# Juniper Validated Design (JVD)

## WAN Edge for SRX Series Firewall

Juniper Networks Validated Designs provide customers with a comprehensive, end-to-end blueprint for deploying Juniper solutions in their network.

These designs are created by Juniper's expert engineers and tested to ensure they meet the customer’s requirements.

Using a validated design, customers can reduce the risk of costly mistakes, save time and money, and ensure that their network is optimized for maximum performance.

# About This Document

When building a modern software-defined WAN (SD-WAN) environment to overlay existing networks and transport technologies for an enterprise, there are several important design considerations. Juniper WAN edge for SRX Series Firewall that provides a solution to meet the specific demands of the enterprise. Before implementing a robust VPN for the enterprise and leveraging these individual designs, some choices need to be made.

This JVD describes the various ways of WAN edge for SRX Series Firewall integration and the test cases that are performed to ensure proper integration in an example network design. We provide information about the different topologies tested and which of the features are evaluated. Additionally, complete configuration examples, using the Mist GUI, are provided in the appendix for your reference.

## Documentation Feedback

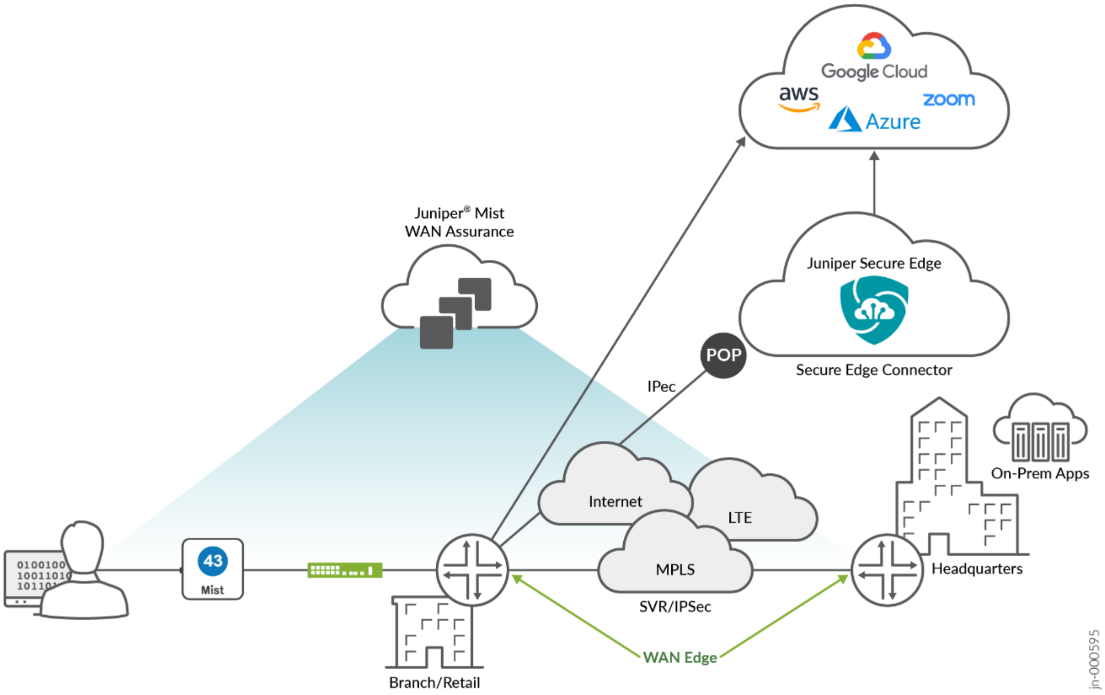
We encourage you to provide feedback so that we can improve our documentation. Send your comments to design-center-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

## Table of Contents

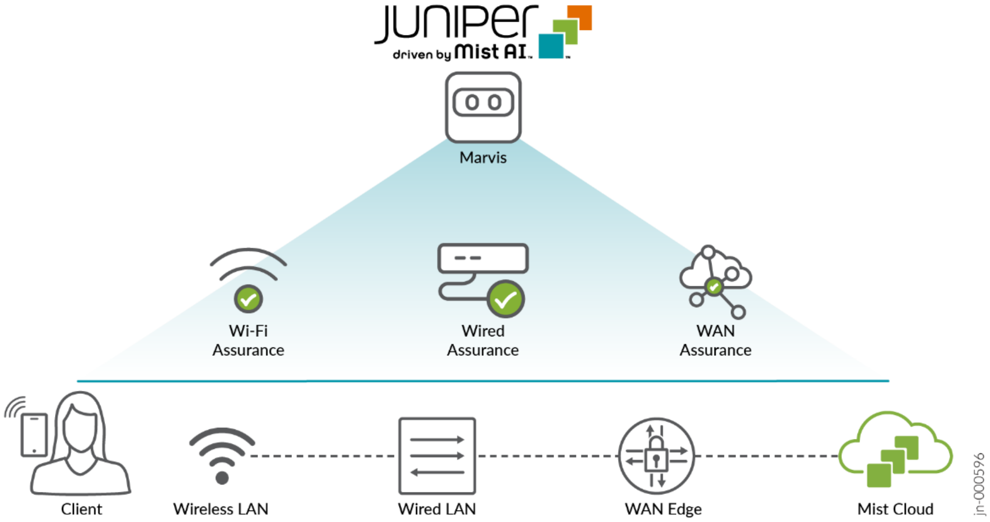
# Solution Benefits and Overview

Introduction to Juniper Mist WAN Assurance

The WAN edge references the demarcation point for your enterprise network to reach the outside world. This boundary is a crucial security and troubleshooting hotspot. The WAN edge can be a simple border between your enterprise network and the outside world. The WAN edge can also be a Juniper SD-WAN driven by Mist AI device such as Juniper SRX Series Firewall or a cloud solution such as Juniper Secure Edge.



The WAN edge transforms with Juniper's AI-driven SD-WAN solution and acts as your centralized policy enforcement point (PEP). Combined with the Juniper Mist WAN Assurance cloud service, the Juniper SD-WAN solves many of the security, monitoring, and troubleshooting challenges of legacy SD-WAN solutions. Bring deployment, monitoring, and troubleshooting across your network by integrating Juniper Mist Wired Assurance, Juniper Mist Wireless Assurance, and now Juniper Mist WAN Assurance under a cohesive Mist AI dashboard. Juniper Mist WAN Assurance securely connects branch offices with Juniper SRX Series Firewalls across a SD-WAN.

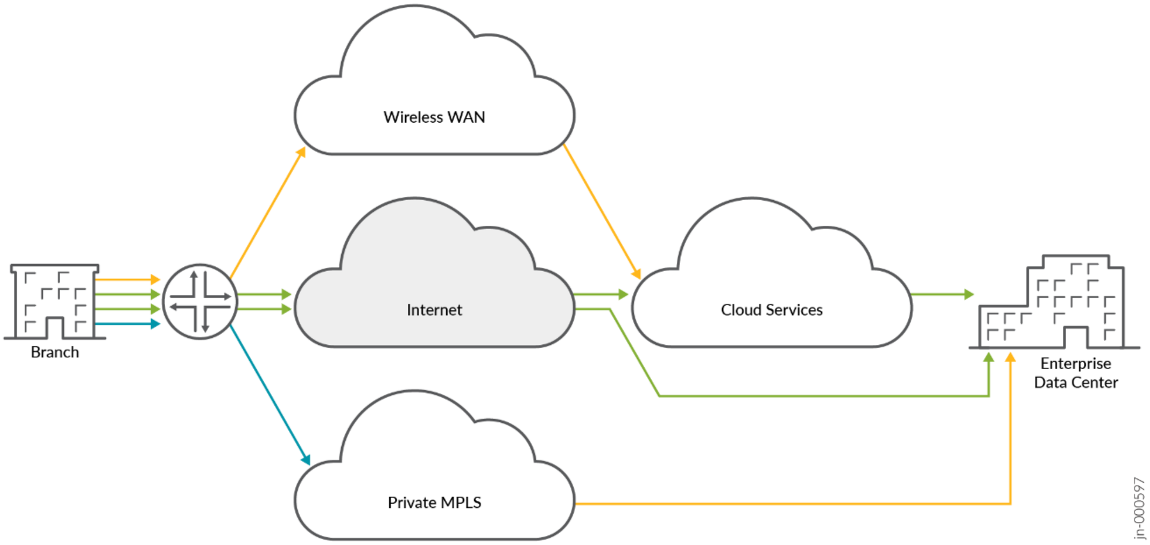


Watch the following video for an overview of the Juniper Mist WAN Assurance feature.

Site-to-Site Connectivity (SD-WAN)

Your WAN edge transforms when integrated with Juniper SD-WAN driven by Mist AI. Your edge device becomes fast, secure, and application-aware with Juniper Mist WAN Assurance. SD-WAN traffic from remote sites travels through an abstracted overlay across less expensive broadband service provider networks. This connectivity design replaces expensive legacy MPLS solutions. Edge devices deliver stateful failover across various connection types, including MPLS, broadband, satellite, and LTE. This real-time switch for critical applications is imperceptible to the user. Additionally, Juniper Mist WAN Assurance provides visibility to your WAN edge with targeted insights for health, tunnel activity, connectivity, and active sessions. By creating that software-defined space, you can influence traffic at the application level with greater control over access and security.

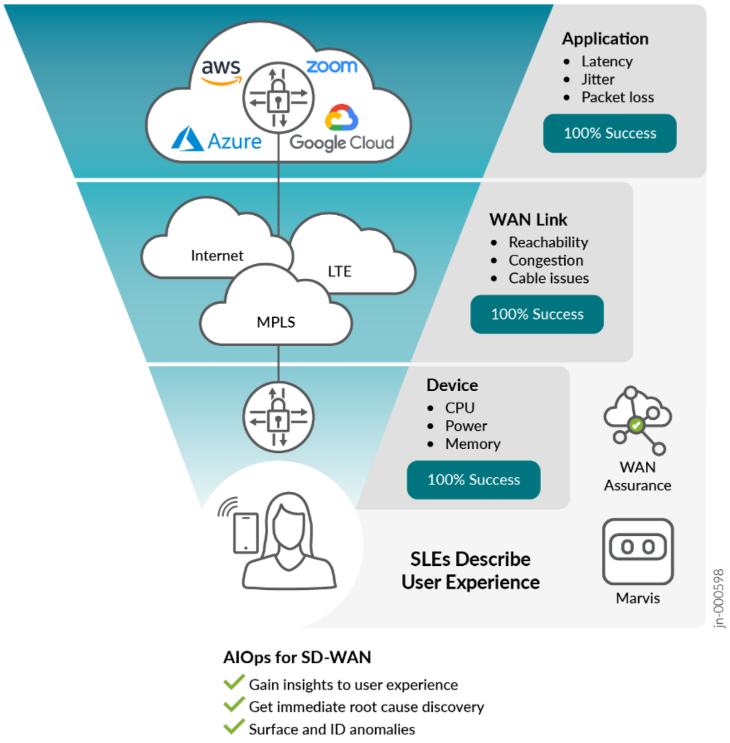
Figure 1: Site-to-Site Connectivity Options



## Juniper Mist WAN Assurance SLEs

Mist’s Predictive Analytics and Correlation Engine (PACE) provides data science and machine learning (ML) to help you understand the end-user experience. The WAN SLE metrics are WAN edge health, WAN link health, and application health. Juniper Mist WAN Assurance identifies the root cause of WAN issues that impact user experiences. SLEs enable simpler operations, better visibility into end-user experiences, and simplify monitoring and troubleshooting your network.

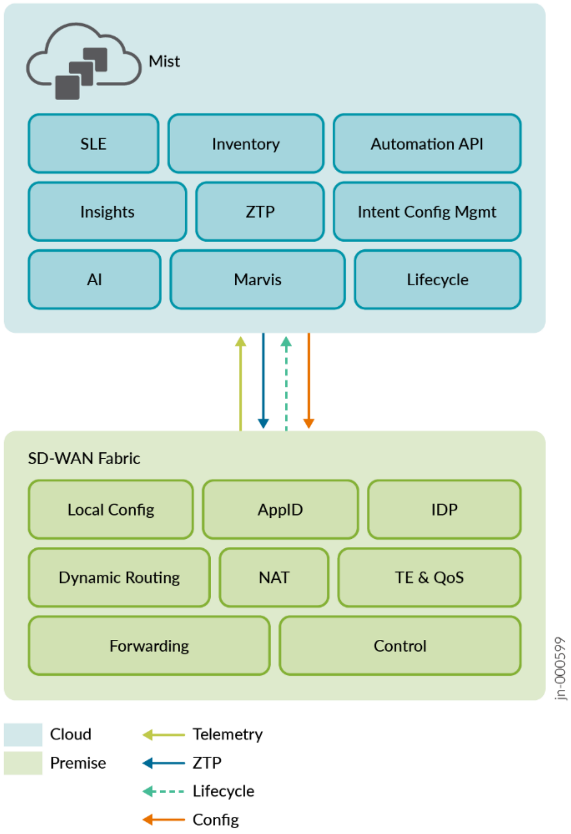
Figure 2: WAN Assurance SLE Metrics



## Mist Management Model

Juniper’s AI-driven SD-WAN solution is a single management platform for branch wireless, wired, and SD-WAN. Juniper SD-WAN zero-touch provisioning (ZTP), life cycle, and configuration are done through a single Mist dashboard.

Figure 3: Mist Management Model



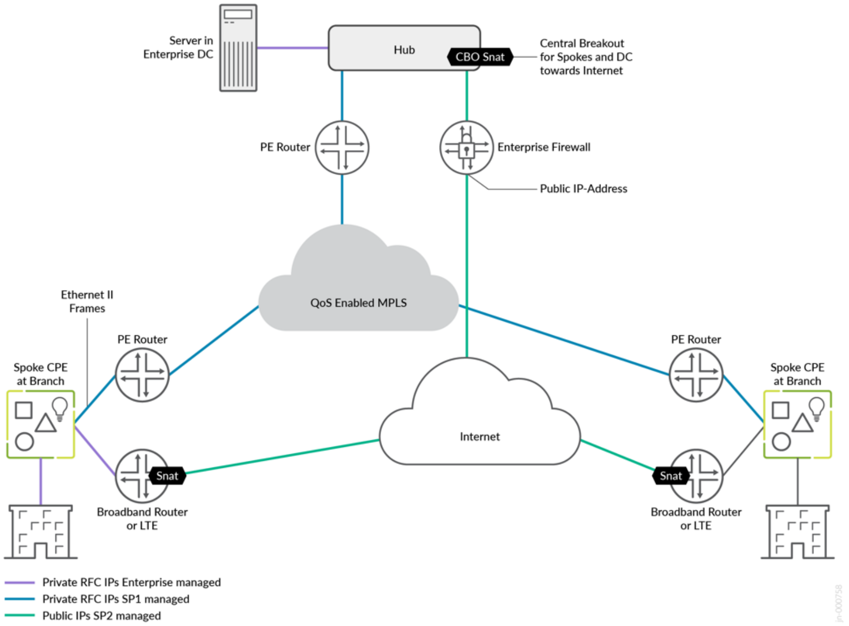
# Use Case and Reference Architecture

In this chapter, we describe an example of SD-WAN implementation in a typical hub-and-spoke scenario that leverages different transport technologies to show how it is implemented. A similar lab was built to test this JVD which you can see in the test report.

Keep the following design goals in mind:

- Design for a hub-and-spoke scenario from day one on. Mesh designs always have scale limitations and are not usually friendly to cheap broadband Internet and LTE connections.
- Ensure your hubs have the right connectivity so that the spokes can reach them using the transport network.
  - If you have an MPLS network, your service provider usually provides a routed private IP address to you or the end-customers manage their own private IP address range (VPLS).
  - When the device has any broadband or LTE connection, you can assume that there is a kind of source NAT applied on the path or the IP addresses on the local router are not permanent. In this case, the hub must have a statically assigned public IP address that is reachable from the spoke trying to make an IKE/IPsec connection.
- Local country regulations should not filter or restrict communication on destination UDP ports 500 and 4500. Because these ports must be open to setup the tunnels between spokes and hubs on the overlay network.

- Consider allowing only VPN traffic inside your SD-WAN to lower the overall traffic. All traffic to services outside your VPN should use local breakout at the spoke. Because the SRX Series Firewall has firewalling capabilities that help to protect your environment, central firewalling at the hub might not be needed.



A lab that simulates the real world would have two underlay paths, each with different behavior:

- You can emulate an MPLS path (without the MPLS framing in-between) with private IP addresses that are visible end-to-end. In a real-world environment, those private IP addresses are managed and distributed by the MPLS service provider's route reflector. hub-and-spokes get static IP's assigned to the interfaces.
- An Internet path that is subject to a lot of NAT might make the connection of devices difficult. However, this tends to be what you see in production environments today.
    - Spoke devices get a DHCP address lease from an emulated local broadband router. The emulated router applies symmetric source NAT, especially if the device is connected through Dual-Stack Lite (DS-Lite). This forces the spoke to open a tunnel toward the public IP address of the hub using IKE (UDP destination port 500) and IPsec NAT-T (UDP destination port 4500).
    - Hub devices get a private static IP address that is assigned to the local interface. In front of the hub there is an emulated public IP where all spokes must send the traffic to if they want to connect to the hub or the Internet. We then emulate a router or firewall that applies 1:1 NAT forwarding to the private interface IP address of the hub. This emulates the exact behavior you would see when the hub is a VM inside a public cloud. A public cloud provider would not give you the option of assigning a public IP directly to an interface on your hub device.
    - The LTE modem connection of a spoke device is expected to have the same topology requirements. Typically, the mobile service provider (MSP) does some kind of carrier-grade NAT (CG-NAT) in its network. However, simulating an LTE Network is tricky as privately owned LTE networks and frequencies are rare. Hence, the simulated broadband router should implement a similar behavior where CGNAT is done in the network before traffic appears on the Internet.

- Both paths are assumed to be completely isolated from each other using an internal firewall. Any intentional cross-path communication needs to leverage the hub which has interfaces on both paths for fail-over.

Based on these two different path designs, we have implemented and tested four different topologies in this JVD:

- A basic hub-and-spoke design with two independent hubs and three spokes. This serves as a need-to-know, base scenario. The other three topologies are extensions or changes to the base topology to achieve other goals. See Basic SD-WAN Topology with 3 Spokes and 2 Hubs.
- A topology where the servers at the hub are not directly attached to the LAN interface and there is a router that is placed between the hub and server. This router then exchanges routes using BGP with the hub to advertise its servers and its VPN-reachable networks. We also enabled a hub to hub mesh using the hubs' WAN interfaces as a way to implement a kind of hub redundancy on layer 3 (L3). See Extended Topology with Hub-Mesh and BGP Peering.
- A topology where we form redundant high-availability hub and spokes using the SRX Cluster feature. Those clusters need local layer 2 (L2) adjacency between the two devices. See Topology with Highly Available Spoke and Hub Using Clustered SRX Pairs.
- A topology where we add at the spoke a Juniper EX Series Switch and a Juniper Mist AP. This is a most common scenario at a branch where Juniper provided the Full-Stack Networking environment with all components controlled by a single UI in the Juniper Mist cloud. Please check Full-Stack Topology with Juniper EX-Switch and Mist AP.

## Basic SD-WAN Topology with Three Spokes and Two Hubs

This lab represents the default structure where we emulate the following:

- Installation of three spoke devices
- Installation of two hub devices
- Two underlay paths with different behaviour. In the lab, the underlay address range is 192.168.0.0/16.
  - MPLS path with private IP addresses.
  - Internet path, subjected to NAT.
- An overlay network managed by the enterprise. It is implemented on the LAN side of hub and spokes. In the lab, the overlay address range is 10.0.0.0/8.

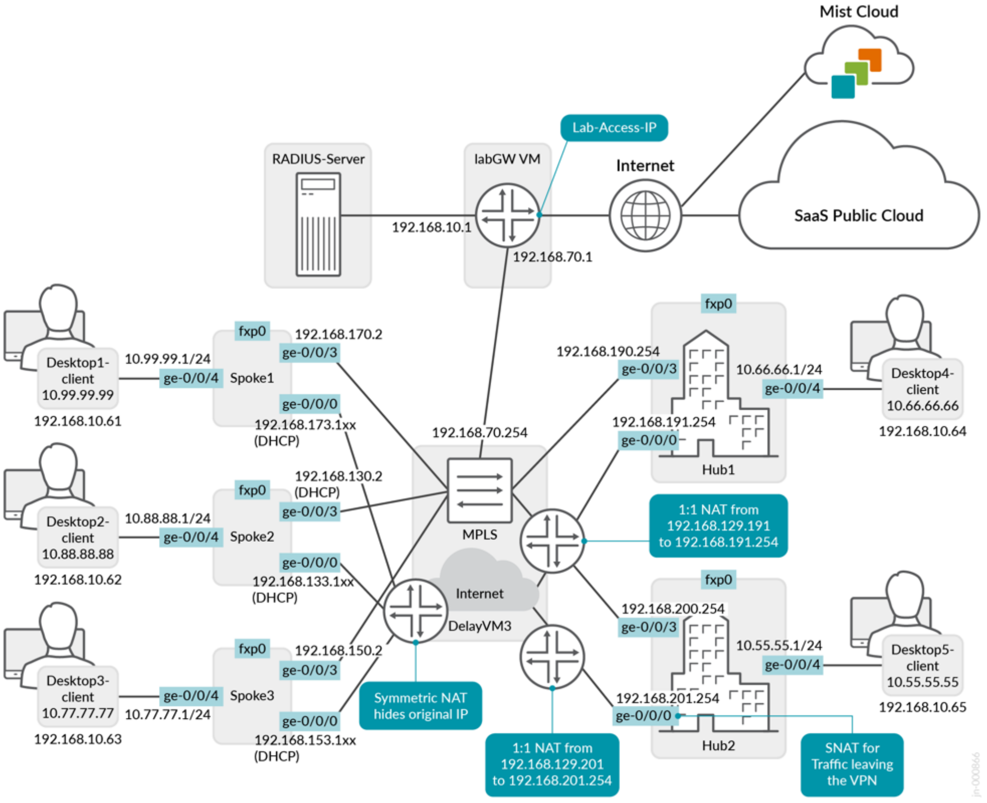
Table 1: Interfaces and IP Addresses Used in this Lab

| Device | Interface | IF-Type | Path | IP Address | Assigned |
|---|---|---|---|---|---|
| Spoke1 | ge-0/0/0 | WAN | INET | 192.168.173.1xx | DHCP |
| Spoke1 | ge-0/0/3 | WAN | MPLS | 192.168.170.2 | static |
| Spoke1 | ge-0/0/4 | LAN | Overlay | 10.99.99.1/24 | static |
| Spoke2 | ge-0/0/0 | WAN | INET | 192.168.133.1xx | DHCP |

| Device | Interface | IF-Type | Path | IP Address | Assigned |
|---|---|---|---|---|---|
| Spoke2 | ge-0/0/3 | WAN | MPLS | 192.168.130.2 | static |
| Spoke2 | ge-0/0/4 | LAN | Overlay | 10.88.88.1/24 | static |
| Spoke3 | ge-0/0/0 | WAN | INET | 192.168.153.1xx | DHCP |
| Spoke3 | ge-0/0/3 | WAN | MPLS | 192.168.150.2 | static |
| Spoke3 | ge-0/0/4 | LAN | Overlay | 10.77.77.1/24 | static |
| Hub1 | ge-0/0/0 | WAN | INET | 192.168.191.254 | static |
| Hub1 | ge-0/0/3 | WAN | MPLS | 192.168.190.254 | static |
| Hub1 | ge-0/0/4 | LAN | Overlay | 10.66.66.1/24 | static |
| Hub2 | ge-0/0/0 | WAN | INET | 192.168.201.254 | static |
| Hub2 | ge-0/0/3 | WAN | MPLS | 192.168.200.254 | static |
| Hub2 | ge-0/0/4 | LAN | Overlay | 10.55.55.1/24 | static |

Note: In this lab, the emulated public IP addresses are 192.168.129.191 for Hub1 and 192.168.129.201 for Hub2. The spokes to connect to these addresses.

Figure 4: Network Topology for SRX with Three Spokes and Two Hubs



# Extended Topology with Hub Mesh and BGP Peering

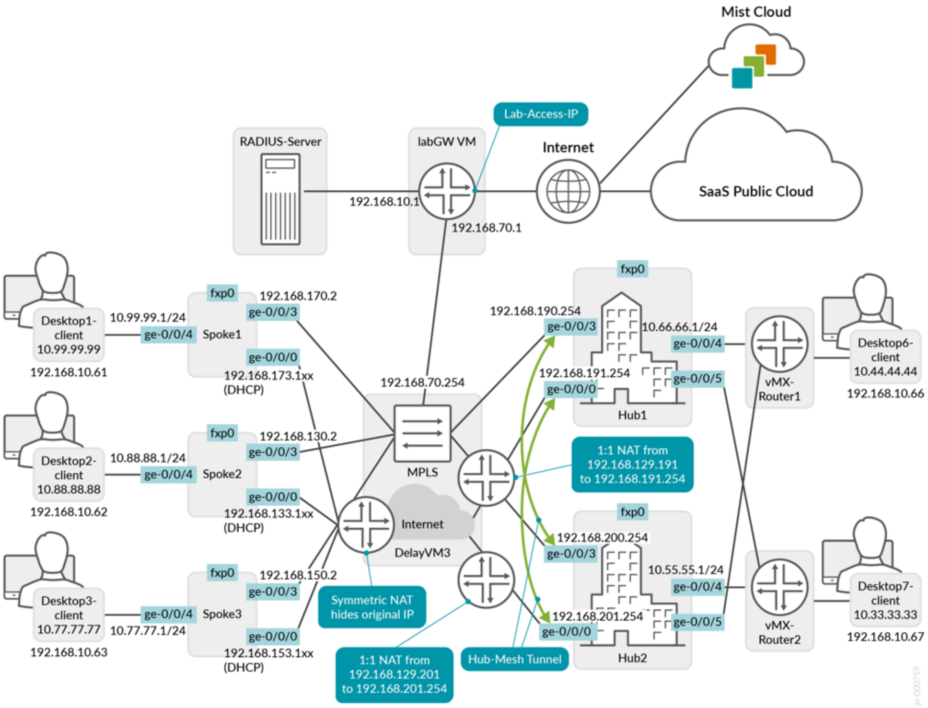
This is a topology where the servers at the hub are not directly attached to the LAN interface. There is a router that is placed between the hub and the server. This router exchanges routes over BGP with the hub to advertise its servers and the VPN-reachable networks. We also enabled a hub-to-hub mesh, using the WAN interfaces of the hubs, as a means of hub redundancy at L3.

The two MX Routers attached to the LAN interfaces and the following additional networks:

- 10.44.44.0/24 attached to the router of Hub1.
- 10.33.33.0/24 attached to the router of Hub2.

These networks are additionally defined. The hub mesh is an added configuration in the Mist GUI.

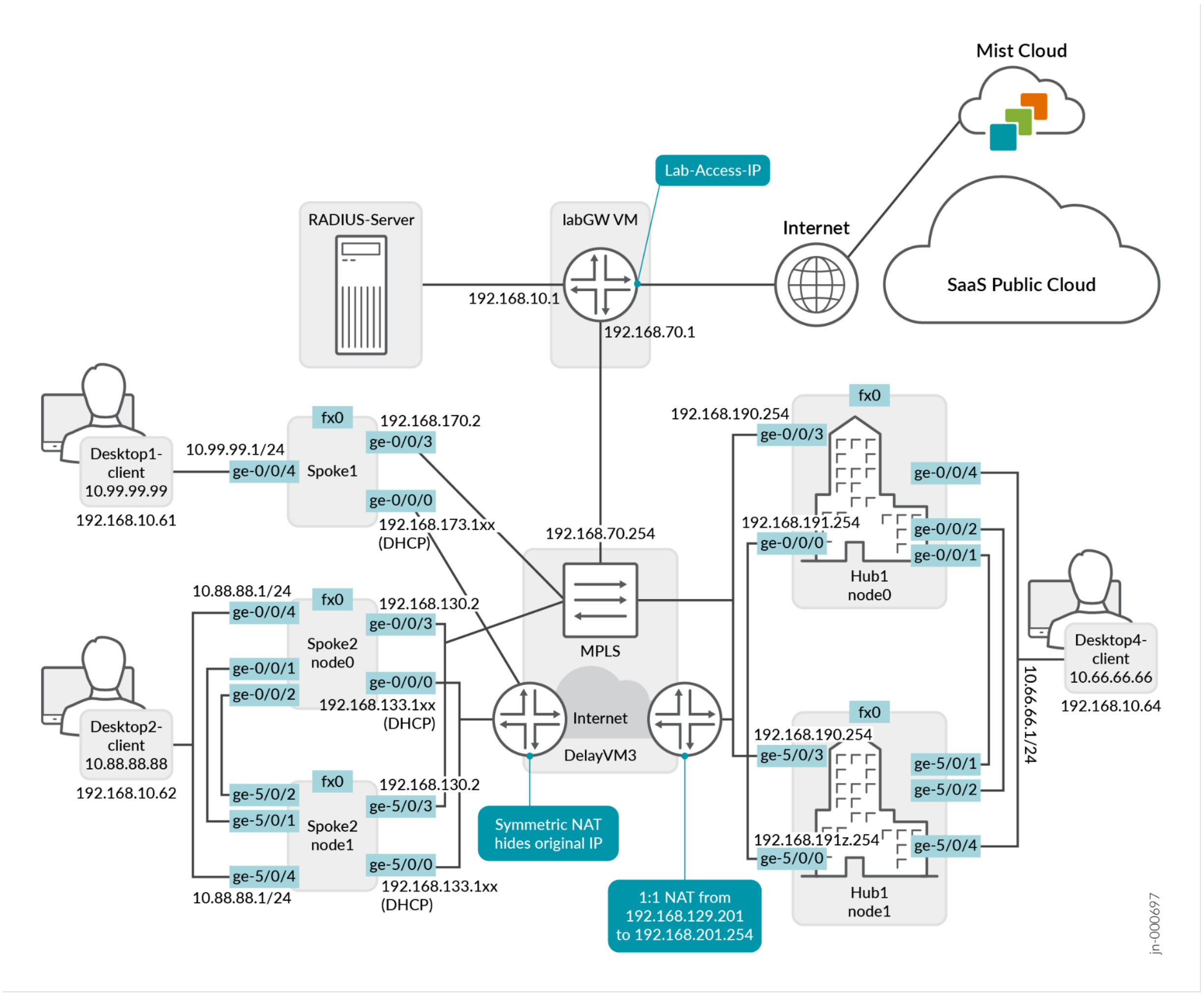
Figure 5: Network Topology for SRX with Hub Mesh and BGP Peering



## High Availability Hub-and-Spoke Using SRX Chassis Cluster Pairs Topology

In this topology,  we form redundant high-availability hub-and-spokes using the SRX Cluster feature. Each cluster is built using the same SRX Series device model plus local (L2 adjacency and two additional cables for HA-Control/Fabric. Note that the LAN interfaces are shared with the same IP address. The WAN interfaces are not shared.

Figure 6: Topology with Highly Available Spoke and Hub Using Clustered SRX Pairs



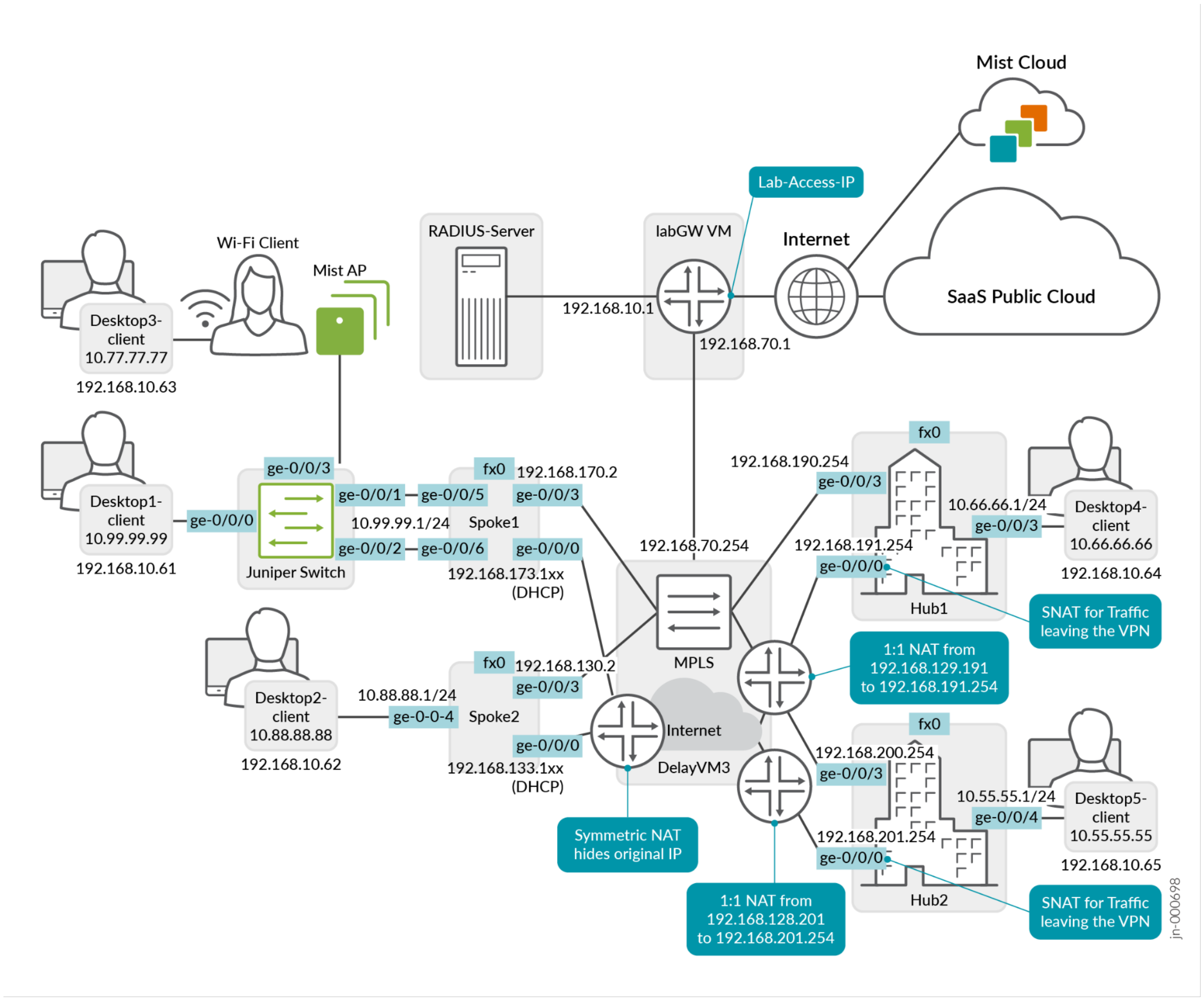
Note: This type of deployment for a hub is impossible in most public clouds since you might have a VM-based hub. This is because the strict rules governing public clouds usually do not allow MAC address moves between interfaces. Consider hub mesh instead.

## Full Stack Topology with Juniper EX Switch and Juniper Mist AP

In this topology, we are adding Juniper EX Series Switches and Mist AP to provide an end-to-end, full stack solution to the branch. To boot the EX Series Switch up behind the SRX Series Firewall as WAN router, we also utilize:

- A DHCP server on the spoke to handout DHCP address leases to the EX Series Switch, Juniper Mist AP, and all wired and wireless clients.
- Two interfaces between the EX switch and WAN router with LAG and active LACP.
- Support for force-up on one of the uplink ports of the WAN router because initially, the LAG configuration on the EX Series Switch is not present. This configuration allows in-band management of the switch though it’s revenue ports. Without the force-up feature, you would need a dedicated cable from the management port of the switch to the WAN router or a more complex staging method to form the LAG without losing device management.

Figure 7: Full Stack Topology with Juniper EX Series Switch and Juniper Mist AP



Note: Ignore the Desktop3 VM with attached Wi-Fi client. This was part of the initial build of this lab to test wireless connections.

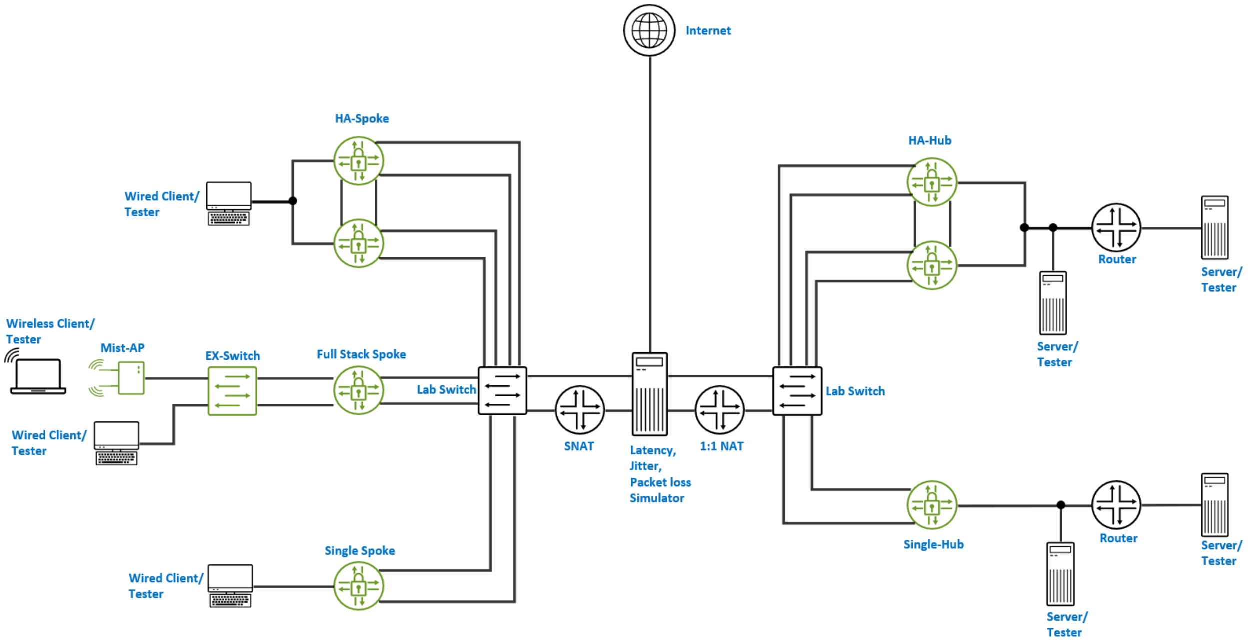
# Validation Framework

## Test Bed Overview

In a production network, all hubs would need public IP addresses to be reachable for traffic from broadband or LTE networks as their traffic moves through the Internet as transport.

Figure 8 shows a lab topology that provides all needed functionality locally without using the Internet for Juniper Mist cloud management and services that are hard to simulate locally such as Outlook 365, Facebook, and so on. A similar lab was built to test the four major topologies and the additional functions that WAN edge provides for SRX Series Firewall.

Figure 8: Lab Topology



# Platforms and Devices Under Test (DUT)

All tests were performed with the current recommended Junos OS release for WAN edge for SRX Series Firewall.

| Devices Under Test | | |
|---|---|---|
| **Platform** | **Device** | **Junos OS Release** |
| SRX300 | Spoke | 21.2R3-S7 |
| SRX320 (pair) | HA Spoke | 21.2R3-S7 |
| SRX345 | Spoke | 21.2R3-S7 |
| SRX1500 | Hub2 | 21.2R3-S7 |
| SRX4600 (pair) | HA Hub1 | 21.2R3-S7 |

# Test Bed Configuration

We are sharing information about exactly how some of the tests performed in the appendix section of this document. Contact your Juniper representative to obtain the full archive of the test bed configuration used for this JVD.

# Test Objectives

## Test Goals

The testing for this JVD was performed with the following goals. For more information, see the test report of this JVD.

The goal was to test the following features and functions:

- Testing was performed and passed on all four major topologies:
  - Basic SD-WAN Topology with 3 Spokes and 2 Hubs
  - Extended Topology with Hub Mesh and BGP Peering
  - Topology with Highly Available Hub and Spoke Using SRX Chassis Cluster Pairs
  - Full Stack Topology with Juniper EX Switch and Juniper Mist AP
- WAN link-related features:
  - Multiple WAN links
  - MTU
  - Auto negotiation
  - Interface static IP
  - Interface DHCP IP
  - WAN source-NAT interface
  - WAN SLE
  - Failover when WAN links broken (RPM)
- LAN link-related features:
  - VLAN tagging
  - DHCP server
  - Multiple interfaces for the same LAN (access)
  - Multiple LANs on same interface (trunk)
  - IEEE 802.3ad LAG with active LACP
    - Using force-up option on one interface for EX Series Switch behind ZTP.
- VPN overlay features:
  - Spoke-to-hub overlay
  - Hub-to-spoke overlay
  - Spoke-to-spoke overlay (through Hub)
  - Hub-to-hub overlays using hub mesh
- Traffic steering and forwarding features:
  - Central breakout at hub
  - Local breakout at spoke
  - Static route at spoke
  - Static route at hub
  - BGP route at hub
  - Failover when WAN links get broken (IPsec DPD)
  - Secure Edge Connector–JSE

- Application policy features:
  - Source-attached LAN
  - Source non-attached user
  - Various applications as defined in next section
  - IDP enabled
  - Imported organization application policies
- Applications are defined using the following parameters:
  - Applications defined by IP prefixes
  - Applications defined by protocol and port
  - Applications defined by DNS-FQDN
  - Applications defined by predefined-app
  - Applications defined by app categories
  - Applications learned through Learned Applications selection
- Redundancy and high availability options:
  - Two or more independent hubs with failover at spoke
  - Chassis Clustered hub
  - Chassis Clustered spoke
  - Hub redundancy using hub mesh
- Security features:
  - Stateful firewalling
  - Application Tracking (AppTrack)
  - Web filtering
    - URL Subcategory
  - IDP
    - IDP bypass
    - IDP critical signature
  - Secure Edge Connector
- General options and features:
  - EX Series Switch behind SRX WAN router
  - Juniper Mist AP behind EX Series Switch
  - Site variables
  - Application path visibility
  - WAN edge Insights
- Scale testing (see Test Report)

## Test Non-Goals

Testing for this JVD was not performed, for various reasons, on the following items:

- No LTE, PPPoE, and VDSL testing was performed. This was a lab limitation.
- Features that need more than 10 additional CLI lines because the focus on JVD testing is to test end-user configurable features and not application of Junos OS CLI commands.

# Recommendations

- Ensure you have a valid AppTrack license configured and enabled for each device. This is mandatory for WAN edge with SRX Series Firewall. Additional features might need license.
- Design for a hub-and-spoke topology from day one. It's the most scalable topology with the least connectivity issues.
- Hubs that need to be reachable through broadband connections, LTE, or other Internet services must have static and public IP addresses (directly or indirect assigned).
- Consider local breakout at the spoke for all services that are reachable on the Internet. Do not burden your VPN with that local breakout or service.
- Check local regulations as they must not filter or restrict communication on destination ports 500 and 4500 UDP. These ports are needed to set up the tunnels between spokes and hubs.
- Avoid creating too many versions of your templates to account for small changes. Instead, make use of site variables to change settings.
- If the SRX Series device is behind a firewall, confirm that the ports needed for communication with the Juniper Mist cloud are open. See **Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration | Mist | Juniper Networks**.

# APPENDIX: Test Case Example Information

## Day-0 Operation to Claim or Adopt the SRX Series Devices to the Juniper Mist Cloud

> Note: Before you start any SRX Series device deployment, you ensure to have a valid appid-sig or idp-sig (depending on your device) license installed on the device. This is a mandatory license for WAN edge for SRX Series Firewall.

The below is an example of what you should see through console.

```
# if your device is a vSRX or SRX1500
# then check if your appid-license is still valid and that you have one
show system license | match appid-sig
  appid-sig                         0          1          0   2022-01-21 00:00:00 UTC
.
.

# if your device is an SRX3xx
# then check if your idp-license is still valid and that you have one
show system license | match idp-sig
  idp-sig                           0          5          0   2022-01-22 00:00:00 UTC
.
.
```

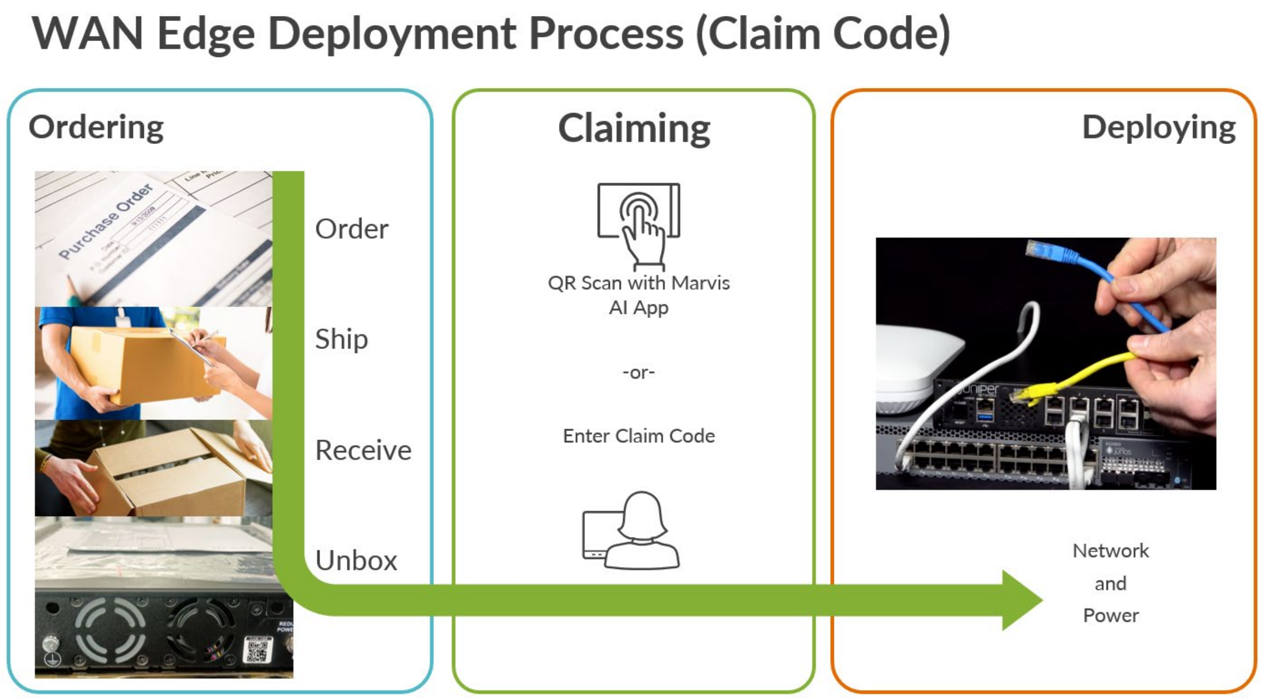
With an unmodified factory default configuration, it is expected that the device gets a DHCP-lease on the first interface (usually ge-0/0/0) and uses the provided information to reach out to the Juniper Mist cloud to obtain further configuration information. The usage and meaning of all other interfaces can be changed later through configuration. But the best practice is to consider that the **first interface is a WAN-Interface obtaining an initial DHCP lease**.

Ensure that you are not blocking destination port 2200 towards Juniper Mist cloud as it uses an out-bound SSH connection to communicate through TCP-Transport with the Juniper Mist Cloud. This is essential to manage this device. See: Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration | Mist | Juniper Networks.

### Claim and ZTP-Based Installation

> Note: The claim and ZTP method is limited to Juniper SRX300 Series product family only. For all other SRX devices, you are requested to use the adopt method. Also, not every port asks for a DHCP-lease to start ZTP. Use Interface ge-0/0/0 in typical scenarios for ZTP and consult the table for Clustered SRX which interface to use.

The claim and ZTP method allow you to bring a device into the Juniper Mist cloud inventory without the need to pre-provision it. It is designed to allow deploying new devices without special trained personal on site.



## WAN Edge Deployment Process (Claim Code)

Ordering

Order

Ship

Receive

Unbox

Claiming

QR Scan with Marvis AI App

-or-

Enter Claim Code

Deploying

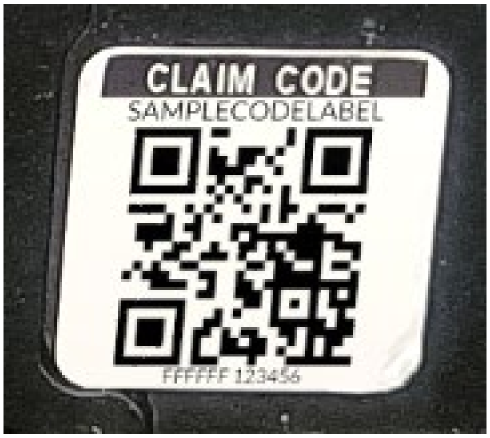
Network and Power

Activation

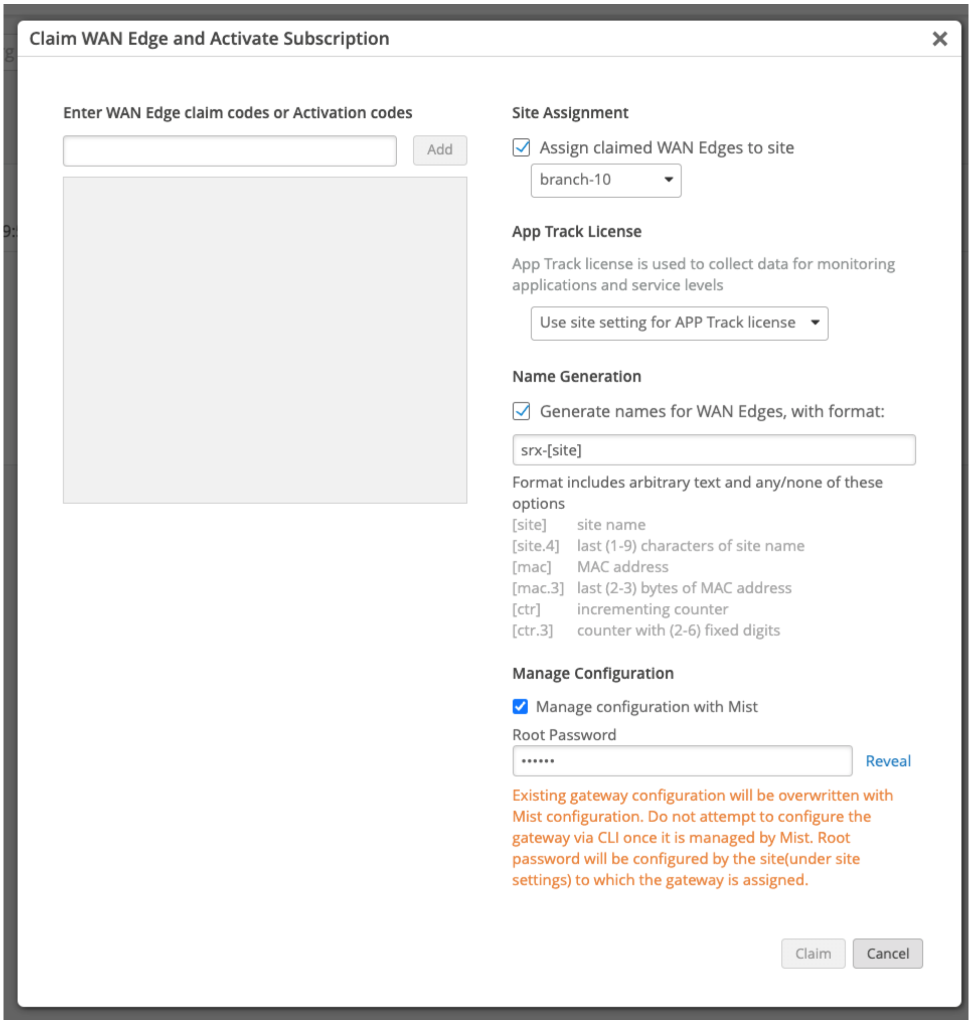
- Enter the individual WAN edge Claim Code
- OR enter the activation code received from Juniper Sales Ops.

The device is registered as a Mist-managed device on the Juniper redirect server and when the device phones home it gets redirected to Juniper Mist.

The claim code is found as QR code on the device:



Then, go to **Organization** > **Inventory** > and select **WAN Edges** > **Claim WAN Edges** to fill the claim code.



Claim WAN Edge and Activate Subscription ✕

Enter WAN Edge claim codes or Activation codes

Site Assignment

☑ Assign claimed WAN Edges to site

branch-10 ▾

App Track License

App Track license is used to collect data for monitoring applications and service levels

Use site setting for APP Track license ▾

Name Generation

☑ Generate names for WAN Edges, with format:

srx-[site]

Format includes arbitrary text and any/none of these options

| | |
|---|---|
| [site] | site name |
| [site.4] | last (1-9) characters of site name |
| [mac] | MAC address |
| [mac.3] | last (2-3) bytes of MAC address |
| [ctr] | incrementing counter |
| [ctr.3] | counter with (2-6) fixed digits |

Manage Configuration

☑ Manage configuration with Mist

Root Password

•••••• Reveal

Existing gateway configuration will be overwritten with Mist configuration. Do not attempt to configure the gateway via CLI once it is managed by Mist. Root password will be configured by the site(under site settings) to which the gateway is assigned.

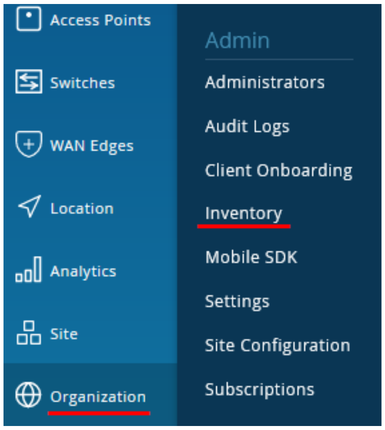
Part of this process is that the device sends an HTTPS request to https://redirect.juniper.net to get the location of the Juniper Mist cloud back. Ensure you allow this communication.

## Adoption Code-Based I

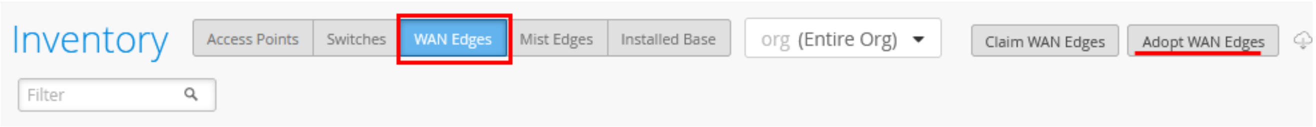
This method works as well even if the device is older and did not get a claim code during manufacturing. However, you need some way to apply Junos OS CLI to the device. Usually through a console connection locally onto the device to some other way of pre-staged configuration.

To run Junos OS CLI on the device:

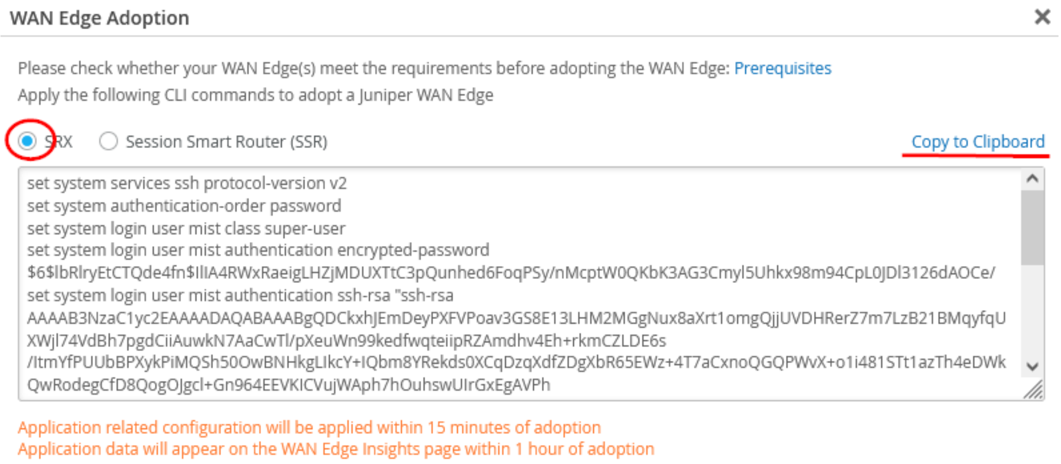
1. Go to **Organization** > **Inventory**.



2. Select **WAN Edges** and then click **Adopt WAN Edges**.



3. Select **SRX** and **Copy to Clipboard** or other methods to extract the displayed CLI content.



WAN Edge Adoption ✕

Please check whether your WAN Edge(s) meet the requirements before adopting the WAN Edge: Prerequisites
Apply the following CLI commands to adopt a Juniper WAN Edge

● SRX ○ Session Smart Router (SSR) Copy to Clipboard

```
set system services ssh protocol-version v2
set system authentication-order password
set system login user mist class super-user
set system login user mist authentication encrypted-password
$6$lbRlryEtCTQde4fn$IlIA4RWxRaeigLHZjMDUXTtC3pQunhed6FoqPSy/nMcptW0QKbK3AG3Cmyl5Uhkx98m94CpL0JDl3126dAOCe/
set system login user mist authentication ssh-rsa "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDCkxhJEmDeyPXFVPoav3GS8E13LHM2MGgNux8aXrt1omgQjjUVDHRerZ7m7LzB21BMqyfqU
XWjl74VdBh7pgdCiiAuwkN7AaCwTl/pXeuWn99kedfwqteiipRZAmdhv4Eh+rkmCZLDE6s
/ItmYfPUUbBPXykPiMQSh50OwBNHkgLIkcY+IQbm8YRekds0XCqDzqXdfZDgXbR65EWz+4T7aCxnoQGQPWvX+o1i481STt1azTh4eDWk
QwRodegCfD8QogOJgcl+Gn964EEVKICVujWAph7hOuhswUIrGxEgAVPh
```

Application related configuration will be applied within 15 minutes of adoption
Application data will appear on the WAN Edge Insights page within 1 hour of adoption

> Note: The same registration code works for all SRX WAN edge devices in this entire organization.

