 1. SD-WAN Cluster Administered by Using Citrix Command Center

The WCCP protocol supports up to 32 appliances in a fault-tolerant, load balanced array called a cluster. In the example below, three identical appliances (same model, same software version) are cabled identically and configured identically except for their IP addresses. Appliances using the same service groups with the same router can become a load balanced WCCP cluster. When a new appliance registers itself with the router, it can join the existing pool of appliances and receive its share of traffic. If an appliance leaves the network (as indicated by the absence of heartbeat signals), the cluster is rebalanced so that only the remaining appliances are used.

Figure 2. A load-balanced WCCP cluster with three appliances

One appliance in the cluster is selected as the designated cache, and controls the load-balancing behavior of the appliances in the cluster. The designated cache is the appliance with the lowest IP address. Because the appliances have identical configurations, it doesn’t matter which one is the designated cache. If the current designated cache goes offline, a different appliance becomes the designated cache.

The designated cache determines how the load-balanced traffic is allocated and informs the router of these decisions. The router shares information with all members of the cluster, so the cluster can operate even if the designated cache goes offline.

Note: As normally configured, a SD-WAN 4000/5000 appliance appears as two WCCP caches to the router.

Load-Balancing Algorithm

Load balancing in WCCP is static, except when an appliance enters or leaves the cluster, which causes the cluster to be rebalanced among its current members.
The WCCP standard supports load balancing based on a mask or a hash. For example, SD-WAN WCCP clustering uses the mask method only, using a mask of 1-6 bits of the 32-bit IP address. These address bits can be non-consecutive. All addresses yielding the same result when masked are sent to the same appliance. Load balancing effectiveness depends on choosing an appropriate mask value: a poor mask choice can result in poor load-balancing or even none, with all traffic sent to a single appliance.
Deployment Topology

Sep 11, 2014

Depending on your network topology, you can deploy WCCP cluster either with a single router or with multiple routers. Whether connected to a single router or multiple routers, each appliance in the cluster must be connected identically to all routers in use.

In the following diagram, three SD-WAN appliances accelerate the datacenter's 200 Mbps WAN. The site supports 750 XenApp users.

As shown on the SD-WAN Datasheet, a SD-WAN 3000-100 can support 100 Mbps and 400 users, so a pair of these appliances supports 200 Mbps and 800 users, which satisfies the datacenter's requirements of a 200 Mbps link and 750 users.

For fault tolerance, however, the WCCP cluster should continue to operate without becoming overloaded if one appliance fails. That can be accomplished by using three appliances when the calculations call for two. This is called the N+1 rule.

Failure is an unusual event, so usually all three appliances are in operation. In this case, each appliance is supporting only 67 Mbps and 250 users, leaving plenty of headroom and making good use of the fact that the cluster has three times the CPU power and three times the compression history of a single appliance.

Without WCCP clustering, the same level of capacity and fault-tolerance would require a pair of SD-WAN 4000-500 appliances in high availability mode. Only one of these appliances is active at a time.

Using multiple WAN routers is very similar to using a single WAN router. If the previous example is changed to include two 100 Mbps links instead of one 200 Mbps link, the topology changes, but the calculations do not.
Limitations

Sep 08, 2014

Configuring appliances in a WCCP cluster has the following limitations:

- All appliances within a cluster must be the same model and use the same software release.
- Parameter synchronization between appliances within the cluster is not automatic. Use Command Center to manage the appliances as a group.
- SD-WAN traffic shaping is not effective, because it relies on controlling the entire link as a unit, and none of the appliances are in a position to do this. Router QoS can be used instead.
- The WCCP-based load-balancing algorithms do not vary dynamically with load, so achieving a good load balance can require some tuning.
- SD-WAN traffic shaping is not effective, because it relies on controlling the entire link as a unit, and none of the appliances are in a position to do this. Router QoS can be used instead.
- The hash method of cache assignment is not supported. Mask assignment is the supported method.
- While the WCCP standard allows mask lengths of 1-7 bits, the appliance supports masks of 1-6 bits.
- Multicast service groups are not supported; only unicast service groups are supported.
- All routers using the same service group pair must support the same forwarding method (GRE or L2).
- The forwarding and return method negotiated with the router must match: both must be GRE or both must be L2. Some routers do not support L2 in both directions, resulting in an error of "Router's forward or return or assignment capability mismatch." In this case, the service group must be configured as GRE.
- SD-WAN VPX does not support WCCP clustering.
- The appliance supports (and negotiates) only unweighted (equal) cache assignments. Weighted assignments are not supported.
- Some older appliances, such as the SD-WAN 700, do not support WCCP clustering.
- (SD-WAN 4000/5000 only) Two accelerator instances are required per interface in L2 mode. No more than three interfaces are supported per appliance (and then only on appliances with six or more accelerator instances.)
- (SD-WAN 4000/5000 only) WCCP control packets from the router must match one of the router IP addresses configured on the appliance for the service group. In practice, the router's IP address for the interface that connects it to the appliance should be used. The router's loopback IP should not be used.
Planning Your Deployment

Jan 30, 2014
Deploying appliances in a WCCP cluster requires more planning than does deploying a single appliance. Read the following sections carefully before proceeding.
Selecting Appliances

Jan 30, 2014

The appliances you select for the deployment must all be the same model, running the same software version. Otherwise, management and troubleshooting can become impractical.

Your appliance choice is generally made by comparing your site’s WAN bandwidth and number of WAN users to the capacities of the different appliances in the SD-WAN Data Sheet. For fault tolerance, always order one more appliance than is absolutely required according to the data sheet.

The number of appliances you need is found as follows, rounding up all fractions:

\[
\text{appliances} = \max(\text{appliances}_\text{bw}, \text{appliances}_\text{users}),
\]

where

\[
\text{appliances}_\text{bw} = \left(\frac{\text{WAN bandwidth}}{\text{Optimized WAN capacity}}\right) + 1
\]

\[
\text{appliances}_\text{users} = \left(\frac{\text{WAN users}}{\text{Maximum HDX sessions}}\right) + 1
\]

Note that if \(\text{appliances} = 2\), you can use just a single appliance instead of WCCP clustering, or an HA pair instead of WCCP clustering, since the equation builds in a spare appliance. In other words, WCCP clustering is not necessary (from a capacity perspective) unless appliances is 3 or more.

**Example.** Suppose you have 700 users and a 100 Mbps link. Some appliances you might consider are the SD-WAN 2000-050, the SD-WAN 3000-100, and the SD-WAN 4000-310.

<table>
<thead>
<tr>
<th>Model</th>
<th>Optimized WAN Capacity</th>
<th>Maximum HDX Sessions</th>
<th>Appliances_bw</th>
<th>Appliances_users</th>
<th>Appliances</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000-050</td>
<td>50 Mbps</td>
<td>300</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3000-100</td>
<td>100 Mbps</td>
<td>400</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4000-310</td>
<td>310 Mbps</td>
<td>750</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

As you can see from the above table, the higher-performance platforms require fewer appliances to get the job done, as you would expect. The SD-WAN 4000-310 meets the requirements with a single appliance, and evaluates to two appliances only because the equations build in a spare.

You can always add more capacity by adding more appliances, but that is not always necessary. The bandwidth limits of two of the three choices, the SD-WAN 3000-100 and the SD-WAN 4000-310, can be increased through a license upgrade. The SD-WAN 2000-050 however, is already at the high end of the range for SD-WAN 2000 appliances.
Load-Balancing in the WCCP Cluster

Sep 12, 2014

Traffic is distributed among the appliances in the WCCP cluster. If an appliance leaves the cluster (through failure, overload, or being manually disabled), its traffic is rebalanced by distributing it among the surviving members. If an appliance joins the cluster, traffic is rebalanced once more to give the new appliance its fair share.

The Address Mask

Traffic is distributed on the basis of an address mask that is applied to the source and destination addresses of WAN traffic. You must select an appropriate mask field for efficient load-balancing. An inappropriate mask can result in load-balancing that is poor to nonexistent. For example, if the mask matches an address field that is identical at all your remote sites, all your WAN traffic is sent to a single appliance, overloading it. For example, if all of your remote sites have an address in the form of 10.0.x.x, and your mask bits are within the 10.0 portion of the address all traffic is sent to a single appliance.

The address bits extracted by the address mask are used as an index that is used (indirectly) to select one of the WCCP caches (appliances). For example, an address mask with two “one” bits results in four possible values, depending on the address. Each of these values can be thought of as a bucket. With two mask bits, you have four buckets, numbered 0-3. The buckets are assigned to WCCP caches. To be effective, there must be at least as many buckets as caches. If you use a two-bit mask and have five or more caches, some caches are idle, because each bucket is assigned to only one cache, and there are not enough buckets to cover all five caches:

<table>
<thead>
<tr>
<th>Cache</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buckets</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>-</td>
</tr>
</tbody>
</table>

If there are more buckets than caches, some caches are assigned multiple buckets. For example, if you set three mask bits, creating eight buckets, and you have four caches, two buckets are assigned to each cache. If you have five caches, three caches are assigned two buckets each, and two caches are assigned just one. If each bucket represents the same number of users, you have a 2:1 load imbalance across caches:

<table>
<thead>
<tr>
<th>Cache</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buckets</td>
<td>0-1</td>
<td>2-3</td>
<td>4-5</td>
<td>6</td>
<td>7</td>
</tr>
</tbody>
</table>

Increasing the number of set mask bits reduces this imbalance. With four mask bits (16 index values) and five caches, four caches receive three buckets and one cache receives four buckets, resulting in only a 4:3 imbalance. With six set mask bits (the largest number supported), four caches receive 13 buckets and one receives 12, which is only a 13:12 load imbalance.

<table>
<thead>
<tr>
<th>Cache</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buckets</td>
<td>0-12</td>
<td>13-25</td>
<td>26-38</td>
<td>39-51</td>
<td>52-63</td>
</tr>
</tbody>
</table>

Ideally, you would like each remote site to be directed to a single appliance in the WCCP cluster, so that all traffic to and from a given site is stored in the same compression history. With this arrangement, any traffic from one user at the site can be used to compress similar traffic from any other user at that site. In other words, for compressibility, load-balancing works best if it the address mask selects the bits that differentiate one remote site from another. These are often the least-significant bits of the subnet portion of the IP address. Using these bits tends to allocate the same number of remote sites (not users) per local appliance. A mask that aligns with the host portion of the address instead of the subnet results in a
more equal number of remote users (not sites) per appliance, but at the expense of compression effectiveness. (Compression is only effective when connections flow through the same appliances, and splitting traffic from the same remote site between two or more local appliances interferes with this.)

Finally, for good load-balancing, each “one” bit in the address mask must be set to one on 50% of the remote addresses, and set to zero on 50% of the remote addresses. This is not the case on all address bits, since in most WANs, the highest-order network bits never change at all (such as the 10 in 10.x.x.x). Such bits must never be selected by the address mask.

In addition, many subnets are only sparsely populated. For example, if only 50 addresses are used in the subnet 10.12.0/24, and they are assigned sequentially, the two higher-order host bits (representing the unused range of 10.12.64-10.12.255) for this subnet never change, and if these two bits are included in the address mask, three-fourths of the buckets receive no traffic.

Useful compromises between these two extremes can generally be found.

Follow these rules:
- The number of “one” bits in the address mask must allow at least as many combinations as there are WCCP caches in the cluster. That is, if you have eight appliances, the address mask must contain at least three “one” bits.
- The “one” bits in the address mask must each be inside the active address range for most of your remote subnets, or they skew the load-balancing distribution.
- The mask should split the address range of individual remote sites into as few pieces as possible, for best compression performance.
- If a remote appliance is faster than the local members of the WCCP cluster, the mask should be designed to divide its traffic between multiple local appliances. For example, a 100 Mbps remote appliance should have its traffic split between two 50 Mbps local appliances by setting a bit inside the remote appliance’s active address range.
- The “one” bits in the mask are typically contiguous, but this is not required. They can be in any pattern.

Example: Suppose you set an address mask of 0x0000 0f00, which has four “one” bits. This defines a four-bit field that is extracted from the IP address, yielding 16 possible results (16 buckets). These buckets are in turn assigned to the actual WCCP caches in the WCCP cluster.

<table>
<thead>
<tr>
<th>Address</th>
<th>Masked Address (mask = 0x0000 0f00)</th>
<th>Bucket</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.5</td>
<td>0.0.0.0</td>
<td>0</td>
</tr>
<tr>
<td>10.0.128</td>
<td>0.0.1.0</td>
<td>1</td>
</tr>
<tr>
<td>155.0.2.55</td>
<td>0.0.2.0</td>
<td>2</td>
</tr>
<tr>
<td>253.100.255.2</td>
<td>0.0.15.0</td>
<td>15</td>
</tr>
<tr>
<td>10.0.15.1</td>
<td>0.0.15.0</td>
<td>15</td>
</tr>
</tbody>
</table>

Zero bits in the mask are ignored, and the “one” bits are used to define the extracted field. So if the mask is 0x10 10 10 10, these widely separated “one” bits are extracted into a four-bit field, declaring 16 buckets and a bucket numbers in the range of 0-15.

If the mask value is set to zero, a default value of 0x00 00 0f 00 is used.
Assigning Buckets to Appliances

Sep 08, 2014

The mapping of bucket to appliances is subject to several variables:

- Which appliances are available: If an appliance is down, its share of buckets are given to the available appliance. If a new appliance is added to the cluster, it is given its fair share of buckets.
- The mapping algorithm used (deterministic or least-disruptive).
- The order in which appliances come online (least-disruptive mapping only).
- The IP addresses of the appliances. WCCP algorithms can use a sorted list of appliance IP addresses; for example, assigning buckets to appliances in the same order as the appliance IP addresses.

The most important of these factors, from an administrator’s point of view, is the mapping algorithm.

**Deterministic mapping.** The deterministic mapping algorithm is less graceful than the least-disruptive algorithm, but it supports Hot Standby Router Protocol (HSRP) and Global Server Load Balancing (GSLB) routing, and is required when multiple routers using such protocols share the WCCP cluster.

Deterministic mapping is also the preferred method when the cluster has only two appliances.

Assignments are based on the IP addresses of the active appliances. Each appliance gets its fair share of bucket, with the lowest-numbered bucket being assigned to the appliance with the lowest IP address. If there are more appliances than buckets, the leftover appliances (with no bucket assigned to them) are the ones with the highest-numbered IP addresses. This deterministic assignment allows traffic to arrive for a single connection through any of the routers in the service group and be forwarded to the same appliance.

Reassignment can be disruptive to accelerated connections, which are reset if they migrate to a different appliance. With deterministic mapping, the number of buckets that are reassigned to new appliances can be quite high if there are three or more appliances.

**Least-disruptive mapping.** When a bucket is assigned to a different appliance, any open accelerated connections that used the old appliance is reset. The least-disruptive algorithm keeps the reassignment to a minimum. For example, if you have three appliances, and one appliance fails, the new mapping preserves roughly two-thirds of the assignments and remaps the remaining third (which fails anyway, because their appliance failed). The least-disruptive algorithm does not support HSRP or GSLB routing, because it is not guaranteed to result in identical mappings on all the routers in the service group, and therefore, packets from a single connection might be sent to two different appliances by two different routers, which causes accelerated connections to fail.
Startup and Failover Behavior

Each appliance registers itself with the routers specified in its service class definitions. The first appliance to register itself, becomes the designated cache, and works with the routers to apportion traffic between itself and the other caches (called subordinate caches). Because your appliances use identical WCCP algorithms, it does not matter which one becomes the designated cache.

As additional appliances come online, they are added to the WCCP cluster, and the traffic is reapportioned among the active appliances. This happens at ten-second increments. After a cold start of the routers or appliances, all of the appliances might come online within the same ten-second window, or they might arrive over multiple ten-second windows, causing traffic to be reapportioned multiple times before it stabilizes. In the latter case, the appliances that come online first may can become overloaded until additional appliances come online.

An accelerated connection fails when allocated to a different appliance, making reallocation disruptive. This is not true of non-accelerated connections, which generally experience a delay of thirty seconds or more, and then continue. The least-disruptive mapping option minimizes the amount of reallocation when an appliance fails.

If an appliance fails or otherwise goes offline, its absence is noted, and the designated cache reapportions its traffic to the remaining appliances. If the designated cache itself goes offline, the role of designated cache is also reapportioned. It takes about thirty seconds for the cluster to react to the loss of a cache.
## Deployment Worksheet

On the following worksheet, you can calculate the number of appliances needed for your installation and the recommended mask field size. The recommended mask size is 1-2 bits larger than the minimum mask size for your installation.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Model Used</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Supported XenApp and XenDesktop Users Per Appliance</td>
<td>Uspec =</td>
<td>From data sheet</td>
</tr>
<tr>
<td>XenApp and XenDesktop Users on WAN Link</td>
<td>Uwan =</td>
<td>—</td>
</tr>
<tr>
<td>User overload Factor</td>
<td>Uoverload = Uwan/Uspec =</td>
<td>—</td>
</tr>
<tr>
<td>Supported BW Per Appliance</td>
<td>BWspec =</td>
<td>From data sheet</td>
</tr>
<tr>
<td>WAN Link BW</td>
<td>BWwan =</td>
<td>—</td>
</tr>
<tr>
<td>BW Overload Factor</td>
<td>BWoverload = BWwan/BWspec =</td>
<td>—</td>
</tr>
<tr>
<td>Number of appliances required</td>
<td>N = max(Uoverload, BWoverload) + 1 =</td>
<td>Includes one spare</td>
</tr>
<tr>
<td>Min number of buckets</td>
<td>Bmin = N, rounded up a power of 2 =</td>
<td>—</td>
</tr>
<tr>
<td>If SD-WAN 4000 or 5000,</td>
<td>Bmin = 2*N, rounded up to a power of 2 =</td>
<td>—</td>
</tr>
<tr>
<td>Recommended value</td>
<td>B = 4 * Bmin if Bmin &lt;= 16, else 2 * Bmin =</td>
<td>—</td>
</tr>
<tr>
<td>Number of “one” bits in address mask</td>
<td>M = log2(B)</td>
<td>If B=16, M=4.</td>
</tr>
</tbody>
</table>

Mask value: The mask value is a 32-bit address mask with a number of “one” bits equal to M in the above worksheet. Often
these bits can be the least-significant bits in the WAN subnet mask used by your remote sites. If the masks at your remote sites vary, use the median mask. (Example: With /24 subnets, the least significant bits of the subnet are 0x00 00 nn 00. The number of bits to set to one is log2(mask size); if mask size is 16, set four bits to one. So with a mask size of 16 and a /24 subnet, set the mask value to 0x00 00 0f 00.): ______

The above guidelines work only if the selected subnet field is evenly distributed in your traffic, that is, that each address bit selected by the mask is a one for half the remote hosts, and a zero for the other half. Otherwise, load-balancing is impaired. This even distribution might be true for only a small number of bits in the network field (perhaps only two or three bits). If this is the case with your network, instead of masking bits in the offending area of the subnet field, displace those bits to a portion of the host address field that has the 50/50 property. For example, if only three subnet bits in a /24 subnet have the 50/50 property, and you are using four mask bits, a mask of 0x00 00 07 10 avoids the offending bit at 0x00 00 0800 and displaces it to 0x00 00 00 10, a portion of the address field that is likely to have the 50/50 property if your remote subnets generally use at least 32 IP addresses each.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final Mask Value</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>Accelerated Bridge</td>
<td>Usually apA</td>
<td></td>
</tr>
<tr>
<td>WAN Service Group</td>
<td>A service group not already in use on your router (51-255)</td>
<td></td>
</tr>
<tr>
<td>LAN Service Group</td>
<td>Another unused service group</td>
<td></td>
</tr>
<tr>
<td>Router IP address</td>
<td>IP address of router interface on port facing the appliance</td>
<td></td>
</tr>
<tr>
<td>WCCP Protocol (usually &quot;Auto&quot;)</td>
<td>—</td>
<td>Use “Deterministic” if you have only two appliances or are using dynamic load balancing like HSRP or GSLB. Otherwise, use “Least Disruptive.”</td>
</tr>
<tr>
<td>DC Algorithm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring WCCP Clustering

Sep 11, 2014

After you have finalized the deployment topology, considered all limitations, and filled in the deployment worksheet, you are ready to deploy your appliances in a WCCP cluster. To configure the WCCP cluster, you need to perform the following tasks:

- Configuring the NetScaler Instances
- Configuring the Router
- Configuring the Appliance
Configuring the Router

Sep 12, 2014

WCCP configuration on the router is simple, because most WCCP parameters are set by the appliances.

Unlike legacy SD-WAN WCCP support, WCCP clustering uses two service groups for TCP traffic. One service group is used on the router's WAN interface, and the other is used on the router's LAN interfaces (except for the LAN interface used by the SD-WAN appliances themselves, when deployed in L2-mode WCCP cluster).

As shown in the following figure, you need to configure two service groups because WCCP allows the mask to be applied to either the source IP or the destination IP address, which is not quite what is required. To keep connections between two endpoints together, regardless of which endpoint initiates the connection, the appliance applies the address mask to the source IP address of incoming WAN traffic, and to the destination IP address of incoming LAN traffic. This requires two service groups.

The WAN service group uses WCCP source-ip address masking, while the LAN service group uses dest-ip masking. In some deployments, it may be necessary to reverse the assignments, using the "WAN" service group for your LAN interface and vice versa. This might occur if the number of local IP addresses greatly exceeds the number of remote IP addresses.

Figure 1. SD-WAN WCCP Cluster

To configure WCCP clustering on the router

This procedure assumes Cisco routers, but is similar on other routers. It uses the first of the two methods, discussed above, of redirecting WCCP traffic with an ip wccp redirect in statement on both LAN and WAN ports.

1. Fill in the WCCP clustering Deployment Worksheet.
2. Log on to your router
3. In the global declarations section, declare each service group on the WCCP clustering worksheet, listed as **WAN service group** and **LAN Service group**. For example, **ip wccp 61** and **ip wccp 62**.
   
   Note: The ip wccp command allows, but does not require, a more elaborate syntax than this, and can specify an ACL name or a password. Both service groups must have the same password, if one is used. The ACLs can be different.
4. Inside the interface declarations for each WAN interface that connects to remote SD-WAN appliances, add an **ip wccp x redirect in statement**, where **x** is the WAN service group from the WCCP clustering worksheet.
5. Inside the interface declarations for each LAN interface (except the one connecting to the WCCP cluster, if you are using L2 mode), add an **ip wccp y redirect in statement**, where **y** is the LAN service group from the WCCP clustering worksheet.
6. Save your configuration.

**Example**. The following example uses service group 61 for the WAN service group and service group 62 for the LAN service group. Three router interfaces are used. One is connected to the WAN, one is connected to the LAN, and one is connected to the WCCP cluster.

```bash
! Example is for WCCP clustering using WCCP redirect in statements
! on LAN and WAN interfaces.
! This definition is appropriate for modern Cisco routers.

! Global declarations
ip wccp 61
ip wccp 62
```

---

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.792
interface GigabitEthernet1/1
description LAN interface. SG 62 is used for LAN
ip address 172.80.1.56 255.255.255.0
ip wccp 62 redirect in
!
interface GigabitEthernet1/2
description LAN interface attaching SD-WAN L2-WCCP appliances
description (No wccp redirect statements are used on this interface)
ip address 172.80.21.56 255.255.255.0
!
interface GigabitEthernet1/3
description WAN interface. SG 61 is used for WAN
ip address 172.80.22.56 255.255.255.0
ip wccp 61 redirect in
!

Note: If the router used multiple ports for LAN traffic, each port is configured with an ip wccp 62 redirect in statement.
Similarly, if the router used multiple ports for WAN traffic, each port is configured with an ip wccp 61 redirect in statement.
- If the router used multiple ports for LAN traffic, each port is configured with an ip wccp 62 redirect in statement.
  Similarly, if the router used multiple ports for WAN traffic, each port is configured with an ip wccp 61 redirect in statement.
- If multiple routers shared the same WCCP cluster, they use the same service groups.

It is also possible to use ip wccp redirect statements on only the WAN interfaces:
! Example for WCCP clustering using WCCP redirect in/out statements on
! WAN interface only
! This definition is appropriate for modern Cisco routers.
interface GigabitEthernet1/3
description WAN interface. SG 61 is used for WAN. SG 62 is used for LAN.
ip address 172.80.22.56 255.255.255.0
ip wccp 61 redirect in
ip wccp 62 redirect out
!

In many routers, the ip wccp redirect out path is not optimized in hardware, but uses the CPU. If the router's capabilities along this path exceeds the WAN speed, this method is practical, and is simpler than using redirect statements on every interface.

Router ACLs can be used to limit redirection. For example, for initial testing, perhaps only a single remote IP address might be allowed to be redirected through WCCP.
Configuring the Appliance

Sep 09, 2014
Repeat the following procedure for each appliance in the cluster:
1. Fill in the WCCP clustering Deployment Worksheet.
2. Navigate to Configuration > Appliance Settings > WCCP page.
3. Click Enable to enable WCCP mode on the appliance.
4. Select Cluster (Multiple Caches) option.
5. Fill in parameters in the Select SD-WAN Cluster section.
6. Enter T5 from your worksheet as the Cache 1 IP, T6 as the Cache 2 IP, T2 as the Subnet Mask, and T1 as the Gateway. Click Save. The Configure Service Group section appears.
7. In the Service Group Details section, specify the WAN and LAN service groups (T11 and T12 from your worksheet).
8. In the Priority field, select 100 (in practice this value is somewhat arbitrary).
9. From the Protocol list, select TCP.
10. In the DC Algorithm field, select Deterministic or Least Disruptive. “Deterministic” is always safe to use, and should be used if you are using only two appliances, or are using multiple routers. “Least Disruptive” disrupts fewer user sessions on failover when used with clusters of three or more appliances, but has restrictions on its use.
11. Set Service Group Pair Status to On.
12. If your router is configured to require a password, enter the password in the Service Group Password field. Otherwise, leave the field blank.
13. In the Router Communications Details section, enter the IP address of the router (T8 on your worksheet: often identical to T1 as well). This is the IP address of the appliance-facing router interface. If you use multiple routers to communicate with the appliance, list them all here.
14. From the Router Forwarding list, select Level 2 or GRE, according to the capabilities of your router. Use Level 2 if you can, and GRE if you must.
15. For the Mask Value, enter the value you determined from the WCCP Clustering worksheet. This is a critical value: a poor choice will result in poor load-balancing or none at all.
16. Click Create. This creates the WAN and LAN service groups.
17. On the Configuration > Optimization Rules > Link Definitions page, change the bandwidth limits on each defined WAN to 95% of the aggregate speed of all your WANs. This prevents the link from being under-utilized when load-balancing is imperfect. If ICA (XenApp/XenDesktop) is the dominant use, set each appliance to (95% of WAN bandwidth)/N, where N is the number of appliances (or twice the number of appliances if they are SD-WAN 4000 or 5000 units), to divide the bandwidth equally among the appliances. This latter method is most appropriate for applications with large numbers of active connections that have relatively low bandwidth requirements.
Testing and Troubleshooting

Jan 31, 2014

The Monitoring > Appliance > Application Performance > WCCP page shows the current state of not only the local appliance but of all other appliances that have joined the cluster. Select a WCCP cache and click Get Info.

The Cache Status tab shows the local appliance's status. When all is well, the status is “25: has assignment.” You must refresh the page manually to monitor changes in status. If the appliance does not reach the status of “25: has assignment” within a timeout period, other informative status messages are displayed.

Additional information is displayed when you click on the Service Group or the Routers tabs.

The Cluster Summary tab displays information about the WCCP cluster as a whole. As a side effect of the WCCP protocol, each member of the cluster has information about all the others, so this information can be monitored from any appliance in the cluster.

Your router can also provide status information. See your router documentation.
Inline Mode

Sep 27, 2013

Note: This documentation is valid only for appliances that were provisioned from a factory-reset state with the release 7.1 Configuration Wizard. For appliances that have been updated to release 7.1, but not reprovisioned from a factory-reset state, see the release 7.0 documentation.

When you deploy a SD-WAN 4000/5000 appliance in inline mode, pairs of Ethernet ports on the appliance function as accelerated bridges. Traffic flows into one bridge port and out the other. When two sites with appliances communicate, TCP connections between the sites can be accelerated. Traffic that cannot be accelerated is passed through transparently, as if the appliance were not there.

For maximum reliability, the bridge pairs are equipped with a bypass feature that causes the two ports to be connected to each other should the appliance fail or lose power, allowing traffic to continue flowing even during such an outage.

Starting in release 7.1, inline mode depends on the NetScaler “add interfacePair” command to isolate bridge traffic, ensuring that traffic from one bridge pair stays on that pair. In previous releases, this was done with VLAN definitions. Appliances that were provisioned with release 7.1 have this feature enabled by default. Appliances that were upgraded to release 7.1 without reprovisioning retain their old configuration.

Inline mode is currently recommended only for sites where WCCP is not practical, and which have a single WAN link, or have fully independent WAN links that do not use dynamic routing, load-balancing, or fail-over.
The following figure shows a SD-WAN 4000/5000 appliance in inline mode.

As shown in the above figure, inline mode is a two-arm mode. For inline deployments, the NetScaler instance is configured in L2 (bridged) mode, but the accelerators are connected internally to the NetScaler instance in a one-arm configuration.

Inline mode is the easiest mode to configure. You connect one port of an accelerated pair to the WAN router and the other to the LAN network. The appliance transparently accelerates traffic flowing between the two ports, which to the rest of the network appear to be an Ethernet bridge.

You can also deploy the appliance to accelerate traffic from certain resources only, such as back-end servers, and not the traffic of the entire network. Such an arrangement reserves the appliance's resources for the selected traffic. In this case, you install the appliance on the branch network that includes the resources for which you want to accelerate traffic.

The following figure shows partial site acceleration:

As shown in the above figure, inline mode is a two-arm mode. For inline deployments, the NetScaler instance is configured in L2 (bridged) mode, but the accelerators are connected internally to the NetScaler instance in a one-arm configuration.

As shown in the above figure, inline mode is a two-arm mode. For inline deployments, the NetScaler instance is configured in L2 (bridged) mode, but the accelerators are connected internally to the NetScaler instance in a one-arm configuration.
Port Affinity

Sep 27, 2013

Port traffic on a given bridge must be isolated to that bridge. In release 7.1, this is done as part of the provisioning process. It can also be done manually with the “add interfacePair” command in the NetScaler command line interface.

The following examples show how this command is used to create port affinity on all bridged pairs in the appliance:

**SD-WAN 4000**
- add interfacePair 1 -ifnum 1/1 1/2
- add interfacePair 2 -ifnum 1/3 1/4
- add interfacePair 3 -ifnum 1/5 1/6
- add interfacePair 4 -ifnum 1/7 1/8
- add interfacePair 5 -ifnum 10/1 10/2

**SD-WAN 5000**
- add interfacePair 1 -ifnum 10/1 10/2
- add interfacePair 2 -ifnum 10/4 10/5
- add interfacePair 3 -ifnum 10/6 10/7
VLAN Trunking

Sep 27, 2013
VLAN trunking is also known as tagged VLAN and 802.1Q tagging. The 802.1Q tagging enables a networking device to add information to a frame at Layer 2 to identify the VLAN membership of the frame. Tagging also enables network environments to have VLANs that span multiple devices. A device that receives the packet reads the tag and recognizes the VLAN to which the frame belongs.

When you configure tagging on bridged interfaces, the VLAN configuration must be identical on both ports of the bridge.

Tagged VLANs are not supported on the management interfaces (ports 0/1 and 0/2).

For example, if your WAN link uses VLAN 412, you declare VLAN 412 as a tagged VLAN in the NetScaler instance, and bind it to both ports of the bridge (such as ports 10/1 and 10/2), as shown in the example below.

Figure 1. Tagged VLANs for VLAN trunking. VLAN 412 is tagged

VLANs can be declared in either of two ways:

1. From the System > Settings > Configure NSVLAN Settings dialog box. This method declares a VLAN whose broadcast traffic is isolated from other VLANs. This method is recommended for the management subnet. It requires a restart to take effect.
   Note: This VLAN configuration method is neither synchronized nor propagated in high availability mode. Therefore, you must perform the configuration independently on each appliance of a high availability setup.

2. From the Create VLANs dialog box (reached from Network > VLANs > Add.). This method does not create an isolated broadcast domain, from traffic originating in the NetScaler instance until we bind the NetScaler IP addresses to the VLAN. Adding such a VLAN does not require a restart. This method is recommended for all VLANs except the management subnet.
Ethernet Bypass

The appliance includes a bypass feature for inline mode. In a power failure, a relay closes and the input and output ports become electrically connected. This feature allows the Ethernet signal to pass through from one port to the other, as if the appliance were not there. The appliance functions like a cross-over cable connecting the two ports.

Besides a power failure, any failure of the appliance hardware or software also closes the relay. When the appliance is restarted, the bypass relay remains closed until the appliance is fully initialized, maintaining network continuity at all times. This feature is automatic and requires no user configuration.

When the bypass relay is closed, the bridge ports of the appliance are inaccessible.

- The bypass feature is disabled when the NetScaler instance is set to L3 mode. Because L3 mode is the factory default, inline mode should be configured before the appliance is placed in line with data traffic.
- The bypass feature is disabled when the appliance is in HA mode.
- A bypass event causes all bypass-enabled port pairs (except the loopback ports) to enter the bypass mode.
- The loopback ports never enter bypass mode.
- A bypass event occurs if the NetScaler instance or the bypass daemon in Dom-0 becomes unresponsive.
- A bypass event is not triggered by accelerators becoming unresponsive.
- The 1-Gigabit bypass ports are copper, and 10-Gigabit bypass ports are fiber ports.
Configuring Inline Mode

Dec 05, 2013

Note: These instructions are valid only for appliances that were provisioned from a factory-reset state with the release 7.1 Configuration Wizard. For appliances that have been updated to release 7.1, but not reprovisioned from a factory-reset state, see the release 7.0 documentation.

Basic configuration is performed by the release 7.1 Configuration Wizard. Additional configuration is required only if you use VLAN trunking on data passing through the bridges.

1. Do not attach the bridges to your traffic networks yet. Begin by provisioning the appliance with the configuration wizard.
2. If your traffic does not contain tagged VLAN traffic, skip to the last step of this procedure.
3. Navigate to the NetScaler instance at Configuration > NetScaler > Instances and click on the IP address of the NetScaler instance.
4. If the Citrix SD-WAN Connector Get Started page appears, ignore it.
5. Click Configuration > Network > VLANs > Add.
6. In the Create VLAN dialog box, configure the tagged VLANs to use bridge #1. In the VLAN Id field, enter the VLAN ID of the first tagged VLAN (VLAN1.1 on your worksheet). Under Interfaces, clear all the check boxes. Then, select Active and Tagged for the first port of the bridge (T9 on your worksheet) and the second port of the bridge (T10). Click Create.
7. Repeat the previous step for any remaining VLANs using bridge #1 (VLAN1.2, VLAN1.3, and so on).
8. Repeat for any additional bridge pairs.
9. Click Close.
10. Click Save to save your configuration.
11. Connect the bridges to your traffic networks. Configuration is complete.
Configuring the High Availability Setup on the Appliances

Aug 20, 2013

High availability (HA) works directly between the NetScaler instances of two SD-WAN 4000 or 5000 appliances. As shown in the configuration, the two appliances are configured almost identically, except for management network IP addresses.

Note: The accelerator instances on the two appliances are not synchronized, and must be kept consistent manually. Take this into account when deciding whether to use HA.

Note: For a smooth installation, install and test one appliance before adding the second one, noting all configuration changes, especially to the accelerator.

Note: You must use the same aPA and signaling addresses on both appliances. However, all management subnet IP addresses must be unique on each appliance.

If the active appliance becomes unavailable, the passive appliance transparently takes over the function of the primary appliance. This is called “failover.” As a result, disruption of services over the network is minimal. After a failover, all clients must reestablish their connections to the managed servers, but the session persistence rules are maintained as they were before the failover.

HA is supported in all deployment modes, and the HA configuration procedure is the same for all modes. The two appliances should be running identical hardware, licensing, and software releases, and must be deployed identically, using the same deployment modes on the same subnets.

When you enable HA, the configuration of the primary appliance's NetScaler instance is copied to the secondary appliance as part of the NetScaler HA synchronization process.

To configure a high availability setup of NetScaler instances

1. Complete the configuration for your chosen deployment mode (inline or WCCP). Note that all parameters for the external traffic subnet and the private traffic subnet are identical for both appliances, but some management subnet values are different on the two appliances.

2. Fully configure appliance #1 and test it thoroughly. If inline mode is used, do not connect the traffic network to the bridge ports on appliance #2.

3. Fully configure appliance #2. Note that some parameters are different on the two appliances: H1, H4, H5, H6, and H17 are used on the second appliance in place of M1, M4, M5, M6, and M17. Make sure that the accelerators are configured identically to the ones on appliance #1, and that both appliances have identical VLAN definitions in the NetScaler instances.

4. Access the NetScaler instance on appliance #1, by specifying its IP address (M17) in a web browser.

5. Log on to the NetScaler instance.

6. In the Navigation pane, expand the System node.

7. Select the High Availability node.

8. Click Add, as shown in the following figure.

   Figure 1. Configuring a high availability setup of the NetScaler instances

9. In the remote Node IP Address field of the High Availability Setup dialog box, specify the NSIP address of the NetScaler instance of the other appliance #2 (H17 on your worksheet), as shown in the following figure.
Figure 2. Configuring a high availability setup of the NetScaler instances

10. Click OK. The appliances are now configured as a high availability pair, as shown in the following figure.

Figure 3. Configuring high availability on the NetScaler instance

Note: To learn more about setting up high availability on a NetScaler instance, see the High Availability node of the Citrix eDocs website.
Putting your appliance online in a production network requires special attention to prevent disruption or confusion, especially in a complex environment.

When deploying SD-WAN 4000/5000, the basic rollout decision is whether to activate the entire deployment at once or to roll it out in stages. In a large or complex environment, a phased approach avoids trouble, and the deployment can be extended at will. This type of approach calls for the use of WCCP. The following example illustrates one approach for such a site:

1. Configure the system as described in the installation procedure, except for the router. There, instead of setting up WCCP redirection for all incoming and outgoing WAN traffic, set it up for traffic to and from either a single remote site or a single IP address at that site. The remote site must already contain an enabled SD-WAN appliance.

2. The accelerator page. If not, check your WCCP configuration on the router and on the accelerators, and check your NAT definitions on the NetScaler instance by using Monitoring: WCCP page. If not, check your WCCP configuration on the router and on the accelerators, and check your NAT definitions on the NetScaler instance by using nstrace. If nstrace reveals an issue, and your definitions look correct, rebooting the appliance may resolve the issue.

3. Test acceleration between the new site and the remote site, with the remote site as the client side and the SD-WAN 4000/5000 equipped site as the server side, as described in General Monitoring.

4. If traffic does not appear, the router is not sending traffic to the SD-WAN 4000/5000 properly. The error could be in the Router configuration, the NetScaler configuration, or the SD-WAN WCCP configuration. Double-check these settings.

5. If traffic appears but is not accelerated, you might have a problem with asymmetrical routing, with not having a SD-WAN license installed, or with having acceleration disabled either globally or on the service classes associated with the traffic.

6. When all is working properly, test reverse connections, where a site on the SD-WAN 4000/5000 side is the client and the remote site is the server, if applicable.

7. If using NetScaler HA, save the configuration of the individual WCCP-enabled instances from the individual instances' GUIs, and save the configuration of the accelerator, do basic configuration manually, then restore the saved configurations, first of the accelerators as a whole, and then restore the two WCCP-enabled instances. Once this is done (and NetScaler HA is enabled), test failover by powering down the primary appliance. Be careful to avoid IP address conflicts.

8. If using NetScaler HA, save the configuration of the individual WCCP-enabled instances from the individual instances' GUIs, and save the configuration of the accelerator, restore these saved configurations, first of the accelerators as a whole, and then restore the two WCCP-enabled instances. Once this is done (and NetScaler HA is enabled), test failover by powering down the primary appliance. Be careful to avoid IP address conflicts.

9. Expand the scope of acceleration to include more remote sites, and repeat the above testing. When doing so, also examine the Monitoring: System Load page, especially during peak periods, to verify that the SD-WAN 4000/5000 is not heavily loaded.

10. Continue this process until the entire WAN is being accelerated.
Use the SD-WAN 4000/5000 GUI to monitor traffic after you configure a LAN link and a WAN link. SD-WAN 4000/5000 allows a very simple link definition.

**Configuring the Links**

To enable monitoring, you must first configure one LAN link and one WAN link. To do so, edit the default links on the Configure: Links page as follows:

1. Edit one link so its name is "LAN," its type is "LAN," and its speed is 10 Gbps in both directions. Delete its existing filter rule, then click Add Rule, and then click Save to save a link definition that matches all traffic.
2. Edit the other link so that its name is "WAN," its type is "WAN," its speed is 95% of the aggregate speed of your site's WAN links in each direction. Delete its existing filter rule, then click Add Rule, and then click Save to save a link definition that matches all traffic.

To verify that link configuration is working correctly, traffic must be flowing. If the network does not have enough traffic to fill the WAN link to capacity, run test traffic to fill the network to capacity. Then look at the link reports on the Reports: Link Usage tab. The following figure shows these reports.

**General Monitoring**

1. If WCCP is configured, verify that the service groups are in operation and the routers are redirecting traffic. (Note that the SD-WAN WCCP page packet counts are not present in SD-WAN 4000/5000. Check traffic by other means, such as on the Monitoring: Active Connections page, and on the router.)
2. On the remote SD-WANs, verify that outgoing connections are being accelerated, and that all accelerated connections to the datacenter report the same Partner Unit on the remote appliance's Monitoring: Connections page. When load-balancing is working properly, all outgoing accelerated connections show the same Partner Unit. (However, incoming accelerated connections might show different units.)
3. Double-check remote SD-WANs for correctly set bandwidth limits, to prevent remote issues from being misidentified as datacenter issues.
4. Generally monitor the SD-WAN 4000/5000 unit for alerts.
5. In the broker UI, use the Dashboard, the Monitoring: Remote Partners, and perhaps the Monitoring: Appliance Load pages to monitor the overall activity and load of the system.
Troubleshooting Tips

Jan 28, 2011

While most installations complete smoothly, some installations require knowledge of the appliance's internal structure or the use of little-known features before you can perform additional monitoring and troubleshooting. These troubleshooting tips provide information and techniques that allow a more in-depth analysis of the appliance.

Understanding Internal Addresses

Some reports show addresses on the private subnets within the SD-WAN 4000/5000, so it's good to know what these addresses mean. These subnets connect the virtual machines together, without connecting to external ports.

All these addresses are on the local link subnet 169.254.0.0/16, described in RFC3927. This address space is segmented into three partly overlapping subnets: system management, private traffic, and accelerator management subnets.

