CenturyLink® Versa SD-WAN
Network Configuration Guide

v16.1R2
# Table of Contents

General Disclaimer .................................................................................................................. 3
Preface ....................................................................................................................................... 4
SD-WAN Overview .................................................................................................................... 7
Versa Director UI Overview ..................................................................................................... 11
Real-Time Device Monitoring ................................................................................................. 16
Monitoring Customer Organizations ....................................................................................... 42
SD-WAN Analytics ................................................................................................................... 51
Security Analytics .................................................................................................................... 67
Configuring Hardware Devices in Inventory .......................................................................... 83
Configuring Branch Device Groups ......................................................................................... 85
Defining Interfaces .................................................................................................................. 87
Defining Networks .................................................................................................................. 95
Defining Virtual Routers ......................................................................................................... 96
Configuring IPsec Profiles ..................................................................................................... 99
Managing Staging and Post-Staging Templates .................................................................... 102
Configuring Service Templates ............................................................................................ 105
Associating Templates with Service Templates .................................................................... 107
Configuring Certificates for IPsec ......................................................................................... 109
Configuring Adaptive Shaping .............................................................................................. 133
Configuring CGNAT ............................................................................................................... 135
Defining Class of Service ...................................................................................................... 141
Stateful Firewall ...................................................................................................................... 152
General Disclaimer

Although CenturyLink has attempted to provide accurate information in this guide, CenturyLink does not warrant or guarantee the accuracy of the information provided herein. CenturyLink may change the programs or products mentioned at any time without prior notice. Mention of non-CenturyLink products or services is for information purposes only and constitutes neither an endorsement nor a recommendation of such products or services or of any company that develops or sells such products or services.

ALL INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED “AS IS,” WITH ALL FAULTS, AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED OR STATUTORY. CENTURYLINK AND ITS SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES RELATED TO THIS GUIDE AND THE INFORMATION CONTAINED HEREIN, WHETHER EXPRESSED OR IMPLIED OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

CENTURYLINK AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUES, COSTS OF REPLACEMENT GOODS OR SERVICES, LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF THE GUIDE OR ANY CENTURYLINK PRODUCT OR SERVICE, OR DAMAGES RESULTING FROM USE OF OR RELIANCE ON THE INFORMATION PROVIDED IN THIS GUIDE, EVEN IF CENTURYLINK OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and other information used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Many of the CenturyLink products and services identified in this guide are provided with, and subject to, written software licenses and limited warranties. Those licenses and warranties provide the purchasers of those products with certain rights. Nothing in this guide shall be deemed to expand, alter, or modify any warranty or license or any other agreement provided by CenturyLink with any CenturyLink product, or to create any new or additional warranties or licenses.
Preface

Introduction
This guide explains configuring Versa FlexVNF Advanced Software-Defined WAN (SD-WAN) solution through Versa Director, version 16.1R2.

Audience
This document is for experienced network administrators and system administrators who are well-versed with virtualization concepts, technologies, and setup hybrid cloud.

The efficiency and agility gains of cloud computing have redefined what digital transformation really means. As your trusted advisor with design, implementation, and support expertise; CenturyLink can help you drive your transformation. With expansive connections to premier cloud service providers worldwide, and multi-cloud management tools and services, our hybrid cloud solutions give you both choice and control to drive improved governance, simplify your environment. and efficiently expand for driving new market innovation.

Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description/Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomous System (AS)</td>
<td>Collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the IANA.</td>
</tr>
<tr>
<td>BFD</td>
<td>Bidirectional Forwarding Detection</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>CMS</td>
<td>Cloud Management System</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated Services Code Point</td>
</tr>
<tr>
<td>EBGP</td>
<td>External Border Gateway Protocol</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>FlexVNF Branch</td>
<td>Branch is the distributed routing and service node in an SD-WAN topology.</td>
</tr>
<tr>
<td><strong>FlexVNF Hub</strong></td>
<td>The FlexVNF hub is a uniquely named FlexVNF branch node, running the same FlexVNF software as a branch node, but potentially running multiple tenant organizations, additional scalable centralized services, and may run on elastic cloud and data-center based server resources. The FlexVNF hub may also act as a traffic exchange site in a distributed star topology and may also assist in hosting IPsec connectivity for sites with restrictive NAT traversal requirements.</td>
</tr>
<tr>
<td><strong>Hub</strong></td>
<td>A common connection point for devices in a network. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.</td>
</tr>
<tr>
<td><strong>LEF</strong></td>
<td>Logging and Export Function</td>
</tr>
<tr>
<td><strong>MPLS</strong></td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td><strong>NAT</strong></td>
<td>Network Address Translation</td>
</tr>
<tr>
<td><strong>NAPT</strong></td>
<td>Network Address Port Translation</td>
</tr>
<tr>
<td><strong>NLRI</strong></td>
<td>Network Layer Reachability Information</td>
</tr>
<tr>
<td><strong>Post-staging</strong></td>
<td>After the staging phase, the branch goes into the post-staging phase. During this phase, the branch is configured for communication with Versa Director.</td>
</tr>
<tr>
<td><strong>Router</strong></td>
<td>A router is a device that forwards data packets along networks. A router is connected to at least two networks and is located at gateways, the places where two or more networks connect.</td>
</tr>
<tr>
<td><strong>SD-WAN</strong></td>
<td>Software-Defined WAN</td>
</tr>
<tr>
<td><strong>Staging</strong></td>
<td>A branch goes through a staging phase. During the staging phase, the branch is delivered from a staging server to clients during its initial attachment to the network. The configuration contains a controller address, IPsec and authentication information to connect to the controller(s) hosting the site-specific SD-WAN.</td>
</tr>
<tr>
<td><strong>SD-WAN Controller</strong></td>
<td>Controller is a specially configured FlexVNF acting as the primary control node for SD-WAN routing and IPSec connectivity. Rather than creating a full mesh of IPsec IKE and security associations, the controller manages the distribution of SD-WAN topology using BGP.</td>
</tr>
<tr>
<td><strong>Switch</strong></td>
<td>A device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model.</td>
</tr>
<tr>
<td>Tenant Organizations</td>
<td>Tenant organizations are logical containers that enable grouping and partitioning between enterprise organizations (for example, HR, Finance) or customers (for example, Coca Cola, Pepsi). One or more parent organizations are created (for example, Service Provider), along with tenant organizations that are be defined within SD-WAN controllers, hubs and branch nodes.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>TTL</td>
<td>Time To Live what</td>
</tr>
<tr>
<td>VCSN</td>
<td>Versa Control and Service Node</td>
</tr>
<tr>
<td>VNF</td>
<td>Virtual Network Function</td>
</tr>
<tr>
<td>VNI</td>
<td>Virtual Network Interface</td>
</tr>
<tr>
<td>VPN</td>
<td>A virtual private network (VPN) is a technology that creates an encrypted connection over a less secure network. The benefit of using a VPN is that it ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it.</td>
</tr>
<tr>
<td>VRRP</td>
<td>Virtual Router Redundancy Protocol</td>
</tr>
<tr>
<td>VXLAN</td>
<td>Virtual Extensible LAN</td>
</tr>
<tr>
<td>Versa Director</td>
<td>VNF Manager for all controllers, SD-WAN hubs, and branch nodes. Versa Director is provisioned at one or more data centers with connectivity to management and control networks for the SD-WAN.</td>
</tr>
<tr>
<td>Versa Analytics</td>
<td>The Versa Analytics node provides a pre-integrated solution to a full operational visibility into the SD-WAN topology. The Analytics node gathers IPFIX data from the controller, hub, and branch sites and archives and displays this data in readily accessible formats.</td>
</tr>
</tbody>
</table>
SD-WAN Overview

Versa’s Software-Defined WAN (SD-WAN) solution is for service providers and enterprises. The implementation design combines Versa SD-WAN Branch (FlexVNF), Versa Director, and Versa Analytics software to deliver managed service capabilities.

The SD-WAN solution topology:

- **Portal (Director & Analytics)**
  - Realtime visibility to network status and performance
  - Analytics of historical traffic and events
  - Configuration Management

- **Controllers**
  - Encrypted tunnels from Appliances to Controllers
  - Controllers distribute configuration updates
  - Appliances send alarms and utilization data
  - Controllers distribute routing information
  - Controllers provide in-band management access

- ** Appliances**
  - All customer traffic flows directly between Appliances
  - LAN Routing can be Static, BGP, BGP+BFD or OSPF
  - Customer monitoring via SNMP available

The components in the network topology are explained in the following topics.

### Portal (Director & Analytics)

Versa Director is the Virtual Networks Function (VNF) manager that manages a set of FlexVNF software instances running on general purpose servers. Versa Director provides a single pane for provisioning, configuration, and management of FlexVNFs irrespective of:

- The functions provided by the FlexVNFs that can be intelligent transport or a combination of intelligent transport and other layer 4 through layer 7 network services.
- The location of the FlexVNF that can be branch-site, hub-site, or a cloud service provider.

Versa Director performs these functions:

- Responsible for the life-cycle management of the FlexVNFs.
- Centralized configuration and management of the SD-WAN controllers, branch-sites, and hub-sites.
• Supports generalized templates. A group of branch-sites having similar configuration can be bunched together and a template could be associated with this branch-group. Versa Director allows a provider to build a template, which can accommodate branch-specific arguments for variables within the template. LAN-side subnets, DHCP pools, access policy rules, and policy based forwarding rules are a few examples configurations that can be parameterized.

• Deployed as an active-standby pair for redundancy.

SD-WAN Controller

Versa SD-WAN controller plays a role in the solution and serves as a primary attachment point to the virtual private network (VPN). The SD-WAN controller provides a central control-plane entry point for zero-touch deployment of branches. The controller authenticates the branch FlexVNF instances by using PKI certificates as part of an IKE exchange. The secure channel established by using IKE, provides a transport-channel between a branch node and the SD-WAN controller for transport of routes, policy, and configuration. A single SD-WAN controller can serve as the attachment point for VPNs belonging to several different customers. The SD-WAN controllers can be deployed in a cluster for redundancy and scale.

Additionally, each individual SD-WAN controller supports intra-FlexVNF high availability.

SD-WAN Appliances

FlexVNFs are service appliances that can exist at branch-sites and hub-sites.

A Versa FlexVNF can be deployed in either of the high availability (HA) modes:

• Inter-VNF redundancy
• Intra-VNF redundancy

In both cases, the service state is replicated from the active to standby component.

A branch FlexVNF can be used for providing intelligent secure connectivity and multiple network services. Some FlexVNF connectivity features:

• Secured connectivity
• Intelligent load-sharing of traffic over various access circuits based on factors such as:
  o Company policy
  o Any field of the received packet
  o SLA requirements of layer 3 layer 7 applications
  o Result of SLA monitoring of multiple paths between various branches
  o Network state
  o User identity
- Geographical location
- Time of the day
  - Centralized configuration, management, and policy enforcement
  - Generalized templates
  - Multiple layer 3 protocols:
    - Multiprotocol BGP
    - OSPF
    - Static
    - VRRP
  - Hierarchical QoS, including adaptive shaping
  - High availability

Some FlexVNF network services:
  - Direct internet access
  - Avoids sprawl of appliances with support for multiple services:
    - Carrier grade NAT (CGNAT)
    - Stateful and Next Gen firewall
    - URL filtering
    - DDoS
    - File blocking
    - Antivirus* (coming in 2019)
    - Intrusion prevention system
  - Support for high availability with stateful replication

**SD-WAN Analytics**

Versa Analytics (VAN) is a big data solution that analyzes logs, events, and provides powerful reports, analytics as well as feedback loop capabilities. FlexVNF at various branch-sites continuously provides monitoring data relating to link, network-path, and services to the Versa Analytics server. All this data can be used for dynamic application-based traffic steering, capacity planning, and security forensics.

For SD-WAN, the Versa Analytics supports historical and realtime data reporting for:
  - Application use based on total sessions, volume, bandwidth
  - Application performance based on latency, jitter, packet loss
  - Performance of various paths between any two branches
• Use of the different access circuit of branches
Versa Director UI Overview

Versa Director lets you orchestrate your network functions using the web-based Versa Director network management interface. The web interface offers a tile view or a tabular view of the different network elements, providing granularity as you navigate the elements. Versa Director has two similar user interfaces, based on the view:

Director view
Configure and manage Versa Director at the global level. Typically, the configuration applies to the templates that are deployed across organizations (tenants) and appliances.

Appliance view
Configure and manage specific Versa FlexVNF instances. The configuration applies to the selected FlexVNF appliance and the associated tenant(s).