Then, add the Junos OS snippet to the device that you want to adapt. Here we used the console to the device:

```
Cli
edit

# paste your clip-board code
set system services ssh protocol-version v2
set system authentication-order password
set system login user mist class super-user
set system login user mist authentication encrypted-password
$6$lbRlryEtCTQde4fn$IlIA4RWxRaeigLHZjMDUXTtC3pQunhed6FoqPSy/nMcptW0QKbK3AG3Cmyl5Uhkx98
m94CpL0JDl3126dAOCe/
set system login user mist authentication ssh-rsa “ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDCkxhJEmDeyPXFVPoav3GS8E13LHM2MggNux8aXrt1omgQjjUVDHRerZ
7m7LzB21BMqyfqUXWjl74VdBh7pgdCiiAuwkN7AaCwTl/pXeuWn99kedfwqteiipRZAmdhv4Eh+rkmCZLDE6s/
ItmYfPUUbBPXykPiMQSh50OwBNHkgLIkcY+Iqbm8Yrekds0XCqDzqXdfZDgXbR65Ewz+4T7aCxnoQGQPWvX+o1
i481STt1azTh4eDWkQwRodegCfD8QogOJgcl+Gn964EEVKICVujWAph7hOuhswUIrGxEgAVPh/CVvlYm2pIJlb
sT8Zt4iXzieUmSt9IPGGiUTl9fp9kIZP6VnR9l1IZ9rJS8Cyp++IT+NiofWIV1ZCrhw+w7P2qtWSubq5vYMAPa
20f0ihFX671T8AJ3CUwiDh/90oTrMDV4YWGtP2dsK+G5u5zz52nq54G3o0owmzEh8wLS8OqtdjbF2+v8adJBo5
27DXC2BRDZ4Os/zBNZItTJ7h1z0= mist@b4565781-c9c8-4613-ae34-57d6487a7f9”"
set system services outbound-ssh client mist device-id b4565781-c9c8-4613-ae34-
57d6487a7f91
set system services outbound-ssh client mist secret
74b0755eb367dd5a75cb7b592a0152c1e6ac8088cce50ea795b52b1a27bb2adef24436962c2c2fb10f2d5e
95845d4d95631f0f652e72178abffe1a337dc0b23e
set system services outbound-ssh client mist services netconf keep-alive retry 12
timeout 5
set system services outbound-ssh client mist oc-term.mist.net port 2200 timeout 60
retry 1000
delete system phone-home

commit and-quit
```

Run the following command to check if you’ve made a successful connection to the Juniper Mist cloud:

```
cli
show system connections | match 2200
tcp4       0      0  192.168.133.117.65094                          34.238.21.247.2200
ESTABLISHED
tcp4       0      0  192.168.133.117.64360                          52.6.66.225.2200
TIME_WAIT
```

## Restore Factory Default on a Failed Device

In case you encounter any issue with the onboarding process towards Juniper Mist cloud, we recommend that you load the factory default configuration and try again. The below steps highlight the process and give some tips on what to check.

**OPTIONAL:** If the device is in the cluster mode before, then you need to apply the following first to get it back into regular standalone mode followed by a zeroization of the device. This ensures that there is no previous configuration left on the device.

```
cli
set chassis cluster disable

For cluster-ids greater than 15 and when deploying more than one
cluster in a single Layer 2 BROADCAST domain, it is mandatory that
fabric and control links are either connected back-to-back or
are connected on separate private VLANS.

request system zeroize
yes
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no) yes

warning: zeroizing node0
```

```
.
# Device reboots here
.
.
# After the device is up again check that
cli
show chassis cluster status
error: Chassis cluster is not enabled.
```

The **regular device-reset** preparation method follows now.

```
cli
edit
load factory-default
delete chassis auto-image-upgrade
set system root-authentication plain-text-password

# we are adding the below as a best practice
set system name-server 8.8.8.8
set protocols lldp interface all
set protocols lldp-med interface all
set interfaces ge-0/0/0 unit 0 family inet dhcp force-discover
run clear dhcp server binding all
commit and-quit

# restart the local dhcpd to get a DHCP-lease
restart dhcp-service
Junos Dynamic Host Configuration Protocol process started, pid 3855

# now check that you got a lease and have a default route
show route

inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Access-internal/12] 00:00:31, metric 0
                    >  to 192.168.133.1 via ge-0/0/0.0
192.168.1.0/24     *[Direct/0] 00:07:47
                    >  via fxp0.0
192.168.1.1/32     *[Local/0] 00:07:47
                       Local via fxp0.0
192.168.2.0/24     *[Direct/0] 00:07:43
                    >  via irb.0
192.168.2.1/32     *[Local/0] 00:07:43
                       Local via irb.0
192.168.133.0/24   *[Direct/0] 00:00:31
                    >  via ge-0/0/0.0
192.168.133.117/32 *[Local/0] 00:00:31
                       Local via ge-0/0/0.0

# test you can ping a site in the internet
root> ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=53 time=5.371 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=5.175 ms

# test DNS working as well
root> ping www.google.com inet
PING www.google.com (142.251.32.36): 56 data bytes
64 bytes from 142.251.32.36: icmp_seq=0 ttl=112 time=24.966 ms
```

```
64 bytes from 142.251.32.36: icmp_seq=1 ttl=112 time=18.031 ms
64 bytes from 142.251.32.36: icmp_seq=2 ttl=112 time=9.661 ms
64 bytes from 142.251.32.36: icmp_seq=3 ttl=112 time=8.440 ms
```

**Check the device RTC-Clock!** When a device is  in stock for a longer time, the battery clock might get lost or screwed. Phone-Home ZTP (Juniper uses RFC 8071) checks the server certificate and with a clock set to year 1970 would not work.

```
# optional: set a local NTP server of this lab
cli
edit
set system ntp boot-server 216.239.35.0
set system ntp server 216.239.35.0
commit and-quit

# check current time else ZTP CA-Certificates may be rejected
show system uptime
Current time: 2020-01-08 14:16:34 UTC
.
.
# In case the date is below Year 2020 manually adjust the local time
# set date YYYYMMDDhhmm.ss
# or check if you already have enough connectivity to do that via our lab ntp
# set date ntp 216.239.35.0

restart phone-home-client
Phone home client daemon signaled but still running, waiting 28 seconds more
Phone home client daemon still running, sending another terminate signal
Phone home client daemon started, pid 7197
```

## Generic Workflows and Operations When Creating a Topology

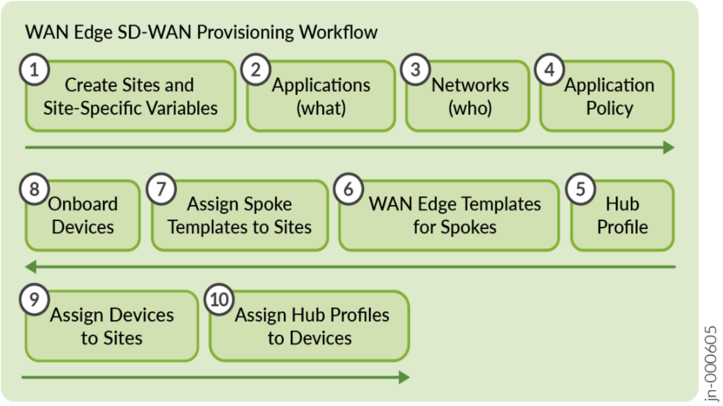
This overview illustrates how to use the Juniper Mist cloud console (the GUI) to provision a simple hub-and-spoke network using Juniper SRX Series Firewalls. Conceptually, you can think of the network as an enterprise with branch offices connecting over a provider WAN to on-premises data centers. Examples include an auto-parts store, a hospital, or a series of point-of-sale kiosks—anything that requires a remote extension of the corporate LAN for services such as authentication or access to applications.

We assume that before you begin configuring WAN Assurance in your sandbox, you have:

- Onboarded your hardware to the Juniper Mist cloud.
- Connected the cables  to support the configuration
- Interfaces and VLANs are valid for your sandbox.

Figure 9 illustrates the workflow for configuring WAN using the Juniper Mist cloud portal.

Figure 9: WAN Configuration Workflow


WAN Edge SD-WAN Provisioning Workflow
1 Create Sites and Site-Specific Variables
2 Applications (what)
3 Networks (who)
4 Application Policy
8 Onboard Devices
7 Assign Spoke Templates to Sites
6 WAN Edge Templates for Spokes
5 Hub Profile
9 Assign Devices to Sites
10 Assign Hub Profiles to Devices
jn-000605

The sequence of configuration tasks in this example is as follows:

1. Create Sites and Variables—Create a site for the hubs and spokes. Configure site variables for each site. You use these variables later in the templates for WAN edge devices and the hub profile.

2. Configure Applications—Applications are destinations that you define using IP prefixes. Applications represent traffic destinations.

3. Set Up Networks—Define the Networks. Networks are the source of traffic that is defined through IP prefixes.

4. Create Application Policies— Application policies determine which networks or applications you can access, and according to which traffic steering policy.

5. Create Hub Profiles—You assign hub profile to standalone or clustered devices to automate overlay path creation.

6. Create WAN Edge Templates—WAN edge templates automatically configure repetitive information such as an IP address, gateway, or VLAN when applied to sites.

7. Assign Spoke Templates to individual sites where they should be used.

8. Onboard Devices. The steps are explained in the chapter “Day-0 operation to claim/ZTP or adopt the SRX Series Devices towards Juniper Mist Cloud”.

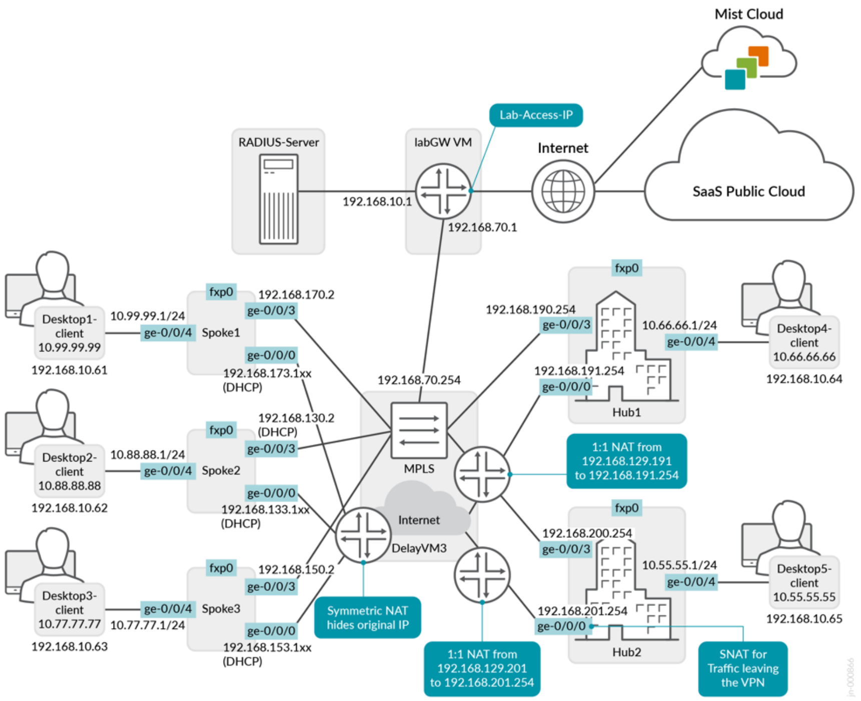
9. After the devices are onboarded and appear in the Juniper Mist cloud inventory, you need to assign them to an individual site.

10. Complete the onboarding by attaching hub profiles and spoke templates to the respective hub sites and spoke sites. This final step brings the topology together.

In the next chapter, we will show and use the entire process to build a first topology.

# Basic SD-WAN Topology with Three Spokes and Two Hubs (All Steps)

In this chapter, we will implement the first topology that we have discussed above and show you the entire workflow. Remember the Topology is a three Spoke and two Hub design.



# Configure Sites and Variables for SRX Series Firewalls

A site is a subset of your organization in the Juniper Mist cloud. You need a unique site for each physical (or logical) location in the network. You can configure and modify sites with required privileges. The configuration changes in the sites are automatically applied to (or at least available to) all the devices included in the site.

In addition, the Juniper SRX Series Firewall must have an Application Security license. AppSecure is a suite of application-aware security services that provides visibility and control over the types of applications traversing in the networks, which allows the Juniper Mist cloud to track and report applications passing through the device.

In this task, you also create site variables. Site variables provide simplicity and flexibility for deployment at a large scale. Site variables are configured on a per-site basis. When planning a network design, you can create standard templates for specific WAN edges devices and use variables in templates or the WAN edge configuration page.

Site variables provide a way to use tags (such as WAN1_PUBIP) to represent real values (such as 192.168.200.254) so that the value can vary according to the context where you use the variable. For example, for Site 1, you can define WAN1_PUBIP to be 192.168.200.254, while for Site 2 the value you give WAN1_PUBIP is 192.168.1.10. You can then use the tag to replace the IP address for Juniper Mist cloud configurations such as in the WAN edge template. That is, when you attach the template to different sites, Juniper Mist cloud uses the appropriate IP address automatically in each site when the configuration is rendered and pushed to the device.

You can also define entire IP subnets of the first three octets in variables, leaving minimal configuration at each device.

You can define the site variable by using double brackets to format the variable name. Example: {{SPOKE_LAN1_PFX}}

To configure sites:

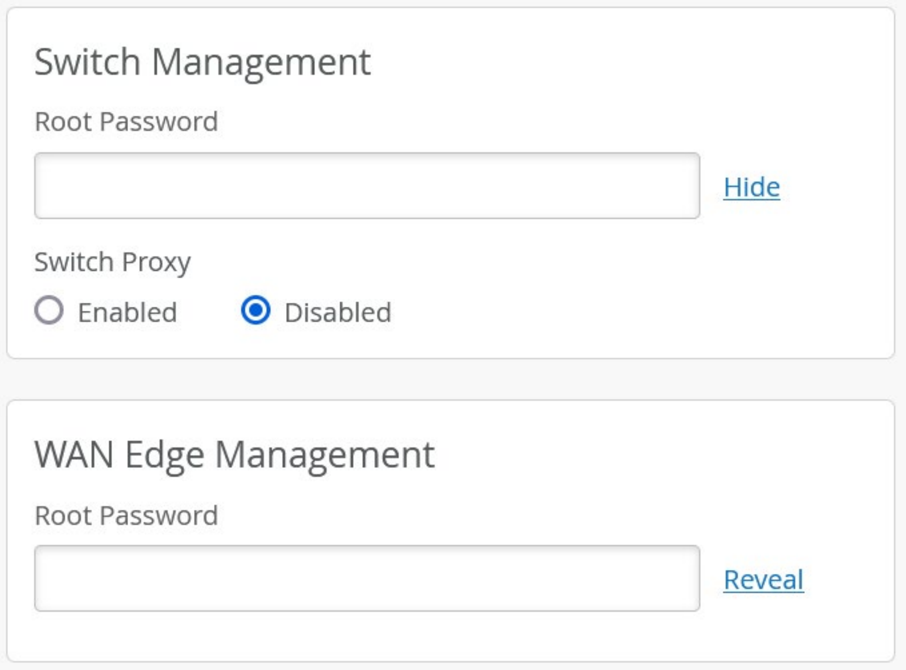
- In the Juniper Mist cloud portal, click **Organization** > **Admin** > **Site Configuration**.

  A list of existing sites, if any, appears.

- Click **Create Sites** in the upper-right corner. The New Site window appears.
  - Give the site a name. A Site ID is generated automatically. In this task, you create five sites (hub1-site, hub2-site, spoke1-site, spoke2-site, and spoke3-site).
  - Enter the street address of your site or use the map to locate it.

- Scroll down the page to the **Switch Management** and **WAN Edge Management** settings pane and configure the root password.

Figure 10: Setting Root Password



Switch Management

Root Password

Switch Proxy

○ Enabled ● Disabled

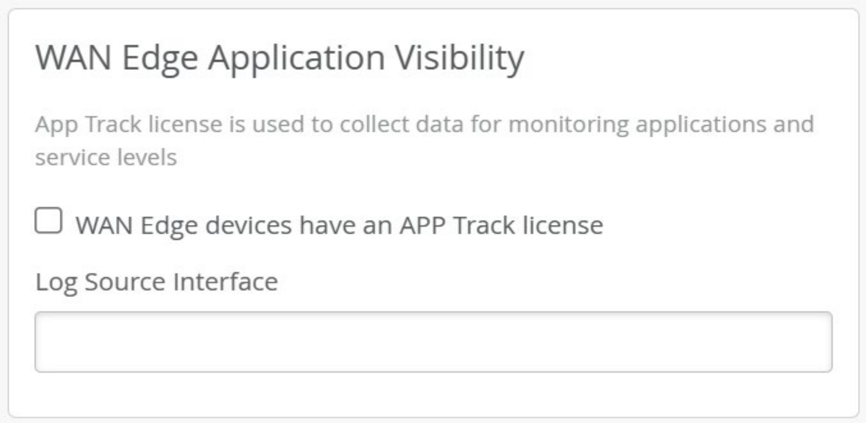
WAN Edge Management

Root Password

Ensure that you always set a root password for WAN edge devices and switches on the site. Otherwise, after you activate the device that Juniper Mist cloud manages, the system assigns a random root password for security reasons.

- Scroll down the page to the WAN Edge Application Visibility section, and then enable the WAN Edge devices that have an AppTrack license option.

Figure 11: Enable Application Visibility



WAN Edge Application Visibility

App Track license is used to collect data for monitoring applications and service levels

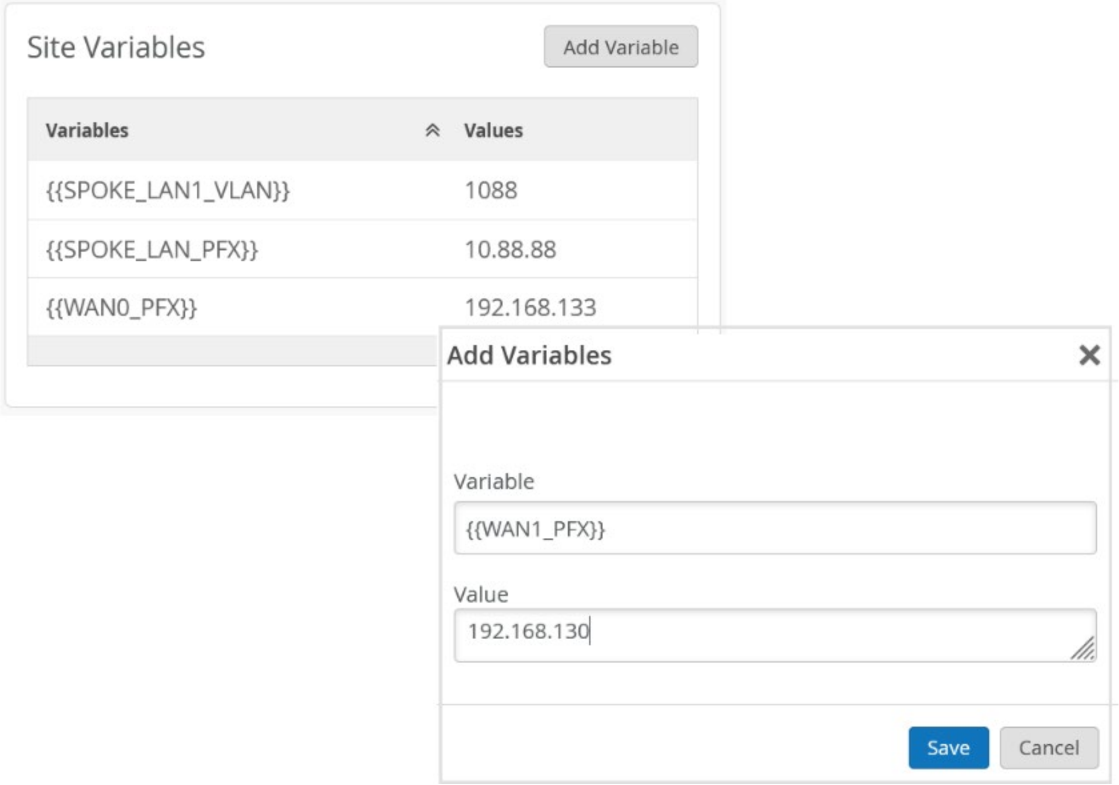
☐ WAN Edge devices have an APP Track license

Log Source Interface

**Note**: An application security license is mandatory for all (SD-WAN) SRX Series Firewall devices. Ensure that you have a valid license installed on the device.

- Scroll down the screen to the **Site Variables** settings pane.
    - Click **Add Variable**.
    - In the pop-up screen that appears, type a name for the variable and specify the value it represents.

Figure 12: Configuring Variables



Site Variables

| Variables | Values |
|---|---|
| {{SPOKE_LAN1_VLAN}} | 1088 |
| {{SPOKE_LAN_PFX}} | 10.88.88 |
| {{WAN0_PFX}} | 192.168.133 |

Add Variables

Variable: {{WAN1_PFX}}

Value: 192.168.130

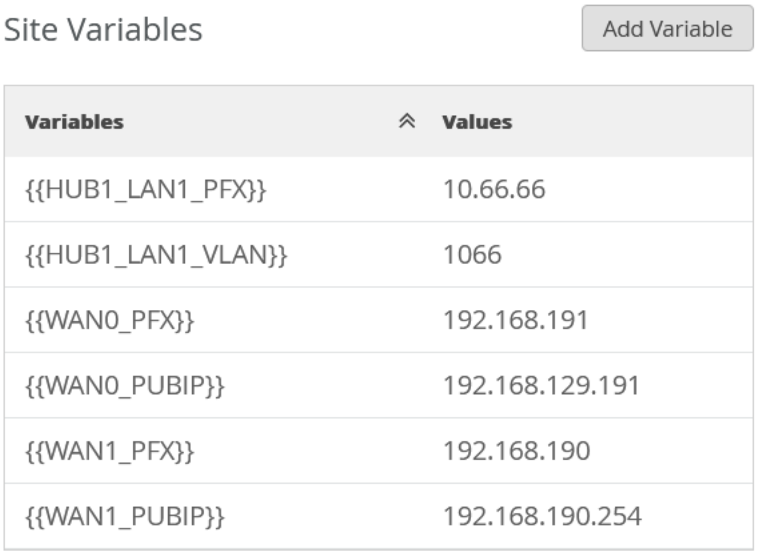
Table 1 shows the complete list of variables that you need to add.

Table 1: Variable Settings for Sites

| Site Name | Variable | Value |
|---|---|---|
| spoke1-site | {{SPOKE_LAN1_PFX}} | 10.99.99 |
| | {{SPOKE_LAN1_VLAN}} | 1099 |
| | {{WAN0_PFX}} | 192.168.173 |
| | {{WAN1_PFX}} | 192.168.170 |
| spoke2-site | {{SPOKE_LAN1_PFX}} | 10.88.88 |
| | {{SPOKE_LAN1_VLAN}} | 1088 |
| | {{WAN0_PFX}} | 192.168.133 |
| | **{{WAN1_PFX}}** | 192.168.130 |
| spoke3-site | {{SPOKE_LAN1_PFX}} | 10.77.77 |
| | {{SPOKE_LAN1_VLAN}} | 1077 |
| | {{WAN0_PFX}} | 192.168.153 |
| | {{WAN1_PFX}} | 192.168.150 |
| hub1-site | {{HUB1_LAN1_PFX}} | 10.66.66 |
| | {{HUB1_LAN1_VLAN}} | 1066 |
| | {{WAN0_PFX}} | 192.168.191 |
| | {{WAN1_PFX}} | 192.168.190 |
| | {{WAN0_PUBIP}} | 192.168.129.191 |
| | {{WAN1_PUBIP}} | 192.168.190.254 |
| hub2-site | {{HUB2_LAN1_PFX}} | 10.55.55 |
| | {{HUB2_LAN1_VLAN}} | 1055 |
| | {{WAN0_PFX}} | 192.168.201 |
| | {{WAN1_PFX}} | 192.168.200 |
| | {{WAN0_PUBIP}} | 192.168.129.201 |
| | {{WAN1_PUBIP}} | 192.168.200.254 |

- The variables such as {{SPOKE_LAN1_PFX}}, {{HUB1_LAN1_PFX}}, {{HUB2_LAN1_PFX}}, {{WAN0_PFX}} and {{WAN1_PFX}} represent first three octets of an IP address or a prefix.
- The variables such as {{SPOKE_LAN1_VLAN}}, {{HUB1_LAN1_VLAN}}, {{HUB2_LAN1_VLAN}} contain the individual VLAN IDs. In this example, use VLAN tagging to break up the broadcast domain and separate the traffic.
- The variables {{WAN0_PUBIP}} and {{WAN1_PUBIP}} defined for the WAN interfaces of hubs use the public IP address:
  - The IP address of interfaces on the Internet path is in 192.168.129.x format. You can set up Network Address Translation (NAT) rules for the interface.
  - The IP address of interfaces on the MPLS path is 192.168.x.254.
  - Use the /24 subnet mask and do not create a variable for this field.
- For the remaining fields, use the default values except for when you define your site variables.
- Click **Save** to add the variable to the list.

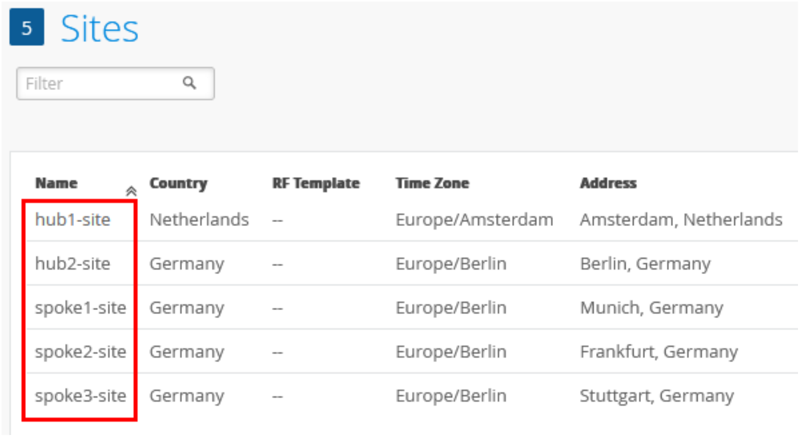
Figure13: Site Variables Sample



| Variables | Values |
|---|---|
| {{HUB1_LAN1_PFX}} | 10.66.66 |
| {{HUB1_LAN1_VLAN}} | 1066 |
| {{WAN0_PFX}} | 192.168.191 |
| {{WAN0_PUBIP}} | 192.168.129.191 |
| {{WAN1_PFX}} | 192.168.190 |
| {{WAN1_PUBIP}} | 192.168.190.254 |

You should now have five new sites created with variables for each so that the Template you apply later have their individual changes known.

Figure 14: Newly Created Sites



| Name | Country | RF Template | Time Zone | Address |
|---|---|---|---|---|
| hub1-site | Netherlands | -- | Europe/Amsterdam | Amsterdam, Netherlands |
| hub2-site | Germany | -- | Europe/Berlin | Berlin, Germany |
| spoke1-site | Germany | -- | Europe/Berlin | Munich, Germany |
| spoke2-site | Germany | -- | Europe/Berlin | Frankfurt, Germany |
| spoke3-site | Germany | -- | Europe/Berlin | Stuttgart, Germany |

# Configure Applications for SRX Series Firewalls

**Applications** represent traffic destinations. On Juniper SRX Series Firewall, applications determine the destination used in a security policy.

Applications are the services or apps that your network users connect to in a Juniper Mist WAN Assurance design. You can define these applications manually in the Juniper Mist cloud portal. You define applications by selecting the category (such as Social Media) or selecting individual applications (such as Microsoft Teams) from a list. Another option is to use the predefined list of common traffic types. You can also create a custom application to describe anything that is not otherwise available.

For users to access applications, you must first define the applications and then use application policies to permit or deny access. That is, you associate these applications with users and networks and then assign a traffic steering policy and access rule (allow or deny).

To configure applications:

- In the Juniper Mist cloud portal, click **Organization** > **WAN**> **Applications**. A list of existing applications, if any, appears.
- Click **Add Applications** in the upper-right corner. The **Add Application** window appears.

Note: SRX Series Firewall has many other ways to define applications. In this chapter, we will introduce and use applications that are identified by **IP address destination prefixes**. Those will leverage the custom application option for configuration. This is to introduce you to what the minimum requirements for a VPN are. We are going to extend and explain the applications configurations deeper in another chapter.

### Define Custom Applications with IP Prefixes Only

Juniper Mist cloud enables you to define your own custom applications with destination IP addresses or domain names.

When defining custom applications, you can:

- Use multiple destination IP addresses or domain names separated by a comma to define a single application.
- Select a protocol (any, TCP, UDP, ICMP, GRE, or custom) and port range to narrow down your selection. This option enables the system to identify the destination at a granular level.
- Define a prefix of 0.0.0.0/0 with protocol "any". A prefix of 0.0.0.0/0 with protocol "any", is resolved to *any host* within the Juniper Mist WAN Assurance policy. Now, w **only uses applications defined as IP-prefixes.**

To define the custom applications with IP prefixes for this Lab:

- In the Juniper Mist cloud portal, under the **Add Application** pane, select the **Type** as **Custom Apps**.
- Create a custom application using IP prefixes. For more information, see Use IP prefixes when configuring applications. Ensure that you keep the configuration separate for applications and application identification (which might be required at a later stage).

Table 3: Custom Application Configuration

| Custom Application | IP Address | Description |
|---|---|---|
| ANY | 0.0.0.0/0 | A wild card IP address. The IP address 0.0.0.0 also serves as a placeholder address. |
| SPOKE-LAN1 | 10.0.0.0/8 | A match criterion for all IP addresses inside the corporate VPN. |
| HUB1-LAN1 | 10.66.66.0/24 | A match criterion for all IP addresses attached at the LAN-interface of the Hub1 device. |
| HUB2-LAN1 | 10.55.55.0/24 | A match criterion for all IP addresses attached at the LAN interface of the Hub2 device. |

**Tip**: The Juniper Mist cloud portal assigns an IP address directly or indirectly to all LAN interfaces of hubs and spokes. In the beginning, you may use only few IP prefixes such as 10.77.77.0/24 + 10.88.88.0/24 + 10.99.99.0/24. You might want to create a custom application for these addresses only. But at a later stage, you might have many more interfaces. So, as a good practice, create applications with a wildcard match criteria IP prefix (such as 10.0.0.0/8). A wildcard match allows easy extensions without a need to change the ruleset in your environment.

- Click **Save**. The **Applications** page displays the list of all applications you created.

# Configure Networks for SRX Series Firewalls

Networks are sources of the request in your Juniper WAN Assurance design. On the Juniper SRX Series Firewall, networks create address books used as the source for security policies and advanced policy-based routing (APBR) policies.

Networks enable you to define groups of users. In a WAN design, you need to identify the sources accessing your applications over the LAN segment and set up the users. Users are source addresses, which you can use later in the application policies.

Once you have created networks in the Juniper Mist cloud portal, you can use networks across the entire organization in the portal. WAN Assurance design uses networks as the source in the application policy.

To configure networks:

1. In the Juniper Mist cloud portal, click **Organization** > **WAN** > **Networks**.
   A list of existing networks, if any, appears.

2. Click **Add Networks** in the upper-right corner.
   The **Add Network** window appears. Table 2 summarizes the options you can set in a network.

Table 2: Network Options

| Fields | Description |
|---|---|
| Name | Enter a unique name for the network. The name can contain alphanumeric characters, underscores, and hyphens, and must be less than 32 characters long. |
| Subnet IP Address | Enter the network IP address. You can either use absolute values (example: 192.0.2.0) or use variables (example:{{SPOKE_LAN1_PFX}}.0). |
| Prefix Length | Enter the length of the address prefix, from 0 through 32. You can also use variables for prefix length. Example: {{PFX1}} |
| VLAN ID | (Optional) Enter the VLAN ID that is associated with the network.<br>If your device is using an untagged interface, you should use 1 as the VLAN ID instead of the variable. |
| Source NAT Pool Prefix | (Optional) Enter IPv4 prefix for source NAT. Source NAT translates the source IP address of the traffic (which is a private IP address), to a public IP address. |
| Access to Mist Cloud | Check the option to allow services on SRX Series Firewalls to access the Juniper Mist cloud. |
| Advertised via Overlay | Check the option to advertise the network to the hub devices through the overlay tunnels. This option announces the network through iBGP. The IP Address |

| Fields | Description |
|---|---|
| | and Prefix Length fields below the option are filled in automatically. |
| Users | (Optional) Additional networks or users. Example: remote networks or users connected to the main network.<br>Click the **Add User** option and enter the **Name** and **IP Prefix** of the additional user. |
| Static NAT | (Optional) Perform a one-to-one static mapping of the original private host source address to a public source address. |
| Destination NAT | (Optional) Translate the destination IP address of a packet. |

3. Complete the configuration according to the details available in **Table 3**.
   In this task, you use the variables for both the subnet IP address and prefix length fields to configure three networks: SPOKE-LAN1, HUB1-LAN1, and HUB2-LAN1.

Table 3: Network Configuration Example

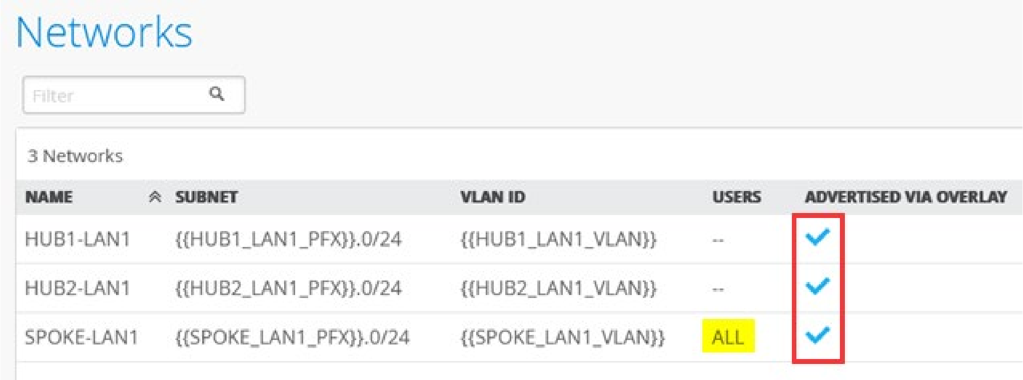
| Fields | Network 1 | Network 2 | Network 3 |
|---|---|---|---|
| Name | SPOKE-LAN1 | HUB1-LAN1 | HUB2-LAN1 |
| Subnet IP Address | {{SPOKE_LAN1_PFX}}.0 | {{HUB1_LAN1_PFX}}.0 | {{HUB2_LAN1_PFX}}.0 |
| Prefix Length | 24 | 24 | 24 |
| VLAN ID | {{SPOKE_LAN1_VLAN}} | {{HUB1_LAN1_VLAN}} | {{HUB2_LAN1_VLAN}} |
| Access to Mist Cloud | Checked | Checked | Checked |
| Advertised via Overlay | Checked | Checked | Checked |
| Users | **Name**=All<br>IP-Prefixes=10.0.0.0/8 | - | - |

Note: The user "All" with IP prefix 10.0.0.0/8 serves as a wildcard for all the future LAN segments in the range. The SRX Series Firewall in hubs can use the same username (All) and IP prefix (10.0.0.0/8) to identify all spoke LAN interfaces using a single rule.

Note: When you use variables, do not assume that the system imports all LAN segments on the hub site automatically if you forgot to set a variable at a certain site. When a variable is used but do not define the system might apply an Any netmask, which has a wide scope and may generate security issues.

Figure 15 shows you the list of newly created networks.

Figure 15: Networks Summary



Networks

3 Networks

| NAME | SUBNET | VLAN ID | USERS | ADVERTISED VIA OVERLAY |
|---|---|---|---|---|
| HUB1-LAN1 | {{HUB1_LAN1_PFX}}.0/24 | {{HUB1_LAN1_VLAN}} | -- | ✓ |
| HUB2-LAN1 | {{HUB2_LAN1_PFX}}.0/24 | {{HUB2_LAN1_VLAN}} | -- | ✓ |
| SPOKE-LAN1 | {{SPOKE_LAN1_PFX}}.0/24 | {{SPOKE_LAN1_VLAN}} | ALL | ✓ |

Remember that we used variables to use later only a few Templates. It is not recommended to create a template with individual hardcoded values for each site even if it's technically possible.

# Configure Application Policies on SRX Series Firewalls

Application policies are security policies in Juniper WAN Assurance design, where you define which network and users can access which applications, and according to which traffic steering policy. To define application policies, you must create networks, applications, and traffic steering profiles. You then use these details as matching criteria to allow access to or block access from applications or destinations.

In the Juniper Mist cloud portal, the **Networks or Users** setting determines the source zone. The **Applications** + **Traffic Steering** setting determines the destination zone. Traffic steering paths determine the destination zone in Juniper Networks SRX Series Firewalls, so ensure that you assign traffic steering profiles to the application policies.

Notes about the application policies:

- You can define application policies in one of three ways: at the organization-level, inside a WAN edge template, or inside a hub profile.
- When you define an application policy at the organization-level, you can import and use the policy in multiple WAN edge templates or in hub profiles. That is, you can follow the "define once, use multiple times" model.
- When you define an application policy directly inside a WAN edge or hub profile, the scope of the policy is limited to that WAN edge template or hub profile only. You cannot re-use the policy in other templates or profiles.
- Mist evaluates and applies policies in the order of their appearance in the policies list.

## Configure Application Policies

To configure application policies:

1. In the Juniper Mist cloud portal, select **Organization** > **WAN** > **Application Policy** to create a policy at the organization-level.

   If you want to create the policy at a WAN edge template or at a hub profile level, select **Organization** > **WAN** > **WAN Edge Templates** or **Hub Profile** and select the required template or profile.

2. Scroll down to the Application Policies section and click **Add Application Policy**.

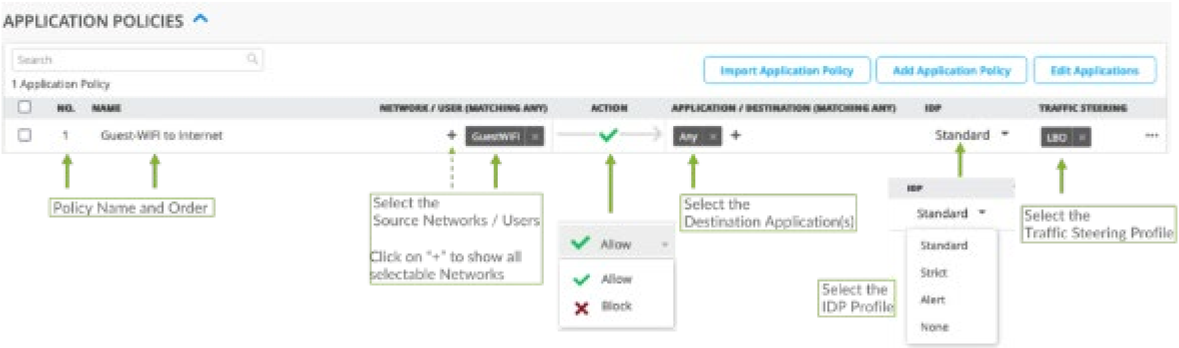
**Note**: You can import a global policy into the WAN edge template or hub profile by clicking the **Import Application Policy** option.

The Juniper Mist cloud portal displays the imported policies in gray to differentiate from local policies defined in the template or profile.

3. Click the new field under the **Name** column, give the policy a name, and then click the blue tick icon to apply your changes.

**Figure 16** shows the options that are available to you when you configure an application policy.

Figure 16: Application Policy Configuration Options



APPLICATION POLICIES

1 Application Policy

| □ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| □ | 1 | Guest-WiFi to Internet | + GuestWiFi | ✓ | Any + | Standard | LBO |

Search
Import Application Policy
Add Application Policy
Edit Applications
Policy Name and Order
Select the Source Networks / Users
Click on "+" to show all selectable Networks
Allow
Allow
Block
Select the Destination Application(s)
IDP
Standard
Standard
Strict
Alert
None
Select the IDP Profile
Select the Traffic Steering Profile

The following table explains the configuration options available for an application policy.

Table 6: Application Policies Options

| Field | Description |
|---|---|
| No. | Abbreviation for *number*. This entry indicates the position of the application policy. Mist evaluates and applies policies by their position, meaning the order in which they are listed in this field. |
| Name | Name of the application policy. You can use up to 32 characters for naming the application including alphanumerics, underscores, and dashes. |
| Network/User | Networks and users of the network. Networks are sources of the request in your network. You can select a network from the available list of networks. If you have associated a user to the network, the Juniper Mist cloud portal displays the detail as ***user.network*** format in the drop-down menu. |

| Field | Description |
|---|---|
| Action | Policy actions. Select one of these policy actions:<br>- Allow<br>- Block |
| Application / Destination | Destination end point. Applications determine the destinations used in a policy.<br>You can select applications from the list of already defined applications. |
| IDP | (Optional) Intrusion Detection and Prevention (IDP) profiles. Select one of the IDP profiles:<br>- **Standard**—Standard profile is the default profile and represents the set of IDP signatures and rules recommended by Juniper Networks. The actions include:<br>  - Close the client and server TCP connection.<br>  - Drop current packet and all subsequent packets<br>- **Strict**—Strict profile contains a similar set of IDP signatures and rules as the standard profile. However, when the system detects an attack, profile actively blocks any malicious traffic or other attacks detected in the network.<br>- **Alert**—Alert profile generates alert only and does not take any additional action. Alerts profiles are suitable only for low severity attacks. The IDP signature and rules are the same as in the standard profile.<br>- **None**—No IDP profile applied.<br>The IDP profile that you apply in your application policy performs traffic inspection to detect and prevent intrusions on the allowed traffic. |
| Traffic Steering | Traffic steering profiles. Traffic steering profile defines the traffic path or paths.<br>Steering profiles are required for deploying the policy to the WAN edge spoke device or to a hub device. |

> Note: The No. (order number) and Traffic Steering fields are not available for organization-level application policies. When you define an application policy directly inside a WAN edge or hub profile, you need to specify the order number and traffic steering options.

4. Complete the configuration according to the details available in the following Table:

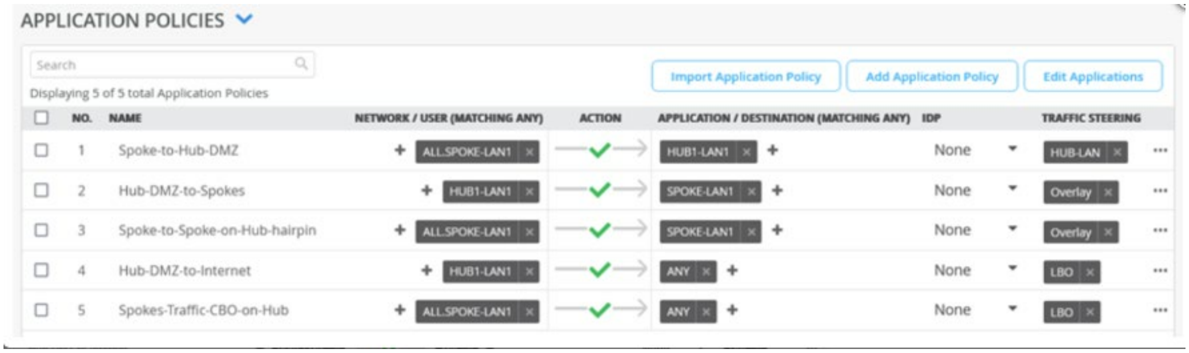
Table 7: Application Policy Examples

| S.No. | Rule Name | Network | Action | Destination | Steering |
|---|---|---|---|---|---|
| 1 | Spoke-to-Hub-DMZ | ALL.SPOKE-LAN1 | Pass | HUB1-LAN1 | HUB-LAN |
| 2 | Hub-DMZ-to-Spokes | HUB1-LAN1 | Pass | SPOKE-LAN1 | Overlay |
| 3 | Spoke-to-Spoke-on-Hub-Hairpin | ALL.SPOKE-LAN1 | Pass | SPOKE-LAN1 | Overlay |
| 4 | Hub-DMZ-to-Internet | HUB1-LAN1 | Pass | ANY | LBO |
| 5 | Spokes-Traffic-CBO-on-Hub | ALL.SPOKE-LAN1 | Pass | ANY | LBO |

5. Click **Save**.

The below Figure shows the list of newly created application policies.

Figure17: Application Policies Summary



APPLICATION POLICIES

Search

Displaying 5 of 5 total Application Policies

Import Application Policy | Add Application Policy | Edit Applications

| ☐ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| ☐ | 1 | Spoke-to-Hub-DMZ | ALL.SPOKE-LAN1 | ✓ | HUB1-LAN1 | None | HUB-LAN |
| ☐ | 2 | Hub-DMZ-to-Spokes | HUB1-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| ☐ | 3 | Spoke-to-Spoke-on-Hub-hairpin | ALL.SPOKE-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| ☐ | 4 | Hub-DMZ-to-Internet | HUB1-LAN1 | ✓ | ANY | None | LBO |
| ☐ | 5 | Spokes-Traffic-CBO-on-Hub | ALL.SPOKE-LAN1 | ✓ | ANY | None | LBO |

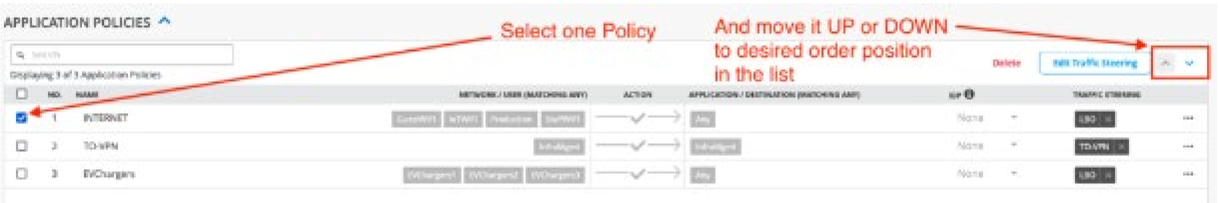
## Reorder and Delete Application Policies

Reordering application policy allows you to move the policies around after they are created.

Juniper Mist evaluates policies and executes policies in the order of their appearance in the policies list, you must know the following:

- Policy order is important. Because policy evaluation starts from the top of the list.
- New policies go to the end of the policy list.
- Select a policy and use Up Arrow or Down Arrow to change the order. You can change the policy order anytime.

Figure 18: Changing Policy Order



APPLICATION POLICIES ^

Select one Policy

And move it UP or DOWN to desired order position in the list

Displaying 3 of 3 Application Policies

Delete | Edit Traffic Steering

| ☐ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| ☑ | 1 | INTERNET | GuestWiFi, IoTWiFi, Production, StaffWiFi | ✓ | Any | None | LBO |
| ☐ | 2 | TO-VPN | InfraMgmt | ✓ | InfraMgmt | None | TO-VPN |
| ☐ | 3 | EVChargers | EVCharger1, EVCharger2, EVCharger3 | ✓ | Any | None | LBO |

To delete an application policy, select the application policy you want to delete, and then click **Delete** that appears on the upper-right side of the pane.

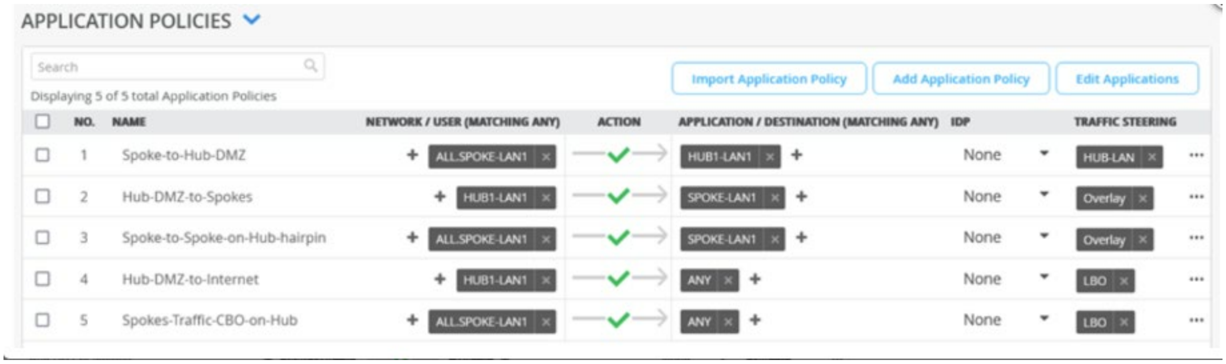
**Why Use the Same IP Prefixes in Networks and Applications?**

In the application policies configuration, **Network/Users** belong to the source zone, and **Applications/Destination** belong to the destination zone.

You can use the same IP addresses and prefixes for both networks and applications when you define them for different purposes; that is, they act as a source in one policy and as a destination in another policy.

Review the example below:

Figure 19: Application Policies Details



APPLICATION POLICIES

Search

Displaying 5 of 5 total Application Policies

Import Application Policy | Add Application Policy | Edit Applications

| ☐ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| ☐ | 1 | Spoke-to-Hub-DMZ | ALL.SPOKE-LAN1 | ✓ | HUB1-LAN1 | None | HUB-LAN |
| ☐ | 2 | Hub-DMZ-to-Spokes | HUB1-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| ☐ | 3 | Spoke-to-Spoke-on-Hub-hairpin | ALL.SPOKE-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| ☐ | 4 | Hub-DMZ-to-Internet | HUB1-LAN1 | ✓ | ANY | None | LBO |
| ☐ | 5 | Spokes-Traffic-CBO-on-Hub | ALL.SPOKE-LAN1 | ✓ | ANY | None | LBO |

Here, you have a **Network/Users** SPOKE-LAN1 that has an IP address 192.168.200.0/24 for a spoke LAN interface. The screenshot shows that the following policies are using the same network in different ways:

- **Spoke-to-Spoke-via-Hub**—This policy allows inbound and outbound spoke-to-spoke traffic through a hub. Here, we defined *SPOKE-LAN1* as both a network and as an application.
- **Spoke-to-Hub-DMZ**—This policy allows spoke-to-hub traffic. Here, we defined *SPOKE-LAN1* as a network.
- **Hub-DMZ-to-Spoke**—This policy allows hub-to-spoke traffic. Here, we defined *SPOKE-LAN1* as an application.

## Configure Hub Profiles for SRX Series Firewalls

Each hub device in a Juniper Mist cloud topology must have its own profile. Hub profiles are a convenient way to create an overlay and assign a path for each WAN link on that overlay in Juniper WAN Assurance.

The difference between a hub profile and a WAN edge template is that you apply the hub profile to an individual device that's at a hub site. And the WAN edge templates are bound to spoke sites that have multiple devices and bound with the same template across multiple sites. Every Hub WAN interface creates an overlay endpoint for spokes. Spoke WAN interfaces map the appropriate Hub WAN interfaces, defining the topology. Hub profiles drive the addition, removal of paths on your overlay.

When you create a hub profile for the Juniper Networks SRX Series Firewall, the Juniper Mist cloud generates and installs the SSL certificates automatically. It also sets up WAN uplink probes for failover detection.

In this task, you create a hub profile and then clone the same profile to create a second hub profile in the Juniper Mist cloud portal.

## Configure a Hub Profile

A hub profile comprises the set of attributes that associate with a particular hub device. Hub profiles include name, LAN, WAN, traffic steering, application policies, and routing options. You can assign the hub profile to a hub device and after a hub profile is loaded onto the site, the device assigned to the site picks up the attributes of that hub profile.

To configure a hub profile:

1. In the Juniper Mist cloud portal, click **Organization** > **WAN** > **Hub Profiles**.

   A list of existing profiles, if any, appears.

2. Click **Create Profile** in the upper right corner.
   - You can also create a hub profile by importing a JavaScript Object Notation (JSON file) using the **Import Profile** option.
   - Enter the name of the profile and click **Create**.

The table below summarizes the options you can set in a hub profile.

Table 8: Hub Profile Options

| Field | Description |
|---|---|
| Name | The profile name. Enter a unique name for the profile. The profile name can include up to 64 characters. Example: hub1. |
| NTP | IP address or hostname of the Network Time Protocol (NTP) server. NTP allows network devices to synchronize their clocks with a central source clock on the Internet. |
| Applies to Device | Site to associate the hub profile. The drop-down menu shows a list of the WAN edge devices available in the inventory of the current site. |
| DNS Settings | IP address or host name of Domain Name System (DNS) servers. Network devices use the DNS name servers to resolve hostnames to IP addresses. |

| Field | Description |
|---|---|
| Secure Edge Connectors | Secure Edge connector details. Secure Edge performs traffic inspection for the WAN edge devices that the Juniper Mist cloud portal manages. |
| WAN | WAN interface details. The hub profile uses these details to create an overlay endpoint for spokes. For each of the WAN links, you can define the physical interface, the type of WAN (Ethernet or DSL), the IP configuration, and the overlay hub endpoints for the interfaces. See WAN Interfaces. |
| LAN | LAN interface details. This section lists the hub side of the LAN interfaces that connect the hub to the LAN segment.<br>You assign the networks, create VLANs, and set up IP addresses and DHCP options (none, relay, or server).<br>See LAN Interfaces. |
| Traffic Steering | Steering paths. Define the different paths the traffic can take to reach its destination. For any traffic steering policy, you can include paths for traffic to traverse, as well as the strategies for utilizing those paths. See Traffic Steering policy. |
| Application Policies | Policies to enforce rules for traffic. Define network (source), application (destination), traffic steering policies, and policy action. See Application policies. |
| Routing | Routing options for routing traffic between the hub and spokes. You can s enable Border Gateway Protocol (BGP) underlay routing, where routes are learned dynamically or use static routing to define routes manually. |
| CLI Configuration | CLI configuration commands. If you want to configure settings that are not available in the template's GUI, you can configure them using CLI commands in the **set** format. |

3. Click **Save**.

## Add WAN Interfaces to the Hub Profile

Create WAN interfaces for the hub profile. WAN interfaces become the connection across the SD-WAN. The hub profile automatically creates an overlay endpoint for each WAN interface. Note that the overlay hub endpoints is where you tell the spoke (branch) about the hub endpoints.

To add WAN interfaces to the hub profile:

1. Scroll down to the WAN section and click **Add WAN** to open the Add WAN Configuration pane.

2. Complete the configurations according to the details provided below Table.

Table 9: WAN Interface Configuration

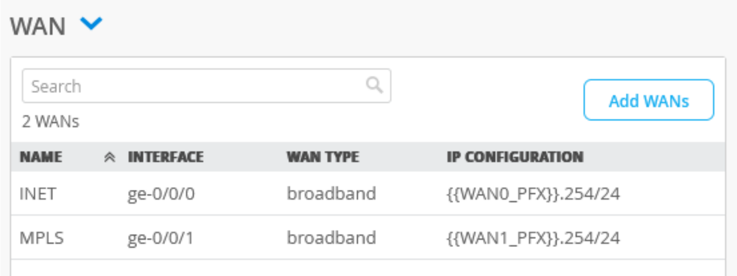
| Field | WAN Interface 1 | WAN Interface 2 |
|---|---|---|
| **Name** (a label and not a technology) | INET | MPLS |
| **Overlay Hub Endpoint** (generated automatically) | hub1-INET | hub1-MPLS |
| WAN Type | Ethernet | Ethernet |
| Interface | ge-0/0/0 | ge-0/0/1 |
| VLAN ID | - | - |
| IP Address | {{WAN0_PFX}}.254 | {{WAN1_PFX}}.254 |
| Prefix Length | 24 | 24 |
| Gateway | {{WAN0_PFX}}.1 | {{WAN1_PFX}}.1 |
| Source NAT | Check Interface. | Check Interface. |
| Override for Public IP | Check Override for Public IP.<br>Provide Public IP={{WAN0_PUBIP} } | Check Override for Public IP.<br>Provide Public IP={{WAN1_PUBIP} } |
| Public IP | {{WAN0_PUBIP}} | {{WAN1_PUBIP}} |

Note: Use Network Address Translation (NAT) along with advertising the public IP address unless the WAN address is a publicly routable address.

3. Click **Save**

The below shows the list of WAN interfaces you just have created.

Figure 20: Configured WAN Interfaces



WAN

Search

Add WANs

2 WANs

| NAME | INTERFACE | WAN TYPE | IP CONFIGURATION |
|---|---|---|---|
| INET | ge-0/0/0 | broadband | {{WAN0_PFX}}.254/24 |
| MPLS | ge-0/0/1 | broadband | {{WAN1_PFX}}.254/24 |

## Add a LAN Interface to the Hub Profile

Hub-side of LAN interfaces connect a hub device to the LAN segment.

To add a LAN interface to the hub profile:

1. Scroll down to the LAN section, click the **Add LAN** button to open the Add LAN Configuration pane.

2. Complete the configuration according to the details provided in the below table.

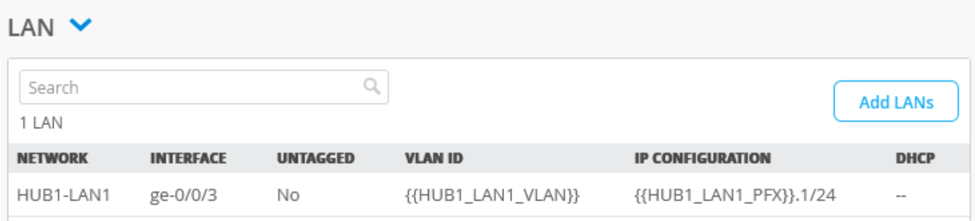
Table 10: LAN Interface Configuration

| Field | LAN Interface |
|---|---|
| Network | HUB1-LAN1 (existing network selected from drop-down list) |
| Interface | ge-0/0/4 |
| IP Address | {{HUB1_LAN1_PFX}}.1 |
| Prefix Length | 24 |
| Untagged VLAN | No |
| DHCP | No |

3. Click **Save**.

Figure 21 shows the LAN interface you created.