System Management Subnet, 169.254.0.0/16

<table>
<thead>
<tr>
<th>Function</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Service</td>
<td>169.254.0.10/16</td>
</tr>
<tr>
<td>NetScaler Instance</td>
<td>169.254.0.11/16</td>
</tr>
<tr>
<td>XenServer</td>
<td>169.254.0.1/16</td>
</tr>
</tbody>
</table>

Private Traffic Subnet, 169.254.10.0/24

<table>
<thead>
<tr>
<th>Function</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>apA IP, accelerators 1-8</td>
<td>169.254.10.21/24 - 169.254.10.28/24</td>
</tr>
<tr>
<td>apA Signaling IP, accelerators 1-8</td>
<td>169.254.10.121/24 - 169.254.10.128/24</td>
</tr>
<tr>
<td>NetScaler Instance</td>
<td>169.254.10.11/24</td>
</tr>
</tbody>
</table>

Accelerator Management Subnet, 169.254.0.21-28/24

<table>
<thead>
<tr>
<th>Function</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accelerator unified management IP (controls all accelerators)</td>
<td>169.254.0.20/24</td>
</tr>
<tr>
<td>Primary Port IP, accelerators 1-8</td>
<td>169.254.0.21/24 - 169.254.0.28/24</td>
</tr>
</tbody>
</table>

Figure 1. Virtual machines in the SD-WAN 4000 and 5000. The system management subnet is not shown in this diagram. The traffic shaper manages traffic from all accelerators and is controlled via the accelerator GUI.

Checking and Correcting Accelerator Instance Status
Sometimes an error message may indicate an issue with one of the virtual machines in the appliance. To check their status, go to the System Configuration page and select an Instance view of either the SD-WAN or NetScaler subsystems. For example, the SD-WAN page is shown below:

- A fully active instance will show a green circle for VM State, Instance State, and Licensed.
- Your appliance may have more instances present than are licensed; ignore the unlicensed instances.
- If the VM State or Instance State of the remaining instances are not green, use the “Rediscover” action to attempt to bring these instances back into operation.

You can also get detailed information for each instance, as shown below:

- Every instance should have a Status of “Inventory from SD-WAN Instance completed.”
- Every instance should be running the same version of the software.
- Every instance should have the netmask (255.255.255.0) and gateway (169.254.0.20).
- Instances that show an uptime shorter than other instances have rebooted since the last whole-system reboot.

Logging Into the NetScaler Instance
Sometimes it is useful to log into the NetScaler instance to check its status or do configuration. You can log into the NetScaler instance from the NetScaler Instances page of the System Configuration view, as shown below. Click the IP Address link.

You can also log into the NetScaler instance directly from your browser if you know its IP address on the management port (port 0/1).

Once logged in, you will see the NetScaler GUI, which identifies itself as NetScaler VPX at the top of the page.

This is the standard NetScaler user interface. Using monitoring features is safe. Configuration changes should be made with caution, as the SD-WAN 4000/5000 makes undocumented assumptions about how the NetScaler instance is configured.

Using Ping and Traceroute
The ping and traceroute utilities are not available on the accelerator instances, as they are on other SD-WAN products. Instead, you can use the equivalent features on the NetScaler instance, using the Diagnostics page as shown below.

These features will work over your external network and on the appliance’s internal subnets.

Using the System Dashboard
Unlike the SD-WAN Dashboard, the System Dashboard page is devoted largely to hardware monitoring.

- The System Health tables show a status summary, with a Details link for expanded information in graphical form.
- The Events tables show a status summary, with a Show Events link to see the related log entries.

The system below shows a conditions worth investigating:

- The power supply was struggling, as can be seen in both the Hardware Sensors Summary and the System Health Events log. (The count in the System Health Events heading shows that there was only one event, the Date field shows that it
happened long before the screen was displayed, and the Message indicates that the incident was Non-Critical, so replacing the power supply is likely not called for.)

- Several ports are marked as Down, which is only an error if a cable is supposed to be present. Most appliances have several unused ports.
- Fail To Wire lists FTW Disabled for all ports. This means that the network bypassing feature is not enabled on this appliance. Examination of the FTW Events showed that there were no actual events, indicating that the feature is probably disabled.

For each warning or error, additional details are available through the Details links or Show Events buttons.

**Logging In To Different Instances via SSH**

You can log into some of the virtual machines from the management port (port 0/1) using an ssh utility (such as PuTTY on Windows), logging in either as root or nsroot and using the administrative password. This will give you a shell prompt.

The most common use for logging on via SSH is to restore the IP address of an instance, typically the management service, that has become unreachable due to misconfigured network parameters. Otherwise, SSH is not recommended, as configuration changes can render the appliance unstable or unusable.

If neither of the two instances below are accessible over the network, you can log into the XenServer instance using the RS-232 port, which will give you a shell prompt.

<table>
<thead>
<tr>
<th>Instance</th>
<th>Login</th>
<th>Password</th>
<th>Actual username</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Service</td>
<td>nsroot</td>
<td>Admin password</td>
<td>root</td>
</tr>
<tr>
<td>Management Service</td>
<td>root</td>
<td>Admin password</td>
<td>root</td>
</tr>
<tr>
<td>XenServer</td>
<td>nsroot</td>
<td>Admin password</td>
<td>nsroot</td>
</tr>
<tr>
<td>XenServer</td>
<td>root</td>
<td>Admin password</td>
<td>root</td>
</tr>
</tbody>
</table>

Once logged into one of these virtual machines, you can use SSH from the shell prompt to reach the NetScaler instance or the accelerator at the appropriate 169.254.x.x address.

The usual UNIX/Linux commands are available, including the vi text editor.

**Monitoring Individual Accelerator Instances**

Logging into the accelerator GUI IP allows you to manage all the accelerator instances as a unit. Changes are automatically propagated to all the accelerator instances.

On rare occasions, you may wish to troubleshoot individual accelerator instances. To do this, use the following URL's:

<table>
<thead>
<tr>
<th>Accelerator Instance</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>https://&lt;accelerator_ip&gt;:4001</td>
</tr>
<tr>
<td>2</td>
<td>https://&lt;accelerator_ip&gt;:4002</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>
The login for the instances is admin. The password is the same admin password as is used on the other instances.

This is recommended for monitoring, not for making permanent changes, since any parameter you set in an instance may be overwritten later by the synchronization process.

Using Individual Elements of the Update Bundle
The update bundles distributed by Citrix are in a simple .tgz format (a tar archive compressed with gzip). It is sometimes useful to extract individual components from the archive, rather than going back to the the Citrix Web site and downloading them individually. This is most commonly useful with the management service (build-svm*.tgz) or the accelerator release (orbital*.bin).

The update bundle can be managed by tar/gzip or by archiving utilities like 7-zip.
NetScaler SD-WAN 400 and 410 Standard Edition Appliances

Nov 30, 2016
The NetScaler SD-WAN 400 SE and 410 SE are 1U appliances for use in small branch offices.

The NetScaler SD-WAN 410 SE Series is the next generation of SD-WAN Standard Edition appliances with Virtual WAN functionality.

- SD-WAN 400 Series: A small, affordable 1U appliance suitable for smaller branch offices. The SD-WAN 400 SE Series has two accelerated bridges and supports WAN speeds of up to 50 Mbps.
- SD-WAN 410 Series: A small, affordable 1U appliance suitable for smaller branch offices. The SD-WAN 410 SE Series supports WAN speeds of up to 150 Mbps.

The 400-SE platform is Hypervisor based and 410-SE is a baremetal appliance.

Within a given series, all models use the same hardware, and the different WAN speed ratings are obtained through different licensing options. For example, the SD-WAN 410 SE models (the 410-20, 410-50, 410-100, and 410-150) use the same hardware, and an appliance can be licensed as either a 20 Mbps, 50 Mbps, 100 Mbps, or 150 Mbps appliance.

The licensed bandwidth applies only to the sending direction, so a SD-WAN 410 SE-20, rated at 20 Mbps in the sending direction, is appropriate for Virtual Path (fixed/dynamic) with a 16 Mbps/8 Mbps download/upload bandwidth.

In addition to differences in WAN bandwidth capabilities, the different series vary in CPU power, installed RAM, and installed disk capacity.

All models use solid-state drives instead of conventional hard drives for increased speed and reliability.

The Citrix Compliance Regulatory models for SD-WAN 400-SE and 410-SE are:

- SD-WAN 400-SE: CB 504-2
- SD-WAN 410-SE: 512-2

For more information, see the NetScaler product platform datasheet.
NetScaler SD-WAN 400 SE

Apr 07, 2017

The SD-WAN 400 SE platform has a dual-core processor and 8GB of memory. This platform has a bandwidth of up to 50 Mbps.

The following figure shows the front panel of a SD-WAN 400 SE appliance.

Figure 1. SD-WAN 400 SE, front panel

The front panel of the SD-WAN 400 SE appliance has a power button and five LEDs.

The power button switches main power (the power to the power supply) on or off.

The reset button restarts the appliance.

The LEDs provide critical information about different parts of the appliance.

- **Power Fail**—Indicates that a power supply unit has failed.
- **Information LED**—Indicates the following:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuously on and red</td>
<td>The appliance is overheated.</td>
</tr>
<tr>
<td></td>
<td>(This might be a result of cable congestion.)</td>
</tr>
<tr>
<td>Blinking red (1Hz)</td>
<td>Fan failure.</td>
</tr>
<tr>
<td>Blinking red (0.25Hz)</td>
<td>Power failure.</td>
</tr>
<tr>
<td>Solid blue</td>
<td>Local UID has been activated. Use this function to locate the server in a rack mount environment.</td>
</tr>
<tr>
<td>Blinking blue (300 m/s)</td>
<td>Remote UID is on. Use this function to identify the server from a remote location.</td>
</tr>
</tbody>
</table>

- **NIC1 and NIC2**—Indicate network activity on the LAN1 and WAN1 ports.
- **HDD**—Indicates the status of the hard disk drive.
- **Power**—When blinking, indicates that the power supply unit is receiving power and operating normally.
The following figure shows the back panel of a SD-WAN 400 SE appliance.

Figure 2. SD-WAN 400 SE appliance, back panel

The following components are visible on the back panel of a SD-WAN 400 SE appliance:

- Cooling fan
- Single power supply, rated at 200 watts, 110-240 volts
- Accelerated pairs of Ethernet ports (apA and apB) which function as accelerated bridges. Individual port assignments:
  - LAN1 is apA.1, WAN1 is apA.2, LAN2 is apB.1, LAN2 is apB.2.
- RS-232 serial console port
- One Aux Ethernet port and one management port
- Two USB ports
- One Solid State Drive (SSD)
- SD-WAN 400 - 160 GB SSD
NetScaler SD-WAN 410 SE

Apr 07, 2017

The SD-WAN 410 SE platform has a dual-core processor and 8GB of memory. This platform has a bandwidth of up to 150 Mbps.

The following figure shows the front panel of a SD-WAN 410 SE appliance.

The power button switches main power (the power to the power supply) on or off.

The reset button restarts the appliance.

- **apA, apB, and apC** - Indicate network activity on the LAN and WAN ports.
- **Bypass port** - Indicates the status of the third pair of bypass ports.
- **Power** - When blinking, indicates that the appliance is doing factory reset.

The LEDs provide critical information about different parts of the appliance.

- **Power Fail** - Indicates that a power supply unit has failed.
- **Information LED** - Indicates the following:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuously on yellowish orange (looks like red)</td>
<td>Data ports are in bypass mode (FTW)</td>
</tr>
<tr>
<td>Continuously ON and red.</td>
<td>The appliance is overheated. (This might be a result of cable congestion.)</td>
</tr>
<tr>
<td>Blinking red (1Hz) - slow blinking red</td>
<td>Fan failure.</td>
</tr>
<tr>
<td>Blinking red (0.25Hz) - fast blinking red</td>
<td>Power failure.</td>
</tr>
<tr>
<td>Solid blue</td>
<td>Local UID has been activated. Use this function to locate the server in a rack mount environment.</td>
</tr>
</tbody>
</table>
Remote UID is on. Use this function to identify the server from a remote location.

Appliance is working fine.

**Note**

The terms FTW and bypass are inter-exchangeably. The bypass port is the FTW port.

The above figure shows the back panel of a SD-WAN 410 SE appliance.

The following components are visible on the back panel of a SD-WAN 410 SE appliance:

- **Cooling fan** - This platform is intended for use in a branch typically desktop mounted with ambient air temperature. Fanless operation is highly desired and expected.
- **Single power supply**, rated at 200 watts, 110-240 volts. Power supply has an LED that indicates the status of the power supply, as described in [hardware-common-components-con1.html](https://docs.citrix.com).
- **One RJ45 management port**:
  - 1GigE Copper (1000BASE-TX)
  - BMC available, but disabled by default. Located at the front of the appliance. No LOM port
  - Does not support fail-to-wire
- **Two USB ports**
- **One Solid State Drive (SSD)** - 64 GB SATADOM
- **Power switch**, which turns power to the appliance on or off. Press the switch for less than two seconds to turn off the power.

For information about installing the rails, rack mounting the hardware, and connecting the cables, see "Installing the Hardware."

For information about performing initial configuration of your appliance, see "Initial Configuration."

The ports on the fail-to-wire cards are labeled to facilitate SD-WAN (Virtual WAN) feature. The ports on the FTW card are labeled in pairs. The label appears as a white rectangle around the ports that comprise the FTW.
All data ports are labeled in the order they are enumerated by the Operating System. The ports use odd port numbers for LAN ports and even port numbers for WAN ports. 1/1 is used for the first LAN port, 1/2 for the first WAN port, 1/3 for the second LAN Port, 1/4 for the second WAN port, 1/5 for the third LAN Port, and 1/6 for the third WAN Port.
## Summary of Hardware Specifications

The following table summarizes the specifications of the SD-WAN 400 SE and 410 SE hardware platforms.

### Table 1. Citrix NetScaler SD-WAN 400 and 410 Platforms Summary

<table>
<thead>
<tr>
<th>Feature</th>
<th>SD-WAN 400 SE Details</th>
<th>SD-WAN 410 SE Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform Performance</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Up to 6 Mbps</td>
<td>Up to 150 Mbps</td>
</tr>
<tr>
<td></td>
<td>Model 400-002: 2 Mbps</td>
<td>Model 410-020: 20 Mbps</td>
</tr>
<tr>
<td></td>
<td>Model 400-006: 6 Mbps</td>
<td>Model 410-050: 50 Mbps</td>
</tr>
<tr>
<td></td>
<td>Model 410-100: 100 Mbps</td>
<td>Model 410-100: 100 Mbps</td>
</tr>
<tr>
<td></td>
<td>Model 410-150: 150 Mbps</td>
<td>Model 410-150: 150 Mbps</td>
</tr>
<tr>
<td>Acceleration Plug-in CCUs</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td><strong>Hardware Specifications</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td>2 Cores</td>
<td>4 Cores</td>
</tr>
<tr>
<td>Total disk space</td>
<td>1 x 160 GB SSD</td>
<td>64 GB SATADOM</td>
</tr>
<tr>
<td>SSD (dedicated Compression history)</td>
<td>40 GB</td>
<td>N/A</td>
</tr>
<tr>
<td>RAM</td>
<td>8 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>2 pair with bypass 10/100/1000</td>
<td>N/A</td>
</tr>
<tr>
<td>Transceiver support</td>
<td>No</td>
<td>No. The FTW ports are pre-installed with Transceivers.</td>
</tr>
<tr>
<td>Power supplies</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Physical Dimensions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rack Units</td>
<td>1U</td>
<td>1U</td>
</tr>
<tr>
<td>System width</td>
<td>EIA 310-D for 19-inch racks</td>
<td>EIA 310-D for 19-inch racks</td>
</tr>
<tr>
<td>System depth</td>
<td>10.5” (26.7 cm)</td>
<td>10.5” (26.7 cm)</td>
</tr>
<tr>
<td>System weight</td>
<td>8 lbs (3.5 kg)</td>
<td>12 lbs (3.5 kg)</td>
</tr>
<tr>
<td>Shipping dimensions and weight</td>
<td>26L x 18.5W x 6.5” H</td>
<td>14Lx16.8Wx1.7H</td>
</tr>
<tr>
<td></td>
<td>14 lbs</td>
<td>12 lbs</td>
</tr>
<tr>
<td><strong>Environmental and Regulatory</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voltage</td>
<td>100/240 VAC, 50-60 Hz</td>
<td>100/240 VAC, 50-60 Hz</td>
</tr>
<tr>
<td>Power consumption (Max.)</td>
<td>200W</td>
<td>200W</td>
</tr>
<tr>
<td>Operating Temperature (degree Celsius)</td>
<td>10 to 35°C</td>
<td>-5 to 45°C</td>
</tr>
<tr>
<td>Non-operating Temperature (degree Celsius)</td>
<td>-40 to +70°C</td>
<td>-0 to 60°C</td>
</tr>
</tbody>
</table>
| **Allowed Relative Humidity** | 8%–90% | Operating: 20 to 80% RH (noncondensing)  
Non-operating: 5 to 95% RH (noncondensing) |
|-------------------------------|---------|--------------------------------------------------------------------------------------------------|
| **Safety certifications**     | CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)  
CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe) |
| **Electromagnetic and susceptibility certifications** | FCC (Part 15 Class A), CCC, KCC, NOM, CITC, EAC, DoC, CE, VCCI, RCM  
FCC (Part 15 Class A), CCC, KCC, NOM, CITC, EAC, DoC, CE, VCCI, RCM |
| **Environmental certifications** | RoHS, WEEE  
RoHS, WEEE, REACH (optional) |

200W
Preparing for Installation

Mar 16, 2012
Before you install your new appliance, carefully unpack your appliance and make sure that all parts were delivered. Once you are satisfied that your appliance has been delivered to your expectations, verify that the location where the appliance will be installed meets temperature and power requirements and that the server cabinet or floor-to-ceiling cabinet is securely bolted to the floor and has sufficient airflow.

Only trained and qualified personnel should install, maintain, or replace the appliance, and efforts should be taken to ensure that all cautions and warnings are followed.
Unpacking the SD-WAN Appliance (non-ZTD)

Apr 09, 2014

The hardware accessories for your particular appliance, such as cables, adapters, and rail kit, vary depending on the hardware platform you ordered. Unpack the box that contains your new appliance on a sturdy table with plenty of space and inspect the contents.

If you ordered a SD-WAN 400 or 410 appliance, the box should contain:

- The appliance you ordered
- One RJ45 console cable
- One 6 ft CAT5 network cable
- One power cable
- One standard 4-post rail kit

In addition to the items included in the box with your new appliance, you will need the following items to complete the installation and initial configuration process.

- Ethernet cables for each additional Ethernet port that you will connect to your network
- One available Ethernet port on your network switch or hub for each Ethernet port you want to connect to your network
- A computer to serve as a management workstation
Preparing the Site and Rack

Apr 09, 2014

SD-WAN appliances have specific site and rack requirements. You must make sure that adequate environmental control and power density are available. Racks must be bolted to the ground, have sufficient airflow, and have adequate power and network connections. Preparing the site and rack are important steps in the installation process and will help ensure a smooth installation.

The appliance should be installed in a server room or server cabinet with the following features:

Environment control
An air conditioner, preferably a dedicated computer room air conditioner (CRAC), capable of maintaining the cabinet or server room at a temperature of no more than 27 degrees C/80.6 degrees F at altitudes of up to 2100 m/7000 ft, or 18 degrees C/64.4 degrees F at higher altitudes, a humidity level no greater than 45 percent, and a dust-free environment.

Power density
Wiring capable of handling at least 4,000 watts per rack unit in addition to power needs for the CRAC.

The rack on which you install your appliance should meet the following criteria:

Rack characteristics
Racks should be either integrated into a purpose-designed server cabinet or be the floor-to-ceiling type, bolted down at both top and bottom to ensure stability. If you have a cabinet, it should be installed perpendicular to a load-bearing wall for stability and sufficient airflow. If you have a server room, your racks should be installed in rows spaced at least 1 meter/3 feet apart for sufficient airflow. Your rack must allow your IT personnel unfettered access to the front and back of each server and to all power and network connections.

Power connections
At minimum, two standard power outlets per unit.

Network connections
At minimum, four Ethernet connections per rack unit.

Space requirements
One empty rack unit for each SD-WAN 400 and 410 SE appliances.

Note: You can order the following rail kits separately.
- Compact 4-post rail kit, which fits racks of 23 to 33 inches.
- 2-post rail kit, which fits 2-post racks.
Cautions and Warnings

Mar 24, 2010

Updated: 2014-02-06

Caution: During installation or maintenance procedures, wear a grounding wrist strap to avoid ESD damage to the electronics of the appliance. Use a conductive wrist strap attached to a good earth ground or to the appliance. You can attach it to the connector beside the ESD symbol on the back. Follow basic electrical safety precautions to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch, so that you can quickly remove power to the appliance if an electrical accident occurs.
- Remove all jewelry and other metal objects that might come into contact with power sources or wires before installing or repairing the appliance. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and may cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.
- Use a regulating, uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Never stack the appliance on top of any other server or electronic equipment.
- All appliances are designed to be installed on power systems that use TN earthing. Do not install your device on a power system that uses either TT or IT earthing.
- Make sure that the appliance has a direct physical connection to the earth during normal use. When installing or repairing an appliance, always make sure that the ground circuit is connected first and disconnected last.
- Make sure that a fuse or circuit breaker no larger than 120 VAC, 15 A U.S. [240 VAC, 16 A international] is used on all current-carrying conductors on the power system to which your appliances are connected.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, first shut down the appliance, and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages can be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload. Always unplug any appliance before performing repairs or upgrades.
- Do not overload the wiring in your server cabinet or on your server room rack.
- During thunderstorms, or anticipated thunderstorms, avoid performing any hardware repairs or upgrades until the danger of lightning has passed.
- When you dispose of an old appliance or any components, follow any local and national laws on disposal of electronic waste.
- To prevent possible explosions, replace expired batteries with the same model or a manufacturer-recommended substitute and follow the manufacturer's instructions for battery replacement.
- Never remove a power supply cover or any sealed part that has the following label

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.821
Determine the placement of each component in the rack before you install the rails.

Install the heaviest appliance first, at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.

Allow the power supply units and hard drives to cool before touching them.

Install the equipment near an electrical outlet for easy access.

Mount equipment in a rack with sufficient airflow for safe operation.

For a closed or multiple-unit rack assembly, the ambient operating temperature of the rack environment might be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.

For a single-rack installation, attach a stabilizer to the rack.

For a multiple-rack installation, couple (attach) the racks together.

Always make sure that the rack is stable before extending a component from the rack.

Extend only one component at a time. Extending two or more simultaneously might cause the rack to become unstable.

The handles on the left and right of the front panel of the appliance should be used only for extending the appliance out of the rack. Do not use these handles for mounting the appliance on the rack. Use the rack-rail hardware, described later, instead.
Installing the Hardware

Dec 12, 2013

After you have determined that the location where you will install your appliance meets the environmental standards and the server rack is in place according to the instructions, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you will use for initial configuration. To complete the installation, you turn on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.
Rack Mounting the Appliance

Apr 09, 2014

SD-WAN 400 and 410 SE appliances require one rack unit. These appliances are rack-mount devices that can be installed into two-post relay racks or four-post EIA-310 server racks. Verify that the rack is compatible with your appliance.

To mount a SD-WAN appliance, you must first install the rails and then install the appliance in the rack, as follows:

- Remove the inner rails from the rail assembly.
- Attach the inner rails to the appliance.
- Install the rack rails on the rack.
- Install the appliance in the rack.

To remove the inner rails from the rail assembly

1. Place the rail assembly on a flat surface.
2. Slide out the inner rail toward the front of the assembly.
3. Depress the locking tabs until the inner rail comes all the way out of the rail assembly.
4. Repeat steps 1 through 3 to remove the second inner rail.

To attach the inner rails to the appliance

1. Position the right inner rail behind the ear bracket on the right side of the appliance.
2. Align the holes on the rail with the corresponding holes on the side of the appliance.
3. Attach the rail to the appliance with the provided screws.
4. Repeat steps 1 through 3 to install the left inner rail on the left side of the appliance.

To install the rack rails

1. Position the rack rails at the desired location in the rack, keeping the sliding rail guide facing inward.
2. Snap the rails to the rack.
   - Note: Make sure that both rack rails are at same height and that the rail guides are facing inward.

To install the appliance in the rack

1. Align the inner rails, attached to the appliance, with the rack rails.
2. Slide the appliance into the rack rails, keeping the pressure even on both sides, and push the appliance into the rack rails until it locks into place.
3. Verify that the appliance is locked in place by pulling it all the way out from the rack.
   - Note: The illustration in the following figure might not represent your actual appliance.

Figure 1. Rack Mounting the Appliance
Step 1: Attach the inner rail to the appliance by using the screws provided.

Step 2: Attach the outer rails to the rack.

Step 3: Press in latch to slide out the appliance from the rack.
Connecting the Cables

Apr 09, 2014

When the appliance is securely mounted on the rack, determine which ports you should use. You are then ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

Danger: Remove all jewelry and other metal objects that might come in contact with power sources or wires before installing or repairing the appliance. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly, and may cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.

A typical installation using a single accelerated-bridge uses three Ethernet ports (the Primary port and apA).

The appliance has two motherboard ports. The Primary port is used for initial configuration.

On a SD-WAN 410-SE appliance, ports 1/1 and 1/2 are the accelerated pair A (apA) bridge ports, ports 1/3 and 1/4 are the apB ports, and ports 1/5 and 1/6 are the apC bridge ports.

Updated: 2014-01-20

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on a 10/100/1000BASE-T port.

To connect an Ethernet cable to a 10/100/1000BASE-T port

1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port of the appliance.
2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.
3. Verify that the LED glows amber when the connection is established.

Updated: 2014-01-20

You can use the console cable to connect your appliance to a computer or terminal, from which you can configure the appliance. Before connecting the console cable, configure the computer or terminal to support VT100 terminal emulation, 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE. Then connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

To connect the console cable to a computer or terminal

1. Insert the DB-9 connector at the end of the cable into the console port.
   Note: To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.
2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.

Updated: 2014-01-20
A SD-WAN appliance has one power supply, unless you have installed a second. A separate ground cable is not required, because the three-prong plug provides grounding. Provide power to the appliance by installing the power cord.

To connect the appliance to the power source

1. Connect one end of the power cable to the power outlet on the back panel of the appliance, next to the power supply.
2. Connect the other end of the power cable to a standard 110V/220V power outlet.
Switching on the Appliance

Jan 20, 2014

After you have installed the appliance in a rack and connected the cables, verify that the power cable is properly connected. If you have installed a second power supply, make sure the second cable is connected to an outlet for a different circuit than the first. After verifying the connections, you are ready to switch on the appliance.

1. Verify that the appliance is connected through a console or Ethernet port. This will ensure that you can configure the appliance after it is switched on.
2. Depending on the appliance, press the ON/OFF toggle power switch or the power button to switch on the appliance.

Caution: Be aware of the location of the emergency power off (EPO) switch, so that if an electrical accident occurs you can quickly remove power from the appliance.
Initial Configuration

Aug 12, 2014

The appliance shipped from Citrix has default IP addresses configured on it. To deploy the appliance on the network, you must configure the appropriate IP addresses on the appliance to accelerate the network traffic.

You can connect the ethernet cable to the appliance management port, and login to the web management interface using the default IP address.

To perform initial configuration:
- Identify the prerequisites for the initial configuration.
- Record various values required in the initial configuration procedure.
- Configure the appliance by connecting it to the Ethernet port.
- Perform additional configuration for Windows.
- Assign management IP address through the serial console.
- Troubleshoot initial configuration issues.

By default, the initial configuration deploys the appliance in inline mode.

Note
On the SD-WAN 410-SE appliance, the default static IP address is 192.168.100.1. It also has DHCP enabled (by default) for Management access. When you enable the SD-WAN service, or install SD-WAN license using default static IP (192.168.100.1), this IP is lost.

You should assign a static IP address or be notified of the DHCP IP address that is assigned to this appliance. In order to see the DHCP IP address, you can log into the SD-WAN command line interface using admin/password, to view the management IP address. The LCD console on the 410-SE appliance will not display the IP address.
Prerequisites

Aug 12, 2014

Note

The default static IP address is 192.168.100.1. The static IP address has DHCP enabled (by default) for Management access.

When you enable the SD-WAN service, or install SD-WAN license using the default static IP (192.168.100.1), this IP is disabled, and you can obtain DHCP address within the network.

Always assign a Static IP address or be aware of the DHCP address that is assigned to the appliance. To view the DHCP IP address, you can login to SD-WAN CLI (using admin/password) that displays the management IP or go to Configuration -> Appliance Settings -> Network Adapters -> Ethernet.

1. Ensure that you have permanent DHCP address assigned to SD-WAN appliances.
2. The DHCP address should be associated to the management NIC address.
3. Connect the management NIC address to the DHCP enabled LAN or reboot the appliance when ready.

Before you begin configuring the appliance, make sure that the following prerequisites have been met:

- You should have physical access to the appliance.
- In the Worksheet, record all IP addresses and other values you would use to configure the appliance. Preferably, print out the worksheet before you start the configuration process.
- You should already have a SD-WAN license key from Citrix, sent in an email. If you are using remote licensing, you need the IP address of the licensing server.
- WAN Send and Receive Speeds.
Setting up the SD-WAN Appliance

Nov 17, 2016
To set up your NetScaler SD-WAN Appliance hardware, see the instructions documented in the Setting up the Appliance Hardware section.
Deployment Modes

A SD-WAN appliance acts as a virtual gateway. It is neither a TCP endpoint nor a router. Like any gateway, its job is to buffer incoming packets and put them onto the outgoing link at the right speed. This packet forwarding can be done in different ways, such as inline mode, virtual inline mode, and WCCP mode (WANOP appliance only). Although these methods are called *modes*, you do not have to disable one forwarding mode to enable another. If your deployment supports more than one mode, the mode that the appliance uses is determined automatically by the Ethernet and IP format of each packet.

Because the appliance supports different forwarding modes and different kinds of non-forwarded connections, it needs a way of distinguishing one kind of traffic from another. It does so by examining the destination IP address and destination Ethernet address (MAC address), as shown in table below. For example, in inline mode, the appliance is acting as a bridge. Unlike other traffic, bridged packets are addressed to a system beyond the appliance, not to the appliance itself. The address fields contain neither the appliance's IP address nor the appliance's Ethernet MAC address.

In addition to pure forwarding modes, the appliance has to account for additional types of connections, including management connections to the GUI and the heartbeat signal that passes between members of a high-availability pair. For completeness, these additional traffic modes are also listed in table below.

<table>
<thead>
<tr>
<th>Destination IP Address</th>
<th>Destination Ethernet Address</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not appliance</td>
<td>Not appliance</td>
<td>Inline or Pass-through</td>
</tr>
<tr>
<td>Not appliance</td>
<td>Appliance</td>
<td>Virtual Inline or L2 WCCP</td>
</tr>
<tr>
<td>Appliance</td>
<td>Appliance</td>
<td>Direct (UI access)</td>
</tr>
<tr>
<td>Appliance (VIP)</td>
<td>Appliance</td>
<td>High-Availability, Proxy mode</td>
</tr>
<tr>
<td>Appliance (Signaling IP)</td>
<td>Appliance</td>
<td>Signaling Connection (SD-WAN plugin Signaling Connection (SD-WAN plugin, Secure Peer) or Redirector Mode Connection (SD-WAN plugin)</td>
</tr>
</tbody>
</table>

All modes can be active simultaneously. The mode used for a given packet is determined by the Ethernet and IP headers.

The forwarding modes are:
- **Inline mode**, in which the appliance transparently accelerates traffic flowing between its two Ethernet ports. In this mode, the appliance appears (to the rest of the network) to be an Ethernet bridge. Inline mode is recommended, because it requires the least configuration.
- **Virtual inline mode**, in which a router sends WAN traffic to the appliance and the appliance returns it to the router. In this mode, the appliance appears to be a router, but it uses no routing tables. It sends the return traffic to the real router. Virtual inline mode is recommended when inline mode and high-speed WCCP operation are not practical.
- **High availability mode**, which allows to appliances to operate as an active/standby high availability pair. If the primary
appliance fails, the secondary appliance takes over.

Additional traffic types are listed here for completeness:

- **Pass-through traffic** refers to any traffic that the appliance does not attempt to accelerate. It is a traffic category, not a forwarding mode.
- **Direct access**, where the appliance acts as an ordinary server or client. The GUI and CLI are examples of direct access, using the HTTP, HTTPS, SSH, or SFTP protocols. Direct access traffic can also include the NTP and SNMP protocols.
- **Appliance-to-appliance communication**, which can include signaling connections (used in secure peering and by the SD-WAN plugin), VRRP heartbeats (used in high-availability mode), and encrypted GRE tunnels (used by group mode).
- **Deprecated modes**. Proxy mode and redirector mode are legacy forwarding modes that should not be used in new installations.
Customizing the Ethernet ports

Dec 26, 2012

A typical appliance has four Ethernet ports: two accelerated bridged ports, called accelerated pair A (apA.1 and apA.2), with a bypass (fail-to-wire) relay, and two unaccelerated motherboard ports, called Primary and Aux1. The bridged ports provide acceleration, while the motherboard ports are sometimes used for secondary purposes. Most installations use only the bridged ports.

Some SD-WAN appliances have only the motherboard ports. In this case, the two motherboard ports are bridged.

The appliance's user interface can be accessed by a VLAN or non-VLAN network. You can assign a VLAN to any of the appliance's bridged ports or motherboard ports for management purposes.

Figure 1. Ethernet Ports

The ports are named as follows:

Table 1. Ethernet Port Names

<table>
<thead>
<tr>
<th>Motherboard port 1</th>
<th>Primary (or apA.1 if no bypass card is present)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motherboard port 2</td>
<td>Auxiliary1 or Aux1 (or apA.2 if no bypass card is present)</td>
</tr>
<tr>
<td>Bridge #1</td>
<td>Accelerated Pair A (apA, with ports apA.1 and apA.2)</td>
</tr>
<tr>
<td>Bridge #2</td>
<td>Accelerated Pair B (apB, with ports apB.1 and apB.2)</td>
</tr>
<tr>
<td>Bridge #3</td>
<td>Accelerated Pair C (apC, with ports apC.1 and apC.2)</td>
</tr>
</tbody>
</table>
Port Parameters

May 24, 2013

Each bridge and motherboard port can be:

- Enabled or disabled
- Assigned an IP address and subnet mask
- Assigned a default gateway
- Assigned to a VLAN
- Set to 1000 Mbps, 100 Mbps, or 10 Mbps
- Set to full duplex, half-duplex, or auto (on SD-WAN 4000/5000 WANOP and SD-WAN 4000 SE/5100 SE appliances, some ports can be set to 10 Gbps)

All of these parameters except the speed/duplex setting are set on the Configuration: IP Address page. The speed/duplex settings are set on the Configuration: Interface page.

Notes about parameters:

- Disabled ports do not respond to any traffic.
- The browser-based UI can be enabled or disabled independently on all ports.
- To secure the UI on ports with IP addresses, select HTTPS instead of HTTP on the Configuration: Administrator Interface: Web Access page.
- Inline mode works even if a bridge has no IP address. All other modes require that an IP address be assigned to the port.
- Traffic is not routed between interfaces. For example, a connection on bridge apA does not cross over to the Primary or Aux1 ports, but remains on bridge apA. All routing issues are left to your routers.
Accelerated Bridges (apA, apB, and apC)

Dec 07, 2012

Every appliance has at least one pair of Ethernet ports that function as an accelerated bridge, called apA (for accelerated pair A). SD-WAN 410-SE appliance has three pairs of ethernet ports (apA, apB, and apC). A bridge can act in inline mode, functioning as a transparent bridge, as if it were an Ethernet switch. Packets flow in one port and out the other. Bridges can also act in one arm mode, in which packets flow in one port and back out the same port.

An appliance that has a bypass card maintains network continuity if a bridge or appliance malfunctions.

Some units have more than one accelerated pair, and these additional accelerated pairs are named apB, apC, and so on.

If the appliance loses power or fails in some other way, an internal relay closes and the two bridged ports are electrically connected. This connection maintains network continuity but makes the bridge ports inaccessible. Therefore you might want to use one of the motherboard ports for management access.

Caution: Do not enable the Primary port if it is not connected to your network. Otherwise, you cannot access the appliance, as explained in Ethernet Bypass and Link-Down Propagation

Bypass cards are standard on some models and optional on others. Citrix recommends that you purchase appliances with bypass cards for all inline deployments.

The bypass feature is wired as if a cross-over cable connected the two ports, which is the correct behavior in properly wired installations.

Important: Bypass installations must be tested - Improper cabling might work in normal operation but not in bypass mode. The Ethernet ports are tolerant of improper cabling and often silently adjust to it. Bypass mode is hard-wired and has no such adaptability. Test inline installations with the appliance turned off to verify that the cabling is correct for bypass mode.

If the appliance is equipped with two accelerated bridges, they can be used to accelerate two different links. These links can either be fully independent or they can be redundant links connecting to the same site. Redundant links can be either load-balanced or used as a main link and a failover link.

Figure 1. Using dual bridges

When it is time for the appliance to send a packet for a given connection, the packet is sent over the same bridge from which the appliance received the most recent input packet for that connection. Thus, the appliance honors whatever link decisions are made by the router, and automatically tracks the prevailing load-balancing or main-link/failover-link algorithm in real time. For non-load-balanced links, the latter algorithm also ensures that packets always use the correct bridge.

Multiple bridges are supported in both WCCP mode (WANOP) and virtual inline mode. Usage is the same as in the single-bridge case, except that WCCP (WANOP) has the additional limitation that all traffic for a given WCCP (WANOP) service group must arrive on the same bridge.
Two units with multiple bridges can be used in a high-availability pair. Simply match up the bridges so that all links pass through both appliances.
Motherboard Ports

Dec 05, 2012

Although the Ethernet ports on a bypass card are inaccessible when the bypass relay is closed, the motherboard ports remain active. You can sometimes access a failed appliance through the motherboard ports if the bridged ports are inaccessible.

The Primary Port

If the Primary port is enabled and has an IP address assigned to it, the appliance uses that IP address to identify itself to other acceleration units. This address is used internally for a variety of purposes, and is most visible to users as the Partner Unit field on the Monitoring: Optimization: Connections page. If no motherboard port is enabled, the appliance uses the IP address of Accelerated Pair A.

The Primary port is used for:

- Administration through the web based UI
- A back channel for group mode
- A back channel for high-availability mode
VLAN Support

Dec 05, 2012

A virtual local area network (VLAN) uses part of the Ethernet header to indicate which virtual network a given Ethernet frame belongs to. SD-WAN appliances support VLAN trunking in all forwarding modes (inline, WCCP (WANOP), virtual inline, and group mode). Traffic with any combination of VLAN tags is handled and accelerated correctly.

For example, if one traffic stream passing through the accelerated bridge is addressed to 10.0.0.1, VLAN 100, and another is addressed to 10.0.0.1, VLAN 111, the appliance knows that these are two distinct destinations, even though the two VLANs have the same IP address.

You can assign a VLAN to all, some, or none of the appliance's Ethernet ports. If a VLAN is assigned to a port, the management interfaces (GUI and CLI) listen only to traffic on that VLAN. If no VLAN is assigned, the management interfaces listen only to traffic without a VLAN. This selection is made on the Configuration: Appliance Settings: Network Adapters: IP Addresses tab.
Inline Mode

In inline mode, traffic passes into one of the appliance's Ethernet ports and out of the other. When two sites with inline appliances communicate, every TCP connection passing between them is accelerated. All other traffic is passed through transparently, as if the appliance were not there.

For example, when you have an SD-WAN appliance deployed in Inline-Mode with only 4 VLANs on interface group. If there are 6 VLANs going through the traffic, only traffic that matches the 4 VLANs configured is recognized by the appliance.

Figure 1. Inline mode, Accelerating All Traffic on a WAN

Note

Any TCP-based traffic passing through both units is accelerated. No address translation, proxying, or per-site setup is required. Inline mode is auto-detecting and auto-configuring.

Configuration is minimized with inline mode, because your WAN router need not be aware of the appliance's existence.

Depending on your configuration, inline mode's link-down propagation can affect management access to the appliance if a link goes down.

Inline mode is most effective when applied to all traffic flowing into and out of a site, but it can be used for only some of the site's traffic.
Ethernet Bypass and Link-Down Propagation

Oct 30, 2013

Most 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 the other as if the appliance were not there. In fail-to-wire mode, the appliance looks like a cross-over cable connecting the two ports.

Any failure of the appliance hardware or software also closes the relay. When the appliance is restarted, the bypass relay remains closed until the appliance is fully initialized, maintaining network continuity at all times. This feature is automatic and requires no user configuration.

When the bypass relay is closed, the appliance's bridge ports are inaccessible.

If carrier is lost on one of the bridge ports, the carrier is dropped on the other bridge port to ensure that the link-down condition is propagated to the device on the other side of the appliance. Units that monitor link state (such as routers) are thus notified of conditions on the other side of the bridge.

Link-down propagation has two operating modes:

- If the Primary port is not enabled, the link-down state on one bridge port is mirrored briefly on the other bridge port, and then the port is re-enabled. This allows the appliance to be reached through the still-connected port for management, HA heartbeat, and other tasks.
- If the Primary port is enabled, the appliance assumes (without checking) that the Primary port is used for management, HA heartbeat, and other tasks. The link-down condition on one bridge port is mirrored persistently on the other port, until carrier is restored or the unit is rebooted. This is true even if the Primary port is enabled in the GUI but not connected to a network, so the Primary port should be disabled (the default) when not in use.
Accelerating an Entire Site

Dec 05, 2012

Inline mode, Accelerating All Traffic on a WAN shows a typical configuration for inline mode. For both sites, the appliances are placed between the LAN and the WAN, so all WAN traffic that can be accelerated is accelerated. This is the simplest method for implementing acceleration, and it should be used when practical.

Because all the link traffic is flowing through the appliances, the benefits of fair queuing and flow control prevent the link from being overrun.

In IP networks, the bottleneck gateway determines the queuing behavior for the entire link. By becoming the bottleneck gateway, the appliance gains control of the link and can manage it intelligently. This is done by setting the bandwidth limit slightly lower than the link speed. When this is done, link performance is ideal, with minimal latency and loss even at full link utilization.
Partial-Site Acceleration

Dec 27, 2012

To reserve the appliance's accelerated bandwidth for a particular group of systems, such as remote backup servers, you can install the appliance on a branch network that includes only those systems. This is shown in the following figure.

Figure 1. Inline Mode, Accelerating Selected Systems Only

SD-WAN traffic shaping relies on controlling the entire link, so traffic shaping is not effective with this topology, because the appliance sees only a portion of link traffic. Latency control is up to the bottleneck gateway, and interactive responsiveness can suffer.
Configuring and Troubleshooting Inline Mode

Dec 26, 2012

Inline mode requires only basic configuration, because it is applied automatically to any packets passing through the accelerated bridge.
Virtual Inline Mode

Dec 28, 2012

Note: Use virtual inline mode only when both inline mode and WCCP mode are impractical. Do not mix inline and virtual inline modes within the same appliance. However, you can mix virtual inline and WCCP modes within the same appliance. Citrix does not recommend virtual inline mode with routers that do not support health monitoring.

In virtual inline mode, the router uses policy based routing (PBR) rules to redirect incoming and outgoing WAN traffic to the appliance for acceleration, and the appliance forwards the processed packets back to the router. Almost all of the configuration tasks are performed on the router. The only thing to be configured on the appliance is the forwarding method, and the default method is recommended.