Director view
Director view menu tabs:

- Monitor—the Director view offers real-time system summary of Versa Director with multiple status and resource information.

![ Versa Director UI Overview](image)

Configurations
Templates. This tab has the following menus:

- Device templates—configure staging and post staging templates.
- Service templates—add service templates.
- Common template—configure common templates. A common template gets created automatically for each organization with template name <organization-name>-data store. Any objects like zones, custom applications defined in the common template can be referred from service and device templates associated with the organization.
Configurations

Devices menus:
- Devices—add devices.
- Device Groups—configure device groups.
- Device Bind Data—configure device bind data.

Configurations

Objects menus:
- WAN Networks—add WAN networks.
- DHCP Options Profiles—configure DHCP options profiles.

Workflows is used by CenturyLink when your service is configured.

Workflows menus:
- Infrastructure
- Organizations—configure customer organizations.
- Templates—configure staging and post staging templates.
- Application template—configure application templates.
- Spoke groups—configure spoke groups.
- Service chains—configure service chains.

Devices—configure devices and device groups for branches.

Administration menus:
Organizations—add organizations.
Appliances—add appliances.
Connectors—manage connectors of different types: Local, CMS, Authentication, Syslog, AQMP, and Analytics.
Director User Management—configure users, roles, and map roles to users.
Inventory—configure hardware devices and download security packages.
Appliance view

Appliance view menu tabs:

Monitor—monitor devices associated with organizations.

Configurations menus:

Networking — configure interfaces (Ethernet, tunnel, loopback, fabric, management) network zones, virtual wires, routers, policies (QoS), zones, zone protection profiles, and DHCP.

Services — configure services such as CGNAT, NextGen firewall, IPsec, SD-WAN. Create new instances of network functions, such as NextGen firewall, VPN, carrier-grade NAT (CGNAT), layer 4 load balancer, SD-WAN or routing services, provisioned virtually through the appliance.

Objects — common network functions or service instances, like address, address groups, schedules. Objects are created exclusively for an organization but are reusable across network services and child organizations. Objects are visible as optional, while configuring organizations, appliances, or services.

Others — configure profiles, logs, and certificate servers.
Administration menus:

- Organizations—manage organizations.
- Security Package—configure the security package.
- Elasticity—configure the elasticity.
- Entitlement—configure the entitlement.
- Operations—configure the operations.
- Config Snapshots—configure the configuration snapshots.
- System License—configure the system license.
Real-Time Device Monitoring

Along with Versa Analytics, Versa Director polls the devices instantly to gain insight into what is happening in realtime on the device. While Versa does have a CLI, what is exposed via Versa’s realtime monitor dashboards can be used to assist in the troubleshooting and information gathering process.

Select Versa Director > Monitor > Devices > device name to access the real-time monitor. The monitor dashboard consists of these tabs:

Devices—displays the devices associated with the provider. The dashboard displays realtime statistics with respect to the complete device.

Select the Devices tab to view the realtime health and performance of the device. Click a device to view the device details.

Summary

Click the Summary tab to view a snapshot of the device. It displays these tiles:

- CPE interfaces—displays a breakdown of interfaces and the traffic going over them in four second increments. This can be for all traffic or all SD-WAN traffic.
- SD-WAN application traffic—a filtering option to look at a specific SD-WAN traffic flow between FlexVNF’s and gives the ability to see SLA performance in realtime.
- Recent events—recent alarms received from the FlexVNF.
- Health monitor—current health of the FlexVNF looking at:
  - Is the configuration on the device in sync with the template on Director, Versa Directors reachability to the remote FlexVNF.
- Versa services status.
- Number of interfaces, up or down. Number of BGP adjacencies, up or down. IKE status, up or down.
- SD-WAN paths, up or down.
- Policy violations—any SD-WAN policy violations occurred on that device.
- Appliance activity—top applications going through the FlexVNF.
CPE Interfaces

Click the **eye** icon (next to the interface name on the CPE Interfaces screen) to view interface details.

- It provides specific information about that interface including:
- IP address—configured and public IP, if different.
- Current RX/TX bps.
- Configured RX/TX bps VRF.
SD-WAN Application Traffic (Filter)

Under SD-WAN application traffic, you can look at an aggregate of all SD-WAN traffic to a specific branch, along with looking at traffic for a specific SD-WAN policy. Traffic counters will be displayed in the same four second increments as the CPE interfaces section. If a SD-WAN policy and branch is selected, you can also see the associated SLA metrics and the thresholds that are set to deem that link out of policy.

SD-WAN Application Traffic (Metrics)

Health Monitor—current health of the FlexVNF looking at:

- Is the configuration on the device in sync with the template on Director. Versa Directors reachability to the remote FlexVNF.
- Versa services status.
- Number of interfaces, up or down. Number of BGP adjacencies, up or down. IKE status, up or down.
- SD-WAN paths, up or down.
Policy Violations—any SD-WAN policy violations occurred on that device.
Appliance Activity—top Applications going through the SD-WAN.

Recent Events—alarms
Click **Detail** to see all alarms associated with the device.

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Organization Name</th>
<th>Alarm Type</th>
<th>Handling SLA</th>
<th>Severity</th>
<th>Status Change Time</th>
<th>Alarm Text</th>
<th>Serial Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>SATLAB-Atlanta</td>
<td>SATLAB</td>
<td>sdwan-datapath sla-viol ...</td>
<td></td>
<td>major</td>
<td>Mon, Jan 14, 2019, 15:22</td>
<td>SLA violation for rule BusinessApps-Intern...</td>
<td>KSA3015251</td>
</tr>
<tr>
<td>SATLAB-Atlanta</td>
<td>SATLAB</td>
<td>sdwan-datapath sla-viol ...</td>
<td></td>
<td>major</td>
<td>Mon, Jan 14, 2019, 13:22</td>
<td>SLA violation for rule BusinessApps-SaaS-o...</td>
<td>KSA3015251</td>
</tr>
<tr>
<td>SATLAB-Atlanta</td>
<td>SATLAB</td>
<td>sdwan-datapath sla-viol ...</td>
<td></td>
<td>major</td>
<td>Mon, Jan 14, 2019, 13:22</td>
<td>SLA violation for rule BusinessApps-Intern...</td>
<td>KSA3015251</td>
</tr>
<tr>
<td>SATLAB-Atlanta</td>
<td>SATLAB</td>
<td>sdwan-datapath sla-viol ...</td>
<td></td>
<td>major</td>
<td>Mon, Jan 14, 2019, 13:22</td>
<td>SLA violation for rule BusinessApps-SaaS-o...</td>
<td>KSA3015251</td>
</tr>
<tr>
<td>SATLAB-Atlanta</td>
<td>SATLAB</td>
<td>sdwan-datapath sla-viol ...</td>
<td></td>
<td>major</td>
<td>Mon, Jan 14, 2019, 13:22</td>
<td>SLA violation for rule BusinessApps-Intern...</td>
<td>KSA3015251</td>
</tr>
<tr>
<td>SATLAB-Atlanta</td>
<td>SATLAB</td>
<td>sdwan-datapath sla-viol ...</td>
<td></td>
<td>major</td>
<td>Mon, Jan 14, 2019, 13:22</td>
<td>SLA violation for rule BusinessApps-SaaS-o...</td>
<td>KSA3015251</td>
</tr>
<tr>
<td>SATLAB-Atlanta</td>
<td>SATLAB</td>
<td>sdwan-datapath sla-viol ...</td>
<td></td>
<td>major</td>
<td>Mon, Jan 14, 2019, 13:22</td>
<td>SLA violation for rule BusinessApps-Intern...</td>
<td>KSA3015251</td>
</tr>
<tr>
<td>SATLAB-Atlanta</td>
<td>SATLAB</td>
<td>sdwan-datapath sla-viol ...</td>
<td></td>
<td>major</td>
<td>Mon, Jan 14, 2019, 13:22</td>
<td>SLA violation for rule BusinessApps-SaaS-o...</td>
<td>KSA3015251</td>
</tr>
</tbody>
</table>

The services section is a quick way to get information from a branch FlexVNF without having to login to the CLI and run a command. This is useful for operations teams to track down an issue as well as for daily operational tasks which can include looking at traffic flows or seeing the health of IPSEC tunnels. The items shown in the services section fall under two categories Services and Networking. Under Services.

**Services**

**SD-WAN**

Sites—all the SD-WAN sites this specific branch has connectivity to.
Aggregate Traffic—from the branch you are on to another branch or a controller (selected in the list), you can look at the aggregate amount of traffic that has traversed over the encrypted or plain-text tunnels.

Transport Paths—from the branch you are on to another branch or a controller, you can look at each transport and see how much data has traversed over the plain-text or encrypted tunnels.

SLA Paths—from the branch you are on to another branch or a controller, you can look at what the current SLA paths by forwarding class to see if they are up, the last time they flapped and if adaptive monitoring is active or not.
### SLA Metrics

SLA Metrics—from the branch you are on to another branch or a controller, what the current SLA metrics are between the devices.

<table>
<thead>
<tr>
<th>Path Handle</th>
<th>First Class</th>
<th>Local WAN Link</th>
<th>Remote WAN Link</th>
<th>Remote WAN Link</th>
<th>Two Way Delay</th>
<th>Two Delay Var</th>
<th>PDU Loss Rate</th>
<th>PDU Loss Rate (%)</th>
<th>PDU Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>6600264</td>
<td>fc_at</td>
<td>88</td>
<td>DIA</td>
<td>1</td>
<td>2</td>
<td>60</td>
<td>8</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6600264</td>
<td>fc_at</td>
<td>MPLS</td>
<td>MPLS</td>
<td>2</td>
<td>1</td>
<td>61</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Policies

Policies—how many times a policy has been hit and the transmit and receive bytes/packets.

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Hit Count</th>
<th>To Port Tunnel</th>
<th>To Bytes Tunnel</th>
<th>Rx Port Tunnel</th>
<th>Rx Bytes Tunnel</th>
<th>Skip Count</th>
<th>Next Hop Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalWanTunIn</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>UplinkSLA-SecApp</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>UplinkSLA-Forapp</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>PetersonRouting</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>User Disconnect</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>UserCoA</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>UserCoA-NAT46</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>UserCoA-NAT6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>LoadProfile</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>BusinessAppSecure</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>BusinessAppInternet</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>GeneralTraffic</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Up</td>
</tr>
</tbody>
</table>

### Forwarding Profiles

Forwarding Profiles—displays the forwarding profile statistics. The data includes the profile name, hit count, valid link drop count, SLA fail drop count, SLA fail forward count, and turn redirect count.

<table>
<thead>
<tr>
<th>Name</th>
<th>Hit Count</th>
<th>No Valid Link Drop Count</th>
<th>SLA Fid Drop Count</th>
<th>SLA Fid Fail Count</th>
<th>Turn Redirect Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default-LRP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LoadBalanced</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LoadBalanced_LTE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Peterson</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Peterson_LTE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Preprod-DIA-MPLS</td>
<td>155</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Preprod-MPLS-DIA</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Preprod-MPLS-DIA-LTE</td>
<td>7960</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Sessions—active number of SDWAN sessions going through the local FlexVNF.

Clicking on the eyeball, lets you search for SD-WAN sessions by supplying any one of the following criteria to search for:

- Source IP address/prefix source port
- Destination IP address/prefix destination port
- Protocol
- Predefined application predefined URL category

CGNAT

Rules—hit count, forward packet/byte count, and reverse packet/byte count for configured rules.

Pools—configured pool use.
Sessions—NAT sessions created.

Clicking on the eyeball, lets you search for CGNAT sessions by supplying any one of the following criteria to search for:

- Source IP address/prefix source port
- Destination IP address/prefix destination port
- Protocol
- Predefined application predefined URL category

NGFW

Zone Protection—displays the statistics of zone protection profiles.
DDoS—displays the DDoS policy details.

Decryption—displays decryption filter, with the following choices.

- Global—displays decryption data within the associated organization.
- Profile—displays decryption data associated with user-defined profiles.
- Policy—displays decryption data associated with user-defined policies.
- VFP—displays the hit count, forward packet/byte count, reverse packet/byte count, hit rate, and inactive session count for configured NGFW rules.
IP Filtering—display predefined or user-defined IP filtering policies.

URL Filtering—display URL filtering for:
- Profile—displays URL traffic data associated with user-defined profiles.
- Global—displays URL statistics based on the total URL traffic in an organization.
- User Category Predefined—the security administrator can apply various types of policies based on the predefined URL categories.
- User Category User-defined—the security administrator can create user-defined URL category objects for certain URLs and override predefined URL categorization values.
- URL Reputation Predefined—the security administrator can filter websites based on their predefined reputation values.
- URL Reputation User-defined—the security administrator can define URL reputation values and filter websites.