Figure 21: Configured LAN Interfaces



1 LAN

| NETWORK | INTERFACE | UNTAGGED | VLAN ID | IP CONFIGURATION | DHCP |
|---|---|---|---|---|---|
| HUB1-LAN1 | ge-0/0/3 | No | {{HUB1_LAN1_VLAN}} | {{HUB1_LAN1_PFX}}.1/24 | -- |

## Configure Traffic Steering Policies

Traffic steering is where you define the different paths that application traffic can take to traverse the network. The paths that you configure within traffic steering determine the destination zone. For any traffic steering policy, you need to define the paths for traffic to traverse and strategies for utilizing those paths. Strategies include:

- Ordered—Starts with a specified path and failover to backup path(s) when needed.
- Weighted—Distributes traffic across links according to a weighted bias, as determined by a cost that you input. (This option currently does not apply to SRX Series devices).
- Equal-cost multipath—Load balances traffic equally across multiple paths.

When you apply a hub profile to a device, the traffic steering policy determines the overlay, WAN and LAN interfaces, order of policies, and usage of Equal Cost Multi-Path (ECMP). The policy also determines how interfaces, or a combination of interfaces interact to steer the traffic.

To configure traffic steering policies:

1. Scroll down to the Traffic Steering section and click **Add Traffic Steering** to display the Traffic Steering configuration pane.

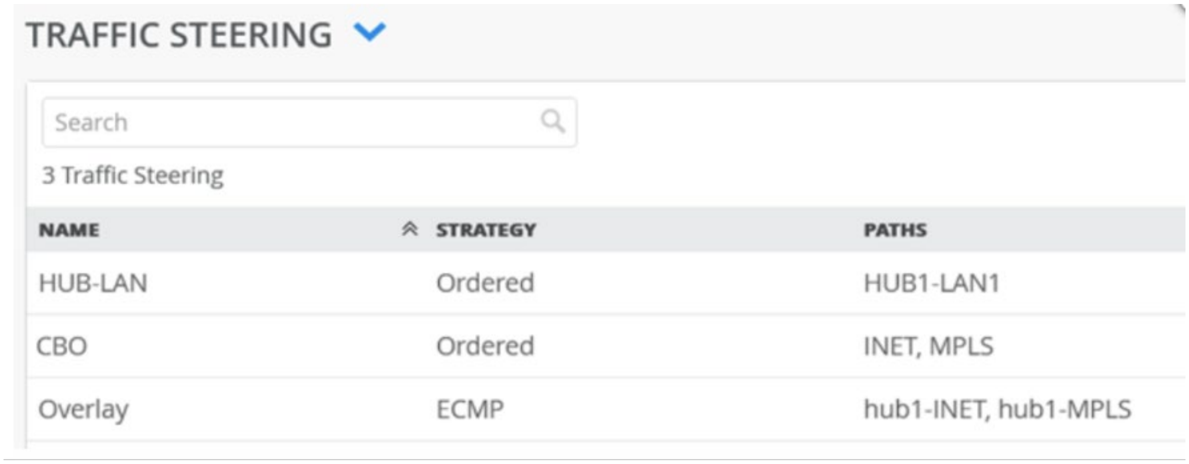
2. Configure three traffic steering policies: one for the overlay, one for the underlay, and one for the central breakout, according to the details provided in below table.

Table 11: Traffic Steering Policy Configuration

| Field | Traffic Steering Policy 1 | Traffic Steering Policy 2 | Traffic Steering Policy 3 |
|---|---|---|---|
| Name | Underlay (HUB-LAN) | Overlay | Central Breakout |
| Strategy | Ordered | ECMP | Ordered |
| **PATHS** For path types, existing LAN and WAN networks are made available for selection as endpoints. | **Type**—LAN<br>**Network** —HUB1-LAN1 | **Type**—WAN<br>**Network** —hub1-INET and hub1-MPLS | **Type**—WAN<br>**Network** —WAN: INET and WAN: MPLS |

The figure below shows the list of the traffic steering policies that you created.

Figure 22: Traffic Steering Policies



TRAFFIC STEERING

Search

3 Traffic Steering

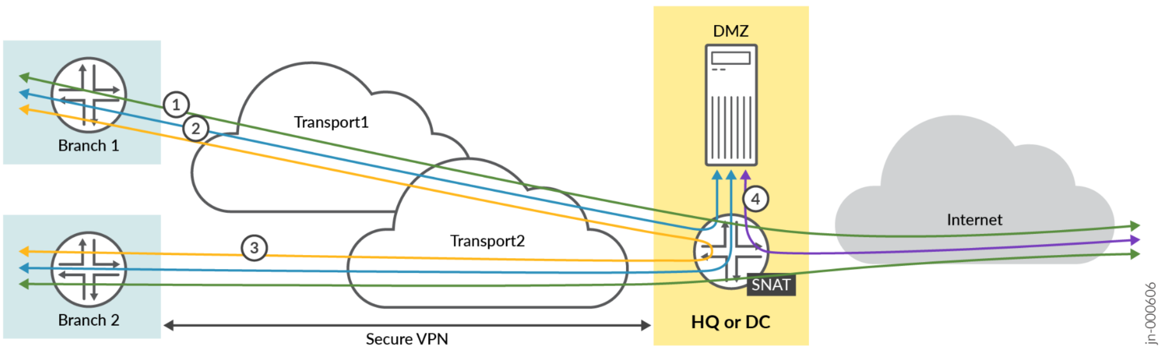
| NAME | STRATEGY | PATHS |
|---|---|---|
| HUB-LAN | Ordered | HUB1-LAN1 |
| CBO | Ordered | INET, MPLS |
| Overlay | ECMP | hub1-INET, hub1-MPLS |

## Configure an Application Policy

Application policies are where you define which network and users can access which applications, and according to which traffic steering policy. The settings in Networks/Users determine the source zone. The Applications and traffic steering path settings determine the destination zone. Additionally, you can assign a policy action— permit or deny to allow or block traffic. Mist evaluates and applies application policies in the order in which you list them in the portal. You can use Up Arrow and Down arrows to change the order of policies.

The figure below shows different traffic-direction requirements in this task. The image depicts a basic initial traffic model for a corporate VPN setup (third spoke device and second hub device are not shown).

Figure 23: Traffic-Direction Topology



In this task, you create the following application rules to allow traffic:

- Rule 1—From the spoke devices to the Internet directly (not passing through the hub device). In this rule, define the destination as "Any" with IP address 0.0.0.0/0. The traffic uses the WAN underlay interface with SNAT applied to reach IP addresses on the Internet as a local breakout. This method implements a central breakout at the hub for all spoke devices. This will be the last Policy in our below configuration as it is kind of a catch-up all rules.

- Rule 2-Needs later two Policies for implementing bidirectional traffic.
  - Allows traffic from spoke sites to reach the hub (and to a server in the DMZ attached to the hub device).
  - Allows traffic from servers in the DMZ attached to the hub to reach spoke devices.
- Rule 3—Allows traffic from spoke devices to reach spoke device hair-pinning through a hub device.
- Rule 4—Allows Internet-bound traffic from the hub device to the Internet (local breakout). In this rule, define the destination as "Any" with IP address 0.0.0.0/0. The traffic uses the WAN underlay interface with SNAT applied to reach IP addresses on the Internet as a local breakout.

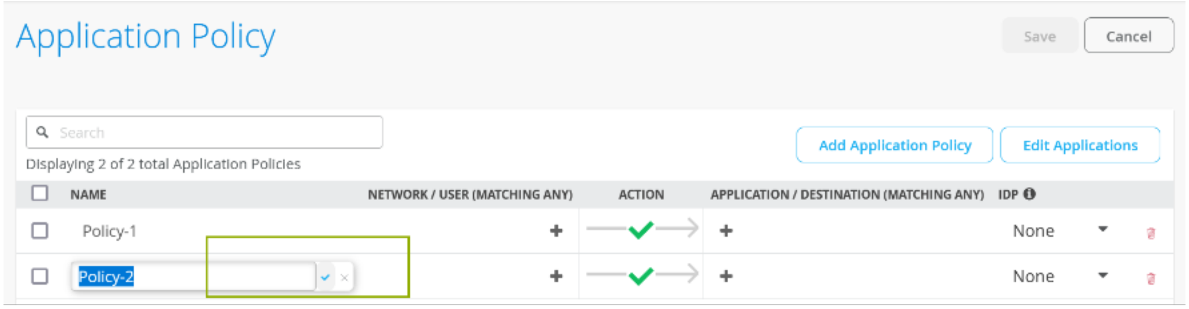
  **Note**: Avoid creating rules with same destination name and IP address 0.0.0.0/0. If required, create destinations with different names using IP address 0.0.0.0/0.

> Note1: For SRX Series Firewalls, you must associate a traffic steering policy to the application policy.
>
> Note2: The order of application policies in the policies list is very important for SRX Series Firewalls.

To configure an application policy:

- Scroll down to the **Application Policy** section, click **Add Policy** to create a new rule in the policy list.
- Click the **Name** column and give the policy a name, and then click the blue checkmark to apply your changes.

Figure 24: Adding a New Application Policy



Displaying 2 of 2 total Application Policies

| □ | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP |
|---|---|---|---|---|---|
| □ | Policy-1 | + | ✓ | + | None |
| □ | Policy-2 | + | ✓ | + | None |

- Create application rules according to the details provided in below Table

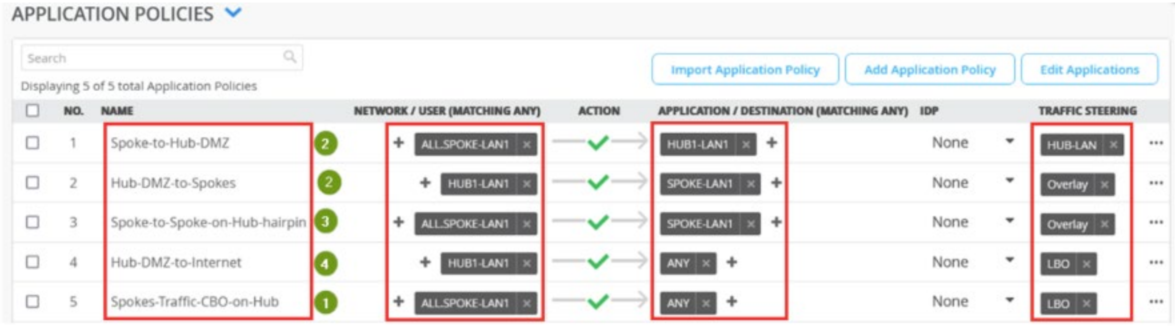
Table 12: Application Policy Rule Configuration

| No. (Policy Order) | Rule Name | Network | Action | Destination | Steering |
|---|---|---|---|---|---|
| 1 | Spoke-to-Hub-DMZ | ALL.SPOKE-LAN1 | Pass | HUB1-LAN1 | HUB-LAN |

| No. (Policy Order) | Rule Name | Network | Action | Destination | Steering |
|---|---|---|---|---|---|
| 2 | Hub-DMZ-to-Spokes | HUB1-LAN1 | Pass | SPOKE-LAN1 | Overlay |
| 3 | Spoke-to-Spoke-on-Hub-Hairpin | ALL.SPOKE-LAN1 | Pass | SPOKE-LAN1 | Overlay |
| 4 | Hub-DMZ-to-Internet | HUB1-LAN1 | Pass | ANY | LBO |
| 5 | Spokes-Traffic-CBO-on-Hub | ALL.SPOKE-LAN1 | Pass | ANY | LBO |

The below Figure shows a list of the application policies that you created.

Figure 25: Application Policy Summary



APPLICATION POLICIES

Search

Displaying 5 of 5 total Application Policies

| ☐ | NO. | NAME | | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | Spoke-to-Hub-DMZ | 2 | ALL.SPOKE-LAN1 | ✓ | HUB1-LAN1 | None | HUB-LAN |
| ☐ | 2 | Hub-DMZ-to-Spokes | 2 | HUB1-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| ☐ | 3 | Spoke-to-Spoke-on-Hub-hairpin | 3 | ALL.SPOKE-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| ☐ | 4 | Hub-DMZ-to-Internet | 4 | HUB1-LAN1 | ✓ | ANY | None | LBO |
| ☐ | 5 | Spokes-Traffic-CBO-on-Hub | 1 | ALL.SPOKE-LAN1 | ✓ | ANY | None | LBO |

In the above illustration, the green counter mark indicates the policies you have created for the traffic requirements in above Figure in relation to the original rules defined.

- OPTIONAL: Allow ICMP pings for debugging and for checking device connectivity.

  The default security configuration for SRX Series Firewalls does not allow ICMP pings from LAN device to the local interface of the WAN edge router. You might need to test connectivity before devices attempt to connect to the outside network. You allow ICMP pings for debugging and for checking device connectivity.

  On an SRX Series Firewall, you can use the following CLI configuration statement to allow pings to the local LAN interface for debugging.

```
set security zones security-zone HUB1-LAN1 host-inbound-traffic system-services ping
```

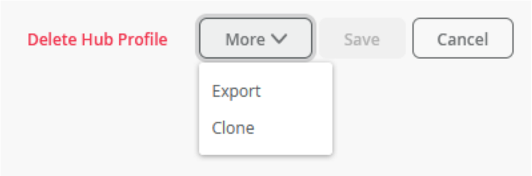
Create a Second Hub Profile by Cloning the Existing Hub Profile

Hub devices are unique throughout your network. You have to create an individual profile for each hub device. Juniper Mist enables you to create a hub profile by cloning the existing profile and applying modifications wherever required.

To create a second hub profile by cloning an existing hub profile:

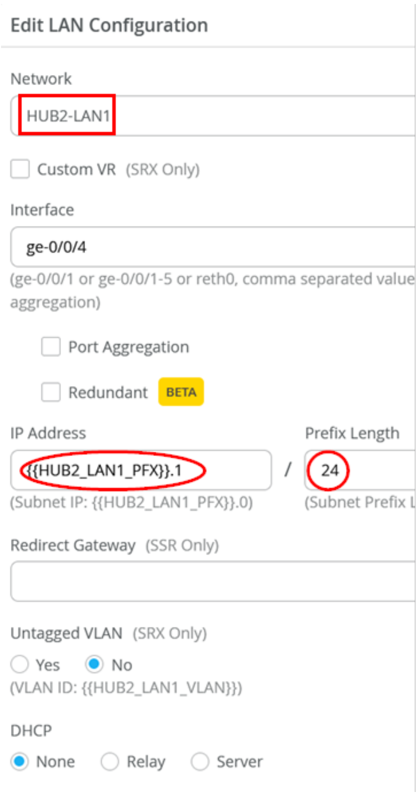
- In the Juniper Mist cloud portal, click **Organization** > **WAN** > **Hub Profiles**.
  - A list of existing hub profiles, if any, appears.
- Click the hub profile (example: hub1) that you want to clone. The profile page of the selected hub profile opens.
- In the upper right corner of the screen, click **More** and select **Clone**.

Figure26: Create a New Hub Profile By Using the Clone Option



- Name the new profile (example: hub2) and click **Clone**.
  - If you see any errors while naming the profile, refresh your browser.
- Start configuring the profile. Since you've used variables when creating the original hub profile, you don't need to configure all options from the beginning. You need to change only the required configurations to reflect HUB2 details. For example, change **Network** to **HUB2-LAN1** and change **IP Address** to **{{HUB2_LAN1_PFX}}.1**.

Figure27: Edit a Cloned Profile



Edit LAN Configuration

Network

HUB2-LAN1

☐ Custom VR (SRX Only)

Interface

ge-0/0/4

(ge-0/0/1 or ge-0/0/1-5 or reth0, comma separated value
aggregation)

☐ Port Aggregation

☐ Redundant BETA

IP Address / Prefix Length

{{HUB2_LAN1_PFX}}.1 / 24

(Subnet IP: {{HUB2_LAN1_PFX}}.0) (Subnet Prefix L

Redirect Gateway (SSR Only)

Untagged VLAN (SRX Only)

○ Yes ● No

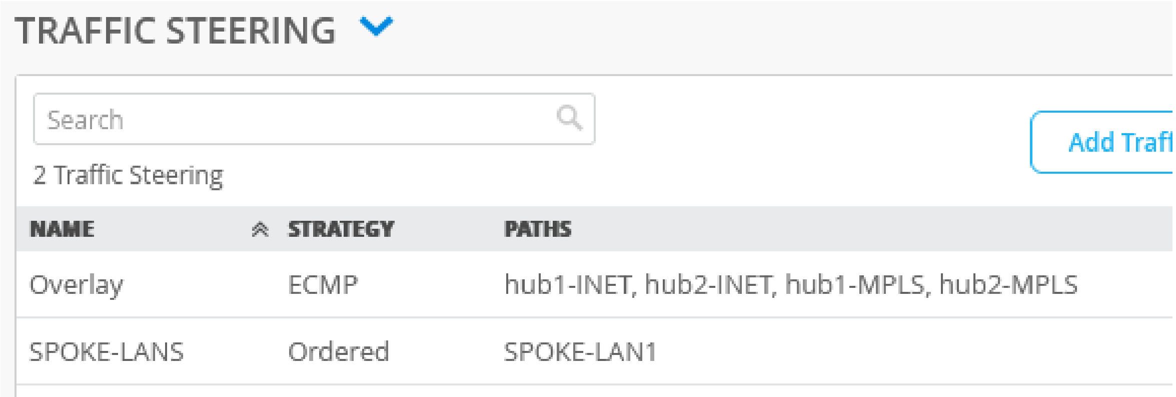
(VLAN ID: {{HUB2_LAN1_VLAN}})

DHCP

● None ○ Relay ○ Server

- Change the LAN interface to include HUB2. Example: HUB2-LAN1 and {{HUB2_LAN1_PFX}}.1
- Confirm that the variables in the configuration have changed to reflect hub2 profile details. Example: Overlay definitions have changed to hub2-INET and hub2-MPLS.

Figure28: Updated Traffic Steering Policy



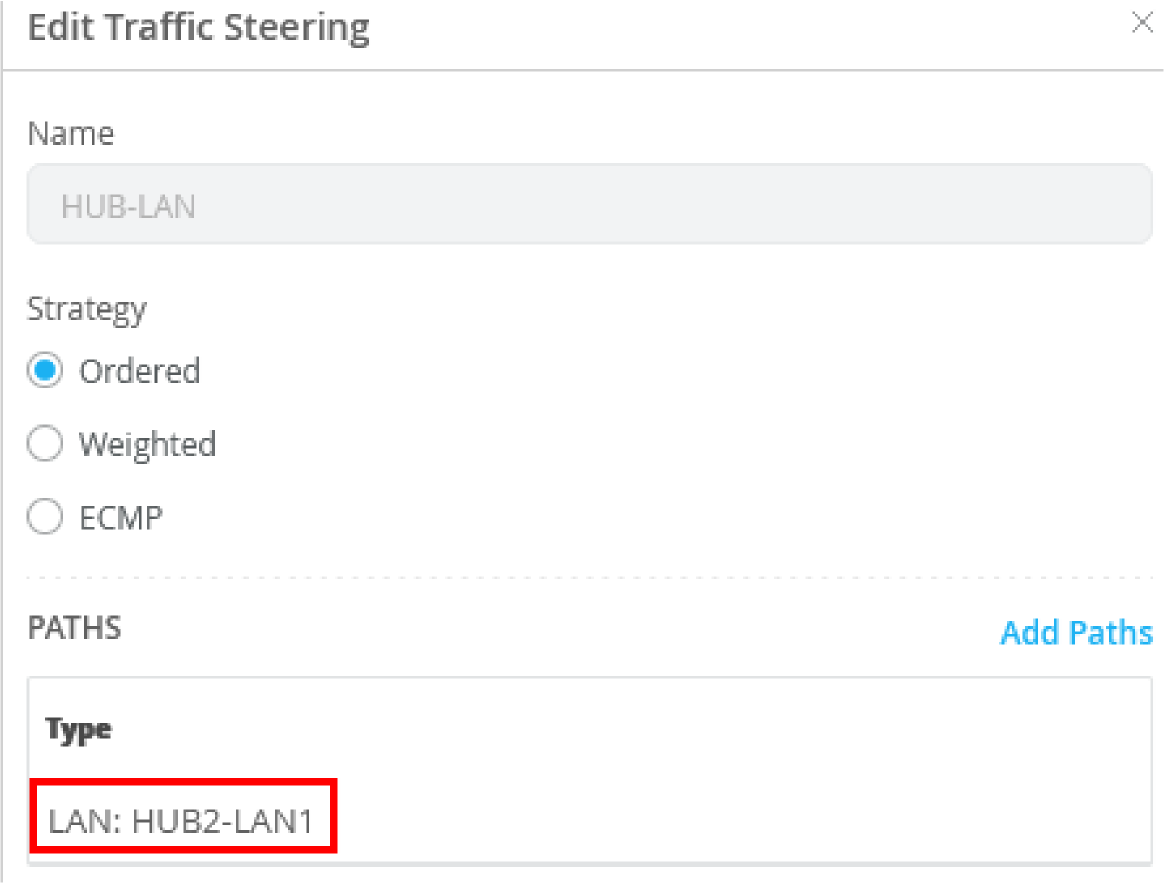
TRAFFIC STEERING

2 Traffic Steering

| NAME | STRATEGY | PATHS |
|---|---|---|
| Overlay | ECMP | hub1-INET, hub2-INET, hub1-MPLS, hub2-MPLS |
| SPOKE-LANS | Ordered | SPOKE-LAN1 |

- Scroll down to the TRAFFIC STEERING pane and edit the entry to change the **Paths** to LAN: HUB2-LAN1.

Figure29: Update Paths in a Traffic Steering Policy



Edit Traffic Steering

Name: HUB-LAN

Strategy
- ● Ordered
- ○ Weighted
- ○ ECMP

PATHS

Type: LAN: HUB2-LAN1

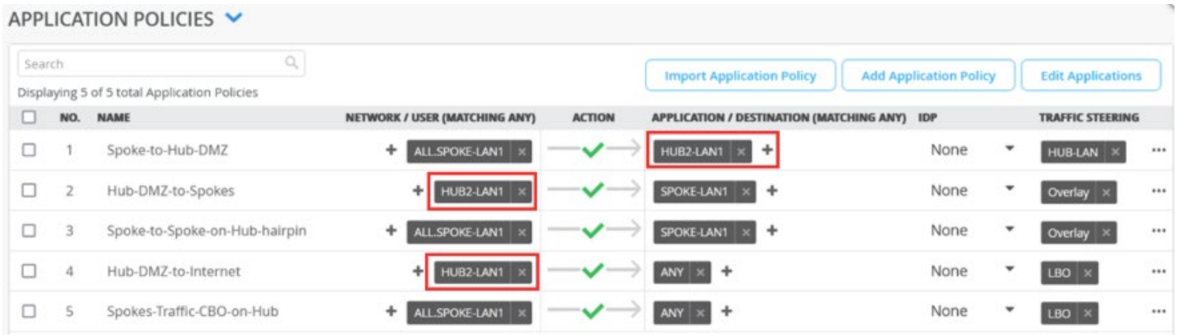
- Update the application rules according to the details provided in below Table. For example, wherever applicable, change HUB1-LAN to HUB2-LAN.

Table 13: Application Rules Configuration

| S.No. | Rule Name | Network | Action | Destination | Steering |
|---|---|---|---|---|---|
| 1 | Spoke-to-Hub-DMZ | ALL.SPOKE-LAN1 | Pass | HUB2-LAN1 | HUB-LAN |
| 2 | Hub-DMZ-to-Spokes | HUB2-LAN1 | Pass | SPOKE-LAN1 | Overlay |
| 3 | Spoke-to-Spoke-on-Hub-Hairpin | ALL.SPOKE-LAN1 | Pass | SPOKE-LAN1 | Overlay |
| 4 | Hub-DMZ-to-Internet | HUB2-LAN1 | Pass | ANY | LBO |
| 5 | Spokes-Traffic-CBO-on-Hub | ALL.SPOKE-LAN1 | Pass | ANY | LBO |

The Figure below shows the details of the updated application policies after you save your changes.

Figure30: Updated Application Policy Summary



APPLICATION POLICIES

Displaying 5 of 5 total Application Policies

| □ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| □ | 1 | Spoke-to-Hub-DMZ | ALL.SPOKE-LAN1 | ✓ | HUB2-LAN1 | None | HUB-LAN |
| □ | 2 | Hub-DMZ-to-Spokes | HUB2-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| □ | 3 | Spoke-to-Spoke-on-Hub-hairpin | ALL.SPOKE-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| □ | 4 | Hub-DMZ-to-Internet | HUB2-LAN1 | ✓ | ANY | None | LBO |
| □ | 5 | Spokes-Traffic-CBO-on-Hub | ALL.SPOKE-LAN1 | ✓ | ANY | None | LBO |

## 1.) Configure WAN Edge Templates for SRX Series Firewalls

The WAN edge template in Juniper Mist WAN Assurance enables you to define common spoke characteristics including WAN interfaces, traffic steering rules, and access policies. You then apply these configurations to the Juniper Networks SRX Series Firewall deployed as a WAN edge device. When you assign a WAN edge device to a site, the device automatically adopts the configuration from the associated template. This automatic process enables you to manage and apply consistent and standardized configurations across your network infrastructure, streamlining the configuration process.

You can have one or more templates for your spoke devices.

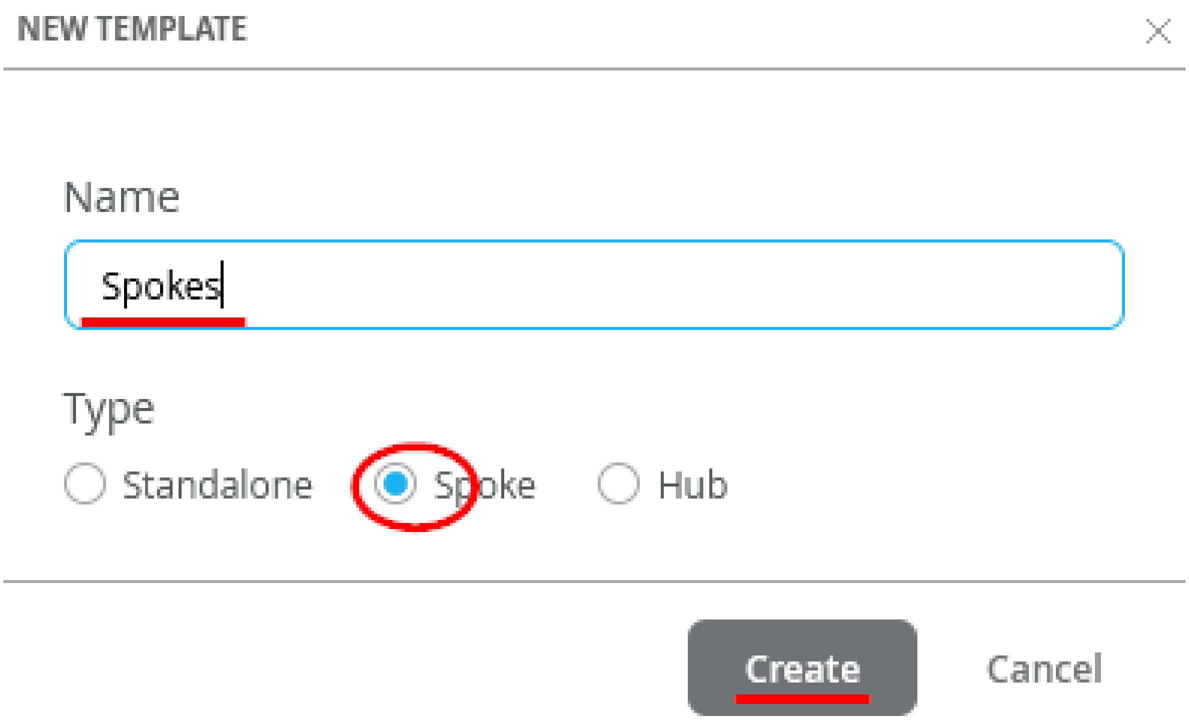
In this task, you create and configure a WAN edge template for a spoke device in the Juniper Mist cloud portal.

Configure a WAN Edge Template

To configure a WAN edge template:

- In the Juniper Mist portal, click **Organization** > **WAN** > **WAN Edge Templates**. A list of existing templates, if any, appears.
- Click the **Create Template** button in the upper right corner.
    - Note: You can also create a WAN edge template by importing a JavaScript Object Notation (JSON) file using the Import Profile option.
- In the box that appears, enter the name for the template, click **Type** and select Spoke, and then click **Create**.

Figure31: Select the Template Type



NEW TEMPLATE

Name

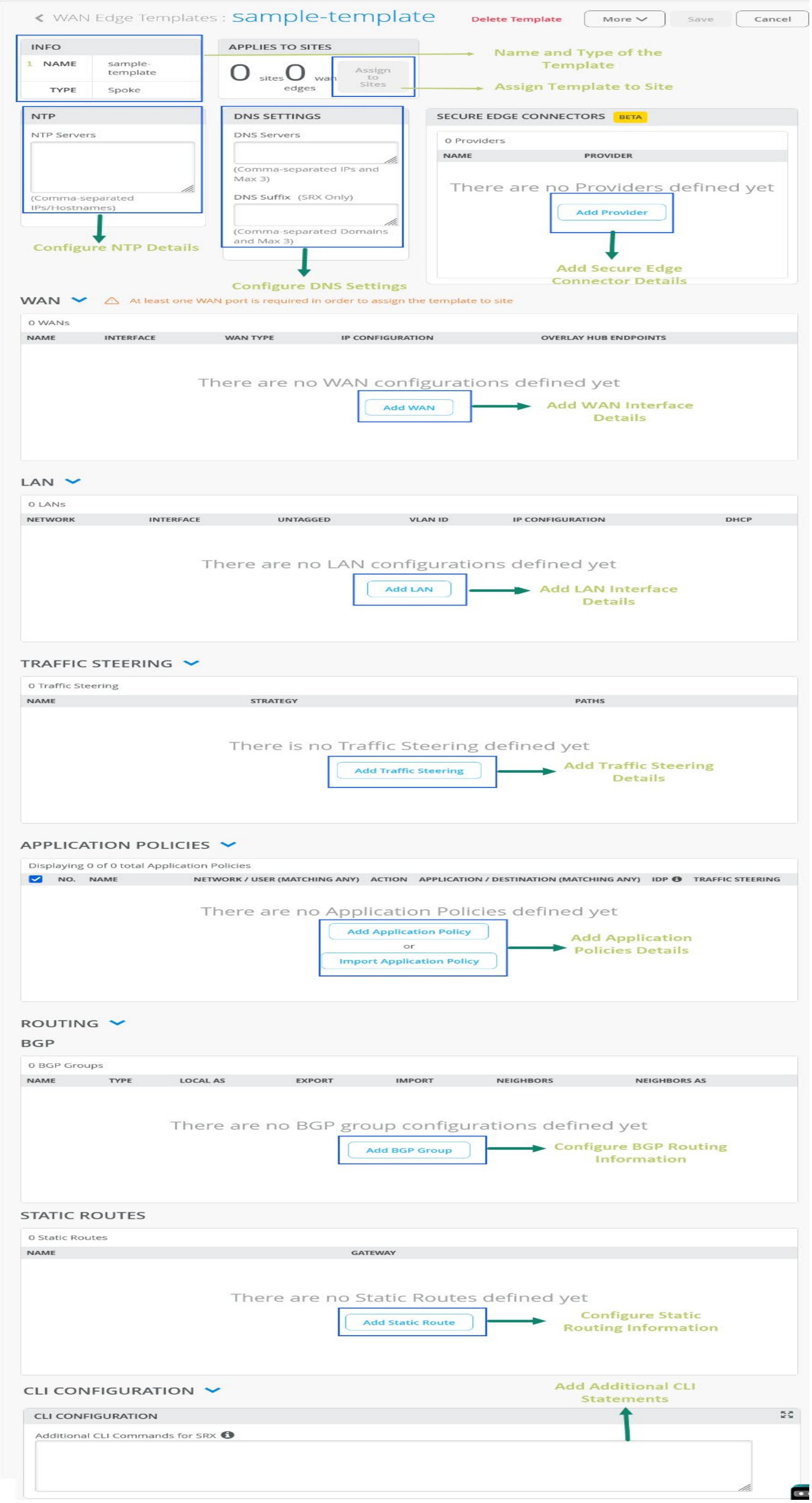
Spokes

Type

○ Standalone ● Spoke ○ Hub

Here's an illustration that shows the GUI elements on the WAN edge template configuration page.

Figure32: WAN Edge Template Configuration Options



INFO

| | |
|---|---|
| NAME | sample-template |
| TYPE | Spoke |

APPLIES TO SITES

0 sites 0 wan edges

Name and Type of the Template

Assign Template to Site

NTP

NTP Servers

(Comma-separated IPs/Hostnames)

Configure NTP Details

DNS SETTINGS

DNS Servers

(Comma-separated IPs and Max 3)

DNS Suffix (SRX Only)

(Comma-separated Domains and Max 3)

Configure DNS Settings

SECURE EDGE CONNECTORS BETA

0 Providers

| NAME | PROVIDER |
|---|---|

There are no Providers defined yet

Add Secure Edge Connector Details

WAN

⚠ At least one WAN port is required in order to assign the template to site

0 WANs

| NAME | INTERFACE | WAN TYPE | IP CONFIGURATION | OVERLAY HUB ENDPOINTS |
|---|---|---|---|---|

There are no WAN configurations defined yet

Add WAN Interface Details

LAN

0 LANs

| NETWORK | INTERFACE | UNTAGGED | VLAN ID | IP CONFIGURATION | DHCP |
|---|---|---|---|---|---|

There are no LAN configurations defined yet

Add LAN Interface Details

TRAFFIC STEERING

0 Traffic Steering

| NAME | STRATEGY | PATHS |
|---|---|---|

There is no Traffic Steering defined yet

Add Traffic Steering Details

APPLICATION POLICIES

Displaying 0 of 0 total Application Policies

| ☑ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|

There are no Application Policies defined yet

Add Application Policies Details

ROUTING

BGP

0 BGP Groups

| NAME | TYPE | LOCAL AS | EXPORT | IMPORT | NEIGHBORS | NEIGHBORS AS |
|---|---|---|---|---|---|---|

There are no BGP group configurations defined yet

Configure BGP Routing Information

STATIC ROUTES

0 Static Routes

| NAME | GATEWAY |
|---|---|

There are no Static Routes defined yet

Configure Static Routing Information

CLI CONFIGURATION

Add Additional CLI Statements

CLI CONFIGURATION

Additional CLI Commands for SRX

- Complete the configurations according to the details provided in below table.

Table 14: WAN Edge Profile Options

| Fields | Description |
|---|---|
| Name | Profile name. Enter a unique profile name with up to 64 characters. |
| Type | WAN edge profile type. Select one of the following options:<br>Standalone—To manage a standalone device in your site.<br>Spoke—To manage a spoke device that is connecting to a hub device in your configuration. |
| NTP | The IP address or hostname of the Network Time Protocol (NTP) server. NTP is used to synchronize the clocks of the switch and other hardware devices on the Internet. |
| Applies to Device | Site to associate the WAN edge template. The drop-down menu shows a list of the WAN edge devices that have been added to the inventory of the current site. |
| DNS Settings | IP address or host names of Domain Name System (DNS) servers. Network devices use the DNS name servers to resolve hostnames to IP addresses. |
| Secure Edge Connectors | Secure Edge connector details. Juniper Secure Edge performs traffic inspection for the WAN edge devices managed by Juniper Mist Cloud portal. |
| WAN | WAN interfaces details. This WAN interface corresponds to the WAN interface on hub. That is—Mist creates an IPsec VPN tunnel between WAN interface on the hub to WAN interface on the spoke. For each of the WAN links, you can define the physical interface, the type of WAN (Ethernet or DSL), the IP configuration, and the overlay hub endpoints for the interfaces. See WAN Interfaces. |
| LAN | LAN interfaces. LAN interfaces that connect the LAN segment. You assign the networks, create VLANs, and set up IP addresses and DHCP options (none, or relay, or server). See LAN Interfaces. |
| Traffic Steering | Steering paths. Define different paths the traffic can take to reach its destination. For any traffic steering policy, you can include paths for traffic to traverse, as well as the strategies for utilizing those paths. See Traffic Steering. |

| Fields | Description |
|---|---|
| Application Policies | Policies to enforce rule for traffic. Define network (source), application (destination), traffic steering policies, and policy action. See Application Policies. |
| Routing | Routing options for routing traffic between the hub and spokes. You can enable Border Gateway Protocol (BGP) underlay routing, where routes are learned dynamically or use static routing to define routes manually.. |
| CLI Configuration | CLI option. For any additional settings that are not available in the template's GUI, you can still configure them using CLI **set** commands. |

- Click **Save**.

Add WAN Interfaces to the Template

The WAN interface on the spoke corresponds to the WAN interface on hub. That is—Mist creates an IPsec VPN tunnel between WAN interface on the hub to WAN interface on the spoke.

In this task, add two WAN interfaces to the WAN edge template.

To add WAN interfaces to the template:

- In the Juniper Mist portal, scroll down to the WAN section and click **Add WAN** to open the Add WAN Configuration pane.
- Complete the configuration according to the details provided in below Table.

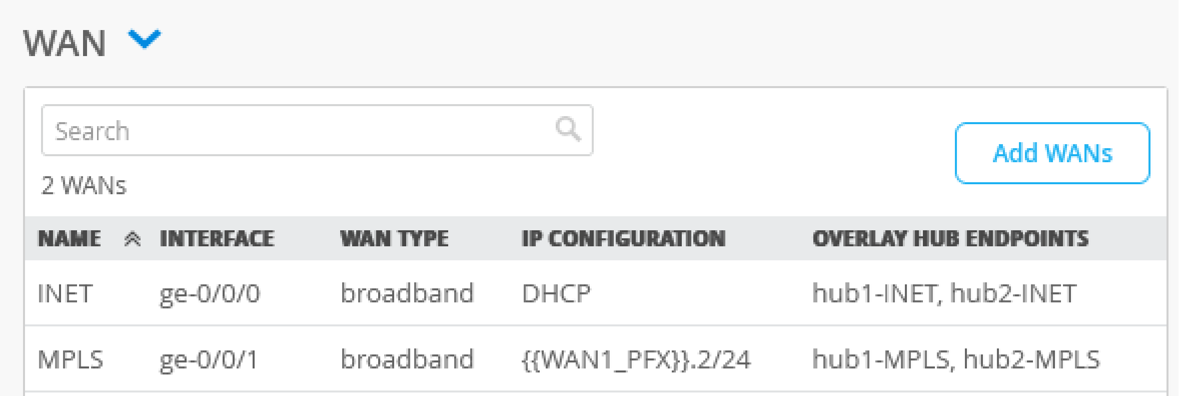
Table 15: WAN Interface Configuration Options

| Fields | WAN Interface 1 | WAN Interface 2 |
|---|---|---|
| **Name** (a label and not a technology) | INET | MPLS |
| WAN Type | Ethernet | Ethernet |
| Interface | ge-0/0/0 | ge-0/0/3 |
| VLAN ID | - | - |
| IP Configuration | DHCP | Static<br>**IP Address**={{WAN1_PFX}}.2<br>Prefix Length=24<br>**Gateway**={{WAN1_PFX}}.1 |

| Fields | WAN Interface 1 | WAN Interface 2 |
|---|---|---|
| Source NAT | Interface | Interface |
| **Overlay Hub Endpoint** (generated automatically). | hub1-INET, hub2-INET (BFD profile Broadband) | hub1-MPLS and hub2-MPLS |

The Figure below shows list of WAN interfaces you created.

Figure33: WAN Interfaces Summary



2 WANs

| NAME | INTERFACE | WAN TYPE | IP CONFIGURATION | OVERLAY HUB ENDPOINTS |
|---|---|---|---|---|
| INET | ge-0/0/0 | broadband | DHCP | hub1-INET, hub2-INET |
| MPLS | ge-0/0/1 | broadband | {{WAN1_PFX}}.2/24 | hub1-MPLS, hub2-MPLS |

Add a LAN Interface

LAN interface configuration identifies your request source from the name of the network you specify in the LAN configuration.

To add a LAN interface:

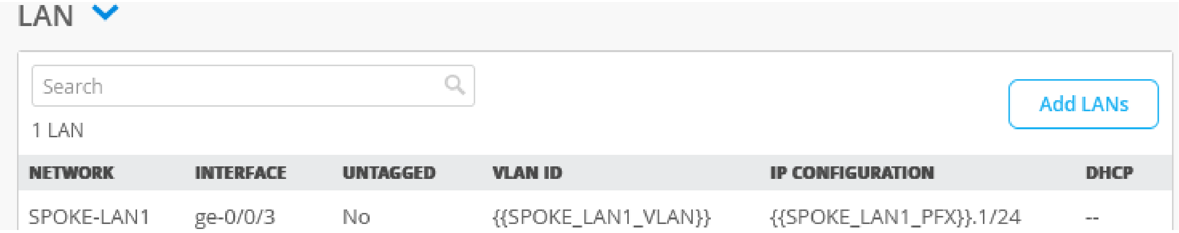
- In the Juniper Mist portal, scroll down to the LAN pane and click **Add LAN** to open the Add LAN Configuration panel.
- Complete the configuration according to the details provided in below Table.

Table 16: LAN Interface Details

| Fields | LAN Interface |
|---|---|
| Network | SPOKE-LAN1 (Select from the list of networks that appears. When you do, the remaining configuration will be filled in automatically.) |
| Interface | ge-0/0/3 |
| IP Address | {{SPOKE_LAN1_PFX}}.1 |
| Prefix Length | 24 |
| Untagged VLAN | No |
| DHCP | No |

The Figure below shows the list of LAN interface you created.

Figure34: Summary of LAN Interface



| NETWORK | INTERFACE | UNTAGGED | VLAN ID | IP CONFIGURATION | DHCP |
|---|---|---|---|---|---|
| SPOKE-LAN1 | ge-0/0/3 | No | {{SPOKE_LAN1_VLAN}} | {{SPOKE_LAN1_PFX}}.1/24 | -- |

Configure Traffic Steering Policies

Just like with hub profiles, traffic steering in a Juniper Mist network is where you define the different paths that application traffic can take to traverse the network. The paths that you configure within traffic steering also determine the destination zone.

To configure traffic steering policies:

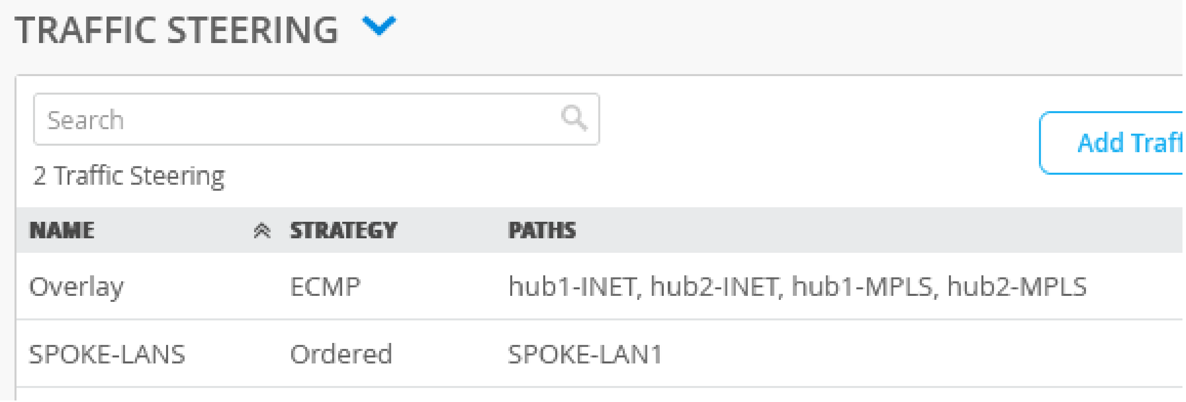
- In the Juniper Mist portal, scroll down to the Traffic Steering section, and click **Add Traffic Steering** to display the Traffic Steering configuration pane.
- Complete the configuration according to the details provided in below Table.

Table 17: Traffic Steering Policy Configuration

| Fields | Traffic Steering Policy 1 | Traffic Steering Policy 2 |
|---|---|---|
| Name | SPOKE-LANS | Overlay |
| Strategy | Ordered | ECMP |
| **PATHS** (For path types, you can select the previously created LAN and WAN networks as endpoints.) | **Type**—LAN<br>**Network**—SPOKE-LAN1 | **Type**— WAN<br>Network —<br>hub1-INET<br>hub2-INET<br>hub1-MPLS<br>hub2-MPLS |

The Figure below shows the list of traffic steering policies you created.

Figure35: Traffic Steering Policies Summary



TRAFFIC STEERING

Search

Add Traffi

2 Traffic Steering

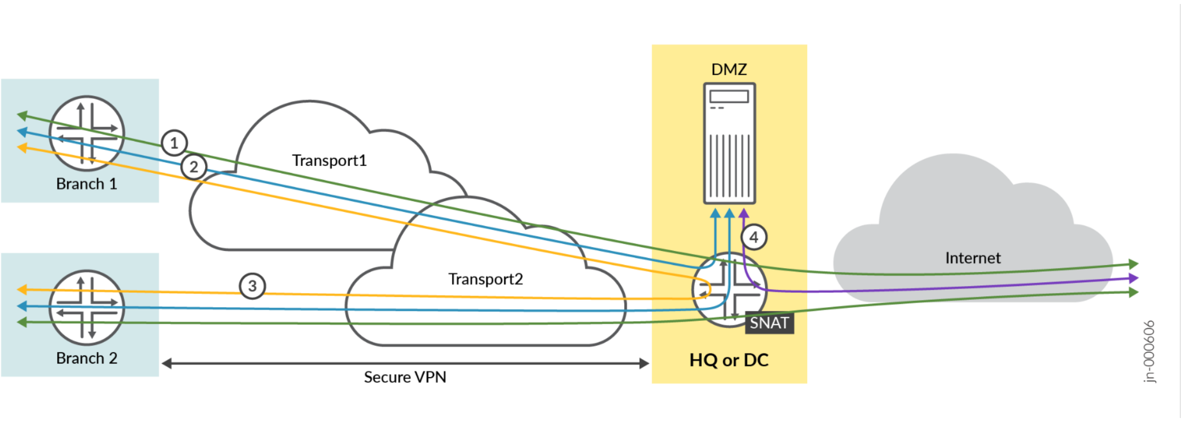
| NAME | STRATEGY | PATHS |
|---|---|---|
| Overlay | ECMP | hub1-INET, hub2-INET, hub1-MPLS, hub2-MPLS |
| SPOKE-LANS | Ordered | SPOKE-LAN1 |

Configure Application Policies

In a Mist network, application policies are where you define which network and users can access which applications, and according to which traffic steering policy. The **Networks/Users** settings determine the source zone. The **Application** + **Traffic Steering** settings determine the destination zone. Additionally, you can assign an action of Permit or Deny. Mist evaluates and applies application policies in the order in which you list them.

Consider the traffic-flow requirements in the Figure below. The image depicts a basic initial traffic model for a corporate VPN setup (third spoke device and second hub device are not shown).

Figure36: Traffic Flow and Distribution



To meet the preceding requirements, you need to create the following application policies:

- Policy 1—Allows traffic from spoke sites to the hub. In this case, the destination prefix used in address groups represents the LAN interface of two hubs.
- Policy 2—Allows spoke-to-spoke traffic through the corporate LAN through an overlay.

  - **Note**: A DIRECT Spoke to Spoke communication is hard to archive today. This may not be feasible in the real world except on expensive MPLS networks with managed IPs. Managed IPs can send traffic directly to the other spoke. In our case we do NOT assume such capability hence Spoke to Spoke Traffic has to traverse via the Hub which is feasible without special Network design assumptions.

- Policy 3—Allows traffic from both the hub and the DMZ attached to the hub to the spoke devices.
- Policy 4—Allows Internet-bound traffic to flow from spoke devices to the hub device. From there, the traffic breaks out to the Internet. In this case, the hub applies source NAT to the traffic and routes traffic to a WAN interface, as defined in the hub profile. This rule is general, so you should place it after the specific rules. Because Mist evaluates application policies in the order, they are placed in the policies list.

To configure application polices:

- In the Juniper Mist portal, scroll down to Application Policy section, click **Add Policy** to add a new policy in the policy list.
- Complete the configuration according to the details provided in below Table.

Table 18: Application Policies Configuration

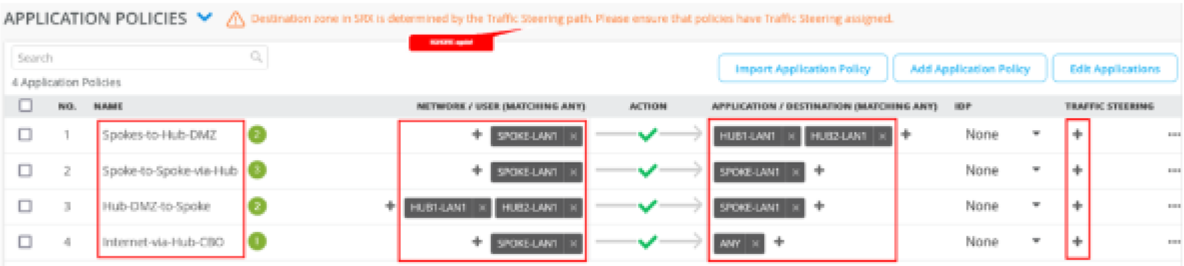
| S.No. | Rule Name | Network | Action | Destination | Steering |
|---|---|---|---|---|---|
| 1 | Spoke-to-Hub-DMZ | SPOKE-LAN1 | Pass | HUB1-LAN1 + HUB2-LAN1 | Overlay |
| 2 | Spoke-to-Spoke-via-Hub | SPOKE-LAN1 | Pass | SPOKE-LAN1 | Overlay |
| 3 | Hub-DMZ-to-Spoke | HUB1-LAN1 + HUB2-LAN1 | Pass | SPOKE-LAN1 | SPOKE-LANS |
| 4 | Internet-via-Hub-CBO | SPOKE-LAN1 | Pass | ANY | Overlay |

Note1: For SRX Series Firewalls, you must associate a traffic steering policy to the application policy.

Note2: The order of application policies in the policies list is very important for SRX Series Firewalls.

The Figure below shows the list of application policies you created.

Figure37: Application Policy Summary



APPLICATION POLICIES ⚠ Destination zone in SRX is determined by the Traffic Steering path. Please ensure that policies have Traffic Steering assigned.

Search

Import Application Policy | Add Application Policy | Edit Applications

4 Application Policies

| ☐ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| ☐ | 1 | Spokes-to-Hub-DMZ | SPOKE-LAN1 | ✓ | HUB1-LAN1, HUB2-LAN1 | None | + |
| ☐ | 2 | Spoke-to-Spoke-via-Hub | SPOKE-LAN1 | ✓ | SPOKE-LAN1 | None | + |
| ☐ | 3 | Hub-DMZ-to-Spoke | HUB1-LAN1, HUB2-LAN1 | ✓ | SPOKE-LAN1 | None | + |
| ☐ | 4 | Internet-via-Hub-CBO | SPOKE-LAN1 | ✓ | ANY | None | + |

- OPTIONAL: Allow Internet Control Message Protocol (ICMP) pings for debugging and for checking device connectivity.

  The default security configurations for SRX Series Firewalls do not allow ICMP ping requests from the LAN device to the local interface of the WAN edge router. We recommend that you test connectivity before the device attempts to connect to the outside network. We also recommend that you allow ICMP ping requests for debugging and for checking device connectivity.

  On the SRX Series Firewall, use the following CLI configuration statement to allow ping requests to the local LAN interface for debugging:

```
set security zones security-zone HUB1-LAN1 host-inbound-traffic system-services ping
```

## 2.) Assign a WAN Edge Spoke Template to a Site

You can attach the templates that you configured in the Juniper Mist cloud to one or more sites.

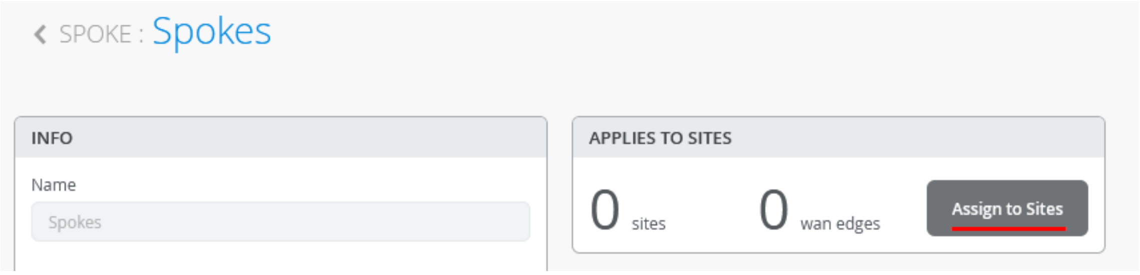
The template that you created in *Configure WAN Edge Templates* now exists in the Juniper Mist cloud as an object that you can assign to one or more sites. WAN edge templates are a quick and easy way to group the common attributes of WAN edge spoke devices. You can apply a single template to multiple sites. Any changes to the WAN edge template are applied to all the sites without any additional steps.

If a site already has a template assigned to it, assigning another template will replace the existing template. That is, one site cannot have two templates, and the newer template will overwrite the older template.

To assign a WAN edge spoke template to a site:

- In the Juniper Mist portal, select **Organization** > **WAN** > **WAN Edge Templates** and select the required template.
- Scroll to the top of the WAN Edge Templates page and click **Assign to Sites**.

Figure38: Assign Spoke Templates to Sites



SPOKE : Spokes

INFO

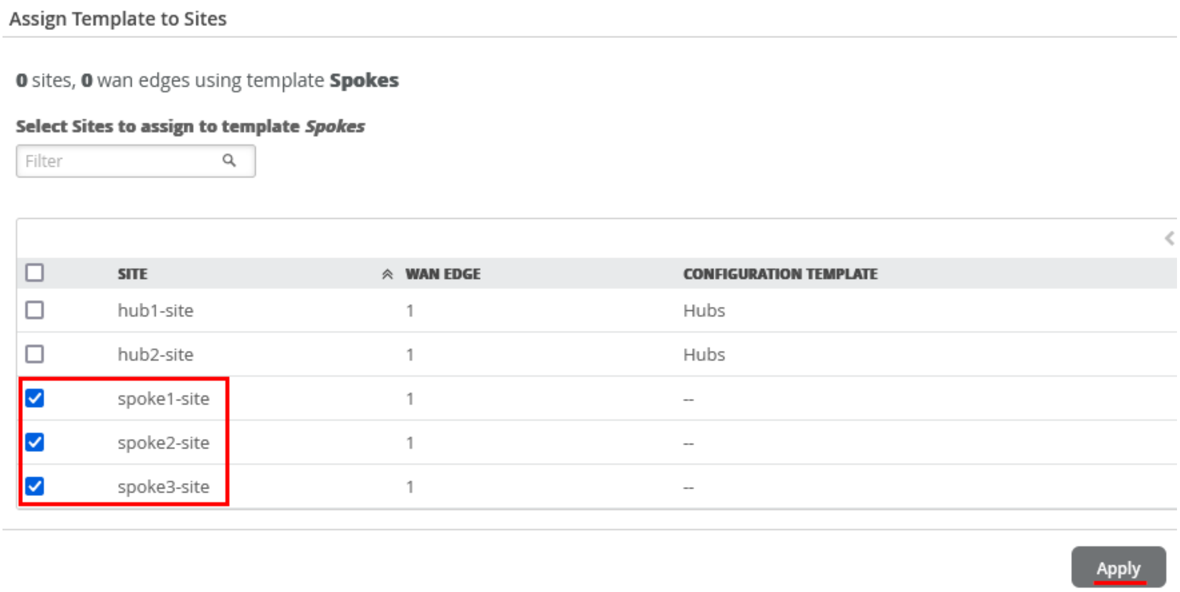
Name: Spokes

APPLIES TO SITES

0 sites 0 wan edges

- In the Assign Template to Sites window, select the required sites and click **Apply**.

Figure39: Select Sites to Assign Spoke Templates



Assign Template to Sites

**0** sites, **0** wan edges using template **Spokes**

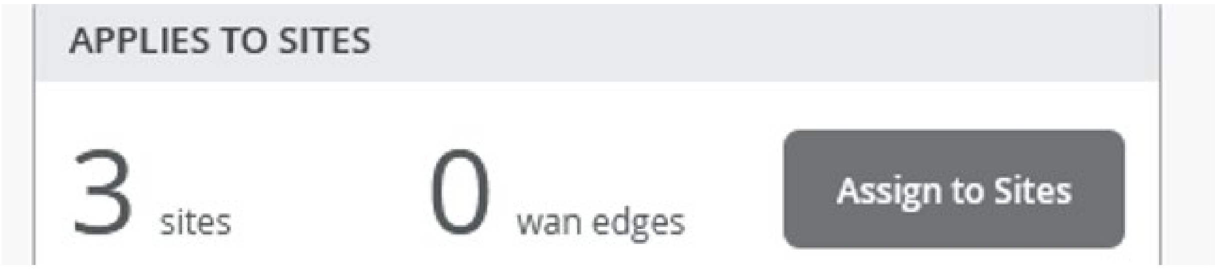
**Select Sites to assign to template *Spokes***

Filter

| ☐ | SITE | WAN EDGE | CONFIGURATION TEMPLATE |
|---|---|---|---|
| ☐ | hub1-site | 1 | Hubs |
| ☐ | hub2-site | 1 | Hubs |
| ☑ | spoke1-site | 1 | -- |
| ☑ | spoke2-site | 1 | -- |
| ☑ | spoke3-site | 1 | -- |

The WAN Edge Templates page reflects the updated status. The Figure below indicates that three sites are using the template.

Figure40: WAN Edge Templates Applied to Sites



APPLIES TO SITES

3 sites

0 wan edges

## 3.) Onboard SRX Series Firewalls for WAN Configuration

In a Juniper Mist network, you must onboard your Juniper Networks® SRX Series Firewalls by assigning them to sites. Complete the onboarding by attaching hub profiles and spoke templates to the respective hub sites and spoke sites. This final step brings the topology together.