Like WCCP, Virtual inline deployment requires no rewiring and no downtime, and it provides a solution for asymmetric routing issues faced in a deployment with two or more WAN links. Unlike WCCP, it contains no built-in status monitoring or health checking, making troubleshooting difficult. WCCP is thus the recommended mode, and virtual inline is recommended only when inline and WCCP modes are both impractical.

The following figure shows a simple network in which all traffic destined for or received from the remote site is redirected to the appliance. In this example, both the local site and remote site use virtual inline mode.

Figure 1. Virtual Inline Example

Following are some configuration details for the network in this example:

- Endpoint systems have their gateways set to the local router (which is not unique to virtual inline mode).
- Each router is configured to redirect both incoming and outgoing WAN traffic to the local appliance.
- Each appliance processes the traffic received from its local router and forwards it back to the router.
- PBR rules configured on the router prevent routing loops by allowing packets to make only one trip to and from the appliance. The packets that the appliance forwards back to the router are sent to their original (local or remote) destination.
- Each appliance has its default gateway set to the address of the local router, as usual (on the Configuration: Network Adapters page). The options for forwarding packets back to the router are Return to Ethernet Sender and Send to Gateway.
Configuring Packet Forwarding on the Appliance

Dec 18, 2013

Virtual inline mode offers two packet-forwarding options:

Return to Ethernet Sender (default)—This mode allows multiple routers to share an appliance. The appliance forwards virtual inline output packets back to where they came from, as indicated by the Ethernet address of the incoming packet. If two routers share a single appliance, each gets its own traffic back, but not the traffic from the other router. This mode also works with a single router.

Send to Gateway (not recommended)—In this mode, virtual inline output packets are forwarded to the default gateway for delivery, even if they are destined for hosts on the local subnet. This option is usually less desirable than the Return to Ethernet Sender option, because it adds an easily forgotten element of complexity to the routing structure.

To specify the packet-forwarding option—On the Configuration: Optimization Rules: Tuning page, next to Virtual Inline, select Return to Ethernet Sender or Send to Gateway.
The router has three tasks when supporting virtual inline mode:
1. It must forward both incoming and outgoing WAN traffic to the SD-WAN appliance.
2. It must forward SD-WAN traffic to its destination (WAN or LAN).
3. It must monitor the health of the SD-WAN appliance so that the appliance can be bypassed if it fails.

In virtual inline mode, the packet forwarding methods can create routing loops if the routing rules do not distinguish between a packet that has been forwarded by the appliance and one that has not. You can use any method that makes that distinction.

A typical method involves dedicating one of the router's Ethernet ports to the appliance and creating routing rules that are based on the Ethernet port on which packets arrive. Packets that arrive on the interface dedicated to the appliance are never forwarded back to the appliance, but packets arriving on any other interface can be.

The basic routing algorithm is:
- Do not forward packets from the appliance back to the appliance.
- If the packet arrives from the WAN, forward it to the appliance.
- If packet is destined for the WAN, forward to the appliance.
- Do not forward LAN-to-LAN traffic to the appliance.
- Traffic shaping is not effective unless all WAN traffic passes through the appliance.

Note: When considering routing options, keep in mind that returning data, not just outgoing data, must flow through the appliance. For example, placing the appliance on the local subnet and designating it as the default router for local systems does not work in a virtual inline deployment. Outgoing data would flow through the appliance, but incoming data would bypass it. To force data through the appliance without router reconfiguration, use inline mode.

If the appliance fails, data should not be routed to it. By default, Cisco policy based routing does no health monitoring. To enable health monitoring, define a rule to monitor the appliance's availability, and specify the "verify-availability" option for the "set ip next-hop" command. With this configuration, if the appliance is not available, the route is not applied, and the appliance is bypassed.

Following is an example of a rule for monitoring the availability of the appliance:
```
!- Use a ping (ICMP echo) to see if appliance is connected track   123 rtr 1 reachability !  rtr 1  type echo protocol IpIcmpecho 192.168.1.200 schedule 1 life forever start-time now
```
This rule pings the appliance at 192.168.1.200 periodically. You can test against 123 to see if the unit is up.
Routing Examples

Feb 06, 2014

The following examples illustrate configuring Cisco routers for the local and remote sites shown in Virtual inline example. To illustrate health monitoring, the configuration for the local site includes health monitoring, but the configuration for the remote site does not.

Note: The configuration for the local site assumes that a ping monitor has already been configured. The examples conform to the Cisco IOS CLI. They might not be applicable to routers from other vendors.

Local Site, Health-Checking Enabled

!  For health-checking to work, do not forget to start
!  the monitoring process.
!
!  Original configuration is in normal type.
!  appliance-specific configuration is in bold.
!
ip cef
!
interface FastEthernet0/0
ip address 10.10.10.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 172.68.1.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.1.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.1.1
!
ip access-list extended client_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
  !  Now set the appliance as the next hop, if it’s up.
  set ip next-hop verify-availability 192.168.1.200 20 track 123
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop verify-availability 192.168.1.200 10 track 123
Remote Site (No Health Checking)

! This example does not use health-checking.
! Remember, health-checking is always recommended,
! so this is a configuration of last resort.
!
!
ip cef
!
interface FastEthernet0/0
ip address 20.20.20.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 171.68.2.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.2.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.2.1
!
ip access-list extended client_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
set ip next-hop 192.168.2.200
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop 192.168.2.200
!

Each of the above examples applies an access list to a route map and attaches the route map to an interface. The access lists identify all traffic originating at one accelerated site and terminating at the other (A source IP of 10.10.10.0/24 and destination of 20.20.20.0/24 or vice versa). See your router’s documentation for the details of access lists and route-maps.

This configuration redirects all matching IP traffic to the appliances. If you want to redirect only TCP traffic, you can change the access-list configuration as follows (only the remote side's configuration is shown here):
!
ip access-list extended client_side
permit tcp 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit tcp 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!

Note that, for access lists, ordinary masks are not used. Wildcard masks are used instead. Note that when reading a
wildcard mask in binary. "1" is considered a "don't care" bit.
Virtual Inline for Multiple-WAN Environments

Dec 27, 2012
Enterprises with multiple WAN links often have asymmetric routing policies, which seem to require that an inline appliance be in two places at once. Virtual inline mode solves the asymmetric routing problem by using the router configuration to send all WAN traffic through the appliance, regardless of the WAN link used. The below figure shows a simple multiple-WAN link deployment example.

The two local-side routers redirect traffic to the local appliance. The FE 0/0 ports for both routers are in the same broadcast domain as the appliance. The local appliance must use the default virtual inline configuration (Return to Ethernet Sender).

Figure 1. Virtual Inline Mode With Two WAN Routers
Virtual Inline Mode and High-Availability

Dec 27, 2012

Virtual Inline mode can be used in a high availability (HA) configuration. The below figure shows a simple HA deployment. In virtual inline mode, a pair of appliances acts as one virtual appliance. Router configuration is the same for an HA pair as with a single appliance, except that the Virtual IP address of the HA pair, not the IP address of an individual appliance, is used in the router configuration tables. In this example, the local appliances must use default virtual inline configuration (Return to Ethernet Sender).

Figure 1. High-availability Example
Monitoring and Troubleshooting

Dec 17, 2012
In virtual inline mode, unlike WCCP mode (WANOP), the appliance provides no virtual inline-specific monitoring. To troubleshoot a virtual inline deployment, log into the appliance and use the Dashboard page to verify that traffic is flowing into and out of the appliance. Traffic forwarding failures are typically caused by errors in router configuration.

If the Monitoring: Usage or Monitoring: Connections pages show that traffic is being forwarded but no acceleration is taking place (assuming that an appliance is already installed on the other end of the WAN link), check to make sure that both incoming WAN traffic and outgoing WAN traffic are being forwarded to the appliance. If only one direction is forwarded, acceleration cannot take place.

To test health-checking, power down the appliance. The router should stop forwarding traffic after the health-checking algorithm times out.
High-Availability Mode

Dec 11, 2013
Two identical appliances on the same subnet can be combined as a high-availability pair. The appliances each monitor the other's status by using the standard Virtual Router Redundancy Protocol (VRRP) heartbeat mechanism. The pair has a common virtual IP address for management, in addition to each appliance's management IP address. If the primary appliance fails, the secondary appliance takes over. Failover takes approximately five seconds.

High availability mode is a standard feature.
How High-Availability Mode Works

Dec 06, 2012

In a high availability (HA) pair, one appliance is primary, and the other is secondary. The primary monitors its own and the secondary’s status. If it detects a problem, traffic processing fails over to the secondary appliance. Existing TCP connections are terminated. To ensure successful failover, the two appliances keep their configurations synchronized. In a WCCP mode (WANOP) high availability configuration, the appliance that is processing traffic maintains communication with the upstream router.

Status monitoring—When high availability is enabled, the primary appliance uses the VRRP protocol to send a heartbeat signal to the secondary appliance once per second. In addition, the primary appliance monitors the carrier status of its Ethernet ports. The loss of carrier on a previously active port implies a loss of connectivity.

Failover—If the heartbeat signal of the primary appliance should fail, or if the primary appliance loses carrier for five seconds on any previously active Ethernet port, the secondary appliance takes over, becoming the primary. When the failed appliance restarts, it becomes the secondary. The new primary announces itself on the network with an ARP broadcast. MAC spoofing is not used. Ethernet bridging is disabled on the secondary appliance, leaving the primary appliance as the only path for inline traffic. Fail-to-wire is inhibited on both appliances to prevent loops.

Caution: The Ethernet bypass function is disabled in HA mode. If both appliances in an inline HA pair lose power, connectivity is lost. If WAN connectivity is needed during power outages, at least one appliance must be attached to a backup power source.

Note: The secondary appliance in the HA pair has one of its bridge ports, port apA.1, disabled to prevent forwarding loops. If the appliance has dual bridges, apB.1 is also disabled. In a one-arm installation, use port apA.2. Otherwise, the secondary appliance becomes inaccessible when HA is enabled.

Primary/secondary assignment—If both appliances are restarted, the first one to fully initialize itself becomes the primary. That is, the appliances have no assigned roles, and the first one to become available takes over as the primary. The appliance with the highest IP address on the interface used for the VRRP heartbeat is used as a tie-breaker if both become available at the same time.

Connection termination during failover—Both accelerated and unaccelerated TCP connections are terminated as a side effect of failover. Non-TCP sessions are not affected, except for the delay caused by the brief period (several seconds) between the failure of the primary appliance and the failover to the secondary appliance. Users experience the closing of open connections, but they can open new connections.

Configuration synchronization—The two appliances synchronize their settings to ensure that the secondary is ready to take over for the primary. If the configuration of the pair is changed through the browser based interface, the primary appliance updates the secondary appliance immediately.

HA cannot be enabled unless both appliances are running the same software release.
Cabling Requirements

May 24, 2013

The two appliances in the high availability pair are installed onto the same subnet in either a parallel arrangement or a one-arm arrangement, both of which are shown in the following figure. In a one-arm arrangement, use the apA.2 port (and, optionally, the apB.2 port), not the apA.1 port. Some models require a separate management LAN, whether deployed in inline or one-armed mode. This is depicted only in the middle diagram.

Figure 1. Cabling for High-Availability Pairs

Do not break the above topology with additional switches. Random switch arrangements are not supported. Each of the switches must be either a single, monolithic switch, a single logical switch, or part of the same chassis.

If the spanning-tree protocol (STP) is enabled on the router or switch ports attached to the appliances, failover will work, but the failover time may increase to roughly thirty seconds. Without STP, failover time is roughly five seconds. Thus, to achieve the briefest possible failover interval, disable STP on the ports connecting to the appliances.

Figure 2. Ethernet Port Locations (Older Models)
Other Requirements

Dec 06, 2012

Both appliances in an HA pair must meet the following criteria:

- Have identical hardware, as shown by on the System Hardware entry on the Dashboard page.
- Run exactly the same software release.
- Be equipped with Ethernet bypass cards. To determine what is installed in your appliances, see the Dashboard page.

Appliances that do not support HA display a warning on the Configuration: High Availability page.
Management Access to the High-Availability Pair

Jan 03, 2013

When configuring a high-availability (HA) pair, you assign the pair a virtual IP (VIP) address, which enables you to manage the two appliances as if they were a single unit. After you enable high-availability mode, managing the secondary appliance through its IP address is mostly disabled, with most parameters grayed out. A warning message displays the reason on every page. Use the HA VIP for all management tasks. You can, however, disable the secondary appliance's HA state from its management UI.
You can configure two newly installed appliances as a high-availability pair, or you can create an HA pair by adding a second appliance to an existing installation.

Prerequisites: Physical installation and basic configuration procedures

To configure high availability

1. Make sure that no more than one appliance is connected to the traffic networks (on the accelerated bridges). If both are connected, disconnect one bridge cable from the active bridges on the second appliance. This will prevent forwarding loops.
2. On the Features page of the first appliance, disable Traffic Processing. This disables acceleration until the HA pair is configured.
3. Repeat for the second appliance.
4. On the first appliance, go to the Configuration: Advanced Deployments: High Availability tab, show below.
5. Select the Enabled Check box.
6. Click the Configure HA Virtual IP Address link and assign a virtual IP address to the apA interface. This address will be used later to control both appliances as a unit.
7. Return to the High Availability page and, in the VRRP VRID field, assign a VRRP ID to the pair. Although the value defaults to zero, the valid range of VRRP ID numbers is 1 through 255. Within this range, you can specify any value that does not belong to another VRRP device on your network.
8. In the Partner SSL Common Name field, type the other appliance’s SSL Common Name, which is displayed on that appliance’s Configuration: Advanced Deployments: High Availability tab, in the Partner SSL Common Name field. The SSL credentials used here are factory-installed.
9. Click Update.
10. Repeat steps 3-8 on the second appliance. If you are managing the appliance via an accelerated bridge (such as apA), you may have to reconnect the Ethernet cable that you removed in step 1 to connect to the second appliance. If so, plug this cable in and disconnect the corresponding cable on the first appliance.
11. With your browser, navigate to the virtual IP address of the HA pair. Enable Traffic Processing on the Features page. Any further configuration will be performed from this virtual address.
12. Plug in the cable that was left disconnected.
13. On each appliance, the Configuration: Advanced Deployments: High Availability page should now show that high availability is active and that one appliance is the primary and the other is the secondary. If this is not the case, a warning banner appears at the top of the screen, indicating the nature of the problem.

Figure 1. High-availability configuration page
Updating Software on a High-Availability Pair

Dec 06, 2012

Updating the SD-WAN software on an HA pair causes a failover at one point during the update.

Note: Clicking the Update button terminates all open TCP connections.

To update the software on an HA pair

1. Log on to both appliances.
2. On the secondary appliance, update the software and reboot. After the reboot, the appliance is still the secondary. Verify that the installation succeeded. The primary appliance should show that the secondary appliance exists but that automatic parameter synchronization is not working, due to a version mismatch.
3. On the primary appliance, update the software, and then reboot. The reboot causes a failover, and the secondary appliance becomes the primary. When the reboot is completed, HA should become fully established, because both appliances are running the same software.
Saving/Restoring Parameters of an HA Pair

Dec 06, 2012

The System Maintenance: Backup/Restore function can be used to save and restore parameters of an HA pair as follows:

To back up the parameters

Use the backup feature as usual. That is, log on to the GUI through the HA VIP address (as is normal when managing the HA pair) and, on the System Management: Backup/Restore page, click Download Settings.

To restore the parameters

1. Disable HA on both appliances by clearing the Enabled check box on the Configuration: Advanced Deployments: High Availability (HA) tab.
2. Unplug a network cable from the bridge of one appliance. (Call it “Appliance A.”)
3. Unplug the power cord from Appliance A.
4. Restore the parameters on the other appliance (Appliance B), by uploading a previously saved set of parameters on the System Maintenance: Backup/Restore page and clicking Restore Settings. (Completing this operation requires a restart, which reenables HA).
5. Wait for Appliance B to restart. It becomes the primary.
6. Restart Appliance A.
7. Log on to Appliance A’s GUI and reenable HA on the Configuration: Advanced Deployments: High Availability (HA) tab. The appliance get its parameters from the primary.

Both appliances are now restored and synchronized.
If the appliances report any failure to enter high-availability mode, the error message will also note the cause. Some issues that can interfere with high-availability mode are:

- The other appliance is not running.
- The HA parameters on the two appliances are not identical.
- The two appliances are not running the same software release.
- The two appliances do not have the same model number.
- Incorrect or incomplete cabling between the appliances does not allow the HA heartbeat to pass between them.
- The HA SSL Certificates on one or both appliances are damaged or missing.
Factory Reset on 410-SE

Dec 20, 2017

The factory reset option is applicable only to the SD-WAN 410-Standard Edition appliance.

To perform factory reset on 410-SE:

1. Once the power LED is flashing, power OFF the appliance with using the power button to the right of the NMI reset button as shown in the image above. Hold the power button for few seconds (10-20 seconds) until the green LED and other LED lights are turned off.

Note
Press and hold the power button for a few seconds to turn off the appliance.

2. Press the NMI reset button once and then power ON the appliance using the power button.

The green LED starts blinking on and off for the next 20-25 minutes until the eUSB recovery process is finished.

3. Wait for few minutes, approximately 5 minutes initially as no activity will happen on the CLI. Non-activity in CLI does not mean nothing is happening. The system is initializing the process.

Tip
- Pressing the reset button even number of times cancels the reset action and results in normal appliance reboot.
- Pressing the reset button odd number of times performs a factory reset.
- Power LED flash indicates that the appliance is being reset.

4. After 5 mins the appliance restarts and the CLI is displayed. There will be couple of reboots (approximately, 4-5) for extracting the software image from the eUSB (sdb) and copying, programming, and re-flashing to the SATADOM (sda).
The appliance restarts 4 to 5 times as it extracts, copies, and initializes the boot process.

5. At the login prompt, you can start configuring the appliance using CLI or the web management interface.
NetScaler SD-WAN 4000, 4100, and 5100 Standard Edition Appliances

May 16, 2017
Citrix NetScaler SD-WAN Standard Edition 4000/4100/5100 appliances are high-performance appliances for busy datacenters. These appliances combines multiple virtual accelerator instances with a single virtual instance of the NetScaler load-balancer, providing the performance of multiple SD-WAN Standard Edition appliances in a single package.

SD-WAN 4000/4100/5100 Standard Edition appliances are designed to with Virtual WAN links with speeds in excess of 1 Gbps, especially for busy datacenters that communicate with a large number of branch and regional sites.

SD-WAN 4000/4100/5100 SE is recommended at the hub of a hub-and-spoke deployment, where smaller appliances are used at the spokes, whenever the link speed or the number of XenApp/XenDesktop users is higher than that can be supported by a smaller appliance.
Citrix NetScaler SD-WAN 4000 SE

May 15, 2017

Citrix NetScaler SD-WAN 4000 is a 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 48 gigabytes (GB) of memory. The Citrix NetScaler SD-WAN 4000 SE has a bandwidth of 300Mbps, 500Mbps, 1Gbps, and 2Gbps respectively.

The following figures shows the front panel of the Citrix NetScaler SD-WAN 4000 SE appliance.

Figure 1. Citrix NetScaler SD-WAN 4000 SE, front panel

The Citrix NetScaler SD-WAN 4000 SE appliances have the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.
  Note: The LEDs on the LOM port are not operational by design.

- RS232 serial console port.

- Two 10/100/1000Base-T copper Ethernet management ports (RJ45). These ports are used to connect directly to the appliance for system administration functions.

- Network Ports
  - NetScaler SD-WAN 4000 SE (without FTW cards). Eight 1G SFP ports and four 10G SFP+ ports.
  - NetScaler SD-WAN 4000 SE (with FTW cards). Eight 1G copper Ethernet ports and four 10G ports.

The following figure shows the back panel of the Citrix NetScaler SD-WAN 4000 SE appliance.

Figure 2. Citrix NetScaler SD-WAN 4000 SE, back panel

The following components are visible on the back panel of the Citrix NetScaler SD-WAN 4000 SE appliance:

- Four 600 GB removable solid-state drives. The 256 GB solid-state drive below the hard disk drive stores the appliance's software. Newer editions of 4000-SE have 800 GB removable SSD and 240 GB SSD.
- USB port (reserved for a future release).
- A 1 TB removable hard disk drive.
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Disable alarm button. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies (either AC or DC), each rated at 850 watts, 100-240 volts.
Citrix NetScaler SD-WAN 4100 SE

May 10, 2017

Citrix NetScaler SD-WAN 4100 is a 2U appliances. Each model has two 6-core processors for a total of 12 physical cores (24 cores with hyper-threading), and 96 gigabytes (GB) of memory. The Citrix NetScaler SD-WAN 4100 SE has a virtual WAN bandwidth of 1Gbps and 2Gbps.

The following figures shows the front panel of the Citrix NetScaler SD-WAN 4100 SE appliance.

Figure 1. Citrix NetScaler SD-WAN 4100 SE, front panel

![Citrix NetScaler SD-WAN 4100 SE, front panel](image)

The Citrix NetScaler SD-WAN 4100 SE appliances have the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software. The LEDs on the LOM port are not operational by design.
- RS232 serial console port.
- Two 10/1000Base-T copper Ethernet management ports (RJ45). These ports are used to connect directly to the appliance for system administration functions.
- 2 port 10G FTW
- 4 port 10G/1G SFP+
- 4 port 10/100/1000 FTW RJ 45

The following figure shows the back panel of the Citrix NetScaler SD-WAN 4100 SE appliance.

Figure 2. Citrix NetScaler SD-WAN 4100 SE, back panel

The following components are visible on the back panel of the Citrix NetScaler SD-WAN 4100 SE appliance:

- 2 X 1 TB HDD in RAID 1.
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Disable alarm button. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies (either AC or DC), each with max power of 850 watts, 100-240 volts.
Citrix NetScaler SD-WAN 5100 SE

Apr 17, 2018

Citrix NetScaler SD-WAN 5100 SE is a 2U appliance. Each model has two 10-core processors for a total of 20 physical cores (40 cores with hyper-threading), and 128 gigabytes (GB) of memory. The Citrix NetScaler SD-WAN 5100 SE has a bandwidth of 1 Gbps, 2 Gbps, 3 Gbps, and 4 Gbps respectively.

The Citrix NetScalerSD-WAN 5100 SE appliance front panel has the following ports:

- 10/100Base-T copper Ethernet Port (RJ45), also called LOM port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software. The LEDs on the LOM port are not operational by design.
- RS232 serial console port.
- Two 10/100/1000Base-T copper Ethernet management ports (RJ45). These ports are used to connect directly to the appliance for system administration functions.
- Eight 10G ports.

The following components are visible on the back panel of the Citrix NetScaler SD-WAN 5100 SE appliance:

- 2 X 1 TB removable hard disk drive.
- USB port (reserved for a future release).
- Power switch, which turns off power to the appliance, just as if you were to unplug the power supply. Press the switch for five seconds to turn off the power.
- Disable alarm button. This button is functional only when the appliance has two power supplies. Press this button to stop the power alarm from sounding when you have plugged the appliance into only one power outlet or when one power supply is malfunctioning and you want to continue operating the appliance until it is repaired.
- Dual power supplies (either AC or DC), each rated at 850 watts, 100-240 volts.

The below figure illustrates NetScaler SD-WAN 5100-SE Appliance model.

![NetScaler SD-WAN 5100 SE Appliance](image)

Upgrade 5100 SE Appliance to 5100 EE Appliance

**Insert Solid State Drive (SSD)**

1. Insert the required SSD in the standard edition appliance. For instructions about how to insert SSD, see Solid State Drive (Field Replaceable Unit).

- 5100 SE appliance requires 800 GB more SSD. Insert the SSD into the 3rd bay.

2. Reboot the appliance through the SD-WAN web management interface.

3. Ensure that the software release version installed on the appliance is 9.3.3.
Appliances shipped with software release version 9.2.1 or earlier

For appliances shipped with software release version 9.2.1 or earlier versions, upgrade the appliances to software release version 9.3.3. Follow the steps below:

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

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

5. When BIOS loads, choose the external USB drive, for example; Sandisk to boot the appliance.
6. Confirm the reimage by selecting Yes to proceed, then press the Enter key.
Upgrade process takes approximately 30-40 minutes to complete. The system reboots after 1-2 minutes and the login prompt is displayed.

7. Unplug USB stick after the procedure is complete.

The reimage process will begin after the edition selection menu appears. Note that on the 1000 and 2000 appliances, “Enterprise Edition” will be listed, but after reimage, the Standard Edition will be presented in the GUI when accessing the default IP address 192.168.100.1, and Enterprise Edition will only be available upon installation of an Enterprise Edition license file.

Note

All Enterprise Edition appliances have Standard Edition software installed as the core software. The WANOP instance is dormant making the appliance a Standard Edition appliance, until the appropriate Enterprise Edition license is installed and configuration in place to enable WANOP capabilities on an EE appliance.


9. Perform single step upgrade to upgrade appliance software release version from 9.3.3 to 10.0. For more information, see; upgrading and updating software.

10. Enable WANOP as a feature of Enterprise Edition sites in the Configuration Editor of the MCN appliance or SD-WAN Center.

Configure Management IP Address Using Serial Console

1. Access serial console of the appliance.
2. Log in to dom0 using the root/nsroot credentials.
3. Type the `ssh admin@169.254.0.60 -l admin` command.
4. Type password: `password`.
5. Type the `management_ip` command.
6. Type the `set interface 192.168.100.1 255.255.255.0 192.168.100.254` command.
7. Type the `apply` command.
# Summary of Hardware Specifications

May 22, 2017

The following table summarizes the specifications of Citrix NetScaler SD-WAN 4000, 4100, and 5100 SE hardware platforms.

<table>
<thead>
<tr>
<th>Specifications</th>
<th>SD-WAN 4000 SE</th>
<th>SD-WAN 4100 SE</th>
<th>SD-WAN 5100 SE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory Model Number</td>
<td>4x10GE SFP+8xSFP</td>
<td>2U1P1B</td>
<td>2U1P1D</td>
</tr>
<tr>
<td>Processors</td>
<td>Two 6-core</td>
<td>Two 6-core</td>
<td>Two 10-core</td>
</tr>
<tr>
<td>Memory</td>
<td>96 GB</td>
<td>96 GB</td>
<td>128 GB</td>
</tr>
<tr>
<td>Number of power supplies</td>
<td>1 (optional second power supply for redundancy)</td>
<td>1 (optional second power supply for redundancy)</td>
<td>1 (optional second power supply for redundancy)</td>
</tr>
<tr>
<td>AC power supply, input voltage, frequency and current</td>
<td>100-240VAC, 47-63 hz</td>
<td>100-240VAC, 47-63 hz 7.0-3.5A</td>
<td>100-240VAC, 47-63 hz 9.0-4.5A</td>
</tr>
<tr>
<td>Maximum AC power consumption</td>
<td>650 W</td>
<td>850 W</td>
<td>850 W</td>
</tr>
<tr>
<td>Package weight</td>
<td>69 lbs</td>
<td>69 lbs</td>
<td>69 lbs</td>
</tr>
<tr>
<td>Shipping dimensions</td>
<td>36.5’ L X 24.5’ W X 11’ H</td>
<td>36.5’ L X 24.5’ W X 11’ H</td>
<td>36.5’ L X 24.5’ W X 11’ H</td>
</tr>
<tr>
<td>System weight</td>
<td>60 lbs</td>
<td>60 lbs</td>
<td>60 lbs</td>
</tr>
<tr>
<td>Rack unit</td>
<td>2RU</td>
<td>2RU</td>
<td>2RU</td>
</tr>
<tr>
<td>Rack options - Width</td>
<td>EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets</td>
<td>EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets</td>
<td>EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting bracket</td>
</tr>
<tr>
<td>Depth</td>
<td>28” (72 cm)</td>
<td>28” (72 cm)</td>
<td>28” (72 cm)</td>
</tr>
<tr>
<td>Operating temperature</td>
<td>32 – 104 F (0 – 40 C)</td>
<td>32 – 104 F (0 – 40 C)</td>
<td>32 – 104 F (0 – 40 C)</td>
</tr>
<tr>
<td>Humidity (non-condensinal)</td>
<td>20% - 80%</td>
<td>20% - 80%</td>
<td>20% - 80%</td>
</tr>
<tr>
<td>Safety Specifications</td>
<td>SD-WAN 4000 SE</td>
<td>SD-WAN 4100 SE</td>
<td>SD-WAN 5100 SE</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>EMC and susceptibility</td>
<td>USA (FCC), Europe (CE), Japan (VCCI), Australia (RCM), China (CCC), Korea (KCC), India (BIS), Mexico (NOM), Saudi Arabia (CITC), South Africa (ICASA), Russia (EAC), Taiwan (BSMI), Brazil (Anatel), Israel (MoC)</td>
<td>USA (FCC), Europe (CE), Japan (VCCI), Australia (RCM), China (CCC), Korea (KCC), India (BIS), Mexico (NOM), Saudi Arabia (CITC), South Africa (ICASA), Russia (EAC), Taiwan (BSMI), Brazil (Anatel), Israel (MoC)</td>
<td>USA (FCC), Europe (CE), Japan (VCCI), Australia (RCM), China (CCC), Korea (KCC), India (BIS), Mexico (NOM), Saudi Arabia (CITC), South Africa (ICASA), Russia (EAC), Taiwan (BSMI), Brazil (Anatel), Israel (MoC)</td>
</tr>
<tr>
<td>Environmental compliance</td>
<td>ROHS, WEEE</td>
<td>ROHS, WEEE</td>
<td>ROHS, WEEE</td>
</tr>
</tbody>
</table>
Preparing for Installation

Mar 16, 2012
Before you install your new appliance, carefully unpack your appliance and make sure that all parts were delivered. Once you are satisfied that your appliance has been delivered to your expectations, verify that the location where the appliance will be installed meets temperature and power requirements and that the server cabinet or floor-to-ceiling cabinet is securely bolted to the floor and has sufficient airflow.

Only trained and qualified personnel should install, maintain, or replace the appliance, and efforts should be taken to ensure that all cautions and warnings are followed.
Unpacking the Appliance

May 05, 2017

Unpack the box that contains your new appliance on a sturdy table with plenty of space and inspect the contents.

Use the following list to verify that you received everything that should have been included in the box.

- The appliance you ordered
- One RJ-45 to DB-9 adapter
- One 6 ft RJ-45/DB-9 cable
- One or Two power cables depending on the platform edition
- One standard 4-post rail kit

Note: If the kit that you received does not fit your rack, contact your Citrix sales representative to order the appropriate kit.

In addition to the items included in the box with your new appliance, you will need the following items to complete the installation and initial configuration process.

- Ethernet cables for each additional Ethernet port that you will connect to your network.
- One available Ethernet port on your network switch or hub for each Ethernet port you want to connect to your network.
- A computer to serve as a management workstation.
Preparing the Site and Rack

May 15, 2017

There are specific site and rack requirements for the SD-WAN 4000/4100/5100 SE appliances. You must make sure that adequate environmental control and power density are available. Racks must be bolted to the ground, have sufficient airflow, and have adequate power and network connections. Preparing the site and rack are important steps in the installation process and help ensure a smooth installation.

Site Requirements

The appliance should be installed in a server room or server cabinet with the following features:

Environment control
An air conditioner, preferably a dedicated computer room air conditioner (CRAC), capable of maintaining the cabinet or server room at a temperature of no more than 27 degrees C/80.6 degrees F at altitudes of up to 2100 m/7000 ft, or 18 degrees C/64.4 degrees F at higher altitudes, a humidity level no greater than 45 percent, and a dust-free environment.

Power density
Wiring capable of handling at least 4,000 watts per rack unit in addition to power needs for the CRAC.

Rack Requirements

The rack on which you install your appliance should meet the following criteria:

Rack characteristics
Racks should be either integrated into a purpose-designed server cabinet or be the floor-to-ceiling type, bolted down at both top and bottom to ensure stability. If you have a cabinet, it should be installed perpendicular to a load-bearing wall for stability and sufficient airflow. If you have a server room, your racks should be installed in rows spaced at least 1 meter/3 feet apart for sufficient airflow. Your rack must allow your IT personnel unfettered access to the front and back of each server and to all power and network connections.

Power connections
At minimum, two standard power outlets per unit.

Network connections
At minimum, Ethernet connection per rack unit.

Space requirements
Two empty rack units for SD-WAN 4000/4100/5100 SE appliances.

Note

You can order the following rail kits separately.

- Compact 4-post rail kit, which fits racks of 23 to 33 inches.
- 2-post rail kit, which fits 2-post racks.
Cautions and Warnings

May 05, 2017

Electrical Safety Precautions

**Warning**
During installation or maintenance procedures, wear a grounding wrist strap to avoid ESD damage to the electronics of the appliance. Use a conductive wrist strap attached to a good earth ground or to the appliance. You can attach it to the connector beside the ESD symbol on the back.

Follow basic electrical safety precautions to protect yourself from harm and the appliance from damage.

- Be aware of the location of the emergency power off (EPO) switch, so that you can quickly remove power to the appliance if an electrical accident occurs.
- Remove all jewelry and other metal objects that might come into contact with power sources or wires before installing or repairing the appliance. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and may cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.
- Use a regulating, uninterruptible power supply (UPS) to protect the appliance from power surges and voltage spikes, and to keep the appliance operating in case of power failure.
- Never stack the appliance on top of any other server or electronic equipment.
- All appliances are designed to be installed on power systems that use TN earthing. Do not install your device on a power system that uses either TT or IT earthing.
- Make sure that the appliance has a direct physical connection to the earth during normal use. When installing or repairing an appliance, always make sure that the ground circuit is connected first and disconnected last.
- Make sure that a fuse or circuit breaker no larger than 120 VAC, 15 A U.S. (240 VAC, 16 A international) is used on all current-carrying conductors on the power system to which your appliances are connected.
- Do not work alone when working with high voltage components.
- Always disconnect the appliance from power before removing or installing any component. When disconnecting power, first shut down the appliance, and then unplug the power cords of all the power supply units connected to the appliance. As long as the power cord is plugged in, line voltages can be present in the power supply, even when the power switch is OFF.
- Do not use mats designed to decrease static electrical discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Make sure that the power source can handle the appliance's maximum power consumption rating with no danger of an overload. Always unplug any appliance before performing repairs or upgrades.
- Do not overload the wiring in your server cabinet or on your server room rack.
- During thunderstorms, or anticipated thunderstorms, avoid performing any hardware repairs or upgrades until the danger of lightning has passed.
- When you dispose of an old appliance or any components, follow any local and national laws on disposal of electronic waste.
- To prevent possible explosions, replace expired batteries with the same model or a manufacturer-recommended substitute and follow the manufacturer's instructions for battery replacement.
- Never remove a power supply cover or any sealed part.
Appliance Precautions

- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest appliance first, at the bottom of the rack, and then work upward. Distribute the load on the rack evenly. An unbalanced rack is hazardous.
- Allow the power supply units and hard drives to cool before touching them.
- Install the equipment near an electrical outlet for easy access.
- Mount equipment in a rack with sufficient airflow for safe operation.
- For a closed or multiple-unit rack assembly, the ambient operating temperature of the rack environment might be greater than the ambient temperature of the room. Therefore, consider the lowest and highest operating temperatures of the equipment when making a decision about where to install the appliance in the rack.

Rack Precautions

- Make sure that the leveling jacks on the bottom of the rack are fully extended to the floor, with the full weight of the rack resting on them.
- For a single-rack installation, attach a stabilizer to the rack.
- For a multiple-rack installation, couple (attach) the racks together.
- Always make sure that the rack is stable before extending a component from the rack.
- Extend only one component at a time. Extending two or more simultaneously might cause the rack to become unstable.
- The handles on the left and right of the front panel of the appliance should be used only for extending the appliance out of the rack. Do not use these handles for mounting the appliance on the rack. Use the rack-rail hardware, described later, instead.
Installing the Hardware

May 07, 2017

After you have determined that the location where you will install your appliance meets the environmental standards and the server rack is in place according to the instructions, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you will use for initial configuration. To complete the installation, you turn on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.
Rack Mounting the Appliance

May 11, 2017

Most appliances can be installed in standard server racks that conform to EIA-310-D specification. The appliances ship with a set of rails, which you must install before you mount the appliance. The only tools that you need for installing an appliance are a Phillips screwdriver and a flathead screwdriver.

Citrix SD-WAN 4000/4100/5100 appliances requires two rack units.

Each appliance ships with a mounting rail kit that contains two rail assemblies, one for the left side and the other for the right side of the appliance, and screws to attach the rails. An assembly consists of an inner rail and a rack rail. The supplied rail kit is 28 inches long (38 inches extended). Contact your Citrix sales representative to order a 23-inch (33 inches extended) rail kit.

To mount the appliance, you must first install the rails and then install the appliance in the rack.

Perform the following tasks to mount the appliance:

- Remove the inner rails from the rail assembly.
- Attach the inner rails to the appliance.
- Install the rack rails on the rack.
- Install the appliance in the rack.

**Note**

The same rail kit is used for both square-hole and round-hole racks. See figure 4 for specific instructions for threaded, round-hole racks.

**Warning**

If you are installing the appliance as the only unit in the rack, mount it at the bottom. If the rack contains other units, make sure that the heaviest unit is at the bottom. If the rack has stabilizing devices available, install them before mounting the appliance.

To remove the inner rails from the rail assembly

1. Place the rail assembly on a flat surface.
2. Slide out the inner rail toward the front of the assembly.
3. Depress the latch until the inner rail comes all the way out of the rail assembly.
4. Repeat steps 1 through 3 to remove the second inner rail.

To attach the inner rails to the appliance

1. Position the right inner rail behind the handle on the right side of the appliance.
2. Align the holes on the rail with the corresponding holes on the side of the appliance.
3. Attach the rail to the appliance with the provided screws: 5 per side, as shown in the following figure.
Figure 1. Attaching inner rails

To install the rack rails on the rack

1. If you have a round-hole, threaded rack, skip to step 3.
2. Install square nut retainers into the front post and back post of the rack as shown in the following figures. Before inserting a screw, be sure to align the square nut with the correct hole for your appliance. The three holes are not evenly spaced.

   Figure 2. Installing Retainers into the Front Rack Posts

   ![Figure 2](https://docs.citrix.com)

   Figure 3. Installing Retainers into the Rear Rack Posts

   ![Figure 3](https://docs.citrix.com)

3. Install the adjustable rail assembly into the rack as shown in the following figures. Use a screw to lock the rear rail flange into the rack. With the screw securing the rail in place, you can optionally remove the latching spring.

   Figure 4. Installing the Rail Assembly to the Rack

   ![Figure 4](https://docs.citrix.com)
To install the appliance in the rack

1. Align the inner rails, attached to the appliance, with the rack rails.
2. Slide the appliance into the rack rails, keeping the pressure even on both sides.
3. Verify that the appliance is locked in place by pulling it all the way out from the rack.

Figure 5. Rack Mounting the Appliance
Installing and Removing 1G SFP Transceivers

May 08, 2017

A Small Form-Factor Pluggable (SFP) is a compact transceiver that can operate at speeds of up to 1 gigabit per second and is available in both copper and fiber types. Inserting a 1G SFP copper transceiver converts the 1G SFP port to a 1000BASE-T port. Inserting a 1G SFP fiber transceiver converts the 1G SFP port to a 1000BASE-X port. Auto-negotiation is enabled by default on the 1G SFP port into which you insert your 1G SFP transceiver. As soon as a link between the port and the network is established, the speed and mode are matched on both ends of the cable.

**Note**

Some SD-WAN Standard Edition appliances do not require SFP transceivers.

**Important**

SFP transceivers must be ordered separately. With exception to fiber FTW ports that have integrated transceivers, which are not removable.

To install a 1G SFP transceiver

1. Remove the 1G SFP transceiver carefully from its box.
   
   Align the 1G SFP transceiver to the front of the 1G SFP transceiver port on the front panel of the appliance, as shown in the following figure.

   ![Image of 1G SFP transceiver installation](image)

   **Warning**

   Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.

2. Hold the 1G SFP transceiver between your thumb and index finger and insert it into the 1G SFP transceiver port, pressing it in until you hear the transceiver snap into place.
3. Lock the transceiver.

4. Verify that the LED is green and blinks twice, which indicates that the transceiver is functioning correctly.

5. If you are using a fiber 1G SFP transceiver, do not remove the dust caps attached to the transceiver and the cable until you are ready to insert the cable.

To remove a 1G SFP transceiver

1. Disconnect the cable from the 1G SFP transceiver. If you are using a fiber optic cable, replace the dust cap on the cable before putting it away.
   Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.
2. Unlock the 1G SFP transceiver.
3. Hold the 1G SFP transceiver between your thumb and index finger and slowly pull it out of the port.
4. If you are removing a fiber 1G SFP transceiver, replace the dust cap before putting it away.
5. Put the 1G SFP transceiver into its original box or another appropriate container.

**Warning**

Insert 1G SFP transceivers into the 1G SFP ports on the front panel of the appliance. Frequent installation and removal of transceivers shortens their life span. Follow the removal procedure carefully to avoid damaging the 1G SFP transceiver or the appliance.

Do not install the transceivers with the cables attached. Doing so can damage the cable, the connector, or the optical interface of the transceiver.
Installing and Removing 10G SFP+ Transceivers

May 11, 2017

A 10-Gigabit Small Form-Factor Pluggable (SFP+) is a compact optical transceiver that can operate at speeds of up to 10 gigabits per second. Autonegotiation is enabled by default on the 10G SFP+ ports into which you insert your 10G SFP+ transceiver. As soon as a link between the port and the network is established, the mode is matched on both ends of the cable and for 10G SFP+ transceivers, the speed is also autonegotiated.

Important

SFP transceivers must be ordered separately. With exception to fiber FTW ports that have integrated transceivers, which are not removable.

To install a 10G SFP+ transceiver

1. Remove the 10G SFP+ transceiver carefully from its box. Align the 10G SFP+ transceiver to the front of the 10G SFP+ transceiver port on the front panel of the appliance.
2. Hold the 10G SFP+ transceiver between your thumb and index finger and insert it into the 10G SFP+ transceiver port, pressing it in until you hear the transceiver snap into place.
3. Move the locking hinge to the DOWN position.
4. Verify that the LED is green and blinks twice, which indicates that the transceiver is functioning correctly.
5. Do not remove the dust caps attached to the transceiver and cable until you are ready to insert the cable.

Warning

Do not look directly into fiber optic transceivers and cables. They emit laser beams that can damage your eyes.

To remove a 10G SFP+ transceiver

1. Disconnect the cable from the 10G SFP+ transceiver. Replace the dust cap on the cable before putting it away.
   Danger: Do not look directly into fiber optic transceivers or cables. They emit laser beams that can damage your eyes.
2. Unlock the 10G SFP+ transceiver by moving the locking hinge to the UP position.
3. Hold the 10G SFP+ transceiver between your thumb and index finger and slowly pull it out of the port.
4. Replace the dust cap on the transceiver before putting it away.
5. Put the 10G SFP+ transceiver into its original box or another appropriate container.

Warning

Insert the 10G SFP+ transceivers into the 10G SFP+ ports on the front panel of the appliance. Frequent installation and removal of transceivers shortens their life span. Follow the removal procedure carefully to avoid damaging the transceiver or the appliance.