Anti-Virus—select the antivirus type, for example User Defined Profile, from the list. Select the scanning profile from the list. Select the profile type from the list. **Note:** anti-virus is not yet a supported feature by CenturyLink.
Vulnerability—select the type of vulnerability profile from the list to view details:

- **User Defined**—refers to profiles as defined by an administrator.
- **Pre Defined**—refers to system-defined profiles.
- **Sessions**—refers to vulnerable sessions during the current system up time.

Vulnerability Signature—lets the administrator see a profile/rule to identify vulnerabilities it is protecting against.
Click View to see what signature id is associated with the policy.

Security Package—displays the security package details. The details include the installation date, version, flavor, release date, update type, and installation status.
Sessions—displays NGFW session details. The details include the total number of NGFW sessions, number of sessions created, number of sessions closed, total number of NAT sessions, number of NAT sessions created, number of NAT sessions closed, and number of NAT sessions failed.

IPSEC

Overview—the IPSEC details of the local FlexVNF.

Branch to Branch—connection details from an IPSEC profile view.
IKE History—IKE history from a IPSEC profile view.

IKE Security Associations—IKE SA details from a IPSEC profile view.

IPSEC History—IPSEC History IPSEC profile view.

IPSEC Security Associations—IPSEC SA details from a IPSEC profile view.

Profile Statistics—profile statistics from the local FlexVNF based on a IPSEC profile view.
Sessions

Allows you to look at any of the session tables, SDWAN/CGNAT/NFGW or search across the session tables.

Networking

Interfaces

Displays the WAN and LAN interface statistics with respect to the organization associated with the device. The table displays the latest cumulative values at the time of polling after the interface is activated, unless a clear operation is performed. The packets per second (PPS) and bits per second (BPS) counters average out over a maximum of 30 seconds. The PPS and BPS numbers represent the observable rate of a stable flow. For example, if the traffic drops to zero at the 20th second, the value of these averages will drop to zero as well and will not use the values of the first 20 seconds to calculate the rate.

Click the eyeball to get more detail about the configured IP address, VRF, Interface status, and type.
Routes
Show either IPv4 or IPv6 routes from a specific routing-instance.

BGP
Show BGP neighbor adjacencies from a specific routing-instance.

OSPF
Show OSPF neighbor adjacencies from a specific routing-instance.

OSPFv3—show OSPFv3 neighbor adjacencies from a specific routing-instance
**Neighbor view**

**BFD**
Show BFD adjacencies from a specific routing-instance.

**DHCP**
Show DHCP active leases, lease history, and DHCP statistics.

### Active leases

### Lease history
DHCP statistics

CoS

Show the following:

QoS Policy—layer 2-4 QoS policies and their hit count, forward packets/bytes, dropped packets/bytes.

AppQoS Policy—layer 2-7 QoS policies and their hit count, forward packets/bytes, dropped packets/bytes.

Interfaces—displays the COS interface details. The details include the transmitted and received packets, number of transmitted packets per second, number of transmitted packets dropped, number of received packets per second, number of received packets dropped, number of transmitted bytes per second, and the number of bytes dropped in transmission.
Services

Centrality may change or cancel products and services or substitute similar products and services at its sole discretion without notice. ©2019 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.

Networking

VRRP
Displays details of VRRP master/slave, configured priority, VIP address.

LEF
Log Export Functionality—displays the status and statistics of configured LEF devices/groups status.

ARP
Shows ARP information for a given routing-instance.
IP-SLA

Shows state, address, routing-instance, interval, and threshold for configured IP-SLA.

System

The system tab displays the following information about the local FlexVNF:

- CPE Resources—displays the CPU, disk, and memory use for all the CPE resources.
- Firmware Summary—displays the hardware and software details.
- Device Summary—displays the device location and address.
- System Overall Status—displays the status of all the processes running on the system.
- Associate Templates—displays the name of the templates associated with the device.
- NTP Client Statistics—displays the NTP statistics.
- License—displays the license mode and status.
Monitoring Tools

As a part of the troubleshooting process, Versa Networks exposes the following toolsets via the monitor tab.

Ping
Traceroute

TCPDump—can be run from the monitor tab with regular TCPDump syntax. After TCPDump is stopped, a .pcap is downloaded to the local workstation.

SpeedTest—a device can be setup as a speedtest server and from the local FlexVNF you can run a speedtest to test the link.
Monitoring Customer Organizations

Similar to the monitoring provider organization, each customer organization monitor dashboard displays the summary and detailed information of its associated devices, along with their network health and service information.

The information includes:

- Customer organizations connecting to different core elements such as the controllers and different device types associated with the customer organization.
- Map displaying the different core elements and devices’ location. You can click on a device on the map to view the device details. Firmware summary of the associated devices.
- Multiple device health summary with functionality to view the device list with their respective status.
- Alarm summary and functionality to view the list of devices with their respective events.
- Application use of all the associated devices.
- Subscribed services view for each customer organization.
- Policy violations view for each customer organization.

Go to Monitor > Provider Organization > Customer Organization in the left panel to view its dashboard.

Tenant Summary

Go to Monitor > Provider Organization > Customer Organization > Tenant Summary.

Displays the number of core elements associated and devices associated with the customer organization. The information includes the number of:
- Controllers associated with the customer organization.
- Hubs associated with the customer organization.
- Branches associated with the customer organization.
- Non SD-WAN nodes such as routers, DHCP, NAT, and security standalone devices.
Click **Detail** on Tenant Summary to view the tenant information in a table.

Click **Back** to go back to the tile vi

**Map View**

Go to Monitor > Provider Organization > Customer Organization > Map View.
Displays OpenStreet maps to show the location of the customer organization.

- Blue displays the location of controllers.
- Green displays the location of branches.
- Orange displays the location of hubs.

**Tenant Health**

Go to Monitor > Provider Organization > Customer Organization > Tenant Health.
Displays the summary information of all the devices associated with the customer organization.

<table>
<thead>
<tr>
<th>Tenant Health</th>
<th>Up</th>
<th>Down</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Sync Status</td>
<td>15</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Reachability Status</td>
<td>15</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Service Status</td>
<td>15</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Interfaces</td>
<td>43</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>BGP Adjacencies</td>
<td>98</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>IKE Status</td>
<td>58</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Paths</td>
<td>168</td>
<td>32</td>
<td></td>
</tr>
</tbody>
</table>

- **Config Sync Status**—represents whether Versa Director’s device configuration is in sync with the device.
- **Reachability Status**—represents whether a device is reachable via ping or SSH from Versa Director.
- **Service Status**—represents whether all the device services are running in a good state.
- **Interfaces**—represents the interfaces’ status up and down count with respect to LAN and WAN interfaces.
- **BGP Adjacencies**—represents the number of BGP adjacencies in the established, connect, and idle state.
- **IKE Status**—represents the number of IKE connections in the up and down state.
- **Paths**—represents the number of paths with respect to devices associated in the up and down state.
- **Click on a row to more information.**
- Click **Back** to go to the previous screen.
- Click **Search** to search for a device.
- Click **Sort** to sort the data in the ascending or descending order.
- Click on a row for more information. The screen shows the status of each interface.

### Recent Events

Go to Monitor > Provider Organization > Customer Organization > Recent Events.

Provides the summary of all the alarms across the customer organizations and the associated devices. Alarms have multiple levels—critical, major, minor, indeterminate, and warning. All alarms are clickable, which displays the device details of the said alarms.
Click **Detail** on Recent Events to view the device information for each alarm type in a table.

- Click **Back** to go back to the tile view of this screen.
- Click **Column Filter** to select the columns to be displayed.
- Click **Alarms Filter** to filter the alarms.
Click on the device to view the history of the alarms raised or cleared.

**System Summary**

Go to Monitor > Provider Organization > Child Organization > System Summary.

Displays the summary of the number of devices, along with their hardware and software version information.

Click any row to get details of each.
Application Activity

Go to Monitor > Provider Organization > Customer Organization > Application Activity.

Provides a visual representation of the top ten used applications on the device based on these parameters:

- Sessions
- Transactions
- Total Bytes Forward
- Total Bytes Reverse

Services

Go to Monitor > Provider Organization > Customer Organization > Services.

Displays the total number of services that are turned on each device with respect to the customer organization and the associated devices.
SD-WAN Analytics

SD-WAN branches, hubs, and controllers generate various logs and events for providing topology view, availability reports, traffic visibility reports, and SLA metrics.

Click the Director context in the Versa Director Web UI and then select Analytics > Home > SD-WAN to view the SD-WAN analytic dashboard. The dashboard provides you with a tenant level view across all the sites.

- Top sites by bandwidth.
- Top access circuits by bandwidth.
- SD-WAN site map.
- SD-WAN dashboard displaying top sites by bandwidth and top access circuits.
- SD-WAN dashboard displaying SD-WAN site map.

Sites View

Select Sites to see the overall SD-WAN traffic use for this tenant.

To view the site analytics:

1. Click the Director Context and an appliance in the Versa Director Web UI and then select Analytics > Home > SD-WAN > Sites to view the dashboard.
2. Click the tenant and time range. This displays the top site use over time.
Click the **Availability** tab to view the reachability of the site from the controller.

Click the **Connections** tab to view the top 50 site-to-site connections.
Click the **HeatMap** tab to view the site availability.

- It provides activity and availability of all the sites of a tenant in a single view. The size of the block is based on the number of sessions processed by the site and color of the block is based on the percentage site availability for the specified interval.

### SD-WAN Site View

Select a tab from the table to view a SD-WAN report:

- Use
- Availability
- Access Circuits
- Users
- Applications
- Rules
- SLA Metrics
• SLA Violations
• VRF
• QoS
• APM
• MOS

To understand the content of each of these tabs:

• Click the **Usage** tab to view analytic statistics of the overall SD-WAN traffic use for the selected site.
Click the **Availability** tab to view the reachability of the site from the controller. It displays these tiles:

- Total availability and availability over time for selected site.

![Availability tile](image)

Site Controller status log.

![Site Controller status log](image)

Click the **Access Circuit** tab to view the traffic use on each of the WAN links of the selected site.

SD-WAN use over time of selected site by total bandwidth.

![Access Circuit tab](image)
Click the **Users** tab to view the top traffic sources. User name is displayed if there is an active directory or any other user identification schemes configured on the FlexVNF, else the source IP address is used to identify the user.

Get more information about users including top applications and traffic use over time by bandwidth.
Click the **Applications** tab to view top applications.

- Top applications of selected site by bandwidth.
- Any application provides more detail such as use of time per WAN link, as well as the top users of the application.
- Application use over time per WAN link by bandwidth.
Click the menu to change the type of metric displayed.

Application summary statistics.

Click the **Rules** tab to view SD-WAN traffic steering rule use and violations. SD-WAN forwarding rules are configured on the SD-WAN branches to steer traffic matching the rules to different paths based on the SLA conformance on each of the paths. These are the reports available:

- Top rules use of selected site by bandwidth.
- Top rules use over time selected site by bandwidth.
- Top rules, remote sites use of selected site by bandwidth.
- Top rules, remote sites seeing SLA violations.
Clicking on a remote site provides use of the rule over time on various paths.

Clicking on a remote site also provides FEC and traffic replication statistics per rule and WAN link.

Click the **SLA Metrics** tab to view SD-WAN per path SLA metrics. SLA monitoring is done on each of the paths of a SD-WAN branch. Metrics computed are delay, forward/reverse delay variation, forward/reverse loss, and PDU loss. You can view these paths and its associated metrics:

- Top SLA measurement of the selected site by delay.
- SLA measurement of the selected site.
Clicking on a path provides detailed SLA metrics per path and traffic class.
Click the **SLA Violations** tab to get summary reports and SLA related alarms. Provides information about aggregated reports for SD-WAN path flaps and SLA violations events per path. If SD-WAN branches are configured to generate alarms for path disconnect and path SLA violation events, they are also displayed in this page. It displays these tiles:

- Top remote sites of the selected site seeing path files based on SLA.
- Top remote sites of the selected site seeing SLA violations.
- SLA alarms of the selected site.