We assume that you have your SRX Series Firewall already onboarded to the Juniper Mist cloud. We also assume that the physical connections such as cabling are already in place and that you are using valid interfaces and VLANs in your sandbox.

For details on getting your SRX Series Firewall up and running in the Mist cloud, see the first chapter of this Appendix “Day-0 operation to claim/ZTP or adopt the SRX Devices towards Mist cloud”.

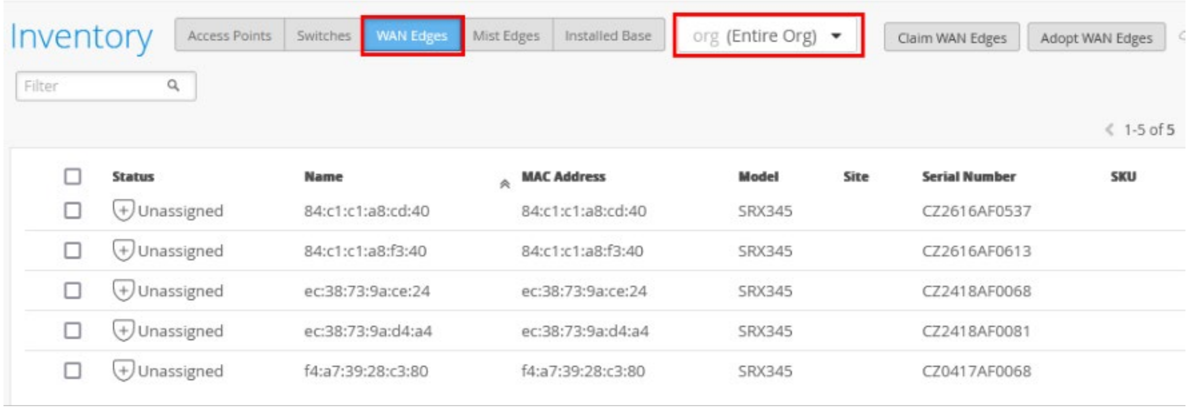
## 9.) Assign an SRX Series Firewall to a Site

To assign your SRX Series Firewall devices to sites, the devices must be present in the Juniper Mist inventory. You can claim or adopt your SRX Series Firewall to onboard it in the Juniper Mist cloud. After the device is on board, the organization inventory shows the device.

To assign an SRX Series Firewall to a site:

- In the Juniper Mist portal. click **Organization** > **Admin** > **Inventory**.
- Refresh your browser and check under **WAN Edges** to find out if your SRX Series Firewall is part of the inventory.

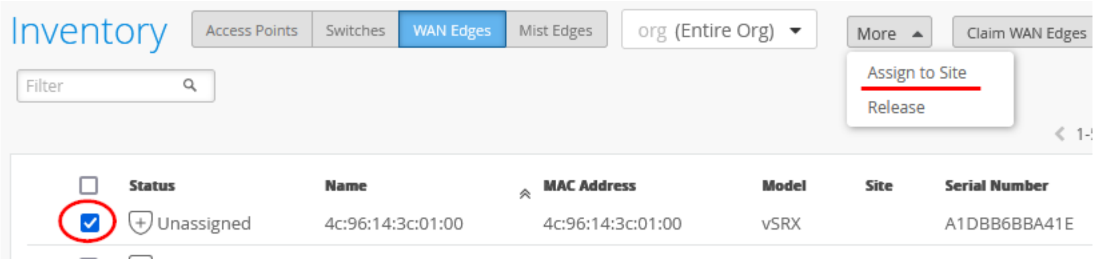
Figure41: SRX Series Firewall in Inventory



| ☐ | Status | Name | MAC Address | Model | Site | Serial Number | SKU |
|---|---|---|---|---|---|---|---|
| ☐ | Unassigned | 84:c1:c1:a8:cd:40 | 84:c1:c1:a8:cd:40 | SRX345 | | CZ2616AF0537 | |
| ☐ | Unassigned | 84:c1:c1:a8:f3:40 | 84:c1:c1:a8:f3:40 | SRX345 | | CZ2616AF0613 | |
| ☐ | Unassigned | ec:38:73:9a:ce:24 | ec:38:73:9a:ce:24 | SRX345 | | CZ2418AF0068 | |
| ☐ | Unassigned | ec:38:73:9a:d4:a4 | ec:38:73:9a:d4:a4 | SRX345 | | CZ2418AF0081 | |
| ☐ | Unassigned | f4:a7:39:28:c3:80 | f4:a7:39:28:c3:80 | SRX345 | | CZ0417AF0068 | |

- Assign each SRX Series Firewall to an individual site using the **Assign to Site** option.

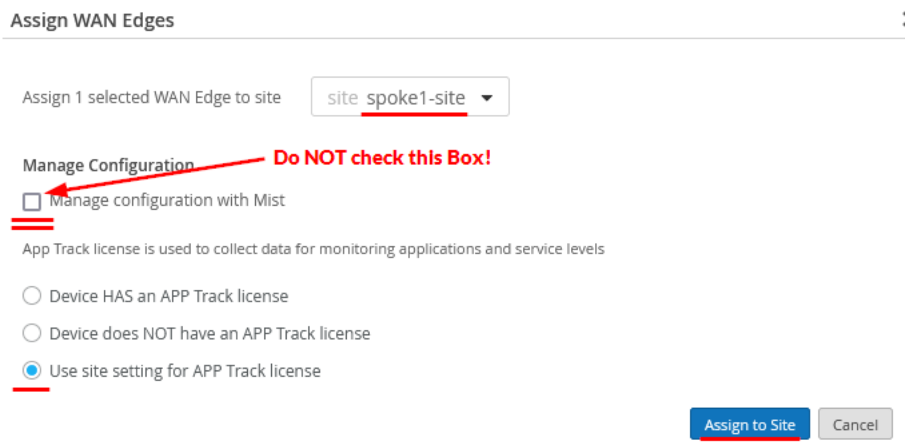
Figure42: Assign SRX Series Firewalls to Sites



| ☐ | Status | Name | MAC Address | Model | Site | Serial Number |
|---|---|---|---|---|---|---|
| ☑ | Unassigned | 4c:96:14:3c:01:00 | 4c:96:14:3c:01:00 | vSRX | | A1DBB6BBA41E |

- On the Assign WAN Edges page, select the site you want to assign from the list of available sites.

Figure43: Select a Site



Assign WAN Edges

Assign 1 selected WAN Edge to site: site spoke1-site

Manage Configuration

Do NOT check this Box!

□ Manage configuration with Mist

App Track license is used to collect data for monitoring applications and service levels

○ Device HAS an APP Track license

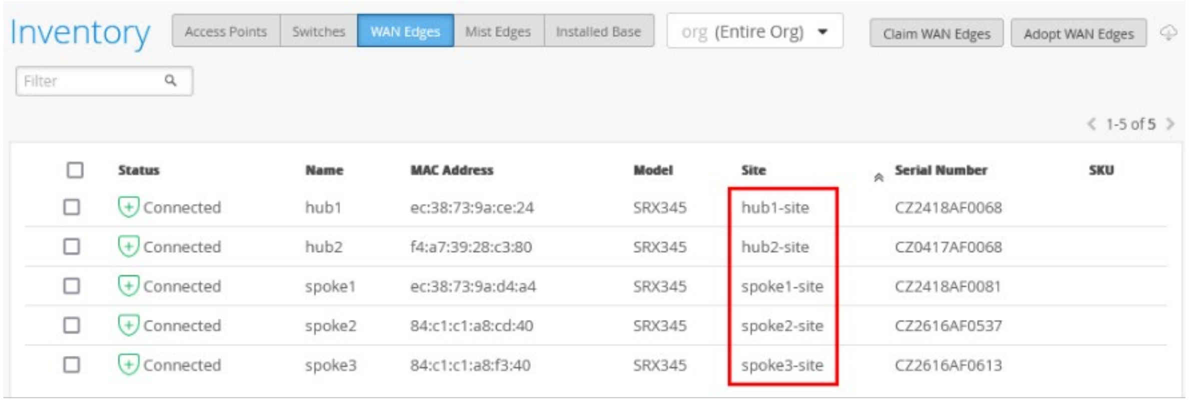
○ Device does NOT have an APP Track license

● Use site setting for APP Track license

- Do not select the **Manage configuration with Mist** option. If you do, you may see unwanted changes on your SRX Series Firewall. You can enable the option later if required, after you've assigned the device to the site.
- Check the **Use site setting for APP Track license** option if you have a valid Application Security license, and then click **Assign to Site**.

The below Figure shows changes in the inventory once you assign the device to the site.

Figure44: Site Assignment Summary



| □ | Status | Name | MAC Address | Model | Site | Serial Number | SKU |
|---|---|---|---|---|---|---|---|
| □ | Connected | hub1 | ec:38:73:9a:ce:24 | SRX345 | hub1-site | CZ2418AF0068 | |
| □ | Connected | hub2 | f4:a7:39:28:c3:80 | SRX345 | hub2-site | CZ0417AF0068 | |
| □ | Connected | spoke1 | ec:38:73:9a:d4:a4 | SRX345 | spoke1-site | CZ2418AF0081 | |
| □ | Connected | spoke2 | 84:c1:c1:a8:cd:40 | SRX345 | spoke2-site | CZ2616AF0537 | |
| □ | Connected | spoke3 | 84:c1:c1:a8:f3:40 | SRX345 | spoke3-site | CZ2616AF0613 | |

## 10.) Assign a Hub Profile to the SRX Series Firewall

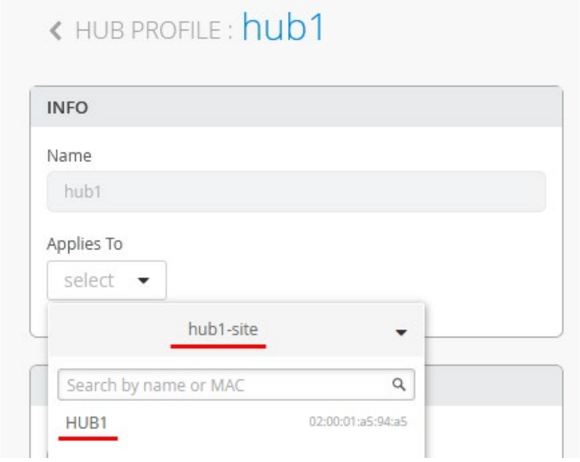
A hub profile comprises the set of attributes that are associated with a particular hub device. Each hub device in a Juniper Mist cloud topology must have its own profile. You apply the hub profile to an individual device that's at a hub site.

To assign a hub profile to the SRX Series Firewall, which is part of a hub site:

- In the Juniper Mist portal, click **Organization** > **WAN** > **Hub Profiles**. The Hub Profile displays the list of existing profiles.
- Click the hub profile that you want to assign to a site.

- Under the **Applies To** option, select the site from the list of available sites.

Figure45: Select Devices on Sites



HUB PROFILE : hub1

INFO

Name: hub1

Applies To: select

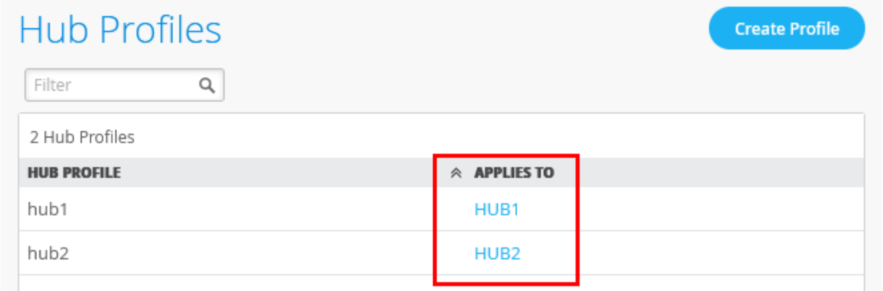
hub1-site

Search by name or MAC

HUB1 02:00:01:a5:94:a5

- Click **Save** to continue.
- Repeat the same steps to add more hub sites. You can see the result on the **Hub Profiles** page.

Figure46: Hub Profile Assignment Summary

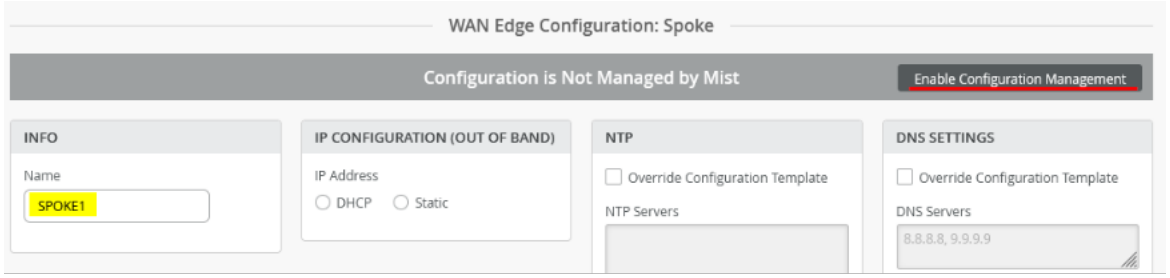


2 Hub Profiles

| HUB PROFILE | APPLIES TO |
|---|---|
| hub1 | HUB1 |
| hub2 | HUB2 |

**You've almost made it.** The last step is to go to each SRX device and put it into management-mode so that the Mist Cloud starts pushing concrete configurations to create your SD-WAN VPN.

- Enable management mode on the first Hub and wait 10minutes until its configured fully.
- Enable management mode on the second Hub and wait 10minutes until its configured fully.
- Enable management mode on any of your Spoke devices. The order does not matter, and you can do multiple at the same time depending on how fast you can roll them out.



WAN Edge Configuration: Spoke

Configuration is Not Managed by Mist

INFO

Name: SPOKE1

IP CONFIGURATION (OUT OF BAND)

IP Address: ○ DHCP ○ Static

NTP

□ Override Configuration Template

NTP Servers

DNS SETTINGS

□ Override Configuration Template

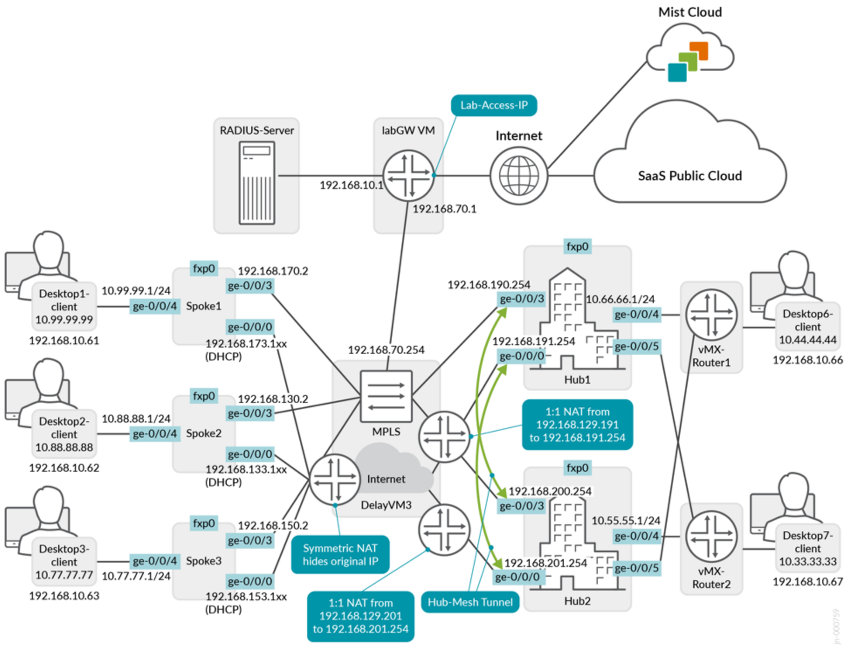
DNS Servers: 8.8.8.8, 9.9.9.9

# Extended Topology with Hub-Mesh and BGP Peering

In this chapter we will implement the second topology that we have discussed above and show you the entire workflow by this. **This design only shows the changes from the first design and not the complete process again.** We assume you learnt the basics already with the first topology hence we keep this crisp and only show the diffs to that.

With this configuration example, you're expanding the basic network capabilities by:

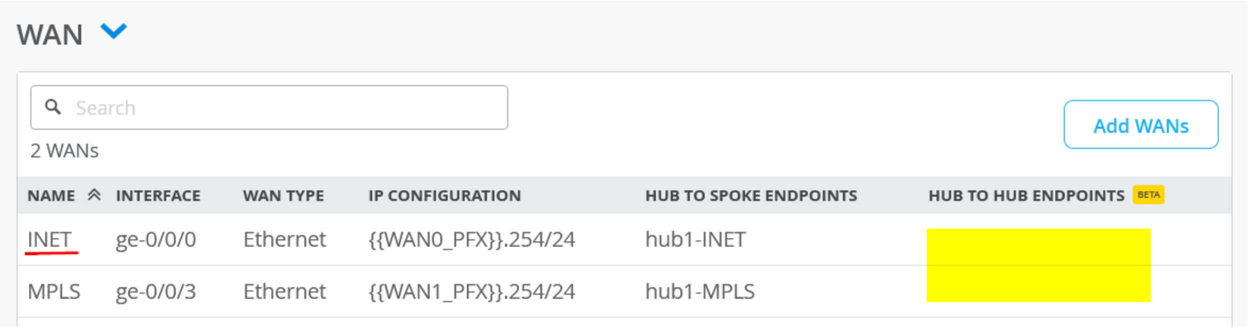
- Establishing Tunnels between the WAN-Interfaces of our Hubs to establish a Mesh between them.
- We are adding Routers on the LAN-Interface of the Hub that exchange routes with the Hub via eBGP. Attached to the Router are Servers that are reachable though them. This mimics a scenario seen in Data center and Public Cloud hosting services. The Routes propagated via the LAN-Interface of the Hub's need to be visible in the Overlay and reachable for Spokes.



## Enable Hub-Meshing

To enable Hub-Meshing we add a bit of additional configuration on our primary Hub like seen below:

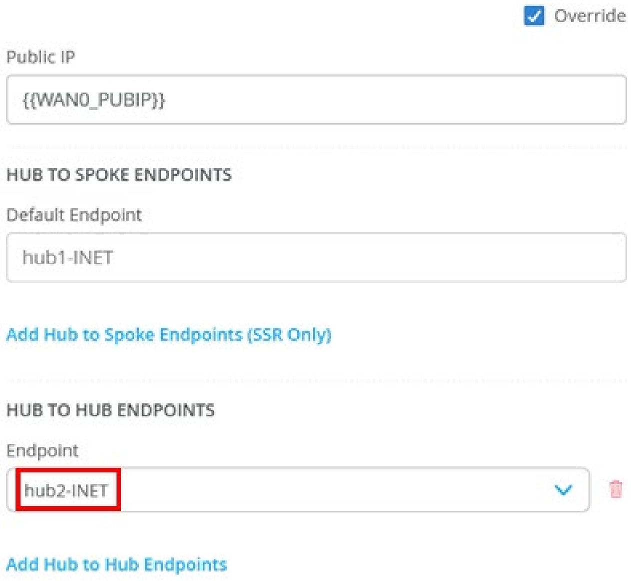
- Go to **Organization > Hub Profiles > Select: "hub1"**
- Scroll to the WAN-Interface setting and notice that yet there are no Hub-to-Hub Endpoints configured as shown below.



2 WANs

| NAME | INTERFACE | WAN TYPE | IP CONFIGURATION | HUB TO SPOKE ENDPOINTS | HUB TO HUB ENDPOINTS BETA |
|---|---|---|---|---|---|
| INET | ge-0/0/0 | Ethernet | {{WAN0_PFX}}.254/24 | hub1-INET | |
| MPLS | ge-0/0/3 | Ethernet | {{WAN1_PFX}}.254/24 | hub1-MPLS | |

- Edit the Interface with the name “INET”
- Add the Hub to Hub Endpoint: “hub2-INET” as it is a corresponding Interface on the second Hub in the same Topology.



☑ Override

Public IP: {{WAN0_PUBIP}}

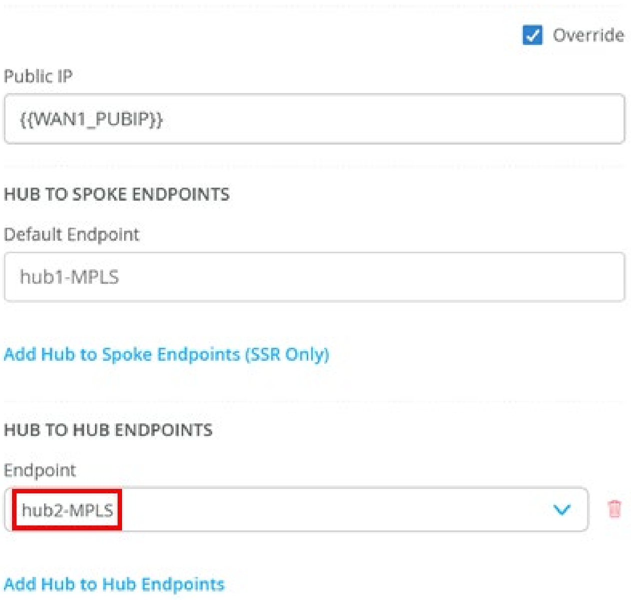
HUB TO SPOKE ENDPOINTS

Default Endpoint: hub1-INET

HUB TO HUB ENDPOINTS

Endpoint: hub2-INET

- Edit the Interface with the name “MPLS”
- Add the Hub-to-Hub Endpoint: “hub2-MPLS” as it is a corresponding Interface on the second Hub in the same Topology.



☑ Override

Public IP

{{WAN1_PUBIP}}

HUB TO SPOKE ENDPOINTS

Default Endpoint

hub1-MPLS

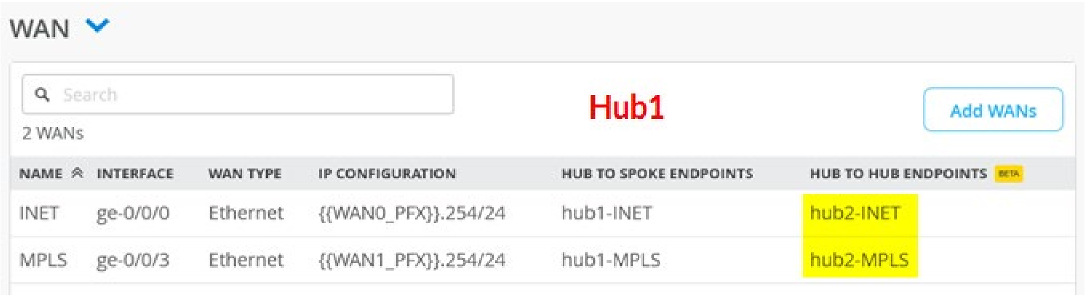
HUB TO HUB ENDPOINTS

Endpoint

hub2-MPLS

- "Save" your changes on the primary Hub so that the system applies them now (also automatically on the secondary Hub).

After your changes are completed, the primary Hub should now have the corresponding Interfaces of the second Hub configured as Hub-to-Hub Endpoints.

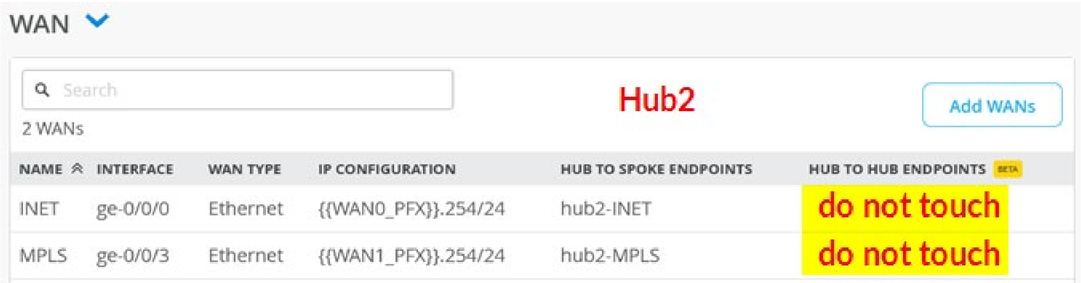


2 WANs

| NAME | INTERFACE | WAN TYPE | IP CONFIGURATION | HUB TO SPOKE ENDPOINTS | HUB TO HUB ENDPOINTS BETA |
|---|---|---|---|---|---|
| INET | ge-0/0/0 | Ethernet | {{WAN0_PFX}}.254/24 | hub1-INET | hub2-INET |
| MPLS | ge-0/0/3 | Ethernet | {{WAN1_PFX}}.254/24 | hub1-MPLS | hub2-MPLS |

Note: This feature is only configured on one Hub (here the primary) to establish a Tunnel for Mesh with another Hub. Do not do the same configuration on the other side.

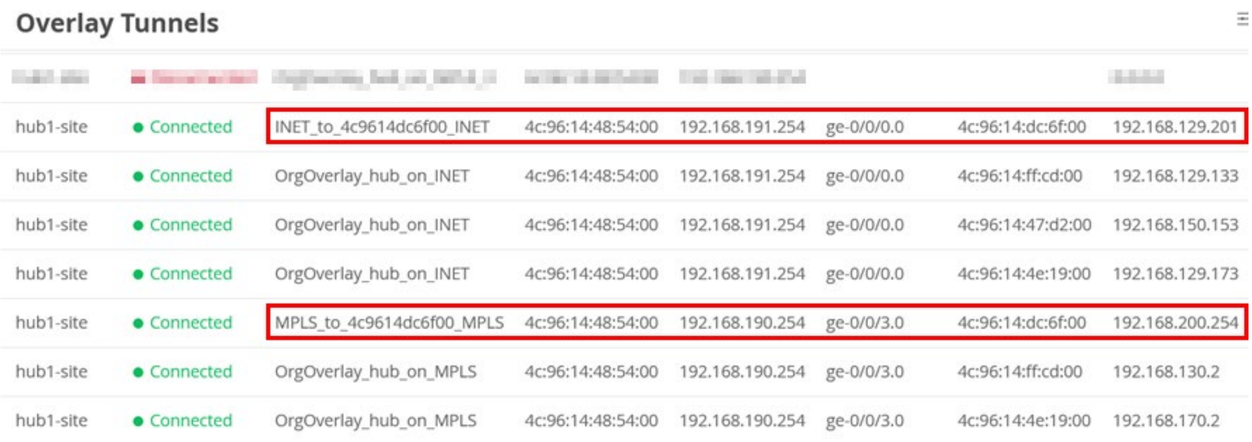
The below is just to reinsure that you do not need to change the configuration on the second Hub.



2 WANs

| NAME | INTERFACE | WAN TYPE | IP CONFIGURATION | HUB TO SPOKE ENDPOINTS | HUB TO HUB ENDPOINTS BETA |
|---|---|---|---|---|---|
| INET | ge-0/0/0 | Ethernet | {{WAN0_PFX}}.254/24 | hub2-INET | do not touch |
| MPLS | ge-0/0/3 | Ethernet | {{WAN1_PFX}}.254/24 | hub2-MPLS | do not touch |

When you go into WAN Edge Insights of Hub1 you will now notice these additional two IPsec Tunnels established that we marked in the below Figure.



Overlay Tunnels

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | | | [redacted] |
| hub1-site | ● Connected | INET_to_4c9614dc6f00_INET | 4c:96:14:48:54:00 | 192.168.191.254 | ge-0/0/0.0 | 4c:96:14:dc:6f:00 | 192.168.129.201 |
| hub1-site | ● Connected | OrgOverlay_hub_on_INET | 4c:96:14:48:54:00 | 192.168.191.254 | ge-0/0/0.0 | 4c:96:14:ff:cd:00 | 192.168.129.133 |
| hub1-site | ● Connected | OrgOverlay_hub_on_INET | 4c:96:14:48:54:00 | 192.168.191.254 | ge-0/0/0.0 | 4c:96:14:47:d2:00 | 192.168.150.153 |
| hub1-site | ● Connected | OrgOverlay_hub_on_INET | 4c:96:14:48:54:00 | 192.168.191.254 | ge-0/0/0.0 | 4c:96:14:4e:19:00 | 192.168.129.173 |
| hub1-site | ● Connected | MPLS_to_4c9614dc6f00_MPLS | 4c:96:14:48:54:00 | 192.168.190.254 | ge-0/0/3.0 | 4c:96:14:dc:6f:00 | 192.168.200.254 |
| hub1-site | ● Connected | OrgOverlay_hub_on_MPLS | 4c:96:14:48:54:00 | 192.168.190.254 | ge-0/0/3.0 | 4c:96:14:ff:cd:00 | 192.168.130.2 |
| hub1-site | ● Connected | OrgOverlay_hub_on_MPLS | 4c:96:14:48:54:00 | 192.168.190.254 | ge-0/0/3.0 | 4c:96:14:4e:19:00 | 192.168.170.2 |

OPTIONAL: One can open a remote Shell to Hub1 SRX and inspect the VPN-Overlay Routeing Table where:

- You will notice that the default route now also has the two new Tunnels to the other Hub included.
- You additionally see the LAN-Network of the second Hub in the Table. That was not something we had before. Instances from Hub1 could only reach Spoke but not Hub2 until now.

```
root@hub1> show route table vpn_OrgOverlay.inet.0

vpn_OrgOverlay.inet.0: 35 destinations, 39 routes (35 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 00:41:10
                    >  to 192.168.190.1 via ge-0/0/3.0
                    [BGP/170] 00:00:44, localpref 100, from 100.101.0.2
                      AS path: I, validation-state: unverified
                    >  to 100.67.0.1 via st0.8
                       to 100.68.0.1 via st0.9
10.55.55.0/24      *[BGP/170] 00:00:44, localpref 100, from 100.101.0.2
                      AS path: I, validation-state: unverified
                       to 100.67.0.1 via st0.8
                    >  to 100.68.0.1 via st0.9
10.66.66.0/24      *[Direct/0] 00:41:25
                    >  via ge-0/0/4.1066
.
```

To prove the above statement, we now can reach Hub2 Instances from Hub1 LAN-Interface we utilize the Desktop4 VM (IP address:10.66.66.66) of the Lab attached to Hub1 to ping the Desktop5 VM of the Lab attached to Hub2 (IP address:10.55.55.55) which succeeds now as demonstrated below.

```
root@desktop4:~# ping 10.55.55.55
PING 10.55.55.55 (10.55.55.55) 56(84) bytes of data.
64 bytes from 10.55.55.55: icmp_seq=1 ttl=62 time=1.54 ms
64 bytes from 10.55.55.55: icmp_seq=2 ttl=62 time=1.42 ms
64 bytes from 10.55.55.55: icmp_seq=3 ttl=62 time=1.50 ms
.
```

Hub-Mesh is not only used to share services among Hubs. Should, for some reason, a Spoke not be able to reach to a certain Hub anymore BUT the Hub mesh between these Hub is still intact then the Spoke is able to still reach these services at the first hub via the second hub and the mesh between them. This situation was also tested as part of this JVD.

## BGP-Peering with DC

When establishing a Route exchange with a Router attached at a LAN-Interface we need to configure a couple of items in the Mist UI to establish that exchange. In our case we leverage exterior BGP so we need to configure

- A unique, private local autonomous system number (AS). Pick your own private AS please excluding 65000. Note: AS 65000 cannot be used as it is already in use for interior BGP by the VPN that WAN edge for SRX builds automatically.
- We need to remember the local LAN IP prefix on our Hub already assigned.
- The WAN-Router must have an IP address in the local LAN IP prefix reachable for BGP hence we must configure that as BGP-neighbor Address.
- A unique, private remote autonomous system number (AS). Pick your own private AS please excluding 65000.
- We most know in advance all Prefixes that will be advertised by the attached Router. This is to be able to modify the Firewall statements accordingly to let the Traffic from learned routes pass. Without proper configuration you may be able to learn routes, but the configuration will still block that Traffic because those new IP prefixes are denied by either Spoke or Hub Firewall.

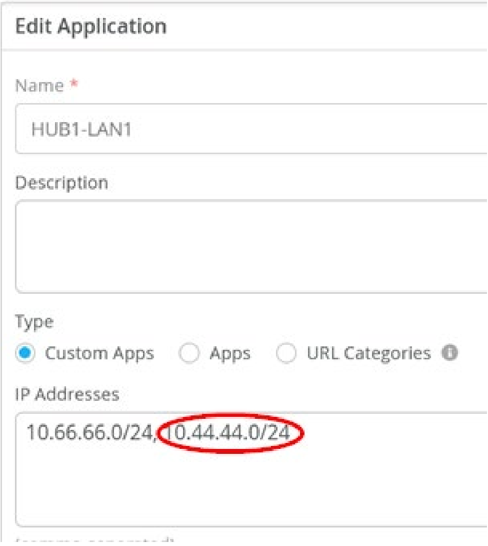
The below Table is what we are going to configure and need to know as additional items for our Lab.

| Hub | Local AS | Direct attached LAN IP Prefix | Remote Neighbor | Remote AS | Indirect via Router Larned IP Prefixes |
|---|---|---|---|---|---|
| Hub1 | 65011 | 10.66.66.0/24 | 10.66.66.66 | 65012 | 10.44.44.0/24 |
| Hub2 | 65021 | 10.55.55.0/24 | 10.55.55.55 | 65022 | 10.33.33.0/24 |

Extensions Needed for Firewall to Allow Traffic to Indirect Routes at Hubs

First, we extend the custom Applications describing our two Hub-LANs. This will allow the Spoke-side Application Policies to get updated and allow this Traffic towards Hub (assumed the Routes are learned as well under the hood).

- Go to **Organization > Applications**
- Edit exiting custom Application called “HUB1-LAN1”
  - Add the new indirect reachable Prefix “10.44.44.0/24” to the already existing Prefix “10.66.66.0/24”.



Edit Application

Name *

HUB1-LAN1

Description

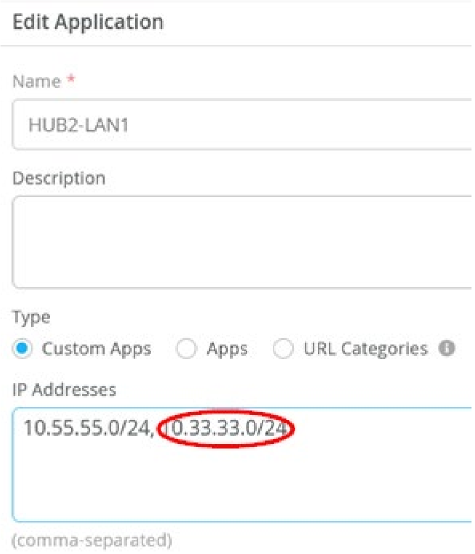
Type

● Custom Apps ○ Apps ○ URL Categories

IP Addresses

10.66.66.0/24,10.44.44.0/24

- Edit exiting custom Application called “HUB2-LAN1”
  - Add the new indirect reachable Prefix “10.33.33.0/24” to the already existing Prefix “10.55.55.0/24”.



Edit Application

Name *

HUB2-LAN1

Description

Type

● Custom Apps ○ Apps ○ URL Categories

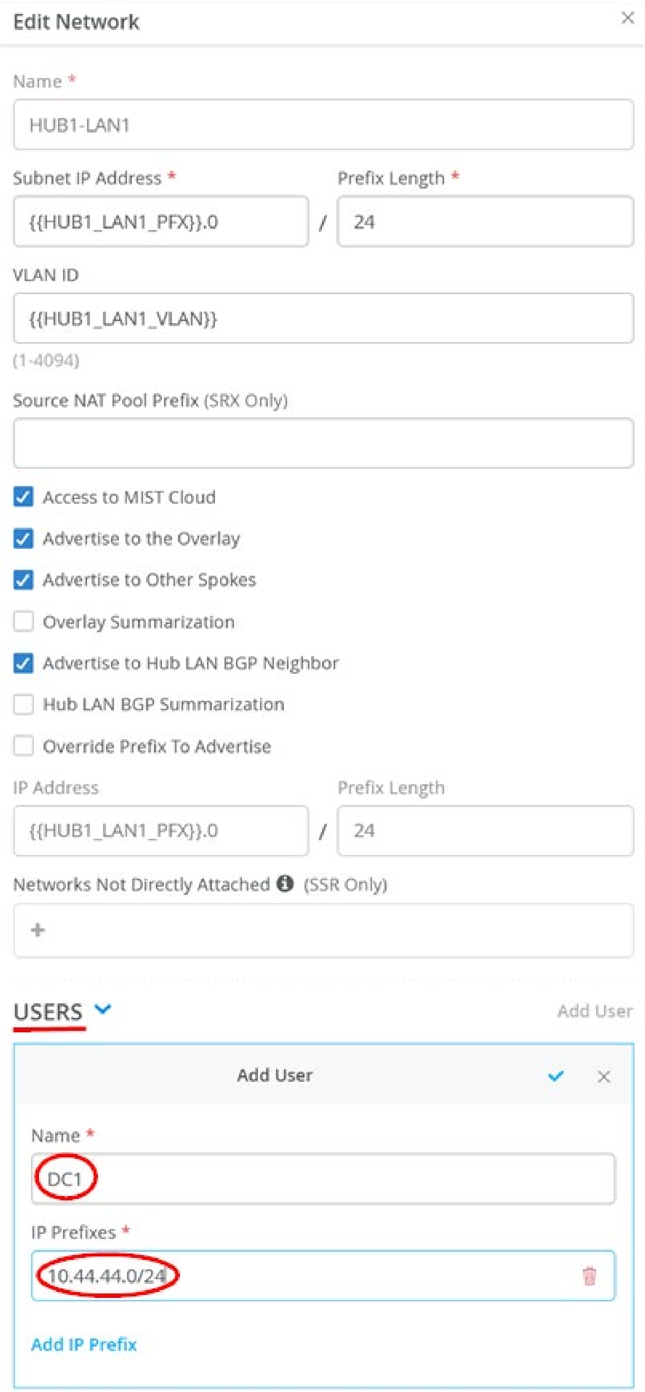
IP Addresses

10.55.55.0/24, 10.33.33.0/24

(comma-separated)

The next Item we need to extend is the definition for the two Networks assigned to our Hubs. Our indirect/learned Networks need to be added as a “Users”-object there.

- Go to **Organization > Networks**
- Edit exiting Network called “HUB1-LAN1”
  - Add under Users a new Object with the Name: “DC1” and IP Prefix: “10.44.44.0/24”.



Edit Network

Name *
HUB1-LAN1

Subnet IP Address * {{HUB1_LAN1_PFX}}.0 / Prefix Length * 24

VLAN ID
{{HUB1_LAN1_VLAN}}
(1-4094)

Source NAT Pool Prefix (SRX Only)

☑ Access to MIST Cloud
☑ Advertise to the Overlay
☑ Advertise to Other Spokes
☐ Overlay Summarization
☑ Advertise to Hub LAN BGP Neighbor
☐ Hub LAN BGP Summarization
☐ Override Prefix To Advertise

IP Address {{HUB1_LAN1_PFX}}.0 / Prefix Length 24

Networks Not Directly Attached (SSR Only)

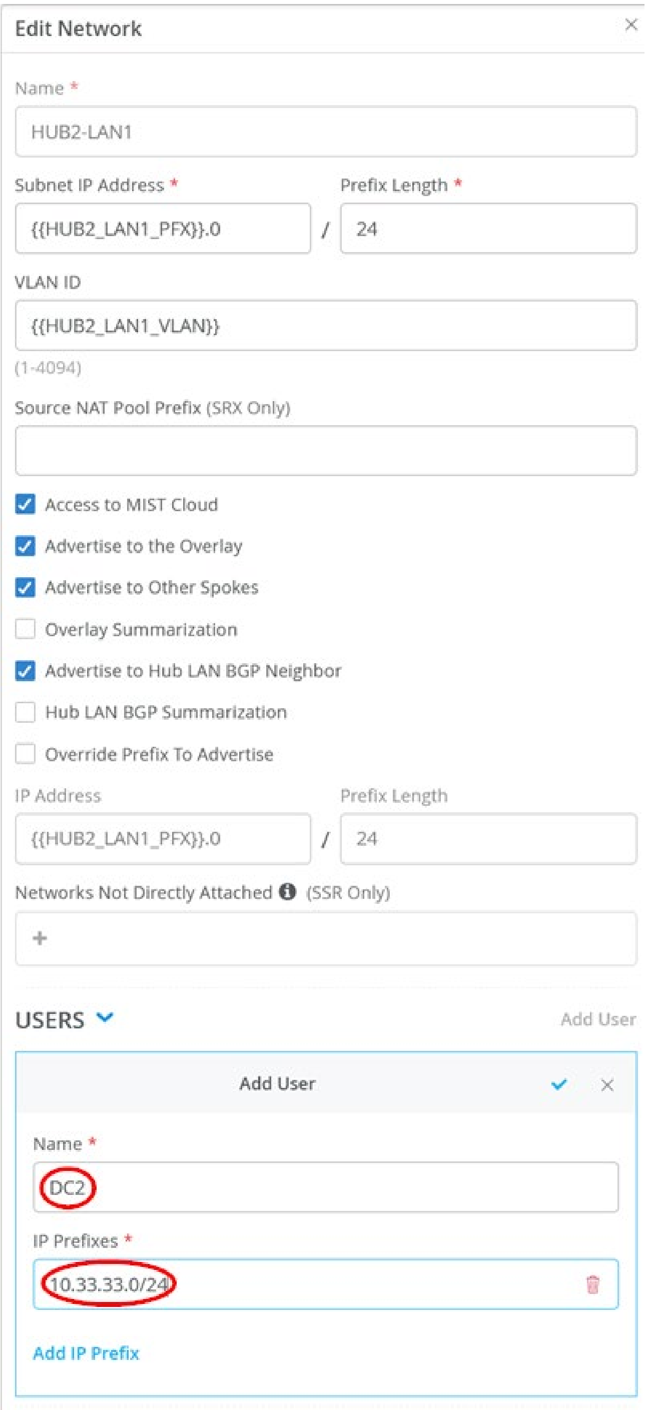
USERS

Add User

Name *
DC1

IP Prefixes *
10.44.44.0/24

- Edit exiting Network called "HUB2-LAN1"
  - Add under Users a new Object with the Name: "DC2" and IP Prefix: "10.33.33.0/24".



Edit Network

Name *

HUB2-LAN1

Subnet IP Address * {{HUB2_LAN1_PFX}}.0 / Prefix Length * 24

VLAN ID

{{HUB2_LAN1_VLAN}}

(1-4094)

Source NAT Pool Prefix (SRX Only)

☑ Access to MIST Cloud

☑ Advertise to the Overlay

☑ Advertise to Other Spokes

□ Overlay Summarization

☑ Advertise to Hub LAN BGP Neighbor

□ Hub LAN BGP Summarization

□ Override Prefix To Advertise

IP Address {{HUB2_LAN1_PFX}}.0 / Prefix Length 24

Networks Not Directly Attached (SSR Only)

USERS

Add User

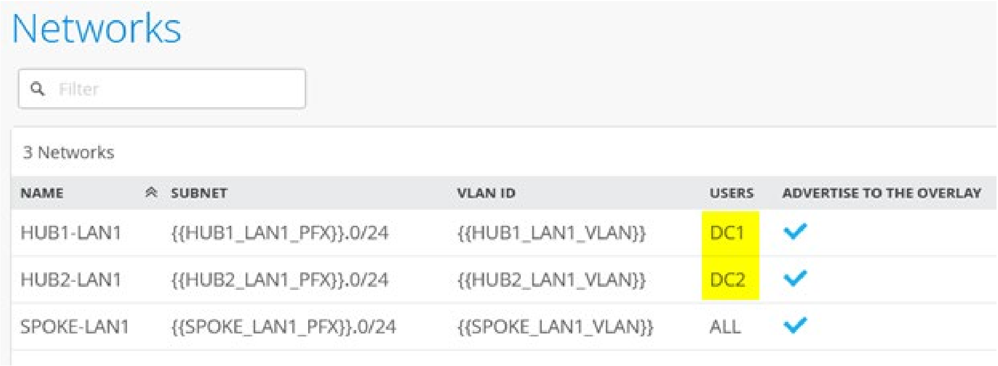
Name *

DC2

IP Prefixes *

10.33.33.0/24

After you have made the required changes your Networks overview should now show the added objects like below.



Networks

Filter

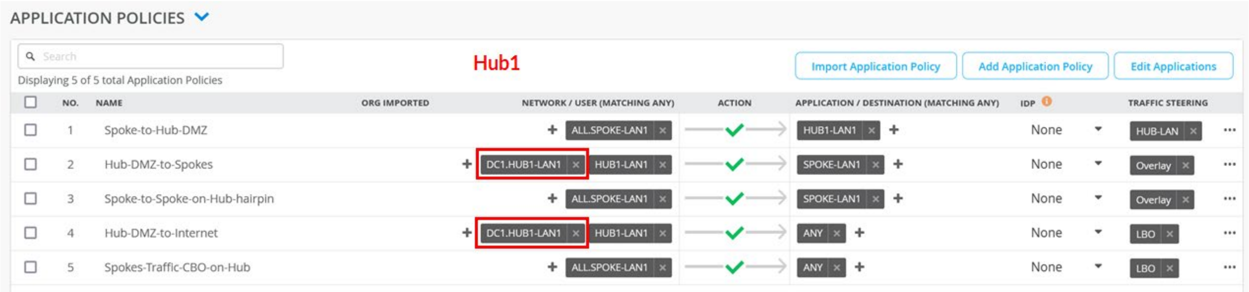
3 Networks

| NAME | SUBNET | VLAN ID | USERS | ADVERTISE TO THE OVERLAY |
|---|---|---|---|---|
| HUB1-LAN1 | {{HUB1_LAN1_PFX}}.0/24 | {{HUB1_LAN1_VLAN}} | DC1 | ✓ |
| HUB2-LAN1 | {{HUB2_LAN1_PFX}}.0/24 | {{HUB2_LAN1_VLAN}} | DC2 | ✓ |
| SPOKE-LAN1 | {{SPOKE_LAN1_PFX}}.0/24 | {{SPOKE_LAN1_VLAN}} | ALL | ✓ |

Just extending the “Users”-Object is however not enough yet. We also need now to extend the Application Policies on each Hub to recognize those additional statements.

- Go to **Organization > Hub Profiles**
- Edit exiting Hub Profile “hub1” . Everywhere we have defined HUB1-LAN1 we must also now add the Users-Object “DC1.HUB1-LAN1”. This is our case will be:
  - Add to the second Rule called “Hub-DMZ-to-Spokes” the User “DC1.HUB1-LAN1”.
  - Add to the fourth Rule called “Hub-DMZ-to-Internet” the User “DC1.HUB1-LAN1”.

Your changes should look like in the below Figure now.



APPLICATION POLICIES

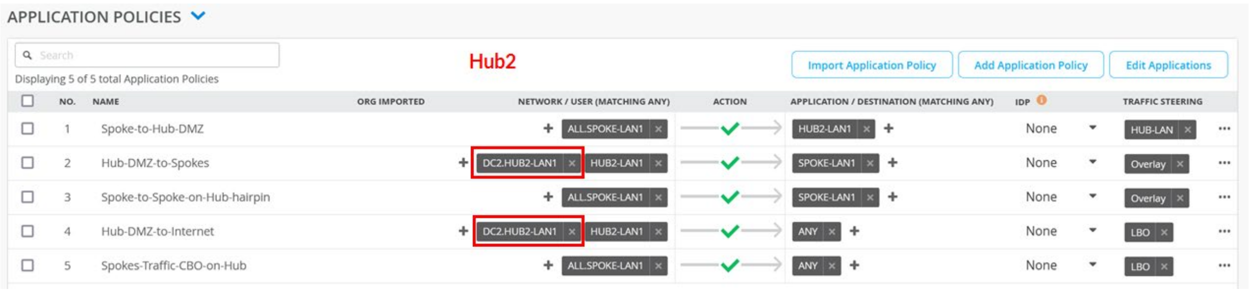
Hub1

Displaying 5 of 5 total Application Policies

| NO. | NAME | ORG IMPORTED | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| 1 | Spoke-to-Hub-DMZ | | ALL.SPOKE-LAN1 | ✓ | HUB1-LAN1 | None | HUB-LAN |
| 2 | Hub-DMZ-to-Spokes | | DC1.HUB1-LAN1<br>HUB1-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| 3 | Spoke-to-Spoke-on-Hub-hairpin | | ALL.SPOKE-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| 4 | Hub-DMZ-to-Internet | | DC1.HUB1-LAN1<br>HUB1-LAN1 | ✓ | ANY | None | LBO |
| 5 | Spokes-Traffic-CBO-on-Hub | | ALL.SPOKE-LAN1 | ✓ | ANY | None | LBO |

- Edit exiting Hub Profile “hub2” . Everywhere we have defined HUB2-LAN1 we must also now add the Users-Object “DC2.HUB2-LAN1”. This is our case will be:
  - Add to the second Rule called “Hub-DMZ-to-Spokes” the User “DC2.HUB2-LAN1”.
  - Add to the fourth Rule called “Hub-DMZ-to-Internet” the User “DC2.HUB2-LAN1”.

Your changes should look like in the below Figure now.



APPLICATION POLICIES

Hub2

Displaying 5 of 5 total Application Policies

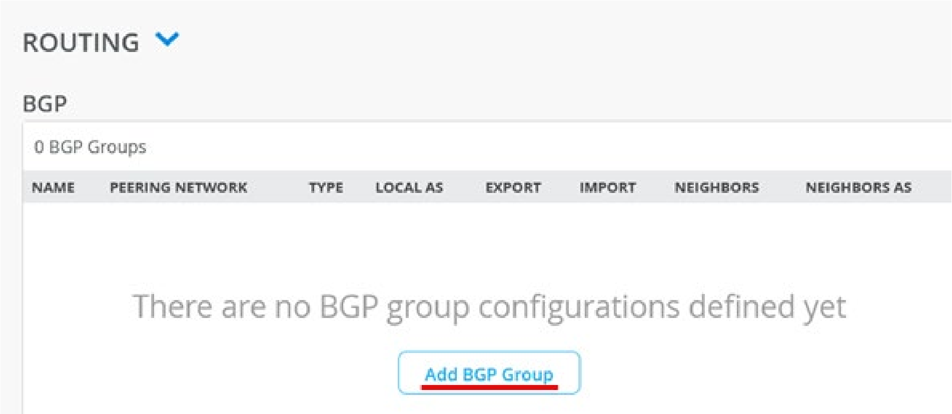
| NO. | NAME | ORG IMPORTED | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| 1 | Spoke-to-Hub-DMZ | | ALL.SPOKE-LAN1 | ✓ | HUB2-LAN1 | None | HUB-LAN |
| 2 | Hub-DMZ-to-Spokes | | DC2.HUB2-LAN1<br>HUB2-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| 3 | Spoke-to-Spoke-on-Hub-hairpin | | ALL.SPOKE-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| 4 | Hub-DMZ-to-Internet | | DC2.HUB2-LAN1<br>HUB2-LAN1 | ✓ | ANY | None | LBO |
| 5 | Spokes-Traffic-CBO-on-Hub | | ALL.SPOKE-LAN1 | ✓ | ANY | None | LBO |

This ends the need for extensions for the Firewall ruleset and we can now configure the BGP Peer exchange.

Adding BGP Peers

We can now configure the route exchange with the Datacenter Routers.

- Go to **Organization > Hub Profiles**
- Edit exiting Hub Profile “hub1”.
- Under Routing > BGP add a new BGP Group



ROUTING

BGP

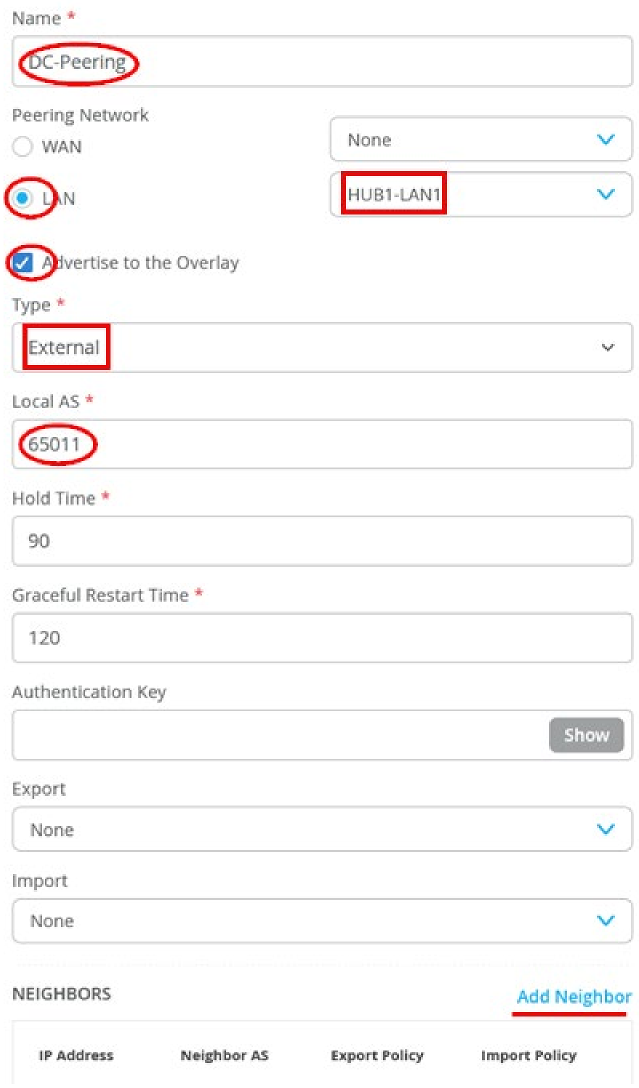
0 BGP Groups

| NAME | PEERING NETWORK | TYPE | LOCAL AS | EXPORT | IMPORT | NEIGHBORS | NEIGHBORS AS |
|---|---|---|---|---|---|---|---|

There are no BGP group configurations defined yet

Configure the following for this new BGP-Peer:

- Name: “DC-Peering”
- Peering Network: “LAN” and select “HUB1-LAN1”
- Advertise to the Overlay: Enabled/Checked
- Type: “External”
- Local AS: “65011”
- Under Add Neighbor:
  - IP address: “10.66.66.66”
  - Neighbor AS: “65012”



Name *

DC-Peering

Peering Network

○ WAN None

● LAN HUB1-LAN1

☑ Advertise to the Overlay

Type *

External

Local AS *

65011

Hold Time *

90

Graceful Restart Time *

120

Authentication Key

Export

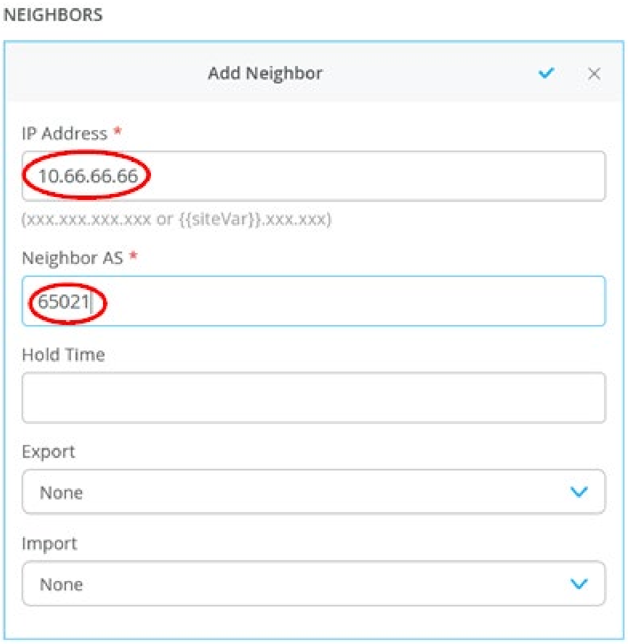
None

Import

None

NEIGHBORS

| IP Address | Neighbor AS | Export Policy | Import Policy |
|---|---|---|---|



NEIGHBORS

Add Neighbor ✓ ✕

IP Address *

10.66.66.66

(xxx.xxx.xxx.xxx or {{siteVar}}.xxx.xxx)

Neighbor AS *

65021

Hold Time

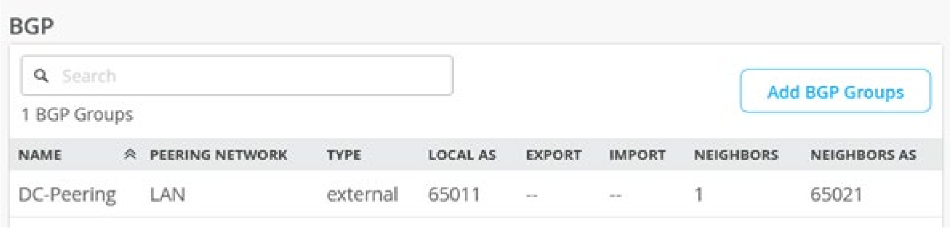
Export

None

Import

None

Your changes should now look like the ones in the Figure below.



BGP

Search

Add BGP Groups

1 BGP Groups

| NAME | PEERING NETWORK | TYPE | LOCAL AS | EXPORT | IMPORT | NEIGHBORS | NEIGHBORS AS |
|---|---|---|---|---|---|---|---|
| DC-Peering | LAN | external | 65011 | -- | -- | 1 | 65021 |

- “Save” your changes so that the system activates them.

Note: It is now assumed that you configure the first Datacenter Router with the reverse entries about BGP-Peering. The exact configuration is not shown here.

After the remote Peer is also configured and does exchange routes with the Hub its best using a Remote Shell to see if everything is fine. The below shows that we have an established peering with the Data center router.

```
root@hub1> show bgp summary
Threading mode: BGP I/O
Default eBGP mode: advertise - accept, receive - accept
Groups: 2 Peers: 5 Down peers: 0
Unconfigured peers: 3
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn
State|#Active/Received/Accepted/Damped...
10.66.66.66           65021          3          3       0       0          17 Establ
  lan.inet.0: 1/1/1/0
100.101.0.2           65000        207        211       0       1     1:31:03 Establ
  vpn_OrgOverlay.inet.0: 1/5/5/0
.
```

Now review the routing table for the lan-Interfaces if that new additional route appears which is the case in the example below.