Do not install the transceivers with the cables attached. Doing so can damage the cable, the connector, or the optical interface of the transceiver.
Connecting the Cables

When the appliance is securely mounted on the rack, you are ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

**Warning**

Before installing or repairing the appliance, remove all jewelry and other metal objects that might come in contact with power sources or wires. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.

Connecting the Appliance to the Network

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on a 10/100/1000BASE-T port.

**To connect an Ethernet cable to a 10/100/1000BASE-T port**

1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port on the front panel of the appliance, as shown in the following figure.
   
   ![Figure 1. Inserting an Ethernet cable](image)

   2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.

   3. Verify that the LED glows amber when the connection is established.

Connecting the Console Cable

You can use the console cable to connect your appliance to a computer or terminal, from which you can configure the appliance. Before connecting the console cable, configure the computer or terminal to support VT100 terminal emulation, 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE. Then connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

**To connect the console cable to a computer or terminal**

1. Insert the DB-9 connector at the end of the cable into the console port that is located on the front panel of the appliance.
2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.

**Note**
To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.

**Connecting the Appliance to a Power Source**

The SD-WAN 4100/5100 SE appliances have two power supplies, with one serving as a backup. A separate ground cable is not required, because the three-prong plug provides grounding. Power up the appliance by installing one or both power cords.

**To connect the appliance to the power source**

1. Connect one end of the power cable to the power outlet on the back panel of the appliance, next to the power supply, as shown in the following figure.  
   Figure 3. Inserting a power cable

3. Connect the other end of the power cable to a standard 110V/220V power outlet.

4. Repeat steps 1 and 2 to connect the second power supply.

**Note**
The appliance emits a high-pitched alert if one power supply fails or if you connect only one power cable to the appliance. To silence the alarm, you can press the small red button located on the back panel of the appliance.
Switching on the Appliance

May 08, 2017

After you have installed the appliance in a rack and connected the cables, verify that the power cable is properly connected. If you have installed a second power supply, make sure the second cable is connected to an outlet for a different circuit than the first. After verifying the connections, you are ready to switch on the appliance.

To switch on the appliance

1. Verify that the appliance is connected through a console or Ethernet port. This will ensure that you can configure the appliance after it is switched on.

2. Press the ON/OFF toggle power switch on the back panel of the appliance.

Warning

Be aware of the location of the emergency power off (EPO) switch, so that if an electrical accident occurs you can quickly remove power from the appliance.
Planning the Deployment

May 15, 2017
SD-WAN 4000/4100/5100 deployments require adequate planning, especially for units deployed in large datacenters:

- An appropriate appliance or group of appliances must be selected to support both the current and anticipated load.
- A deployment mode must be selected to match the requirements of your site.
- Other aspects must also be considered.
Sizing Guidelines

May 07, 2017

For successful deployment of one or more SD-WAN 4000/4100/5100 appliances in your datacenter, keep the following principles in mind:

- You must provide enough SD-WAN 4000/4100/5100 peak-load capacity, in terms of WAN bandwidth and the number of users. See the current specifications sheet for the capacities of different SD-WAN 4000/4100/5100 models: https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/netscaler-sd-wan-datasheet.pdf
- Provide enough capacity for expected expansion over the life of the deployment. SD-WAN 4000/4100/5000 appliances using the same hardware platform can have their capacity upgraded with a new license as part of the Citrix pay-as-you-grow program.
- For more capacity than can be provided by a single appliance, multiple SD-WAN 4000/4100/5100 appliances can be cascaded behind a stand-alone NetScaler appliance.
- Different models have differing numbers of traffic ports. If you require multiple bridges, make sure your model has at least as many as you need.
Selecting a Deployment Mode

May 15, 2017

The SD-WAN 4000/4100/5100 appliance can be deployed inline or in a one-arm mode. Inline deployments do not require router reconfiguration; one-arm modes do. SD-WAN 4000/4100/5100 offers internal port bypassing (fail-to-wire) to allow traffic to continue flowing in inline mode if the appliance fails.

Deploying a Single SD-WAN 4000/4100/5100 Appliance (or HA Pair)

A standalone SD-WAN 4000/4100/5100 appliance can be deployed in either of these recommended modes:
- Inline, bridged (L2 inline). This closely resembles a standard SD-WAN inline deployment. Packets enter one bridge port and exit the other bridge port.
- Inline, routed. The NetScaler instance uses routing rules instead of bridging rules to determine how to forward packets.
- Virtual inline. This resembles WCCP, but lacks built-in health-checking.

In L2 inline mode, SD-WAN 4000/4100/5100 is placed between your LAN and your WAN router (or other aggregation point at the LAN-WAN boundary). In a one-arm mode, SD-WAN 4000/4100/5100 is generally connected directly to a dedicated port on your WAN router.

In cases where the WAN router ports are not as fast as the LAN (for example, when the WAN router has gigabit Ethernet, but the LAN has 10 gigabit Ethernet), inline mode provides better performance, because its LAN-side traffic is not limited to the speed of the router interface. (Compression allows the LAN-side traffic to be much faster than WAN-bound traffic under favorable conditions.)

Considerations:
- The inline modes require no reconfiguration of your routers, but involves a service disruption when bringing the appliance into service.
- One-arm modes require router reconfiguration but do not require a service disruption.
- Inline mode has higher performance than the other modes.
- One-arm modes are limited to half the speed of the router or switch port they are attached to.

Recommendation:
- Inline mode is convenient for smaller WAN networks and simpler datacenters.
Gathering Information Needed for Configuration

May 07, 2017

Accurate information about both the local and the remote sites is essential to troubleshooting. Before installing the SD-WAN 4000/4100/5100 appliance, make sure that you have done the following:

1. Obtained or drawn an accurate network diagram of your local site (the one in which you are installing SD-WAN 4000/4100/5100). The local network topology and the capabilities of your WAN routers determine which deployment modes are appropriate for the site.

2. Chosen the deployment mode of the local SD-WAN 4000/4100/5100 appliance (inline, with or without HA and cascading).

3. Compiled a list of critical applications that must be tested to validate the deployment.

4. Obtained or drawn an accurate network diagram of your WAN, including both the local and the remote WAN links, their bandwiths in both directions, their subnets. In deployments with many remote sites, an aggregate of the different categories (accelerated and non-accelerated) is probably sufficient, and only the largest remote sites need to be considered individually.

5. Determined whether there are multiple datacenters with datacenter-to-datacenter traffic, and whether any remote datacenters have a SD-WAN 4000/4100/5100 appliance.

6. Decided whether you plan to increase WAN capacity, the number of sites, or the number of users in the next 24 months. If so, the corresponding SD-WAN 4000/4100/5100 capacity should be installed now.

7. If possible, formed an idea of the traffic breakdown over the WAN, including TCP traffic to and from SD-WAN sites, other TCP traffic, ICA users, and real-time traffic such as VoIP. SD-WAN 4000/4100/5100 needs to be provisioned for the peak loads in terms of accelerated TCP connections, ICA users, and total WAN link capacity.

8. Determined the number of WAN links in the local site. Are they independent, or are they load balanced? If so, are they active-active or active-standby?

9. Determined the current, unaccelerated RTT of the remote sites during peak periods.

10. Identified any QoS devices or proxies in the path between the local and remote sites. QoS devices should be on the WAN side of SD-WAN 4000/4100/5100. Proxies should be on the LAN side.
Initial Configuration

May 07, 2017

After checking the connections, you are ready to deploy the SD-WAN 4000, 4100, and 5100 appliances on the network.

The appliance shipped from Citrix has default IP addresses configured on it. To deploy the appliance on the network, you must configure the appropriate IP addresses on the appliance to accelerate the network traffic.

Initial configuration consists of the following tasks:
- Identify the prerequisites for the initial configuration.
- Record various values required in the initial configuration procedure.
- Configure the appliance by connecting it to the Ethernet port.
- Assign management IP address through the serial console.

By default, the fail-to-wire network adapters are in bypass state.
Configuring the Appliance

May 07, 2017
Before you start configuring the appliance, you must change the IP address of the management service to the one in your management network, so that you can access the appliance over the network. You can change the management IP address by connecting a computer to the appliance through either the Ethernet port or the serial console.
Assigning a Management IP Address through the Ethernet Port

Aug 25, 2017

Use the following procedure for initial configuration of every SD-WAN 4000, 4100, or 5100 appliance. The procedure accomplishes the following tasks:

- Configure the appliance for use on your site.
- Install the Citrix license.

For detailed steps, see Assigning a Management IP Address.

If you want to configure the appliance by connecting it to the computer through the serial console, assign the management service IP address from your Worksheet by completing the Assigning a Management IP Address through the Serial Console procedure, and then run steps 4 through 11 of the following procedure.

Note: You must have physical access to the appliance.

To configure the appliance by connecting a computer to the SD-WAN appliance’s Ethernet port 0/1

1. Set the Ethernet port address of a computer (or other browser-equipped device with an Ethernet port), to 192.168.100.1, with a network mask of 255.255.0.0. On a Windows device, this is done by changing the Internet Protocol Version 4 properties of the LAN connection, as shown below. You can leave the gateway and DNS server fields blank.
2. Using an Ethernet cable, connect this computer to the port labeled PRI on the SD-WAN appliance.
3. Switch on the appliance. Using the web browser on the computer, access the appliance by using the default management service IP address, which is http://192.168.1.1.
4. On the login page, use the following default credentials to log on to the appliance, user: admin and password: password.
5. A redirection to new management IP message appears.
6. Click OK.
7. Unplug your computer from the Ethernet port and connect the port to your management network.
8. Reset the IP address of your computer to its previous setting.
9. From a computer on the management network, log on to the appliance by entering the new management service IP address, such as https://<Management_IP_Address>, in a web browser.
10. To continue the configuration, accept the certificate and continue. The option to continue varies according to the web browser you are using.
11. Log on to the appliance.
Assigning a Management IP Address through the Serial Port

Aug 25, 2017
If you do not want to change the settings of your computer, you can configure the appliance by connecting it to your computer with a serial null modem cable. You must have physical access to the appliance.

For more information, see the Assigning a Management IP address through the serial port procedure.
Deployment Modes

May 07, 2017
SD-WAN 4000/4100/5100 SE appliances have one recommended deployment mode: Inline. This mode is commonly used without high availability (HA), and less commonly with HA.

Although not all of the following modes are recommended at this time, they are all supported:

- Inline mode
- Inline mode in HA
- Virtual inline mode
- Virtual inline mode in HA
Virtual Inline Mode

May 07, 2017

In virtual inline mode, the router uses policy based routing (PBR) rules to redirect incoming and outgoing WAN traffic to the appliance and the appliance forwards the processed packets back to the router.

The tasks for configuring virtual inline mode are performed on the router.

See the Virtual Inline Deployment mode instructions for more information.
Configuring the High Availability Setup on the Appliances

May 16, 2017

High Availability (HA) is supported in all deployment modes, and the HA configuration procedure is the same for all modes. The two appliances should be running identical hardware, licensing, and software releases, and must be deployed identically, using the same deployment modes on the same subnets.

To learn more about setting up high availability on SD-WAN appliances, see the High Availability section.
NetScaler SD-WAN 1000, 2000, and 2100 Standard Edition Appliances

May 17, 2017
The SD-WAN Standard Edition 1000, 2000, and 2100 appliances combine virtualized instances of the SD-WAN appliance.

The SD-WAN Standard Edition 1000, 2000, and 2100 appliances are based on the Citrix branch architecture, which supports multiple virtual machines. All branch appliances contain a SD-WAN Standard Edition instance and management service instance.

The SD-WAN instance is typically used in inline mode, with the SD-WAN instance interposed between the WAN router and the LAN. The SD-WAN instance can also be deployed in virtual inline mode.

The appliance has two modes; two-port mode and four-port mode, which determine how ports 1/3 and 1/4 are used.
Netscaler SD-WAN 1000 SE

May 16, 2017

The SD-WAN 1000-SE with platform has a quad-core processor and 32 GB of memory. This platform has a bandwidth of up to 100 Mbps.

The following figure shows the front panel of a SD-WAN 1000-SE appliance.

Figure 1. Citrix NetScaler SD-WAN 1000-SE front panel

The front panel of the SD-WAN 1000-SE appliance has a power button and five LEDs.

The power button is used to switch the appliance on or off.

The reset button restarts the appliance.

The LEDs provide critical information related to different parts of the appliance.

- Power Fail – Indicates the power supply unit has failed.
- Information LED – Indicates the following:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuously ON and red</td>
<td>The appliance is overheated. (This might be a result of cable congestion.)</td>
</tr>
<tr>
<td>Blinking red (1Hz)</td>
<td>Fan failure, check for an inoperative fan.</td>
</tr>
<tr>
<td>Blinking red (0.25Hz)</td>
<td>Power failure, check for the non-operational power supply.</td>
</tr>
<tr>
<td>Solid blue</td>
<td>Local UID has been activated. Use this function to locate the server in a rack mount environment.</td>
</tr>
<tr>
<td>Blinking blue (300 m/s)</td>
<td>Remote UID is on. Use this function to identify the server from a remote location.</td>
</tr>
</tbody>
</table>

- NIC1 and NIC2 – Indicate network activity on the LAN1 and WAN1 ports.
- HDD – Indicates the status of the hard disk drive.
Power – Indicates that the power supply units are receiving power and operating normally.

The following figure shows the back panel of a SD-WAN 1000-SE appliance.

Figure 2. Citrix NetScaler SD-WAN 1000-SE appliance, back panel

The following components are visible on the back panel of a SD-WAN 1000-SE appliance:

- Cooling fan.
- Single power supply, rated at 200 watts, 110-240 volts.
- Accelerated pairs of Ethernet ports (apA and apB).
- RS-232 serial console port.
- One AUX Ethernet port and one management port.
- Two USB ports.

Power on Appliance After Graceful Shut Down

To power on the appliance after a graceful shut down:

1. Connect a Serial console cable to the rear of the appliance and to the serial port on a management laptop.

2. On the management laptop, restart a putty session using the following configuration settings:
   - Serial line: COM1
   - Speed: 9600

3. Power on the appliance and as it is booting, press the following key in the Putty session to enter the BIOS configuration screen.

   **Keypress: DEL**

4. When in the BIOS, navigate to,
5. When in the Boot Feature screen, change the value of the parameter **Restore on AC Power Loss**; from **Last State > Power ON**.

6. Navigate to Save and Exit.
   - Select **Save changes** and **Reset**.
   - Select **Yes**.

   Allow the system to restart. This takes approximately five minutes.
7. After the appliance is powered on, login to the appliance management instance (SVM). The default IP address for the appliance is: 192.168.100.1, user name is: admin/password.

8. In the SD-WAN appliance GUI, navigate to Configuration > Maintenance > Reboot Appliance. Allow the appliance to fully shut down. Ensure that there are no power lights on the appliance when the shut down process has completed.
9. Power on the appliance to confirm that the BIOS configuration change has been applied successfully. This can be either done through the APC intelligent PDU Web Management console or by physically pulling the power cable out of the shut down SD-WAN appliance, waiting for 10 seconds and then plugging it back in again. The appliance power ups automatically from all shut down scenarios.
The Citrix NetScaler SD-WAN 2000-SE platform is a 1U appliance with one quad-core processor and 24 gigabytes (GB) of memory.

The following figure shows the front panel of the SD-WAN 2000-SE appliance.

Figure 1. Citrix NetScaler SD-WAN 2000-SE appliance, front panel

SD-WAN 2000-SE appliance has the following ports:

- An RS232 serial console port.
- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.
- A copper Ethernet (RJ45) management port, numbered 0/1, and named PRI (primary). The management port is used to connect directly to the appliance for system administration functions. You can use this port for initial provisioning of Virtual WAN. The LOM port also operates as a management port.
- Four 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right. The four ports form two accelerated pairs, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA), and 1/3 and 1/4 are accelerated pair B (apB).

Figure 2. Citrix NetScaler SD-WAN 2000-SE appliance, back panel

The following components are visible on the back panel of the SD-WAN 2000-SE appliance:

- 600 GB removable solid-state drive, which stores the appliance's software and user data, and 1 TB hard disk drive.
- Power switch. Press the switch for five seconds to switch off the power.
- USB port (reserved for a future release).
- Non-maskable interrupt (NMI) button, for use at the request of Technical Support to produce a core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Single power supply, rated at 300 watts, 100-240 volts.
The Citrix NetScaler SD-WAN 2100-SE platform is a 1U appliance with 8 core processor and 32 gigabytes (GB) of memory.

The following figure shows the front panel of the SD-WAN 2100-SE appliance.

**Figure 1. Citrix NetScaler SD-WAN 2100-SE appliance, front panel**

SD-WAN 2100-SE appliance has the following ports:

- An RS232 serial console port.
- Copper Ethernet (RJ45) Port called the Lights out Management (LOM) port labelled LOM, and management port labelled 0/1. You can use these ports to remotely monitor and manage the appliance independently of the appliance's software.
- USB ports.
- Four 1000Base-TX copper Ethernet ports.
- Four 1GE SFP ports.

<table>
<thead>
<tr>
<th>Port Labels - old 2100-SE Front Bezel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOM</td>
<td>Lights Out Management</td>
</tr>
<tr>
<td>0/1</td>
<td>Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port Labels - new 2100-SE Front Bezel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOM 0/1</td>
<td>Lights Out Management</td>
</tr>
<tr>
<td>0/2</td>
<td>Reserved for future use (Management)</td>
</tr>
</tbody>
</table>

- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port labelled LOM and 0/1. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.
- A copper Ethernet (RJ45) management port, labelled 0/2. This management port cannot be used for system
administration functions. This port is reserved for future use.

Figure 2. Citrix NetScaler SD-WAN 2100-SE appliance, back panel

The following components are visible on the back panel of the SD-WAN 2100-SE appliance:

- 240 GB removable solid-state drive, which stores the appliance's software and user data, and 1 TB hard disk drive.
- Power switch, which switches power to the appliance on or off. Press the switch for five seconds to switch off the power.
- Non-maskable interrupt (NMI) button, for use at the request of Technical Support to produce a core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Single power supply, rated at 450 watts, 100-240 volts.

Upgrade 2100 SE Appliance to 2100 EE Appliance

Insert Solid State Drive (SSD)

1. Insert the required SSD in the standard edition appliance. For instructions about how to insert SSD, see Solid State Drive (Field Replaceable Unit).

2. Restart the appliance through the SD-WAN web management interface.

3. Ensure that the software release version installed on the appliance is SD-WAN release version 9.3.3.

Appliances shipped with software release version 9.2.1 or earlier

For appliances shipped with software release version 9.2.1 or earlier versions, upgrade the appliances to software release version 9.3.3. Follow the steps below:

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

c. Press the number 1 key (**SHIFT** + 1 = !) and release all keys.

d. Repeat steps a, b, and c until the cursor stops moving.

**Note**

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

5. When BIOS loads, choose the external USB drive, for example; Sandisk to boot the appliance.
6. Confirm the reimage by selecting **Yes** to proceed, then press the **Enter** key.

Upgrade process takes approximately 30-40 minutes to complete. The system reboots after 1-2 minutes and the login prompt is displayed.
7. Unplug USB stick after the procedure is complete.

The reimage process will begin after the edition selection menu appears. Note that on the 1000 and 2000 appliances, “Enterprise Edition” will be listed, but after reimage, the Standard Edition will be presented in the GUI when accessing the default IP address 192.168.100.1, and Enterprise Edition will only be available upon installation of an Enterprise Edition license file.

Note

All Enterprise Edition appliances have Standard Edition software installed as the core software. The WANOP instance is dormant making the appliance a Standard Edition appliance, until the appropriate Enterprise Edition license is installed and configuration in place to enable WANOP capabilities on an EE appliance.


9. Perform single step upgrade to upgrade appliance software release version from 9.3.3 to 10.0. For more information, see: upgrading and updating software.

10. Enable WANOP as a feature of Enterprise Edition sites in the Configuration Editor of the MCN appliance or SD-WAN Center.

Configure Management IP Address Using Serial Console

1. Access serial console of the appliance.
2. Log in to dom0 using the root/nsroot credentials.
3. Type the \texttt{ssh admin@169.254.0.60 -l admin} command.
4. Type password: \texttt{password}.
5. Type the \texttt{management_ip} command.
6. Type the \texttt{set interface 192.168.100.1 255.255.255.0 192.168.100.254} command.
7. Type the \texttt{apply} command.
# Summary of Hardware Specifications

May 22, 2017

The following table summarizes the specifications of the SD-WAN 1000-SE, 2000-SE, and 2100-SE hardware platforms.

<table>
<thead>
<tr>
<th>Specifications</th>
<th>SD-WAN 1000-SE</th>
<th>SD-WAN 2000-SE</th>
<th>SD-WAN 2100-SE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>Upto 100 Mbps</td>
<td>Upto 300 Mbps</td>
<td>Upto 1.5 Gbps</td>
</tr>
<tr>
<td>Total sessions, Max Virtual Paths</td>
<td>10,000</td>
<td>20,000</td>
<td>128/32</td>
</tr>
<tr>
<td>(Static/Dynamic)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td>4 Cores</td>
<td>4 Cores</td>
<td>8-Core 2.1GHz</td>
</tr>
<tr>
<td>Total Disk Space</td>
<td>1X480 GB SSD</td>
<td>1X800 GB SSD</td>
<td>1X240 GB SSD</td>
</tr>
<tr>
<td>RAM</td>
<td>16 GB</td>
<td>24 GB</td>
<td>32 GB</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>2 pair with bypass 10/100/1000</td>
<td>2 pair with bypass 10/100/1000</td>
<td>2 pair with bypass of 1G 4 x 1GE SFP 2 GigE ports for Management and AUX ports</td>
</tr>
<tr>
<td>Power Supplies</td>
<td>1</td>
<td>1</td>
<td>1 module and 1 optional FRU</td>
</tr>
<tr>
<td>Rack Units</td>
<td>1U</td>
<td>1U</td>
<td>1U</td>
</tr>
<tr>
<td>System Width</td>
<td>EIA 310-D for 19-inch racks</td>
<td>EIA 310-D for 19-inch racks</td>
<td>EIA 310-D for 19-inch racks</td>
</tr>
<tr>
<td>System Depth</td>
<td>10&quot; (25.4 cm)</td>
<td>28&quot; (7.2 cm)</td>
<td>28&quot; (7.2 cm)</td>
</tr>
<tr>
<td>System Weight</td>
<td>8.5 lbs (3.9 kg)</td>
<td>32 lbs (14.5 kg)</td>
<td>32 lbs (14.5 kg)</td>
</tr>
<tr>
<td>Shipping dimensions and weight</td>
<td>26 L x 18.5 W x 6.5&quot; H 14.5 lbs</td>
<td>32 L x 23.5 W x 7.5&quot; H 39 lbs</td>
<td>33&quot; L x 24&quot; W x 8&quot; H 40 lbs</td>
</tr>
<tr>
<td>Voltage</td>
<td>100/240 VAC, 50-60 Hz</td>
<td>100/240 VAC, 50-60 Hz</td>
<td>100/240 VAC, 50-60 Hz</td>
</tr>
<tr>
<td>Power consumption (Max.)</td>
<td>200 W</td>
<td>300 W</td>
<td>450 W</td>
</tr>
<tr>
<td>Operating Temperature (degree Celsius)</td>
<td>10–35</td>
<td>0–40</td>
<td>0–40</td>
</tr>
<tr>
<td>Non-operating</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specifications</td>
<td>SD-WAN 1000-SE</td>
<td>SD-WAN 2000-SE</td>
<td>SD-WAN 2100-SE</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allowed Relative Humidity</td>
<td>8% – 90% non-condensing</td>
<td>5%–95% non-condensing</td>
<td>20%-80% non-condensing</td>
</tr>
<tr>
<td>Safety certifications</td>
<td>CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)</td>
<td>CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)</td>
<td>CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)</td>
</tr>
<tr>
<td>Electromagnetic and susceptibility certifications</td>
<td>FCC Class A, EN 55022 Class A, EN 61000-3-2/-3-3, CISPR 22 Class A</td>
<td>FCC (Part 15 Class A), CE, C-Tick, VCCI-A, CCC, KCC, NOM, SASO, SABS, PCT</td>
<td>FCC (Part 15 Class A), CCC, KCC, NOM, CICT, EAC, DoC, CE, VCCI, RCM</td>
</tr>
<tr>
<td>Environmental certifications</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
</tr>
</tbody>
</table>
Installing the Appliance

Apr 03, 2017

After you have determined that the location where you will install your appliance meets the environmental standards and the server rack is in place according to the instructions, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you will use for initial configuration. You can also connect the appliance to a computer through Ethernet port for initial configuration. On SD-WAN 1000-SE appliance, this port is labeled as MGMT (management) port and on SD-WAN 2000-SE and SD-WAN 2100-SE appliances, the port is labeled as PRI (primary) port. To complete the installation, you switch on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.
Rack Mounting the Appliance

Apr 09, 2014
A SD-WAN 1000-SE or 2000-SE appliance requires one rack unit. Both are rack-mount devices that can be installed into two-post relay racks or four-post EIA-310 server racks. Verify that the rack is compatible with your appliance.
Rack Mounting an SD-WAN 1000-SE Appliance

Apr 09, 2014
SD-WAN 1000-SE appliance is not shipped with rails. You can mount the appliance to the rack by using the front mounting ports.
Rack Mounting an SD-WAN 2000-SE Appliance

Apr 09, 2014

A SD-WAN 2000-SE appliance requires one rack unit. Both are rack-mount devices that can be installed into two-post relay racks or four-post EIA-310 server racks. Verify that the rack is compatible with your appliance.

To mount a SD-WAN appliance, you must first install the rails and then install the appliance in the rack, as follows:

- Remove the inner rails from the rail assembly.
- Attach the inner rails to the appliance.
- Install the rack rails on the rack.
- Install the appliance in the rack.

To remove the inner rails from the rail assembly

1. Place the rail assembly on a flat surface.
2. Slide out the inner rail toward the front of the assembly.
3. Depress the locking tabs until the inner rail comes all the way out of the rail assembly.
4. Repeat steps 1 through 3 to remove the second inner rail.

To attach the inner rails to the appliance

1. Position the right inner rail behind the ear bracket on the right side of the appliance.
2. Align the holes on the rail with the corresponding holes on the side of the appliance.
3. Attach the rail to the appliance with the provided screws.
4. Repeat steps 1 through 3 to install the left inner rail on the left side of the appliance.

To install the rack rails

1. Position the rack rails at the desired location in the rack, keeping the sliding rail guide facing inward.
2. Snap the rails to the rack.
   - Note: Make sure that both rack rails are at same height and that the rail guides are facing inward.

To install the appliance in the rack

1. Align the inner rails, attached to the appliance, with the rack rails.
2. Slide the appliance into the rack rails, keeping the pressure even on both sides, and push the appliance into the rack rails until it locks into place.
3. Verify that the appliance is locked in place by pulling it all the way out from the rack.
   - Note: The illustration in the following figure might not represent your actual appliance.

Figure 1. Rack Mounting the Appliance
Connecting the Cables

Jun 12, 2014

When the appliance is securely mounted on the rack, determine which ports you should use. You are then ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

Warning: Before installing or repairing the appliance, remove all jewelry and other metal objects that might come in contact with power sources or wires. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.

Ports

A typical installation using a single accelerated bridge uses four Ethernet ports (the Primary port and apA) and six IP addresses (four on the Primary port’s subnet and two on apA’s subnet).

The appliance has two motherboard ports and two accelerated bridges.

- The motherboard ports are labeled as MGMT (management) and AUX1 (auxiliary) ports in SD-WAN 1000-SE appliance and PRI (primary) and AUX (auxiliary) in SD-WAN 2000-SE appliance. You use MGMT port of the SD-WAN 1000-SE appliance and PRI port of the SD-WAN 2000-SE appliance for initial configuration.
- Accelerated bridge ports are apA and apB are available on the back panel of SD-WAN 1000-SE appliance and the front panel of SD-WAN 2000-SE appliance. On 1000-SE appliance, these ports are labeled as LAN1 and WAN1, and LAN2 and WAN2, respectively. However, on 2000-SE appliance, these ports are labeled as 1/1 and 1/2, and 1/3 and 1/4, respectively.

Connecting the Ethernet Cables

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on a 10/100/1000BASE-T port.

To connect an Ethernet cable to a 10/100/1000BASE-T port

1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port.
   - On 1000-SE appliance, the ports are available on the back panel and labeled as LAN1 and WAN1 for apA bridged port for LAN and WAN links, respectively.
   - On 2000-SE appliance, the ports are available on the front panel. The ports are labeled as 1/1 and 1/2 for the apA bridged port. You can use 1/1 for LAN and 1/2 for WAN link.

2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.
3. Verify that the LED glows amber when the connection is established.

Connecting the Console Cable

You can use the console cable to connect your appliance to a computer or terminal, from which you can configure the appliance. Before connecting the console cable, configure the computer or terminal to support VT100 terminal emulation, 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE. Then connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

To connect the console cable to a computer or terminal

1. Insert the DB-9 connector at the end of the cable into the console port.
   - On 1000-SE appliance, the port is located on the back panel.
   - On 2000-SE appliance, the port is located on the front panel.
Note: To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.

2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.

Connecting the Power Cable

A SD-WAN appliance has one power supply. A separate ground cable is not required, because the three-prong plug provides grounding. Provide power to the appliance by installing the power cord. Connect the other end of the power cable to a standard 110V/220V power outlet.
Switching on the Appliance

Jun 12, 2014

After you have installed the appliance in a rack and connected the cables, verify that the power cable is properly connected. After verifying the connections, you are ready to switch on the appliance.

To switch on the appliance

1. Verify that the appliance is connected through a console or Ethernet port, so that you can configure the appliance after it is switched on.
2. Press the ON/OFF toggle power switch on the appliance. The power button is at the rear of the SD-WAN 2100-SE appliance.
3. On SD-WAN 2000-SE and 2100-SE appliances, verify that the LCD on the front panel is backlit and the start message appears.

Caution: Be aware of the location of the emergency power off (EPO) switch, so that if an electrical accident occurs, you can quickly remove power from the appliance.
Initial Configuration

Aug 12, 2014
After checking the connections, you are ready to deploy the SD-WAN 1000-SE and 2000-SE appliances on the network.

The appliance shipped from Citrix has default IP addresses configured on it. To deploy the appliance on the network, you must configure the appropriate IP addresses on the appliance to accelerate the network traffic.

To perform initial configuration:

- Identify the prerequisites for the initial configuration.
- Record various values required in the initial configuration procedure.
- Configure the appliance by connecting it to the Ethernet port.
- Perform additional configuration for Windows.
- Assign management IP address through the serial console.
- Troubleshoot initial configuration issues.

By default, the initial configuration deploys the appliance in inline mode.
Setting up the SD-WAN Appliance

Jun 20, 2017

Before you start configuring the appliance, you must change the IP address of the management service to the one in your management network, so that you can access the appliance over the network. You can change the management IP address by connecting a computer to the appliance through either the Ethernet port or the serial console.

To set up your NetScaler SD-WAN Appliance hardware, see the instructions documented in the Setting up the Appliance Hardware section.

To provision and configure the SD-WAN appliance, see the instructions documented in the Getting Started with SD-WAN section.

Use the following procedure for initial configuration of every SD-WAN 4000, 4100, or 5100 appliance. The procedure accomplishes the following tasks:

- Configure the appliance for use on your site.
- Install the Citrix license.

For detailed steps, see Assigning a Management IP Address.

If you want to configure the appliance by connecting it to the computer through the serial console, assign the management service IP address from your Worksheet by completing the Assigning a Management IP Address through the Serial Console procedure, and then run steps 4 through 11 of the following procedure.

Note: You must have physical access to the appliance.

To configure the appliance by connecting a computer to the SD-WAN appliance’s Ethernet port 0/1:

1. Set the Ethernet port address of a computer (or other browser-equipped device with an Ethernet port) to 192.168.100.1, with a network mask of 255.255.0.0. On a Windows device, this is done by changing the Internet Protocol Version 4 properties of the LAN connection, as shown below. You can leave the gateway and DNS server fields blank.
2. Using an Ethernet cable, connect this computer to the port labeled PRI on the SD-WAN appliance.
3. Switch on the appliance. Using the web browser on the computer, access the appliance by using the default management service IP address, which is http://192.168.100.1.
4. On the login page, use the following default credentials to log on to the appliance, user: admin and password: password.
5. A redirection to new management IP message appears.
6. Click OK.
7. Unplug your computer from the Ethernet port and connect the port to your management network.
8. Reset the IP address of your computer to its previous setting.
9. From a computer on the management network, log on to the appliance by entering the new management service IP address, such as https://<Management_IP_Address>, in a web browser.
10. To continue the configuration, accept the certificate and continue. The option to continue varies according to the web browser you are using.
11. Log on to the appliance.
Deployment Modes

May 22, 2017

SD-WAN 1000, 2000, and 2100 SE appliances have one recommended deployment mode: Inline. This mode is commonly used without high availability (HA), and less commonly with HA.

Although not all of the following modes are recommended at this time, the following modes are supported:

- Inline mode
- Inline mode in HA
- Virtual inline mode
- Virtual inline mode in HA

The forwarding modes are:

- **Inline mode**, in which the appliance transparently accelerates traffic flowing between its two Ethernet ports. In this mode, the appliance appears (to the rest of the network) to be an Ethernet bridge. Inline mode is recommended, because it requires the least configuration.

- **Virtual inline mode**, in which a router sends WAN traffic to the appliance and the appliance returns it to the router. In this mode, the appliance appears to be a router, but it uses no routing tables. It sends the return traffic to the real router. Virtual inline mode is recommended when inline mode and high-speed WCCP operation are not practical.

- **High availability mode**, which allows to appliances to operate as an active/standby high availability pair. If the primary appliance fails, the secondary appliance takes over.
Virtual Inline Mode

May 22, 2017

Note

Use virtual inline mode only when inline mode is not possible. Do not mix inline and virtual inline modes within the same appliance. However, you can mix virtual inline and WCCP (WANOP appliance supported deployment) modes within the same appliance. Citrix does not recommend virtual inline mode with routers that do not support health monitoring.

In virtual inline mode, the router uses policy based routing (PBR) rules to redirect incoming and outgoing WAN traffic to the appliance for acceleration, and the appliance forwards the processed packets back to the router. Almost all of the configuration tasks are performed on the router. The only thing to be configured on the appliance is the forwarding method, and the default method is recommended.

Virtual inline deployment requires no rewiring and no downtime, and it provides a solution for asymmetric routing issues faced in a deployment with two or more WAN links. It contains no built-in status monitoring or health checking, making troubleshooting difficult. Virtual inline is recommended only when inline mode is impractical.

The following figure shows a simple network in which all traffic destined for or received from the remote site is redirected to the appliance. In this example, both the local site and remote site use virtual inline mode.

Figure 1. Virtual Inline Example

Following are some configuration details for the network in this example:

- Endpoint systems have their gateways set to the local router (which is not unique to virtual inline mode).
- Each router is configured to redirect both incoming and outgoing WAN traffic to the local appliance.
- Each appliance processes the traffic received from its local router and forwards it back to the router.
- PBR rules configured on the router prevent routing loops by allowing packets to make only one trip to and from the appliance. The packets that the appliance forwards back to the router are sent to their original (local or remote) destination.
- Each appliance has its default gateway set to the address of the local router, as usual (on the Configuration: Network Adapters page). The options for forwarding packets back to the router are Return to Ethernet Sender and Send to Gateway.
High-Availability Mode

Jun 20, 2017

High Availability (HA) is supported in all deployment modes, and the HA configuration procedure is the same for all modes. The two appliances should be running identical hardware, licensing, and software releases, and must be deployed identically, using the same deployment modes on the same subnets.

To learn more about setting up high availability on SD-WAN appliances, see the High Availability section.
NetScaler SD-WAN 1000 and 2000 Enterprise Edition Appliances

Nov 30, 2016
The SD-WAN Enterprise Edition 1000 and 2000 appliances combine virtualized instances of WAN optimization and Virtual WAN functionality installed on the appliance.

It offers a combination of Virtual WAN and WAN Optimization capabilities.

The SD-WAN 1000 EE and 2000 EE appliances are based on the Citrix branch architecture, which supports multiple virtual machines. All branch appliances contain a SD-WAN instance, a management service instance, and a Xen hypervisor.

The SD-WAN instance is typically used in inline mode, with the SD-WAN instance interposed between the WAN router and the LAN, so WAN traffic flows through the accelerated bridge. The SD-WAN instance can also be deployed in virtual inline mode, using a single accelerated bridge port.

In addition to the accelerated bridges and the Windows LAN port, a management port connects to all virtual machines (instances) and the hypervisor.

The appliance has two modes, two-port mode and four-port mode, which determine how ports 1/3 and 1/4 are used.
The Citrix NetScaler SD-WAN 2000 EE platform is a 1U appliance with one quad-core processor and 24 gigabytes (GB) of memory.

The following figure shows the front panel of the SD-WAN 2000 EE appliance.

Figure 1. Citrix NetScaler SD-WAN 2000 EE appliance, front panel

SD-WAN 2000 EE appliance has the following ports:
- An RS232 serial console port.
- A copper Ethernet (RJ45) Port called the Lights out Management (LOM) port. You can use this port to remotely monitor and manage the appliance independently of the appliance's software.
- A copper Ethernet (RJ45) management port, numbered 0/1, and named PRI (primary). The management port is used to connect directly to the appliance for system administration functions. You can use this port for initial provisioning of WAN optimization and Windows Server.
  Note: The LOM port also operates as a management port.
- Four 10/100/1000Base-T copper Ethernet ports numbered 1/1, 1/2, 1/3, and 1/4 from left to right. The four ports form two accelerated pairs, which function as accelerated bridges. Ports 1/1 and 1/2 are accelerated pair A (apA), and 1/3 and 1/4 are accelerated pair B (apB).

The following figure shows the back panel of the SD-WAN 2000 EE appliance.

Figure 2. Citrix SD-WAN 2000 EE appliance, back panel

The following components are visible on the back panel of the SD-WAN 2000 EE appliance:
- 600 GB removable solid-state drive, which stores the appliance's software and user data, and 1 TB hard disk drive.
- Power switch, which switches power to the appliance on or off. Press the switch for five seconds to switch off the power.
- USB port (reserved for a future release).
- Non-maskable interrupt (NMI) button, for use at the request of Technical Support to produce a core dump. You must use a pen, pencil, or other pointed object to press this red button, which is recessed to prevent unintentional activation.
- Single power supply, rated at 300 watts, 100-240 volts.
The Citrix NetScaler SD-WAN 1000 EE platform has a quad-core processor and 32 GB of memory. This platform has a bandwidth of up to 100 Mbps.

The following figure shows the front panel of a SD-WAN 1000 EE appliance.

Figure 1. Citrix NetScaler SD-WAN 1000 EE, front panel

The front panel of the SD-WAN 1000 EE appliance has a power button and five LEDs.

The power button is used to switch the appliance on or off.

The reset button restarts the appliance.

The LEDs provide critical information related to different parts of the appliance.

- **Power Fail** – Indicates the power supply unit has failed.
- **Information LED** – Indicates the following:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuously ON and red</td>
<td>The appliance is overheated. <em>(This might be a result of cable congestion.)</em></td>
</tr>
<tr>
<td>Blinking red (1Hz)</td>
<td>Fan failure, check for an inoperative fan.</td>
</tr>
<tr>
<td>Blinking red (0.25Hz)</td>
<td>Power failure, check for the non-operational power supply.</td>
</tr>
<tr>
<td>Solid blue</td>
<td>Local UID has been activated. Use this function to locate the server in a rack mount environment.</td>
</tr>
<tr>
<td>Blinking blue (300 m/s)</td>
<td>Remote UID is on. Use this function to identify the server from a remote location.</td>
</tr>
</tbody>
</table>

- **NIC1 and NIC2** – Indicate network activity on the LAN1 and WAN1 ports.
- **HDD** – Indicates the status of the hard disk drive.
• Power – Indicates that the power supply units are receiving power and operating normally.

The following figure shows the back panel of a SD-WAN 1000 EE appliance.

Figure 2. Citrix NetScaler SD-WAN 1000 EE appliance , back panel

The following components are visible on the back panel of a SD-WAN 1000 EE appliance:

• Cooling fan
• Single power supply, rated at 200 watts, 110-240 volts
• Accelerated pairs of Ethernet ports (apA and apB) which function as accelerated bridges
• RS-232 serial console port
• One AUX Ethernet port and one management port
• Two USB ports

To power on the appliance after a graceful shut down:

1. Connect a Serial console cable to the rear of the appliance and to the serial port on a management laptop.

2. On the management laptop, restart a putty session using the following configuration settings:

   • Serial line: COM1
   • Speed: 9600

3. Power on the appliance and as it is booting, press the following key in the Putty session to enter the BIOS configuration screen.

   Keypress: DEL

4. When in the BIOS, navigate to,
5. When in the Boot Feature screen, change the value of the parameter **Restore on AC Power Loss;** from **Last State > Power ON.**

6. Navigate to Save and Exit.

- **Select Save changes** and **Reset.**
- **Select Yes.**

Allow the system to restart. This takes approximately five minutes.
7. After the appliance is powered on, login to the appliance management instance (SVM). The default IP address for the appliance is: 192.168.100.1, user name is: admin/password.

8. In the SD-WAN appliance GUI, navigate to Configuration > Maintenance > Reboot Appliance. Allow the appliance to fully shut down. Ensure that there are no power lights on the appliance when the shut down process has completed.
9. Power on the appliance to confirm that the BIOS configuration change has been applied successfully. This can be either done through the APC intelligent PDU Web Management console or by physically pulling the power cable out of the shut down SD-WAN appliance, waiting for 10 seconds and then plugging it back in again. The appliance power ups automatically from all shut down scenarios.
The following tables summarize the specifications of the SD-WAN 1000 EE and 2000 EE platforms.