Click the **VRF** tab to view traffic use per VRF. The VRF reports provide a breakdown of per LAN VRF traffic sent/received on the WAN links. Traffic type indicates if it is SD-WAN or DIA (native) traffic. It displays these tiles:

- VRF use over time of selected site by bandwidth.
- VRF use of the selected site.
Click the QoS tab to view the traffic shaping reports for a WAN link. If shaping is enabled on the WAN link, bandwidth, volume sent, and volume dropped can be obtained per traffic class for each of the WAN links. This would help determine if there was oversubscription of traffic. It displays these tiles:

- Traffic volume from the select WAN link by all transmit.
- Traffic bandwidth from the selected WAN link by all bandwidth.
- Volume dropped at the selected WAN link by all drop.
Click the APM tab to view TCP application performance metrics for all TCP based traffic. You can configure Versa FlexVNFs to generate TCP metrics per application, destination network prefix and users. Source IP address is used to identify the user if there is no active directory or other schemes configured on the FlexVNF. These metrics are collected:

- Number of sessions.
- Average duration (ms).
- Aborted connections.
- Refused connections.
- SAA (Syn-Ack to Ack) (µs).
- SSA (Syn to Syn-Ack) (µs).
- Network response time (ms).
- Number of TCP packets sent.
- Number of TCP packets received.
- Percentage of forward TCP retransmits.
- Percentage of reverse TCP retransmits.

The dashboard is an overview of TCP application performance by session and by response time. You can modify these charts to show information pertaining to any of the TCP metrics that are collected. It displays these tiles:

- TCP application performance of the selected device by sessions.
- TCP applications performance over time of the selected device.
- TCP application performance details of the selected device.
For a detailed information on how an application is performing, click on an application to see the metrics on a per user basis.

Click the MOS Reports tab to view the MOS score computed by passive monitoring of customer VOIP traffic by the FlexVNFs. You can use MOS reports as a SLA metrics in traffic steering policies. These are the MOS based reports available:

- MOS scores of various WAN links of selected branch.
- Active sessions per MOS range.
- MOS Score per codec.
Sites Map

Click the Director context and an appliance in the Versa Director Web UI and then select Analytics > Home > SD-WAN > Sites Map to view the SD-WAN sites map dashboard.

Site map provides a global view of the site location, site availability and traffic activity between sites.

SD-WAN Traffic Logs

Click Analytics > Home > Logs > SD-WAN to view the generated logs. CenturyLink does not enable detailed flow logs by default and they are only enabled for troubleshooting purposes.
Security Analytics

Versa FlexVNF security solution uses Versa Analytics to provide visibility and analytics of the traffic. Policy rules are configured on Versa FlexVNF appliances to send traffic logs for specific traffic of interest to Versa Analytics.4

Versa’s security analytics has built-in dashboards for:

- Application visibility
- Web visibility
- Firewall
- Threat filtering and detection

Click Analytics > Home > Security to view the security analytics dashboard. For releases previous to 16.1R2 you have to first select the Director Context and an appliance in the Versa Director Web UI and then click Analytics > Home > Security. The dashboard provides a summary of security features in a tiled format. It displays these tiles:

- Top applications
- Top URL categories
- Top bandwidth consuming
- Applications top rules
- Top destination addresses top source addresses
- Top zone firewall actions
- Top threat types
These images show the security analytics dashboard displaying the top data for each of the security parameters:

**Application Visibility**

An application is determined based on deep packet inspection (DPI). The firewall uses IP address and port numbers for enforcing policies. This is based on users connecting to the network from a fixed location and access particular resource using specific port numbers.

Versa supports more than 2,600 applications that are automatically recognized based on application signatures. Each application is associated with attributes, like family, subfamily and tags. Versa supports user-defined applications, application groups, and dynamic application filters. The Versa analytics shows the visibility of the applications based on predefined and user-defined applications, application groups, and dynamic application filters.

To view the application analytics:

Click the Director Context and an appliance in the Versa Director Web UI and then select Analytics > Home > Security > Applications to view the dashboard. The dashboard has these tabs:
Applications
Risk
Productivity
Families
Sub Families
Click the default **Application** tab to view analytical statistics for:
Top applications by session—displays information of top applications by session.
Application use over time by bandwidth—displays information of application use over different hours of the day by bandwidth.
Application—displays the summary details of the application by session and bandwidth and other session related information like volume received (bytes) and volume transmitted (bytes) per session, average duration of each session (milliseconds), and bandwidth received and transmitted (bps) per session.
Click the **Risk** tab to view traffic use per risk level and top applications with the risk value.

Click the **Productivity** tab to view traffic use for a productivity level. Click on a productivity to see the top applications with the productivity value.

Click the **Families** tab to view traffic use per predefined application family. Click on a specific family value to see top applications for that family.
Click the **Sub Families** tab to view traffic use per predefined sub family. Click on a specific sub family value to see top applications for that sub family.

**Web Visibility**

To view the web traffic visibility:

Click the **Director Context** and an appliance in the Versa Director Web UI and then select Analytics > Home > Security > Web to view the dashboard. The dashboard has these tabs:

- URL Categories
- URL Reputation

- Click the **URL Categories** tab to view traffic use per URL category.

- URL Category Usage over time by bandwidth—displays the bandwidth use of the traffic that matches the URL category configured in the security access policy rules. Click on each legend to view individual category specific data.

- URL Category Usage—displays the detailed log for each URL category and its bandwidth use and other related details.
Click the **URL Reputation** tab to view traffic use per URL reputation.

- **URL Reputation usage over time by bandwidth**—displays the bandwidth use of the traffic that matches the URL reputation configured in the security access policy rules.
URL Reputation usage—displays the detailed log for each URL reputation and its bandwidth use and other related details.

**Firewall**

To view the firewall reports: Select Analytics > Home > Security > Firewall to view the dashboard.

For releases prior to 16.1R2 click the **Director Context** and an appliance in the Versa Director Web UI and then select Analytics > Home > Security > Firewall to view the dashboard. The dashboard has these tabs:

- Rules
- Source
- Destination
- Zone
- Forwarding class
Rule usage over time by bandwidth—displays the bandwidth use of the traffic that matches the security access policy rules.

Source usage over time by bandwidth—displays the bandwidth use of the traffic based on source location.
Destination usage over time by bandwidth—displays the bandwidth use of the traffic based on destination.

Zone usage over time by bandwidth—displays the bandwidth use of the traffic that matches the security access policy rules based on zones.
Click the **Forwarding Class** tab to view analytical statistics of the security policy rule based on the forwarding class. The data is displayed for:

- Forwarding Class usage over time by bandwidth—displays the bandwidth use of the traffic that matches the security access policy rules based on forwarding class.
- Forwarding Class usage—displays the detailed log for each forwarding class and its bandwidth use and other related details.

### Threat Monitoring

Versa’s threat monitoring solution offers security capabilities, in addition to all the security features of NextGen firewall:

- To view Threat Monitoring reports: Select Analytics > Home > Security > Threats to view the dashboard.
- For releases prior to 16.1R2 select the Director Context and an appliance in the Versa Director Web UI and then select Analytics > Home > Security > Threats to view the dashboard. The dashboard has these tabs:
  - Web Filtering
  - IP Filtering
  - Malware
• Vulnerabilities
• DDoS
• Summary

Click the Default Web tab to view reports for URL filtering using the firewall and URL filtering profiles. It displays these tiles: Top URL Categories, Top URL Reputation, Top URL Filtering Profiles, Top URL Filtering Source.

Provides detailed view of the URL filtering events matching the drill key.
Click the **IP** tab to view IP filtering report. It displays these tiles:

- Top IP Filtering Action
- Top IP Filtering Profiles
- Top Filtering Destination Reputation
- Top IP Filtering Source

![IP Filtering Report](image-url)
Provides detailed view of the IP filtering events matching the drill key.

Click the **Malware** tab to view antivirus scan reports. It displays these tiles:

- Top Anti-Virus Malwares
- Top infected Applications
- Top Victims
- Top Attackers

**Note:** CenturyLink anti-virus is not a supported feature and will be available late 2019. These charts will show “No data to display” if anti-virus is not enabled.
Click the **Vulnerabilities** tab to view IDP threat reports. It displays these tiles:

- Top Threats
- Top Signature ID
- Top Source
- Top Destination
Click the **DDOS** tab to view DOS threat reports. It displays the Top DDoS Threads information.

Click the **Summary** tab to view the threat reports. The tiles display the summary of:

- Top Appliances with Threats
• **Top Threat Types**

![Chart showing top threat types]

Services not available everywhere. CenturyLink may change or cancel products and services or substitute similar products and services at its sole discretion without notice. ©2019 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.
Configuring Hardware Devices in Inventory

To add hardware devices to be used by the branches:

1. In the Director view, go to Workflows (or Configuration) > Devices > Devices. Select an organization name from the Organization list.

2. Click the + sign to add a device.

3. Click the Basic tab:
   a. In the Name field, type a name for the device.
   b. The Global Device ID field auto-populates.
   c. From the Organization list, select an organization.
   d. From the Deployment Type list, select the type of deployment.
   e. In the Serial Number field, type the serial number for the device.
   f. From the Device Groups list, select the device groups to relate a device to or click +Device Group to create a new device group.
   g. In the Email field, type an email address for the device location.
   h. In the Phone Number field, type the location contact phone number.
4. Click the **Location Information** tab, type enter the address, latitude, and longitude.

5. Click the **Bind Data** tab, type the WAN and LAN attributes for the specific appliance. From the Service Template list, select the template that will be associated to this new appliance.

6. Click **Save**.
Configuring Branch Device Groups

To create branch device group(s), in which devices to be used are grouped together. This is useful to associate a service template with an entire group of devices in a single step.

1. In the Director view, go to Configuration > Devices > Device Groups.
2. Click the + sign to add a device group.
3. Complete the Add Device Group section:
   a. In the Name field, type a name for the group.
   b. In the Description field, type information about the device group.
   c. In the Organization field, select organization the group belongs to.
   d. Select the Enable Two Factor Auth checkbox to enable two factor authentication.
   e. Leave the Staging Template list blank.
   f. From the Post Staging Template list, select the post staging template of the device group.
g. In the Email field, type an email address for the device group.

4. Click OK.
Defining Interfaces

Configuring Ethernet Interfaces/Sub-Interfaces for LAN

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization from the left panel and a post-staging template from the dashboard. This takes you to the Appliance view.

2. In the Appliance view, go to Configuration. The Networking tab on the left panel displays the Interfaces menu.

3. Click the + sign to add an ethernet interface.
   a. In the Interface fields, enter the port and slot number.
b. Select the Sub-interfaces radio button and click the + sign to add a sub-interface.

   i. In the Unit field, type a unit number.
   ii. Fill in either the IPv4 or IPv6 section, do one of the following:
       iii. Click the IPv4 tab, select the Static Address checkbox and click to parameterize the value in IP Address/Mask. The value is derived from the bind data.
       iv. Click the IPv6 tab, select the Static Address checkbox and click to parameterize the value in IP Address/Mask. The value is derived from the bind data.
   c. Click OK.
Configuring Ethernet Interfaces/Sub-Interfaces for WAN

1. In the Director view, go to Configuration > Templates > Device Templates. Select a post-staging template from the dashboard. This takes you to the Appliance view.

2. In the Appliance view, go to Configuration. The Networking tab on the left panel displays the Interfaces menu.

3. Click the + sign to add an ethernet interface.

   a. In the Interface field, type the vni port and slot numbers.

   b. Select the Sub-interfaces radio button and click the + sign to add a sub-interface.
i. In the Unit field, type the unit number (non-zero value).

ii. In the VLAN ID field, type the VLAN ID number.

iii. Select the Static Address checkbox and click [ ] to parameterize the value in IP Address/Mask. The value is derived from the bind data.

iv. Click OK.

Configuring ESP Tunnel Interfaces

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization from the left panel and a post-staging template from the dashboard. This takes you to the Appliance view.

2. In the Appliance view, go to Configuration. The Networking tab [ ] on the left panel displays the Interfaces menu. Click the Tunnel tab.
3. Click the **sign +** to add an interface.

   ![Add Tunnel Interface](image)

   a. In the Interface field, type the port and slot numbers.
   b. From the Mode list, select **IPsec**.
c. From the Tunnel Type list, select **Point-to-multi-point IPsec tunnel**.

![Edit Sub-interface](image)

- **Static Address**
  - To add a IPv4 static address, click the + sign and click to parameterize the value in IP Address/Mask. The value is derived from bind data.
  - To add an IPv6 static address, click IPv6.
  - Click OK.

**d. In the Edit Sub-interface section:**

i. Enter the Unit number.

ii. To add a IPv4 static address, click the + sign and click to parameterize the value in IP Address/Mask. The value is derived from bind data.

iii. To add an IPv6 static address, click IPv6.

iv. Click OK.