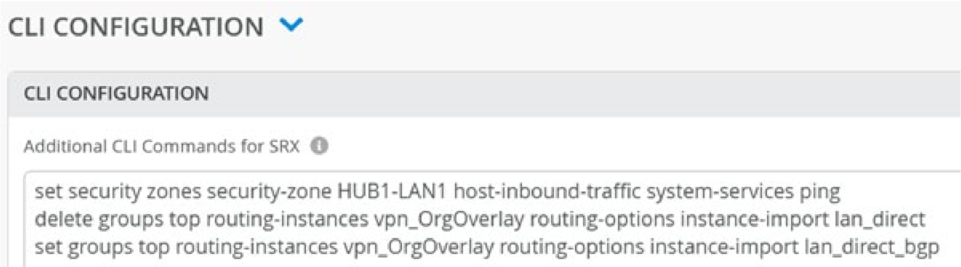
```
root@hub1> show route table lan.inet.0

lan.inet.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 02:15:08
                    >  to 192.168.190.1 via ge-0/0/3.0
10.44.44.0/24      *[BGP/170] 00:03:56, localpref 100
                      AS path: 65021 I, validation-state: unverified
                    >  to 10.66.66.66 via ge-0/0/4.1066
10.66.66.0/24      *[Direct/0] 02:15:23
                    >  via ge-0/0/4.1066
10.66.66.1/32      *[Local/0] 02:15:23
                       Local via ge-0/0/4.1066
.
```

The next step is to verify if that route exactly also appears in the Overlay so that the Spoke can also see them. The below CLI is our succeeded verification.

```
root@hub1> show route table vpn_OrgOverlay.inet.0 10.44.44.44

vpn_OrgOverlay.inet.0: 37 destinations, 41 routes (37 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.44.44.0/24      *[BGP/170] 00:42:26, localpref 100
                      AS path: 65021 I, validation-state: unverified
                    >  to 10.66.66.66 via ge-0/0/4.1066
```

**BUG:** If the above verification shows only a default route or nothing, then you may hit a bug that was found during the JVD eval. The system at that time did only import direct (LAN-Interface routes) towards the VPN-Overlay and not our additional BGP learned Routes. There is workaround via additional Junos CLI to change this behavior to the needed. Simply add the two lines below deleting the wrong import rule and adding the needed import rule. You see an example below.

```
set security zones security-zone HUB1-LAN1 host-inbound-traffic system-services ping
delete groups top routing-instances vpn_OrgOverlay routing-options instance-import
lan_direct
set groups top routing-instances vpn_OrgOverlay routing-options instance-import
lan_direct_bgp
```

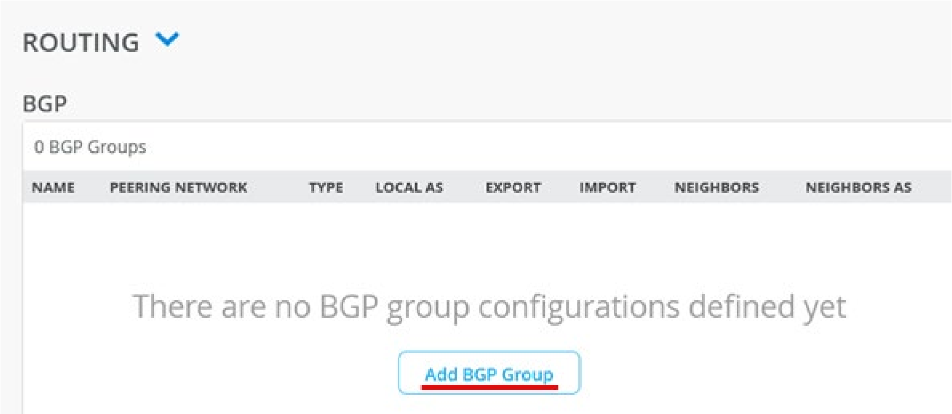


```
set security zones security-zone HUB1-LAN1 host-inbound-traffic system-services ping
delete groups top routing-instances vpn_OrgOverlay routing-options instance-import lan_direct
set groups top routing-instances vpn_OrgOverlay routing-options instance-import lan_direct_bgp
```

Now we can test if Spokes can reach services that are reachable via the Datacenter Router of Hub1. We utilize desktop1 VM (IP address:10.99.99.99) to ping desktop6 VM (IP address:10.44.44.44) which succeeds.

```
root@desktop1:~# ping 10.44.44.44
PING 10.44.44.44 (10.44.44.44) 56(84) bytes of data.
64 bytes from 10.44.44.44: icmp_seq=1 ttl=61 time=1.41 ms
64 bytes from 10.44.44.44: icmp_seq=2 ttl=61 time=1.88 ms
64 bytes from 10.44.44.44: icmp_seq=3 ttl=61 time=1.88 ms
.
```

- Go to **Organization > Hub Profiles**
- Edit exiting Hub Profile “hub2”.
- Under Routing > BGP add a new BGP Group



ROUTING

BGP

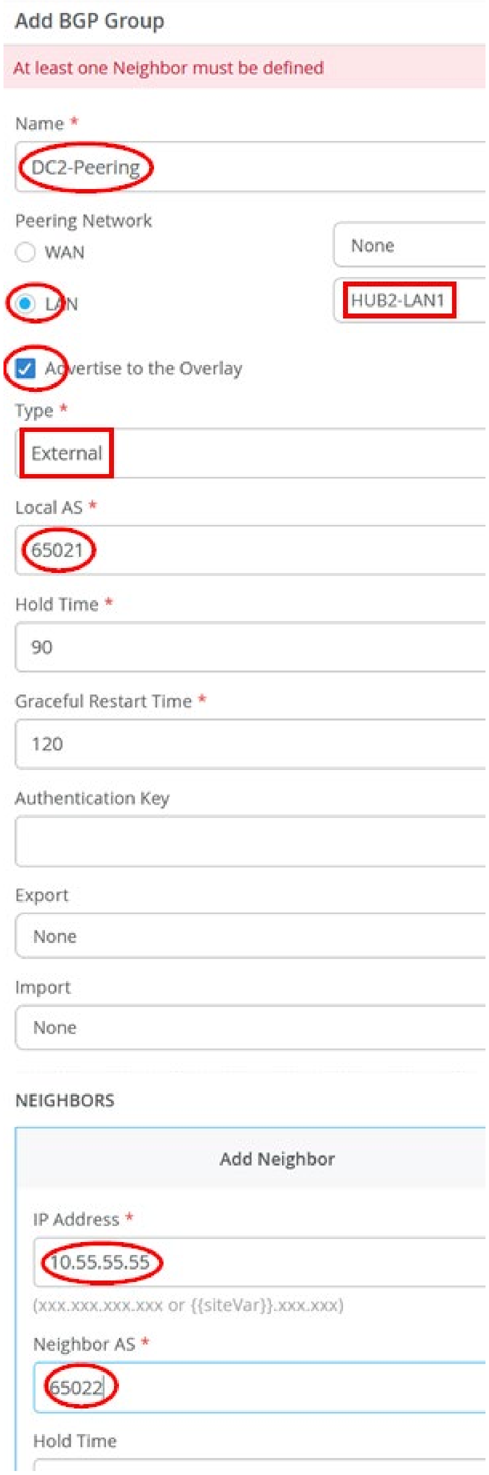
0 BGP Groups

| NAME | PEERING NETWORK | TYPE | LOCAL AS | EXPORT | IMPORT | NEIGHBORS | NEIGHBORS AS |
|---|---|---|---|---|---|---|---|

There are no BGP group configurations defined yet

Configure the following for this new BGP-Peer:

- Name: “DC2-Peering”
- Peering Network: “LAN” and select “HUB2-LAN1”
- Advertise to the Overlay: Enabled/Checked
- Type: “External”
- Local AS: “65021”
- Under Add Neighbor:
  - IP address: “10.55.55.55”
  - Neighbor AS: “65052”


Add BGP Group

At least one Neighbor must be defined

Name * DC2-Peering

Peering Network
○ WAN None
● LAN HUB2-LAN1

☑ Advertise to the Overlay

Type * External

Local AS * 65021

Hold Time * 90

Graceful Restart Time * 120

Authentication Key

Export None

Import None

NEIGHBORS

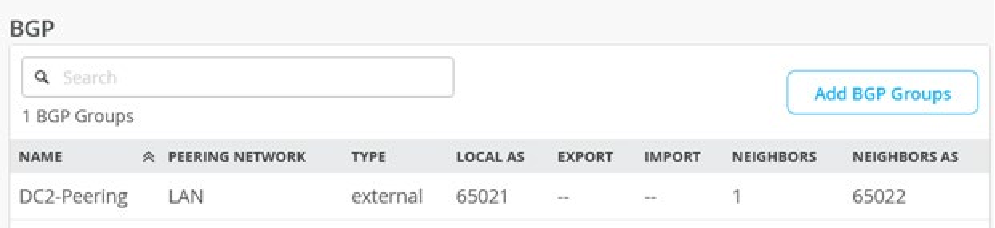
Add Neighbor

IP Address * 10.55.55.55
(xxx.xxx.xxx.xxx or {{siteVar}}.xxx.xxx)

Neighbor AS * 65022

Hold Time

Your changes should now look like the ones in the Figure below.



1 BGP Groups

| NAME | PEERING NETWORK | TYPE | LOCAL AS | EXPORT | IMPORT | NEIGHBORS | NEIGHBORS AS |
|---|---|---|---|---|---|---|---|
| DC2-Peering | LAN | external | 65021 | -- | -- | 1 | 65022 |

- “Save” your changes so that the system activates them.

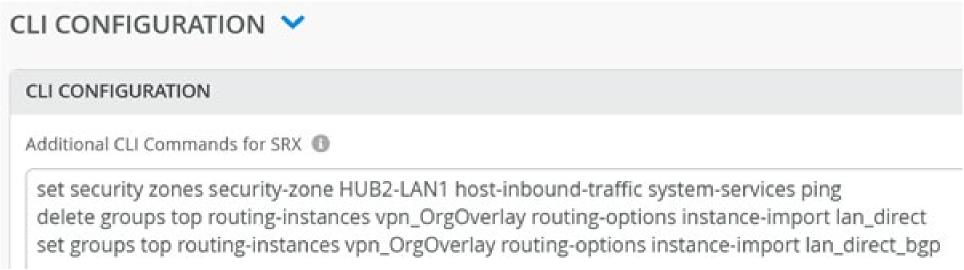
> Note: It is now assumed that you configure the second Datacenter Router with the reverse entries about BGP-Peering. The exact configuration is not shown here.

- Execute the evaluation via remote Shell as already shown for Hub1 again with the proper values like in below example:

```
show bgp summary
show route table lan.inet.0
show route table vpn_OrgOverlay.inet.0 10.33.33.33
```

You may need to apply the same workaround as already shown above.

```
set security zones security-zone HUB2-LAN1 host-inbound-traffic system-services ping
delete groups top routing-instances vpn_OrgOverlay routing-options instance-import
lan_direct
set groups top routing-instances vpn_OrgOverlay routing-options instance-import
lan_direct_bgp
```



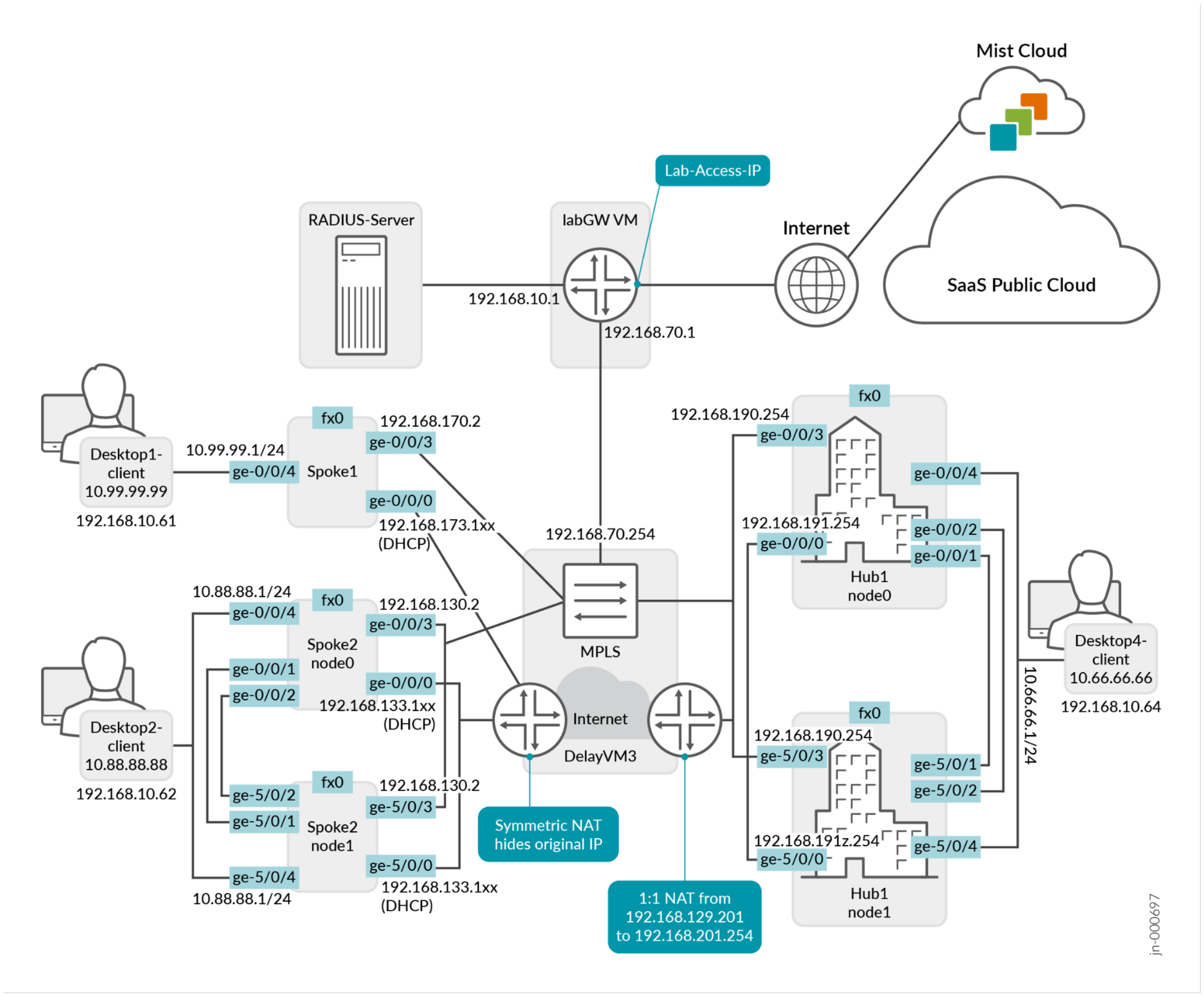
```
set security zones security-zone HUB2-LAN1 host-inbound-traffic system-services ping
delete groups top routing-instances vpn_OrgOverlay routing-options instance-import lan_direct
set groups top routing-instances vpn_OrgOverlay routing-options instance-import lan_direct_bgp
```

Now we can test if Spokes can reach services that are reachable via the Datacenter Router of Hub1. We utilize desktop1 VM (IP address:10.99.99.99) to ping desktop7 VM (IP address:10.33.33.33) which succeeds.

```
root@desktop1:~# ping 10.33.33.33
PING 10.33.33.33 (10.33.33.33) 56(84) bytes of data.
64 bytes from 10.33.33.33: icmp_seq=1 ttl=61 time=1.45 ms
64 bytes from 10.33.33.33: icmp_seq=2 ttl=61 time=1.90 ms
64 bytes from 10.33.33.33: icmp_seq=3 ttl=61 time=1.59 ms
.
```

# Topology with clustered SRX Highly Available Spoke and Hub

In this chapter we will implement the third topology that we have discussed above and show you the entire workflow by this. **This design only shows the changes from the first design and not the complete process again.** We assume you learnt the basics already with the first topology hence we keep this crips and only show the diffs to that.



One of the most important considerations for WAN design is High Availability. High availability ensures business continuity and disaster recovery by maximizing the availability and increasing redundancy within and across different sites.

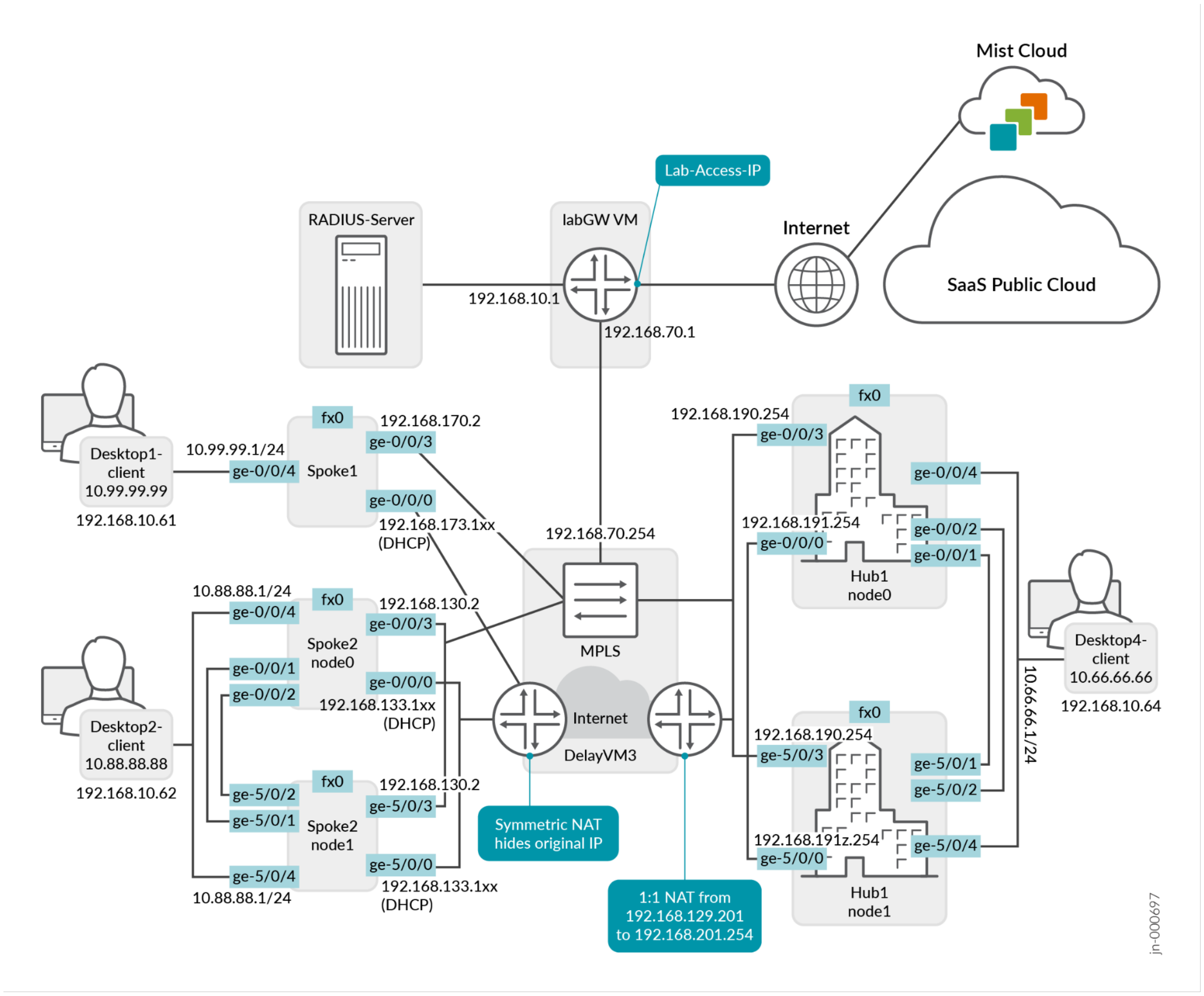
Juniper SRX Series Firewall High Availability (HA) design example is for administrators who want to deploy HA Juniper SRX Series Firewall at the Edge, but not for Whitebox setups.

In this documentation, you'll find step-by-step guidance for setting up a highly available hub and spoke deployment using SRX Series Firewalls. Since this HA deployment builds upon the configurations referenced in the Juniper® Mist WAN Assurance configuration, you'll need to configure your network with those settings first. In this example, you'll learn how to setup SRX Series Firewalls in an HA cluster configuration.

Overview

You will deploy a highly available Hub and Spoke as shown in the Figure below. Here we see the SRX Series highly available Juniper Mist WAN Assurance topology for this HA Design Guide.

Figure47: Juniper Validated Design Mist WAN Assurance with HA SRX Series WAN Edges



The topology uses one standalone and one high-available cluster setup of spoke and high-available cluster setup of hub on the other side.

The supported SRX Series high-available clustering for the WAN edge deployment requires local Layer2 adjacency for a spoke or a hub setup.

## Before You Begin

- Understand how to configure high-availability cluster with SRX Series Firewalls.
- The two clustered devices need to be:
  - Same Device Type
  - Have all needed Licenses applied individually on each device.
  - Have a local Layer-2 adjacency (else review the second Topology with Hub-Mesh).
- You'll need a dedicated HA-control interface that is defined by the device type. This interface is connected usually using a patch cable between the two devices. You must use the same port for HA control interface. To know which port your device supports, see Understanding SRX Series Chassis Cluster Slot Numbering and Physical Port and Logical Interface Naming.

- The WAN edge configuration might automatically select the fabric interface next to the HA control interface. For details, log in https://manage.mist.com and refer documentation.
- You'll need a dedicated fabric-data interface. This interface is connected usually using a patchable between the two devices. For WAN edge configuration, selecting any port as fabric port is not supported. We recommend using the port the one next to the control port. Also see https://api.mist.com/api/v1/docs/Site#ha-cluster
- Similar to virtual chassis, the ports on the secondary node are renumbered after the formation of chassis cluster.
- Building the Cluster always involves the configuring two nodes and rebooting them after initial commands issues to build the cluster. See Example: Setting the Node ID and Cluster ID for Security Devices in a Chassis Cluster .

## Interface Details for HA Cluster

The following examples show interfaces usage for the chassis cluster configuration recommended. You might note that for SRX 300/320 we do NOT have the ability to utilize Interface ge-0/0/0 to boot the System and connect it with the Internet providing access to the Mist cloud. This is because this interface will get used for a different purpose when building the cluster. Hence, we leverage on those devices Port ge-0/0/7 (which requires to plan for an additional SFP) as the other Ports do not ask for a DHCP-Lease.

Primary Node0 Interface Table

| Device | MGM (fxp0) | HA Control | Fabric Data | WAN0 ZTP-IF | WAN1 | LAN1 | LAN2 optional |
|---|---|---|---|---|---|---|---|
| vSRX-N0 | Mgmt | em0 | ge-0/0/0 | ge-0/0/1 | ge-0/0/3 | ge-0/0/4 | ge-0/0/5 |
| SRX300-N0 | ge-0/0/0 | ge-0/0/1 | ge-0/0/2 | ge-0/0/7 | ge-0/0/3 | ge-0/0/4 | ge-0/0/5 |
| SRX320-N0 | ge-0/0/0 | ge-0/0/1 | ge-0/0/2 | ge-0/0/7 | ge-0/0/3 | ge-0/0/4 | ge-0/0/5 |
| SRX340-N0 | Mgmt | ge-0/0/1 | ge-0/0/2 | ge-0/0/0 | ge-0/0/3 | ge-0/0/4 | ge-0/0/5 |
| SRX345-N0 | Mgmt | ge-0/0/1 | ge-0/0/2 | ge-0/0/0 | ge-0/0/3 | ge-0/0/4 | ge-0/0/5 |
| SRX380-N0 | Mgmt | ge-0/0/1 | ge-0/0/2 | ge-0/0/0 | ge-0/0/3 | ge-0/0/4 | ge-0/0/5 |
| SRX550-N0 | Mgmt | ge-0/0/1 | ge-0/0/2 | ge-0/0/0 | ge-0/0/3 | ge-0/0/4 | ge-0/0/5 |
| SRX1500-N0 | Mgmt | ha_control | ge-0/0/1 | ge-0/0/0 | ge-0/0/3 | ge-0/0/4 | ge-0/0/5 |
| SRX4100-N0 | Mgmt | ha_control | ha_data | xe-0/0/0 | xe-0/0/3 | xe-0/0/4 | xe-0/0/5 |
| SRX4200-N0 | Mgmt | ha_control | ha_data | xe-0/0/0 | xe-0/0/3 | xe-0/0/4 | xe-0/0/5 |
| SRX4600-N0 | Mgmt | ha_control | ha_data | xe-1/0/0 | xe-1/0/3 | xe-1/0/4 | xe-1/0/5 |

Once you configure the chassis cluster and reboot both the nodes, the second node (node 1) renumbers its interfaces as shown in the following sample. You must use the interface numbering when you configure the second WAN/LAN interface in the Juniper Mist portal.

Secondary Node1 Interface Table RENUMBERING

| Device | MGMT (fxp0) | HA Control | Fabric Data | WAN0 ZTP-IF | WAN1 | LAN1 | LAN2 optional |
|---|---|---|---|---|---|---|---|
| vSRX-N1 | Mgmt | em0 | ge-7/0/0 | ge-7/0/1 | ge-7/0/3 | ge-7/0/4 | ge-7/0/5 |
| SRX300-N1 | ge-1/0/0 | ge-1/0/1 | ge-1/0/2 | ge-1/0/7 | ge-1/0/3 | ge-1/0/4 | ge-1/0/5 |
| SRX320-N1 | ge-3/0/0 | ge-3/0/1 | ge-3/0/2 | ge-3/0/7 | ge-3/0/3 | ge-3/0/4 | ge-3/0/5 |
| SRX340-N1 | Mgmt | ge-5/0/1 | ge-5/0/2 | ge-5/0/0 | ge-5/0/3 | ge-5/0/4 | ge-5/0/5 |
| SRX345-N1 | Mgmt | ge-5/0/1 | ge-5/0/2 | ge-5/0/0 | ge-5/0/3 | ge-5/0/4 | ge-5/0/5 |
| SRX380-N1 | Mgmt | ge-5/0/1 | ge-5/0/2 | ge-5/0/0 | ge-5/0/3 | ge-5/0/4 | ge-5/0/5 |
| SRX550-N1 | Mgmt | ge-9/0/1 | ge-9/0/2 | ge-9/0/0 | ge-9/0/3 | ge-9/0/4 | ge-9/0/5 |
| SRX1500-N1 | Mgmt | ha_control | ge-7/0/1 | ge-7/0/0 | ge-7/0/3 | ge-7/0/4 | ge-7/0/5 |
| SRX4100-N1 | Mgmt | ha_control | ha_data | xe-7/0/0 | xe-7/0/3 | xe-7/0/4 | xe-7/0/5 |
| SRX4200-N1 | Mgmt | ha_control | ha_data | xe-7/0/0 | xe-7/0/3 | xe-7/0/4 | xe-7/0/5 |
| SRX4600-N1 | Mgmt | ha_control | ha_data | xe-8/0/0 | xe-8/0/3 | xe-8/0/4 | xe-8/0/5 |

HA Interfaces

Each path and Node in an HA network require their own designated WAN interface. This ensures Active/Active usage, meaning that these interfaces stay active and engaged, no matter what. The WAN interfaces can contain either a static IP address or be linked to a DHCP-Lease, giving you flexibility in how you manage them.

In certain scenarios, you may be limited to just one WAN IP address, especially for MPLS Networks. In these cases, you can configure the interface as a shared VRRP interface between two Nodes. This sets up an Active/Passive usage of the links, maintaining the balance and ensuring continuity. A second IP address for that second node enhances your setup's performance even further.

## Configure High Availability

You should have already configured **Networks**, **Applications**, **Sites**, **Variables**, **Hub Profiles** and **WAN Edge Templates**. If these steps are new to you, please follow the Mist WAN Configuration Guide first before proceeding with the HA design guide.

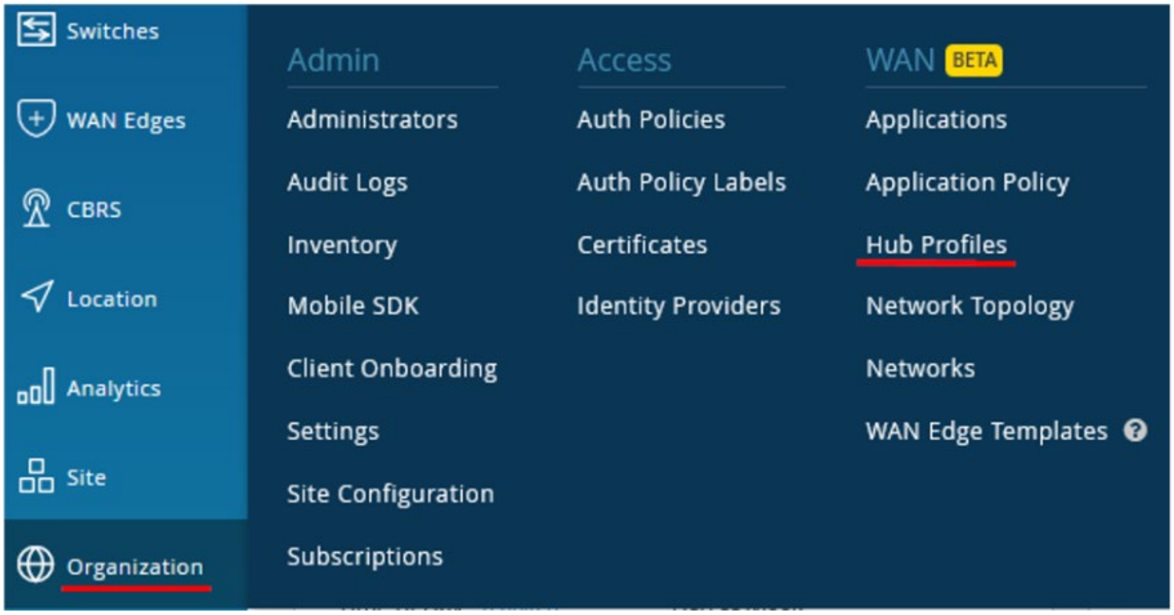
The following steps outline the process of creating high availability cluster.

## Create a New Hub Profile

Now it's time to add the second Node in your highly available Hub. In this next step, you'll create a new Hub profile by cloning the existing one. Then, you'll modify the clone to meet new requirements for the HA hub.

- In the Juniper Mist cloud portal, click **Organization** > **WAN** > **Hub Profiles**.

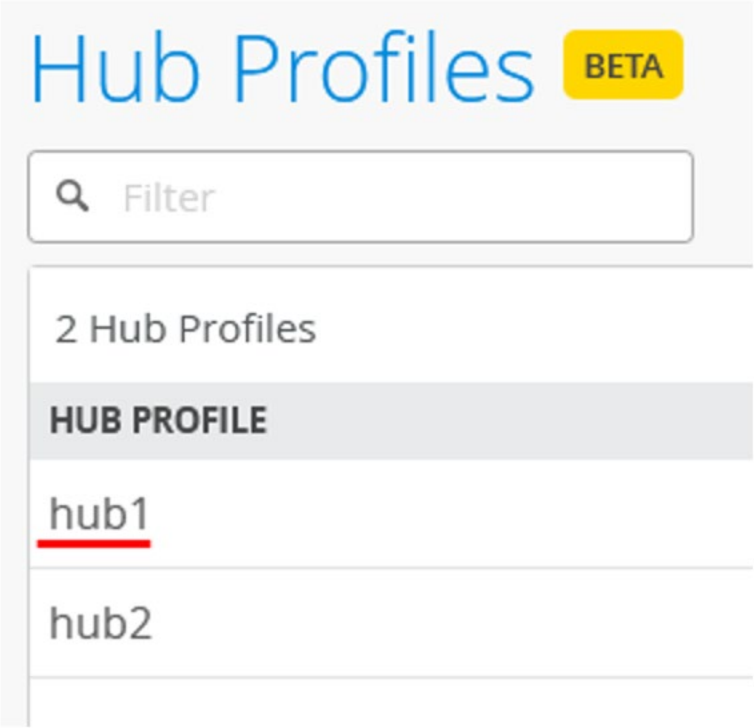
Figure48: Configure Hub Profiles



A list of existing hub profiles, if any, appears.

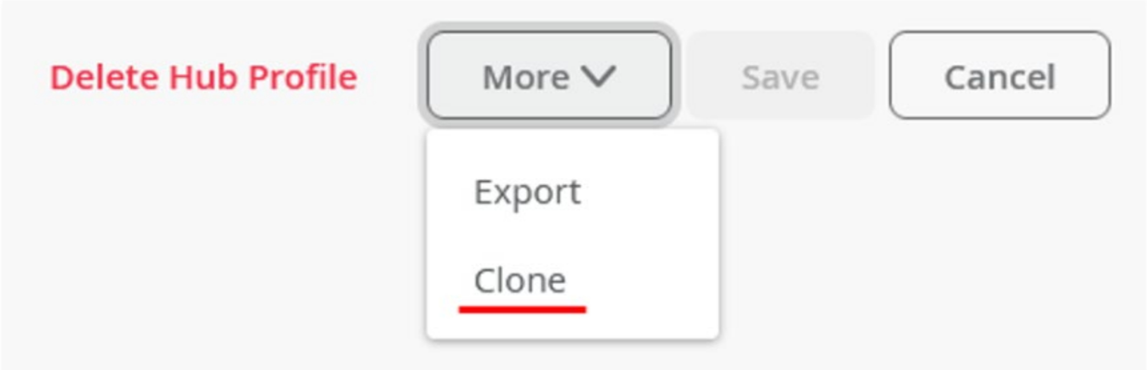
- Click the hub profile (hub1) that you want to clone.

Figure49: Select Hub Profile for Cloning



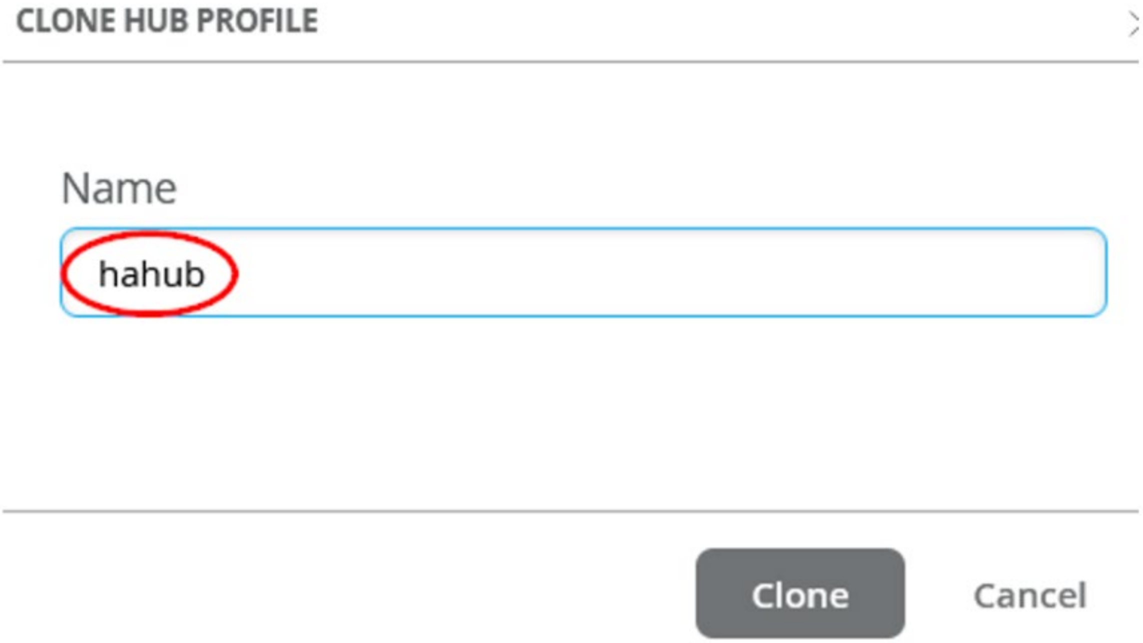
- In the upper right corner of the screen, click **More** and select **Clone**.

Figure50: Selecting Clone Option



- Name the new profile (**hahub**) and click **Clone**.

Figure51: Rename Cloned Hub Profile


CLONE HUB PROFILE

Name: hahub

**Note**: After you clone, refresh your browser. This makes sure everything updates properly.

- Modify the new profile and create four new WAN interfaces. Delete the existing WAN interfaces from the clone and configure the WAN interfaces according to the details provided in the Table below.

Table 30: WAN Interfaces Details in Hub Profile

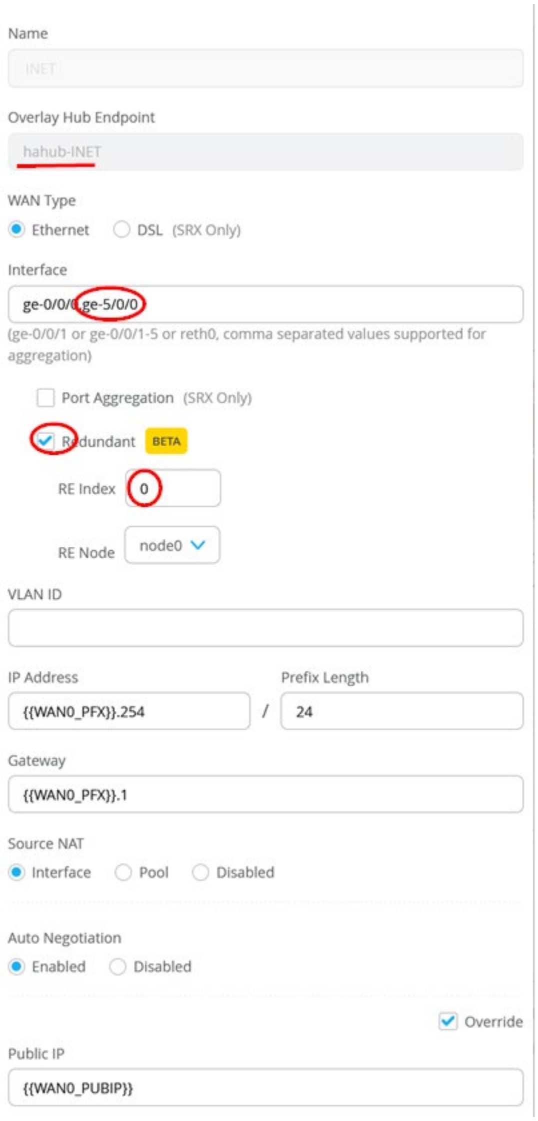
| Option | First WAN | Second WAN |
|---|---|---|
| Name: (This indicates which topology it uses.) | INET | MPLS |
| Interface | ge-0/0/0, ge-5/0/0 | ge-0/0/3, ge-5/0/3 |
| Redundant | Enabled | Enabled |
| RE Index (as a convention, use the last octet as index) | 0 | 0 |

For the WAN interfaces, we've added a redundant interface according to the secondary node interface naming convention used for SRX340 to SRX380. Ensure that you use correct interfaces as per the SRX Series device you are configuring. IP Address, prefix, gateway and public IP address remain same.

The portal generates the overlay hub endpoints as **hahub-INET** and **hahub-MPLS** automatically.

The Table below shows WAN interface configuration.

Figure52: WAN Interface Configuration (First)



Name

INET

Overlay Hub Endpoint

hahub-INET

WAN Type

● Ethernet ○ DSL (SRX Only)

Interface

ge-0/0/0,ge-5/0/0

(ge-0/0/1 or ge-0/0/1-5 or reth0, comma separated values supported for aggregation)

□ Port Aggregation (SRX Only)

☑ Redundant BETA

RE Index 0

RE Node node0

VLAN ID

IP Address {{WAN0_PFX}}.254 / Prefix Length 24

Gateway

{{WAN0_PFX}}.1

Source NAT

● Interface ○ Pool ○ Disabled

Auto Negotiation

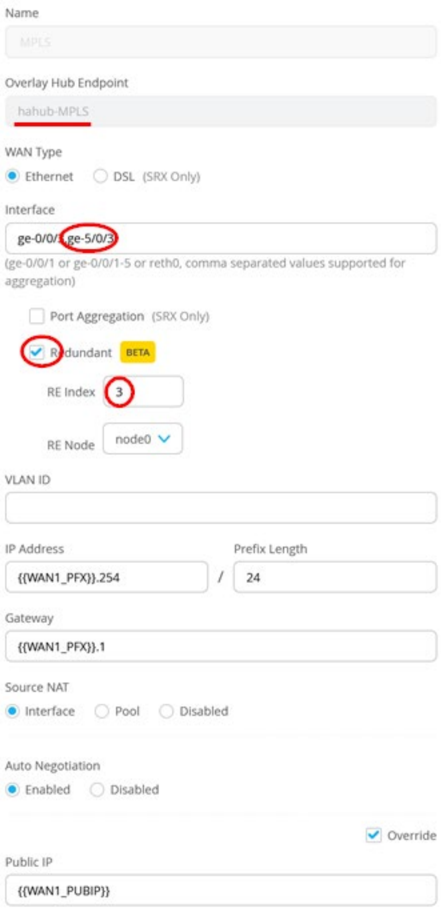
● Enabled ○ Disabled

☑ Override

Public IP

{{WAN0_PUBIP}}

Figure53: WAN Interface Configuration (Second)



Name

MPLS

Overlay Hub Endpoint

hahub-MPLS

WAN Type

● Ethernet ○ DSL (SRX Only)

Interface

ge-0/0/1,ge-5/0/3

(ge-0/0/1 or ge-0/0/1-5 or reth0, comma separated values supported for aggregation)

□ Port Aggregation (SRX Only)

☑ Redundant BETA

RE Index 3

RE Node node0

VLAN ID

IP Address / Prefix Length

{{WAN1_PFX}}.254 / 24

Gateway

{{WAN1_PFX}}.1

Source NAT

● Interface ○ Pool ○ Disabled

Auto Negotiation

● Enabled ○ Disabled

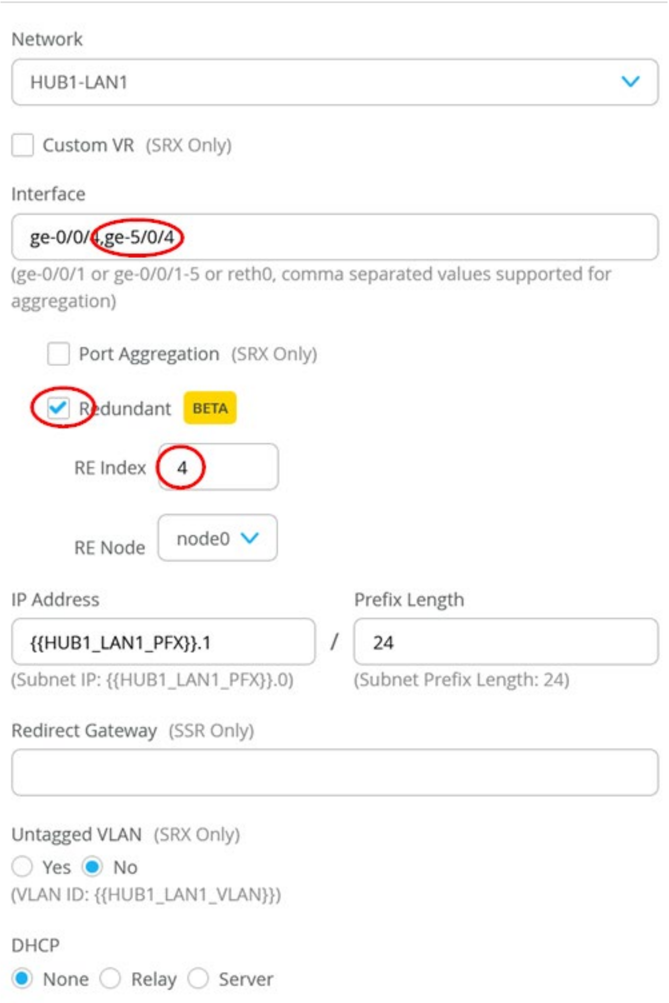
☑ Override

Public IP

{{WAN1_PUBIP}}

- Complete the configuration for the LAN interface.

Figure54: LAN Interface Configuration



Network

HUB1-LAN1

□ Custom VR (SRX Only)

Interface

ge-0/0/4,ge-5/0/4

(ge-0/0/1 or ge-0/0/1-5 or reth0, comma separated values supported for aggregation)

□ Port Aggregation (SRX Only)

☑ Redundant BETA

RE Index 4

RE Node node0

IP Address {{HUB1_LAN1_PFX}}.1 / Prefix Length 24

(Subnet IP: {{HUB1_LAN1_PFX}}.0) (Subnet Prefix Length: 24)

Redirect Gateway (SSR Only)

Untagged VLAN (SRX Only)

○ Yes ● No

(VLAN ID: {{HUB1_LAN1_VLAN}})

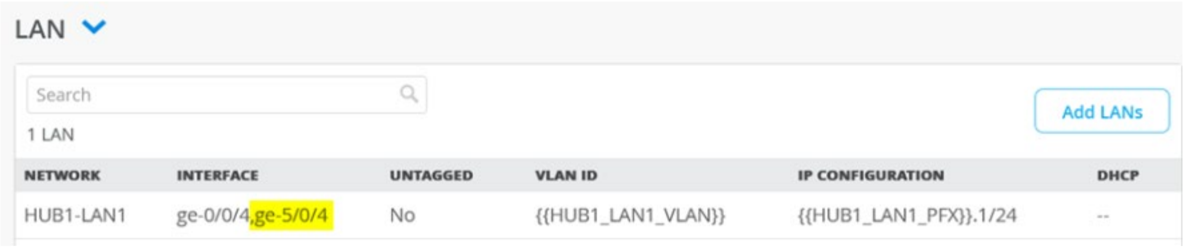
DHCP

● None ○ Relay ○ Server

- Configure LAN interface with the following details:
  - **Interfaces**: ge-0/0/4,ge-5/0/4
  - **Redundant**: Enabled
  - **RE Index**: 4 (As a convention, use the last octet as an index).

  **Note**: IP address and prefix do not change.

Figure55: LAN Interface Configuration



LAN

Search

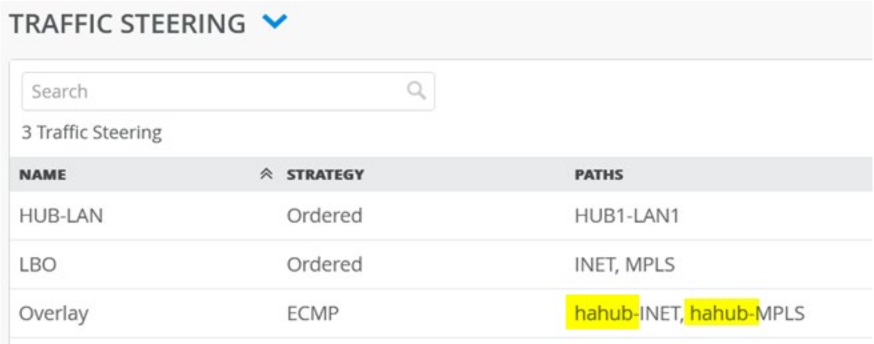
Add LANs

1 LAN

| NETWORK | INTERFACE | UNTAGGED | VLAN ID | IP CONFIGURATION | DHCP |
|---|---|---|---|---|---|
| HUB1-LAN1 | ge-0/0/4,ge-5/0/4 | No | {{HUB1_LAN1_VLAN}} | {{HUB1_LAN1_PFX}}.1/24 | -- |

- Update the traffic steering rules for the new endpoint names.

Figure56: Traffic Steering Rules



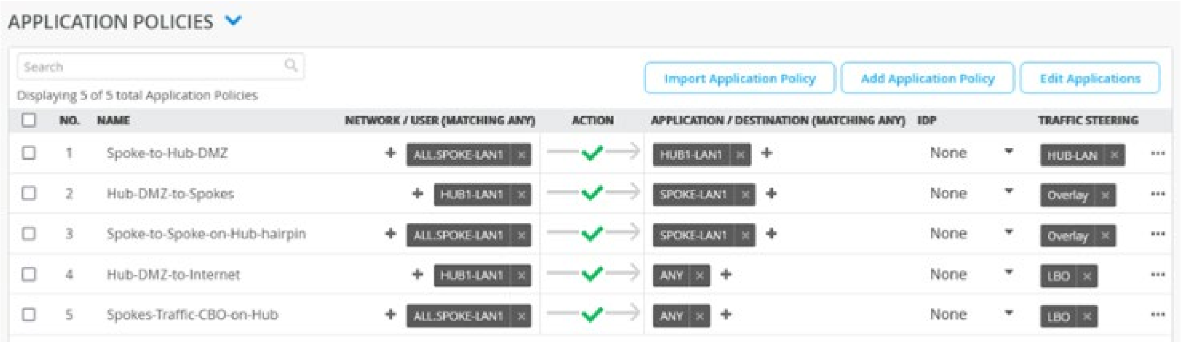
TRAFFIC STEERING

3 Traffic Steering

| NAME | STRATEGY | PATHS |
|---|---|---|
| HUB-LAN | Ordered | HUB1-LAN1 |
| LBO | Ordered | INET, MPLS |
| Overlay | ECMP | hahub-INET, hahub-MPLS |

- Retain the application policies rules.

Figure57: Application Policies Rules



APPLICATION POLICIES

Displaying 5 of 5 total Application Policies

| ☐ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| ☐ | 1 | Spoke-to-Hub-DMZ | ALL.SPOKE-LAN1 | ✓ | HUB1-LAN1 | None | HUB-LAN |
| ☐ | 2 | Hub-DMZ-to-Spokes | HUB1-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| ☐ | 3 | Spoke-to-Spoke-on-Hub-hairpin | ALL.SPOKE-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| ☐ | 4 | Hub-DMZ-to-Internet | HUB1-LAN1 | ✓ | ANY | None | LBO |
| ☐ | 5 | Spokes-Traffic-CBO-on-Hub | ALL.SPOKE-LAN1 | ✓ | ANY | None | LBO |

## Create Spoke Template

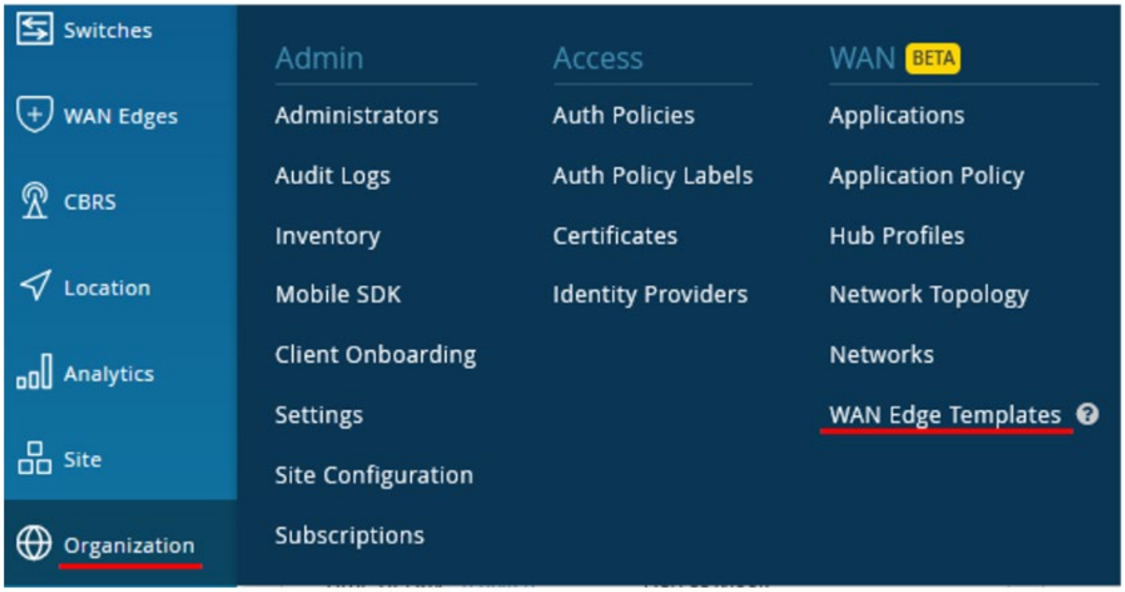
SUMMARY

With our HA Hubs in place, it’s time to create matching spoke templates, one spoke in standalone and the other in high availability cluster setup. We create the new spoke template by cloning the existing one and then modifying the cloned template. In this example, we clone the existing template called “Spokes”.

Create two matching spoke templates. You need spoke template for the device in standalone mode and another spoke template for devices in high availability cluster.

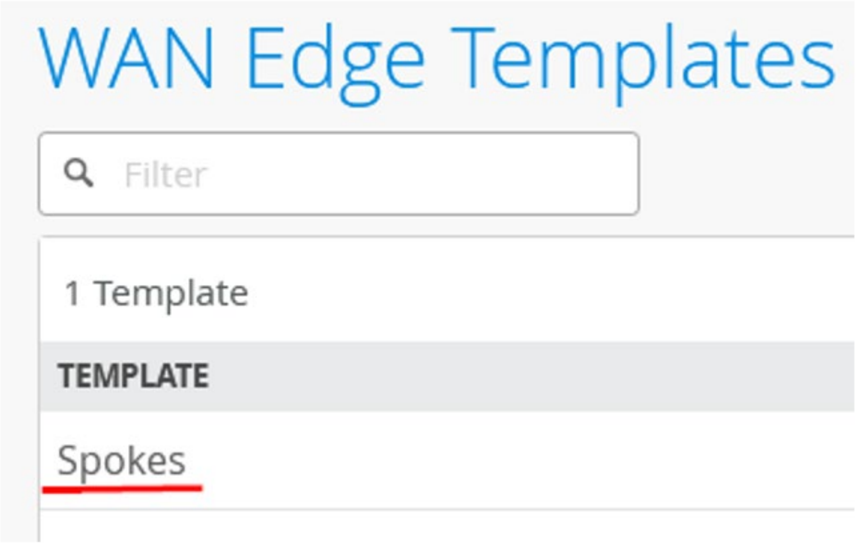
In the Juniper Mist portal, click Organization > WAN > WAN Edge Templates. A list of existing templates, if any, appears.

Figure58: Accessing WAN Edge Templates



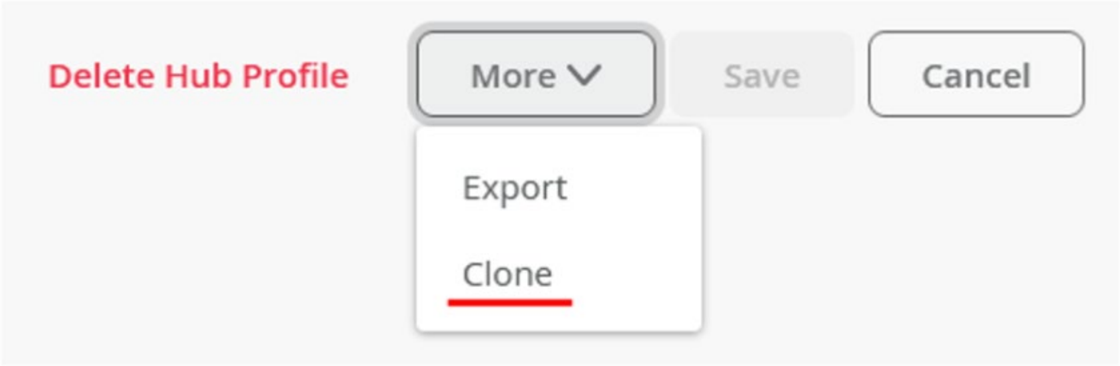
- Create the new **Spoke Template** by cloning the existing template and modifying the clone. Simply select the existing profile Spokes and select **Clone**.

Figure59: WAN Edge Templates



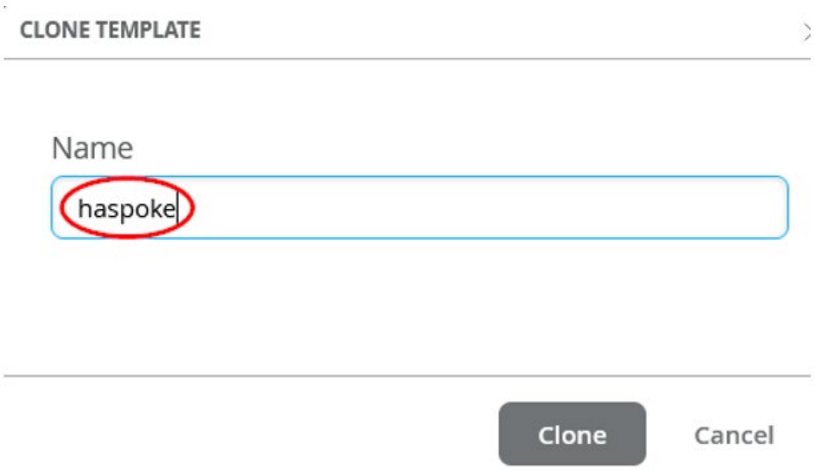
- In the upper right corner of the screen, click More and select Clone.

Figure60: Cloning Existing WAN Edge Template



- Name the new Hub Profile: **haspoke.**

Figure61: Renaming Cloned Template



Name

haspoke

**Best practice**: Refresh your browser after cloning. This ensures that objects are refreshed.

- Modify the new profile and create four new WAN interfaces. Delete the existing WAN interfaces from the clone and configure the WAN interfaces according to the details provided in the Table below.