<table>
<thead>
<tr>
<th>Platform Performance</th>
<th>SD-WAN 1000 EE</th>
<th>SD-WAN 2000 EE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>Up to 100 Mbps</td>
<td>Up to 250 Mbps</td>
</tr>
<tr>
<td>Maximum HDX sessions</td>
<td>Up to 100</td>
<td>300</td>
</tr>
<tr>
<td>Total sessions</td>
<td>10,000</td>
<td>20,000</td>
</tr>
<tr>
<td>Acceleration Plug-in CCUs</td>
<td>N/A</td>
<td>750</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hardware Specifications</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>4 Cores</td>
<td>4 Cores</td>
</tr>
<tr>
<td>Total disk space</td>
<td>1x300 GB SSD and 1x1 TB HDD</td>
<td>1 x 600 GB SSD and 1X1 TB HDD</td>
</tr>
<tr>
<td>SSD (dedicated Compression history)</td>
<td>123 GB for Disk-Based Compression (DBC) 25 GB for video caching</td>
<td>225 GB for Disk-Based Compression (DBC) 50 GB for video caching</td>
</tr>
<tr>
<td>RAM</td>
<td>32 GB</td>
<td>24 GB</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>2 pair with bypass 10/100/1000 2 GigE ports for Management and AUX ports</td>
<td>4 x 10/100/1000 Base-T copper Ethernet 2 GigE ports for Management and AUX ports</td>
</tr>
<tr>
<td>Power supplies</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical Dimensions</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack Units</td>
<td>1U</td>
<td>1U</td>
</tr>
<tr>
<td>System width</td>
<td>EIA 310-D for 19-inch racks</td>
<td>EIA 310-D for 19-inch racks</td>
</tr>
<tr>
<td>System depth</td>
<td>10&quot; (25.4 cm)</td>
<td>25.4&quot; (64.5 cm)</td>
</tr>
<tr>
<td>System weight</td>
<td>8.5 lbs (3.9 kg)</td>
<td>32 lbs (14.5 kg)</td>
</tr>
<tr>
<td>Shipping dimensions and weight</td>
<td>26 L x 18.5 W x 6.5&quot; H 14.5 lbs</td>
<td>32 L x 23.5 W x 7.5&quot; H 39 lbs</td>
</tr>
<tr>
<td>Environmental and Regulatory</td>
<td>640-1000 EE</td>
<td>SD-WAN 2000 EE</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Voltage</td>
<td>100/240 VAC, 50-60 Hz</td>
<td>100/240 VAC, 50-60 Hz</td>
</tr>
<tr>
<td>Power consumption (Max.)</td>
<td>200 W</td>
<td>300 W</td>
</tr>
<tr>
<td>Operating Temperature (degree Celsius)</td>
<td>10–35</td>
<td>0–40</td>
</tr>
<tr>
<td>Non-operating Temperature (degree Celsius)</td>
<td>-40 – +70</td>
<td>-40 – +70</td>
</tr>
<tr>
<td>Allowed Relative Humidity</td>
<td>8% – 90% non-condensing</td>
<td>5%–95%</td>
</tr>
<tr>
<td>Safety certifications</td>
<td>CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)</td>
<td>CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)</td>
</tr>
<tr>
<td>Electromagnetic and susceptibility certifications</td>
<td>FCC (Part 15 Class A), CCC, KCC, NOM, SASO, CITC, EAC, DoC, CE, VCCI, RCM</td>
<td>FCC (Part 15 Class A), CCC, KCC, NOM, SASO, CITC, EAC, DoC, CE, VCCI, RCM</td>
</tr>
<tr>
<td>Environmental certifications</td>
<td>RoHS, WEEE</td>
<td>RoHS, WEEE</td>
</tr>
</tbody>
</table>
When configuring the appliance, you have to specify IP addresses for various Ethernet ports of the appliance. The Ethernet ports are named differently on the front panel of SD-WAN 1000 EE and 2000 EE appliances in the NetScaler SD-WAN instance, as shown in the following table:

<table>
<thead>
<tr>
<th>Front Panel</th>
<th>SD-WAN Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD-WAN 1000 EE</td>
<td>SD-WAN 2000 EE</td>
</tr>
<tr>
<td>MGMT (Blue)</td>
<td>0/1 (LOM/PRI)</td>
</tr>
<tr>
<td>AUX</td>
<td>0/2 (AUX)</td>
</tr>
<tr>
<td>apA LAN1/WCCP (Green)</td>
<td>1/1</td>
</tr>
<tr>
<td>apA WAN1</td>
<td>1/2</td>
</tr>
<tr>
<td>apB LAN2</td>
<td>1/3</td>
</tr>
<tr>
<td>apB WAN2</td>
<td>1/4</td>
</tr>
</tbody>
</table>

* Available to the SD-WAN instance only in four-port mode.
Installing the Appliance

Jun 12, 2014

After you have determined that the location where you will install your appliance meets the environmental standards and the server rack is in place according to the instructions, you are ready to install the hardware. After you mount the appliance, you are ready to connect it to the network, to a power source, and to the console terminal that you will use for initial configuration. You can also connect the appliance to a computer through Ethernet port for initial configuration. On SD-WAN 1000 EE appliance, this port is labeled as MGMT (management) port and on SD-WAN 2000 EE, the port is labeled as PRI (primary) port. To complete the installation, you switch on the appliance. Be sure to observe the cautions and warnings listed with the installation instructions.
Rack Mounting the Appliance

Apr 09, 2014

A SD-WAN 1000 EE or 2000 EE appliance requires one rack unit. Both are rack-mount devices that can be installed into two-post relay racks or four-post EIA-310 server racks. Verify that the rack is compatible with your appliance.
Rack Mounting a SD-WAN 1000 EE Appliance

Apr 09, 2014
SD-WAN 1000 EE appliance is not shipped with rails. You can mount the appliance to the rack by using the front mounting ports.
Rack Mounting a SD-WAN 2000 EE Appliance

Apr 09, 2014

A SD-WAN 2000 appliance requires one rack unit. Both are rack-mount devices that can be installed into two-post relay racks or four-post EIA-310 server racks. Verify that the rack is compatible with your appliance.

To mount a SD-WAN appliance, you must first install the rails and then install the appliance in the rack, as follows:

- Remove the inner rails from the rail assembly.
- Attach the inner rails to the appliance.
- Install the rack rails on the rack.
- Install the appliance in the rack.

To remove the inner rails from the rail assembly

1. Place the rail assembly on a flat surface.
2. Slide out the inner rail toward the front of the assembly.
3. Depress the locking tabs until the inner rail comes all the way out of the rail assembly.
4. Repeat steps 1 through 3 to remove the second inner rail.

To attach the inner rails to the appliance

1. Position the right inner rail behind the ear bracket on the right side of the appliance.
2. Align the holes on the rail with the corresponding holes on the side of the appliance.
3. Attach the rail to the appliance with the provided screws.
4. Repeat steps 1 through 3 to install the left inner rail on the left side of the appliance.

To install the rack rails

1. Position the rack rails at the desired location in the rack, keeping the sliding rail guide facing inward.
2. Snap the rails to the rack.
   Note: Make sure that both rack rails are at same height and that the rail guides are facing inward.

To install the appliance in the rack

1. Align the inner rails, attached to the appliance, with the rack rails.
2. Slide the appliance into the rack rails, keeping the pressure even on both sides, and push the appliance into the rack rails until it locks into place.
3. Verify that the appliance is locked in place by pulling it all the way out from the rack.
   Note: The illustration in the following figure might not represent your actual appliance.

Figure 1. Rack Mounting the Appliance
Connecting the Cables

Jun 12, 2014

When the appliance is securely mounted on the rack, determine which ports you should use. You are then ready to connect the cables. Ethernet cables and the optional console cable are connected first. Connect the power cable last.

Warning: Before installing or repairing the appliance, remove all jewelry and other metal objects that might come in contact with power sources or wires. When you touch both a live power source or wire and ground, any metal objects can heat up rapidly and cause burns, set clothing on fire, or fuse the metal object to an exposed terminal.

Ports

A typical installation using a single accelerated bridge uses four Ethernet ports (the Primary port and apA) and six IP addresses (four on the Primary port's subnet and two on apA's subnet).

The appliance has two motherboard ports and two accelerated bridges.

- The motherboard ports are labeled as MGMT (management) and AUX1 (auxiliary) ports in SD-WAN 1000 appliance and PRI (primary) and AUX (auxiliary) in SD-WAN 2000 appliance. You use MGMT port of the SD-WAN 1000 appliance and PRI port of the SD-WAN 2000 appliance for initial configuration.

- Accelerated bridge ports are apA and apB are available on the back panel of SD-WAN 1000 appliance and the front panel of SD-WAN 2000 appliance. On SD-WAN 1000 appliance, these ports are labeled as LAN1 and WAN1, and LAN2 and WAN2, respectively. However, on SD-WAN 2000 appliance, these ports are labeled as 1/1 and 1/2, and 1/3 and 1/4, respectively.

Connecting the Ethernet Cables

Ethernet cables connect your appliance to the network. The type of cable you need depends on the type of port used to connect to the network. Use a category 5e or category 6 Ethernet cable with a standard RJ-45 connector on a 10/100/1000BASE-T port.

To connect an Ethernet cable to a 10/100/1000BASE-T port

1. Insert the RJ-45 connector on one end of your Ethernet cable into an appropriate port.
   - On SD-WAN 1000 appliance, the ports are available on the back panel and labeled as LAN1 and WAN1 for apA bridged port for LAN and WAN links, respectively.
   - On SD-WAN 2000 appliance, the ports are available on the front panel. The ports on SD-WAN 2000 are labeled as 1/1 and 1/2 for the apA bridged port. You can use 1/1 for LAN and 1/2 for WAN link.

2. Insert the RJ-45 connector on the other end into the target device, such as a router or switch.

3. Verify that the LED glows amber when the connection is established.

Connecting the Console Cable

You can use the console cable to connect your appliance to a computer or terminal, from which you can configure the appliance. Before connecting the console cable, configure the computer or terminal to support VT100 terminal emulation, 9600 baud, 8 data bits, 1 stop bit, parity, and flow control set to NONE. Then connect one end of the console cable to the RS232 serial port on the appliance and the other end to the computer or terminal.

To connect the console cable to a computer or terminal

1. Insert the DB-9 connector at the end of the cable into the console port.
   - On SD-WAN 1000 appliance, the port is located on the back panel.
   - On SD-WAN 2000 appliance, the port is located on the front panel.
Note: To use a cable with an RJ-45 converter, insert the optional converter provided into the console port and attach the cable to it.

2. Insert the RJ-45 connector at the other end of the cable into the serial port of the computer or terminal.

Connecting the Power Cable

A SD-WAN appliance has one power supply. A separate ground cable is not required, because the three-prong plug provides grounding. Provide power to the appliance by installing the power cord. Connect the other end of the power cable to a standard 110V/220V power outlet.
Switching on the Appliance

Jun 12, 2014

After you have installed the appliance in a rack and connected the cables, verify that the power cable is properly connected. After verifying the connections, you are ready to switch on the appliance.

To switch on the appliance

1. Verify that the appliance is connected through a console or Ethernet port, so that you can configure the appliance after it is switched on.
2. Press the ON/OFF toggle power switch on the appliance.
3. On SD-WAN 2000 appliance, verify that the LCD on the front panel is backlit and the start message appears.

Caution: Be aware of the location of the emergency power off (EPO) switch, so that if an electrical accident occurs, you can quickly remove power from the appliance.
Initial Configuration

Aug 12, 2014

After checking the connections, you are ready to deploy the SD-WAN 1000 and 2000 appliances on the network.

The appliance shipped from Citrix has default IP addresses configured on it. To deploy the appliance on the network, you must configure the appropriate IP addresses on the appliance to accelerate the network traffic.

To perform initial configuration:
- Identify the prerequisites for the initial configuration.
- Record various values required in the initial configuration procedure.
- Configure the appliance by connecting it to the Ethernet port.
- Perform additional configuration for Windows.
- Assign management IP address through the serial console.
- Troubleshoot initial configuration issues.

By default, the initial configuration deploys the appliance in inline mode.
Prerequisites

Aug 12, 2014

Before you begin configuring the appliance, make sure that the following prerequisites have been met:

- You should have physical access to the appliance.
- In the Worksheet, record all IP addresses and other values you would use to configure the appliance. Preferably, print out the worksheet before you start the configuration process.
- You should already have a SD-WAN license key from Citrix, sent in an email. If you are using remote licensing, you need the IP address of the licensing server.
- WAN Send and Receive Speeds.
Configuring the Appliance by Connecting a Computer to the Ethernet Port

Aug 12, 2014
For initial configuration of a SD-WAN appliance, perform the following tasks:

- Configure the appliance for use on your site.
- Install the Citrix license.
- Enable acceleration.
- Enable traffic shaping (inline mode only).

With inline deployments, this configuration might be all you need, because most acceleration features are enabled by default and require no additional configuration.

You can configure the appliance connecting the appliance to your computer through either the Ethernet port or the serial console. The following procedure enables you to configure the appliance by connecting it to your computer through the Ethernet port.

Note: On a SD-WAN 1000 appliance, you use the Ethernet port labeled as MGMT. However, on SD-WAN 2000 appliance, you use the Ethernet port labeled as PRI or LOM.

If you want to configure the appliance by connecting it to the computer through the serial console, assign the management service IP address from your Worksheet by completing the Assigning a Management IP Address through the Serial Console procedure, and then run steps 4 through 25 of the following procedure.

Note: Make sure that you have physical access to the appliance.

To configure the appliance by connecting a computer to the SD-WAN appliance's Ethernet port 0/1

1. Set the Ethernet port address of a computer (or other browser-equipped device with an Ethernet port), to 192.168.100.1, with a network mask of 255.255.0.0. On a Windows device, this is done by changing the Internet Protocol Version 4 properties of the LAN connection, as shown below. You can leave the gateway and DNS server fields as blank.

2. Using an Ethernet cable, connect this computer to the port labeled MGMT on a SD-WAN 1000 appliance, or to the port labeled PRI on a SD-WAN 2000 appliance.

3. Switch on the appliance. Using the web browser on the computer, access the appliance by using the default management service IP address http://192.168.100.1.

4. On the login page, use the following default credentials to log on to the appliance.

5. Start the configuration wizard by clicking Get Started.

6. On the Platform Configuration page, enter the respective values from your worksheet, as shown in the following example:

   Note: If, for SD-WAN configuration, you want to use the same network mask and gateway as those for Network Configuration, select the Use System Netmask and Gateway option.

7. Click Done. A screen showing the Installation in Progress… message appears. This process takes approximately 2 to 5 minutes, depending on your network speed.

Note: If you are configuring the appliance by connecting it to your computer through the serial console port, skip step 8 through step 14.

8. A Redirecting to new management IP message appears.
9. Click OK.
10. Unplug your computer from the Ethernet port and connect the port to your management network.
11. Reset the IP address of your computer to its previous setting.
12. From a computer on the management network, log on to the appliance by entering the new Management Service IP address, such as https://<Management_IP_Address>, in a web browser.
13. To continue the configuration, accept the certificate and continue. The option to continue varies according to the web browser you are using.
14. Log on to the appliance.
15. The Configuration wizard starts again. In this wizard, some of the values which you have already provided, appear by default. Specify rest of the values you have recorded in your worksheet.
16. In System Services section, update the values if necessary.
17. In the Licensing section, select the appropriate license type. You can either select a local license or a remote license server to apply a license to the appliance.
   1. If you opt for a local license, you must generate a license by using the host ID of the appliance. To generate a local license for the appliance, see http://support.citrix.com/article/ctx131110. To apply the license, you can navigate to the SD-WAN > Configuration > Appliance Settings > Licensing page, after completing the Configuration wizard.
   2. If you opt for a remote licensing server, you must select a remote appliance model and provide the IP address of the licensing server in the Licensing Server Address field.
18. In the WAN Link Definition section, specify receive and send speeds for the WAN link in the respective fields. Citrix recommends values 10% lower than the WAN bandwidth, to avoid network congestion.
20. Click Install. After the Installation process is complete, the appliance restarts.
21. As soon as the appliance restarts, the Dashboard page appears.
   -
22. To configure the appliance to accelerate the network traffic, open navigate to the Configuration tab.
   Note: Make sure that you have already applied the appropriate license to the appliance.
23. On the Network Adapters page of the Appliance Settings node, verify and, if necessary, assign IP addresses, subnet masks, and gateways to the accelerated bridges (apA and apB) to be used. Applying these changes restarts the appliance.
   Note: You need to assign IP addresses to apA and apB adapters only if you intended to configure WCCP mode, virtual inline mode, or the Video Caching feature on the appliance.
24. The Initial Configuration is complete. Traffic now flows through the appliance. The Dashboard page shows this traffic.
   -
25. You need additional configuration on the appliance if you intend to use some of the modes and features, such as, virtual inline mode, video caching, secure peering, high availability, encrypted CIFS/MAPI acceleration, AppFlow monitoring, or SNMP monitoring.

Note:
- Inline installations place the appliance between your LAN and WAN routers, using both ports of the accelerated bridge, such as ports LAN1 and WAN1 on a SD-WAN 1000 appliance with Windows Server or ports 1/1 and 1/2 on SD-WAN 2000 appliance with Windows Server, for the apA accelerated bridge port.
- WCCP and virtual inline installations connect a single accelerated bridge port to your WAN router.
- Virtual inline installations require that you configure your router to forward WAN traffic to the appliance. See Router Configuration.
- WCCP installations require configuration of your router and the appliance. See WCCP Mode.
Assigning a Management IP Address through the Serial Console

Aug 12, 2014

If you do not want to change the settings of your computer, you can perform initial configuration by connecting the appliance to your computer with a serial null modem cable. Make sure that you have physical access to the appliance.

To configure the appliance through the serial console

1. Connect a serial null modem cable to the appliance's console port.

2. Connect the other end of the cable to the serial COM port of a computer running a terminal emulator, such as Microsoft HyperTerminal, with settings 9600,N,8,1, p.

3. On the HyperTerminal output, press Enter. The terminal screen displays the Logon prompt.
   Note: You might have to press Enter two or three times, depending on the terminal program you are using.

4. At the logon prompt, log on to the appliance with the following default credentials:
   **Username:** nsroot
   **Password:** nsroot.

5. At the $ prompt, run the following command to switch to the shell prompt of the appliance:
   $ ssh 169.254.0.10

6. Enter Yes to continue connecting to the management service.

7. Log on to the shell prompt of the appliance with the following default credentials:
   **Password:** nsroot.

8. At the logon prompt, run the following command to open the Management Service Initial Network Address Configuration menu:
   # networkconfig

9. Type 1 and press Enter to select option 1, and specify a new management IP address for the management service.

10. Type 2 and press Enter to select option 2, and specify a new management IP address for the XenServer server.

11. Type 3 and press Enter to select option 3, and then specify the network mask for the management service IP address.

12. Type 4 and press Enter to select option 4, and then specify the default gateway for the management service IP address.

13. Type 8 and press Enter to save the settings and exit.

14. Access the SD-WAN appliance by entering the new management service IP address of the appliance, such as https://<Management_Service_IP_Address>, in a web browser of a computer on the management network.

15. To continue the configuration, accept the certificate and continue. The option to continue varies according to the web browser you are using.

16. Run steps 4 through 25 of the Configuring the Appliance by Connecting a Computer to the Ethernet Port procedure to complete the configuration process.
Setting up the SD-WAN Appliance

Nov 23, 2016
To set up your NetScaler SD-WAN Appliance hardware, see the instructions documented in the Setting up the Appliance Hardware section.
Deployment Modes

Jan 28, 2011

A SD-WAN appliance acts as a virtual gateway. It is neither a TCP endpoint nor a router. Like any gateway, its job is to buffer incoming packets and put them onto the outgoing link at the right speed. This packet forwarding can be done in different ways, such as inline mode, virtual inline mode. Although these methods are called modes, you do not have to disable one forwarding mode to enable another. If your deployment supports more than one mode, the mode that the appliance uses is determined automatically by the Ethernet and IP format of each packet.

Because the appliance supports different forwarding modes and different kinds of non-forwarded connections, it needs a way of distinguishing one kind of traffic from another. It does so by examining the destination IP address and destination Ethernet address (MAC address), as shown in table below. For example, in inline mode, the appliance is acting as a bridge. Unlike other traffic, bridged packets are addressed to a system beyond the appliance, not to the appliance itself. The address fields contain neither the appliance's IP address nor the appliance's Ethernet MAC address.

In addition to pure forwarding modes, the appliance has to account for additional types of connections, including management connections to the GUI and the heartbeat signal that passes between members of a high-availability pair. For completeness, these additional traffic modes are also listed in table below.

Table 1. How Ethernet and IP Addresses Determine the Mode

<table>
<thead>
<tr>
<th>Destination IP Address</th>
<th>Destination Ethernet Address</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not appliance</td>
<td>Not appliance</td>
<td>Inline or Pass-through</td>
</tr>
<tr>
<td>Not appliance</td>
<td>Appliance</td>
<td>Virtual Inline or L2 WCCP (WAN OP)</td>
</tr>
<tr>
<td>Appliance</td>
<td>Appliance</td>
<td>Direct (UI access)</td>
</tr>
<tr>
<td>Appliance (VIP)</td>
<td>Appliance</td>
<td>High-Availability. Proxy mode</td>
</tr>
<tr>
<td>Appliance (WCCP GRE Packet)</td>
<td>Appliance</td>
<td>WCCP GRE Mode</td>
</tr>
<tr>
<td>Appliance (Signaling IP)</td>
<td>Appliance</td>
<td>Signaling Connection (SD-WAN plugin Secure Peer) or Redirector Mode Connection (SD-WAN plugin)</td>
</tr>
</tbody>
</table>

All modes can be active simultaneously. The mode used for a given packet is determined by the Ethernet and IP headers.

The forwarding modes are:
- **Inline mode**, in which the appliance transparently accelerates traffic flowing between its two Ethernet ports. In this mode, the appliance appears (to the rest of the network) to be an Ethernet bridge. Inline mode is recommended, because it requires the least configuration.
- **WCCP mode (WAN OP)**, which uses the WCCP v. 2.0 protocol to communicate with the router. This mode is easy to configure on most routers. WCCP has two variants: WCCP-GRE and WCCP-L2. WCCP-GRE encapsulates the WCCP
traffic within generic routing encapsulation (GRE) tunnels. WCCP-L2 uses un-encapsulated network Layer 2 (Ethernet) transport.

- **Virtual inline mode**, in which a router sends WAN traffic to the appliance and the appliance returns it to the router. In this mode, the appliance appears to be a router, but it uses no routing tables. It sends the return traffic to the real router. Virtual inline mode is recommended when inline mode and high-speed WCCP operation are not practical.
- **Group mode**, which allows two appliances to operate together to accelerate a pair of widely separated WAN links.
- **High availability mode**, which allows to appliances to operate as an active/standby high availability pair. If the primary appliance fails, the secondary appliance takes over.

Additional traffic types are listed here for completeness:

- **Pass-through traffic** refers to any traffic that the appliance does not attempt to accelerate. It is a traffic category, not a forwarding mode.
- **Direct access**, where the appliance acts as an ordinary server or client. The GUI and CLI are examples of direct access, using the HTTP, HTTPS, SSH, or SFTP protocols. Direct access traffic can also include the NTP and SNMP protocols.
- **Appliance-to-appliance communication**, which can include signaling connections (used in secure peering and by the SD-WAN plugin), VRRP heartbeats (used in high-availability mode), and encrypted GRE tunnels (used by group mode).
- **Deprecated modes**. Proxy mode and redirector mode are legacy forwarding modes that should not be used in new installations.
Customizing the Ethernet ports

Dec 26, 2012

A typical appliance has four Ethernet ports: two accelerated bridged ports, called *accelerated pair A* (apA.1 and apA.2), with a bypass (fail-to-wire) relay, and two unaccelerated motherboard ports, called Primary and Aux1. The bridged ports provide acceleration, while the motherboard ports are sometimes used for secondary purposes. Most installations use only the bridged ports.

Some SD-WAN units have only the motherboard ports. In this case, the two motherboard ports are bridged.

The appliance’s user interface can be accessed by a VLAN or non-VLAN network. You can assign a VLAN to any of the appliance’s bridged ports or motherboard ports for management purposes.

Figure 1. Ethernet Ports

The ports are named as follows:

<table>
<thead>
<tr>
<th>Table 1. Ethernet Port Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motherboard port 1</td>
</tr>
<tr>
<td>Motherboard port 2</td>
</tr>
<tr>
<td>Bridge #1</td>
</tr>
<tr>
<td>Bridge #2</td>
</tr>
</tbody>
</table>


Port Parameters

May 24, 2013
Each bridge and motherboard port can be:

- Enabled or disabled
- Assigned an IP address and subnet mask
- Assigned a default gateway
- Assigned to a VLAN
- Set to 1000 Mbps, 100 Mbps, or 10 Mbps
- Set to full duplex, half-duplex, or auto (on SD-WAN 4000 WAN OP/SE/ 5000 WAN OP appliances, some ports can be set to 10 Gbps)

All of these parameters except the speed/duplex setting are set on the Configuration: IP Address page. The speed/duplex settings are set on the Configuration: Interface page.

Notes about parameters:

- Disabled ports do not respond to any traffic.
- The browser-based UI can be enabled or disabled independently on all ports.
- To secure the UI on ports with IP addresses, select HTTPS instead of HTTP on the Configuration: Administrator Interface: Web Access page.
- Inline mode works even if a bridge has no IP address. All other modes require that an IP address be assigned to the port.
- Traffic is not routed between interfaces. For example, a connection on bridge apA does not cross over to the Primary or Aux1 ports, but remains on bridge apA. All routing issues are left to your routers.
Accelerated Bridges (apA and apB)

Dec 07, 2012

Every appliance has at least one pair of Ethernet ports that function as an accelerated bridge, called apA (for accelerated pair A). A bridge can act in inline mode, functioning as a transparent bridge, as if it were an Ethernet switch. Packets flow in one port and out the other. Bridges can also act in one arm mode, in which packets flow in one port and back out the same port.

An appliance that has a bypass card maintains network continuity if a bridge or appliance malfunctions.

Some units have more than one accelerated pair, and these additional accelerated pairs are named apB, apC, and so on.

If the appliance loses power or fails in some other way, an internal relay closes and the two bridged ports are electrically connected. This connection maintains network continuity but makes the bridge ports inaccessible. Therefore you might want to use one of the motherboard ports for management access.

Caution: Do not enable the Primary port if it is not connected to your network. Otherwise, you cannot access the appliance, as explained in Ethernet Bypass and Link-Down Propagation.

Bypass cards are standard on some models and optional on others. Citrix recommends that you purchase appliances with bypass cards for all inline deployments.

The bypass feature is wired as if a cross-over cable connected the two ports, which is the correct behavior in properly wired installations.

Important: Bypass installations must be tested - Improper cabling might work in normal operation but not in bypass mode. The Ethernet ports are tolerant of improper cabling and often silently adjust to it. Bypass mode is hard-wired and has no such adaptability. Test inline installations with the appliance turned off to verify that the cabling is correct for bypass mode.

If the appliance is equipped with two accelerated bridges, they can be used to accelerate two different links. These links can either be fully independent or they can be redundant links connecting to the same site. Redundant links can be either load-balanced or used as a main link and a failover link.

Figure 1. Using dual bridges

When it is time for the appliance to send a packet for a given connection, the packet is sent over the same bridge from which the appliance received the most recent input packet for that connection. Thus, the appliance honors whatever link decisions are made by the router, and automatically tracks the prevailing load-balancing or main-link/failover-link algorithm in real time. For non-load-balanced links, the latter algorithm also ensures that packets always use the correct bridge.

Multiple bridges are supported in virtual inline mode.
Two units with multiple bridges can be used in a high-availability pair. Simply match up the bridges so that all links pass through both appliances.
Motherboard Ports

Dec 05, 2012

Although the Ethernet ports on a bypass card are inaccessible when the bypass relay is closed, the motherboard ports remain active. You can sometimes access a failed appliance through the motherboard ports if the bridged ports are inaccessible.

The Primary Port

If the Primary port is enabled and has an IP address assigned to it, the appliance uses that IP address to identify itself to other acceleration units. This address is used internally for a variety of purposes, and is most visible to users as the Partner Unit field on the Monitoring: Optimization: Connections page. If no motherboard port is enabled, the appliance uses the IP address of Accelerated Pair A.

The Primary port is used for:
- Administration through the web based UI
- A back channel for group mode
- A back channel for high-availability mode

The Aux1 Port

The Aux1 port is identical to the Primary port. If the Aux1 port is enabled and the Primary port is not, the appliance takes its identity from the Aux1 port's IP address. If both are enabled, the Primary port's IP address is the unit's identity.
VLAN Support

Dec 05, 2012

A virtual local area network (VLAN) uses part of the Ethernet header to indicate which virtual network a given Ethernet frame belongs to. SD-WAN appliances support VLAN trunking in all forwarding modes (inline, virtual inline, and group mode). Traffic with any combination of VLAN tags is handled and accelerated correctly.

For example, if one traffic stream passing through the accelerated bridge is addressed to 10.0.0.1, VLAN 100, and another is addressed to 10.0.0.1, VLAN 111, the appliance knows that these are two distinct destinations, even though the two VLANs have the same IP address.

You can assign a VLAN to all, some, or none of the appliance's Ethernet ports. If a VLAN is assigned to a port, the management interfaces (GUI and CLI) listen only to traffic on that VLAN. If no VLAN is assigned, the management interfaces listen only to traffic without a VLAN. This selection is made on the Configuration: Appliance Settings: Network Adapters: IP Addresses tab.
Inline Mode

Dec 26, 2012

In inline mode, traffic passes into one of the appliance's Ethernet ports and out of the other. When two sites with inline appliances communicate, every TCP connection passing between them is accelerated. All other traffic is passed through transparently, as if the appliance were not there.

Figure 1. Inline mode, Accelerating All Traffic on a WAN

Note: Any TCP-based traffic passing through both units is accelerated. No address translation, proxying, or per-site setup is required. Inline mode is auto-detecting and auto-configuring.

Configuration is minimized with inline mode, because your WAN router need not be aware of the appliance's existence.

Depending on your configuration, inline mode's link-down propagation can affect management access to the appliance if a link goes down.

Inline mode is most effective when applied to all traffic flowing into and out of a site, but it can be used for only some of the site's traffic.
Ethernet Bypass and Link-Down Propagation

Oct 30, 2013

Note: Link-Down propagation was added to the SD-WAN 2000, 3000, 4000, and 5000 appliances with the 7.2.1 release. Most 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 the other as if the appliance were not there. In fail-to-wire mode, the appliance looks like a cross-over cable connecting the two ports.

Any failure of the appliance hardware or software also closes the relay. When the appliance is restarted, the bypass relay remains closed until the appliance is fully initialized, maintaining network continuity at all times. This feature is automatic and requires no user configuration.

When the bypass relay is closed, the appliance's bridge ports are inaccessible.

If carrier is lost on one of the bridge ports, the carrier is dropped on the other bridge port to ensure that the link-down condition is propagated to the device on the other side of the appliance. Units that monitor link state (such as routers) are thus notified of conditions on the other side of the bridge.

Link-down propagation has two operating modes:
- If the Primary port is not enabled, the link-down state on one bridge port is mirrored briefly on the other bridge port, and then the port is re-enabled. This allows the appliance to be reached through the still-connected port for management, HA heartbeat, and other tasks.
- If the Primary port is enabled, the appliance assumes (without checking) that the Primary port is used for management, HA heartbeat, and other tasks. The link-down condition on one bridge port is mirrored persistently on the other port, until carrier is restored or the unit is rebooted. This is true even if the Primary port is enabled in the GUI but not connected to a network, so the Primary port should be disabled (the default) when not in use.
Accelerating an Entire Site

Inline mode, Accelerating All Traffic on a WAN shows a typical configuration for inline mode. For both sites, the appliances are placed between the LAN and the WAN, so all WAN traffic that can be accelerated is accelerated. This is the simplest method for implementing acceleration, and it should be used when practical.

Because all the link traffic is flowing through the appliances, the benefits of fair queuing and flow control prevent the link from being overrun.

In IP networks, the bottleneck gateway determines the queuing behavior for the entire link. By becoming the bottleneck gateway, the appliance gains control of the link and can manage it intelligently. This is done by setting the bandwidth limit slightly lower than the link speed. When this is done, link performance is ideal, with minimal latency and loss even at full link utilization.
Partial-Site Acceleration

Dec 27, 2012
To reserve the appliance’s accelerated bandwidth for a particular group of systems, such as remote backup servers, you can install the appliance on a branch network that includes only those systems. This is shown in the following figure.

Figure 1: Inline Mode, Accelerating Selected Systems Only

SD-WAN traffic shaping relies on controlling the entire link, so traffic shaping is not effective with this topology, because the appliance sees only a portion of link traffic. Latency control is up to the bottleneck gateway, and interactive responsiveness can suffer.
Configuring and Troubleshooting Inline Mode

Dec 26, 2012
Inline mode requires only basic configuration, because it is applied automatically to any packets passing through the accelerated bridge. Troubleshooting is described under.
Virtual Inline Mode

Dec 28, 2012

Note: Use virtual inline mode only when both inline mode and WCCP mode are impractical. Do not mix inline and virtual inline modes within the same appliance. However, you can mix virtual inline and WCCP modes within the same appliance. Citrix does not recommend virtual inline mode with routers that do not support health monitoring.

In virtual inline mode, the router uses policy based routing (PBR) rules to redirect incoming and outgoing WAN traffic to the appliance for acceleration, and the appliance forwards the processed packets back to the router. Almost all of the configuration tasks are performed on the router. The only thing to be configured on the appliance is the forwarding method, and the default method is recommended.

Like WCCP, Virtual inline deployment requires no rewiring and no downtime, and it provides a solution for asymmetric routing issues faced in a deployment with two or more WAN links. Unlike WCCP, it contains no built-in status monitoring or health checking, making troubleshooting difficult. WCCP is thus the recommended mode, and virtual inline is recommended only when inline and WCCP modes are both impractical.

The following figure shows a simple network in which all traffic destined for or received from the remote site is redirected to the appliance. In this example, both the local site and remote site use virtual inline mode.

Figure 1. Virtual Inline Example

Following are some configuration details for the network in this example:

- Endpoint systems have their gateways set to the local router (which is not unique to virtual inline mode).
- Each router is configured to redirect both incoming and outgoing WAN traffic to the local appliance.
- Each appliance processes the traffic received from its local router and forwards it back to the router.
- PBR rules configured on the router prevent routing loops by allowing packets to make only one trip to and from the appliance. The packets that the appliance forwards back to the router are sent to their original (local or remote) destination.
- Each appliance has its default gateway set to the address of the local router, as usual (on the Configuration: Network Adapters page). The options for forwarding packets back to the router are Return to Ethernet Sender and Send to Gateway.
Configuring Packet Forwarding on the Appliance

May 12, 2015
Virtual inline mode offers two packet-forwarding options:

**Return to Ethernet Sender (default)**—This mode allows multiple routers to share an appliance. The appliance forwards virtual inline output packets back to where they came from, as indicated by the Ethernet address of the incoming packet. If two routers share a single appliance, each gets its own traffic back, but not the traffic from the other router. This mode also works with a single router.

**Send to Gateway (not recommended)**—In this mode, virtual inline output packets are forwarded to the default gateway for delivery, even if they are destined for hosts on the local subnet. This option is usually less desirable than the Return to Ethernet Sender option, because it adds an easily forgotten element of complexity to the routing structure.

**To specify the packet-forwarding option**—On the Configuration: Optimization Rules: Tuning page, next to Virtual Inline, select Return to Ethernet Sender or Send to Gateway.
Router Configuration

The router has three tasks when supporting virtual inline mode:
1. It must forward both incoming and outgoing WAN traffic to the SD-WAN appliance.
2. It must forward SD-WAN traffic to its destination (WAN or LAN).
3. It must monitor the health of the SD-WAN appliance so that the appliance can be bypassed if it fails.

In virtual inline mode, the packet forwarding methods can create routing loops if the routing rules do not distinguish between a packet that has been forwarded by the appliance and one that has not. You can use any method that makes that distinction.

A typical method involves dedicating one of the router's Ethernet ports to the appliance and creating routing rules that are based on the Ethernet port on which packets arrive. Packets that arrive on the interface dedicated to the appliance are never forwarded back to the appliance, but packets arriving on any other interface can be.

The basic routing algorithm is:
- Do not forward packets from the appliance back to the appliance.
- If the packet arrives from the WAN, forward it to the appliance.
- If packet is destined for the WAN, forward to the appliance.
- Do not forward LAN-to-LAN traffic to the appliance.
- Traffic shaping is not effective unless all WAN traffic passes through the appliance.

Note: When considering routing options, keep in mind that returning data, not just outgoing data, must flow through the appliance. For example, placing the appliance on the local subnet and designating it as the default router for local systems does not work in a virtual inline deployment. Outgoing data would flow through the appliance, but incoming data would bypass it. To force data through the appliance without router reconfiguration, use inline mode.

If the appliance fails, data should not be routed to it. By default, Cisco policy based routing does no health monitoring. To enable health monitoring, define a rule to monitor the appliance's availability, and specify the "verify-availability" option for the "set ip next-hop" command. With this configuration, if the appliance is not available, the route is not applied, and the appliance is bypassed.

Important: Citrix recommends virtual inline mode only when used with health monitoring. Many routers that support policy-based routing do not support health-checking. The health-monitoring feature is relatively new; it became available in Cisco IOS release 12.3(4)T.

Following is an example of a rule for monitoring the availability of the appliance:
```
! Use a ping (ICMP echo) to see if appliance is connected track   123 rtr 1 reachability  rtr 1 type echo protocol IpIcmpecho 192.168.1.200 schedule 1 life forever start-time now
```
This rule pings the appliance at 192.168.1.200 periodically. You can test against 123 to see if the unit is up.
Routing Examples

Feb 06, 2014

The following examples illustrate configuring Cisco routers for the local and remote sites shown in Virtual inline example. To illustrate health monitoring, the configuration for the local site includes health monitoring, but the configuration for the remote site does not.

Note: The configuration for the local site assumes that a ping monitor has already been configured. The examples conform to the Cisco IOS CLI. They might not be applicable to routers from other vendors.

Local Site, Health-Checking Enabled

! For health-checking to work, do not forget to start
! the monitoring process.
!
! Original configuration is in normal type.
! appliance-specific configuration is in bold.
!
ip cef

interface FastEthernet0/0
ip address 10.10.10.5 255.255.255.0
ip policy route-map client_side_map

interface FastEthernet0/1
ip address 172.68.1.5 255.255.255.0
ip policy route-map wan_side_map

interface FastEthernet1/0
ip address 192.168.1.5 255.255.255.0

ip classless
ip route 0.0.0.0 0.0.0.0 171.68.1.1

ip access-list extended client_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255

route-map wan_side_map permit 20
match ip address wan_side
set ip next-hop verify-availability 192.168.1.200 20 track 123

route-map client_side_map permit 10
match ip address client_side
set ip next-hop verify-availability 192.168.1.200 10 track 123
Remote Site (No Health Checking)

! This example does not use health-checking.
! Remember, health-checking is always recommended,
! so this is a configuration of last resort.

! ip cef
!
interface FastEthernet0/0
ip address 20.20.20.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 171.68.2.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.2.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.2.1
!
ip access-list extended client_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
set ip next-hop 192.168.2.200
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop 192.168.2.200

Each of the above examples applies an access list to a route map and attaches the route map to an interface. The access lists identify all traffic originating at one accelerated site and terminating at the other (A source IP of 10.10.10.0/24 and destination of 20.20.20.0/24 or vice versa). See your router's documentation for the details of access lists and route-maps.

This configuration redirects all matching IP traffic to the appliances. If you want to redirect only TCP traffic, you can change the access-list configuration as follows (only the remote side's configuration is shown here):

! ip access-list extended client_side
permit tcp 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit tcp 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!

Note that, for access lists, ordinary masks are not used. Wildcard masks are used instead. Note that when reading a
wildcard mask in binary, "1" is considered a "don't care" bit.
Virtual Inline for Multiple-WAN Environments

Dec 27, 2012
Enterprises with multiple WAN links often have asymmetric routing policies, which seem to require that an inline appliance be in two places at once. Virtual inline mode solves the asymmetric routing problem by using the router configuration to send all WAN traffic through the appliance, regardless of the WAN link used. The below figure shows a simple multiple-WAN link deployment example.

The two local-side routers redirect traffic to the local appliance. The FE 0/0 ports for both routers are in the same broadcast domain as the appliance. The local appliance must use the default virtual inline configuration (Return to Ethernet Sender).

Figure 1. Virtual Inline Mode With Two WAN Routers
Virtual Inline Mode and High-Availability

Dec 27, 2012

Virtual Inline mode can be used in a high availability (HA) configuration. The below figure shows a simple HA deployment. In virtual inline mode, a pair of appliances acts as one virtual appliance. Router configuration is the same for an HA pair as with a single appliance, except that the Virtual IP address of the HA pair, not the IP address of an individual appliance, is used in the router configuration tables. In this example, the local appliances must use default virtual inline configuration (Return to Ethernet Sender).

Figure 1. High-availability Example
Monitoring and Troubleshooting

Dec 17, 2012

In virtual inline mode, unlike WCCP mode, the appliance provides no virtual inline-specific monitoring. To troubleshoot a virtual inline deployment, log into the appliance and use the Dashboard page to verify that traffic is flowing into and out of the appliance. Traffic forwarding failures are typically caused by errors in router configuration.

If the Monitoring: Usage or Monitoring: Connections pages show that traffic is being forwarded but no acceleration is taking place (assuming that an appliance is already installed on the other end of the WAN link), check to make sure that both incoming WAN traffic and outgoing WAN traffic are being forwarded to the appliance. If only one direction is forwarded, acceleration cannot take place.

To test health-checking, power down the appliance. The router should stop forwarding traffic after the health-checking algorithm times out.
High-Availability Mode

Dec 11, 2013

Two identical appliances on the same subnet can be combined as a high-availability pair. The appliances each monitor the other's status by using the standard Virtual Router Redundancy Protocol (VRRP) heartbeat mechanism. The pair has a common virtual IP address for management, in addition to each appliance's management IP address. If the primary appliance fails, the secondary appliance takes over. Failover takes approximately five seconds.

High availability mode is a standard feature.
How High-Availability Mode Works

Dec 06, 2012

In a high availability (HA) pair, one appliance is primary, and the other is secondary. The primary monitors its own and the secondary's status. If it detects a problem, traffic processing fails over to the secondary appliance. Existing TCP connections are terminated. To ensure successful failover, the two appliances keep their configurations synchronized. In a WCCP mode high availability configuration, the appliance that is processing traffic maintains communication with the upstream router.

Status monitoring—When high availability is enabled, the primary appliance uses the VRRP protocol to send a heartbeat signal to the secondary appliance once per second. In addition, the primary appliance monitors the carrier status of its Ethernet ports. The loss of carrier on a previously active port implies a loss of connectivity.

Failover If the heartbeat signal of the primary appliance should fail, or if the primary appliance loses carrier for five seconds on any previously active Ethernet port, the secondary appliance takes over, becoming the primary. When the failed appliance restarts, it becomes the secondary. The new primary announces itself on the network with an ARP broadcast. MAC spoofing is not used. Ethernet bridging is disabled on the secondary appliance, leaving the primary appliance as the only path for inline traffic. Fail-to-wire is inhibited on both appliances to prevent loops.

Caution: The Ethernet bypass function is disabled in HA mode. If both appliances in an inline HA pair lose power, connectivity is lost. If WAN connectivity is needed during power outages, at least one appliance must be attached to a backup power source.

Note: The secondary appliance in the HA pair has one of its bridge ports, port apA.1, disabled to prevent forwarding loops. If the appliance has dual bridges, apB.1 is also disabled. In a one-arm installation, use port apA.2. Otherwise, the secondary appliance becomes inaccessible when HA is enabled.

Primary/secondary assignment—If both appliances are restarted, the first one to fully initialize itself becomes the primary. That is, the appliances have no assigned roles, and the first one to become available takes over as the primary. The appliance with the highest IP address on the interface used for the VRRP heartbeat is used as a tie-breaker if both become available at the same time.

Connection termination during failover—Both accelerated and unaccelerated TCP connections are terminated as a side effect of failover. Non-TCP sessions are not affected, except for the delay caused by the brief period (several seconds) between the failure of the primary appliance and the failover to the secondary appliance. Users experience the closing of open connections, but they can open new connections.