**Configuring VXLAN Tunnel Interfaces**

The steps to configure a VXLAN tunnel interface are the same as listed for an ESP tunnel interface. The only difference is that you need to select Point-to-multi-point VXLAN tunnel as Tunnel Type on the Add Tunnel Interface screen. This configures a VXLAN tunnel interface for the branch to connect to the controller.
Configuring Pseudo Tunnel Interfaces

All SD-WAN branch appliances require pseudo tunnel virtual interface (PTVI) configuration. Each controller under an organization requires at least one PTVI interface to be defined. **Note:** This is setup by CenturyLink on initial device set up.

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization from the left panel and a post-staging template from the dashboard. This takes you to the Appliance view.

2. In the Appliance view, go to Configuration. The Networking tab on the left panel displays the Interfaces menu. Click the Tunnel tab.

3. Click the **+ sign** to add a pseudo interface.
a. Click the **Pseudo Tunnel** tab.

![Add Tunnel Interface](image)

i. In the **Name** field, type the PTVI name.

ii. From the **Parent Interface** list, select the tunnel interface. This must be the tvi interface of type p2mp-esp in the said organization.

iii. In the **Remote IP Address** field, type the remote IP address to connect to the controller. This must be the secure IP address specified for the said controller.

iv. Click the (+) sign. Repeat the above steps to add multiple PTVI interfaces.

v. Click **OK**.
Defining Networks

This involves configuring a network for the provider tenant, each customer tenant, and WAN.

Configuring Networks

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization from the left panel and a post-staging template from the dashboard. This takes you to the Appliance view.

2. In the Appliance view, go to Configuration and in the Networking tab, go to Networks.

3. Click the + sign to add a network.

   a. In Interfaces, click the + sign to add an interface.

   b. Click OK.
Defining Virtual Routers

Configuring Virtual Routing Instance for WAN Connectivity

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization from the left panel and a post-staging template from the dashboard. This takes you to the Appliance view.

2. In the Appliance view, go to Configuration and in the Networking tab, go to Virtual Routers.

3. Click the + sign to add a virtual router.

   a. In the Instance Name field, type a name for the virtual routing instance to be used for WAN connectivity.

   b. From the Instance type list, select Virtual routing instance.

   c. In the Global VRF ID field, type a unique identifier.

   Note: Under certain scenarios, direct overlay connectivity between two SD-WAN branches cannot be established. An example scenario is when both SD-WAN branches are behind NAT that uses Endpoint Dependent Mapping (a.k.a. Address and Port- Dependent Mapping). Versa SD-WAN solution forwards branch-to-branch traffic under such scenarios via a TURN relay server. For each LAN routing instance for which traffic needs to be carried over the SD-WAN overlay network using TURN relay server, a network-wide unique identifier needs to be configured on Versa SD-WAN appliances. This unique identifier is called global-vrf-ID.

   d. In the Interfaces/Networks section, click the + sign to add an interface/network.

   e. Click OK.
4. Click **Static Routing** in left menu.

![Static Routing Configuration](image)

- a. Click the **+ sign** to add a static route.

![Add Static Route](image)

- b. In the **Destination** field, type an IP address.
- c. In the **Next hop IP Address** field, type the IP address of the nearest virtual router.
- d. Click **OK**.
These steps can be repeated for any additional WAN or LAN virtual routing instances.
Configuring IPsec Profiles

IPsec profiles are configured for the provider tenant and customer tenant.

1. In the Director view, go to Configuration > Templates > Device Templates. Select a provider organization from the left panel and a post-staging template from the dashboard. This takes you to the Appliance view.
2. In the Appliance view, go to Configuration and in the Services tab, go to IPsec > VPN Profiles.
3. Click the + sign to add an IPsec profile.

   a. In the VPN Profile Name field, type a name for the VPN profile.
   b. From the VPN Type list, select the type of VPN.
   c. From the Tunnel Initiate list, select Automatic.
   d. Select the Peer IP radio button.
   e. Select either the Route Based or Policy Based radio button.
   f. From the Tunnel Routing Instance list, select a name of the tunnel routing instance.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Interface</td>
<td>Name of the tunnel interface.</td>
</tr>
</tbody>
</table>

g. Click the IKE tab.

![IKE tab](image_url)

i. From the DH Group list, select the number to be used for key exchange.

ii. From the Rekey Time list, select the time after which a new key is generated for data exchange.

iii. In the Local Auth section:

iv. From the Authentication Type list, select an identity type. *We selected psk.*

v. If psk is the authentication type, type a shared key.

vi. If Certificate is the authentication type, type the Certificate Name, CA Chain. Then from the Certificate Domain list, select the domain.

vii. From the Identity Type list, select an identity type. *We selected Email.*

viii. In the Peer Auth section:

ix. From the Authentication Type list, select an identity type. *We selected psk.* (If psk is the authentication type, type a shared key.)

x. From the Identity Type list, select an identity type. *We selected Email.*
xi. If psk is the authentication type, type a shared key.

xii. If Certificate is the authentication type, type the Certificate Name and CA Chain. Then from the Certificate Domain list, select the domain.

h. Click the IPsec tab.

i. From the Mode list, select the type of mode.

ii. From the Transform list, select the transform option; the Default is aes128-sha1.

iii. From the IPsec Rekey Time list, select the time after which a new key is generated for data exchange.

iv. Click OK.
Managing Staging and Post-Staging Templates

To perform various operations on staging/post-staging templates in the Director Context, go to the Configuration menu. Select Templates > Devices. Here, you can view, delete, clone, import, and export both staging and post-staging templates. However, you cannot create templates; instead, you must use the workflows tab.

Cloning Templates

Cloning templates enable you to reuse existing templates and associate them to other parent and child organizations.

1. In the Director view, go to Configuration > Templates > Device Templates. Select the checkbox of the template to be cloned.

2. Click the Clone icon.

   a. In the New Template Name field, the cloned template name appears.

   b. In the New Organizations section, select the same organization to clone the to the same tenant from the list. If this is a multi-tenant, you can clone the template to another tenant in the hierarchy.
c. Click OK.

**Exporting Templates**

Export an existing template to your local machine with an intent to import it later to reuse the template.

1. In the Director view, go to Configuration > Templates > Device Templates. Select the checkbox of the template to be exported.

2. Click the Export icon. The template is exported as a .cfg file on your local server. Exported files can be imported and associated with organizations.

**Importing Templates**

Templates can be imported to existing templates to copy the configuration of the imported template. The imported template and the template to which it is imported must have the same name.

1. In the Director view, go to Configuration > Templates > Device Templates. Select the checkbox of the template to which you want to import a template.

2. Rename the template to be imported. It should have the same name as the template to which it is imported.

3. Click the Import icon.
4. Click **Browse** to select the template file to be imported. The template must have the same name as the template to which it is imported.

5. Click **OK**.

**Locking and Unlocking Templates**

Users can be blocked from making configuration changes to templates by locking them. However, a locked template can be unlocked.

1. In the Director view, go to Configuration > Templates > Device Templates. Select the checkbox of the template to be locked.

2. Click the Lock icon.

3. Select the radio button for either **Lock for All Users** or **Lock for Other Users**. If you select lock for other users, the template is locked for all users except the user who is logged into the system.

4. Click **OK**.

To unlock a template, click the **Unlock** icon.

Lock and unlock are also available during service template configuration.
Configuring Service Templates

You can create service specific templates such as: NextGen Firewall, QoS, and Stateful Firewall. The main templates have a placeholder for service templates where these are referred to. A service template, is a sub template with specific configuration. A single service template can be used by multiple templates across organizations, allowing you to deploy broader networks configurations, such as firewall and QoS, while having the ability to provide more location specific templates to ease network management.

1. In the Director view, go to Configuration > Templates > Service Templates. Select an organization on the left panel for which a service template is to be created.

2. Click the + sign to add a service template.

   ![Add Service Template](image)

   a. In the Name field, type the name for the service template.

   b. From the Organization list, select the organization.

   c. From the Type list, select the type of template. When you create the service template using the Versa Director GUI with these service types, only the relevant and required Firewall and QoS configuration objects are allowed.

   d. Click OK.

To clone a template. Select a template and click the Clone icon. You can also clone, import, or export a template’s configuration.
1. Select a template and click the View icon to view the template’s CLI configuration.

![Template Configuration](image-url)
Associating Templates with Service Templates

Templates are created using the Create Template menu under Workflows. You can associate the template with a service template although you can also configure templates with a limited configuration.

1. In the Director view, go to Configuration > Templates > Device Templates. In the left panel, select an organization for which it is to be associated.

2. Click the Edit icon to associate a given template with a service template.
3. Click the **Service Templates** tab.

![Service Templates Tab](image)

- a. From the **Organization** list, select the name of the organization.
- b. From the **Override** list, select Override service template to override the provider policies defined in the service template. Or select No conflict if you wish to follow the policies in the main template or service template.
- c. Select the **Security** radio button to indicate the type of security protocol you wish to follow.
- d. In the Class of Service section, select the checkbox of the service template you want.
- e. In the General section, select the checkbox next to the name of the template.
- f. Click **OK**.
Configuring Certificates for IPsec

Certificates are used to set up a secure communication channel between a branch and controller. When a branch or controller needs to communicate with the other, it sends a request for a certificate to the certificate authority. The certificate authority issues certificates.

Configuring Staging Certificates

Certificates are issued by a certificate authority. To configure a certificate, you need to configure the server that hosts the certificate. The branch or controller that requires a certificate sends a certificate request to the server. To configure a staging certificate involves configuring a certificate server and configuring a certificate request.

Configuring Certificate Server

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization from the left navigation panel and a staging template from the dashboard. This takes you to the Appliance view.

2. In the Appliance view, go to Configuration and in the Objects & Connectors tab, go to Connectors > Certificate Manager.
3. On the Servers tab, click the + sign to configure a server.

![Add Server dialog box]

- In the **Name** field, type a name for the server.
- From the **Server Type** list, select CMP.
- In the **CA Identity** field, type a name for the certificate authority.
- In the **URL** field, type the URL of the server hosting the certificate authority.
- From the **Routing Instance** list, select the routing instance used by the branch or controller to communicate with the server.
- From the **Interface Name** list, select the interface to communicate with the server.
- In the **Retry Interval** field, type the number of seconds in which a branch or controller can retry to get the certificate.
- Click **OK**.
Configuring Certificate Request

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization from the left navigation panel and a staging template from the dashboard. This takes you to the Appliance view.

2. In the Appliance view, go to Configuration and in the Objects & Connectors tab, go to Connectors > Certificate Manager. Click the Requests tab.

3. Click the + sign to configure a request for the certificate.

a. In the Certificate Name field, type a name for the branch certificate.

b. From the Certificate Domain list, select the certificate domain.

c. In the Validity field, type the number of days for which the certificate is valid.

d. Select the Auto Renewal checkbox to renew the request automatically.

e. From the Server list, select the name of the server.

f. In the Common Name field, type the name of the certificate. This is also an identity, which needs to be configured in the Certificate Authority server. Both the names should match.
g. In the **Email ID** field, type the email ID configured in the certificate authority server for the branch or controller.

h. In the **Key Size** field, type the size of the key, the standard size is 1024 bytes.

i. In the **Key Name** field, type a name in which the key is generated.

j. Select either the **PSK** or **Certificate** radio button as the mode to authenticate the certificate request.

   i. If PSK is selected, type the User ID and Shared Key. Shared key is the password and it should be identical to the shared key of the server.

   ![Auth Info](image)

   ii. If Certificate is selected, type the Auth Certificate Name and Auth CA Chain, and from the Provider Org list, select the organization. Type the Key Name and Key Passphrase, and from the Certificate Domain list, select the values for the domain.

k. **Click OK.**

![Configuration](image)

### Configuring Post-Staging Certificates

The same certificate configured for a staging template of a branch can be used for the post-staging phase. You need to repeat the same steps listed in configuring staging certificates section. The only difference is that you need to select the post-staging template instead of the staging template for the branch.
Configuring SLA Profiles

Service level agreement (SLA) profiles are configured to define the network performance parameters to monitor the performance of access circuits and links. An SLA profile defines performance parameters, such as packet delay, packet loss, and jitter for a link. A link or circuit is selected based on the threshold values specified in the SLA profile.

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization from the left navigation panel and a template from the dashboard. This takes you to the Appliance view.