Table 31: WAN Interfaces Details in Hub Profile

| Option | First WAN | Second WAN |
|---|---|---|
| Name: (This indicates which topology it uses.) | INET | MPLS |
| Interface | ge-0/0/0, ge-5/0/0 | ge-0/0/3, ge-5/0/3 |
| Redundant | Enabled | Enabled |

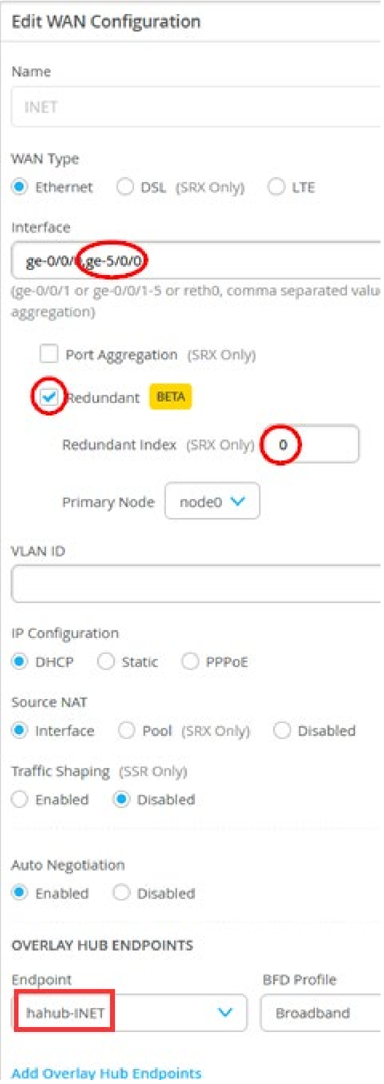
| Option | First WAN | Second WAN |
|---|---|---|
| RE Index (as a convention, use the last octet as index) | 0 | 0 |
| Overlay Hub Endpoints | hahub-INET | hahub-MPLS |

**Note**: IP configuration does not change.

For the WAN interfaces, we've added a redundant interface according to the secondary node interface naming convention used for SRX340 to SRX380 devices. Ensure that you use correct interfaces as per the SRX Series device you are configuring.

The figure below shows WAN interface configuration.

Figure62: WAN Interface Configuration (First)



Edit WAN Configuration

Name: INET

WAN Type: ● Ethernet ○ DSL (SRX Only) ○ LTE

Interface: ge-0/0/1,ge-5/0/0

(ge-0/0/1 or ge-0/0/1-5 or reth0, comma separated valu aggregation)

□ Port Aggregation (SRX Only)

☑ Redundant BETA

Redundant Index (SRX Only): 0

Primary Node: node0

VLAN ID:

IP Configuration: ● DHCP ○ Static ○ PPPoE

Source NAT: ● Interface ○ Pool (SRX Only) ○ Disabled

Traffic Shaping (SSR Only): ○ Enabled ● Disabled

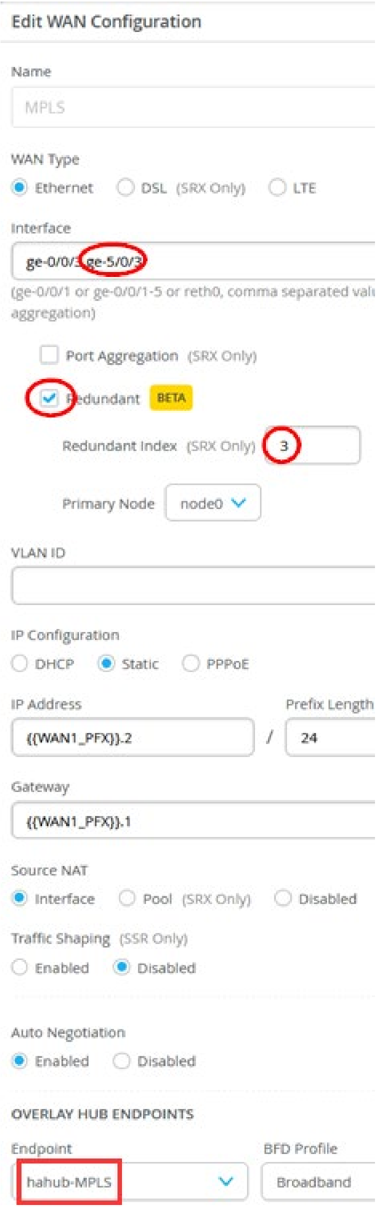
Auto Negotiation: ● Enabled ○ Disabled

OVERLAY HUB ENDPOINTS

| Endpoint | BFD Profile |
|---|---|
| hahub-INET | Broadband |

Add Overlay Hub Endpoints

Figure63: WAN Interface Configuration (Second)



Edit WAN Configuration

Name: MPLS

WAN Type: ● Ethernet ○ DSL (SRX Only) ○ LTE

Interface: ge-0/0/3,ge-5/0/3

(ge-0/0/1 or ge-0/0/1-5 or reth0, comma separated val
aggregation)

□ Port Aggregation (SRX Only)

☑ Redundant BETA

Redundant Index (SRX Only): 3

Primary Node: node0

VLAN ID:

IP Configuration: ○ DHCP ● Static ○ PPPoE

IP Address: {{WAN1_PFX}}.2 / Prefix Length: 24

Gateway: {{WAN1_PFX}}.1

Source NAT: ● Interface ○ Pool (SRX Only) ○ Disabled

Traffic Shaping (SSR Only): ○ Enabled ● Disabled

Auto Negotiation: ● Enabled ○ Disabled

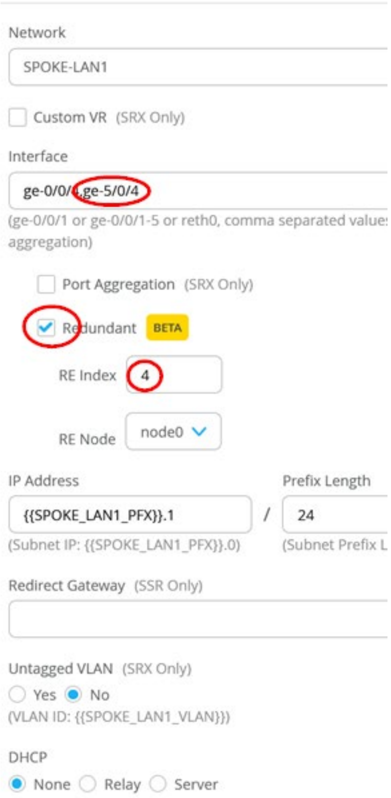
OVERLAY HUB ENDPOINTS

| Endpoint | BFD Profile |
|---|---|
| hahub-MPLS | Broadband |

- Modify LAN interface configurations. The LAN configuration follows a similar pattern as WAN Interface.
  - **Interfaces**—ge-0/0/4,ge-5/0/4
  - Redundant—Enabled
  - **RE Index**—4 (use the last octet as index)

  IP Address and Prefix do not change.

Figure64: LAN Interface Configuration



Network

SPOKE-LAN1

□ Custom VR (SRX Only)

Interface

ge-0/0/4,ge-5/0/4

(ge-0/0/1 or ge-0/0/1-5 or reth0, comma separated values
aggregation)

□ Port Aggregation (SRX Only)

☑ Redundant BETA

RE Index 4

RE Node node0

IP Address {{SPOKE_LAN1_PFX}}.1 / Prefix Length 24

(Subnet IP: {{SPOKE_LAN1_PFX}}.0) (Subnet Prefix L

Redirect Gateway (SSR Only)

Untagged VLAN (SRX Only)

○ Yes ● No

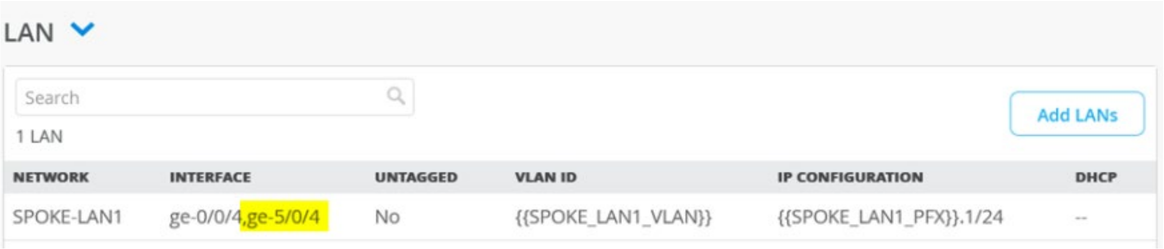
(VLAN ID: {{SPOKE_LAN1_VLAN}})

DHCP

● None ○ Relay ○ Server

The Figure below shows your new LAN-configuration.

Figure65: LAN Interface Configuration

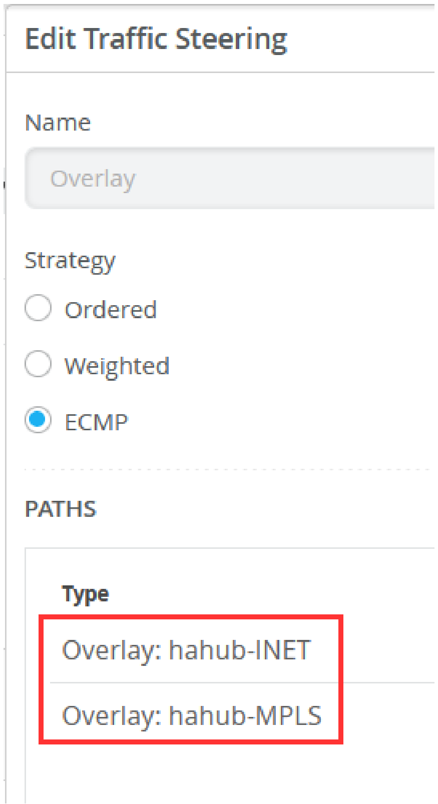


1 LAN

| NETWORK | INTERFACE | UNTAGGED | VLAN ID | IP CONFIGURATION | DHCP |
|---|---|---|---|---|---|
| SPOKE-LAN1 | ge-0/0/4,ge-5/0/4 | No | {{SPOKE_LAN1_VLAN}} | {{SPOKE_LAN1_PFX}}.1/24 | -- |

- Modify the traffic steering profile named “Overlay” to use only the two new Hub endpoints.

Figure66: Traffic Steering Profile



Edit Traffic Steering

Name

Overlay

Strategy

○ Ordered

○ Weighted

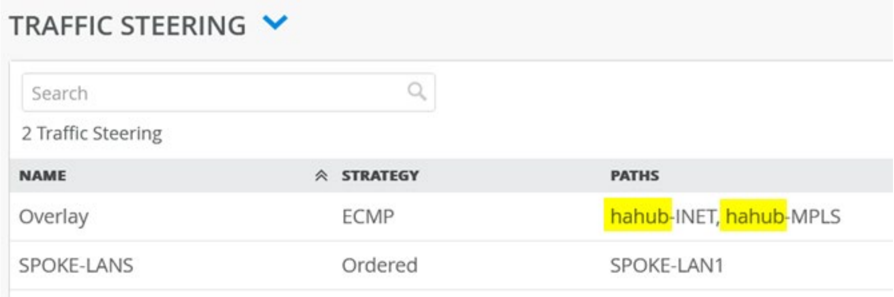
● ECMP

PATHS

| Type |
|---|
| Overlay: hahub-INET |
| Overlay: hahub-MPLS |

The Figure below shows that the traffic steering rules now point to the HA hub endpoints—hahub-INET and hahub-MPLS.

Figure67: Modified Traffic Steering Rules



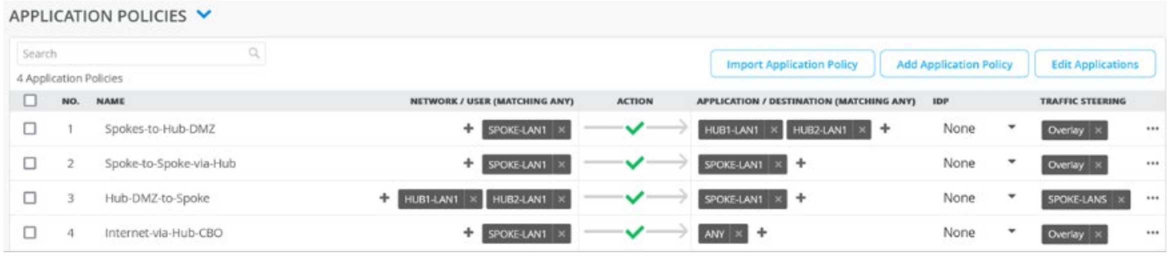
TRAFFIC STEERING

Search

2 Traffic Steering

| NAME | STRATEGY | PATHS |
|---|---|---|
| Overlay | ECMP | hahub-INET, hahub-MPLS |
| SPOKE-LANS | Ordered | SPOKE-LAN1 |

- Retain the application policies without making any changes.



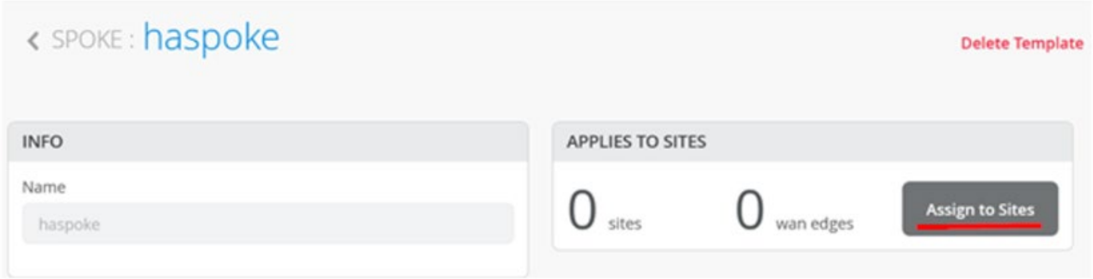
APPLICATION POLICIES

4 Application Policies

| ☐ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| ☐ | 1 | Spokes-to-Hub-DMZ | SPOKE-LAN1 | ✓ | HUB1-LAN1<br>HUB2-LAN1 | None | Overlay |
| ☐ | 2 | Spoke-to-Spoke-via-Hub | SPOKE-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| ☐ | 3 | Hub-DMZ-to-Spoke | HUB1-LAN1<br>HUB2-LAN1 | ✓ | SPOKE-LAN1 | None | SPOKE-LANS |
| ☐ | 4 | Internet-via-Hub-CBO | SPOKE-LAN1 | ✓ | ANY | None | Overlay |

- Assign the spoke template to site. Scroll to the top of the WAN Edge Templates page and click **Assign to Sites** under Spokes pane.

Figure68: Assign Spoke Template to Sites



SPOKE : haspoke

INFO

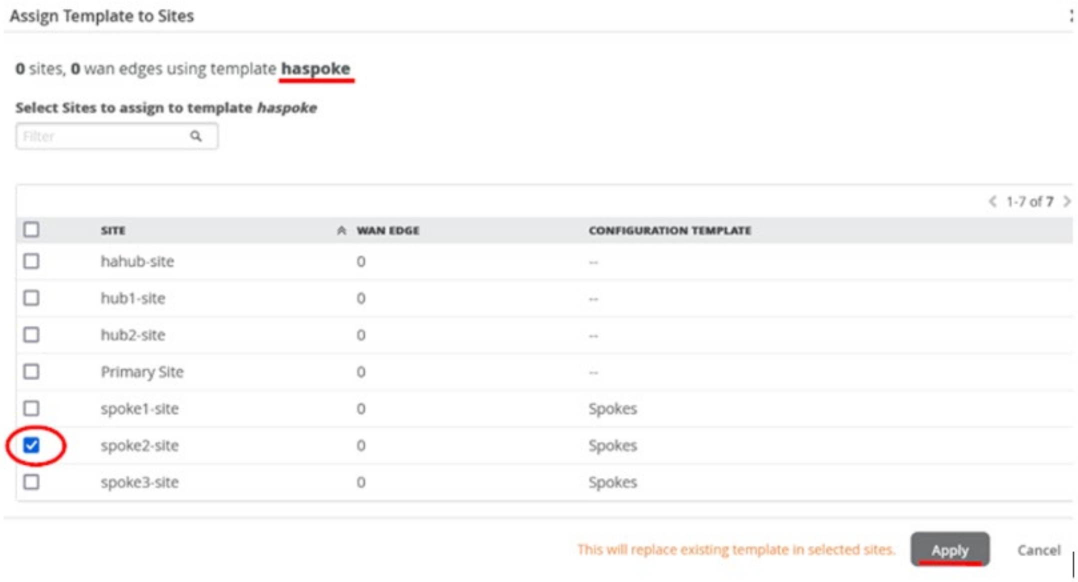
Name: haspoke

APPLIES TO SITES

0 sites 0 wan edges

- In the Assign Template to Sites, check that you are using the **haspoke** template and select the site **spoke2-site** before you hit **Apply**.

Figure69: Selecting Site for Assigning Spoke Template



Assign Template to Sites

**0** sites, **0** wan edges using template **haspoke**

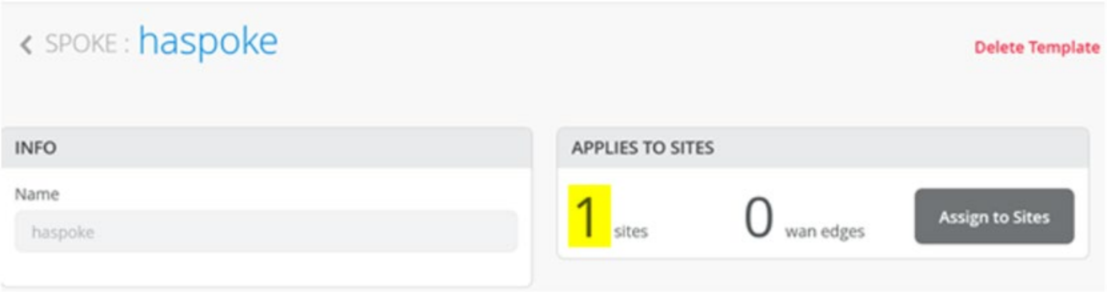
**Select Sites to assign to template *haspoke***

| ☐ | SITE | WAN EDGE | CONFIGURATION TEMPLATE |
|---|---|---|---|
| ☐ | hahub-site | 0 | -- |
| ☐ | hub1-site | 0 | -- |
| ☐ | hub2-site | 0 | -- |
| ☐ | Primary Site | 0 | -- |
| ☐ | spoke1-site | 0 | Spokes |
| ☑ | spoke2-site | 0 | Spokes |
| ☐ | spoke3-site | 0 | Spokes |

This will replace existing template in selected sites.

- Check that your Template has now at least 1 Site assigned.

Figure70: Spoke Templates Applied to Sites


SPOKE : haspoke

Delete Template

INFO

Name

haspoke

APPLIES TO SITES

1 sites

0 wan edges

Assign to Sites

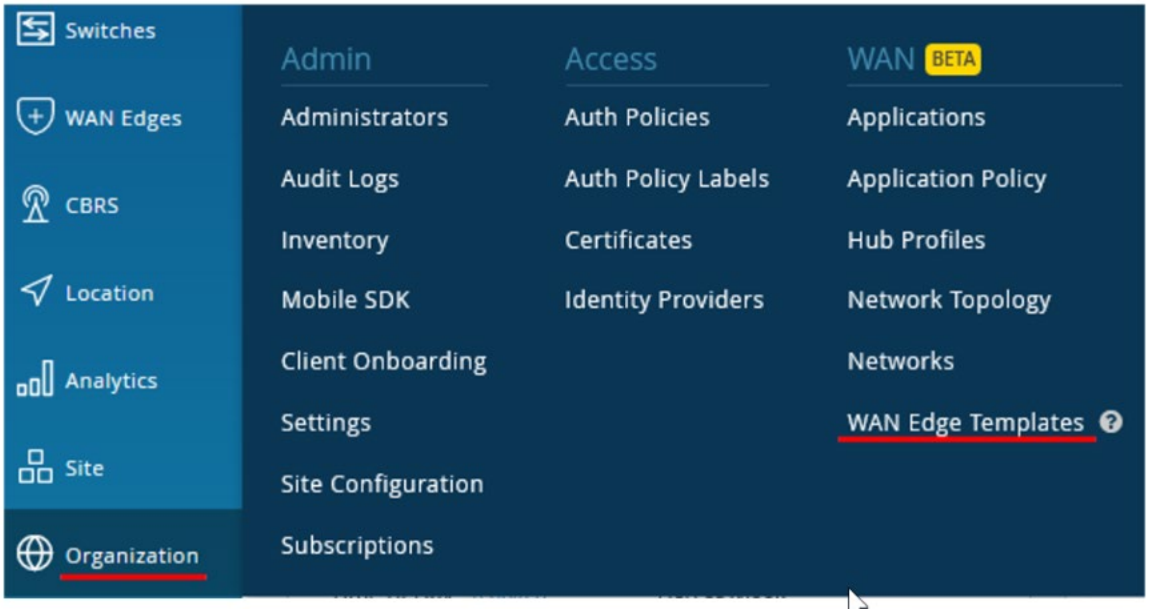
## Create the Second Spoke Template

SUMMARY

Now it’s time to clone our WAN Edge template for our redundant spoke node.

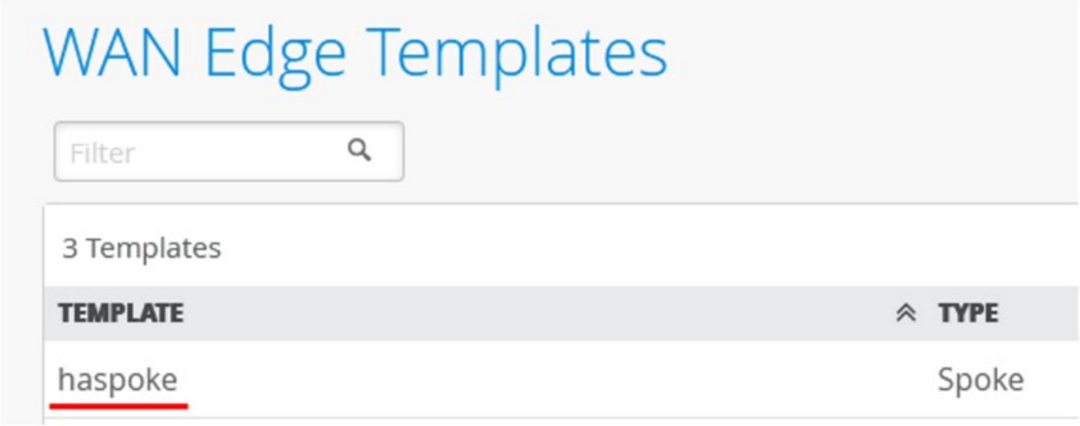
- In the Juniper Mist cloud portal, click **Organization** > **WAN** > **WAN Edge Templates**. A list of existing templates, if any, appears.

Figure71: WAN Edge Template



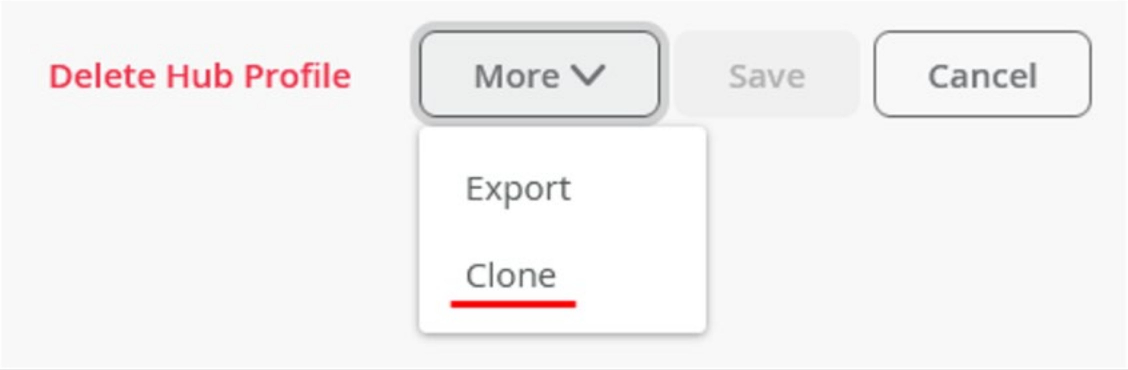
- Create the new **Spoke Template** by cloning the existing and modifying the clone. Click on the existing profile **haspoke**.

Figure72: Select WAN Edge Template for Cloning



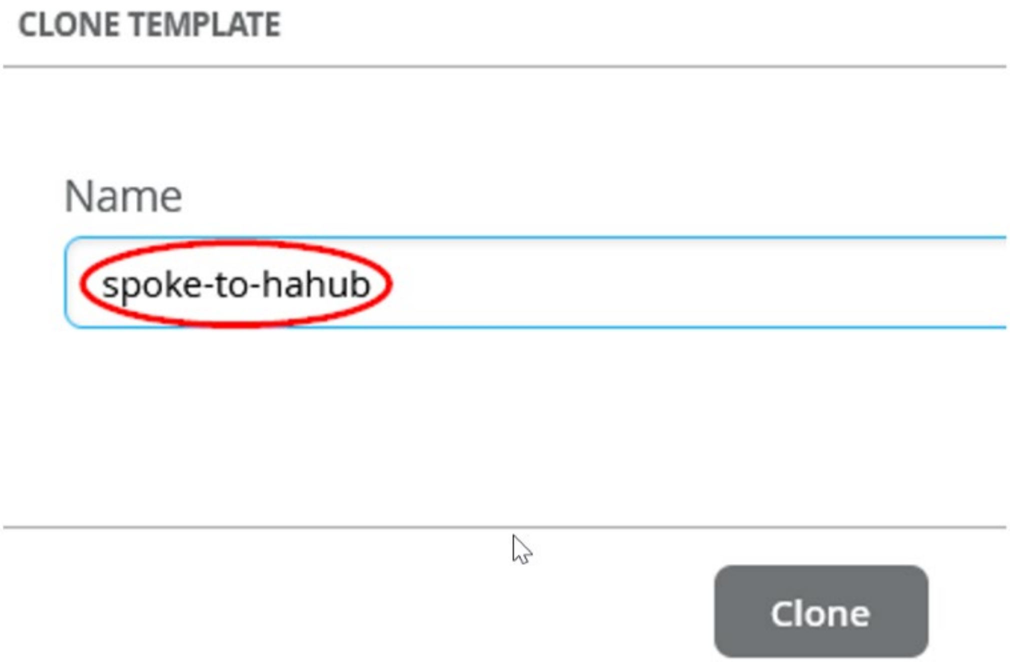
- In the upper right corner of the screen, click **More** and select **Clone**.

Figure73: Cloning WAN Edge Template



- Name the new template as **spoke-to-hahub** and click **Clone**.

Figure74: Renaming Cloned Template


CLONE TEMPLATE

Name

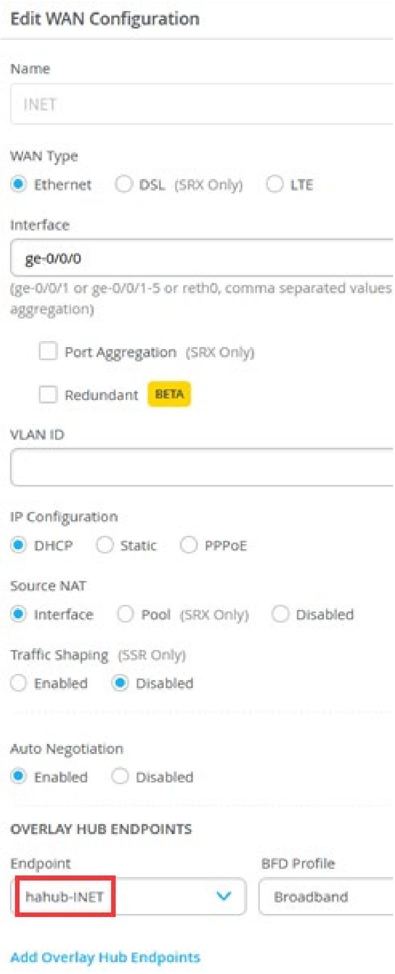
spoke-to-hahub

If you see any errors while naming the profile, refresh your browser.

There are not many differences between this template and the former template, except the Hub Endpoints for the WAN interfaces.

- Modify the interfaces for the template. Change the **Overlay Hub EndPoints** as following:
  - For the interface INET—**hahub-INET**
  - For the interface MPLS—**hahub-MPLS**

Figure75: Modify WAN Interfaces



Edit WAN Configuration

Name

INET

WAN Type

● Ethernet ○ DSL (SRX Only) ○ LTE

Interface

ge-0/0/0

(ge-0/0/1 or ge-0/0/1-5 or reth0, comma separated values
aggregation)

□ Port Aggregation (SRX Only)

□ Redundant BETA

VLAN ID

IP Configuration

● DHCP ○ Static ○ PPPoE

Source NAT

● Interface ○ Pool (SRX Only) ○ Disabled

Traffic Shaping (SSR Only)

○ Enabled ● Disabled

Auto Negotiation

● Enabled ○ Disabled

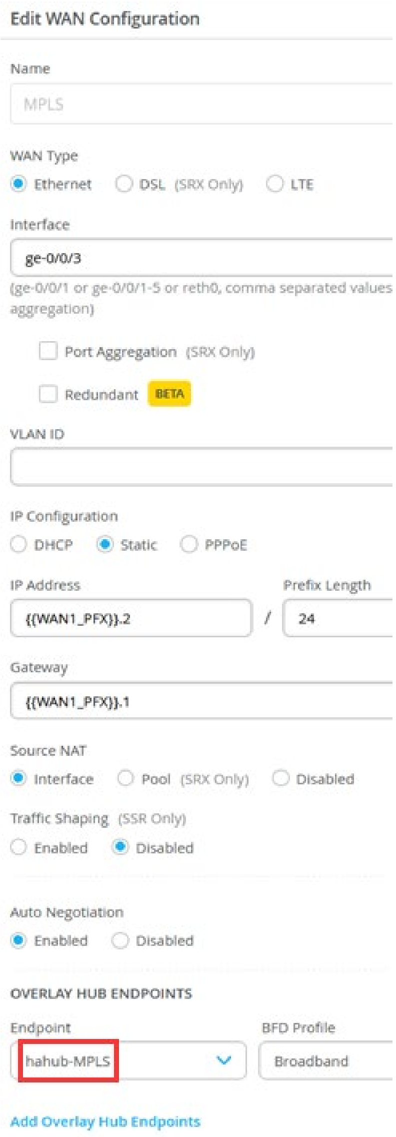
OVERLAY HUB ENDPOINTS

Endpoint: hahub-INET

BFD Profile: Broadband

Add Overlay Hub Endpoints

Figure76: Edit WAN Interfaces



Edit WAN Configuration

Name

MPLS

WAN Type

● Ethernet ○ DSL (SRX Only) ○ LTE

Interface

ge-0/0/3

(ge-0/0/1 or ge-0/0/1-5 or reth0, comma separated values aggregation)

□ Port Aggregation (SRX Only)

□ Redundant BETA

VLAN ID

IP Configuration

○ DHCP ● Static ○ PPPoE

IP Address: {{WAN1_PFX}}.2 / Prefix Length: 24

Gateway

{{WAN1_PFX}}.1

Source NAT

● Interface ○ Pool (SRX Only) ○ Disabled

Traffic Shaping (SSR Only)

○ Enabled ● Disabled

Auto Negotiation

● Enabled ○ Disabled

OVERLAY HUB ENDPOINTS

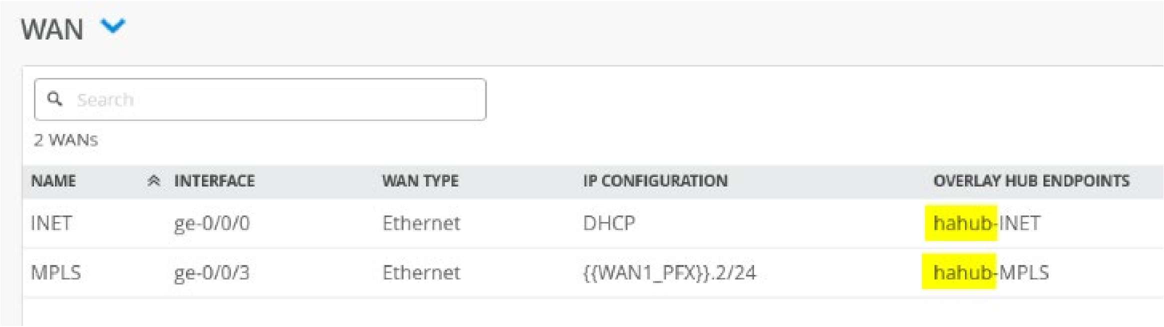
Endpoint: hahub-MPLS

BFD Profile: Broadband

Add Overlay Hub Endpoints

The Figure below shows configured WAN interfaces.

Figure77: WAN Interfaces Configuration



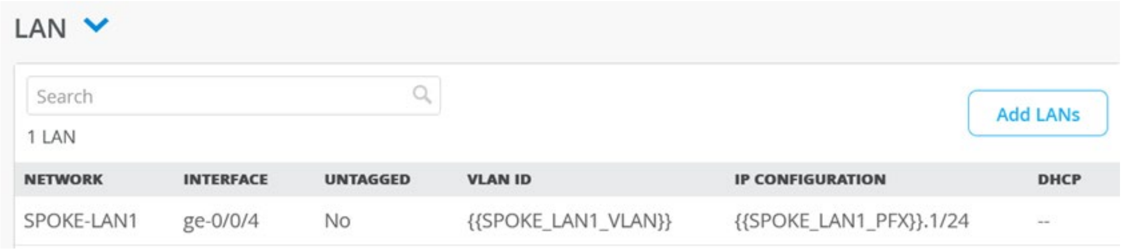
WAN

Search

2 WANs

| NAME | INTERFACE | WAN TYPE | IP CONFIGURATION | OVERLAY HUB ENDPOINTS |
|---|---|---|---|---|
| INET | ge-0/0/0 | Ethernet | DHCP | hahub-INET |
| MPLS | ge-0/0/3 | Ethernet | {{WAN1_PFX}}.2/24 | hahub-MPLS |

- The LAN interfaces are no longer redundant. No changes required for them.



LAN

Search

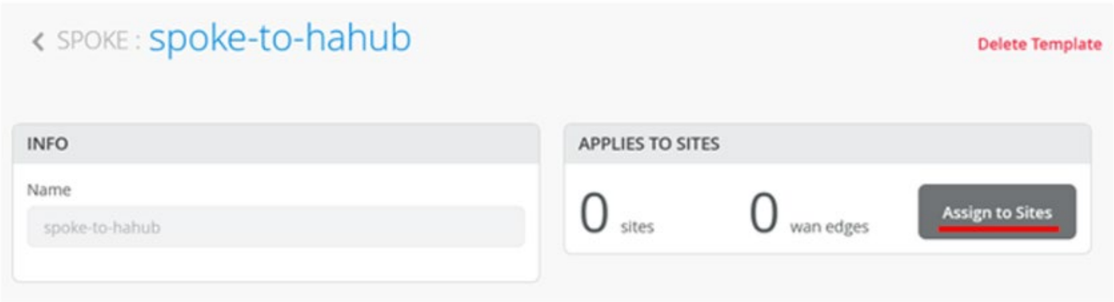
1 LAN

Add LANs

| NETWORK | INTERFACE | UNTAGGED | VLAN ID | IP CONFIGURATION | DHCP |
|---|---|---|---|---|---|
| SPOKE-LAN1 | ge-0/0/4 | No | {{SPOKE_LAN1_VLAN}} | {{SPOKE_LAN1_PFX}}.1/24 | -- |

- Modify the traffic steering profile (**Overlay**) to use only the two new hub endpoints (**hahub**).
- Application Policies are the same as in the last **Template** and do not change the rules.
- Assign the spoke template to site. Scroll to the top of the WAN Edge Templates page and click **Assign to Sites** under Spokes pane

Figure78: Assign Template to Site



SPOKE : spoke-to-hahub

Delete Template

INFO

Name: spoke-to-hahub

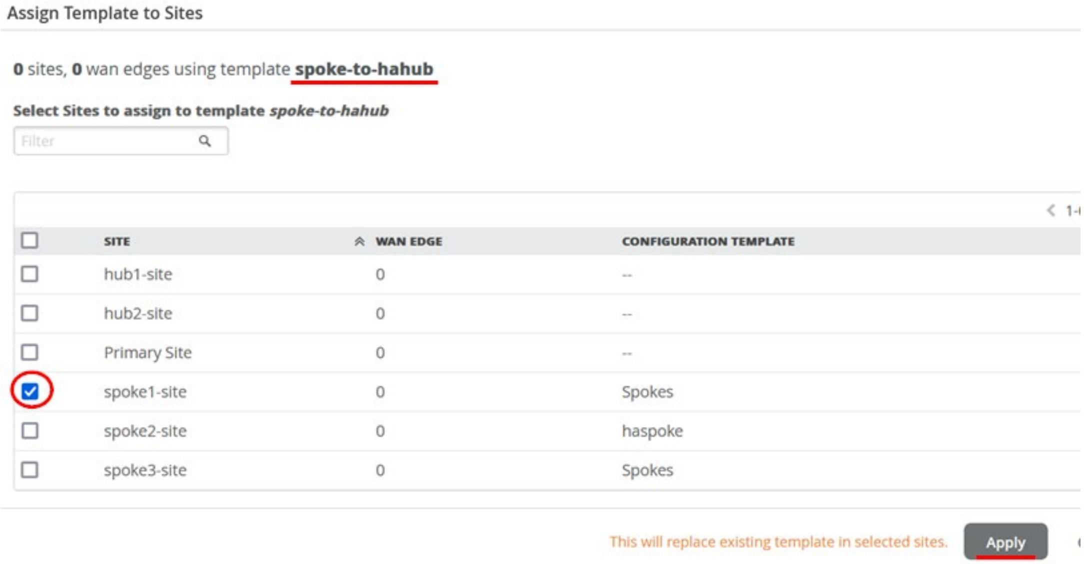
APPLIES TO SITES

0 sites 0 wan edges

Assign to Sites

- In the Assign Template to Sites pane, ensure that you are using the **spoke-to-hahub** template and select the site **spoke1-site**

Figure79: Assign Templates to Site



Assign Template to Sites

**0** sites, **0** wan edges using template **spoke-to-hahub**

**Select Sites to assign to template *spoke-to-hahub***

Filter

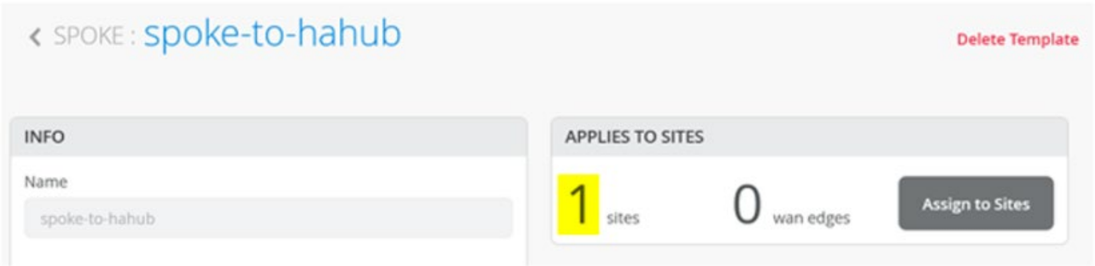
| □ | SITE | WAN EDGE | CONFIGURATION TEMPLATE |
|---|---|---|---|
| □ | hub1-site | 0 | -- |
| □ | hub2-site | 0 | -- |
| □ | Primary Site | 0 | -- |
| ☑ | spoke1-site | 0 | Spokes |
| □ | spoke2-site | 0 | haspoke |
| □ | spoke3-site | 0 | Spokes |

This will replace existing template in selected sites.

Apply

- Click **Apply**.
- Ensure that your template is now assigned to a site. Check that your **Template** now has at least 1 **Site** assigned as shown in No Link Title.

Figure80: Spoke Templates Applied to Sites



INFO

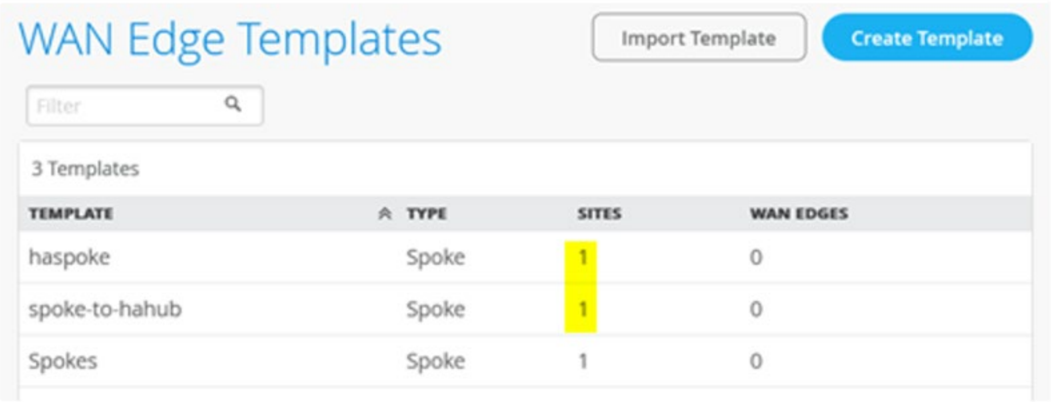
Name: spoke-to-hahub

APPLIES TO SITES

1 sites 0 wan edges

The Figure below shows the list of configured spoke templates.

Figure81: List of WAN Edge Templates



3 Templates

| TEMPLATE | TYPE | SITES | WAN EDGES |
|---|---|---|---|
| haspoke | Spoke | 1 | 0 |
| spoke-to-hahub | Spoke | 1 | 0 |
| Spokes | Spoke | 1 | 0 |

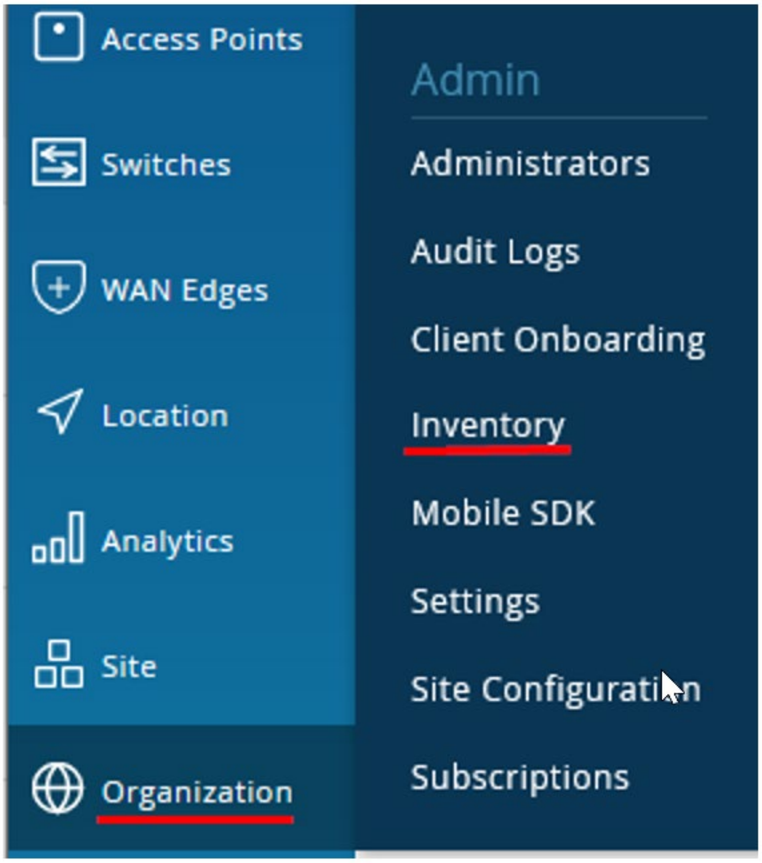
## Onboard your Devices

We assume that you have your SRX Series Firewall already onboarded to the Juniper Mist cloud. We also assume that the physical connections such as cabling are already in place and that you are using valid interfaces for the high availability. All devices that are part of high availability cluster starts in standalone mode and the Mist cloud portal configuration enables devices to operate in cluster mode.

You can **Claim** or **Adopt** to onboard devices into your organization inventory. For details on getting your SRX Series Firewall up and running in the Mist cloud, see the first chapter of this Appendix “Day-0 operation to claim/ZTP or adopt the SRX Devices towards Mist cloud“.

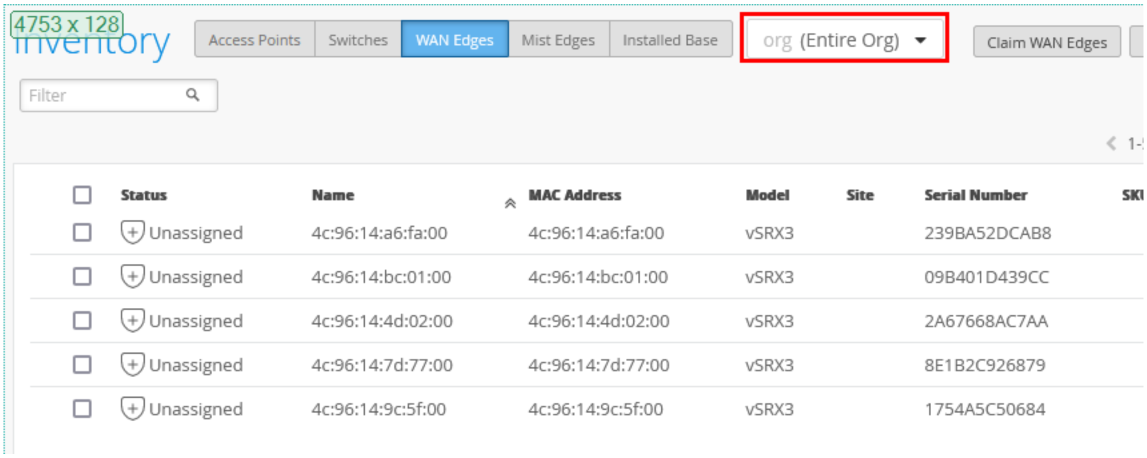
- In the Juniper Mist portal. click **Organization** > **Admin** >**Inventory**.

Figure82: Navigating to Inventory



- Refresh your browser and check under WAN Edges to find out if your Session Smart Router is part of the inventory. Ensure you set the view as **org (Entire Org)** as shown in the Figure below.

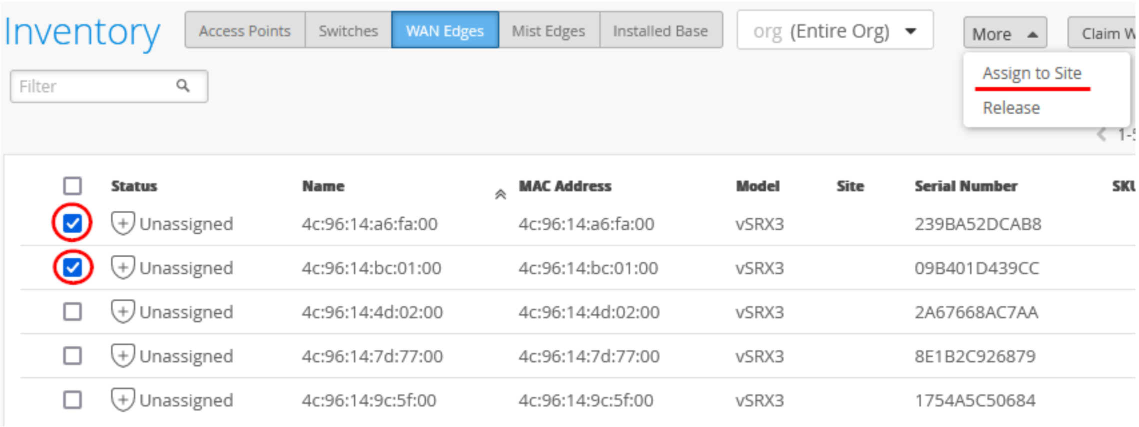
Figure83: SRX Series in Inventory



| ☐ | Status | Name | MAC Address | Model | Site | Serial Number | SKU |
|---|---|---|---|---|---|---|---|
| ☐ | Unassigned | 4c:96:14:a6:fa:00 | 4c:96:14:a6:fa:00 | vSRX3 | | 239BA52DCAB8 | |
| ☐ | Unassigned | 4c:96:14:bc:01:00 | 4c:96:14:bc:01:00 | vSRX3 | | 09B401D439CC | |
| ☐ | Unassigned | 4c:96:14:4d:02:00 | 4c:96:14:4d:02:00 | vSRX3 | | 2A67668AC7AA | |
| ☐ | Unassigned | 4c:96:14:7d:77:00 | 4c:96:14:7d:77:00 | vSRX3 | | 8E1B2C926879 | |
| ☐ | Unassigned | 4c:96:14:9c:5f:00 | 4c:96:14:9c:5f:00 | vSRX3 | | 1754A5C50684 | |

- Select the **two devices/nodes together** for the HA hub and click **Assign to Site**.

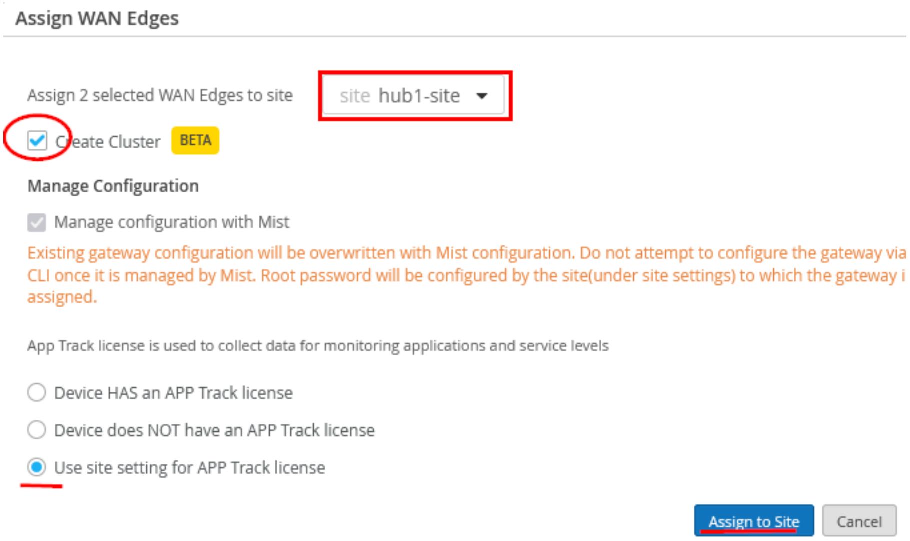
Figure84: Assigning Session Smart Routers (HA Pair) to Site



| ☐ | Status | Name | MAC Address | Model | Site | Serial Number | SKU |
|---|---|---|---|---|---|---|---|
| ☑ | Unassigned | 4c:96:14:a6:fa:00 | 4c:96:14:a6:fa:00 | vSRX3 | | 239BA52DCAB8 | |
| ☑ | Unassigned | 4c:96:14:bc:01:00 | 4c:96:14:bc:01:00 | vSRX3 | | 09B401D439CC | |
| ☐ | Unassigned | 4c:96:14:4d:02:00 | 4c:96:14:4d:02:00 | vSRX3 | | 2A67668AC7AA | |
| ☐ | Unassigned | 4c:96:14:7d:77:00 | 4c:96:14:7d:77:00 | vSRX3 | | 8E1B2C926879 | |
| ☐ | Unassigned | 4c:96:14:9c:5f:00 | 4c:96:14:9c:5f:00 | vSRX3 | | 1754A5C50684 | |

- In Assign WAN Edges page, select **hub1-site** and enable the **Create Cluster** option.

Figure85: Assign Spoke Devices to Site and Initiate Cluster Formation



Assign WAN Edges

Assign 2 selected WAN Edges to site: site hub1-site

☑ Create Cluster

Manage Configuration

☑ Manage configuration with Mist

Existing gateway configuration will be overwritten with Mist configuration. Do not attempt to configure the gateway via CLI once it is managed by Mist. Root password will be configured by the site(under site settings) to which the gateway i assigned.

App Track license is used to collect data for monitoring applications and service levels

○ Device HAS an APP Track license

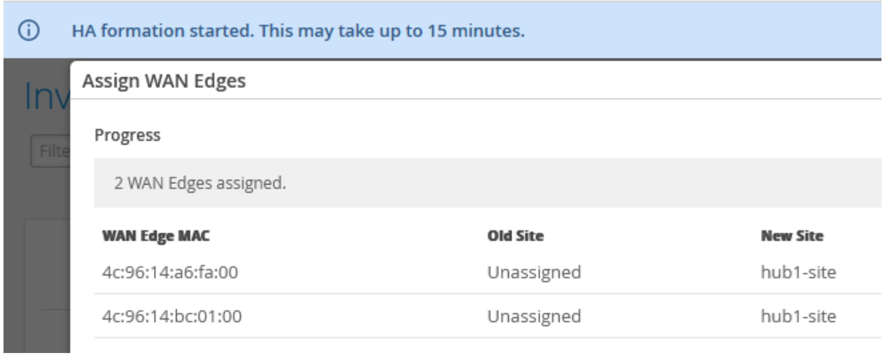
○ Device does NOT have an APP Track license

● Use site setting for APP Track license

- Click Assign to Site.

The portal displays the details of WAN edge devices assigned to site and progress of cluster formation. You can close this dialog box.

Figure86: HA Cluster Formation for Assigned Devices



HA formation started. This may take up to 15 minutes.

Assign WAN Edges

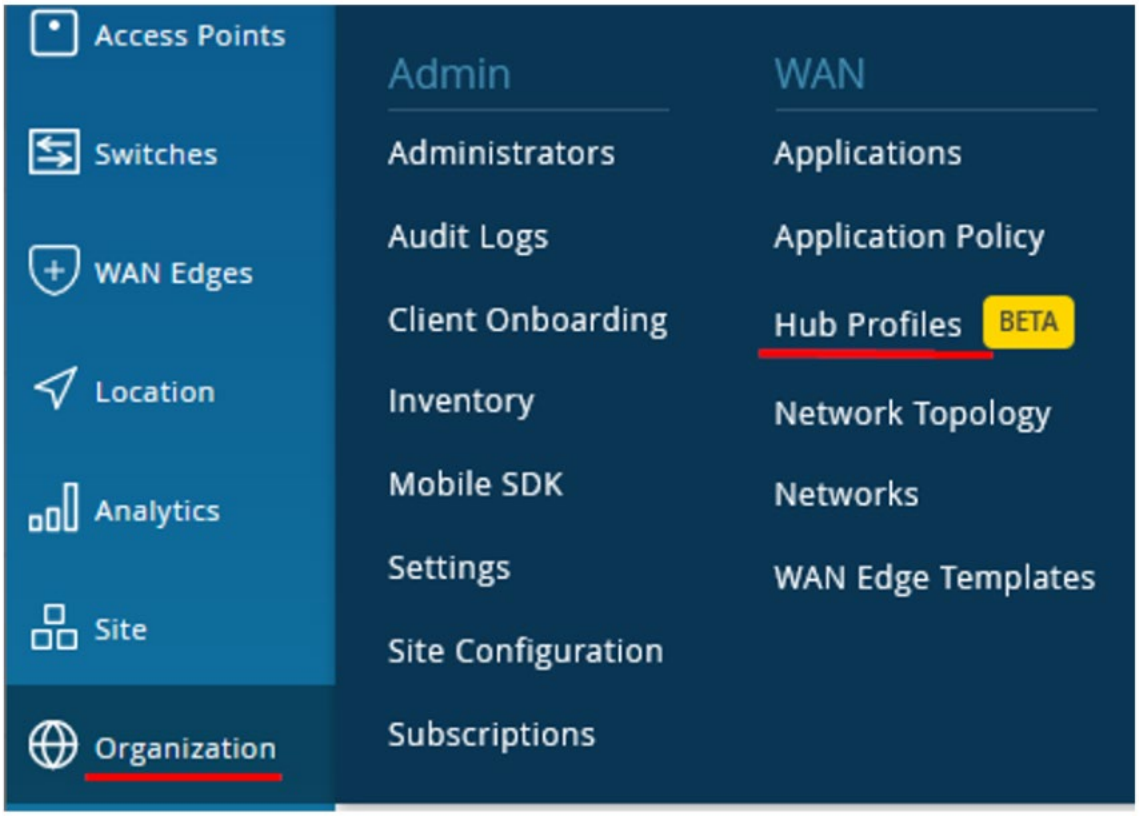
Progress

2 WAN Edges assigned.

| WAN Edge MAC | Old Site | New Site |
|---|---|---|
| 4c:96:14:a6:fa:00 | Unassigned | hub1-site |
| 4c:96:14:bc:01:00 | Unassigned | hub1-site |

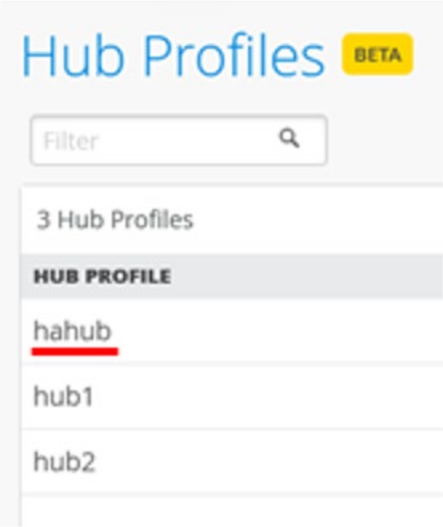
- In the Juniper Mist portal, click **Organization** > **WAN** > **Hub Profiles**. The Hub Profile displays the list of existing profiles.

Figure87: Navigating to Hub Profiles



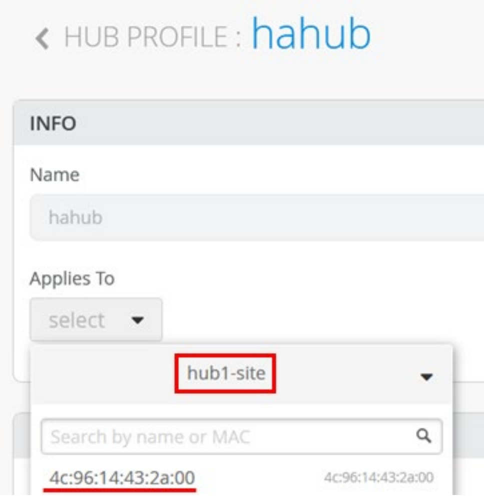
- Click the hub profile (hahub) that you want to assign to a site.