Configuration synchronization—The two appliances synchronize their settings to ensure that the secondary is ready to take over for the primary. If the configuration of the pair is changed through the browser based interface, the primary appliance updates the secondary appliance immediately.

HA cannot be enabled unless both appliances are running the same software release.

HA in WCCP mode—When WCCP is used with an HA pair, the primary appliance establishes communication with the router. The appliance uses its management IP address on apA or apB, not its virtual IP address, to communicate with the router. Upon failover, the new primary appliance establishes WCCP communication with the router.
Cabling Requirements

May 24, 2013
The two appliances in the high availability pair are installed onto the same subnet in either a parallel arrangement or a one-arm arrangement, both of which are shown in the following figure. In a one-arm arrangement, use the apA.2 port (and, optionally, the apB.2 port), not the apA.1 port. Some models require a separate management LAN, whether deployed in inline or one-armed mode. This is depicted only in the middle diagram.

Figure 1. Cabling for High-Availability Pairs

Do not break the above topology with additional switches. Random switch arrangements are not supported. Each of the switches must be either a single, monolithic switch, a single logical switch, or part of the same chassis.

If the spanning-tree protocol (STP) is enabled on the router or switch ports attached to the appliances, failover will work, but the failover time may increase to roughly thirty seconds. Without STP, failover time is roughly five seconds. Thus, to achieve the briefest possible failover interval, disable STP on the ports connecting to the appliances.

Figure 2. Ethernet Port Locations (Older Models)
Other Requirements

Dec 06, 2012

Both appliances in an HA pair must meet the following criteria:

- Have identical hardware, as shown by on the System Hardware entry on the Dashboard page.
- Run exactly the same software release.
- Be equipped with Ethernet bypass cards. To determine what is installed in your appliances, see the Dashboard page.

Appliances that do not support HA display a warning on the Configuration: High Availability page.
Management Access to the High-Availability Pair

Jan 03, 2013
When configuring a high-availability (HA) pair, you assign the pair a virtual IP (VIP) address, which enables you to manage the two appliances as if they were a single unit. After you enable high-availability mode, managing the secondary appliance through its IP address is mostly disabled, with most parameters grayed out. A warning message displays the reason on every page. Use the HA VIP for all management tasks. You can, however, disable the secondary appliance’s HA state from its management UI.
Configuring the High-Availability Pair

Dec 27, 2012
You can configure two newly installed appliances as a high-availability pair, or you can create an HA pair by adding a second appliance to an existing installation.

Prerequisites: Physical installation and basic configuration procedures

To configure high availability
1. Make sure that no more than one appliance is connected to the traffic networks (on the accelerated bridges). If both are connected, disconnect one bridge cable from the active bridges on the second appliance. This will prevent forwarding loops.
2. On the Features page of the first appliance, disable Traffic Processing. This disables acceleration until the HA pair is configured.
3. Repeat for the second appliance.
4. On the first appliance, go to the Configuration: Advanced Deployments: High Availability tab, show below.
5. Select the Enabled Check box.
6. Click the Configure HA Virtual IP Address link and assign a virtual IP address to the apA interface. This address will be used later to control both appliances as a unit.
7. Return to the High Availability page and, in the VRRP VRID field, assign a VRRP ID to the pair. Although the value defaults to zero, the valid range of VRRP ID numbers is 1 through 255. Within this range, you can specify any value that does not belong to another VRRP device on your network.
8. In the Partner SSL Common Name field, type the other appliance's SSL Common Name, which is displayed on that appliance's Configuration: Advanced Deployments: High Availability tab, in the Partner SSL Common Name field. The SSL credentials used here are factory-installed.
9. Click Update.
10. Repeat steps 3-8 on the second appliance. If you are managing the appliance via an accelerated bridge (such as apA), you may have to reconnect the Ethernet cable that you removed in step 1 to connect to the second appliance. If so, plug this cable in and disconnect the corresponding cable on the first appliance.
11. With your browser, navigate to the virtual IP address of the HA pair. Enable Traffic Processing on the Features page. Any further configuration will be performed from this virtual address.
12. Plug in the cable that was left disconnected.
13. On each appliance, the Configuration: Advanced Deployments: High Availability page should now show that high availability is active and that one appliance is the primary and the other is the secondary. If this is not the case, a warning banner appears at the top of the screen, indicating the nature of the problem.

Figure 1. High-availability configuration page
Updating Software on a High-Availability Pair

Dec 06, 2012

Updating the SD-WAN software on an HA pair causes a failover at one point during the update.

Note: Clicking the Update button terminates all open TCP connections.

To update the software on an HA pair

1. Log on to both appliances.
2. On the secondary appliance, update the software and reboot. After the reboot, the appliance is still the secondary. Verify that the installation succeeded. The primary appliance should show that the secondary appliance exists but that automatic parameter synchronization is not working, due to a version mismatch.
3. On the primary appliance, update the software, and then reboot. The reboot causes a failover, and the secondary appliance becomes the primary. When the reboot is completed, HA should become fully established, because both appliances are running the same software.
Saving/Restoring Parameters of an HA Pair

Dec 06, 2012
The System Maintenance: Backup/Restore function can be used to save and restore parameters of an HA pair as follows:

To back up the parameters

Use the backup feature as usual. That is, log on to the GUI through the HA VIP address (as is normal when managing the HA pair) and, on the System Management: Backup/Restore page, click Download Settings.

To restore the parameters

1. Disable HA on both appliances by clearing the Enabled check box on the Configuration: Advanced Deployments: High Availability (HA) tab.
2. Unplug a network cable from the bridge of one appliance. (Call it “Appliance A.”)
3. Unplug the power cord from Appliance A.
4. Restore the parameters on the other appliance (Appliance B), by uploading a previously saved set of parameters on the System Maintenance: Backup/Restore page and clicking Restore Settings. (Completing this operation requires a restart, which reenables HA).
5. Wait for Appliance B to restart. It becomes the primary.
6. Restart Appliance A.
7. Log on to Appliance A’s GUI and reenable HA on the Configuration: Advanced Deployments: High Availability (HA) tab. The appliance get its parameters from the primary.

Both appliances are now restored and synchronized.
Troubleshooting High Availability Pairs

Dec 26, 2012
If the appliances report any failure to enter high-availability mode, the error message will also note the cause. Some issues that can interfere with high-availability mode are:

- The other appliance is not running.
- The HA parameters on the two appliances are not identical.
- The two appliances are not running the same software release.
- The two appliances do not have the same model number.
- Incorrect or incomplete cabling between the appliances does not allow the HA heartbeat to pass between them.
- The HA/Group Mode SSL Certificates on one or both appliances are damaged or missing.
NetScaler SD-WAN VPX

Nov 30, 2016

Citrix NetScaler SD-WAN Standard Edition or WANOP VPX is a virtual Citrix NetScaler SD-WAN appliance that can be hosted on Citrix XenServer, VMware ESX or ESXi, Microsoft Hyper-V, and Amazon AWS virtualization platforms. A SD-WAN VPX appliance supports most of the features of a physical Standard Edition or WANOP appliances.

Because SD-WAN SE/WAN OP Edition VPX is a virtual machine, you can deploy on your choice of hardware, exactly where you need it, and in combination it with other virtual machines -- servers, VPN units, or other appliances -- to create a unit that precisely suits your needs.

SD-WAN WANOP VPX software is available as:
- A Xen virtual machine running under XenServer 5.5 and later.
- A VMware vSphere virtual machine running under ESX/ESXi 4.1-6.0.
- A Hyper-V virtual machine under 64-bit Windows 2008 R2 SP1 - 2012.
- An Amazon EC2 instance.

Note: XenServer and VMware vSphere support VLAN trunking, but Hyper-V does not.

SD-WAN Standard Edition VPX software is available as:
- A Xen virtual machine running under XenServer 6.5 SP1.
- A VMware vSphere virtual machine running under ESX/ESXi 5.5 and 6.0.

When a newly installed SD-WAN SE/WANOP VPX virtual machine is up and running, you configure as you would configure a physical SD-WAN SE/WANOP appliance, using the same configuration screens.

A SD-WAN WANOP VPX virtual appliance is similar to a SD-WAN Repeater 8500 series appliance, including support for the SD-WAN Plug-in and links of up to 45 mbps. Following are the key differences:
- Except for Amazon EC2 instances, licensing via remote license servers is mandatory for retail licenses. Local licensing is available for non-retail licenses, such as evaluation and VPX Express licenses. For Amazon EC2 instances, you can use either Citrix licensing or select a product with built-in licensing for the bandwidth limit you desire (2, 10, 20, or 45 Mbps).
- SD-WAN VPX obtains its SD-WAN Plug-in licenses from the remote license server (except for SD-WAN VPX for Amazon AWS, which does not support Plug-ins). Plug-ins connecting to multiple virtual appliances consume only a single Plug-in license, not one license per appliance, provided that all virtual appliances use the same license server.
- The SD-WAN LCD front-panel display is not supported.
- The RS-232 serial command interface is not supported.
- Multiple accelerated bridges are not supported.
- Ethernet bypass cards are not supported.
- Group mode is not supported.
- SD-WAN High-availability mode is not supported. (XenServer HA and vSphere HA are supported)
- Three ports are supported (apA.1, apA.2, and Primary), except for Amazon AWS instances, which support only a single port.
SD-WAN VPX Usage Scenarios

Oct 24, 2017

You can deploy VPX to accelerate the traffic to or from a branch office, to and from a particular server, or in the cloud. In the data center, you can create a flexible and powerful configuration by assigning a separate VPX instance to each server. Or, at any location, you can assign multiple VPX instances to one server, for different types or levels of acceleration services within the same server.

For employees connecting through VPNs, VPX can accelerate their connections.

As with a physical appliance, inline mode is the most common type of configuration, but WCCP and virtual inline modes can provide an effective deployment.

You can deploy VPX to accelerate the traffic to or from a branch office, or to and from a particular server. In the data center, you can create a flexible and powerful configuration by assigning a separate VPX instance to each server. Or, at any location, you can assign multiple VPX instances to one server, for different types or levels of acceleration services within the same server.

For employees connecting through VPNs, VPX can accelerate their connections.

As with a physical appliance, inline mode is the most common type of configuration, but WCCP mode can provide an effective failover mechanism.

Branch-office accelerator

A VPX image can be installed on the server of your choice and deployed just like a SD-WAN/SD-WAN appliance. VPX has all the functionality of a SD-WAN/SD-WAN appliance, and in addition has advantages provided by virtualization. Group mode and high-availability modes are not supported.

Figure 1. VPX use case #1: Branch-office accelerator

Accelerated branch-office server

If you add a virtual server to the simple branch-office accelerator configuration, you have an accelerated branch-office server, as shown in the figure below. If you assign the virtual networks within the appliance hosting the virtual machines so that the path to the WAN passes through the virtual SD-WAN/SD-WAN, all WAN traffic is accelerated automatically. For example, all web traffic, backups, remote applications, database queries, and operations that require network-file-system access are accelerated.
The virtual environment allows you to add the desired functionality to the server unit, including the operating system and features of your choice. This configuration accelerates all the WAN traffic from every system in the branch office. You can even deploy multiple virtual servers on the same machine, consolidating your branch-office rack down to a single unit running multiple virtual machines.

Figure 2. VPX use case #2: Accelerated branch-office server

Accelerated datacenter servers

Installing VPX VMs on every server in the data center creates a solution that scales perfectly as you add server capacity, while minimizing the number of servers by adding acceleration to the servers themselves. Once you have more than a few accelerated servers, the aggregate acceleration provided by multiple VPX VMs exceeds anything that can be provided with a single appliance.

VPX accelerates all types of network applications, including XenApp, XenDesktop, Citrix Merchandising Server, network file systems, databases, web servers, and more.

Figure 3. VPX use case #3: Accelerated Datacenter Servers

VPN accelerator

By installing the VPN of your choice with VPX, you have an accelerated VPN.
Note: Unlike other configurations, the VPN virtual machine is on the WAN side and the VPX virtual appliance is on the LAN side, because the VPN traffic must be decrypted for compression and application acceleration.

Figure 4. VPX use case #4: VPN accelerator

Multiple VPX Instances on the Same Server

By putting multiple VPX VMs on the same server, you can create different types or levels of acceleration services within the same unit. One VPX instance might be dedicated to a critical application, or each instance dedicated to an individual remote site or customer. Use VLAN switches to direct traffic to the appropriate VPX instance.

Figure 5. VPX use case #5: Multiple Instances for Dedicated Acceleration Resources

WCCP and virtual inline deployment

WCCP and virtual inline modes are suitable for one-arm deployments, which use only one port. The Amazon AWS version of VPX uses only a single port, and is thus always deployed in a one-armed mode.

Figure 6. VPX use case #6: WCCP or virtual inline deployment

In cases where an Ethernet bypass card would be desirable, using WCCP instead of inline mode provides effective fault-tolerance, because WCCP has built-in health-checking. Instead of forwarding traffic through an unresponsive WCCP device, the routers send the traffic directly to the end point.
Branch-office accelerator SD-WAN/SD-WAN VPX can be installed on the server of your choice and deployed just like any other SD-WAN/SD-WAN appliance. VPX has the same functionality as the SD-WAN/SD-WAN appliance along with the additional features provided by virtualization. The group mode and high-availability mode are not supported.

VPX supports Citrix Command Center release 4.0 or later. SD-WAN also supports SD-WAN/SD-WAN VPX Express licenses, which support a maximum accelerated sending rate of 512 kbps, 10 accelerated connections, and 5 SD-WAN/SD-WAN Plug-ins.

- VPX for XenServer special features include:
  - XenServer Essentials Support
  - XenMotion Live Migration
  - XenServer High Availability
  - Workload Balancing
  - Performance Monitoring and Alerts

- VPX for VMware vSphere special features include:
  - VMware vCenter Server (remote management).
  - VMware vSphere HA (high availability).
  - VMware vSphere vMotion (migrate SD-WAN VPX to a different server with identical processors).
  - VMware Guest Customization (replicate VPX with different per-instance parameters).
System Requirements and Provisioning

Jan 23, 2017

SD-WAN VPX runs on XenServer 5.5 or later, VMware vSphere ESX/ESXi 4.1 or later, Hyper-V under 64-bit Windows Server 2008 R2 SP1, and Amazon AWS. SD-WAN VPX supports four configurations, from 2 to 8 GB of RAM and 100 to 500 GB of disk space. The intermediate, 4 GB RAM/250 GB disk configuration is similar to the Repeater 8500 series appliance.

Supported Configurations

The following tables list all supported SD-WAN VM configurations. (Amazon AWS configurations are preselected and are somewhat different.)

<table>
<thead>
<tr>
<th>Type</th>
<th>vCPUs</th>
<th>RAM</th>
<th>Disk</th>
<th>Maximum WAN Speed</th>
<th>Maximum Accelerated Connections</th>
<th>Maximum SD-WAN/SD-WAN Plug-ins</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 GB production config.</td>
<td>2</td>
<td>2 GB</td>
<td>100 GB</td>
<td>2 mbps</td>
<td>1,000</td>
<td>50</td>
</tr>
<tr>
<td>4 GB production config.</td>
<td>2</td>
<td>4 GB</td>
<td>250 GB</td>
<td>10 mbps</td>
<td>10,000</td>
<td>250</td>
</tr>
<tr>
<td>4 GB production config.*</td>
<td>2</td>
<td>4 GB</td>
<td>250 GB</td>
<td>45 mbps</td>
<td>15,000</td>
<td>400</td>
</tr>
<tr>
<td>8 GB production config.</td>
<td>4</td>
<td>8 GB</td>
<td>500 GB</td>
<td>45 mbps</td>
<td>25,000</td>
<td>500</td>
</tr>
</tbody>
</table>

* With 45mbps license

Other configurations (not for production networks)

<table>
<thead>
<tr>
<th>Type</th>
<th>vCPUs</th>
<th>RAM</th>
<th>Disk</th>
<th>Maximum WAN Speed</th>
<th>Maximum Accelerated Connections</th>
<th>Maximum SD-WAN/SD-WAN Plug-ins</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPX Express</td>
<td>2</td>
<td>1 GB</td>
<td>60 GB</td>
<td>512 kbps</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>Min. evaluation</td>
<td>2</td>
<td>1 GB</td>
<td>60 GB</td>
<td>2 mbps</td>
<td>1,000</td>
<td>5</td>
</tr>
<tr>
<td>config.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Minimum Resource Requirements

A SD-WAN VPX virtual machine has the following minimum hardware requirements for a production environment:

- 2 GB RAM
- 100 GB disk (local disks provide the best performance)
- 2 virtual NICs (Ethernet ports), except for Amazon AWS, which requires only one virtual NIC
- 2 virtual CPUs
- A modern CPU (Intel Nehalem or newer or AMD Family 10h or newer, both of which were introduced in 2008). Older CPUs may run at reduced performance due to the use of emulated x86 TSC (timestamp counter) functionality. If clock states
higher than C1 are not used and SpeedStep/PowerNow modes are disabled in the BIOS of older processors, TSC emulation will not be used and the system will run at normal speed.

The server hosting VPX must have RAM, CPU, and disk resources greater than those required by the VPX VM. (VPX does not support VMware hardware over-commit.) Obviously, the server must have enough resources to run the hypervisor as well as the virtual appliance. However, having as many physical Ethernet ports as virtual ones is not mandatory if one of a VPX VM’s Ethernet ports is connected to another virtual machine on the same server. Possible Ethernet options include:

- Mapping the VPX VM’s two virtual ports to two physical ports, rendering its operation equivalent to that of a stand-alone SD-WAN.
- Mapping one of VPX VM’s virtual ports to a physical port, and the other to a virtual network containing one or more virtual machines on the same server, thus creating an accelerated server.
- Mapping each of VPX VM’s virtual ports to a virtual network, thus chaining the VPX VM between two sets of VMs on the same server.

The following figure shows a VPX VM in a one-arm deployment for traffic that terminates on another virtual machine on the same server. Only one physical port is required in this case, but both virtual ports are used.

Figure 1. Ethernet (Network) Port Assignments, One-Arm Operation

Maximum Usable Resources

Following are the maximum amount of resources that a single VPX virtual machine can use effectively:

- 4 virtual CPUs
- 8 GB RAM
- 500 GB disk
- 4 virtual NICs

Server resources not allocated to VPX VMs are available to other VMs on the same server, but be careful to avoid overcommitting resources.

Disk and RAM

As the amounts of RAM and disk space are increased, the additional resources are allocated primarily to the compression subsystem. Increased memory also allows more connections and acceleration partners to be supported.

The SD-WAN compression system makes heavy demands on the disk subsystem. In general, local disk storage outperforms network disk storage and reduces resource contention on both the LAN and the network disk.

The relationship between disk or memory resources and link speed is indirect. Memory and disk sizes have no effect on the speed at which packets are sent over the link (bps). Providing more memory and disk space improves compression...
performance by increasing the amount of compression history that can be used for pattern matching.

**Virtual NICs**

Except for Amazon AWS, two virtual network interfaces are required. They are bridged and used for both acceleration and the browser based user interface. These interfaces must be attached to different virtual networks. Note that, for one-arm operation, the second interface can be a stub, attached only to a VPX VM.

A third virtual network interface provides an independent interface to the VPX VM, which is the equivalent to the Primary port on a physical appliance. It can be used for the browser based interface, but not for acceleration.

**Other Virtual Machines**

- Server resources beyond those allocated to VPX are available for other virtual machines on the same server.
- Resource usage by other VMs affects VPX performance, and vice versa. Acceleration makes intensive use of CPU, memory, disk, and network.

Virtual network routing can be used to connect other VMs on the server to VPX VMs, but the simplest method of connecting such VMs is to attach them to the server's LAN-side Ethernet port. WAN-bound packets then pass through the VPX VM's bridge and are accelerated automatically, whether they originate inside or outside the server hosting VPX.

*Figure 2. An Inline Deployment that Accelerates External Traffic and Traffic from Local VMs*
Installing SD-WAN Virtual Appliances on XenServer

Jan 23, 2017

To install Citrix NetScaler SD-WAN virtual appliances on Citrix XenServer, you must first install XenServer on a machine with adequate system resources. To perform the SD-WAN VPX installation, you use Citrix XenCenter, which must be installed on a remote machine that can connect to the XenServer host through the network.

Before you begin installing a virtual appliance, do the following:

- Install a supported version of XenServer® on hardware that meets the minimum requirements. See the SD-WAN release notes for the supported versions of XenServer.
- Install XenCenter® on a management workstation that meets the minimum system requirements.
- Obtain VPX license files.

With the prerequisites met, you are ready to import the virtual appliances and configure them.

1. Start XenCenter on your workstation.
2. On the Server menu, click Add.
3. In the Add New Server dialog box, in the Hostname text box, type the IP address or DNS name of the XenServer server that you want to connect to.
4. In the User Name and Password text boxes, type the administrator credentials, and then click Connect. The XenServer name appears in the navigation pane with a green circle, which indicates that the XenServer is connected.
5. In the navigation pane, click the name of the XenServer server on which you want to install SD-WAN VPX.
6. On the VM menu, click Import.
7. In the Import dialog box, in Import file, browse to the location at which you saved the SD-WAN VPX .xva image file. Make sure that the Exported VM option is selected, and then click Next.
8. Select the XenServer server on which you want to install the virtual appliance, and then click Next.
9. Select the local storage repository in which to store the virtual appliance, and then click Import to begin the import process.
10. Add, modify, or delete virtual network interfaces as required. Attach virtual network interfaces, interface 0 and interface 1 to the two different virtual adapters (called Networks on this screen). These two interfaces are used as the accelerated bridge of the virtual appliance. If virtual network interface interface 2 exists, it can be assigned as well, and used as a management interface (equivalent to the Primary port).

   Important: Do not attach both virtual adapters to the same network. Doing so creates forwarding loops, which can cause network outages. Also, do not attach the two physical Ethernet ports associated with SD-WAN VPX to the same Ethernet switch.

   When finished, click Next.

11. Clear the Start the VM after Import check box
12. Click Finish to complete the import process. To view the status of the import process, click the Log tab. The newly created virtual machine appears under the server list in the XenCenter interface.

To configure the virtual SD-WAN appliance

1. In XenCenter, select the icon for the SD-WAN VPX virtual machine. Then, on the Storage tab, select Properties and, in
the Properties dialog box, adjust the disk allocation to the desired level.

Note:
- Changing the disk allocation on the SD-WAN VPX virtual machine resizes and reinitializes the compression history. Any accumulated history is lost.
- Do not attempt to change resource allocation while SD-WAN VPX is running.
- Do not use the Force Shutdown or Force Reboot commands. They might not work and can cause problems. Use the Shutdown and Reboot commands instead.

Figure 1. Setting the disk allocation

2. Right-click the Branch Repeater VPX icon and select the Properties option. Under CPU and Memory, select the number of VCPUs and the amount of VM memory corresponding to a supported configuration. See Supported Configurations for more details.

Figure 2. Setting the virtual CPU and memory allocations

3. In the Branch Repeater VPX Properties dialog box, click Startup Options, and then select the Auto-start on server boot check box. (The OS Boot Parameters are not used).

Figure 3. Setting the start-on-server-boot option

4. Set the basic network parameters. Depending on which release you are running, do one of the following:
   1. For Release 6.0, after the virtual machine starts, go to the virtual machine console, log into the command-line interpreter, and set the IP parameters for the accelerated bridge, using the following example as a guide:
      Login: admin
      Password: password
      admin> set adapter apa -ip 172.16.0.213 -netmask 255.255.255.0 -gateway 172.16.0.1
      admin> restart

      Figure 4. Setting the IP parameters for the accelerated bridge

   2. For Release 6.1 or later, when a Repeater VPX virtual machine is started for the first time, it automatically runs the Deployment Wizard. Follow the wizard to set the IP parameters.

5. After the SD-WAN VPX has restarted, log on to the browser-based UI (Default credentials: admin and password) at the IP address that you assigned to apA

6. From the Command menu, select Quick Installation.

7. On the Quick Installation page, perform a quick installation as you would for a physical SD-WAN appliance.

8. Enable bridging by clicking the Enable Bridging link.

9. Check the network assignments in XenCenter to make sure that the two accelerated bridge ports are connected to different networks, and then click OK.

   Important: Connecting the two accelerated bridge ports to the same virtual or physical Ethernet segment creates network loops, which can bring down your entire network. In such a case, shut down the SD-WAN VPX virtual machine and fix the network assignments before proceeding.
10. Complete the configuration.
Installing SD-WAN Virtual Appliances on VMware ESX

Jun 11, 2018

Warning

Ensure that you enable the promiscuous mode on VM Network only. Do not enable the promiscuous mode on the Virtual Switch setting.

Before installing Citrix Branch Repeater virtual appliances on VMware ESX, make sure that VMware ESX server is installed on a machine with adequate system resources. To install virtual appliances on VMware ESX version 4.1 or VMware ESXi version 4.0, or later, you use the VMware vSphere client. The client must be installed on a remote machine that can connect to VMware ESX through the network. After the installation, you can use the vSphere client to manage virtual appliances on either VMware ESX or VMware ESXi.

Before you begin installing a virtual appliance, do the following:

- Install VMware ESX version 4.1 or ESXi 4, or later, on hardware that meets the minimum requirements.
- Install the VMware vSphere client on a management workstation that meets the minimum system requirements.
- Download the SD-WAN VPX setup files.
- Obtain SD-WAN VPX license files.

Also, before installing a SD-WAN VPX virtual appliance, label all the interfaces that you plan to assign to VPX virtual appliances, in a unique format. In large deployments, labeling these interfaces in a unique format helps in quickly identifying them among other interfaces used by other virtual machines, such as Windows and Linux virtual machines. Such labeling is especially important when different types of virtual machines share the same interfaces.

SD-WAN VPX requires non-default networking options. Among other things, you will create two new virtual switches (vswitch0 and vswitch1) for the accelerated bridge, which must be assigned to two different virtual switches.

To label the physical network ports of the VMware ESX server:

This procedure assumes a basic familiarity with VMware vSphere. Details of the vSphere client's operation might change with new releases of the vSphere software. The VMware documentation should be considered definitive. This procedure shows the desired results and one example of achieving them.

1. Log on to the VMware ESX server by using the vSphere client.
2. In the vSphere client, select the Configuration tab, and then click Networking.
3. At the top-right corner of the screen that appears, click Add Networking.
4. In the Add Network Wizard, for Connection Type, select Virtual Machine, and then click Next.
5. Scroll through the list of vSwitch physical adapters, and choose the physical port to map to interface 1/1 on the virtual appliance.
6. Enter NS_NIC_1_1 as the name of the vSwitch to associate with interface 1/1 of the virtual appliances.
7. Click Next to finish the vSwitch creation. Repeat the procedure, beginning with step 2, to add at least one more interface to be used by your virtual appliances. Label the interfaces sequentially, in the correct format (for example, NS_NIC_1_2).
To install SD-WAN virtual appliances on VMware ESX 4.1/ESXi 4:

1. Install VMware ESX 4.1 1 (or later) on the selected server and the vSphere client on a system from which you can manage the server. You can download the software from http://downloads.VMware.com.

2. Configure the setting for the first virtual switch (vSwitch0)

- Log on to the VMware ESX server by using the vSphere client.
- On the vSphere client, select the Configuration tab, and then click Networking.
- On virtual switch vSwitch0, click Properties.

Figure 1. Configuring vSwitch0, continued

On the Properties page, select the VM Network and click Edit.

Figure 2. Configuring vSwitch0, continued

On the Security tab, enable Promiscuous Mode. Click OK.

Figure 3. Configuring vSwitch0: setting promiscuous mode.
In the Properties dialog box, verify the changes, and then click Close.

Figure 4. Configuring vSwitch0, continued
Create the second virtual switch, label it, and configure settings for the new virtual switch (vswitch1).

- Log on to the VMware ESX server by using the vSphere client.
- In the vSphere client, on the Configuration tab, click **Networking**.
- At the top-right corner of the screen that appears, click **Add Networking**.
- In the Add Network Wizard, for Connection Type, select **Virtual Machine**, and then click **Next**.
- Select the **Create a virtual switch** check box.
- Scroll through the list of vSwitch physical adapters, and choose the physical port that will map to interface 1/1 on the virtual appliance.
- Click **Next**.

Figure 5. Creating vSwitch1, continued
**Important**

Do not select Use vSwitch0 to prevent routing loops.

Figure 6. Creating vSwitch1, continued
Verify that all new and modified virtual switches are configured appropriately.

Label the new virtual switch as **apA-1** by clicking on the connection settings and typing **apA-1** in **Network Label** text box.

Click **Next**, and click **Finish**.

Enable promiscuous mode on vSwitch1, following the same steps as for vSwitch0 in Step 2.

**Figure 7. Enabling promiscuous mode on vSwitch1**

4. Create the third virtual switch, vSwitch2, following the procedure in step 3, but attaching it to the port on the WAN.
side of your network and naming it **apA-2**. Enable the promiscuous mode on vSwitch2, as you did on the other ports.

5. Change the name of the virtual machine, if desired, and then click **Next**. Install the virtual machine.

- Start the VMware vSphere client on your workstation.
- In the IP address / Name text box, type the IP address of the VMware ESX server that you want to connect to.
- In the User Name and Password text boxes, type the administrator credentials, and then click Login.
- On the File menu, click Deploy OVF Template.
- In the Deploy OVF Template dialog box, in Deploy from file, browse to the location at which you saved the SD-WAN VPX setup files, select the .ovf file, and click Next.
- Change the name of the virtual machine, if desired, and then click Next.
- Map the networks shown in the CPX OVF template to the networks that you configured on ESX host: LAN-apA1 to apA-1, and WAN-apA2 to apA-2.

### Note

Always assign the two SD-WAN bridge ports (accelerated pair ports) to different virtual and physical Ethernet segments.

If you assign both SD-WAN (accelerated pair) ports to the same virtual or physical Ethernet port or switch, you will cause network loops. These network loops can make managing SD-WAN impossible and can bring down the entire Ethernet segment. For example, you will cause network loops if you assign both SD-WAN ports to vmnic0. The same thing happens if you assign the SD-WAN ports to different physical Ethernet interfaces, but plug both Ethernet interfaces into the same physical switch.

Figure 8. Mapping network interfaces to SD-WAN VPX
Click **Next** to start installing VPX on VMware ESX. When installation is complete, a pop-up window informs you of the successful installation.

6. You are now ready to start the VPX instance. In the navigation pane, right-click the instance that you have just installed, and select **Power On**. Click the **Console tab** to emulate a console port.

7. Optionally, add a Primary Ethernet port.
   - In the navigation pane, right-click the **VPX instance** that you have just installed, and select the **Edit Settings** option. On the Virtual Machine Properties page click **Add**.
   - In **Add Hardware** window, select **Ethernet Adapter** as the device type to add, and then click **Next**.

Figure 9. Installing the Primary interface
Select VMXNET 3 as the adapter type, and select **VM Network** as the network label.

Click **Finish**, and then click **OK**.

If desired, change the memory and hard disk parameters assigned to the SD-WAN VPX virtual machine to match one of the supported, nondefault configurations listed in REF RTF39313235393a204669677572 \n \* MERGEFORMAT <Section xref>.

Figure 10. Adjusting memory and disk allocation
8. If you are running Branch Repeater VPX release 6.0, deploy the virtual appliance as follows:

- At the logon prompt (in the console window), log on with default credentials: admin as the user name and password as the password.
- Use the set adapter apa command to set the accelerated bridge (apA) IP parameters. For example: set adapter apa -ip 172.16.0.213 -gateway 172.16.0.1 -netmask 255.255.255.0.
- If you want a Primary port, use the set adapter primary command to set its IP parameters. This IP address must be different from the one assigned to apA. For example: set adapter primary -ip 172.16.1.222 -gateway 172.16.1.1 -netmask 255.255.255.0.
- Restart the virtual machine to put the parameters into effect. Type: restart.

Note
In systems with a Primary port, do not specify -gateway on both the Primary and apA ports.

9. If you are running VPX release 6.1 or later, the VPX virtual machine automatically runs the Deployment Wizard when started for the first time. Follow the instructions and prompts that appear on the screen.

10. Continue configuration from the web UI, using the URL of either apA or the Primary port. For example (your address may vary): https://172.16.0.213.
11. On the **Quick Installation** page, perform a quick installation, as you would for a physical SD-WAN appliance.

12. Enable bridging by clicking the **Enable Bridging link**.

13. Check the network assignments in XenCenter to make sure that the two network devices are connected to different Networks, and then click **OK**.

**Important**

Connecting two accelerated bridge ports to the same virtual or physical Ethernet segment creates network loops, which can bring down your entire network. In such a case, shut down the VPX virtual machine and fix the network assignments before proceeding.

14. Complete the configuration as you would with any SD-WAN installation.

**Configuring Advanced VMWare Features**

You can configure advanced VMware features to enhance SD-WAN capabilities. Most of the procedures for configuring advanced features use the vSphere Client, and details of its operation can vary with new releases of the vSphere software. The VMware documentation should be considered definitive. The procedures here show the desired results and one example of achieving them.

**VLAN Support**

SD-WAN VPX accelerates VLAN traffic automatically, without special configuration, and is thus compatible with VLAN trunking. To use VLAN trunking in a VPX deployment, the VMware server must have VLAN trunking enabled on the two apA bridge ports (apA.1 and apA.2), whose VLAN IDs must be set to "All(4095)."

**To Enable VLAN Trunking**

1. Log on to the VMware ESX server by using the vSphere client.
2. On the vSphere client, select the **Configuration** tab, and then click **Networking**.
3. On bridge port apA-1, click **Properties**.
4. On the **Properties** page, select the VM Network and click **Edit**.

Figure 11. Enabling VLAN trunking, continued
5. On the **General** tab, select **VLAN ID ALL** (4095). Click **Ok**.
Larger Disks  To support the 500 GB SD-WAN VPX configurations, the datastore must be configured to support a maximum file size of 512 GB or more. This requires that the datastore have a block size of 2 MB or greater.

To Configure the datastore in VMware ESXi 4.1:

1. Log on to the VMware ESX server by using the vSphere client.
2. Delete any existing virtual machines on the server.
3. Delete the existing datastore and create a new datastore with a block size of 2 MB or greater:
   - In the vSphere client, select the **Configuration** tab, and then click **Storage**.
   - In the datastores view, right click the datastore and select **Delete**.

   ![Image of deleting the default datastore](image)

   **Figure 12. Deleting the default datastore**
Click Add Storage… link.

**Figure 13. Adding a new datastore**

In the **Add Storage** window, select the 512 GB, Block size: 2MB as the Maximum File size. Click **Next**.

**Figure 14. Setting the datastore block size**

Create a 500 GB virtual disk.

- In the **Virtual Machine** Properties, on the Hardware tab, click **Hard disk 1**.
- Set the **Provisioned Size** value to 500 GB. Click **OK**.

**Figure 15. Creating a 500 GB virtual disk**
To Configure the Datastore in VMware ESX 4.1:

1. Boot the ESX 4.1 installation DVD.
2. Select the ESX installation as Install ESX in graphical mode.
3. After the ESX Installer welcome screen appears, switch to the shell prompt by pressing the **Ctrl+Alt+F2** keys on your keyboard.
4. Type:
   ```bash
   ps | grep Xorg
   ```
5. Kill the Xorg process. For example, if the PID of Xorg is 582, type:
   ```bash
   kill 582
   ```
6. After you kill the Xorg process, the message Press <return> to reboot appears. Do not reboot, instead, press **Ctrl+Alt+F3** to go to another console and continue working without rebooting.
7. Type:
   ```bash
   cd /usr/lib/vmware/weasel
   ```
8. Edit fsset.py (these instructions assume familiarity with vi). Type:
   ```bash
   vi fsset.py
   ```
9. Search for class vmfs3FileSystem(FileSystemType):
10. Edit the blockSizeMB parameter to 2 (default value is 1)
11. Save the file and exit vi.
12. Go to the root directory and run weasel. Type:
   cd /
   ./bin/weasel

13. Proceed with the normal installation process.

14. Create a 500 GB virtual disk.
   - In the Virtual Machine Properties, on the Hardware tab, click Hard disk 1.
   - Set the **Provisioned Size** value as 500 GB, and then click OK.

VMware Guest Customization VMware guest customization is supported for some SD-WAN parameters, but not all. The parameters for which VMware guest customization is supported are:

- Hostname
- Primary adapter network settings
- Primary DNS configuration

VMware guest customization is not supported for the following parameters:

- Accelerated bridge (apA) networks settings
- Domain name, Area, Location, Secondary DNS, Tertiary DNS, and DNS search path
- Parameters specific to SD-WAN, such as bandwidth limits.

**To configure VMware Guest Customization**

1. Start with a SD-WAN VPX virtual machine that has been configured to include the Primary port as well as apA.
2. Verify that the Ethernet port configuration matches that shown in the following figure.

   Figure 16. Verify Ethernet port assignments

Convert the VPX virtual machine into a template.

- In the **vSphere Client**, right-click Branch Repeater VPX and expand the Template option.
- Select **Convert to Template**.

   Figure 17. Convert to template
Deploy a new virtual machine from the template.

- In the vSphere Client, right-click the Branch VPX instance and select **Deploy Virtual Machine from this Template**.

Figure 18. Deploying the new virtual machine

On the Deploy Template screens, name the new VPX virtual machine, select **Thick Format** for virtual disks, and select **Customize using the Customization Wizard**.

In the Customization Wizard, enter a host name and a dummy domain name for the new VPX virtual machine.

Figure 19. Customization wizard
The value on the Time Zone screen is ignored by SD-WAN. Accept the default and go on to the next screen.

On the Network screen, select Custom Settings if you need to change the Primary port IP address from the one in the template. You then assign this address (plus a subnet mask and default gateway) to NIC3. Do not change NIC1 or NIC2.

On the DNS and Domain Settings screen, enter the DNS address used by SD-WAN VPX in the Primary DNS field. Leave the Secondary DNS and Tertiary DNS paths blank. Add a dummy domain such as test.com as the DNS Search Path.

Figure 20. Setting the DNS server
Click Next, and then click Finish to exit the Guest Customization Wizard.

In the Deploy Template Wizard, clear the Power on the virtual machine after creation check box.

Double check network assignments before powering up the virtual machine.

Attaching both apA ports to the same virtual or real switch causes network loops.

5. Start the virtual machine and continue SD-WAN configuration.
Installing SD-WAN Appliances on the Microsoft Hyper-V Platform

Jan 23, 2017
To install Citrix SD-WAN virtual appliances on Microsoft Windows Server, you must first install Windows Server, with the Hyper-V role enabled, on a machine with adequate system resources. While installing the Hyper-V role, be sure to specify the network interface cards (NICs) on the server that Hyper-V will use to create the virtual networks. You can reserve some NICs for the host. Use Hyper-V Manager to perform the SD-WAN VPX installation.

SD-WAN VPX for Hyper-V is delivered in virtual hard disk (VHD) format. It includes the default configuration for elements such as CPU, network interfaces, and hard-disk size and format. After you install a SD-WAN VPX instance, you can configure its network adapters, add virtual NICs, assign the SD-WAN IP address, subnet mask, and gateway, and complete the basic configuration of the virtual appliance.

Microsoft Server Hardware Requirements

- The server’s processor must support Intel Virtualization Technology.
- The server must run 64-bit Windows 2008 R2 SP1 (Standard, Enterprise, or DataCenter Editions), or 2012 (Standard or DataCenter Editions) with a full installation (not a Core installation), and the Hyper-V component enabled.
- Minimum system configuration is 4 GB RAM, 200 GB hard drive, and 2 physical CPU.
- Two physical Ethernet NICs are required; three are recommended.
  Note: The procedure below uses three NICs.

For more information about Windows Server 2008 R2 system requirements, see http://www.microsoft.com/windowsserver2008/en-us/system-requirements.aspx (the exact location is subject to change by Microsoft at any time).

For information about installing Microsoft Server 2008 R2, see http://technet.microsoft.com/en-us/library/dd379511(WS.10).aspx (the exact location is subject to change by Microsoft at any time).

Prerequisites for Installing SD-WAN Virtual Appliances on the Microsoft Hyper-V platform

Before you begin installing a virtual appliance, do the following:

- Enable the Hyper-V role on Windows Server 2008 R2 or 2012. For more information, see http://technet.microsoft.com/en-us/library/ee344837(WS.10).aspx (the exact location is subject to change by Microsoft at any time).
- Download the VPX setup files. If you do not have a My Citrix account, access the home page at http://www.mycitrix.com, click the New Users link, and follow the instructions to create a new My Citrix account.

To download the SD-WAN VPX setup files

1. In a Web browser, go to http://www.citrix.com/ and click My Citrix.
2. Type your user name and password.
3. Click Downloads.
4. In Search Downloads by Product, select NetScaler SD-WAN.
5. Under Virtual Appliances, select and download the required SD-WAN VPX distribution.
6. Copy the compressed file to your server.
To configure virtual NICs on the SD-WAN VPX

1. Log on to the Windows Server as an Administrator, either at a keyboard or VGA console, or through a NIC that you plan to use for managing the virtual appliance (not at one of the ports that you will use for the accelerated bridge).
2. To start Hyper-V Manager, click Start, point to Administrative Tools, and then click Hyper-V Manager.
3. In the navigation pane, under Hyper-V Manager, select the server on which you want to install SD-WAN VPX.
4. On the Actions menu, click Virtual Network Manager…
5. In the Virtual Network Manager window, in the navigation pane, under Virtual Networks, click New virtual network.
6. Choose External as type of virtual network, and then click Add.
7. Name the new virtual network as apA Network 1 and select the physical NIC to map it to.
8. Click OK to apply the changes.
9. The Apply Networking Changes popup displays a caution indicating that pending changes might disrupt network connectivity. Click Yes.
10. Repeat steps 5 to 9 for the second accelerated bridge port, but name it as apA Network 2 and connect it to a different physical port.
11. Click Apply to apply the networking changes.

Installing SD-WAN VPX on Microsoft Server by using Hyper-V Manager

After you have enabled the Hyper-V role on Microsoft Server and extracted the VPX files, you can use Hyper-V Manager to install SD-WAN VPX. After you import the virtual machine, you must configure the virtual NICs by associating them with the virtual networks created by Hyper-V. Based on the Microsoft server you are using, follow the procedure to complete the installation.

- Microsoft Server 2008 R2
- Microsoft Server 2012
Installing SD-WAN VPX on Microsoft Server 2008 R2

Performing the Installation Procedures

After you have enabled the Hyper-V role on Microsoft Server 2008 R2 and extracted the VPX files, you can use Hyper-V Manager to install SD-WAN VPX. After you import the virtual machine, you must configure the virtual NICs by associating them with the virtual networks created by Hyper-V.

Note: You cannot change any settings while the virtual appliance is running. Shut down the virtual appliance and then make changes.