2. In the Appliance view, go to Configuration > Services > SDWAN > SLA Profiles.

3. Click the + sign to add an SLA profile.

   ![Edit SLA Profile](image)

   a. In the Name field, type a name for the SLA profile.
   b. In the Packet Delay-variation (jitter) field, type an acceptable packet delay in milliseconds.
   c. In the Circuit Transmit Utilization field, type the number of circuit transmit utilizations.
   d. In the Circuit Receive Utilization field, type the number of circuit receive utilizations.
   e. In the Maximum Packet Loss field, type the number of acceptable packet losses.
   f. In the Maximum Forward Packet Loss field, type the number of acceptable packet losses when forwarding packets.
   g. In the Maximum Reverse Packet Loss field, type the number of acceptable packet losses during packet reversal.
   h. In the Maximum Latency field, type the number for acceptable latency.
   i. In the MOS Score field, type a number for an acceptable mean opinion score for voice traffic. This monitors delay, jitter, and loss in traffic. The value can range from 0 to 5, where 5 indicates the best traffic quality and 0 is the lowest traffic quality.
j. Select the checkboxes for Low Delay Variation, Low Latency, Low Forward Packet Loss, Low Packet Loss, and/or Low Reverse Packet Loss, as applicable.
   i. These fields indicate that instead of load balancing traffic between all paths that are in SLA compliance, the best path should be chosen.
   ii. An example: if low forward packet loss is set, it means that the path with the lowest forward loss should be chosen. When low forward packet loss and low delay variation is selected then the best path is chosen in order of the least latency, the least loss, and least delay variation. In this example, select the path with the lowest latency first. If multiple paths have the same latency, then select the path with the least loss. If least delay variation is also checked, it chooses the path with the least delay variation.

k. Click OK.

### Configuring Forwarding Profiles

A forwarding profile determines the traffic path, based on real-time SLA performance of traffic. A forwarding profile defines the properties of WAN circuits to be selected for traffic. It defines the properties such as the load balancing method to use for traffic, priority of circuits, circuit type (broadband or MPLS), circuit media, and other associated attributes.

Forwarding profiles are associated with SLA profiles to determine the selection of WAN circuits in a given order of priority.

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization from the left navigation panel and a template from the dashboard. This takes you to the Appliance view.
2. In the Appliance view, go to Configuration > Services > SDWAN > Forwarding Profiles.
3. Click the **sign** to add a forwarding profile.

![Add Forwarding Profile](image)

4. Click the General tab.

   a. In the **Name** field, type a name for the forwarding profile.
   
   b. In the **Description** field, type a description for the forwarding profile.
   
   c. In the **Tags** field, type a tag for the forwarding profile.
   
   d. From the **SLA profile** list, select the name of the SLA profile to associate to.
   
   e. From the **Encryption** list, select whether the traffic sent across the SD-WAN tunnel should be encrypted or not. Choose from three modes:
      
      i. Optional—encryption should be applied or not depending on whether the WAN link used as the SD-WAN tunnel transport has encryption enabled.
      
      ii. Always—traffic should always be encrypted.
      
      iii. Never—avoid encryption if the end-to-end traffic is already encrypted (for example, secure RTP or SSL traffic).
   
   f. From the **Connection Selection Method** list, select the mode to balance traffic. The following options are available:
      
      i. High Available Bandwidth—the circuit with the highest available bandwidth must be used.
ii. Weighted Round Robin—assigns weight to the various paths, based on the available bandwidth on the corresponding access circuits. Versa periodically measures the current bandwidth consumption of each access circuit. If the circuit’s uplink and downlink bandwidth are configured, Versa determines the available bandwidth on each circuit and assigns weights. For example, if WAN1 is a 10 Mbps link, and is currently reporting 8 Mbps use, it has 2 Mbps of remaining capacity. If WAN2 is a 5 Mbps link and is currently reporting 1 Mbps use, it has 4 Mbps remaining capacity. WAN1 and WAN2 will be allocated load balancing credits in the ratio 2:4 (that is, 1:2). Each session consumes one credit.

iii. Recompute Timer—switches time between circuits when the current circuit does not meet the SLA threshold values. The SLA compliance state of all paths for a forwarding profile is re-evaluated after every recompute interval.

g. From the **SLA Violation Action** list, select the action to be taken if the traffic does not meet the SLA thresholds.

h. From the **Load Balancing Option** list, select the required load balancing.

i. To enable packet replication, select the **Enable** checkbox.

j. In the **Replication factor** field, type the number of copies of data for replication.

k. From the **Start When** list, select when to replicate automatically if traffic does not meet the SLA thresholds.

l. To stop replication automatically, select the **Stop When** checkbox.

m. In the **Circuit Utilization** field, type a percentage value to stop replication automatically when circuit use exceeds the specified threshold.

n. To apply switching during traffic flow, select the **Evaluate Continuously** checkbox. Gradual migration is enabled, and flows are moved off non-compliant paths over a few re-computation cycles, instead of all at once.

i. When evaluate continuously is enabled, but gradual migration is not enabled, all traffic is moved off the non-compliant path. Traffic now causes the second path to go out of compliance and return to the first path. To avoid this, gradual migration can be enabled. This allows traffic flows to move gradually from the original path to the new path, over multiple forwarding re-computation cycles. Flows that move, reduce the load on the original path, mitigating the SLA degradation, so other flows do not have to move. Flows that do move to a new path are retained on that path as long as it is SLA compliant.

o. To forward out-of-order packets in the original order, select the **Reorder** checkbox.

p. For traffic to be sent to a TURN relay (selected as per the assigned circuit priorities), select the **TURN Redirection** checkbox.

ii. Normally, if a remote site is behind the endpoint NAT on a transport path, it is taken out of rotation in favor of other paths that are not behind the endpoint NAT. However, this prevents access circuits that are behind the endpoint NAT from being used. By enabling TURN redirection, an access circuit that is behind the endpoint NAT can still be used to send traffic to a TURN relay that services traffic from that access circuit.

q. To enable symmetric forwarding of traffic, select the **Enable Symmetric Forwarding** checkbox.
i. This dictates how the device steers reverse direction traffic, i.e. traffic returning from the destination branch to origin branch. By default, the return traffic is forwarded symmetrically, on the same path on which the traffic was received. However, for applications where it is beneficial to independently choose the best path in either direction, symmetric forwarding may be turned off.

5. Click the **Circuit Priorities** tab to configure circuit properties for local and remote clients.

![Circuit Priorities Tab](image)

6. Click the **+** sign to define the circuit properties.
   a. Click the **Circuit Names** tab.
i. Click the + sign to select a circuit name for local and remote clients from the list in each section.

![Add Circuit Priorities](image)

b. Click the **Circuit Types** tab.

   i. Click the + sign to select a circuit type for local and remote clients from the list in each section.

   ![Add Circuit Priorities](image)

   ![Add Circuit Priorities](image)

c. Click the **Circuit Media** tab.
d. Click the + sign to select a circuit media for local and remote clients from the list in each section.

![Add Circuit Priorities](image)

e. Click the **Avoid Connections** tab to configure the links that should not be picked. These are defined for the local and remote client links.

![Add Forwarding Profile](image)
f. Click the **FEC** tab to configure Forward Error Correction (FEC) for the forwarding profile.

![Add Forwarding Profile](image)

i. To enable FEC select the **Enable** checkbox.

ii. Stop duplication of the FEC parity packet by deselecting the **Duplicate FEC Packet** checkbox.

iii. In the **Maximum FEC Packet Size** field, type the maximum packet size for the FEC parity packet.

iv. From the **Start When** list, select the SLA Violation. This enables FEC automatically when the traffic does not meet the SLA thresholds.

v. Select the **Stop When** checkbox and in the **Configure Circuit Utilization** field, type a percent to stop FEC automatically when the circuit use exceeds a specified threshold.

vi. Stop packet recovery after receiving FEC packet by deselecting the **Recovery** checkbox.

vii. Stop the reorder of out-of-order packets and forwarding them in the original order by deselecting the **Preserve Order** checkbox.
g. Click the Advanced Settings tab to define smoothing/dampening/migration values.

![Add Forwarding Profile](image)

i. Enable SLA smoothing options:
   - Select the checkbox if you want the system to average the metrics over the smoothing interval instead of the recompute interval. If the path is in the SLA compliant state, the metrics is averaged over the recompute interval.
   - Do not select the checkbox if you want the SLA compliance of a path checked for every recompute interval.

ii. In the SLA smoothening interval (sec) field, type the number of seconds to enable SLA smoothing.
   - Smoothing involves taking a historical perspective before moving the traffic from the non-compliant data path to the compliant data path.
   - The smoothing interval must be larger than the recompute interval. This is especially useful for loss based SLAs, where loss measurement accuracy depends on the amount of packet samples. For example, if the recompute interval is 10 seconds and the smoothing interval is 100 seconds:
     - If the path is SLA compliant, the SLA metrics is averaged over the last 10 seconds (last recompute interval) to determine SLA compliance.
     - If path is SLA non-compliant, the metrics from the last 100 seconds is used to determine SLA compliance. Thus, smoothing helps to react slower to improvements in the network conditions. The default value for SLA smoothening interval is 120 seconds.

iii. Enable SLA violation dampening options:
   - Select the checkbox if you want the recompute interval value associated with the dampening interval value.
Do not select the checkbox if you want the SLA compliance of a path checked for every recompute interval. When a path becomes SLA non-compliant, the system keeps the path as non-compliant for the dampening interval. After that value is reached, the system checks the path again for SLA compliance. This prevents the frequent change of traffic from non-compliant to compliant paths, every recompute interval. For example:

- If the recompute interval is 10 seconds, the path can oscillate between compliant and non-compliant state, every 10 seconds.
- If the dampening interval is set to 60 seconds, traffic may move to non-compliant state in 10 seconds and move back to compliant state only after 60 seconds.

h. Click OK.

**Configuring Application Detection**

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization from the left navigation panel and a template from the dashboard. This takes you to the Appliance view.

2. In the Appliance view, go to Configuration > Services > SDWAN > Application Detection.

3. Click **OK** to define the settings.

   ![Edit Application Detection](image)

   a. In the Application Dynamic Detection section, select the **Enable** radio button to dynamically switch between links when an application is detected during traffic flow.

   b. In the Application Cache section, select the **Enable** radio button to save the destination IP address and port of an application when it is accessed for the first time. This enables a faster connection and a quicker response to the application.

   c. In the URL Category Cache section, select the **Enable** radio button to cache IP addresses associated with URL categories. It is disabled by default.
d. Click OK.

**Configuring SD-WAN Policies**

You can configure policies to select traffic based on matching criteria, such as the traffic source address, destination address, source zone, specific IP packet header information, and apply specific forwarding profiles to the selected traffic.

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization from the left navigation panel and a template from the dashboard. This takes you to the Appliance view.
2. In the Appliance view, go to Configuration > Services > SDWAN > Policies.
3. Click the + sign to add a policy.

4. Click OK.

**Did you know?** CenturyLink creates a default policy when service starts. It is unnecessary to create an additional policy to be able to add rules.

**Configuring Rules**

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization from the left panel and a template from the dashboard. This takes you to the Appliance view.
2. In the Appliance view, go to Configuration > Services > SDWAN > Policies > Rules.
3. Click the + sign to add a rule.

4. To configure source and/or destination addresses as the matching criteria to capture traffic, click the Source/Destination tab.

   a. In the Source Address section, click the + sign to select a source address. Source address refers to the originating address of incoming traffic. Source addresses can be classified by originating country, region, or IP address.

   b. To block traffic to the selected source addresses in the section, select the Source Address Negate checkbox.
c. In the Destination Address section, click the + sign to select a destination IP address. Destination address refers to the destination address of the traffic. Addresses are classified by countries, regions, or IP addresses. To add a new address, click + New Address.

```
Add Address
```

- In the Name field, type a name assigned to the address.
- From the Type list, select the type of address.
- Click OK.

d. To group addresses, click + New Address Group.

```
Add Address Group
```

- In Address section, click the + sign to select an address to be placed in the group.
• To block traffic to the selected destination addresses in this section, select the Destination Address Negate checkbox.

ii. In the Source Zone section, select the source zone of the traffic. Zone refers to a set of interfaces. Click the + sign to select a source zone from the list.

e. To add a zone, click + New Zone.

i. In the Name field, type a name for the zone.

ii. From the Zone Protection Profile list, select the protection profile of the zone.

iii. From the Log Profile list, select the log profile of the zone.

iv. Select the necessary radio buttons for Interface and Networks, Routing Instances, and Organizations, then click the + sign to add those entities.

v. In the Source Site ID section, select the source site IDs.

vi. In the Destination Site ID section, select the destination site IDs.

vii. Click OK.
f. To configure matching criteria based on the IP packet header information, click the **Headers/Schedule** tab.