Figure88: Select Hub Profile



- Under the **Applies To** option, select the site (hub1-site) from the list of available sites.

Figure89: Select Sites for Applying Hub Profile



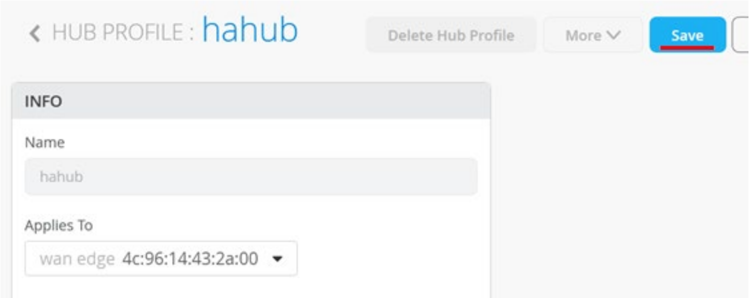
Name
hahub

Applies To
hub1-site

4c:96:14:43:2a:00 4c:96:14:43:2a:00

Check if have correct WAN edge device selected and click **Save**.

Figure90: Select WAN Edge Device to Apply Template



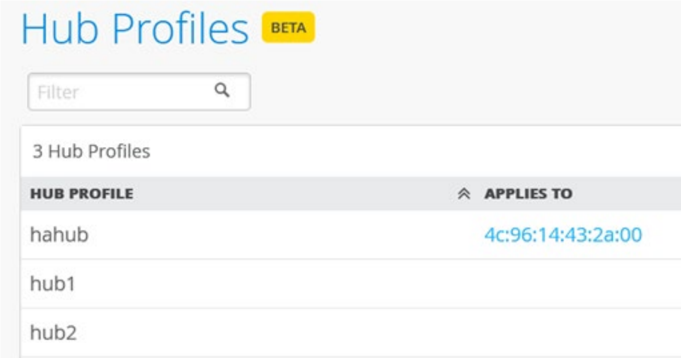
INFO

Name: hahub

Applies To: wan edge 4c:96:14:43:2a:00

- You should now see the HA devices assigned to their **Hub Profile** in the as shown in Figure 156 on page 111.

Figure91: Hub Profile Assignment Summary



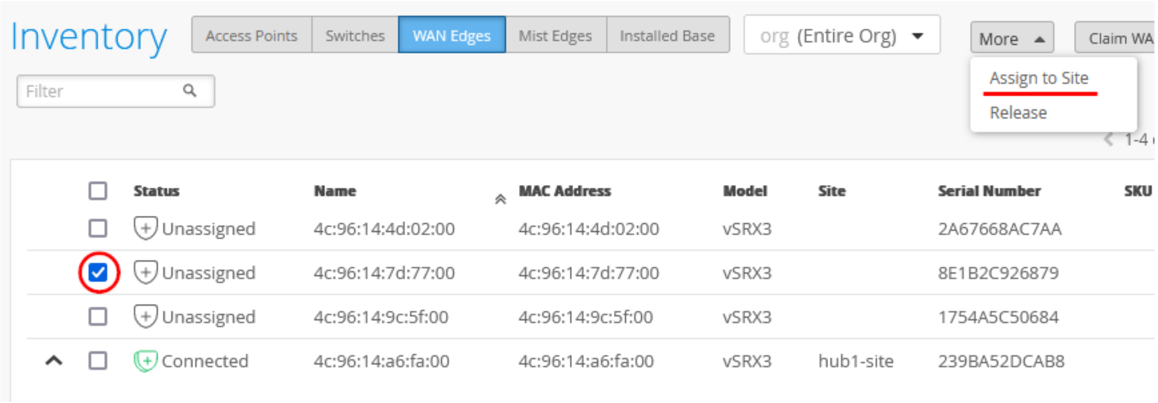
3 Hub Profiles

| HUB PROFILE | APPLIES TO |
|---|---|
| hahub | 4c:96:14:43:2a:00 |
| hub1 | |
| hub2 | |

**Note**: Wait for some time until the setup is up and running! Rebooting a cluster setup takes longer time than a standalone device.

- In the Juniper Mist portal. click **Organization** > **Admin** > **Inventory**.
- Select the spoke device (SPOKE1) and click **Assign to Site**.

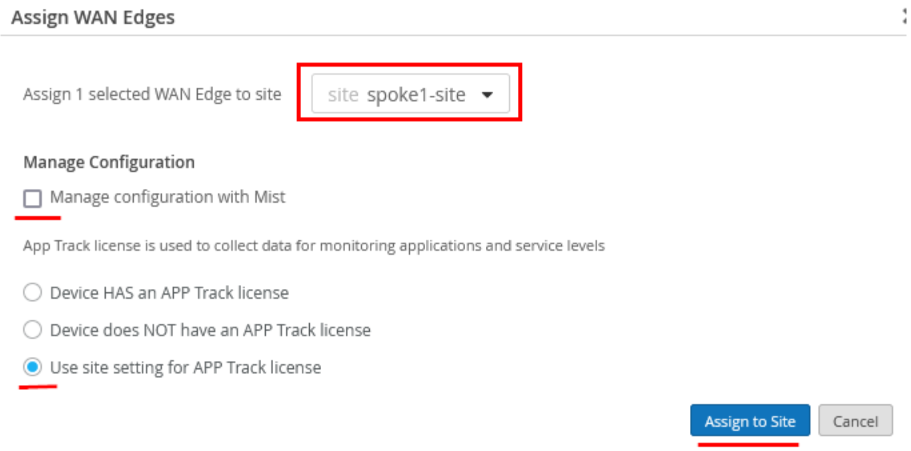
Figure92: Assign Spoke Device To Site



| | Status | Name | MAC Address | Model | Site | Serial Number | SKU |
|---|---|---|---|---|---|---|---|
| □ | Unassigned | 4c:96:14:4d:02:00 | 4c:96:14:4d:02:00 | vSRX3 | | 2A67668AC7AA | |
| ☑ | Unassigned | 4c:96:14:7d:77:00 | 4c:96:14:7d:77:00 | vSRX3 | | 8E1B2C926879 | |
| □ | Unassigned | 4c:96:14:9c:5f:00 | 4c:96:14:9c:5f:00 | vSRX3 | | 1754A5C50684 | |
| □ | Connected | 4c:96:14:a6:fa:00 | 4c:96:14:a6:fa:00 | vSRX3 | hub1-site | 239BA52DCAB8 | |

- In Assign WAN Edges page, select **spoke1-site**.

Figure93: Assign WAN Edge Device to Site



Assign WAN Edges

Assign 1 selected WAN Edge to site: site spoke1-site

Manage Configuration

□ Manage configuration with Mist

App Track license is used to collect data for monitoring applications and service levels

○ Device HAS an APP Track license

○ Device does NOT have an APP Track license

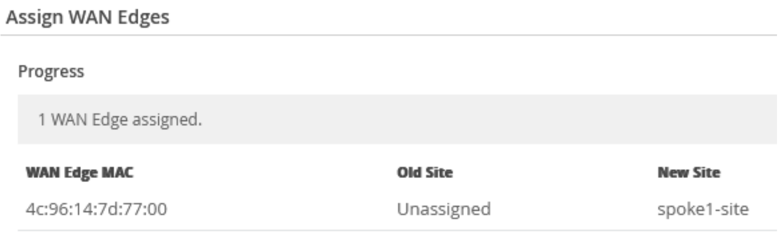
● Use site setting for APP Track license

For now, do not select the **Manage configuration with Mist** option. You can enable this option later. We recommend selecting **Use site settings for App Track License**.

- Click Assign to Site.

The system confirms the assignment to the site as shown in the Figure below.

Figure94: Assigned to Site



Assign WAN Edges

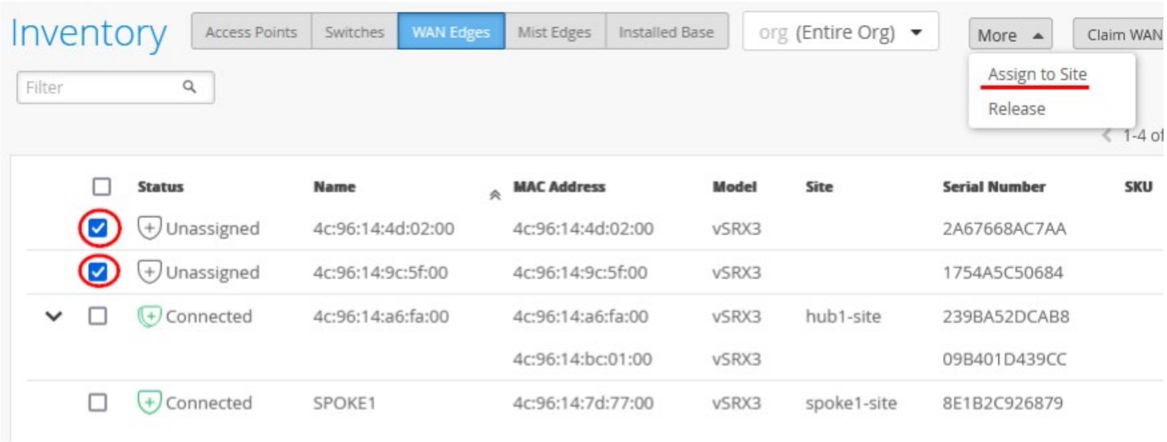
Progress

1 WAN Edge assigned.

| WAN Edge MAC | Old Site | New Site |
|---|---|---|
| 4c:96:14:7d:77:00 | Unassigned | spoke1-site |

- Select the two spoke devices that will form cluster (Spoke-Cluster) and click **Assign to Site**.

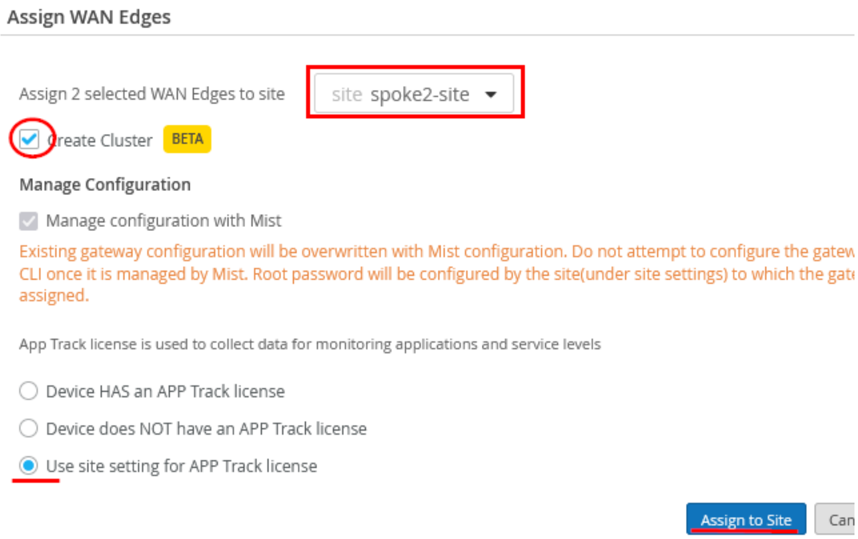
Figure95: Assign Spoke Devices to Site



| □ | Status | Name | MAC Address | Model | Site | Serial Number | SKU |
|---|---|---|---|---|---|---|---|
| ☑ | Unassigned | 4c:96:14:4d:02:00 | 4c:96:14:4d:02:00 | vSRX3 | | 2A67668AC7AA | |
| ☑ | Unassigned | 4c:96:14:9c:5f:00 | 4c:96:14:9c:5f:00 | vSRX3 | | 1754A5C50684 | |
| □ | Connected | 4c:96:14:a6:fa:00 | 4c:96:14:a6:fa:00 | vSRX3 | hub1-site | 239BA52DCAB8 | |
| | | | 4c:96:14:bc:01:00 | vSRX3 | | 09B401D439CC | |
| □ | Connected | SPOKE1 | 4c:96:14:7d:77:00 | vSRX3 | spoke1-site | 8E1B2C926879 | |

- In the Assign WAN Edges, select **spoke2-site** and enable **Create Cluster** .

Figure96: Assign two Spoke Devices to Site and Initiate Cluster Formation



Assign WAN Edges

Assign 2 selected WAN Edges to site: site spoke2-site

☑ Create Cluster BETA

Manage Configuration

☑ Manage configuration with Mist

Existing gateway configuration will be overwritten with Mist configuration. Do not attempt to configure the gatew
CLI once it is managed by Mist. Root password will be configured by the site(under site settings) to which the gat
assigned.

App Track license is used to collect data for monitoring applications and service levels

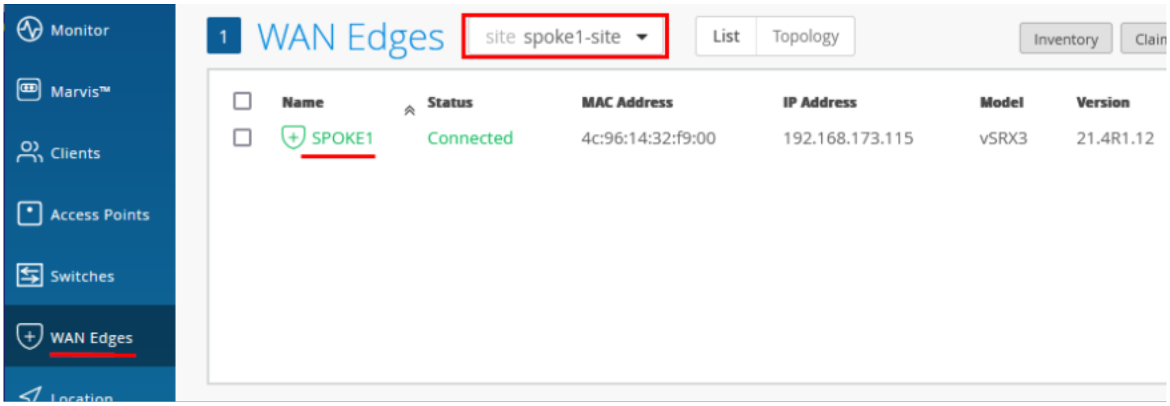
○ Device HAS an APP Track license

○ Device does NOT have an APP Track license

● Use site setting for APP Track license

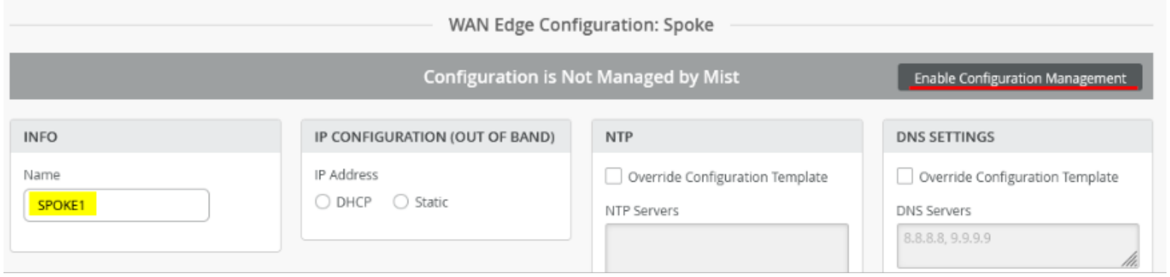
- Go to Inventory Page. The Figure below shows the details of devices assigned to site and high availability pairs.

Figure97: Inventory Display of HA Pair Details



| Name | Status | MAC Address | IP Address | Model | Version |
|---|---|---|---|---|---|
| SPOKE1 | Connected | 4c:96:14:32:f9:00 | 192.168.173.115 | vSRX3 | 21.4R1.12 |

- Verify the correct device is selected, click the **Enable Configuration Management** option.


WAN Edge Configuration: Spoke
Configuration is Not Managed by Mist
Enable Configuration Management
INFO
IP CONFIGURATION (OUT OF BAND)
NTP
DNS SETTINGS

Name: SPOKE1

IP Address: ○ DHCP ○ Static

□ Override Configuration Template

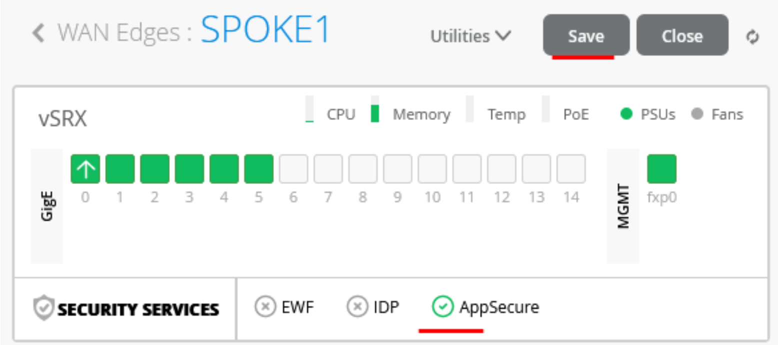
NTP Servers

□ Override Configuration Template

DNS Servers: 8.8.8.8, 9.9.9.9

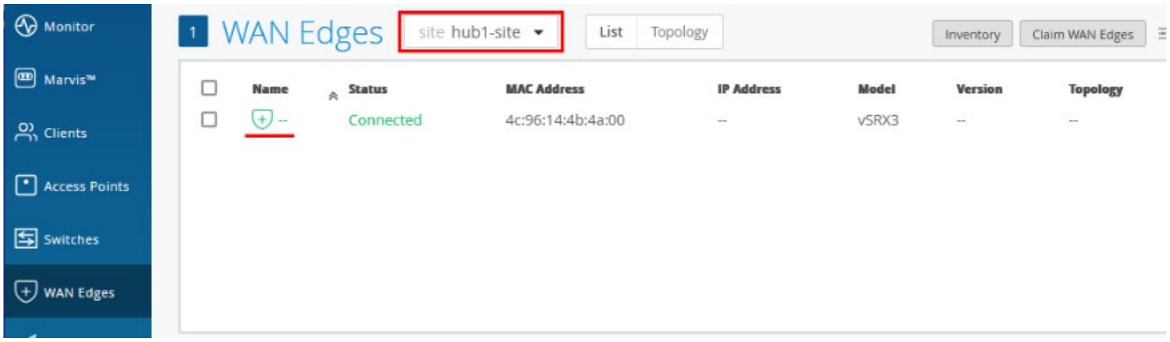
- Save your changes.

Figure98: Saving Spoke Device Configuration Changes



Now you have a topology with highly available hub and spoke Juniper® Networks Session Smart™ Routers using the WAN Assurance solution.

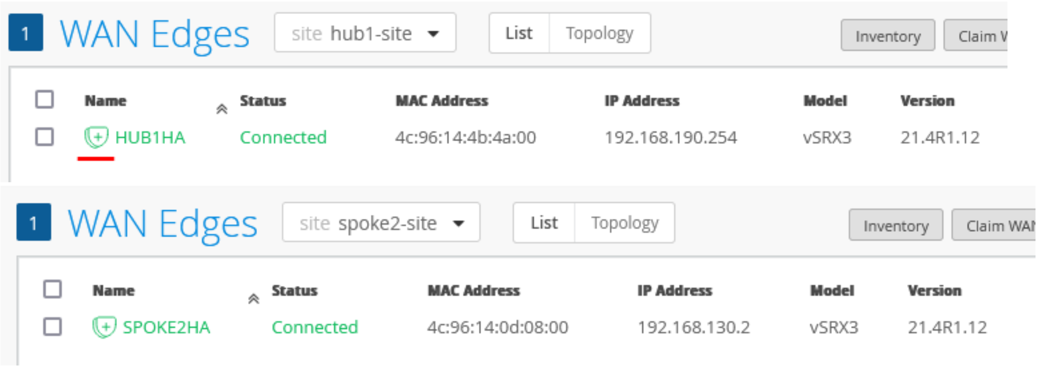
- (Optional) In Juniper Mist portal, go to **WAN Edges** and select **hub1-site.**



| Name | Status | MAC Address | IP Address | Model | Version | Topology |
|---|---|---|---|---|---|---|
| -- | Connected | 4c:96:14:4b:4a:00 | -- | vSRX3 | -- | -- |

- Change the name as "HUB1HA" and save the changes. Similarly, you can rename spoke2-site as "SPOKE2HA".

Figure99: Renaming Hub and Spoke HA Cluster Setup



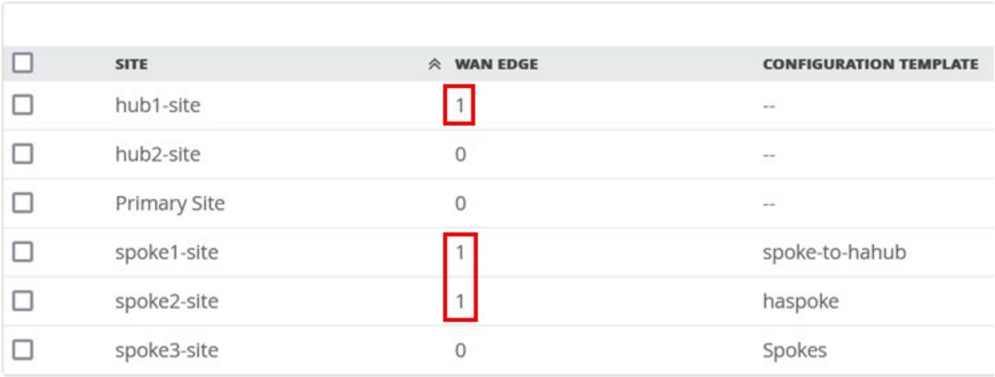
| Name | Status | MAC Address | IP Address | Model | Version |
|---|---|---|---|---|---|
| HUB1HA | Connected | 4c:96:14:4b:4a:00 | 192.168.190.254 | vSRX3 | 21.4R1.12 |

| Name | Status | MAC Address | IP Address | Model | Version |
|---|---|---|---|---|---|
| SPOKE2HA | Connected | 4c:96:14:0d:08:00 | 192.168.130.2 | vSRX3 | 21.4R1.12 |

High availability cluster formation might take approximately 30 minutes or more.

If you review the spoke template assignments, you can notice that a cluster setup is considered as a single device.

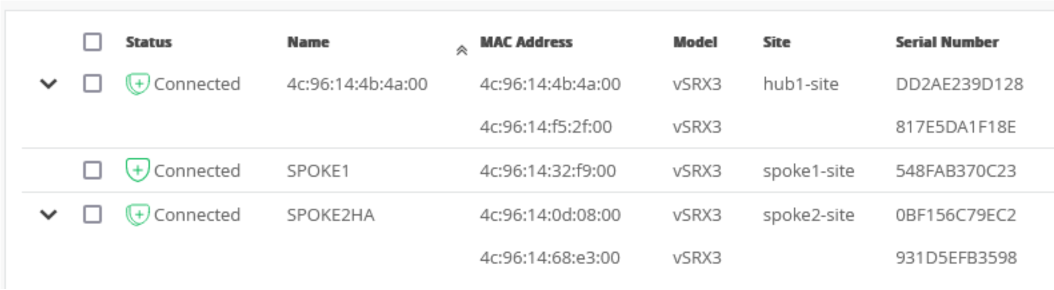
Figure100: WAN Edge Template Assignments



| □ | SITE | WAN EDGE | CONFIGURATION TEMPLATE |
|---|---|---|---|
| □ | hub1-site | 1 | -- |
| □ | hub2-site | 0 | -- |
| □ | Primary Site | 0 | -- |
| □ | spoke1-site | 1 | spoke-to-hahub |
| □ | spoke2-site | 1 | haspoke |
| □ | spoke3-site | 0 | Spokes |

In the device inventory you can see the cluster setup displayed as single device. But the system displays MAC addresses of both devices that are part of cluster setup.

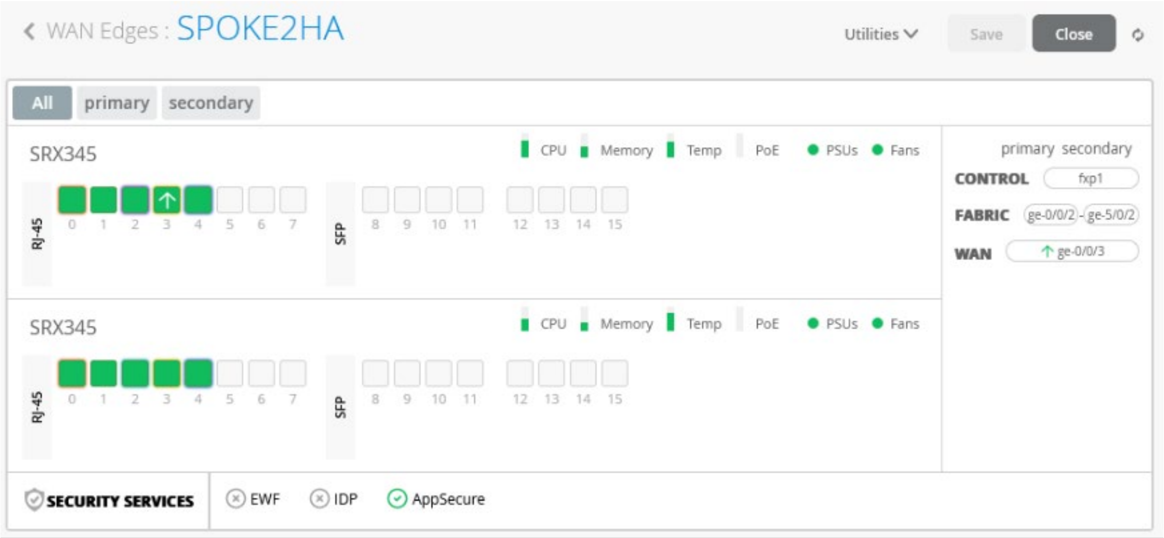
Figure101: Device Inventory



| | □ | Status | Name | MAC Address | Model | Site | Serial Number |
|---|---|---|---|---|---|---|---|
| ⌄ | □ | Connected | 4c:96:14:4b:4a:00 | 4c:96:14:4b:4a:00 | vSRX3 | hub1-site | DD2AE239D128 |
| | | | | 4c:96:14:f5:2f:00 | vSRX3 | | 817E5DA1F18E |
| | □ | Connected | SPOKE1 | 4c:96:14:32:f9:00 | vSRX3 | spoke1-site | 548FAB370C23 |
| ⌄ | □ | Connected | SPOKE2HA | 4c:96:14:0d:08:00 | vSRX3 | spoke2-site | 0BF156C79EC2 |
| | | | | 4c:96:14:68:e3:00 | vSRX3 | | 931D5EFB3598 |

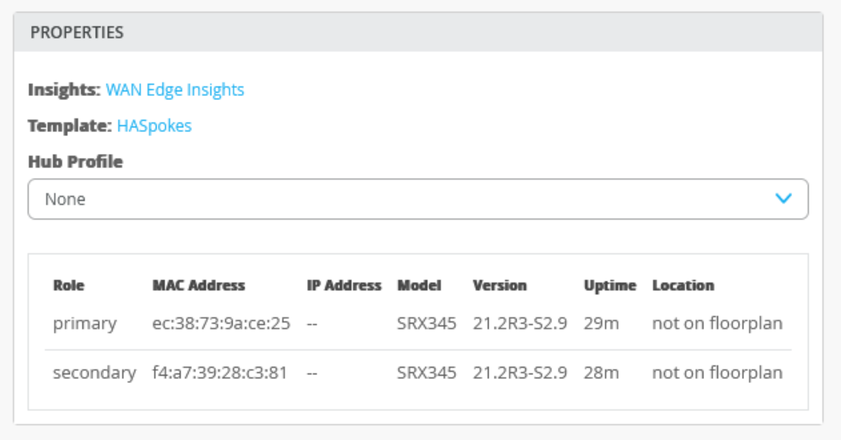
On the dashboard, for example, for the spoke devices that are part of high availability cluster, you can see the notion of primary and secondary device.

Figure102: Example of SRX345 High Availability Cluster Display Details.



The **Properties** pane displays the two devices that are part of high availability cluster.

Figure103: Properties Pane



PROPERTIES

**Insights:** WAN Edge Insights

**Template:** HASpokes

**Hub Profile**

None

| Role | MAC Address | IP Address | Model | Version | Uptime | Location |
|---|---|---|---|---|---|---|
| primary | ec:38:73:9a:ce:25 | -- | SRX345 | 21.2R3-S2.9 | 29m | not on floorplan |
| secondary | f4:a7:39:28:c3:81 | -- | SRX345 | 21.2R3-S2.9 | 28m | not on floorplan |

# Full-Stack Topology with Juniper EX-Switch and Mist AP Added

In this chapter we will implement the fourth topology that we have discussed above and show you the entire workflow by this. **This design only shows the changes from the first design and not the complete process again.** We assume you learnt the basics already with the first topology hence we keep this crips and only show the diffs to that.

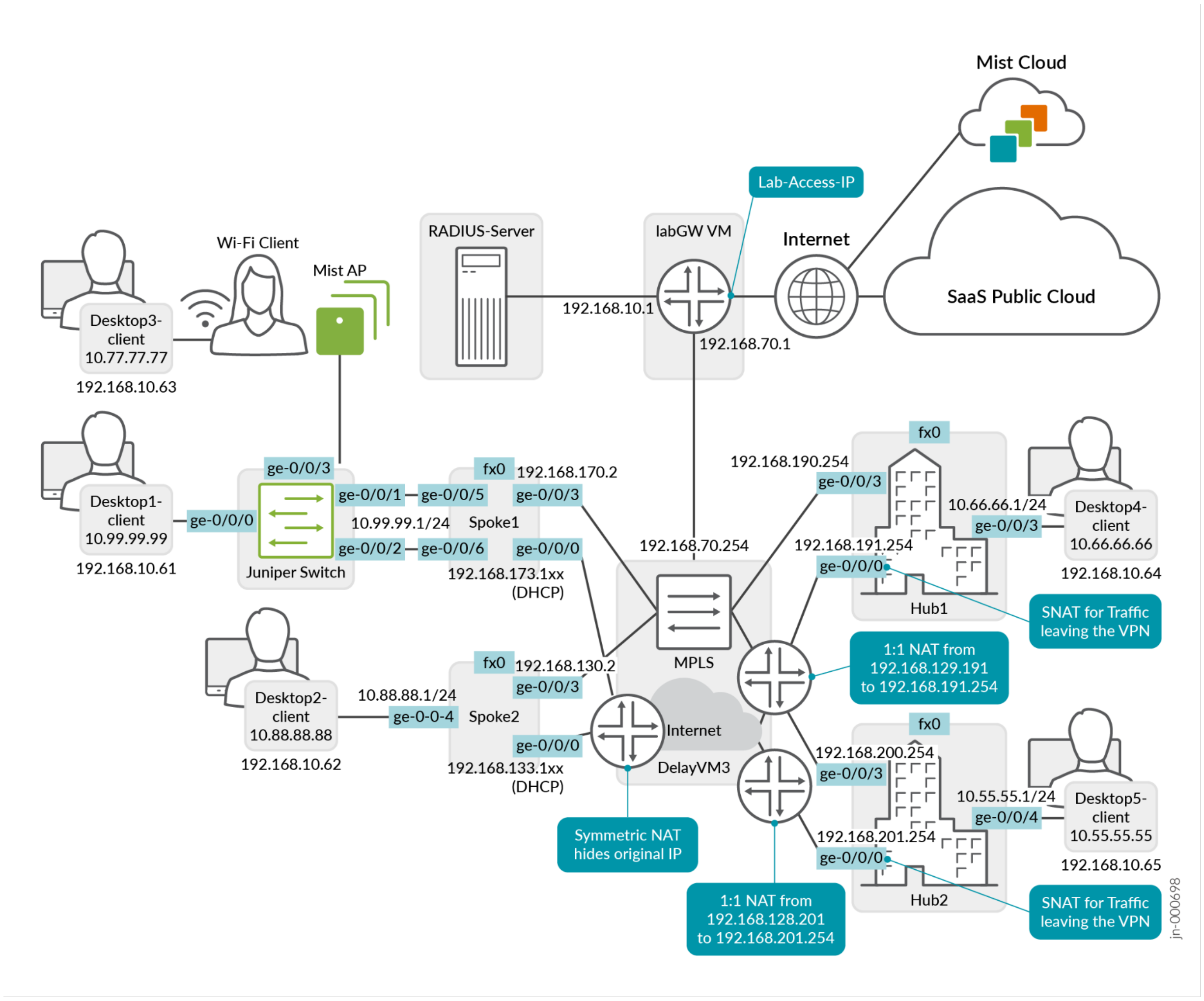
With this configuration example, you're expanding network capabilities by integrating Mist APs and Juniper EX Switches. This full stack example shows you how to set up your Juniper SD-WAN SRX Series WAN edge devices in concert with Juniper EX Series Switches deployed in wired assurance. This brings all your network devices into a cohesive onboarding, monitoring, and troubleshooting dashboard.

The example begins at the highest level of WAN assurance, focusing on SRX Series Firewalls. We assume that you already deployed SRX Series Firewall in a hub and spoke network. The SRX Series Firewall serves as the WAN edge device and foundation for building out your entire network.

For this full-stack design, you'll need at least one Juniper EX Switch to onboard into the Mist cloud. If you plan to do advanced testing with virtual circuits, two EX Switches is ideal. Additionally, you can incorporate a Mist AP into the setup to enhance the wireless capabilities of the network. Integrating APs and switches into your LAN network for management by Mist allows effortless monitoring and control of WAN edge devices, switches, and APs via the Juniper Mist portal dashboard.

The Table below shows the Full Stack Juniper Mist WAN Assurance topology used in this example.

Figure104: Juniper® Mist Validated Design - Mist WAN Assurance with Wireless and Wired Assurance



Requirements

To get started, you'll need to alter some of the interfaces configured on SRX Series Firewall for WAN deployment. In this example, we'll change interfaces using WAN edge templates.

In addition, this example uses:

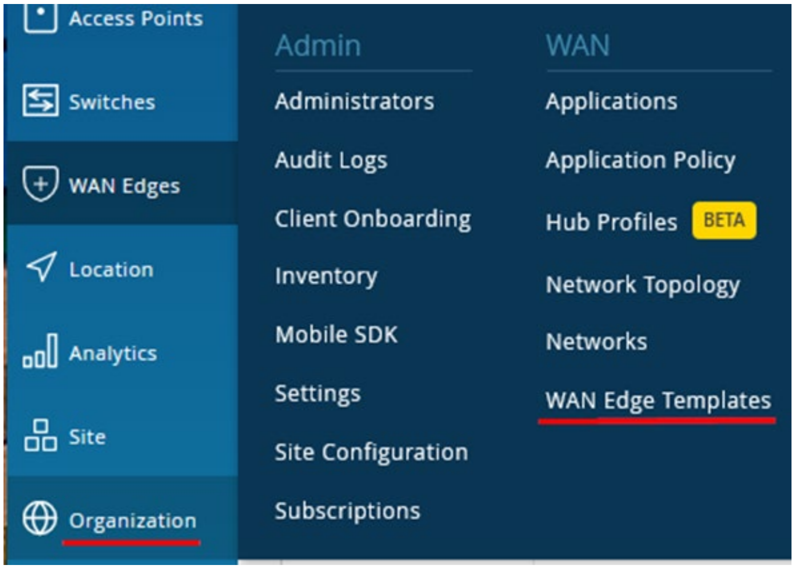
- Desktop3 VM (VLAN1077) - Operates as a viewer for the Raspberry Pi, the wireless client. Alternatively, you could use a local notebook.
- Desktop1 VM (VLAN1099) - Connected to the interface ge-0/0/0 of the new branch switch.

## Create a New Spokes Configuration Template

To create a new spokes configuration quickly and efficiently, you can clone the template for an existing spoke and then make the necessary changes. It makes things much easier.

In the Juniper Mist portal, click Organization > WAN > WAN Edge Templates.

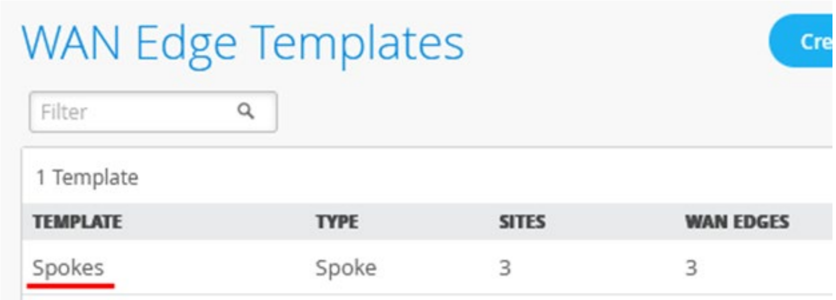
Figure105: Navigate to WAN Edge Template



**Note**: You can create a template by importing the shared JSON file also.

- A list of existing templates, if any, appears.

Figure106: List of WAN Edge Templates



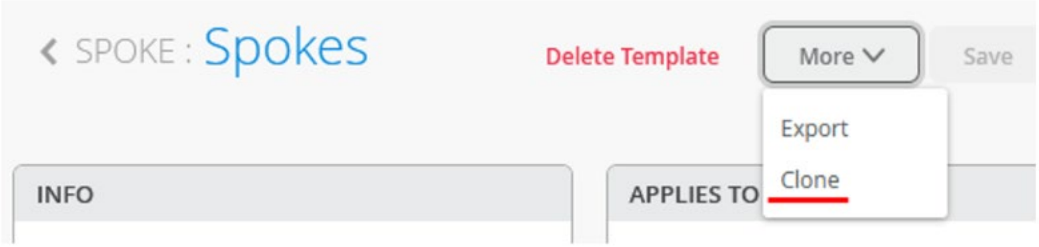
1 Template

| TEMPLATE | TYPE | SITES | WAN EDGES |
|---|---|---|---|
| Spokes | Spoke | 3 | 3 |

Create a spoke template by cloning an existing spoke template.

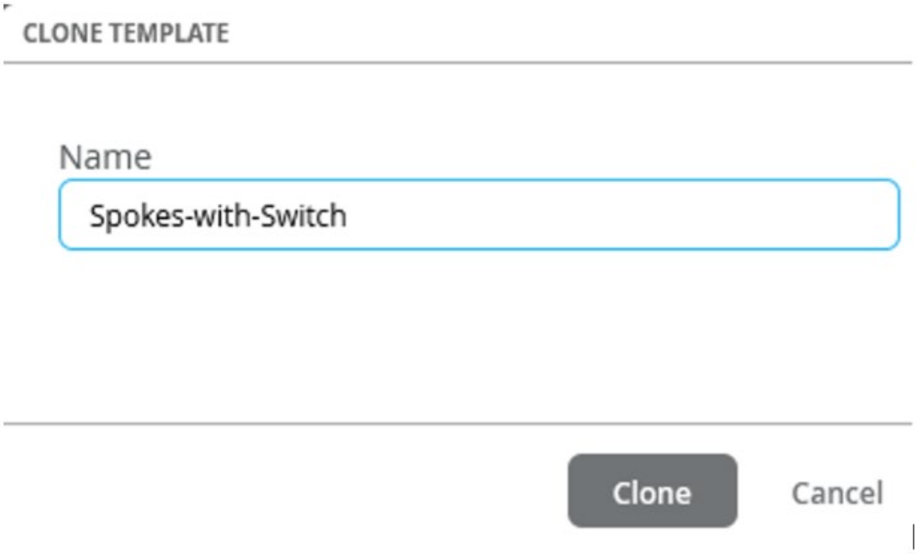
- Click **More** and select **Clone**.

Figure107: Selecting Clone Option for Template



- Enter the name as **Spokes-with-Switch** and click **Clone**.

Figure108: Saving Cloned Template



CLONE TEMPLATE

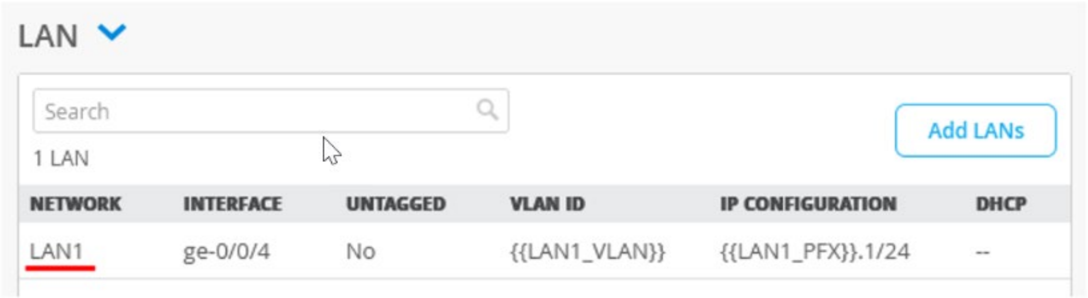
Name: Spokes-with-Switch

**Tip**: Refresh your browser after cloning. This ensures objects displayed are truly refreshed.

Edit the LAN Interface

- On the LAN interface configuration section, edit the existing interface (**LAN1**).

Figure109: LAN Interface Configuration on Template



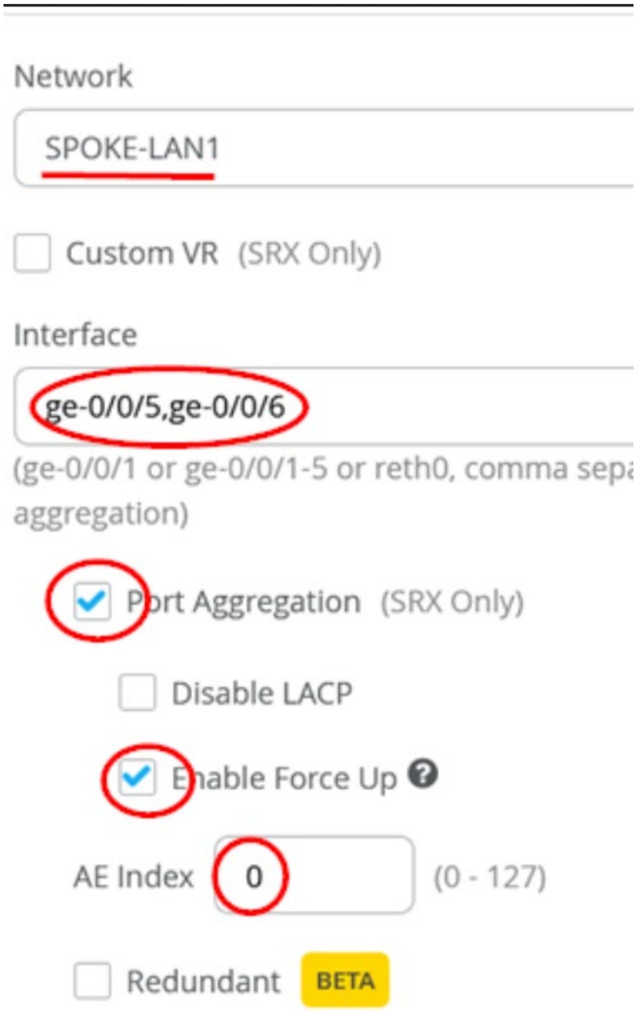
LAN

1 LAN

| NETWORK | INTERFACE | UNTAGGED | VLAN ID | IP CONFIGURATION | DHCP |
|---|---|---|---|---|---|
| LAN1 | ge-0/0/4 | No | {{LAN1_VLAN}} | {{LAN1_PFX}}.1/24 | -- |

- Change the name of LAN1 interface as **SPOKE-LAN1** and apply following changes:
  - **Interface**—ge-0/0/5, ge-0/0/6.
  - Port Aggregation—Enable.
  - **Enable Force Up**—Enable. We recommend this configuration when the switch has no dedicated OOB interface in the LAG and using in-band managed interface. This setting prevents the switch from losing the connection to the Juniper Mist Cloud
  - **AE Index**—0 (as there is no LAG port enabled).

Figure110: Modify LAN Interface Configuration



Network

SPOKE-LAN1

□ Custom VR (SRX Only)

Interface

ge-0/0/5,ge-0/0/6

(ge-0/0/1 or ge-0/0/1-5 or reth0, comma sepa
aggregation)

☑ Port Aggregation (SRX Only)

□ Disable LACP

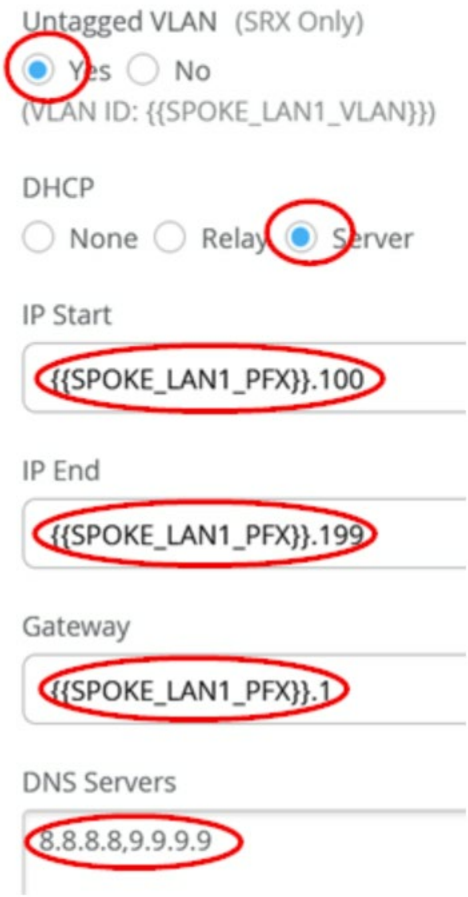
☑ Enable Force Up

AE Index 0 (0 - 127)

□ Redundant BETA

- Continue to configure the **SPOKE-LAN1** interface:
  - **Untagged VLAN**—Yes. This setting enables VLAN access/native to handout DHCP-leases to the switch. Otherwise, set the site variable {{SPOKE_LAN1_VLAN}} to “0” to have the same results.
  - **DHCP**—Server
  - **IP Start**—{{SPOKE_LAN1_PFX}}.100
  - **IP End**—{{SPOKE_LAN1_PFX}}.199
  - **Gateway**—{{SPOKE_LAN1_PFX}}.1
  - **DNS Servers**—8.8.8.8, 9.9.9.9

Figure111: Modify LAN Interface Configuration



Untagged VLAN (SRX Only)

● Yes ○ No

(VLAN ID: {{SPOKE_LAN1_VLAN}})

DHCP

○ None ○ Relay ● Server

IP Start

{{SPOKE_LAN1_PFX}}.100

IP End

{{SPOKE_LAN1_PFX}}.199

Gateway

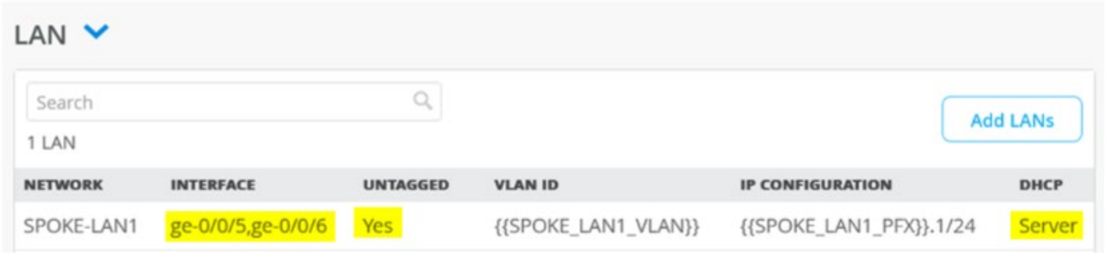
{{SPOKE_LAN1_PFX}}.1

DNS Servers

8.8.8.8,9.9.9.9

The Figure below shows the LAN interface you modified.

Figure112: Summary of LAN Interface

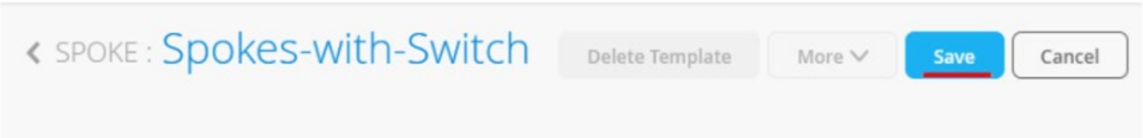


1 LAN

| NETWORK | INTERFACE | UNTAGGED | VLAN ID | IP CONFIGURATION | DHCP |
|---|---|---|---|---|---|
| SPOKE-LAN1 | ge-0/0/5,ge-0/0/6 | Yes | {{SPOKE_LAN1_VLAN}} | {{SPOKE_LAN1_PFX}}.1/24 | Server |

- Click **Save** to save your changes.

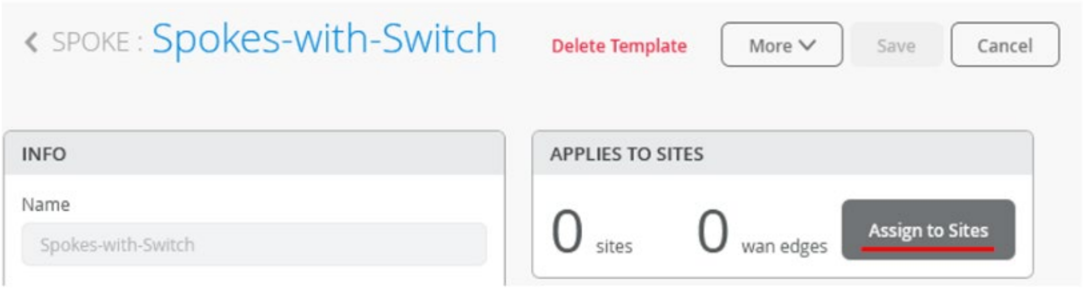
Figure113: Saving WAN Edge Template



## Assign the New Template to a Site

- Scroll to the top of the WAN Edge Templates page and click **Assign to Sites** under Spokes panel.

Figure114: Assign Spoke Templates to Sites

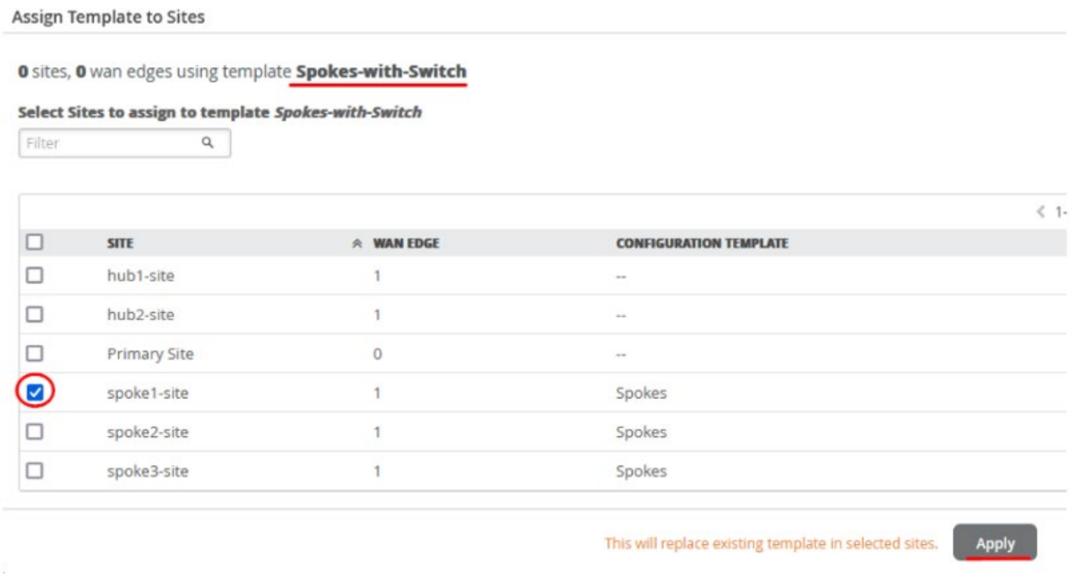


Name: Spokes-with-Switch

0 sites 0 wan edges

- In the Assign Template to Sites pane, select **spoke1-site** template and click **Apply**.

Figure115: Select Sites to Assign Spoke Templates



**0** sites, **0** wan edges using template **Spokes-with-Switch**

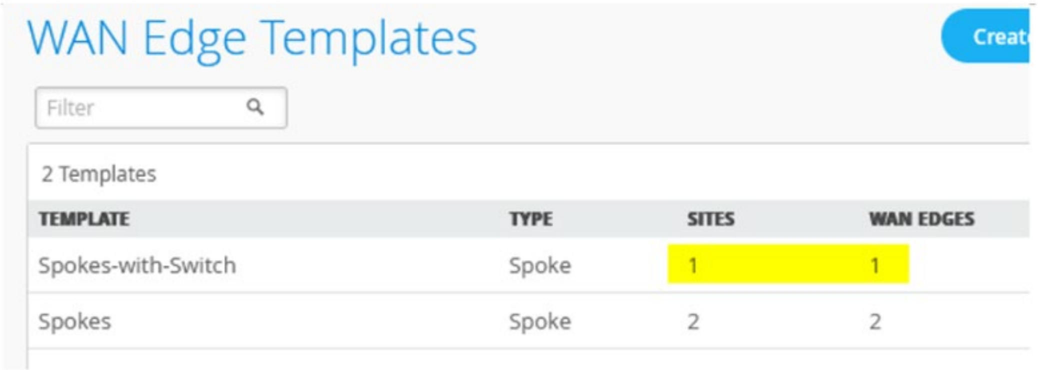
**Select Sites to assign to template *Spokes-with-Switch***

| □ | SITE | WAN EDGE | CONFIGURATION TEMPLATE |
|---|---|---|---|
| □ | hub1-site | 1 | -- |
| □ | hub2-site | 1 | -- |
| □ | Primary Site | 0 | -- |
| ☑ | spoke1-site | 1 | Spokes |
| □ | spoke2-site | 1 | Spokes |
| □ | spoke3-site | 1 | Spokes |

This will replace existing template in selected sites.

Review the template settings as shown in Figure 101 on page 124.

Figure116: Details of WAN Edge Template


WAN Edge Templates

2 Templates

| TEMPLATE | TYPE | SITES | WAN EDGES |
|---|---|---|---|
| Spokes-with-Switch | Spoke | 1 | 1 |
| Spokes | Spoke | 2 | 2 |

## Add Your EX-Switch to the Topology

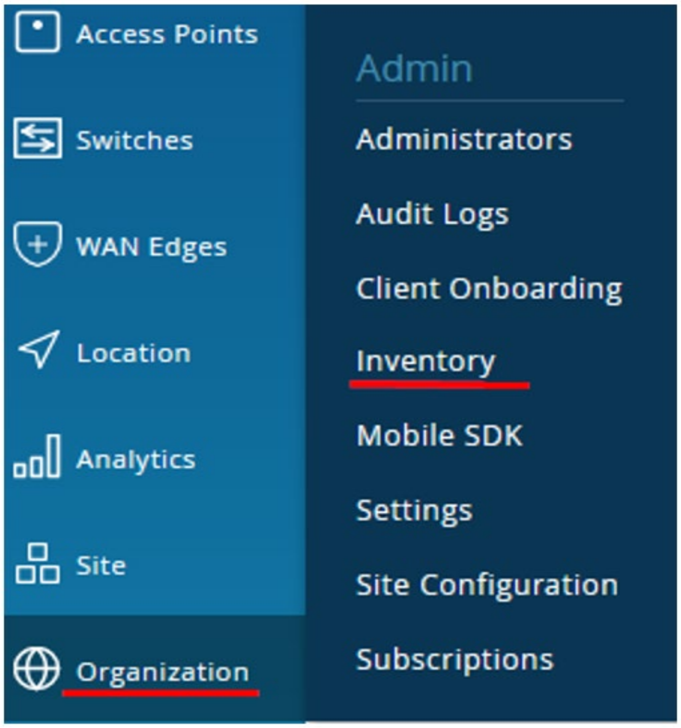
Now it is time to onboard your switch and add it to your infrastructure. For details on how to onboard your switch, refer to the product documentation for your switch in the Juniper TechLibrary.

For details on getting a new cloud-ready EX switch up and running in the Juniper Mist AI cloud portal, see Cloud-Ready EX and QFX Switches with Mist.

To assign a switch to a site:

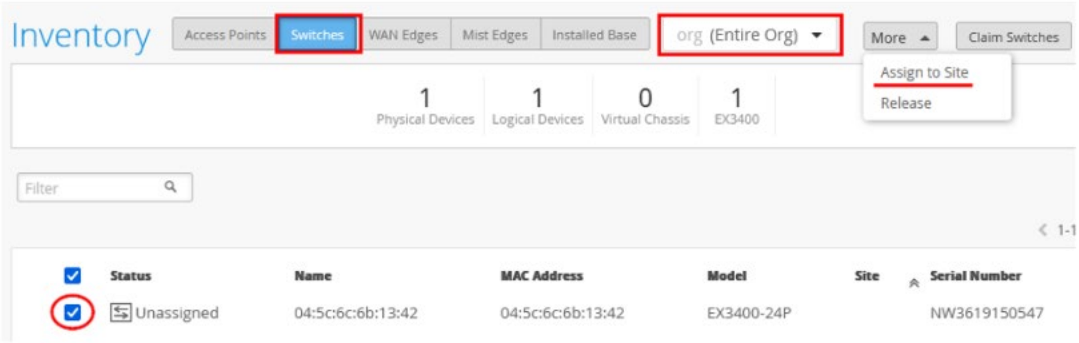
- In the Juniper Mist portal, click **Organization** > **Admin** > **Inventory**.

Figure117: Navigating to Inventory



- In the Inventory page, ensure the inventory view is set to **org (Entire Org)** and refresh your browser until you see all your devices.