To install SD-WAN VPX on Microsoft Server 2008 R2 by using Hyper-V Manager

1. Unzip the SD-WAN distribution that you downloaded from My Citrix.
2. Start Hyper-V Manager.
3. In the navigation pane, under Hyper-V Manager, select the server on which you want to install SD-WAN VPX.
4. On the Actions menu, click Virtual Switch Manager.
5. In the Import Virtual Machine dialog box, in Location, specify the path to the folder that contains the Branch VPX SD-WAN files.
   Note: If you received a compressed file, make sure that you extract the files into a folder before you specify the path to the folder.
6. Click Import.
7. Verify that the virtual appliance that you imported is listed under Virtual Machines.
8. Right-click the imported virtual machine, and then click Settings.
9. In the Settings window's navigation pane, under Hardware, select the first network adapter in the list.
   Figure 1. Configuring Ethernet ports using Hyper-V Manager

   10. In the Network drop down menu, select apA Network 1. This is the LAN interface for apA1.
11. Make sure the Enable spoofing of the MAC addresses box is selected. If it is not, select it and apply the changes.
12. In the Settings window's navigation pane, under Hardware, select the second network adapter in the list. Repeat the step 10 and step 11, and assign the adapter to apA Network 2. This is the WAN interface for apA2.
    Important: Do not configure the same Network for both the network adapters. Incorrect configuration creates packet loops, which can bring down the network.
13. Optionally, change the virtual hard disk size:
    ● In the Settings window navigation pane, under IDE Controller 0, select Hard Drive.
    ● Click Edit.
    ● Follow the steps in the Edit Virtual Hard Disk Wizard to increase the allocation to one of the supported sizes, using the Expand option in the wizard.
    Figure 2. Configuring disk and RAM allocation

14. Optionally, change the memory size.
    ● In the Settings window's navigation pane, under Hardware, select Memory.
    ● Allocate the RAM space by adjusting the memory to one of the supported sizes.
● Click OK.

15. Optionally, define the management port.
   ● Right-click the virtual machine, and then click Settings.
   ● In the Settings window navigation pane, under Hardware, select Add Hardware.
   ● Select Network Adapter from the list of devices, and then click Add.
   ● Name the new virtual network as Primary Network 3.
   ● Make sure the Enable spoofing of MAC addresses check box is selected.
   ● Click OK to apply the changes.

16. Right-click the Branch Repeater VPX virtual machine and select Connect.

17. In the file menu, click Action, and then click Start to start the virtual machine.

Figure 3. Starting the VPX virtual machine

18. When a SD-WAN VPX virtual machine is started for the first time, it automatically starts the Deployment Wizard. This wizard asks questions about the deployment mode: Inline, WCCP, or PBR (virtual inline), or Setup Using Web UI. Select Setup Using Web UI. On the next screen, enter the IP, netmask, and gateway for the apA interface, and click Finish.

19. After SD-WAN VPX has restarted, log on to the browser based UI ((user name: admin, password: password) at the IP address that you assigned to apA, for example: https://172.16.0.213

Additional Configuration
For additional configuration instructions, see the documentation for physical SD-WAN and SD-WAN appliances.

Upgrading to a Previous Release
The software upgrade mechanism built into physical SD-WAN appliances is also supported by SD-WAN VPX. Alternatively, you can install a new virtual machine running the desired release.
Installing SD-WAN VPX on the Microsoft Server 2012

Performing the Installation Procedures

After you have enabled the Hyper-V role on Microsoft Server and extracted the VPX files, you can use Hyper-V Manager to install SD-WAN VPX. After you import the virtual machine, you must configure the virtual NICs by associating them with the virtual networks created by Hyper-V.

Note: You cannot change any settings while the virtual appliance is running. Shut down the virtual appliance and then make changes.

To install SD-WAN VPX on Microsoft Server 2012 by using Hyper-V Manager

1. Unzip the Sd-WAN distribution that you downloaded from My Citrix.
2. Start Hyper-V Manager.
3. In the navigation pane, under Hyper-V Manager, select the server on which you want to install SD-WAN VPX.
5. In the Import Virtual Machine dialog box, in Location box, specify the path to the folder that contains the SD-WAN VPX files.
   Note: If you received a compressed file, make sure that you extract the files into a folder before you specify the path to the folder.
6. Click Import.
7. Verify that the virtual appliance that you imported is listed under Virtual Machines.
8. Right-click the imported virtual machine, and then click Settings.
9. In the Settings window’s navigation pane, under Hardware, select the first network adapter in the list.
10. In the Network drop down menu, select apA1 Network. This is the LAN interface for apA1.
11. Make sure the Enable MAC address spoofing box is selected. If it is not, select it and apply the changes.
12. In the Settings window’s navigation pane, under Hardware, select the second network adapter in the list. Repeat the step 10 and step 11, and assign the adapter to apA2 Network. This is the WAN interface for apA2.
   Important: Do not configure the same Network for both the network adapters. Incorrect configuration creates packet loops, which can bring down the network.
13. Optionally, change the virtual hard disk size:
   - In the Settings window navigation pane, under IDE Controller 0, select Hard Drive.
   - Click Edit.
   - Follow the steps in the Edit Virtual Hard Disk Wizard to increase the allocation to one of the supported sizes, using the Expand option in the wizard.
14. Optionally, change the memory size.
   - In the Settings window’s navigation pane, under Hardware, select Memory.
   - Allocate the RAM space by adjusting the memory to one of the supported sizes.
   - Click OK.
15. Optionally, define the management port.
   - Right-click the virtual machine, and then click Settings.
   - In the Settings window navigation pane, under Hardware, select Add Hardware.
   - Select Network Adapter from the list of devices, and then click Add.
   - Name the new virtual network as Primary Network 3.
- Make sure the **Enable spoofing of MAC addresses** check box is selected.

- Click OK to apply the changes.

16. Right-click the SD-WAN VPX virtual machine and select **Connect**.

17. In the file menu, click **Action**, and then click **Start** to start the virtual machine.

18. When a SD-WAN VPX virtual machine is started for the first time, it automatically starts the Deployment Wizard. This wizard asks questions about the deployment mode. Select **Setup Using Web UI**. On the next screen, enter the IP address, netmask, and gateway for the apA interface, and click Finish.

19. After SD-WAN VPX has restarted, log on to the browser based UI (user name: admin, password: password) at the IP address that you assigned to apA, for example: https://172.16.0.213

**Additional Configuration**

For additional configuration instructions, see the documentation for physical SD-WAN/SD-WAN appliances.

**Downgrading to a Previous Release**

The software upgrade mechanism built into physical SD-WAN/SD-WAN appliances is also supported by Sd-WAN/SD-WAN VPX. Alternatively, you can install a new virtual machine running the desired release.
Installing SD-WAN Standard Edition AMI on Amazon AWS

Jan 23, 2017

The NetScaler SD-WAN SE appliances bond multiple network paths in single virtual path. The virtual paths are monitored so that critical application paths are always routed through optimal paths. This solution enables customers to deploy applications in the cloud and utilize multiple service provider networks for seamless delivery of applications to the end-users.

To create a SD-WAN SE-VPX on Amazon AWS, you go through the same process as with creating any other instance, setting a few instance parameters to non-default settings.

Instantiating a SD-WAN Virtual Appliance (AMI) on AWS:

To install a SD-WAN virtual appliance in an AWS VPC, you need an AWS account. You can create an AWS account at http://aws.amazon.com/. SD-WAN is available as an Amazon Machine Image (AMI) in AWS Marketplace.

Note: Amazon makes frequent minor changes to its AWS pages, so the following instructions may not be up-to-date.

To instantiate a SD-WAN virtual appliance (AMI) on AWS:

1. In a web browser, type http://aws.amazon.com/.
2. Click My Account/Console, and then click My Account to open the Amazon Web Services Sign in page.
3. Use your Amazon AWS account credentials to sign in. This will take you to the Amazon Web Services page.

NetScaler SD-WAN SE appliances offers the following AWS service instances:

VPC Dashboard - isolated portion of the AWS cloud populated by AWS objects, such as EC2 instances

   – Enabled by creating a VPC in AWS. See below for configuration steps.

EC2 Dashboard - elastic compute cloud, resizable virtual services / instances

   – Enabled by creating NetScaler SD-WAN AMI. See below for configuration steps.

   – CIDR – Classless Inter-Domain Routing block, consisting of continuous IP address range, used to specify your VPC (cannot be larger then 16 regions).

SD-WAN Web Interface

   – Configure NetScaler SD-WAN AMI

The following are the requirements and limitations for deploying SD-WAN SE-VPX AMI in AWS:

• Minimum requirements:

   – AWS EC2 Instance Type: c3.2xlarge
   – Virtual CPU: 8
   – RAM: 15 GB
• **Limitations:**

  - AWS does not allow bridging of interface so Fail-to-Wire is not an option for configuring Interface Groups

**NetScaler SD-WAN with AWS**

**Deployment Scenario with AWS**

Extending the Data Center into the Cloud

Deploying an AWS region with a specified Availability Zone. Within that Virtual Private Cloud (VPC) infrastructure, SD-WAN Standard Edition AMI (Amazon Machine Image) is deployed as the VPC Gateway.

- The VPC private has routes towards the VPC Gateway.
- SD-WAN instance has a route towards the AWS VGW (VPN Gateway) for direct connect and another route towards IGW (Internet Gateway) for internet connectivity.
- Connectivity between Data Center, Branch, and Cloud leveraging different transport modes utilizing multiple WAN paths simultaneously.
- Automatic Route Learning with OSPF and BGP.
- Single IPSec tunnel across multiple paths where security re-negotiation is not required upon any link failure occurrences.
In AWS a subnet and IP address must be defined for each SD-WAN AMI interface. The number of interfaces utilized depends on the deployment use case. If the goal is to reliably access application resources that are on the LAN side of the VPX (inside the same Region), the VPX can be configured with three Ethernet interfaces; one for management on eth0, one for LAN on eth1, and one for WAN on eth2.

Alternatively, if the goal is to hair-pin traffic through the VPX to some other region or to the public internet, the VPX can be configured with two Ethernet interfaces; one for management on eth0, and a second for LAN/WAN on eth1.

SD-WAN SE AMI in AWS Overview

1. Create VPC in AWS using VPC Dashboard

To get started with Amazon Virtual Private cloud you need to create a VPC, which is a virtual network dedicated to your AWS account.

- Define CIDR blocks/Subnets and assign to VPC - for identifying the device in the network. For example; 192.168.100.0/22 is selected for the VPC in the example network diagram encompassing the WAN, LAN and Management subnets – 192.168.100.0 – 192.168.103.255) - 192.168.100.0/22
- Define an Internet Gateway for the VPC – for communicating with outside the cloud environment
- Define routing for each defined subnet - for communication between the subnets and Internet
- Define Network ACLs (Access Control List) - for controlling the inflow/outflow of the traffic from/to the subnet for security purposes
- Define Security Group - for controlling the inflow/outflow of the traffic from/to each instance of network device

2. Create an NetScaler SD-WAN AMI

- Define the Network Interfaces for the EC2 instance
- Create Elastic IP addresses for the EC2 instance
- Define Security for the EC2 instance and network interfaces

3. Connect to the SD-WAN web interface
Create a VPC in AWS - Virtual Private Cloud (VPC)

To create VPC:

1. From the AWS management console tool bar, select Services -> VPC (Networking & Content Delivery).

2. Select your VPCs, then click the Create VPC button.

3. Add Name tag, CIDR block according to your network diagram and Tenancy = default, and click Yes, Create.

Define an Internet Gateway for the VPC

To define internet gateway for the VPC:

1. From the AWS management console, select Internet Gateways - > Create Internet Gateway. The Internet Gateway traffic matching the 0.0.0.0/0 route needs to be configured in the route table. It is also required for external
access to the SD-WAN AMI web interface for further configuration.

2. Give the IGW a Name tag, and click Yes, Create.

3. Select newly created IGW and click Attach to VPC.

4. Select the previously created VPC and click Yes, Attach.

Define Subnets for the VPC to differentiate Mgmt, LAN, and WAN

To define subnets for VPC:

1. From the AWS management console, select Subnets > Create Subnets to create Mgmt, LAN and WAN subnets. Use the defined subnets to distinguish between the LAN, WAN and Mgmt subnets defined in the SD-WAN configuration.
2. Enter the details specific for the Mgmt subnet of the VPX, then create it using the Yes, Create button.

- Name tag: name to identify different subnets (Mgmt, LAN or WAN)
- VPC: <the VPC previously created>
- Availability Zone: <set at discretion>
- CIDR block: subnet specific to the defined name (Mgmt, LAN or WAN) that is a smaller subset of the CIDR previously defined

3. Repeat the process until you have created a subnet for the Mgmt, LAN, and WAN networks.

Define Route Tables for the Management Subnet

To define route tables:

1. From the AWS management console, select Route Tables > Create Route Table to create route tables for the
Mgmt, LAN and WAN subnets.

2. Enter the detail for the Mgmt subnet
   - Name tag: name to identify different subnets (Mgmt, LAN or WAN)
   - VPC: The previously created VPC

3. With the newly created route table still highlighted, select Subnet Association > Edit.

4. Make the association with the desired subnet, then click Save.

5. With the newly created route table still highlighted, select Routes > Edit.

6. Click Add another route button (only required for the Mgmt, and WAN subnets), then Save.
   - Destination: 0.0.0.0/0
• Target: The Internet Gateway (igw-xxxxxxx previously defined)

Note
AWS provides a global route table in the EC2 instance but the NetScaler SD-WAN AMI will use local route tables so that the user can control traffic forwarding to the Virtual Path.

Define Route Tables for the WAN Subnet
To define route tables:

1. From the AWS management console, select Route Tables > Create Route Table to create route tables for the Mgmt, LAN and WAN subnets.

2. Enter the details for the WAN subnet:
   • Name tag: name to identify different subnets (Mgmt, LAN or WAN)
   • VPC: The previously created VPC

3. With the newly created route table still highlighted, select Subnet Association > Edit.

4. Make the association with the desired subnet, then click Save.

5. With the newly created route table still highlighted, select Routes > Edit.

6. Click Add another route button (only required for the Mgmt, and WAN subnets), then Save.
   • Destination: 0.0.0.0/0
   • Target: <The Internet Gateway (igw-xxxxxxx previously defined)
Define Route Tables for the LAN Subnet

To define route tables for the LAN subnet:

1. From the AWS management console, select Route Tables > Create Route Table to create route tables for the Mgmt, LAN and WAN subnets.

2. Enter the details for the LAN subnet:
   - Name tag: name to identify different subnets (Mgmt, LAN or WAN)
   - VPC: The previously created VPC

3. With the newly created route table still highlighted, select Subnet Association > Edit.

4. Make the association with the desired subnet, then click Save.

Create an SD-WAN SE AMI

To create EC2 instance:

1. From the AWS management console tool bar, select Services -> EC2 (Compute).
2. Select the EC2 dashboard tool bar, select **Instances > Launch Instance**.

![EC2 Launch Instance](image1)

3. Use the **AWS Marketplace** tab to search for the SD-WAN Amazon Machine Image (AMI) or use the **My AMIs** tab to locate an owned or shared SD-WAN AMI, locate **Citrix NetScaler SD-WAN Standard Edition** and then click **Select**.

![Select AMI](image2)

4. Confirm the selection with **Continue**.

5. On the **Choose Instance Type** screen, select the **EC2 Instance Type** that was identified during preparation, then select **Next: Configure Instance Details**.
6. Enter instance details (anything not specified should be left unset/default):

- Number of Instances: 1
- Network: <select VPC previously created>
- Subnet: <select Mgmt Subnet previously defined>
- Auto-assigning Public IP: enabled
- Network interfaces > Primary IP: <enter predefined Mgmt IP>

7. Click **Next: Add Storage**

**Note**

You must associate the EC2 instance with the Mgmt Subnet in order to associate the first EC2 interface (eth0) with the SD-WAN Mgmt interface. If eth0 is not associated with the SD-WAN Mgmt interface, connectivity will be lost following a reboot.
8. Enter the following information for the Root Storage:

- Volume Type: General Purpose (SSD) GP2

9. Then select **Next: Tag Instance**

10. Give the EC2 instance a name by specifying a value for the default **Name** Tag. Optionally create other desired Tags.

11. Then select **Next: Configure Security Group**.

12. Select an existing **Security Group** or create a new Security Group:

- Default security group generated will include HTTP, HTTPS, SSH

Click the Add Rule button to add two more:

- All ICMP with Source: Custom 0.0.0.0/0
- Custom UDP Rule with Port Range: 4980 and Source: custom <known IP addresses from partner SD-WAN>

13. Select **Review** and **Launch**.
14. After complete with reviewing, select **Launch**.

15. In the **Key Pair** pop-up, either select an existing key pair or create a new key pair, then select **Launch Instance**.

**Important**

If a new key pair is created, be sure to download and store it in a safe location.

16. NetScaler SD-WAN SE AMI should now be launched successfully.

**Note**

A Security Group is a set of firewall rules that controls traffic for an EC2 Instance. Inbound and outbound rules can be edited during and after EC2 launch. Each EC2 Instance must have a Security Group assigned. Additionally, each Network Interface must have a Security Group assigned. Multiple Security Groups can be used to apply distinct sets of rules to individual Interfaces. The default Security Group added by AWS only allow traffic within a VPC.

The Security Group(s) assigned to the NetScaler SD-WAN AMI and its interfaces should accept SSH, ICMP, HTTP, and HTTPS.
Security Group assigned to the WAN interface must also accept UDP on port 4980 (for Virtual Path support). Refer to AWS help for additional detail on Security Group configuration information.

Important
Wait two hours if provisioned from a new account and then retry.

17. Navigate back to your AWS Console: EC2 Dashboard.

18. From the tool bar, under Network & Security select Network Interfaces, highlight the Mgmt interface and Edit the Name tag to give the interface a useful name.

19. Then click Create Network Interface to create the LAN interfaces:

- Description: <a user-defined description for the interface>
- Subnet: <the subnet previously defined for the interface>
- Private IP: <the private IP for the interface previously defined during preparation>
- Security Group: <the appropriate security group for the interface>

20. Repeat and click Create Network Interface to create the WAN interface.
21. Edit the Name tag for each new interface and give a useful name.

22. Highlight the Mgmt Interface and select Actions > Change Source/Dest. Check to disable Source/Dest. Check, then select Save.

23. Repeat for LAN and WAN interfaces.

24. At this point all the Network Interfaces: Mgmt., LAN, and WAN each are configured with a Name, Primary private IP, and disabled for Source/Dest. Check attribute. Only the Mgmt. Network Interface will have a Public IP associated with it.
Important
Disabling the Source/Dest. Check attribute enables the interface to handle network traffic that is not specifically destined for the EC2 instance. As the NetScaler SD-WAN AMI acts as a go-between for network traffic, the Source/Dest. Check attribute must be disabled for proper operation.

The Private IPs defined for these Network Interfaces, ultimately, must match the IP addresses in your SD-WAN configuration. It may be necessary to define more than one Private IP for the WAN Network Interface if that interface will be associated with more than one WAN Link IP in the SD-WAN configuration for this site node. This can be accomplished by defining Secondary Private IPs for the WAN Interface as needed.

25. From the EC2 Dashboard toolbar, select Instances.

26. Highlight the newly created instance, then select Actions > Networking > Attach Network Interface.

27. Attach first the LAN network interface and then the WAN network interface to the SD-WAN SE AMI.
Note

Attaching the Mgmt, LAN, and WAN in that order attaches to eth0, eth1, eth2 in the SD-WAN AMI. This aligns with the mapping of the provisioned AMI and will ensure that interfaces are not reassigned incorrectly in the event of AMI reboot.

28. From the EC2 Dashboard tool bar, select Elastic IPs (EIP), then click Allocate new address.

29. Click Allocate to allocate a new IP address, then Close after the New address request succeeded.

30. Highlight the new EIP and select Action > Associate address to associate the EIP with the Mgmt. Interface, then click Associate.

- Resource type: <network interface>
- Network interface: <previously created Mgmt. Network Interface>
- Private IP: <previously defined private IP for Mgmt>

31. Repeat the process to associate another new EIP with the WAN interface.
Configure SD-WAN SE AMI - SD-WAN Web Management Interface

To configure SD-WAN SE AMI:

1. At this point, you should be able to connect to the SD-WAN SE AMI’s management interface using a web browser.

2. Enter the Elastic IP (EIP) associated with the Mgmt. Interface. You may need to create a security exception, if the security certificate is not recognized.

3. Login to the SD-WAN SE AMI using the following credentials:
   - Username: admin
   - Password: <aws-instance-id> (example: i-00ab111abc2222abcd)

Note

If the Mgmt. Interface cannot be reached, check the following:

- Make sure the EIP is correctly associated with the Mgmt interface
- Make sure the EIP responds to ping
- Makes sure the Mgmt interface Route Table includes an Internet Gateway route (0.0.0.0/0)
- Make sure the Mgmt. interface Security Group is configured to allow HTTP/HTTPS/ICMP/SSH

Starting with release 9.1 SD-WAN AMI, users may also login to the SD-WAN AMI console using `ssh admin@<Mgmt. EIP>`, assuming that the key pair for the EC2 Instance has been added to the user’s SSH key chain.

4. For SD-WAN SE **bring-your-own-license (BYOL) AMI**, a software license must be installed:

- On the SD-WAN web interface, navigate to **Configuration > Appliance Settings > Licensing**
- From **License Configuration: Upload License for this Appliance**, select **Choose File**, browse and open the SD-WAN SE AWS license, then click **Upload and Install**
- After successful upload, License Status will indicate State: Licensed

5. Set the appropriate **Data/Time** for the new AMI:

- On the SD-WAN web interface, navigate to **Configuration > System Maintenance > Date/Time Settings**
- Set the correct date and time using **NTP, Date/Time Setting** or **Timezone**

**Note**

The SD-WAN SE AMI Virtual WAN Service will remain disabled until an appliance package (Software + Configuration) is installed on the AMI.
Add SD-WAN SE AMI to your SD-WAN Environment

To add SD-WAN AMI to your SD-WAN environment:

1. Navigate to your SD-WAN Center or Master Control Node for your SD-WAN environment.

2. Add a new site node using the Configuration Editor:
   - Add site: model CBAWS, Mode: client
   - Interface Groups: awsLAN = eth1, awsWAN = eth2 (untrusted)
   - Virtual IP Address: 192.168.100.5 = awsLAN, 192.168.101.5 = awsWAN

   *with awsLAN virtual IP address being configured, the SD-WAN will advertise the LAN subnet of 192.168.100.5/24 as a local route to the SD-WAN Environment (refer to the Connections > <AWSnode> > Routes).

WAN Links:

- AWSBR-WAN with Access Type Public Internet, Autodetect Public IP if client node or configure the EIC for WAN link if MCN node, Access Interfaces: awsWAN 192.168.101.5 with gateway 192.168.101.1 (#.#.#.1 is typically the AWS reserved gateway).

3. In the Configuration Editor validate the path association under Connections > DC > Virtual Paths > DC-AWS > Paths.
**Note**

The Virtual Path will be used across the AMI WAN interface to push software and configuration updates to the SD-WAN AMI instead of via direct connection to the Mgmt. interface.

Private IP addresses must be defined on EC2 WAN Network Interface for every WAN Link IP in the Configuration Editor. This can be accomplished by defining one or more Secondary Private IPs for the Network Interface as necessary.

---

**Important**

Recall the assigned mapping in AWS EC2 dashboard assigning Mgmt. to eth0, LAN to eth1 and WAN as eth2.

Amazon reservices the first four IP addresses and the last IP address in each subnet CIDR block and can not be assigned to an instance. For example, in a subnet with CIDR block 192.168.100.0/24, the following five IP addresses are reserved:

- 192.168.100.0: Network address
- 192.168.100.1: Reserved by AWS for the VPC router
- 192.168.100.2: Reserved by AWS for the DNS server
- 192.168.100.3: Reserved by AWS for future use
- 192.168.100.255: Network broadcast address, which is not supported in a VPC

---

4. **Save and Export** the newly created SD-WAN configuration and export to the **Change Management Inbox**.
5. Navigate to the MCN Change Management and run through the change management process to push the latest configuration to the SD-WAN environment informing all existing SD-WAN nodes of the newly added AWS node and the subnets (virtual interfaces) associated with it. Make sure to upload the software package specific to CBAWS in the Change Preparation step that matches the current software used by the existing SD-WAN environment.

6. From the Change Management page, download the package generated specifically for the new AWS node using the active link.

7. Navigate back to the SD-WAN SE AMI’s management interface using the assigned EIP for the Mgmt. interface.


9. Click Choose File to browse and Upload the active AWS software/config package recently downloaded.

10. After successful Local Change Management, the web interface should auto-refresh with the latest installed software, with the Virtual WAN Service still disabled.

11. On the SD-WAN SE AMI navigate to Configuration > Virtual WAN Enable/Disable/Purge Flows and enable the service using the Enable button.

12. Upon successful connectivity on the WAN interface, the SD-WAN will report Good Path State on the Monitoring > Statistics > Paths page.
Troubleshooting

The correct private Internet Web Gateway (IWG) IP must be used in the SD-WAN Access Interface configuration

- If an incorrect IWG is used in the Configuration Editor to define the WAN Link for the AWS Site (Virtual IP Address and the correct Gateway) then Virtual Path will fail to establish.
- A quick way to check if the IWG is incorrectly configured is to check the SD-WAN ARP table.

SD-WAN built in Packet Capture tool can help confirm proper packet flow

1. Navigate to the Configuration > System Maintenance > Diagnostic page of the SD-WMA AMI.

2. Select the Packet Capture tab, and set the following settings, then click Capture:
   - Interfaces: 2  //in order to capture on eth2 which was associated with the WAN interface

3. The capture output on the web page should show the UDP probe packets leaving the SD-WAN SE AMI with the WAN VIP/Private IP as the source, with a destination of the Static Public IP(s) used for the MCN, also the returning UDP packet with source of the MCN Static Public IP and destination of the local VIP/Private IP (which was NAT’d by the IWG).
Note

This can typically occur when an IP address is accidently created outside of the CIDR block assigned to the VPC.
# Supported Modes

Jan 23, 2017

Table 1. Features Table for Citrix NetScaler SD-WAN VPX, and Citrix NetScaler SD-WAN VPX for Amazon

<table>
<thead>
<tr>
<th>Feature</th>
<th>Citrix NetScaler SD-WAN VPX</th>
<th>Citrix NetScaler SD-WAN VPX for Amazon</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoConfiguration</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>SD-WAN/SD-WAN Plug-In</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Compression</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RPC over HTTPS</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>SSL Compression</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>TCP Acceleration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Traffic Shaping</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Video Caching</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Windows File System Acceleration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Windows Outlook Acceleration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>XenApp/ XenDesktop Acceleration</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Group Mode Mode</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>High Availability</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Inline Mode</td>
<td>Y</td>
<td>Y**</td>
</tr>
<tr>
<td>Virtual Inline Mode</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>WCCP Mode</td>
<td>N (SD-WAN)</td>
<td>N</td>
</tr>
<tr>
<td>VLANs</td>
<td>Y/Y/N***</td>
<td>N</td>
</tr>
</tbody>
</table>

*Depends on configuration of user-provided hardware.

**See [WAN Optimization for SD-WAN](https://docs.citrix.com).

***The three values are for is for XenServer, VMware, and Hyper-V, respectively. In columns showing only one value, the value applies to all three hypervisors.
Managing the Appliance

Nov 30, 2016

SD-WAN 4000/5000 is an appliance containing multiple virtual SD-WAN WAN accelerators controlled by a single virtual NetScaler load balancer. This combination provides a high-performance WAN accelerator for busy datacenters.
Automatically Configuring SD-WAN WANOP Appliances

Mar 22, 2017
If you are using Citrix Command Center to manage your Citrix SD-WAN WANOP appliances, the AutoConfiguration feature enables a SD-WAN WANOP appliance to automatically register itself with Citrix Command Center. After you have specified a DNS IP address in the setup wizard, the appliance performs reverse and forward lookups to identify the Command Center IP address. If you opt for having the appliance automatically configured by the Command Center server, the server starts configuring the appliance automatically soon after the appliance is registered with it. The Command Center server uses configuration profiles selected for the appliance to run configuration commands on the appliance. Additionally, you can use Citrix Command Center to manage and monitor the appliance remotely.

Note
This feature is supported with Citrix Command Center release 5.2 build 41 and later.

The autoconfiguration feature is supported on the following appliances

• SD-WAN 400 WANOP appliance
• SD-WAN 800 WANOP appliance
• SD-WAN 1000/2000 WANOP appliances
• SD-WAN 3000 WANOP appliance
• SD-WAN 1000/2000 WANOP appliances with Windows Server

Registering a SD-WAN WANOP Appliance with Citrix Command Center
Before you can use Citrix Command Center to manage a SD-WAN WANOP appliance, you must register the appliance with it.

To configure a SD-WAN WANOP appliance for autoconfiguration:

1. In the SD-WAN WANOP setup wizard (System > Configuration > System > Setup Wizard), specify the IP address of the DNS server used by the SD-WAN WANOP device.

2. Enter the registration password that you specified in Configure SD-WAN Registration Settings on the Command Center server, and click OK. Leave this field blank if you have not changed the password.

The SD-WAN WANOP appliance sends a registration request to the Command Center server, which automatically discovers the device and runs the commands available in the configuration profile.
Alternatively, you can navigate to Configuration > Appliance Settings > Logging/Monitoring page and specify the Command Center details on the Command Center tab.

To register the appliance with Citrix Command Center:

1. Navigate to the Configuration > Appliance Settings > Logging/Monitoring page.

2. Click the Command Center tab.

3. In the IP Address field, type the IP address of the Citrix Command Center appliance with which you want to register the SD-WAN appliance.

4. In the Port field, type the port number used for Citrix Command Center. 8443 is the default port number used for Citrix Command Center.

5. In the Registration Password field, type the password that the Command Center administrator has set for a SD-WAN appliance to log on to Citrix Command Center.

Do not specify any password if the Command Center administrator has accepted the default password for registering the appliance.

6. Click Update.

7. Select AutoConfiguration By Citrix Command Center option to automatically configure the appliance through Command Center. The Status field changes from Disabled to Initiated registration, which later changes to Request accepted if the registration of the appliance with Citrix Command Center is successful.

Your SD-WAN WANOP appliance is registered with Citrix Command Center and you can now manage the appliance remotely by using Citrix Command Center.
Installing SD-WAN WANOP Edition AMI on Amazon AWS

Jan 23, 2017

The NetScaler SD-WAN VPX for Amazon AWS brings acceleration support to the Amazon cloud.

Note: At the time of the 7.1.0 software release, the newest supported release of SD-WAN (now SD-WAN) WANOP-VPX for Amazon AWS is 7.0.1. Use this version in conjunction with release 7.1.0 on other appliances.

Five variations are supported, four of which have hardwired licensing, and one of which uses ordinary SD-WAN licensing:

- 2 Mbps
- 10 Mbps
- 20 Mbps
- 45 Mbps
- “Bring your own license,” which uses a standard Citrix license to determined the licensed bandwidth.

Besides the hardwired licensing, the major difference between SD-WAN WANOP-VPX for Amazon AWS is that it supports only a single port for both management and acceleration. This means that the appliance cannot be used in inline mode.

To create a SD-WAN WANOP-VPX on Amazon AWS, you go through the same process as with creating any other instance, setting a few instance parameters to non-default settings.

**Instantiating a SD-WAN Virtual Appliance (AMI) on AWS**


Note: Amazon makes frequent minor changes to its AWS pages, so the following instructions may not be exact.

**To instantiate a SD-WAN virtual appliance (AMI) on AWS**

2. Click My Account/Console, and then click My Account to open the Amazon Web Services Sign in page.
3. Use your Amazon AWS account credentials to sign in. This will take you to the Amazon Web Services page.
4. Click EC2 in the Compute & Networking section, then click Launch Instance.
5. In the Create a New Instance dialog box, select AWS Marketplace, and then click Continue to open the Request Instance Wizard.
6. In the Request Instance Wizard dialog box, click AWS Marketplace tab.
7. In the Search text field, type SD-WAN to search for the SD-WAN AMI, and click Search.
   - On the search result page, select one of the Citrix SD-WAN offerings On the Citrix SD-WAN page, click Continue.
8. On the Launch with EC2 Console tab, click the Accept Terms button, if present, then click Launch with EC2 Console for the region where you want to launch Citrix SD-WAN AMI.
9. On the Request Instance Wizard page, type 1 in the Number of Instances text box, and from the Instance Type drop-down list, select Large (m1.large, 7.5GIB).
10. From the Subnet drop-down list, select the private network subnet, and then click Continue.
11. On the next page, in the Advanced Instance Options section, you can change values from their defaults if you choose, and then click Continue.
   Note: SD-WAN AMI is not supported with more than one network interface. Therefore, the value of Number of Network Interfaces field is set to 1.
12. On the Request Instances Wizard page, enter a name for the EC2 instance in the Value text box, and then click Continue.

   On the Request Instances Wizard page, select one of the three Key Pair options and then click Continue.
13. Verify the EC2 instance configuration details, and then click Launch to launch the EC2 instance.
14. Click Close to close the Launch Instance Wizard dialog box. The new EC2 instance is launched successfully.
Disabling the Source/Destination Check Feature

Oct 18, 2013
You must disable the Source/Destination check feature of SD-WAN AMI instance for it to work properly on AWS.

To disable the Source/Destination check feature
1. On the Amazon EC2 Console Dashboard page, in the navigation pane, click instances. The new EC2 instance should appear in the My Instances list.
2. Select the new EC2 instance. The instance details appear in the EC2 Instances pane.
3. Right-click the new EC2 instance and then select Change Source/Dest Check from the popup menu.
4. In the Change Source / Dest. Check dialog box, click Yes, Disable to disable the feature.
Configuring SNMP Monitoring for the SD-WAN WANOP Edition AMI on AWS

Oct 18, 2013

You must enable SNMP monitoring on the SD-WAN AMI on AWS. Also, you must grant SNMP monitoring access to the paired NetScaler VPX or SD-WAN Connector on AWS by adding its NSIP on the SD-WAN AMI instance.

To configure SNMP monitoring on the SD-WAN Connector AMI by using the SD-WAN graphical user interface:

1. In the navigation pane, expand Configuration, and then click Logging/Monitoring.
2. In the details pane, click the SNMP tab.
3. In the System Information section, in the SNMP Status row, click Enable. This action enables SNMP monitoring on the SD-WAN AMI instance.
4. In the Access Configuration section, add SNMP monitoring access to SD-WAN VPX appliance by setting the following parameters:
   - Community String (set to the string public)
   - Management Station IP (set to the NSIP of the SD-WAN VPX on AWS)

5. Click Add.
Limitations and Usage Guidelines for the SD-WAN WANOP Edition AMI Instances on AWS

Oct 18, 2013

- High Availability setup for SD-WAN AMI instances is not supported.
- SD-WAN AMI instance in Group Mode is not supported.
- SD-WAN plug-ins are not supported.
- Tagged VLAN is not supported because of the inherent limitation of AWS.
- Traffic shaping is not supported.
- You may create only an m1.large SD-WAN AMI instance on AWS.
- IP address/gateway/subnet assignment using the SD-WAN management user interface is not supported.
- Console access is not available for SD-WAN AMI instance on AWS.
- While configuring the SD-WAN instance, you may not change the disk size, which has a default value of 250 GB. A higher capacity disk does not increase the available Disk Based Compression (DBC) cache size.
The process of allocating your SD-WAN licenses has been greatly simplified. The new licensing framework allows you to focus on getting maximum value from Citrix products.

In the SD-WAN configuration utility (GUI), you can use your hardware serial number (HSN) or your license activation code (LAC) to allocate your licenses. Alternatively, if a license is already present on your local computer, you can upload it to the appliance.

For all other functionality, such as returning or reallocating your license, you must use the licensing portal. Optionally, you can still use the licensing portal for license allocation. For more information about the licensing portal, see "http://support.citrix.com/article/CTX131110".

Note:
- On a SD-WAN appliance, you can use the HSN or LAC to allocate your license or upload the license to the appliance from a local computer. On a SD-WAN VPX appliance, you can only upload the license to the appliance from a local computer.
- You must purchase separate licenses for each appliance in a high availability (HA) pair. Make sure that the same type of licenses are installed on both the appliances. For example, if you purchase a platinum license for one appliance, you must purchase another platinum license for the other appliance.

Note: You must purchase separate licenses for each appliance in a high availability (HA) pair. Make sure that the same type of licenses are installed on both the appliances. For example, if you purchase a platinum license for one appliance, you must purchase another platinum license for the other appliance.
Prerequisites

Jun 24, 2014
To use the hardware serial number or license activation code to allocate your licenses:

- The management service virtual machine of the appliance must have an access to public domain.
- Your license must be linked to your hardware, or you must have a valid license activation code (LAC). Citrix sends your LAC by email when you purchase a license.
Allocating your License by using the Configuration Utility

Feb 11, 2014

If your license is already linked to your hardware, the license allocation process can use the hardware serial number. Otherwise, you must type the license activation code (LAC).

To allocate your license

1. In a web browser, type the IP address of the management service of the SD-WAN appliance (for example, http://192.168.100.1).
2. In User Name and Password, type the administrator credentials.
3. Navigate to the System > Configuration tab.
4. On the Configuration tab, navigate to System > Licenses.
5. In the details pane, click Manage Licenses.
6. Click Update Licenses, and then select one of the following options:
   - **Use Hardware Serial Number**—The software internally fetches the serial number of your appliance and uses this number to display your license(s).
   - **Use License Activation Code**—Citrix emails the LAC for the license that you purchased. Enter the LAC in the text box.
7. Click Get Licenses. Depending on the option that you selected, one of the following dialog boxes appears.
   - The following dialog box appears if you selected Hardware Serial Number.
   - The following dialog box appears if you selected License Activation Code.
8. Select the license that you want to allocate, and then click Get.
9. Click Apply for the license to take effect.
Installing the License

Jun 24, 2014
If you downloaded your license file to your local computer by accessing the licensing portal, you must upload the license to the appliance.

To install a license file by using the configuration utility

1. In a web browser, type the IP address of the SD-WAN appliance (for example, http://192.168.100.1).
2. In User Name and Password, type the administrator credentials.
3. On the Configuration tab, navigate to System > Licenses.
4. In the details pane, click Manage Licenses.
5. Click Update Licenses, and then select Upload License Files.
6. Click Add New License, then select Upload license files from a local computer.
7. Click Browse. Navigate to the location of the license files, select the license file, and then click Open.
Verifying SD-WAN Licenses

Dec 01, 2016
Before using a feature, make sure that your license supports the required number of accelerators.

To verify the number of licensed accelerators by using the configuration utility

1. In a Web browser, type the IP address of the appliance, such as http://192.168.100.1.
2. In User Name and Password, type the administrator credentials.
3. Navigate to the **System > Configuration** tab. The License Information section displays the number of accelerators licensed.
4. Alternately, navigate to **SD-WAN > Instances**. The Licensed column displays the status of licensed accelerates as green.
Internet Protocol Version 6 (IPv6) Acceleration - SD-WAN WANOP Appliances

Nov 30, 2016

Note
IPv6 Acceleration is supported only on the SD-WAN WANOP appliances. This feature is not supported on the SD-WAN Standard Edition and Enterprise Edition appliances.

When you connect to the Internet through a device, the device is assigned an IP address. The IP address identifies and indicates the location of the appliance. The number of devices connecting to the Internet is rapidly increasing. As a result, it is difficult to manage the request for the IP addresses with the existing version of Internet Protocol (IP), IPv4, which uses 32-bit addresses. By using IPv4, approximately 4.3 billion addresses can be assigned to the devices connecting to the Internet.

IPv6 addresses this issue by using 128-bit addresses and a hexadecimal label to identify the network interfaces of devices on an IPv6 network. Because IPv6 supports far more IP addresses than does IPv4, organizations and applications are gradually introducing support for the IPv6 protocol.

The IPv4 and IPv6 protocols are not interoperable, which makes the transition difficult. To accelerate the increasing IPv6 traffic from various applications supported on the SD-WAN appliance, you can enable the IPv6 Acceleration feature.

By default, IPv6 is disabled on the appliance.

To enable IPv6 acceleration on a SD-WAN appliance
1. Navigate to the System > Configuration > System page.
2. Click enable the Enable IPv6 for Data Traffic link in the System Settings section.
3. Select the Enable IPv6 for Data Traffic option in the dialog box
4. Click OK, as shown in the following screen shot.
Verifying IPv6 Connections

Nov 30, 2016

After enabling IPv6 acceleration on the appliance, the appliance starts accelerating traffic for the applications using IPv6 protocol. To make sure that the appliance is accelerating the IPv6 traffic, you can monitor such connections on the appliance.

To monitor the IPv6 connections, navigate to the SD-WAN > Monitoring tab. The Connections page of the Monitoring tab display IPv6 protocols traffic related statistics:

- **Connections**: The Connections page lists details of all the connections established with the appliance. This page consists of two tabs, Accelerated Connections and Unaccelerated Connections. The Accelerated Connections tab lists all connections that the appliance is accelerating. You can identify IPv6 traffic in this tab by referring to the Initiator and Responder column of each entry. If these columns contain hexadecimal IP address values, the entry represents an IPv6 connection, as shown in the following screen shot.

  IPv6 connections that are not accelerated, are listed on the Unaccelerated Connections tab. If you want to accelerate these connections, you might need to troubleshoot and fine tune the application parameters on the appliance. As on the Accelerated Connections tab, you can identify the IPv6 connections on this tab by referring to the Initiator and Responder columns of each entry.

- **Top Applications**: The Top Applications page provides granularity in the time frame that you can use to graphically represent the traffic throughput of various applications served by the SD-WAN appliance. By default, traffic throughput is displayed by the last minute. However, you can change the time frame by selecting Last Minute, Last Hour, Last Day, Last Week, or Last Month from the list available on the Title bar of the page. This page has three tabs, Top Applications Graphs, Since Last Restart, and Active Applications (Since Last Restart). The Top Applications Graphs tab contains the following statistics:
  - **Total Application Link Throughput Percentage (Sent)**: This is a pie chart depicting the percentage of traffic that the appliance has sent to each application. If the appliance has sent a significant percentage of traffic for an application using IPv6 protocol, the application has its percentage of traffic depicted in this graph.
  - **Total Application Link Throughput Percentage (Received)**: This is a pie chart depicting the percentage of traffic that the appliance has received from each application. If the appliance has received a significant percentage of traffic from an application using IPv6 protocol, the graph displays the percentage of traffic generated by the application.
  - **Sent Rate**: This is a stacked graph of series of data depicting the rate, in bits per second, at which the appliance has sent traffic to each application. If the appliance has sent data to an application using IPv6 protocol, a series depicting each application using IPv6 protocol is also plotted on this graph.
  - **Received Rate**: This is a stacked graph of series of data depicting the rate, in bits per second, at which the appliance has received traffic from each application. If the appliance has received data from an application using IPv6 protocol, a series depicting each application using IPv6 protocol is also plotted on this graph.
  - **Top Applications table**: This is a table of statistics for each application. The table lists all applications for which the
The appliance has served traffic, along with sent and received rates in bits per second, total bytes sent and received, percentage of the traffic for the application, and the rate at which the appliance has served traffic for the application. If the appliance has served traffic for an application using IPv6 protocol, the application is listed in this table, along with its statistics.

- **Application Groups**: This is a table of statistics for each application, along with its application group and parent application, if any. The table lists bytes sent and received for the application. Each application, and its application group and parent application are displayed as hyperlinks. If you click the hyperlink, granular details of the statistics are displayed for the link you have clicked. If the appliance has served traffic for an application using IPv6 protocol, the application is listed in this table, along with its statistics.