![Edit Rules](image)

i. From the **IP Version** list, select the IP address version.

ii. From the **IP Flags** list, select whether routers can fragment the data packets.

iii. In the **DSCP** field, type the differentiated services code point, which is the value or cost of the policy.

iv. From the **Condition** list, select which match condition to use in the packet's header.

v. In the **Value** field, type the condition value.

vi. From the **Schedules** list, select the frequency of the action to be taken.

vii. To create a new schedule, click **+ New Schedule**.

- In the Services section, select the services to be allowed or blocked. Click the **+ sign** to select a service from the list. The list includes predefined and user-defined services. Service is defined by the destination address and port.
To select traffic based on applications and URLs, click the Applications/URL tab.

- Select the checkbox next to the applications and application groups on which to apply this rule.

To add an application, click New Application.

- In the Name field, type a name for the application.
- In the Host Pattern field, type a host pattern for the application.
iii. In the **Application Timeout** field, type a time after which the application must time out.

iv. Continue filling out the sections Family, Sub-Family, Risk, Productivity, Security, SDWAN, and General columns.

v. Click **OK**.

i. To add an application group, click **+ New Group**.

![Add Application Group](image)

i. In Applications section, click the **+ sign** to select an application filter. Or you can add an application filter by clicking **+ Application Filter**.
ii. Click OK.

![Add Application Filter]

- In the URL Categories section, click the + sign to select a URL category from the list. Or you can add a URL category by clicking + New URL Category.

![Add URL Category]

i. In the Name field, type a name for the URL category.
ii. In the **Confidence** field, type a confidence for the URL match, which will be a tie-breaker in cases where the URL matches the patterns/strings of multiple URL categories.

iii. Click the **URL Patterns** tab

iv. In the **Pattern** field, type a pattern of the URL.

v. From the **Reputation** list, select a value to be assigned to the reputation.

vi. Click the **URL Strings** tab.

vii. In the **String** field, type the URL strings to apply the rule upon.

viii. From the **Reputation** list, select a value to be assigned to the reputation.

ix. Click the + sign to add the data.

k. To select the forwarding profile, logging profile, and monitor parameters, click the **Enforce** tab.

i. From the **Action** list, select whether to allow or deny the flow of traffic:

ii. From the **Forwarding Profile** list, select the forwarding profile to be applied on the traffic.

iii. In the **Nexthop IP address** field, type the IP address of the next hop.

iv. From the **Routing Instance** field, select the routing instance to be used.
v. Select the **Enable Symmetric Forwarding of Return Traffic** checkbox if you want to enable symmetric forwarding of return traffic. The reverse flow of traffic must leave through the forward ingress interface but would go through a route lookup. You can configure a SD-WAN or PBF policy rule such that the reverse direction traffic be subjected to stateful L3 return.

vi. Select the **Enable Symmetric L2** checkbox to forward return traffic. The reverse flow of traffic must leave through the forward ingress interface and is sent to the same mac address from which the forward direction traffic is received, without doing a route lookup. You can configure a SD-WAN or PBF policy rule such that the reverse direction traffic be subjected to stateful L2 return.

vii. From the **LEF Profile** list, select the type of profile to be used as the LEF profile.

viii. Select the **Default Profile** checkbox to set this profile as the default profile.

ix. In the **Address** field, type the ping IP address of the routing instance.

x. From the **Action** list, select the monitoring action to be taken for your traffic.
   - **Wait-Recover**—traffic is dropped until the nexthop recovers.
   - **Failover**—traffic is routed, where SD-WAN traffic policy is not implemented. L3 destination IP is lookup based.
   - **Next-Rule**—the other rules are evaluated until a match is found. If no match is found, traffic is routed.

xi. In the **Threshold (Events)** list, type the number of successive ICMP ping failures after which the nexthop is considered down.

xii. From the **Routing Instance** list, select the routing instance to be used.

xiii. In the **Interval (sec)** field, type the frequency in seconds at which you want to ping traffic.

xiv. Click **OK**.
Configuring Adaptive Shaping

Adaptive shaping refers to the process when a hub dynamically sends a new traffic transmission rate to the branches that are connected to the hub. Based on the new transmission rate, the branches adjust the traffic volume sent to the hub. This is done because the hub has a WAN link with a downlink limit (for example, 100 MB). When the branches connected to the hub start sending traffic to the hub that exceeds the downlink limit of the hub WAN link, the hub can slow down or the ISP will drop the traffic before it even reaches the hub. When this happens, the hub dynamically advertises a different transmission rate to the branches for them to adjust their transmission rate. Adaptive shaping helps in scaling the number of branches connected to the hub without manually changing the traffic transmission rate of each branch.

Adaptive shaping configuration involves: configuring the hub and associating interfaces with branches (covered in QoS – Class of Service). You must specify an input rate range for egress traffic on a WAN interface of a branch, which is advertised to other branches in the network. Adaptive shaping configuration on the hub should be considered as a secondary solution.

Configuring the Hub

1. In the Director view, go to Configuration > Devices > Devices. Select the organization from the left navigation panel and a hub from the list of devices shown in the dashboard. This takes you to the Appliance view.

2. In the Appliance view, go to Configuration and in the Services tab, go to SDWAN > System > Adaptive Shaping.

3. Click to configure the shaping settings.

   a. Select the Enable checkbox to activate the setting.
   b. In the High Threshold field, type a percent for the upper bandwidth limit. When the total traffic bandwidth transmitted to the hub is beyond this value, the hub instructs the branches to reduce the traffic rate to the hub.
c. In the **Low Threshold** field, type a percent for the lower bandwidth limit. When the total traffic bandwidth transmitted to the hub is below this value, the hub instructs the branches to increase the traffic rate to the hub.

d. In the **Percentage Change** field, type a percent increment or decrement in the bandwidth rate, which is advertised to the branches until the transmission is below or above the high or low threshold value.

e. In the **Damping Count** field, type the number of times the hub checks the bandwidth transmitted by the branches connected to the hub.

f. In the **Poll Interval** field, type the time interval for when the checks are made. The checks are made for a total duration of Damping Count * Poll Interval. If the total traffic transmitted by the branches exceeds the uplink limit of the hub link, the hub advertises a shaping rate (bandwidth transmission rate) to the branches.

g. **Click OK.**

The branches respond to the adaptive shaping requests from the hub, only if class of service is configured on its interfaces. Refer to the chapter on class of service for associating interfaces.
Configuring CGNAT

CGNAT is a NAT employed on a large scale. It translates multiple private IPv4 addresses to a limited number public IPv4 addresses using Network Address and Port Translation (NAPT) methods. In CGNAT, only port translation of source address is required for packets communicating from the network to outside. Port translation of destination address is not implemented.

CGNAT can replace NAT devices in enterprise networks. Using CGNAT, you can deliver seamless IPv4 connectivity even while using limited public addresses. You can define private IPv4 address in your network and use CGNAT to manage address translation to the public IPv4 addresses.

To configure CGNAT, define the address pool that must be translated followed by the translation criteria for address translation. This is done by defining a pool and the rules to be applied on the pool. Address translation is of two types: NAT (network address translation) and NAPT (network address port translation).

Configuring Pools

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization in the left navigation panel and a template from the dashboard.
2. In the Appliance view, go to Configuration and in the Services tab, select CGNAT.
3. Click the + sign to add a pool.

   ![Add CGNAT Pool](image)

   a. In the Name field, type a name for the pool.
   b. In the ICMP field, type the number of seconds for the ICMP mapping timeout.
   c. In the TCP field, type the number of seconds for the TCP mapping timeout.
d. In the **UDP** field, type the number of seconds for the UDP mapping timeout.

e. To define the IP addresses for NAT, click the **IP Address** tab.

![IP Address/Range window](image)

i. Select the **IP Address/Range** radio button.

ii. Click the **+** sign to add the IP addresses or IP address range.

iii. Click ![_parameterize_icon] to parameterize the field with a value from bind data.

iv. Select the **Egress Network** radio button.

v. Click ![_parameterize_icon] to parameterize the field with a value from bind data.

vi. Select the **Egress Interface** radio button.

vii. Click ![_parameterize_icon] to parameterize the field with a value from bind data.

viii. In the **Range Name** field, type a name for the IP address range.

ix. In the **Low** field, type the lowest IP address.

x. In the **High** field, type the highest IP address.

xi. From the **Address Allocation Scheme** list, select the scheme that allocates one port from each address in a range.

xii. From the **Routing Instance** list, select the routing instance to be used.
xiii. From the **Provider Org** list, select the provider organization of the CGNAT pool.

f. Click the **Port** tab for NAPT.

![Add CGNAT Pool](image)

i. Select the **Destination port** checkbox if you want the destination port to be used for NAT.

ii. In the **Low Port** field, type the lowest port number of the range.

iii. In the **High Port** field, type the highest port number of the range.

iv. Select the **Source Port** checkbox if you want the source port to be used for NAT.

v. From the **Allocation Scheme** list, select the scheme to be used for source port allocation.

vi. In the **Low Port** field, type the lowest port number of the range. This is applicable when the allocate ports from range is selected as the allocation scheme.

vii. In the **High Port** field, type the highest port number of the range. This is applicable when the allocate ports from range is selected as the allocation scheme.

viii. Select the **Allocate IP/port randomly** checkbox to enable the mode of allocating source ports.

ix. Select the **Preserve source port range** checkbox to enable the mode allocates source ports.

x. Select the **Preserve source port parity** checkbox to enable the mode of allocating source ports.

xi. Select the **Port block allocation** checkbox to enable the mode of allocating source ports.
xii. In the **Block Timeout** field, type the time to wait to get a port before breaking the connection. This is applicable when port block allocation checkbox is selected.

xiii. In the **Block Size** field, type the size of the port block, which must be divisible by two. This is applicable when the port block allocation checkbox is selected.

xiv. In the **Max Block per user** field, type the maximum block size allocated per user. This is applicable when the port block allocation checkbox is selected.

xv. Click **OK**.

---

### Configuring Rules

1. In the Director view, go to Configuration > Templates > Device Templates. Select an organization in the left navigation panel and a template from the dashboard.

2. In the Appliance view, go to Configuration and in the Services tab, select CGNAT. Click the Rules tab.

3. Click the + sign to configure a rule.

   a. In the **Name** field, type the name of the rule.

   b. In the **Precedence** field, type the priority of the rule. You can configure multiple rules and assign each a priority. The increasing order of priority is 1 > 2 > 3. Rules with a higher priority take precedence over the ones with a lower priority.
4. To configure the criteria to select traffic for translation, click the **Match** tab.

![Add CGNAT Rule](image)

a. In the **Source Zones** section, select the checkbox of the packets you wish to match from these zones only.

b. In the source **IP Address/Mask** section, configure ranges by clicking the + sign, then type a name, the low range, and high range.

c. From the **Routing Instance** list, select the routing instance of the incoming packet.

d. In the source **IP Address Range** section, configure ranges by clicking the + sign, then type a name, the low range, and high range.

e. In the **Destination Zones** section, select the checkbox of the packets you wish to match from these zones only.

f. In the destination **IP Address/Mask** section, configure ranges by clicking the + sign, then type a name, the low range, and high range.

g. In the **Low Port** and **High Port** fields, type a low and high number.

h. In the destination **IP Address Range** section, configure ranges by clicking the + sign, then type a name, the low range, and high range.
2. Click the **Action** tab to define the action you’ll take on the traffic that meets the matching criteria.

   ![Add CGNAT Rule](image)

   a. Select the **Disable Translation** checkbox to disable translation.
   
   b. From the **NAT Mode** list, select a mode for the NAT. This is predefined.
   
   c. From the **Source Pool** list, select the source port associated with the translation mode.
   
   d. From the **Destination Pool** list, select the destination port associated with the translation mode.
   
   e. From the **LEF Profile** list, select the logging and export function profile to be applied for logging.
   
   f. Select the **Endpoint Independent Mapping** checkbox to enable endpoint independent mapping. NAT uses endpoint mapping to perform translation for the duration of the session.
   
   g. Select the **Endpoint Independent Filter** checkbox to enable the endpoint independent filter. This checks only the destination IP and destination port of an inbound packet sent by an External endpoint to decide whether to pass the packet or not.
   
   h. Select the **Address Pooling Paired** checkbox to enable address pooling paired. This require all sessions associated with one internal IP address be mapped to the same external IP address for the duration of a session.
   
   i. Click **OK**.
Defining Class of Service

Versa’s Quality of Service (QoS) that is configured in Versa Director’s Class of Service comprises network performance management technologies that ensure its capability to run traffic and high-priority applications in a limited network capacity. It also guarantees a predetermined level of performance with limited network resources. QoS is the ability to provide differentiated priority for different applications and network traffic. Versa uses separate handling and capacity allocation for specific network traffic flows, which enables the network administrator to prioritize the traffic handling and determine the bandwidth for the traffic. QoS can help predict network performance and ensure effective bandwidth use.