The **Since Last Restart** tab contains statistics on the application traffic since the time you restarted the appliance. The tab contains the Total Application Link Throughput Percentage (Sent) and Total Application Link Throughput Percentage (Received) graphs, and Top Applications and Application Groups tables, depicting statistics similar to the Top Applications Graphs tab but with data since the appliance was restarted. The **Active Applications (Since Last Restart)** tab contains a table listing all active applications since the appliance was restarted. This table contains details about sent and receive rate, total bytes sent and received, and total packets sent and received for the applications.
NetScaler SD-WAN Standard Edition in AWS now supports basic CloudWatch for monitoring your SD-WAN instance running on AWS infrastructure. CloudWatch alarms send notifications or automatically make changes to the resources you are monitoring. Under basic monitoring, seven pre-selected metrics at five minute frequency and three status check metrics at one minute frequency are available for your SD-WAN instance for no additional charge. You can view the following metrics for your SD-WAN image.

- a) CPU Utilization - The percentage of allocated compute units that are currently being used for the instance. This metric identifies the processing power required to run an application upon a selected instance.
- b) Diskread operations - Read operations from all instance volumes available for the specified period.
- c) DiskWrite operations – Write operations for all instance store volume available for the instance in a specified duration of time.
- d) DiskReadBytes – Bytes written to all instance store volumes available to the running instance
- e) NetworkIn – This metric identifies the volume of incoming traffic for a single instance.
- f) Network Out - This metric identifies the volume of outgoing traffic for a single instance.
- g) Networkpacketsout – Number of packets sent out on all network interfaces by the instance, this is only available for basic monitoring.
Auto Secure Peering and Manual Secure Peering

Apr 03, 2017

Enterprise Edition appliance can be installed at the data center and has the capability to initiate auto or manual secure peering, create SSL profile and associate service class, and join the appliance to a Windows Domain Controller for allowing users/administrator to make use of the extended rich feature of standalone WANOP appliance.

Following are the deployment modes supported for Auto Secure Peering and Manual Secure Peering:

**Auto Secure Peering Deployments**

1. **To perform auto secure peering to an EE appliance from a standalone WANOP / SDWAN SE/WANOP on the DC site.**

   Steps to initiate this deployment:
   
   - WANOP DC appliance is in LISTEN ON mode (2312/Any non-standard port) and Branch EE is in CONNECT-TO mode.
   
   - WANOP DC initiates automatic secure peering to an EE appliance which installs the Private CA Certs and CERT KEY Pairs and configure CONNECT-TO on the EE appliance with WANOPs LISTEN-ON IP.

2. **To perform Auto-secure peering initiated from EE appliance at DC site and Branch site EE appliance.**

   Steps to initiate this deployment:
   
   - EE DC appliance is in LISTEN ON mode (on port 443). Branch EE is in CONNECT-TO mode.
   
   - EE DC appliance initiates automatic secure peering to an EE Branch appliance which installs the Private CA Certs and CERT KEY Pairs and configures CONNECT-TO on the EE Branch appliance with DC EE's LISTEN-ON IP.
   
   - LISTEN-ON IP for EE is in the interface IP associated to the routing domain for which “Redirect to WANOP” is enabled.

3. **Auto Secure Peering initiated from EE Appliance at DC site and Branch with WANOP/ SDWAN SE appliance.**

   Steps to initiate this deployment:
   
   - EE DC appliance is in LISTEN ON mode (on port 443). Branch WANOP / SDWAN SE is in CONNECT-TO mode.
   
   - EE DC appliance initiates automatic secure peering to Branch WANOP / SDWAN SE appliance which installs the Private CA Certs and CERT KEY Pairs and configures CONNECT-TO on the EE appliance with DC EE's LISTEN-ON IP.

**Manual Secure Peering Deployments**

4. **Manual Secure Peering initiated from EE appliance at DC site to Branch EE Appliance.**

   Steps to initiate this deployment:
   
   - EE DC appliance is in LISTEN ON mode (on port 443). Branch EE is in CONNECT-TO mode.
   
   - LISTEN-ON IP for EE is in the interface IP associated to the routing domain for which “Redirect to WANOP”
5. **Manual Secure Peering initiated from EE appliance at DC site to Branch WANOP/SDWAN-SE Appliance.**

Steps to initiate this deployment:

- EE DC appliance is in LISTEN ON mode (on port 443). Branch WANOP / SDWAN SE is in CONNECT-TO mode.
- LISTEN-ON IP for EE is in the interface IP associated to the routing domain for which “Redirect to WANOP” is enabled.
- Manually upload CA and Cert Key pair certificates obtained from authentic source of certificate authority.
Configuration

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Keystore Password*

Confirm Keystore Password*

Disable Keystore Password

Save  Cancel
### Secure Peering

#### Keystore Settings

- **Keystore Status:** Opened

#### Secure Peering Certificate and Keys

Secure communications with the CloudBridge partner appliance require that you generate OpenSSL credentials, including CA Certificate and Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

- [ ] Enable Secure Peering
- Certificate Configuration
  - Private CA
  - CA Certificate

[Save] [Cancel]

---

### Secure Peering

#### Keystore Settings

- **Keystore Status:** Opened

#### Secure Peering Certificate and Keys

<table>
<thead>
<tr>
<th>Secure Peering</th>
<th>Certificate/Key Pair Name</th>
<th>CA Certificate Store Name</th>
<th>Cipher Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>private_10_100_184_74</td>
<td>PrivateRootCA</td>
<td>IADH/1ECDHE/MDS-HIGH@STRENGTH</td>
</tr>
</tbody>
</table>

#### Connected Peers

- Private Root CA
- Private Root CA
- Private Root CA
Monitoring

VIP of Remote EE App
<table>
<thead>
<tr>
<th>Record</th>
<th>DateTime</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>S335</td>
<td>Mar 01, 2017, 05:50:20</td>
<td>syslog/Log 1:05:49:20 hostname: vps NTRIO(7762) RESPONSE - Status: Success</td>
</tr>
<tr>
<td>S334</td>
<td>Mar 01, 2017, 05:49:20</td>
<td>syslog/Log 1:05:48:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S331</td>
<td>Mar 01, 2017, 05:48:20</td>
<td>syslog/Log 1:05:47:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S330</td>
<td>Mar 01, 2017, 05:47:20</td>
<td>syslog/Log 1:05:47:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S328</td>
<td>Mar 01, 2017, 05:45:20</td>
<td>syslog/Log 1:05:45:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S327</td>
<td>Mar 01, 2017, 05:45:20</td>
<td>syslog/Log 1:05:45:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S326</td>
<td>Mar 01, 2017, 05:44:20</td>
<td>syslog/Log 1:05:45:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S325</td>
<td>Mar 01, 2017, 05:43:20</td>
<td>syslog/Log 1:05:43:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S324</td>
<td>Mar 01, 2017, 05:42:20</td>
<td>syslog/Log 1:05:42:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S323</td>
<td>Mar 01, 2017, 05:41:20</td>
<td>syslog/Log 1:05:41:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S322</td>
<td>Mar 01, 2017, 05:40:20</td>
<td>syslog/Log 1:05:40:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S321</td>
<td>Mar 01, 2017, 05:39:20</td>
<td>syslog/Log 1:05:39:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S320</td>
<td>Mar 01, 2017, 05:38:20</td>
<td>syslog/Log 1:05:38:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S319</td>
<td>Mar 01, 2017, 05:37:20</td>
<td>syslog/Log 1:05:37:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S318</td>
<td>Mar 01, 2017, 05:36:20</td>
<td>syslog/Log 1:05:36:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S317</td>
<td>Mar 01, 2017, 05:35:20</td>
<td>syslog/Log 1:05:35:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S316</td>
<td>Mar 01, 2017, 05:34:20</td>
<td>syslog/Log 1:05:34:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
<tr>
<td>S315</td>
<td>Mar 01, 2017, 05:33:20</td>
<td>syslog/Log 1:05:33:20 hostname: vps NTRIO(7762) PAYLOAD: (&quot;param&quot;=&quot;system_info&quot;)</td>
</tr>
</tbody>
</table>
Configuration

Secure Peering

Keystore Settings

- Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.
- Enable Keystore Password

SSL Profiles

Secure Peering

Keystore Settings

- Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

SSLs allow the appliance to compress SSL traffic such as HTTPS and SSL-encrypted XML/HTTP/SCUDP/SSHP traffic. Secure partner configuration is a prerequisite to SSL acceleration. SSL acceleration requires additional security credentials on the server side. NetScaler SD-WAN INO appliance(s) and SSL-specific configuration (called an SSL profile) for each group of SSL services. This step should be repeated on a client side appliance.
Monitoring
### Citrix NetScaler SD-WAN 2000-250-EE

**System Information**

- **IP Address**: 172.16.16.13
- **(instance)IP**: 172.16.1.14
- **Current IP**: 172.16.1.14
- **Last Connection Error**: No Last Error
- **Bytes Recieved**: 76,354
- **Bytes Sent**: 3,852
- **Number Of Connections**: 2

**Secure Partners**

<table>
<thead>
<tr>
<th>Partner Name</th>
<th>IP Address</th>
<th>Secure</th>
<th>Connection Status</th>
<th>Time Connected</th>
<th>Time Since Last Contacted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure</td>
<td>172.16.16.13</td>
<td>True</td>
<td>Connected Available</td>
<td>13m 6s</td>
<td>9m 6s</td>
</tr>
</tbody>
</table>

**Software Revision**

- **ECDSA-256-SHA-256 bit**
- **Private IP**: 192.168.194.12

---

### Citrix NetScaler SD-WAN (V50)-WO

**Monitoring > Secure Partners**

- **IP Address**: 172.30.194.11
- **Secure**: True
- **Connection Status**: Connected Available
- **Time Connected**: 13m 6s
- **Time Since Last Contacted**: 9m 6s

**Software Revision**

- **Flexible**
- **ECDSA-256-SHA-256 bit**
- **Private IP**: 192.168.194.12
- **Last SSL Connection Error**: No Last Error
- **Last Connection Error**: No Last Error
- **Bytes Recieved**: 76,354
- **Bytes Sent**: 3,852
- **Number Of Connections**: 2
### System Information

<table>
<thead>
<tr>
<th>Peer Name</th>
<th>IP Address</th>
<th>Instance ID</th>
<th>Secure</th>
<th>Connection Status</th>
<th>Time Connected</th>
<th>Last Conn.</th>
<th>Last Contacted</th>
<th>Base TSP</th>
<th>Last TSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname1</td>
<td>172.16.44.48</td>
<td>True</td>
<td>Connected Available</td>
<td>13h as</td>
<td>0m 3s</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Active Partners

<table>
<thead>
<tr>
<th>Peer</th>
<th>Pass TSP</th>
<th>Total Sent Bytes</th>
<th>Total Recv Bytes</th>
<th>Last Minute Sent Rate</th>
<th>Last Minute Recv Rate</th>
<th>Accelerated Connections</th>
<th>Max Active Connections</th>
<th>Max Connects</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Logging

<table>
<thead>
<tr>
<th>Record</th>
<th>Date/Time</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>533</td>
<td>May 01, 2017 05:03:20</td>
<td>syslogInfo 105502 hostname vps NTR007TX23 REQUEST User admin Client IP 127.0.0.1 Method GET Resource system_info</td>
</tr>
<tr>
<td>534</td>
<td>May 01, 2017 05:03:20</td>
<td>syslogInfo 105502 hostname vps NTR007TX23 RESPONSE Status Success</td>
</tr>
</tbody>
</table>
| 535    | May 01, 2017 05:03:20 | syslogInfo 105502 hostname vps NTR007TX23 PAYLOAD ("params":"

---

https://docs.citrix.com  © 1999-2017 Citrix Systems, Inc. All rights reserved.  p.1078
## Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN 10.0 partner require that you generate OpenSSL credentials, including CA Certificate and CA Certificate Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

<table>
<thead>
<tr>
<th>Secure Peering</th>
<th>Certificate Key Pair Name</th>
<th>CA Certificate Store Name</th>
<th>Cipher Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>private_rsa_10_12</td>
<td>PrivateRootCA</td>
<td>AES256-SHA256/OPEN192STRENGTH</td>
</tr>
</tbody>
</table>

## Citrix NetScaler SD-WAN 2000-250-IE

### Configuration

**Connect Peer**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>10.105.184.3</td>
</tr>
<tr>
<td>Username</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>*********</td>
</tr>
</tbody>
</table>
Monitoring

### Secure Peering

#### Keystore Settings
- Fingerprint:

#### Secure Peering Certificate and Keys
- **Name:** Secure Peering
- **Key Info:**
  - **Key File Name:** private_10_151_154_12
  - **Subject:** PrimesiveCA
  - **Validity:**
    - **Not Before:** 2017-01-13 00:00:00
    - **Not After:** 2022-01-12 23:59:59
  - **CRL Distribution Points:** Not Applicable
  - **Certificate Policies:** Not Applicable
  - **Subject Key Identifier:** Not Applicable

#### Connected Peers

<table>
<thead>
<tr>
<th>Partner Name</th>
<th>IP Address</th>
<th>Status</th>
<th>Connected Available</th>
<th>Time Connected</th>
<th>Time Close Last Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.1.2</td>
<td>True</td>
<td>Connected Available</td>
<td>7m 12s</td>
<td>7m 12s</td>
</tr>
</tbody>
</table>

### Monitoring Statistics

#### Certificate and Keys

<table>
<thead>
<tr>
<th>Certificate Key Pairs</th>
<th>Application Date</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA Certificates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate Key Pairs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Last Certificate & Key
- **Name:** private_10_151_154_12
- **Validity:**
  - **Not Before:** 2017-01-13 00:00:00
  - **Not After:** 2022-01-12 23:59:59

### System Information

- **Last Connect:** 10.10.154.12
- **Current Session:** 10.10.154.12
- **Last Connect IP:** 10.10.154.12
- **Current Session IP:** 10.10.154.12
- **Last Connect Status:** Connected Available
- **Time Connect:** 7m 12s
- **Time Close Last Connection:** 7m 12s

### Monitor Statistics

<table>
<thead>
<tr>
<th>Monitor Type</th>
<th>Sent</th>
<th>Received</th>
<th>Error Rate</th>
<th>Connect Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>247.5Mbps</td>
<td>247.5Mbps</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>UDP</td>
<td>247.5Mbps</td>
<td>247.5Mbps</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>IPv6</td>
<td>247.5Mbps</td>
<td>247.5Mbps</td>
<td>0%</td>
<td>100%</td>
</tr>
</tbody>
</table>

---

https://docs.citrix.com © 1999-2017 Citrix Systems, Inc. All rights reserved. p.1081
Troubleshooting
**Configuration**

### CA Certificates

<table>
<thead>
<tr>
<th>Name</th>
<th>Expiration Date</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Feb 25 01:39:42 2032 GMT</td>
<td>1</td>
</tr>
</tbody>
</table>

### Certificate Key Pairs

<table>
<thead>
<tr>
<th>Certificate Key Pair Names</th>
<th>Expiration Date</th>
<th>Cert Count</th>
<th>Key Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA_keypair</td>
<td>2033-07-18 20:01:18</td>
<td>1</td>
<td>RSA</td>
</tr>
</tbody>
</table>
Secure Peering

**Keystore Settings**

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

- Enable Keystore Password

**Secure Peering Certificate and Keys**

Secure communications with the NetScaler SD-WAN WO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

- Enable Secure Peering
- Certificate Configuration
  - Private CA
  - CA Certificate

- Certificate/Key Pair Name
- CA Certificate Store Name

- Certificate Verification
  - Signature/Expiration

- SSL Cipher Specification
  - [GDH=1AEC407IMD/5HIGH@STRENGTH]

- Edit Cipher Specification

[Save] [Cancel]
Monitoring

Citrix NetScaler SD-WAN 2000-250-E

Dashboard  Monitoring  Configuration

Monitoring > WAN Optimization > Partners

System Information
Agent ID: 10.10.10.10

Secure Partners

Partner Name  IP Address  Insecure IP  Secure  Connection Status  Time Connected  Time Since Last Connected
Software Version
Connection Initiation
SSL Options
Last Connection Name
Last OK Connection Time

Active Partners

Partner Name  IP Address  Port
Software Version
Connection Initiation
SSL Options
Last Connection Name
Last OK Connection Time

Troubleshooting
### System Information

#### Secure Partners
- **Agent ID**: 0.0.0.0.0.0

<table>
<thead>
<tr>
<th>Partner Name</th>
<th>IP Address</th>
<th>Instance IP</th>
<th>Secure</th>
<th>Connection Status</th>
<th>Time Connected</th>
<th>Time Since Last Contacted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ipswitch-gui</td>
<td>10.10.1.3</td>
<td>True</td>
<td>Connected Available</td>
<td>10m 12s</td>
<td>1</td>
<td>1.5h A</td>
</tr>
</tbody>
</table>

#### Action Partners

<table>
<thead>
<tr>
<th>Partner Name</th>
<th>Total Acceptedflows</th>
<th>Total Throughput</th>
<th>Last Minute Send Rate</th>
<th>Last Minute Receive Rate</th>
<th>AssociatedConnections</th>
<th>Max-ActionConnections</th>
<th>Max-Connections</th>
<th>Idle</th>
<th>Instance IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ipswitch-gui</td>
<td>10.10.1.3</td>
<td>422.0B</td>
<td>241.0Kbps</td>
<td>756.4Kbps</td>
<td>1</td>
<td>5</td>
<td>6</td>
<td>2m 12s</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>
Configuration

Citrix NetScaler SD-WAN 2000-300-EE

Configuration > WAN Optimization > Secure Acceleration > Certificate and Keys > CA Certificate

Certificate Key Pair

<table>
<thead>
<tr>
<th>Name</th>
<th>Expiration Date</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSLCA</td>
<td>Jan 29, 2022 02:00:00 PM</td>
<td>1</td>
</tr>
</tbody>
</table>

Certificate Key Pair Viewer

Certificate: SSLCA
Expiration Date: Jan 29, 2022 02:00:00 PM

Secure Peering

Keystore Settings

Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for secure acceleration to resume.

Enable Keystore Password

Save Cancel
Secure Peering

Keystore Settings

Security keys and settings are secured by the keystore password. Each time the appliance restarts, the keystore is closed automatically, and must be opened manually for secure acceleration to resume.

Enable Keystore Password

Keystore Password

Save

Secure Peering Certificate and Keys

Secure communications with the NetScaler SD-WAN WO partner appliance requires that you generate OpenSSL credentials, including CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification. If PrivateCA is selected, certificates and keys are generated automatically.

Enable Secure Peering

Certificate Configuration

Private CA

CA Certificate

Certificate/Key Pair Name

CA KeyPair

CA Certificate Store Name

CA

Certificate Verification

Signature/Expiration

SSL Cipher Specification

[ADH=1,3,5,5,3,1,5,9,0,1,9,1,9,0,2,2,0,0]

Edit Cipher Specification

Save

Listen On and Connect To

Listen On and Connect To

Connect To

172.16.104.3

Listen On

172.20.194.3:8443

Connected to

172.16.104.3:8443

Monitoring
Troubleshooting
Domain Join

When the appliance joins the Windows domain, the Windows domain controller accepts the appliance as a delegate user; the appliance becomes a trusted member of the domain for certain functions. This allows the appliance to be a client of the domain's security infrastructure, which in turn allows the acceleration of authenticated and encrypted data streams using Windows protocols such as DFS and NDS. For the purposes of accelerating DFS and NDS, security delegation can be limited to the relevant services as part of the standard Windows delegation mechanism. This constrained delegation is available with Windows Server 2003.
Join the server-side NetScaler SD-WAN appliance to a domain that the Windows file server and Exchange server are both a part of. Joining the domain makes the appliance a trusted member of the Windows security system.

**Domain Name**: [Input Field]

**User Name**: [Input Field]

**Password**: [Input Field]

**DNS Server**: [Input Field]
Delegate User

Add a delegate user account of the Windows domain controller. The NetScaler SD-WAN appliance uses this account on behalf of the users, to authenticate them with the domain controller.

Domain Name

User Name

Password

Add  Cancel

No items
Delegate Users

Add a delegate user account on behalf of the user, to authenticate them with the domain controller.

- Domain Name: 2keepod.com
- User Name: userdel
- Password: ********

Add Cancel

Delegate User Check: Summary

- DNS Reachability Test
- Forward lookup Test
- Domain Reachability Test
- Host Name Validation Test
- Kerberos config file check
- Reverse lookup zone
- Time Skew Check
- Kerberos Port Check
- NTP Port Check
- Server record for kerberos
- Server record for ldap

Close
Delegate Users

Add a delegate user account of the Windows domain controller. The NetScaler SD-WAN appliance uses this account on behalf of the users, to authenticate them with the domain controller.

- Domain Name: `2keeppod.com`
- User Name: `userdel`
- Password: `********`

Add | Cancel

Delegate Users

<table>
<thead>
<tr>
<th>User Name</th>
<th>Domain Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>userdel</td>
<td>2KEEPPOD.COM</td>
<td>Success</td>
</tr>
</tbody>
</table>

Delegate User Details

- Services:
  - `cifs\WIN-KB88EBRNRUD.2KEEPPOD.COM/2KEEPPOD.com`
  - `exchangeMDB\WIN-KB88EBRNRUD.2KEEPPOD.COM`

Close
1. The user's application opens a TCP connection to the server, sending a TCP SYN packet.
   S src: 10.0.0.50, Ddst: 10.200.0.10

2. The WANOP Plug-In looks up the destination address and sees that it matches a subnet accelerated by the appliance. It attaches CloudBridge options to the TCP header of the SYN packet. No addresses are changed.
   S src: 10.0.0.50, D dst: 10.200.0.10

3. The appliance notes the SYN options and recognizes that this is an acceleratable connection. It strips the options from the packet and allows it to pass through to the server. No addresses are changed.
   S src: 10.0.0.50, D dst: 10.200.0.10

4. The server accepts the connection and responds with a TCP SYN-ACK packet.
   S src: 10.200.0.10, Ddst: 10.0.0.50

5. The appliance tags the SYN-ACK packet with a TCP header option that shows that acceleration will take place.
   S src: 10.200.0.10, Ddst: 10.0.0.50

6. The WANOP Plug-In receives the SYN-ACK packet. The options in the packet headers indicate that the connection is accelerated. The Plug-In strips the options and passes the SYN-ACK packet to the application. The connection is now fully open and accelerated.
1. The user's application opens a TCP connection to the server, sending a TCP SYN packet.
   
   Src: 192.0.0.50, Dst: 10.200.0.10

2. The Repeater Plug-in looks up the dst address and decides to redirect the connection to the appliance at 10.200.0.201.
   
   Src: 192.0.0.50, Dst: 10.200.0.201
   (10.200.0.10 is preserved in a TCP option field. Options 24-31 are used for various parameters.)

3. The appliance accepts the connection and forwards the packet to the server (using the dst address from the TCP options field), and gives itself as the src.
   
   Src: 10.200.0.201, Dst: 10.200.0.10

4. The server accepts the connection and responds with a TCP SYN-ACK packet.
   
   Src: 10.200.0.10, Dst: 10.200.0.201

5. The appliance rewrites the addresses and forwards the packet to the Plug-in (placing the server address in an option field).
   
   Src: 10.200.0.201, Dst: 10.0.0.50

6. The connection is now fully open. The client and server send packets back and forth via the appliance.

   While the addresses are altered in Redirector mode, the destination port numbers are not (though the ephemeral port number may be). The data is not encapsulated. Redirector mode is a proxy, not a tunnel.

   There is no 1:1 relationship between packets (though in the end, the data received is always identical to the data sent). Compression may reduce many input packets into a single output packet. CIFS acceleration will perform speculative read-ahead and write-behind operations. Also, if packets are dropped between appliance and the Repeater Plug-in, the retransmission is handled by the appliance, not the server, using advanced recovery algorithms.
Use a Dedicated Appliance When Possible

Use Inline Mode When Possible

Place the Appliances in a Secure Part of Your Network

Avoid NAT Problems

•
•
•
•

Select Softboost Mode
Define Plug-in Acceleration Rules

---

### Repeater Plug-In: Acceleration Rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Rule Type</th>
<th>Destination IP/Netmask</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Exclude</td>
<td>10.200.33.102</td>
<td>All</td>
</tr>
<tr>
<td>2</td>
<td>Exclude</td>
<td>10.200.33.102</td>
<td>All</td>
</tr>
<tr>
<td>3</td>
<td>Exclude</td>
<td>10.200.33.104</td>
<td>All</td>
</tr>
<tr>
<td>4</td>
<td>Exclude</td>
<td>10.200.33.105</td>
<td>All</td>
</tr>
<tr>
<td>5</td>
<td>Accelerate</td>
<td>10.0.0.0/8</td>
<td>All</td>
</tr>
<tr>
<td>Default</td>
<td>Exclude</td>
<td>All</td>
<td>All</td>
</tr>
</tbody>
</table>
IP Port Usage

•

•

TCP Option Usage and Firewalls
Welcome to the Citrix Accelerator Plugin Setup Wizard

The Setup Wizard will install Citrix Accelerator Plugin on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Completed the Citrix Accelerator Plugin Setup Wizard

Click the Finish button to exit the Setup Wizard.

- Signaling IP: 172.16.0.203
- Data Cache: 7.50 GB
- Bandwidth Gain: 39%
- Traffic Graph

Citrix Acceleration plug-in Enabled - 6.1.0.213.200938 (Production)
Deterministic Network Enhancer locking error

Deterministic Network Enhancer installation requires a reboot first, to free locked resources. Please run this install again after restarting the computer.

c:\windows\inf

find "dne2000.cat" oem*.inf

CatalogFile= dne2000.cat

notepad oem13.inf

Other Installation Problems
Advanced Display

Apr 06, 2017

The Advanced page contains four tabs: Rules, Connections, Diagnostics, and Certificates.

At the bottom of the display are buttons to enable acceleration, disable acceleration, and return to the Basic page.

The Rules tab displays an abbreviated list of the acceleration rules downloaded from the appliances. Each list item shows the appliance's signaling address and port, acceleration mode (redirector or transparent), and connection state, followed by a summary of the appliance's rules.

The Connections tab lists the number of open connections of different types:

- **Accelerated Connections**—The number of open connections between the WANOP Client Plug-in and appliances. This number includes one signaling connection per appliance but does not include accelerated CIFS connections. Clicking More opens a window with a brief summary of each connection. (All of the More buttons allow you to copy the information in the window to the clipboard, should you want to share it with Support.)
- **Accelerated CIFS Connections**—The number of open, accelerated connections with CIFS (Windows file system) servers. This is usually the same as the number of mounted network file systems. Clicking More displays the same information as with accelerated connections, plus a status field that reports Active if the CIFS connection is running with WANOP Client Plug-in's special CIFS optimizations.
- **Accelerated MAPI Connections**—The number of open, accelerated Outlook/Exchange connections.
- **Accelerated ICA connections**—The number of open, accelerated XenApp and XenDesktop connections using the ICA or CGP protocols.
- **Unaccelerated Connections**—Open connections that are not being accelerated. You can click More to display a brief description of why the connection was not accelerated. Typically, the reason is that no appliance accelerates the destination address, which is reported as Service policy rule.
- **Opening/Closing Connections**—Connections that are not fully open, but are in the process of opening or closing (TCP "half-open" or "half-closed" connections). The More button displays some additional information about these connections.
The Diagnostics page reports the number of connections in different categories, and other useful information.

- **Start Tracing/Stop Tracing**—If you report a problem, your Citrix representative might ask you to perform a connection trace to help pinpoint problems. This button starts and stops the trace. When you stop tracing, a pop-up window shows the trace files. Send them to your Citrix representative by the means he or she recommends.

- **Clear History**—This feature should not be used.

- **Clear Statistics**—Pressing this button clears the statistics on the Performance tab.

- **Console**—A scrollable window with recent status messages, mostly connection-open and connection-close messages, but also error and miscellaneous status messages.

On the Certificates tab, you can install security credentials for the optional secure peering feature. The purpose of these security credentials is to enable the appliance to verify whether the plug-in is a trusted client or not.

To upload the CA certificate and certificate-key pair:

1. Select **CA Certificate Management**.
2. Click **Import**.

3. Upload a CA certificate. The certificate file must use one of the supported file types (.pem, .crt, .cer, or .spc). A dialog box might appear, asking you to Select the certificate store you want to use and presenting you with a list of keywords. Select the first keyword in the list.

4. Select **Client Certificate Management**.

5. Click **Import**.

6. Select the format of the certificate-key pair (either PKCS12 or PEM/DER).

7. Click **Submit**.

---

**Note**

In the case of PEM/DER, there are separate upload boxes for certificate and key. If your certificate-key pair is combined in a single file, specify the file twice, once for each box.
Updating the WANOP Plug-in

Apr 06, 2017
To install a newer version of the WANOP Client Plug-in, follow the same procedure you used when installing the plug-in for the first time.

To uninstall the WANOP Client Plug-in, use the Windows Add/Remove Programs utility. The WANOP Client Plug-in is listed as Citrix Acceleration Plug-in in the list of currently installed programs. Select it and click Remove.

You must restart the system to finish uninstalling the client.
Troubleshooting WANOP Plug-in

Apr 06, 2017

**Issue:** I am facing signaling channel connectivity issues. How can I resolve these issues?

**Resolution:** To resolve signaling channel connectivity issues, perform the following troubleshooting steps:

- Verify that you have correctly configured the signaling IP address. You can do so by pinging the signaling IP address and verifying the response.
- Verify that the signaling status is enabled on the WANOP appliance.
- Verify that the firewall installed on the network does not remove the WANOP TCP options.
- Verify that a valid WANOP plug-in license is installed on the WANOP appliance.
- Verify that the Signaling Channel Source Filtering configuration does not block the Client Source IP address.
- If you have enabled LAN Detection, verify that the Round Trip Time between the WANOP plug-in and WANOP appliance is an acceptable value.

**Issue:** On a WANOP 4000 appliance, I am not able to disable the WANOP plug-in.

**Cause:** This is a known issue.

**Resolution:** None. You cannot disable the WANOP plug-in on a WANOP 4000 appliance.

**Issue:** When connecting to the WANOP appliance by using the WANOP plug-in, the following error message entry is logged on the Alerts tab:

More WANOP Plug-ins than the current limit of <Number> have attempted to connect to this Appliance.

**Cause:** The number of connections to the WANOP appliance has exceeded the licensed user limit.

**Resolution:** Either wait for a user to disconnect or terminate a connection.

**Issue:** Incorrect signaling IP address is configured on a WANOP 4000 or 5000 appliance.

**Resolution:** To update the signaling IP address on a WANOP 4000 or 5000 appliance, complete the following procedure:

1. Log on to the NetScaler instance of the WANOP appliance.
3. Update the signaling IP address.
4. Save the configuration.

**Issue:** CIFS and ICA traffic is not getting accelerated.

**Resolution:** To resolve this issue, perform the following troubleshooting steps:

- Verify that acceleration rules for IP address and port numbers are correctly defined for the WANOP plug-in.
- Verify that CIFS or ICA connections are established after signaling connection is successful.
- Verify the acceleration policy for the service class being used.
SNMPv3 Polling and Trap Capability

Mar 22, 2017

NetScaler SD-WAN supports 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 Integrate > Configure Events and Alerts page and fill in the fields as required.
Standard MIB Support

Jan 17, 2017
The following standard MIBs are supported by the SD-WAN Appliances.

<table>
<thead>
<tr>
<th>MIB</th>
<th>RFC Definition (Link)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISMAN-EVENT-MIB</td>
<td><a href="https://www.ietf.org/rfc/rfc2981.txt">https://www.ietf.org/rfc/rfc2981.txt</a></td>
</tr>
<tr>
<td>IF-MIB</td>
<td><a href="https://www.ietf.org/rfc/rfc2863.txt">https://www.ietf.org/rfc/rfc2863.txt</a></td>
</tr>
<tr>
<td>IP-FORWARD-MIB</td>
<td><a href="https://www.ietf.org/rfc/rfc4292.txt">https://www.ietf.org/rfc/rfc4292.txt</a></td>
</tr>
<tr>
<td>IP-MIB (Partial)</td>
<td><a href="https://www.ietf.org/rfc/rfc4293.txt">https://www.ietf.org/rfc/rfc4293.txt</a></td>
</tr>
<tr>
<td>SNMPv2-MIB</td>
<td><a href="https://www.ietf.org/rfc/rfc3418.txt">https://www.ietf.org/rfc/rfc3418.txt</a></td>
</tr>
<tr>
<td>TCP-MIB</td>
<td><a href="https://www.ietf.org/rfc/rfc4022.txt">https://www.ietf.org/rfc/rfc4022.txt</a></td>
</tr>
<tr>
<td>P-BRIDGE-MIB.txt</td>
<td><a href="http://www.icir.org/fenner/mibs/extracted/P-BRIDGE-MIB-rfc2674.txt">http://www.icir.org/fenner/mibs/extracted/P-BRIDGE-MIB-rfc2674.txt</a></td>
</tr>
<tr>
<td>RMON2-MIB.txt</td>
<td><a href="https://www.ietf.org/rfc/rfc3273.txt">https://www.ietf.org/rfc/rfc3273.txt</a></td>
</tr>
</tbody>
</table>

You must download the following SNMP files before you can start monitoring a NetScaler SD-WAN appliance:

- CITRIX-COMMON-MIB.txt
- APPACCELERATION-SMI.txt
- APPACCELERATION-PRODUCTS-MIB.txt
- APPACCELERATION-TC.txt
- APPACCELERATION-STATUS-MIB.txt
The MIB files are used by SNMPv3 managers and SNMPv3 trap listeners. The files include the SD-WAN appliance enterprise MIBs, which provides SD-WAN-specific events. To download MIB files, in the SD-WAN web management interface:

1. Navigate to Configuration > Appliance Settings > SNMP > Download MIB File page.

2. Select the required MIB file.

3. Click View.

The MIB file opens in MIB browser.

- 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, for example: Nagios or SolarWinds.

- The Ethernet port packet and byte counters are in the IF-MIB inside the ifTable. System information is in the system object.

- Ethernet ports are included in the ifTable, so walking that should be sufficient to ensure that the SNMP subsystem is running.

- Support for the Q-BRIDGE-MIB and the IP-MIB provides support for the network mapping application in SolarWinds.

References

For additional information about adding SNMP manager, configuring SNMP View/Alarm, and adding SNMP server, see the CloudBridge 7.4 documentation at: http://docs.citrix.com/content/dam/docs/en-us/cloudbridge/7-3/downloads/en.cloudbridge.cb-wrapper-73-con.pdf
Reference Material

Mar 21, 2017

Application Signature Library
A list of applications that the SD-WAN appliance can identify using Deep Packet Inspection.
This article outlines security best practices for the NetScaler SD-WAN solution. It provides general security guidance for NetScaler SD-WAN deployments.

NetScaler SD-WAN Deployment Guidelines

To maintain security through the deployment lifecycle, Citrix recommends the following security consideration:

- Physical Security
- Appliance Security
- Network Security
- Administration and Management

Deploy NetScaler SD-WAN Appliances in a Secure Server Room - The appliance or server on which NetScaler SD-WAN is installed, should be placed in a secure server room or restricted data center facility, which protects the appliance from unauthorized access. At the minimum, access should be controlled by an electronic card reader. Access to the appliance should be monitored by CCTV that continuously records all activity for auditing purposes. In the event of a break-in, electronic surveillance system should send an alarm to the security personnel for immediate response.

Protect Front Panel and Console Ports from Unauthorized Access - Secure the appliance in a large cage or rack with physical-key access control.

Protect Power Supply - Make sure that the appliance is protected with an uninterruptable power supply (UPS).

For appliance security, secure the operating system of any server hosting a NetScaler SD-WAN virtual appliance (VPX), perform remote software updates, and following secure lifecycle management practices:

- Secure the Operating System of Server Hosting a NetScaler SD-WAN VPX Appliance - A NetScaler SD-WAN VPX appliance runs as a virtual appliance on a standard server. Access to the standard server should be protected with role based access control and strong password management. Additionally, Citrix recommends periodic updates to the server with the latest security patches for the operating system, and update-to-date antivirus software on the server.
- Perform Remote Software Updates - Install all security updates to resolve any known issues. Refer to the Security Bulletins web page to sign up and receive up-to-date security alerts.
- Follow Secure Lifecycle Management Practices - To manage an appliance when redeploying, or initiating RMA, and decommissioning sensitive data, complete the data-reminisce countermeasures by removing the persistent data from the appliance.

For network security, do not use the default SSL certificate. Use Transport Layer Security (TLS) when accessing the administrator interface, protect the appliance’s non-routable management IP address, configure a high availability setup, and implement Administration and Management safeguards as appropriate for the deployment.

- Do not use the NetScaler Default SSL Certificate - An SSL certificate from a reputable Certificate Authority simplifies...
the user experience for Internet-facing Web applications. Unlike the situation with a self-signed certificate or a certificate from the reputable Certificate Authority, web browsers do not require users to install the certificate from the reputable Certificate Authority to initiate secure communication to the Web server.

- **Use Transport Layer Security when Accessing Administrator Interface** - Make sure that the management IP address is not accessible from the Internet or is at least protected by a secured firewall. Make sure that the LOM IP address is not accessible from the Internet or is at least protected by a secured firewall.

- **Secure Administration and Management Accounts** – Create an alternative admin account, set strong passwords for admin and viewer accounts. When configure remote account access, consider configuring externally authenticated administrative management of accounts using RADIUS and TACAS. Change the default password for the admin user accounts, configure NTP, use the default session timeout value, use NSMPv3 with SHA Authentication and AES encryption.

NetScaler SD-WAN overlay network protects data traversing the SD-WAN overlay network.

**Secure Administrator Interface**

For secure web management access, replace default system certificates by uploading and installing certificates from a reputable Certificate Authority.

**Configuration > Appliance Settings > Administrator Interface:**

User Accounts:

- Change local user password
- Manage users

HTTPS Certs:

- Certificate
- Key

Miscellaneous:

- Web Console Timeout
Configuration Editor > Advanced > Global > Virtual WAN Network Settings

Global Firewall Settings

- Global Policy Template
- Default Firewall Actions
- Default Connection State Tracking
Global Virtual Path Encryption Settings

- AES 128-bit (default)
- Encryption Key Rotation (Default)
- Extended Packet Encryption Header
- Extended Packet Authentication Trailer
AES-128 data encryption is enabled by default. It is recommended to use AES-128 or additional protection of AES-256 encryption level for path encryption. Ensure that “enable Encryption Key Rotation” is set to ensure key regeneration for every Virtual Path with encryption enabled using an Elliptic Curve Diffie-Hellman key exchange at intervals of 10-15 minutes.

If the network requires message authentication in addition to confidentiality (i.e. tamper protection), Citrix recommends using IPsec data encryption. If only confidentiality is required, Citrix recommends using the enhanced headers.

- Extended Packet Encryption Header enables a randomly seeded counter to be prepended to the beginning of every encrypted message. When encrypted, this counter will serve as a random initialization vector, deterministic only with the encryption key. This will randomize the output of the encryption, providing strong message indistinguishability. Keep in mind that when enabled this option will increase packet overhead by 16 bytes
- Extended Packet Authentication Trailer appends an authentication code to the end of every encrypted message. This trailer allows for the verification that packets are not modified in transit. Keep in mind this option will increase packet overhead.

The recommended Firewall configuration is with a default Firewall action as deny all at first, then add exceptions. Prior to adding any rules, document and review the purpose of the firewall rule. Use Stateful inspection and Application level inspection where possible. Simplify rules and eliminate redundant rules. Define and adhere to a change management process that tracks and allows for review of changes to Firewall settings. Set the Firewall for all appliances to track...
connections through the appliance using the global settings. Tracking connections verifies that packets are properly formed and are appropriate for the connection state. Create Zones appropriate to the logical hierarchy of the network or functional areas of the organization. Keep in mind that zones are globally significant and can allow geographically disparate networks to be treated as the same security zone. Create the most specific policies possible to reduce the risk of security holes, avoid the use of Any in Allow rules. Configure and maintain a Global Policy Template to create a base level of security for all appliances in the network. Define Policy Templates based on functional roles of appliances in the network and apply them where appropriate. Define Policies at individual sites only when necessary.

**Global Firewall Templates** - Firewall templates allow for the configuration of global parameters that impact the operation of the firewall on individual appliances operating in the SD-WAN overlay environment.

**Default Firewall Actions** – Allow enables packets not matching any filter policy are permitted. Deny enables packets not matching any filter policy are dropped.

**Default Connection State Tracking** – Enables bidirectional connection state tracking for TCP, UDP, and ICMP flows that do not match a filter policy or NAT rule. Asymmetric flows will be blocked when this is enabled even when there are no Firewall policies defined. The settings may be defined at the site level which will override the global setting. If there is a possibility of asymmetric flows at a site, the recommendation is to enable this at a site or policy level and not globally.

**Zones** - Firewall zones define logical security grouping of networks connected to the NetScaler SD-WAN. Zones can be applied to Virtual Interfaces, Intranet Services, GRE Tunnels, and LAN IPsec Tunnels.

Untrusted security zone should be configured on WAN links directly connected to a public (unsecure) network. Untrusted will set the WAN link to its most secure state, allowing only encrypted, authenticated and authorized traffic to be accepted on the interface group. ARP and ICMP to the Virtual IP Address are the only other traffic type allowed. This setting will also ensure that only encrypted traffic will be send out of the interfaces associated with the Interface group.

Routing Domains are network systems that include a set of routers that are used to segment network traffic. Newly created sites are automatically associated with the default Routing Domain.

**Configuration Editor > Advanced > Global**

Routing Domains
- Default_RoutingDomain

IPsec Tunnels
- Default Sets
- Secure Virtual Path User Data with IPsec
IPsec Tunnels secure both user data and header information. NetScaler SD-WAN appliances can negotiate fixed IPsec tunnels on the LAN or WAN side with non-SD-WAN peers. For IPsec Tunnels over LAN, a Routing Domain must be
selected. If the IPsec Tunnel uses an Intranet Service, the Routing Domain is pre-determined by the chosen Intranet Service.

IPsec tunnel is established across the Virtual Path before data can flow across the SD-WAN overlay network.

- Tunnel Mode 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.

Internet Key Exchange (IKE) is an IPsec protocol used to create a security association (SA). NetScaler SD-WAN appliances support both IKEv1 and IKEv2 protocols.

- Mode can be either Main Mode or Aggressive Mode.
- Identity can be automatic to identify peer, or an IP address can be used to manually specify peer's IP address.
- Authentication enables Pre-Shared Key authentication or certificate as the method of authentication.
- Validate Peer Identity enables validation of the IKE's Peer Identity if the peer's ID type is supported, otherwise do not enable this feature.
- Diffie-Hellman Groups are available for IKE key generation with group 1 at 768-bit, group 2 at 1024-bit, and group 5 at 1536-bit group.
- Hash Algorithm include MD5, SHA1, and SHA-256 has algorithms are available for IKE messages.
- Encryption Modes include AES-128, AES-192, and AES-256 encryption modes are available for IKE messages.
- IKEv2 settings include Peer Authentication and Integrity Algorithm.