You can use Versa QoS solutions for prioritizing and adjusting network traffic. You can define the order for packet handling and allocate bandwidth per your requirements. This allows you to ensure quality performance for the selected traffic, applications, and users. The service quality factors related to QoS implementation are:

- Bandwidth—the maximum rate of transfer
- Throughput—the actual rate of transfer
- Latency—delay
- Jitter—the variance in latency

Versa QoS can define and control these service quality factors for realtime and high bandwidth traffic, such as VoIP, video on demand, and voice conferencing, which are prone to jitter and latency.

Using Versa QoS allows you to:

- Prioritize network and application traffic. You can limit traffic for non-essential activities or ensure high priority for essential traffic.
- Provide equal sharing of bandwidth for different classes, subnets, users, or classes in a network.
- Allocate bandwidth to internal or external traffic, apply QoS for upload or download traffic (both included) or only to upload traffic or only to download traffic.
- Ensure low latency for network traffic involved in revenue generation within enterprise environments. Implement application traffic profiling for ensuring bandwidth use.

Configuring RW (Rewrite) Tools

Versa QoS supports rewrite rules, which set the appropriate class of service bits in the outgoing packet/stream. You can use a classifier to mark packets/stream that arrive on the input interface and then use rewrite rules to mark packets/stream again while leaving the interface. Rewrite rules apply the packet loss priority and forwarding class information to determine the Differentiated Services Code Point (DSCP) on outbound packets/stream.

The rewrite rules configuration workflow.

1. In the Director view, go to Configuration > Devices > Devices. Select an organization in the left navigation panel and a branch or hub or controller from the dashboard.
2. In the Appliance view, go to Configuration and in the Networking tab, go to Class of Service > RW Rules.

3. Click the + sign to add the required RW Rule.

   ![Add RW Rule](image)

   a. From the **Type** list, select the type of rewrite table

   b. To delete a Forwarding Class, select the checkbox next to its name and click (-).

   c. To define the Forwarding Class, select the + sign to open the add configuration screen.

   ![Add Configuration](image)

   d. In the **Loss Priority** section, select low if the data packets are less likely to drop vs. high loss priority. Or select high if the data packets are more likely to drop vs. low loss priority.
e. From the **Code Point** section, select the matching code point from the list.
f. Click OK.

4. Click OK.

---

**Add QoS Profile**

Create a QoS profile to define the ingress policing and forwarding class as well as loss priority that will define the priority behavior of the traffic that is matched to the profile. CenturyLink supports a default configuration of 7 traffic classes: ***

<table>
<thead>
<tr>
<th>Expedited Forwarding</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ExpiditedForwarding-1</td>
<td></td>
</tr>
<tr>
<td>ExpiditedForwarding-2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assured Forwarding</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AssuredForwarding-1</td>
<td></td>
</tr>
<tr>
<td>AssuredForwarding-2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Best Effort</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BestEffort-1</td>
<td></td>
</tr>
<tr>
<td>BestEffort-2</td>
<td></td>
</tr>
<tr>
<td>BestEffort-3</td>
<td></td>
</tr>
</tbody>
</table>

To add a QoS Profile.

1. In the Networking tab, go to Class of Service > QoS > Profiles.
2. Click the **+ sign** to open the Add QoS Profile screen.
a. In **Name** field, type a name for the profile.
b. In the **Description** field, describe the profile.
c. In **Peak Rate (pps)** field, type the required peak rate for packets per second (pps), in the Peak Rate (Kbps) field, type the kilobytes per second, and in the Peak Burst Size (Bps) field, type the bits per second.
d. From the **Forwarding Class** list, select the applicable forwarding class.
e. From the **Exceed Forwarding Class** list, select the applicable forwarding class.
f. From the **Loss Priority** list, select low if the data packets are less likely to drop vs. high loss priority. Or select high if the data packets are more likely to drop vs. low loss priority.
g. From the **Exceed Loss Priority** list, set the priority of dropping a packet related to the exceed forwarding class.
h. Select the **DSCP Rewrite** checkbox to enable whether the differentiated services code point value in the header of incoming IP packets can be changed. The value can be changed to predefined values. DSCP can be used to indicate any QoS needs from the network. In addition, DSCP defines the way routers should queue packets while they are waiting to be forwarded.
i. Select the **Dot 1P Rewrite** checkbox to enable the dot 1P rewrite.
j. Click **OK**.
Configuring App QoS

App QoS lets you define policies for the network traffic. Use App QoS Policies for associating QoS classes with the selected traffic. The policies determine the classification of traffic for treatment when it passes through a QoS enabled interface. For individual rule, you specify one of the eight classes. You can also assign a schedule to specify the active rule. Unclassified traffic is automatically assigned to class 4. You can define a policy to apply policing/traffic-shaping metrics on traffic that matches certain applications, URL categories and user/user groups.

To configure the App Qos Policies workflow.

1. In the Networking tab, go to Class of Service > App QoS > Policies.
2. Click the + sign to open the Add App QoS Policy screen.

   a. In the Name field, type an app QoS policy name. CenturyLink will create a default-policy on initial setup, so this step will typically not be required.
   b. Click OK.
3. Click the + sign to open the Add App QoS Rule screen for the newly added Policy name.

![Add App QoS Rule Screen]

a. In the Name field, type a name for the QoS rule.

4. Click the Source/Destination tab.

![Source/Destination Tab]

Notice: Services not available everywhere. CenturyLink may change or cancel products and services or substitute similar products and services at its sole discretion without notice. ©2019 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.
a. In the **Source Zone** section select the checkbox next to the Traffic source zone on which to apply the rule. To add a new rule, click the + New Zone.

b. In the **Destination Zone** section, select the traffic destination zone on which to apply the rule.

c. In the **Source Address** section, select the traffic source address on which to apply the rule. To add a new address group, click + New Address Group. You can exclude addresses from the source/destination by selecting the negate checkboxes next to their names.

d. In the **Destination Address** section, select the traffic destination address on which to apply the rule.

5. Click the **Headers/Schedule** tab to specify the rule in relation to the IP and user-defined service list, which you can define via the + New Service screen.

![Edit App QoS Rule](image)

a. To match on DSCP values, click the + button to add a DSCP value.
6. Click the **Applications/URL** tab to define the applications and URL categories for which this rule is applicable. You can define them by clicking **+ New options** or map them through the bind data.

![Add App QoS Rule](image)

   a. Click the **+ sign** to add a new application or URL category to match traffic for the QoS rule. If an application or URL is not in the list, a custom application or URL can be added by clicking **+ New Application** or **+ New URL Category**.

7. Click the **Enforce** tab.

   ![Add App QoS Rule](image)

   a. From the **QoS Profile** list, select the name which you defined in App QoS > Profiles.
b. Click OK.

You can define multiple rules for the App QoS Policies. **Note:** CenturyLink will review recommended and CenturyLink certified QoS default policies and rules that can be pre-configured when you set up your service. You can then edit application matching within the rules to better fit the needs of your network.

**Configuring Associate Interface/Network**

You can do traffic shaping on an interface and network. For example, if the default bandwidth available is 10 Mbps and you need to reduce it to 5 Mbps, then it is possible with interface and network shaping. It is also important to have the interface bandwidth set so any percentage-based profiles are calculated against the defined interface bandwidth.

The traffic shaping configuration workflow on an interface and network.

1. In the Networking tab, go to Class of Service > Associate Interface/Network.
2. Click the + sign to associate an interface and network.

![Diagram of interface association](image)

- In the **Name** field, type a name for the interface.
- In the **Burst Size (Bytes)** field, type the number of bytes for the burst size of data packets.
- In the **Rate (Kpbs)** field, type the maximum number of data packets rate in kilobytes.
- From the **DSCP Rewrite Rule** list, select the differentiated services code point rewrite rule.
- From the **DSCP6 Rewrite Rule** list, select the differentiated services code point6 rewrite rule.
- From the **8021p Rewrite Rule** list, select the type of 8021p rewrite rule.
- From the **Scheduler Map** list, select the name of the scheduler map.
- In the **Logging Interval (Secs)** field, type the number of seconds needed for the logging interval. After this many seconds, the log information will be sent to Versa Analytics for further analysis and data visualization.
i. Select the **Network** ratio button.

![Network interface image]

a. From the **Name** list, select the network name.

b. Click **OK**.

![Network configuration image]
Stateful Firewall

Overview

The stateful firewall enables full visibility of the traffic that traverses through the firewall while also enforcing fine grain access control on the traffic. To classify the traffic, the stateful firewall verifies its destination port and then tracks the state of the traffic and monitors every interaction of each connection until it is closed.

The stateful firewall grants or rejects access based not only on port and protocol but also on the packets history in the state table. When stateful firewall receives a packet, it checks the state table for an established connection or for a request for the incoming packet from an internal host. If nothing is found, then the packets access is subject to the access policy rule.

Configure a security access policy to classify traffic using a security access policy. A security access policy is required for the stateful firewall feature to work. A security access policy includes the stateful firewall rule that collates the defined objects and assigns an action to be taken based on the match conditions.

Note: Stateful firewall is only limited to layer 2 through layer 4. This option is not visible in the Web UI if you have subscribed to the Next Generation Firewall CenturyLink Advanced Security Package.

The stateful firewall spends most of its cycles examining packet information in layer 4 (transport) and lower. For more advanced inspection capabilities, it targets vital packets for layer 7 (application) examination, such as the packet that initializes a connection. If the inspected packet matches an existing firewall rule that permits it, the packet is passed, and an entry is added to the state table. Because the packets in that communication session match an existing state table entry, from this point forward they are allowed access without call for further application layer inspection.

These packets only need to have their layer 3 and 4 information (IP address and TCP/UDP port number) verified against the information stored in the state table to confirm that they are part of the current exchange. This method increases overall firewall performance because only initiating packets need to be encapsulated the entire way to the application layer.
Each security access policy comprises of one or more rules and each rule consists of match criteria and the enforcement action. Use one or more of these traffic attributes to specify the match criteria:

- Source Zone
- Destination Zone
- Source Address
- Destination Address
- Domain Names
- Source Geo-Location
- Destination Geo-Location
- IP Headers
- Services (based on port/protocol)
- Time of Day

A rule is considered a match when all match criteria defined in the rule matches. All rules in the security access policy are evaluated in a top-down order. The first rule that matches is selected and the corresponding security actions are enforced. CenturyLink recommends you configure more specific rules before the generic rules in the security policy.

The stateful firewall policy has these enforcement actions:

1. Logging
   - Start, End, Both, Never
2. Action
   - Allow—allows the sessions matching the configured rule to pass.
   - Deny—drops the sessions matching the rule.
   - Reject—drops the session and sends the RST packet for a TCP session and ICMP port unreachable packet for a UDP session.

## Configuring Security Access Policy

Enable stateful firewall in the configuration and create an access policy. You can define multiple security policies and isolate them on a per-tenant basis. Each security policy must have a unique name for a tenant. The security access policy comprises an ordered set of one or more policy rules.

When multiple security policies are defined then all rules of all the security access policies are evaluated in the order in which the security policies are configured.

To define and configure a security access policy:

1. Select Administration > Appliance and click on the appliance in the dashboard to navigate to the appliance context.

3. Click in the dashboard to add a new security access policy. This opens the Add Access Policy window.

4. Enter the details in the Add Access Policy window.

5. Click OK.

Configuring Security Access Policy Rules

The security access policy comprises of an ordered set of one or more policy rules. Each policy rule comprises a set of match criteria and the enforcement actions. The security access policy rules within the stateful firewall policy are matched based on layer 3 and layer 4 information and/or time of day. These enforcement actions are supported—Allow, Deny, Reject, and Log Generation.

To define and configure a security access policy rule:

1. Select Administration > Appliance and click on the appliance in the dashboard to navigate to the appliance context.

2. In Appliance context, select Configuration > Services > Stateful Firewall > Security > Rule tab in the dashboard.

3. Click the + sign to add a rule for the new security access policy.
4. Click the General tab and configure the name and description for the DoS protection policy rule.

5. Click the Source/Destination tab to define the source zone, source address, destination zone, and destination address of the incoming (source) and outgoing (destination) traffic to which the policy rule applies.

6. Click the Header/Schedule tab to define the IP header, services and schedule to which the security access rule applies.

7. Click the Enforce tab to select the applications and URLs to which the security access rule applies.

8. Click OK.