Figure118: EX Series Switch in Inventory



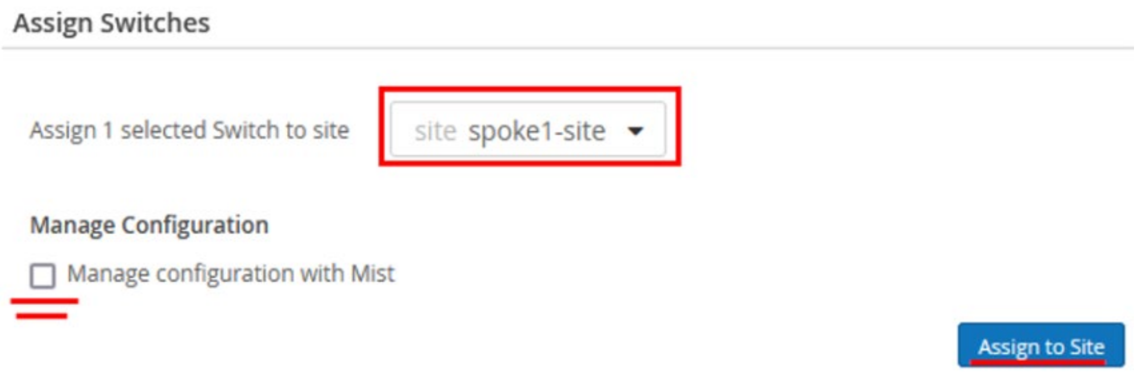
| 1 | 1 | 0 | 1 |
|---|---|---|---|
| Physical Devices | Logical Devices | Virtual Chassis | EX3400 |

| ☑ | Status | Name | MAC Address | Model | Site | Serial Number |
|---|---|---|---|---|---|---|
| ☑ | Unassigned | 04:5c:6c:6b:13:42 | 04:5c:6c:6b:13:42 | EX3400-24P | | NW3619150547 |

Select your new switch and click **Assign to Site**.

- On the Assign Switches page:
  - Select the **spoke1-site**.
  - Disable **Manage configuration with Mist** option. You can enable this option at a later stage if required.

Figure119: Selecting Site for Assigning Switch



Assign Switches

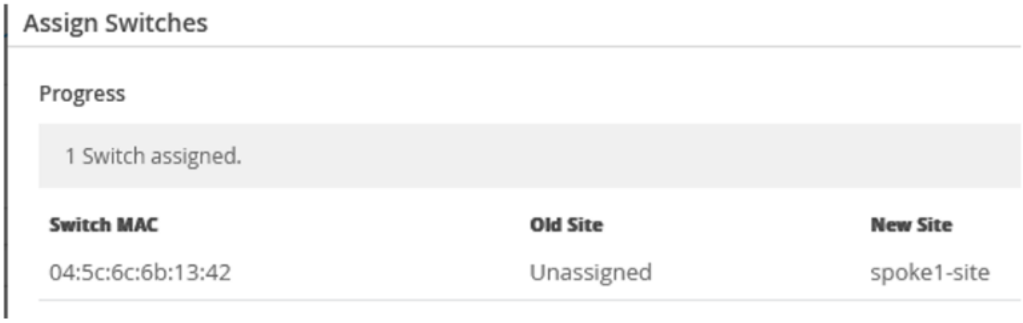
Assign 1 selected Switch to site: site spoke1-site

Manage Configuration

□ Manage configuration with Mist

- Click Assign to Site.
- Confirm the changes in the inventory once you assign the device to the site.
- You can see **spoke1-site** under **New Site**.

Figure120: Assigned Switch to Site Details



Assign Switches

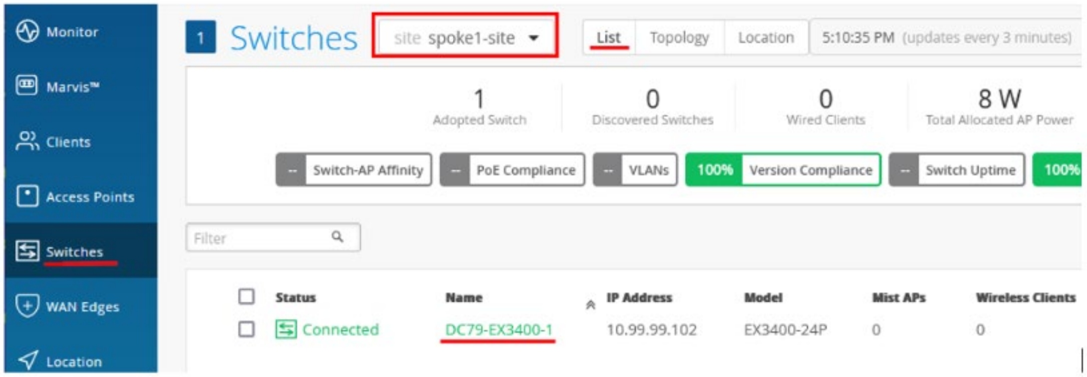
Progress

1 Switch assigned.

| Switch MAC | Old Site | New Site |
|---|---|---|
| 04:5c:6c:6b:13:42 | Unassigned | spoke1-site |

- In the Juniper Mist portal, go to **Switches** and select **spoke1-site**.

Figure121: Selecting Assigned Switch for Modification

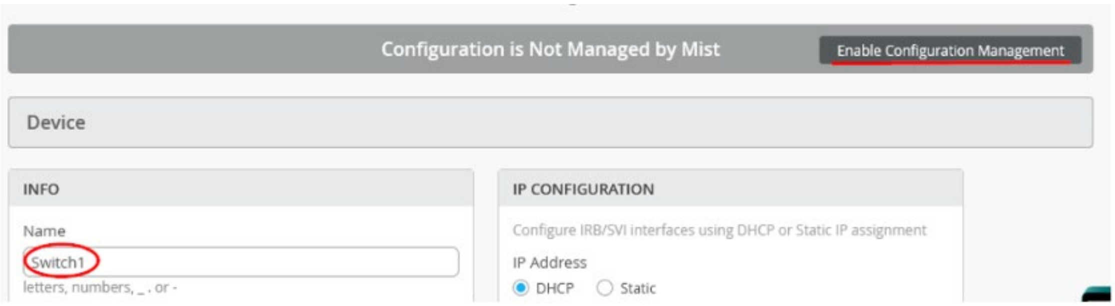


| ☐ | Status | Name | IP Address | Model | Mist APs | Wireless Clients |
|---|---|---|---|---|---|---|
| ☐ | Connected | DC79-EX3400-1 | 10.99.99.102 | EX3400-24P | 0 | 0 |

The page displays the list of switches assigned to the site.

- Click the required switch to open the switch configuration page.
- Verify the device name, then scroll down to **Switch Configuration** section and check **Enable Configuration Management**.

Figure122: Configuration of Assigned Switch



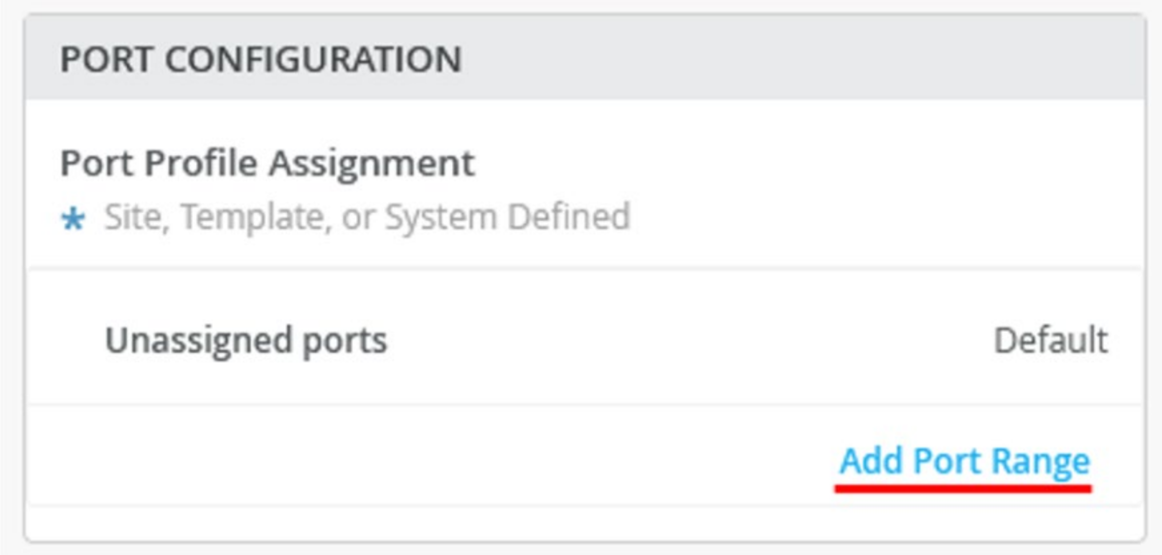
Configuration is Not Managed by Mist
Enable Configuration Management
Device
INFO
IP CONFIGURATION
Configure IRB/SVI interfaces using DHCP or Static IP assignment
letters, numbers, _ . or -

Name: Switch1

IP Address: ● DHCP ○ Static

- Under Port Configuration, click Add Port Range.

Figure123: Port Configuration of Assigned Switch



PORT CONFIGURATION

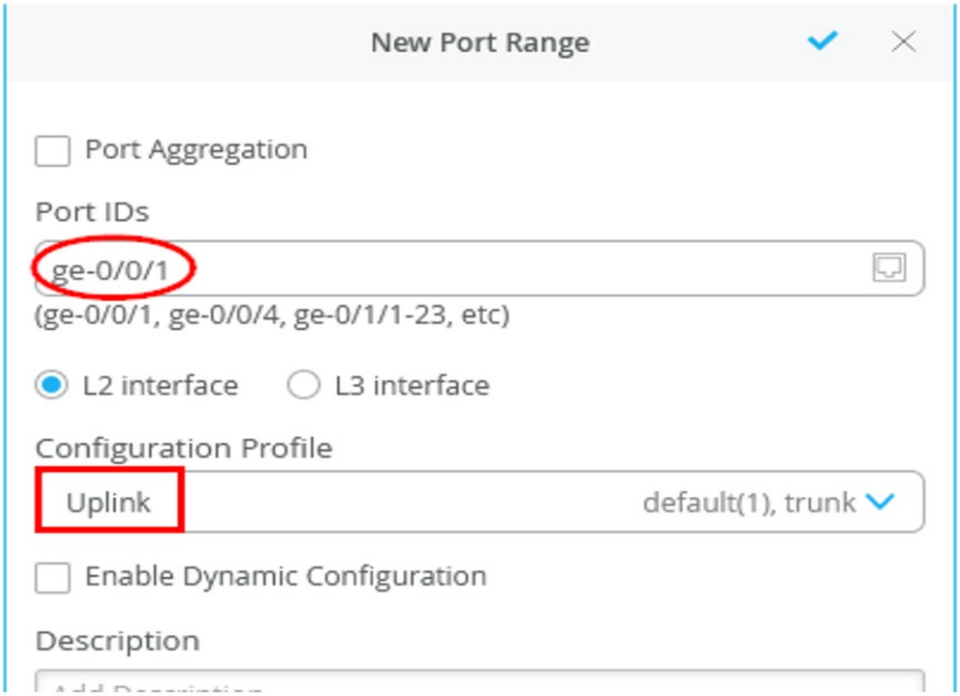
Port Profile Assignment

* Site, Template, or System Defined

| | |
|---|---|
| Unassigned ports | Default |

- In the **New Port Range** page, configure the following options:
  - Enable Port Aggregation.
  - Set **AE Index** to **0** to ensure that the AE index is the same on both sides.
  - Set the **Port IDs** as **ge-0/0/1** and **ge-0/0/2** ( two ports for the LAG).
  - Select the existing Configuration Profile as Uplink.

Figure124: Port Configuration of Assigned Switch



New Port Range

□ Port Aggregation

Port IDs

ge-0/0/1

(ge-0/0/1, ge-0/0/4, ge-0/1/1-23, etc)

● L2 interface ○ L3 interface

Configuration Profile

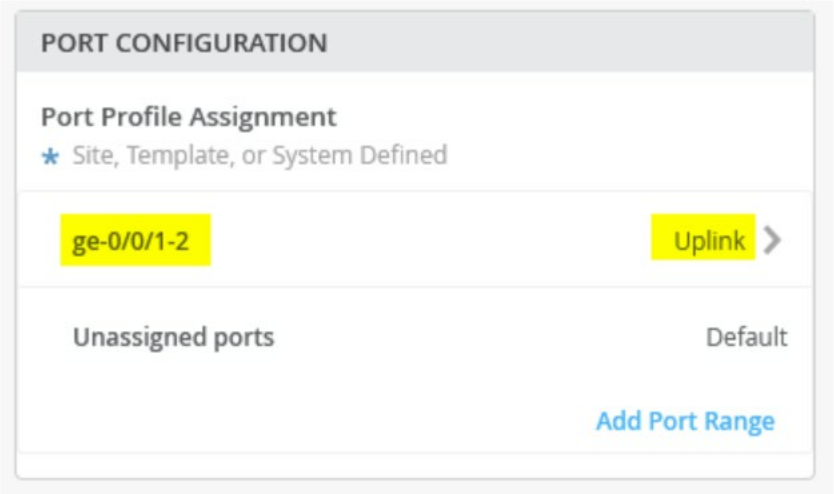
Uplink default(1), trunk

□ Enable Dynamic Configuration

Description

- The Figure below shows the summary of port configuration.

Figure125: Port Configuration of Assigned Switch



PORT CONFIGURATION

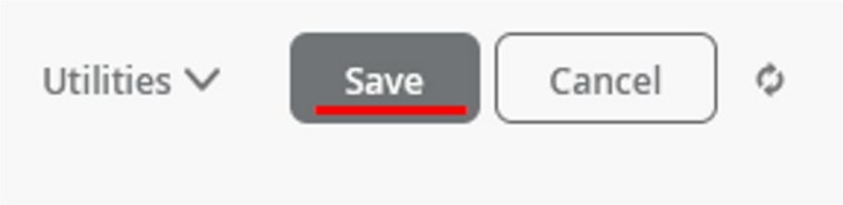
Port Profile Assignment

★ Site, Template, or System Defined

| | |
|---|---|
| ge-0/0/1-2 | Uplink › |
| Unassigned ports | Default |

- Save your changes.

Figure126: Save Changes



You've now added a Juniper switch to your Mist WAN Assurance deployment.

Optionally, you can confirm your switch has the two links towards SRX Series Firewall using Remote Shell as shown in the following sample:

```
show lacp interfaces
Aggregated interface: ae0
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-0/0/1       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/1     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/2       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/2     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-0/0/1                  Current   Fast periodic Collecting distributing
      ge-0/0/2                  Current   Fast periodic Collecting distributing
```

# Topology optimizations, enhancements, and extensions valid for all four Topologies

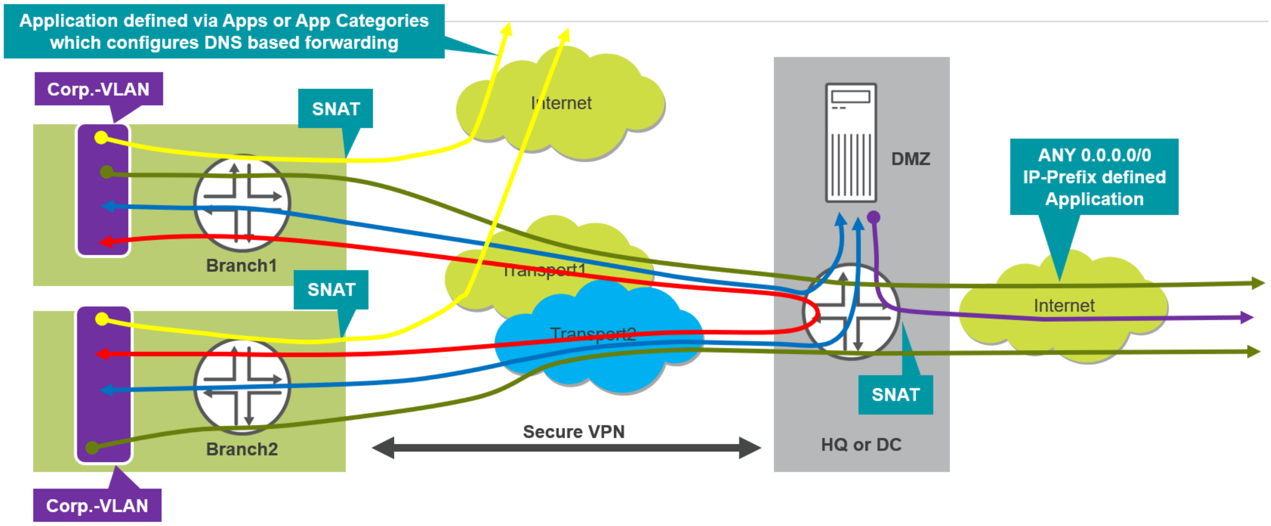
In this chapter we present some of the optional optimizations, enhancements, and extensions one may do to the presented Topologies. This is all about treating some Applications differently than the VPN Model that we have presented so far. Customers have different desires that they typically also want to address in some way. We are presenting here the most typical ones and show how to implement those. You may not use them immediately, but some make sense to be considered already at the start of your SD-WAN implementation. The typical ones are:

- Identifying an application that is not part of the customer's VPN, hence typically reached over the Internet and breakout the Traffic for is right at the Spoke to not burden the VPN with it.
- Some Customers would like to offer something like a Wi-Fi Hotspot that other People can use to browse the Internet. Here it must be secured that this Traffic cannot harm the VPN hence local breakout is often used.
- Making a connection to a Service in the Cloud that offers advanced security screening for Traffic when People want to use it to go further into the Internet. In this case there if less a need to do much screening locally on the Spoke but still some form of Tunnel towards this Cloud service must be created.

## Application Local Traffic Breakout at Spoke

In this model we try to identify certain application Traffic that usually would be in the ANY Traffic category and treat it differently from the usual forwarding. A typical use case is working with an application that is hosted on the Internet. Here it would not make much sense to continue using the VPN overlay and then do central breakout at the Hub. It would make more sense to identify this application and locally breakout the Traffic at the Spoke to have a shorter path to the destination than to congest your VPN with Traffic that then goes to the internet anyway. The below picture demonstrates this.

Basic initial Traffic model with DNS identified Application LBO extension


Application defined via Apps or App Categories which configures DNS based forwarding
Corp.-VLAN
SNAT
Internet
Branch1
SNAT
Transport1
Transport2
DMZ
ANY 0.0.0.0/0 IP-Prefix defined Application
Internet
SNAT
Branch2
Secure VPN
HQ or DC
Corp.-VLAN

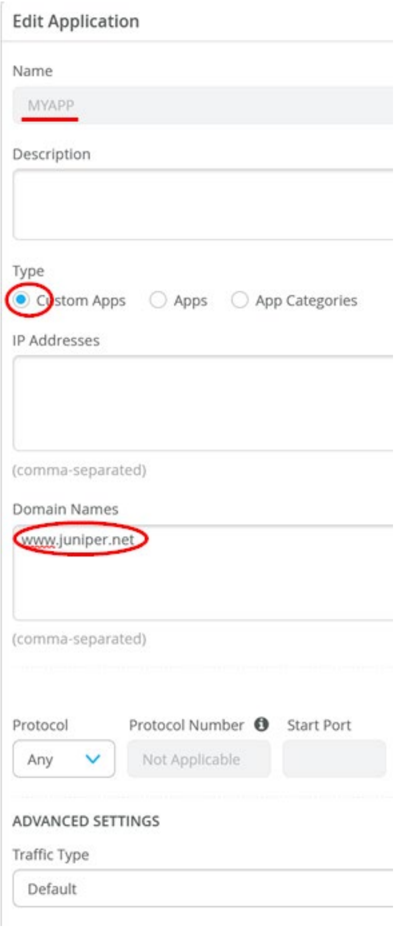
Applications can be defined via the Mist UI by defining the following parameters:

- IP address prefixes. We have done that throughout the Topologies created above in this document. This is good to create your VPN but not very practical for Internet Services.

- Protocol (Number like ICMP/TCP/UDP etc.) but not very practical for Internet Services.
- Destination Ports (Start/End) but not very practical for Internet Services.
- Domain Names. Presently only FQDN’s are configurable through Mist UI.
- Applications. The SRX uses its DPI-Engine to identify those (>7000 presently).
- Application Categories. Here the Applications known by the IDP-Engine are pooled together in a few categories that then represent a bundle of Applications all together. This is easier to maintain when certain Traffic in unwanted.
- Learned Applications. When running Traffic since a while the System now reports what DPI-Engine found in terms of applications and then one can make decisions on those if one wants to keep them inside the VPN or use local breakout.

Note: In our example we use a simple custom application with a DNS-FQDN for demonstration of the feature. However, you are free to use one of the others mentioned above.

- Go to Organization -> Applications and create a new Application with the name: “MYAPP”
  - Type: “Custom Apps”
  - Domain Names: “www.juniper.net”



Edit Application

Name: MYAPP

Description

Type: ● Custom Apps ○ Apps ○ App Categories

IP Addresses

(comma-separated)

Domain Names: www.juniper.net

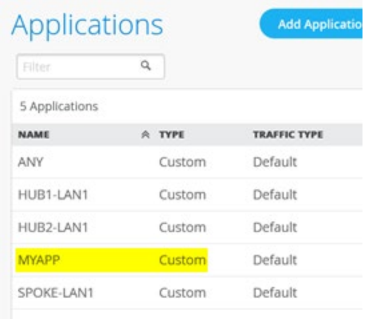
(comma-separated)

Protocol: Any | Protocol Number: Not Applicable | Start Port

ADVANCED SETTINGS

Traffic Type: Default

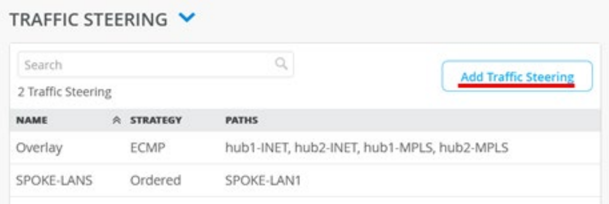
- The resulting Applications overview should look like this.



5 Applications

| NAME | TYPE | TRAFFIC TYPE |
|---|---|---|
| ANY | Custom | Default |
| HUB1-LAN1 | Custom | Default |
| HUB2-LAN1 | Custom | Default |
| MYAPP | Custom | Default |
| SPOKE-LAN1 | Custom | Default |

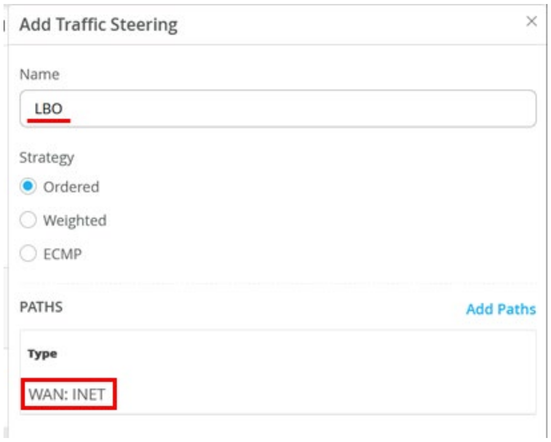
- Now go to Organization -> WAN Edge Templates and edit the existing “Spokes” Template. Add a new Traffic Steering.



2 Traffic Steering

| NAME | STRATEGY | PATHS |
|---|---|---|
| Overlay | ECMP | hub1-INET, hub2-INET, hub1-MPLS, hub2-MPLS |
| SPOKE-LANS | Ordered | SPOKE-LAN1 |

- Configure the new Traffic Steering:
  - Name: “LBO”
  - Path: “WAN: INET”



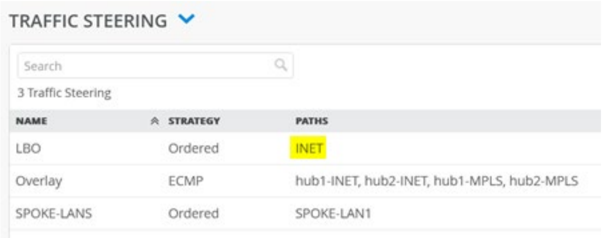
Name: LBO

Strategy
● Ordered
○ Weighted
○ ECMP

PATHS

| Type |
|---|
| WAN: INET |

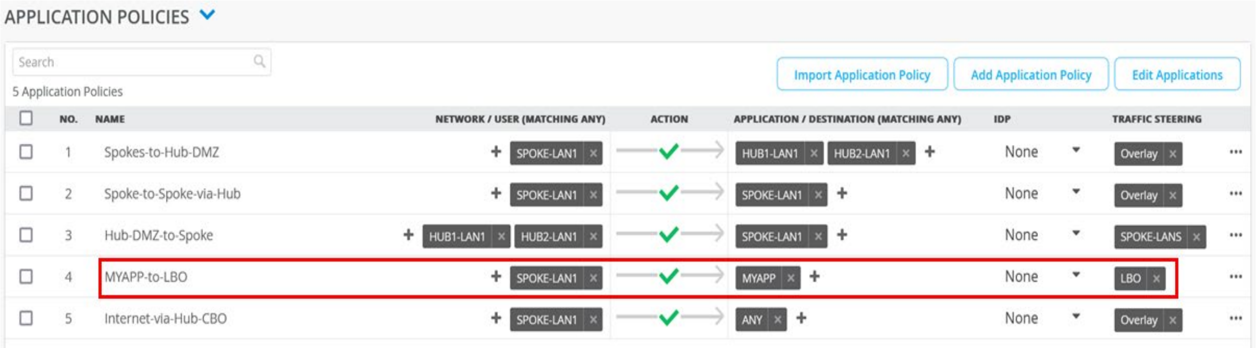
The resulting Traffic Steering overview should look like this.



3 Traffic Steering

| NAME | STRATEGY | PATHS |
|---|---|---|
| LBO | Ordered | INET |
| Overlay | ECMP | hub1-INET, hub2-INET, hub1-MPLS, hub2-MPLS |
| SPOKE-LANS | Ordered | SPOKE-LAN1 |

- Insert BEFORE the last rule a new Application Policy:
  - Name: “MYAPP-to-LBO”
  - Network: “SPOKE1-LAN1”
  - Application: “MYAPP”
  - Traffic Steering: “LBO”

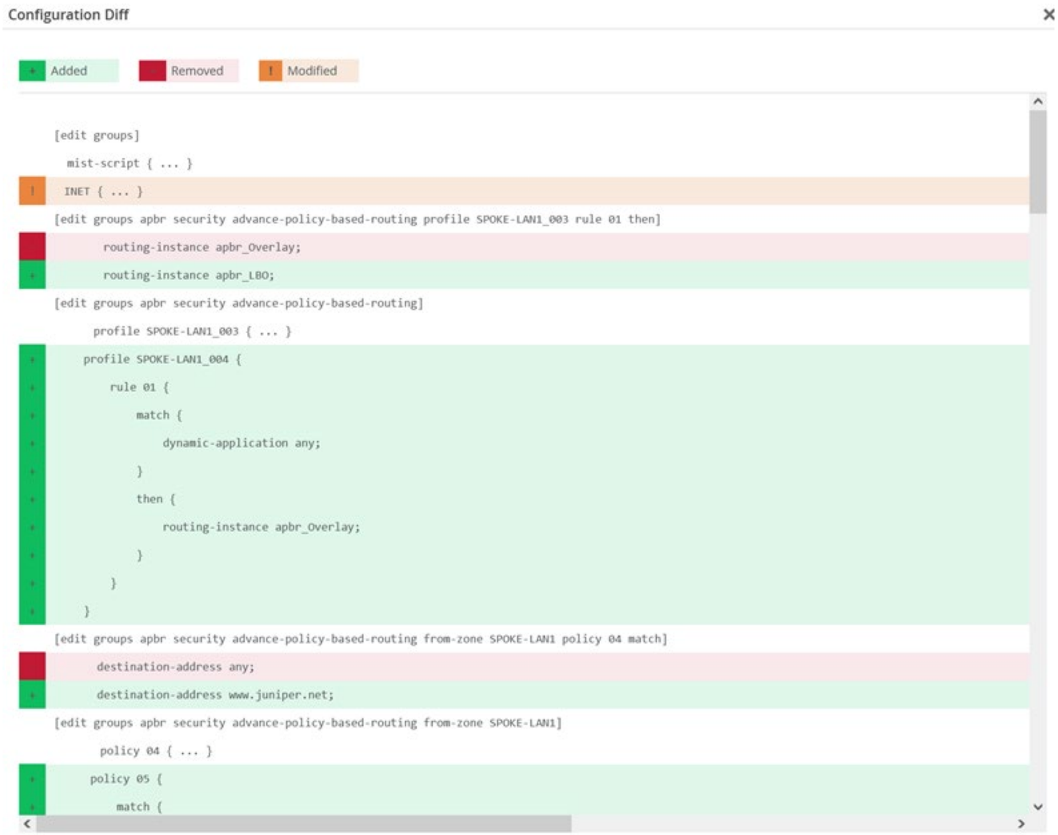


5 Application Policies

| ☐ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| ☐ | 1 | Spokes-to-Hub-DMZ | SPOKE-LAN1 | ✓ | HUB1-LAN1<br>HUB2-LAN1 | None | Overlay |
| ☐ | 2 | Spoke-to-Spoke-via-Hub | SPOKE-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| ☐ | 3 | Hub-DMZ-to-Spoke | HUB1-LAN1<br>HUB2-LAN1 | ✓ | SPOKE-LAN1 | None | SPOKE-LANS |
| ☐ | 4 | MYAPP-to-LBO | SPOKE-LAN1 | ✓ | MYAPP | None | LBO |
| ☐ | 5 | Internet-via-Hub-CBO | SPOKE-LAN1 | ✓ | ANY | None | Overlay |

- “SAVE” your modified Template to activate it on all Spokes.

A few minutes later you can review the configuration change made on the Spoke in insights.



```
  [edit groups]
    mist-script { ... }
!   INET { ... }
  [edit groups apbr security advance-policy-based-routing profile SPOKE-LAN1_003 rule 01 then]
-       routing-instance apbr_Overlay;
+       routing-instance apbr_LBO;
  [edit groups apbr security advance-policy-based-routing]
      profile SPOKE-LAN1_003 { ... }
+     profile SPOKE-LAN1_004 {
+         rule 01 {
+             match {
+                 dynamic-application any;
+             }
+             then {
+                 routing-instance apbr_Overlay;
+             }
+         }
+     }
  [edit groups apbr security advance-policy-based-routing from-zone SPOKE-LAN1 policy 04 match]
-     destination-address any;
+     destination-address www.juniper.net;
  [edit groups apbr security advance-policy-based-routing from-zone SPOKE-LAN1]
      policy 04 { ... }
+     policy 05 {
+         match {
```

If you want to review effects of your changes on the device then we suggest the following:

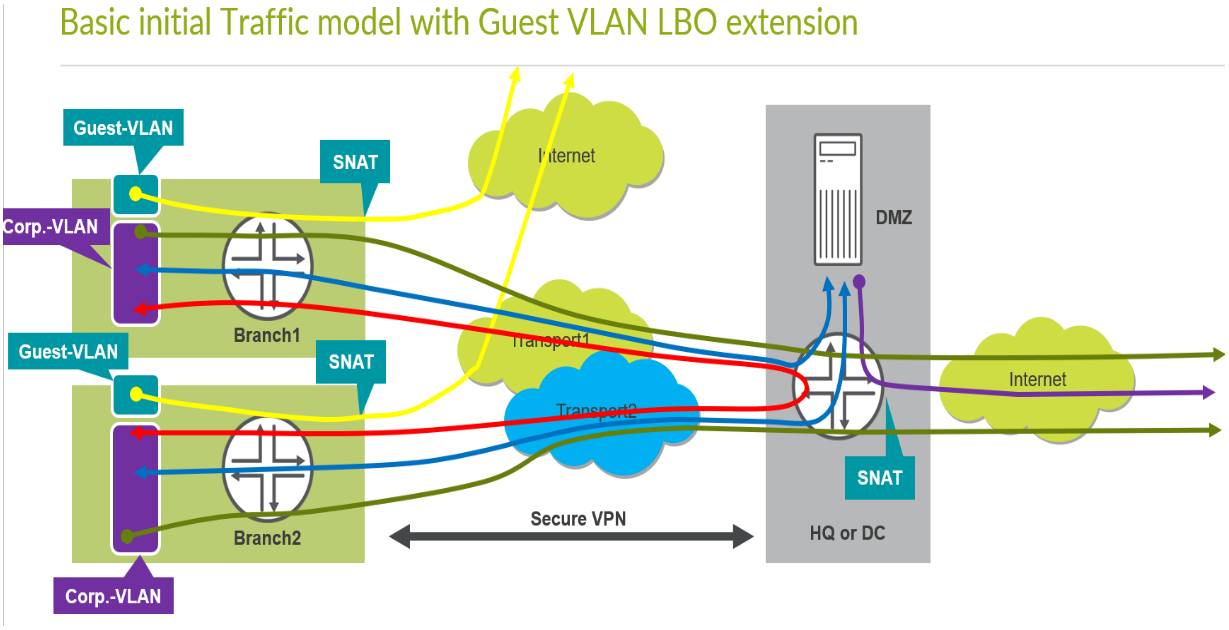
Start a continuous “ping www.juniper.net” on a client that is attached to the LAN-Interface of your Spoke. Please note the IP address DNS is resolved for this moment.

```
root@desktop1:~# ping www.juniper.net
PING e1824.dscb.akamaiedge.net (104.96.100.195) 56(84) bytes of data.
64 bytes from a104-96-100-195.deploy.static.akamaitechnologies.com (104.96.100.195): icmp_seq=1 ttl=49 time=6.24 ms
64 bytes from a104-96-100-195.deploy.static.akamaitechnologies.com (104.96.100.195): icmp_seq=2 ttl=49 time=4.56 ms
64 bytes from a104-96-100-195.deploy.static.akamaitechnologies.com (104.96.100.195): icmp_seq=3 ttl=49 time=4.52 ms
.
.
```

Now using Remote console via the Mist UI open a shell to the Spoke and review the status there like below example via CLI. You can see with the first command which policy is used and that ge-0/0/0 is the destination where the packet is forwarded which is our breakout WAN-interface. When you know the policy name you can dig deeper with the second command.

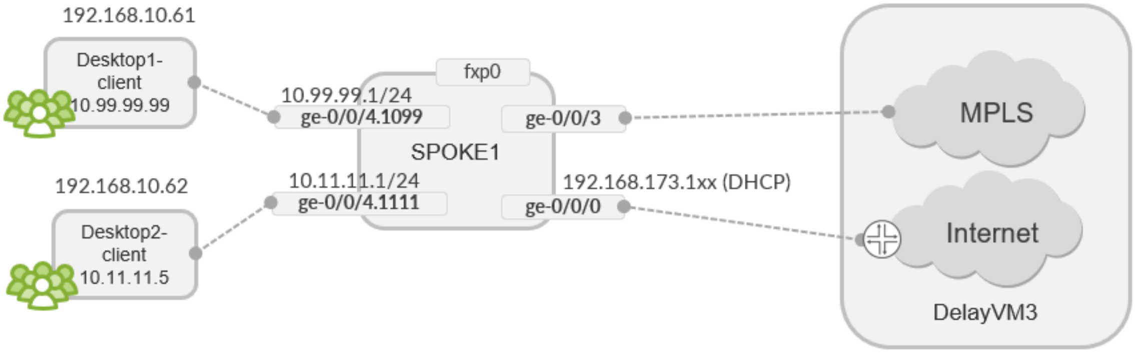
```
show security flow session destination-prefix 104.96.100.195
Session ID: 30064811163, Policy name: 01_MYAPP-to-LBO/7, State: Stand-alone, Timeout: 2, Valid
  In: 10.99.99.99/4 --> 104.96.100.195/43;icmp, Conn Tag: 0x0, If: irb.1099, Pkts: 1, Bytes: 84,
  Out: 104.96.100.195/43 --> 192.168.173.145/13277;icmp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 1,
Bytes: 84,

Session ID: 30064811187, Policy name: 01_MYAPP-to-LBO/7, State: Stand-alone, Timeout: 2, Valid
  In: 10.99.99.99/4 --> 104.96.100.195/41;icmp, Conn Tag: 0x0, If: irb.1099, Pkts: 1, Bytes: 84,
  Out: 104.96.100.195/41 --> 192.168.173.145/24826;icmp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 1,
Bytes: 84,

Session ID: 30064811188, Policy name: 01_MYAPP-to-LBO/7, State: Stand-alone, Timeout: 2, Valid
  In: 10.99.99.99/4 --> 104.96.100.195/42;icmp, Conn Tag: 0x0, If: irb.1099, Pkts: 1, Bytes: 84,
  Out: 104.96.100.195/42 --> 192.168.173.145/29370;icmp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 1,
Bytes: 84,
Total sessions: 3

show security policies policy-name 01_MYAPP-to-LBO detail
Policy: 01_MYAPP-to-LBO, action-type: permit, services-offload:not-configured , State:
enabled, Index: 7, Scope Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: SPOKE-LAN1, To zone: INET
  Source vrf group:
    any
  Destination vrf group:
    any
  Source addresses:
    10-99-99-0_24(global): 10.99.99.0/24
  Destination addresses:
    www.juniper.net(global): 104.96.100.195/32
  Application: any
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination ports: [0-0]
  Dynamic Application:
    any: 0
  Source identity feeds:
    any
  Destination identity feeds:
    any
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
```

## Isolated Guest VLAN

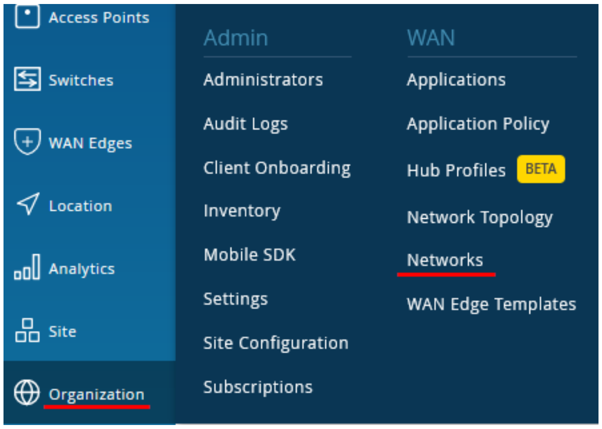

Basic initial Traffic model with Guest VLAN LBO extension

In this example we want to create a second VLAN/Interface on every Spoke for local guests that require simple internet access. They should NOT be able to send Traffic to the corporate VPN. Basically, everything that is coming from this VLAN/Interface shall be broken out locally and sent to the cheapest interface of the WAN interfaces (in our case we will NOT use the MPLS interface) to provide them with a baseline internet connection.

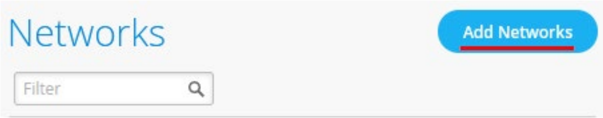
We'll implement the following Topology and will test it using the first Spoke.



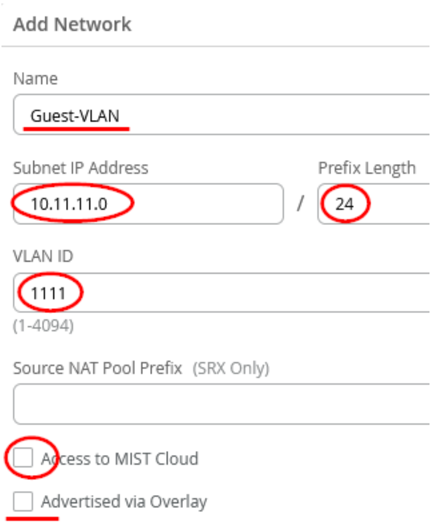
- First, we go to Organization -> Networks



- Add a new network here to the existing ones.



- Configure the new Network in the following way:
  - Name: "Guest-VLAN"
  - Subnet IP Address: "10.11.11.0"
  - Prefix Length: "24"
  - VLAN ID: "1111"
  - Uncheck Access to Mist Cloud
  - Make sure it is NOT advertised via Overlay as this Network should not be routed in the Corporate VPN.



Add Network

Name

Guest-VLAN

Subnet IP Address / Prefix Length

10.11.11.0 / 24

VLAN ID

1111

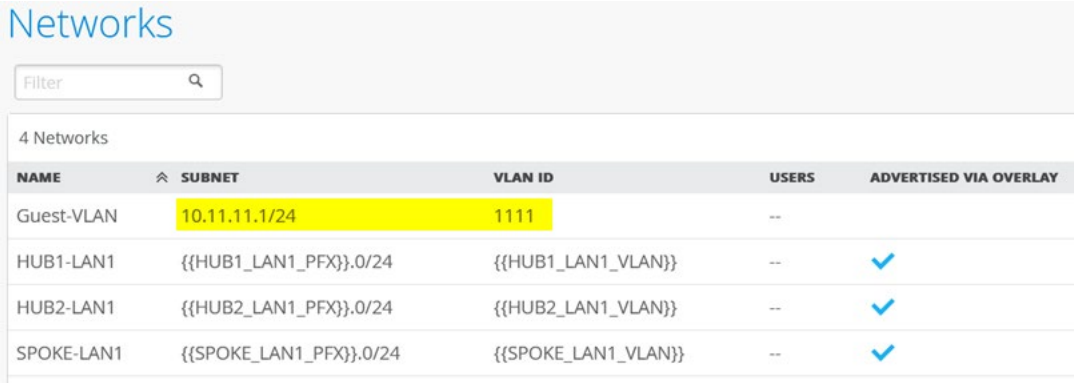
(1-4094)

Source NAT Pool Prefix (SRX Only)

□ Access to MIST Cloud

□ Advertised via Overlay

- After all is configured check your changes.



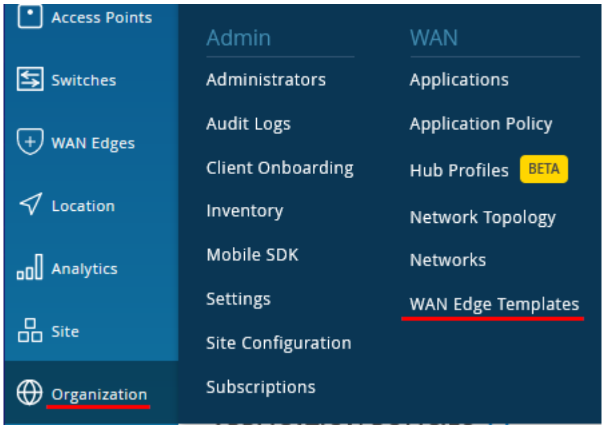
Networks

Filter

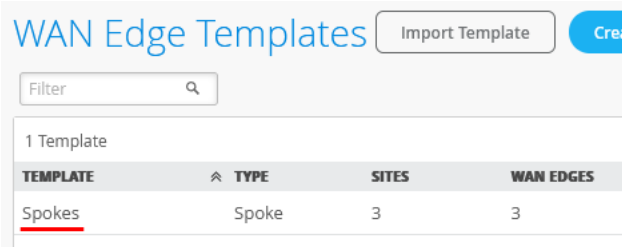
4 Networks

| NAME | SUBNET | VLAN ID | USERS | ADVERTISED VIA OVERLAY |
|---|---|---|---|---|
| Guest-VLAN | 10.11.11.1/24 | 1111 | -- | |
| HUB1-LAN1 | {{HUB1_LAN1_PFX}}.0/24 | {{HUB1_LAN1_VLAN}} | -- | ✓ |
| HUB2-LAN1 | {{HUB2_LAN1_PFX}}.0/24 | {{HUB2_LAN1_VLAN}} | -- | ✓ |
| SPOKE-LAN1 | {{SPOKE_LAN1_PFX}}.0/24 | {{SPOKE_LAN1_VLAN}} | -- | ✓ |

- Now, go to Organization -> WAN Edge Templates



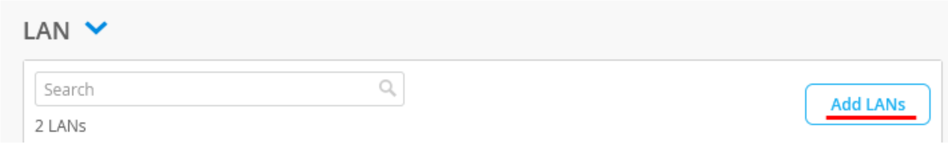
- We are adding this to an existing Template so, select the existing “Spokes” Template



1 Template

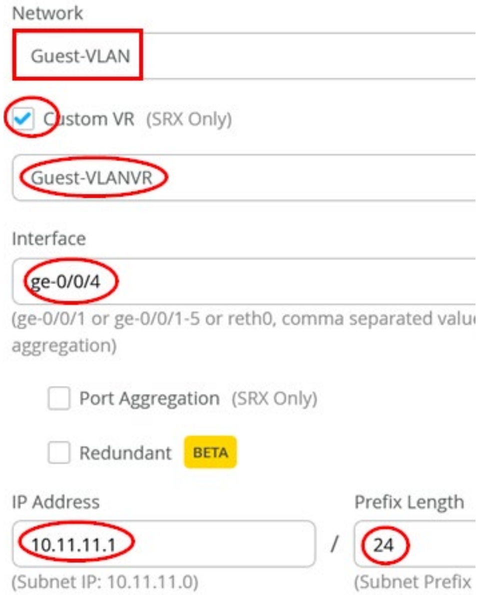
| TEMPLATE | TYPE | SITES | WAN EDGES |
|---|---|---|---|
| Spokes | Spoke | 3 | 3 |

- Add a new LAN-Interface



2 LANs

- Configure the new Lan in the following way:
  - Select as Network: “Guest-VLAN”
  - Check Custom VR and create as VR called: “Guest-VLANVR”
  - Interface: “ge-0/0/4”
  - IP Address: “10.11.11.1”
  - Prefix Length: “24”



Network

Guest-VLAN

☑ Custom VR (SRX Only)

Guest-VLANVR

Interface

ge-0/0/4

(ge-0/0/1 or ge-0/0/1-5 or reth0, comma separated valu aggregation)

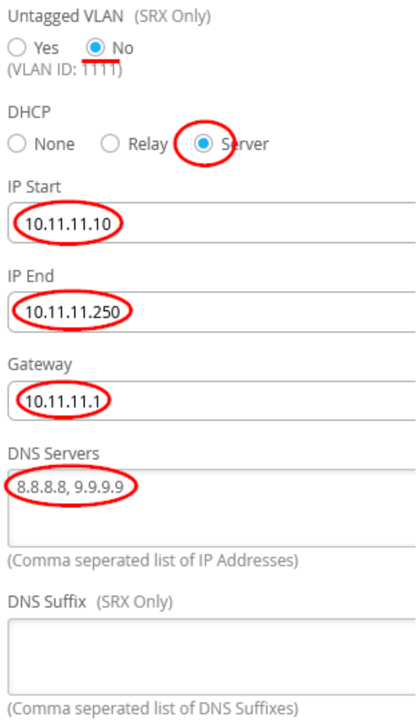
□ Port Aggregation (SRX Only)

□ Redundant BETA

IP Address: 10.11.11.1 / Prefix Length: 24

(Subnet IP: 10.11.11.0) (Subnet Prefix

- Handout DHCP-Leases to your Guests. Continue with the following LAN configuration:
  - Select DHCP Server
  - IP Start: “10.11.11.10”
  - IP End: “10.11.11.250”
  - Gateway: “10.11.11.1”
  - DNS Servers: “8.8.8.8, 9.9.9.9”



Untagged VLAN (SRX Only)

○ Yes ● No

(VLAN ID: 1111)

DHCP

○ None ○ Relay ● Server

IP Start

10.11.11.10

IP End

10.11.11.250

Gateway

10.11.11.1

DNS Servers

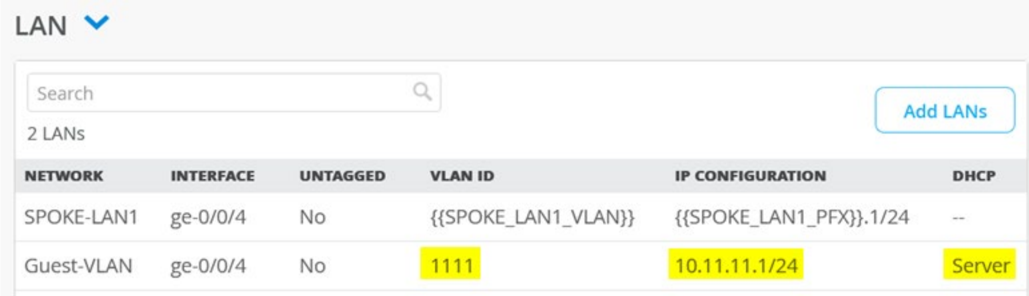
8.8.8.8, 9.9.9.9

(Comma seperated list of IP Addresses)

DNS Suffix (SRX Only)

(Comma seperated list of DNS Suffixes)

- Your resulting changes should look like this in the overview.

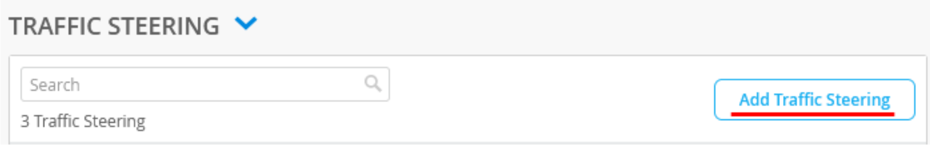


LAN

2 LANs

| NETWORK | INTERFACE | UNTAGGED | VLAN ID | IP CONFIGURATION | DHCP |
|---|---|---|---|---|---|
| SPOKE-LAN1 | ge-0/0/4 | No | {{SPOKE_LAN1_VLAN}} | {{SPOKE_LAN1_PFX}}.1/24 | -- |
| Guest-VLAN | ge-0/0/4 | No | 1111 | 10.11.11.1/24 | Server |

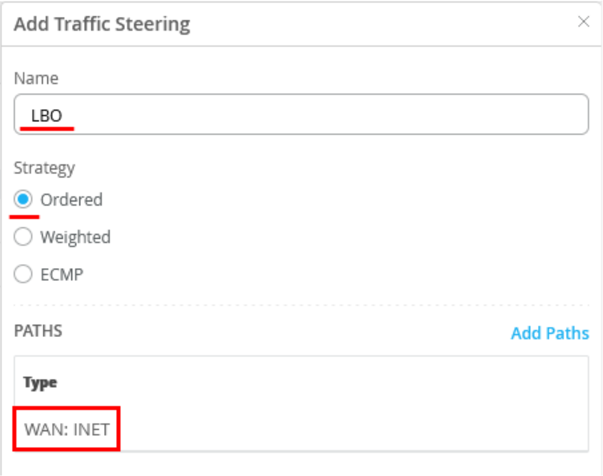
- Now add a new Traffic Steering element.



TRAFFIC STEERING

3 Traffic Steering

- Add the following new Steering configuration:
  - Name: ”LBO”
  - Strategy: “Ordered”
  - Path: “WAN: INET” remember we like to avoid the costs of using the MPLS link for this service.



Add Traffic Steering ×

Name

LBO

Strategy

● Ordered

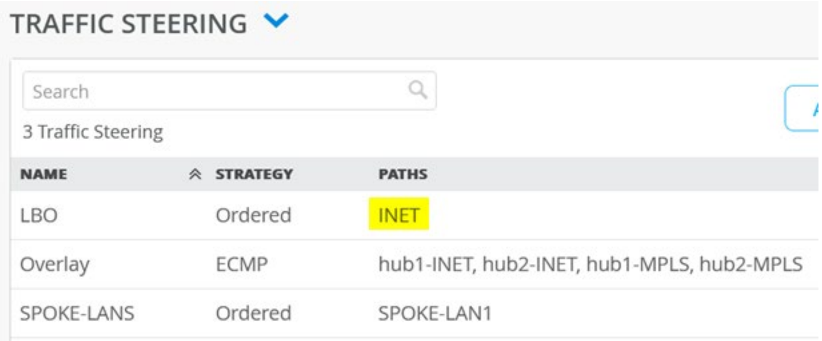
○ Weighted

○ ECMP

PATHS

| Type |
|---|
| WAN: INET |

- Your resulting changes should look like this in the overview.



TRAFFIC STEERING

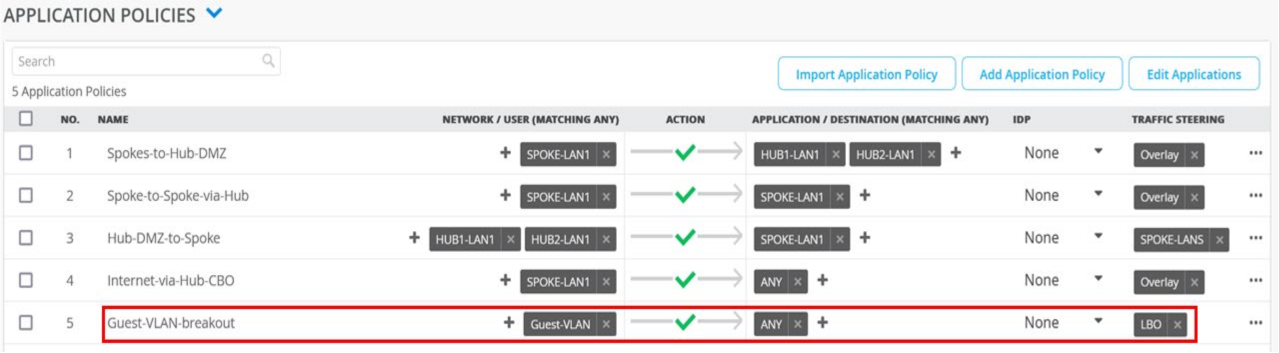
3 Traffic Steering

| NAME | STRATEGY | PATHS |
|---|---|---|
| LBO | Ordered | INET |
| Overlay | ECMP | hub1-INET, hub2-INET, hub1-MPLS, hub2-MPLS |
| SPOKE-LANS | Ordered | SPOKE-LAN1 |

- Now we will add a new Application Policy in the following way.

| No. | Rule Name | Network | Action | Destination | Steering |
|---|---|---|---|---|---|
| 5 | Guest-VLAN-breakout | Guest-VLAN | Pass | ANY | LBO |

- Your resulting changes should look like this in the overview.

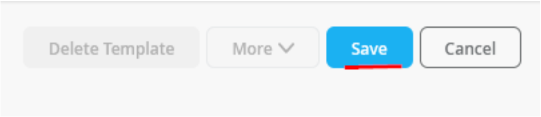


APPLICATION POLICIES

5 Application Policies

| ☐ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| ☐ | 1 | Spokes-to-Hub-DMZ | SPOKE-LAN1 | ✓ | HUB1-LAN1, HUB2-LAN1 | None | Overlay |
| ☐ | 2 | Spoke-to-Spoke-via-Hub | SPOKE-LAN1 | ✓ | SPOKE-LAN1 | None | Overlay |
| ☐ | 3 | Hub-DMZ-to-Spoke | HUB1-LAN1, HUB2-LAN1 | ✓ | SPOKE-LAN1 | None | SPOKE-LANS |
| ☐ | 4 | Internet-via-Hub-CBO | SPOKE-LAN1 | ✓ | ANY | None | Overlay |
| ☐ | 5 | Guest-VLAN-breakout | Guest-VLAN | ✓ | ANY | None | LBO |

- Don’t forget to “Save” your changes so that they are applied.

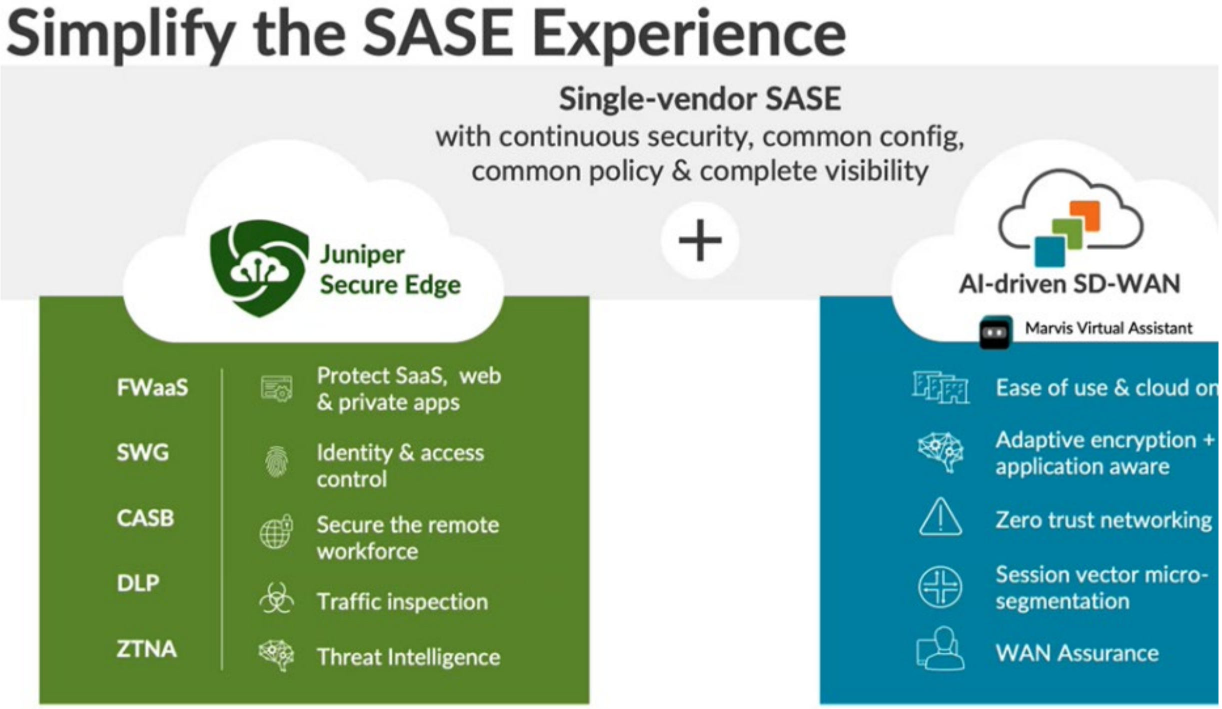


## Secure Edge Connector for SRX Series Firewalls

Juniper® Secure Edge provides full-stack security service edge (SSE) capabilities to protect access to web, SaaS, and on-premises applications. These capabilities also provide consistent threat protection, an optimized network experience, and security policies that follow users wherever they go. Secure Edge acts as an advanced cloud-based security scanner. It enables organizations to protect data and provide users with consistent, secure network access whether users are in the office, on campus, or on the move.

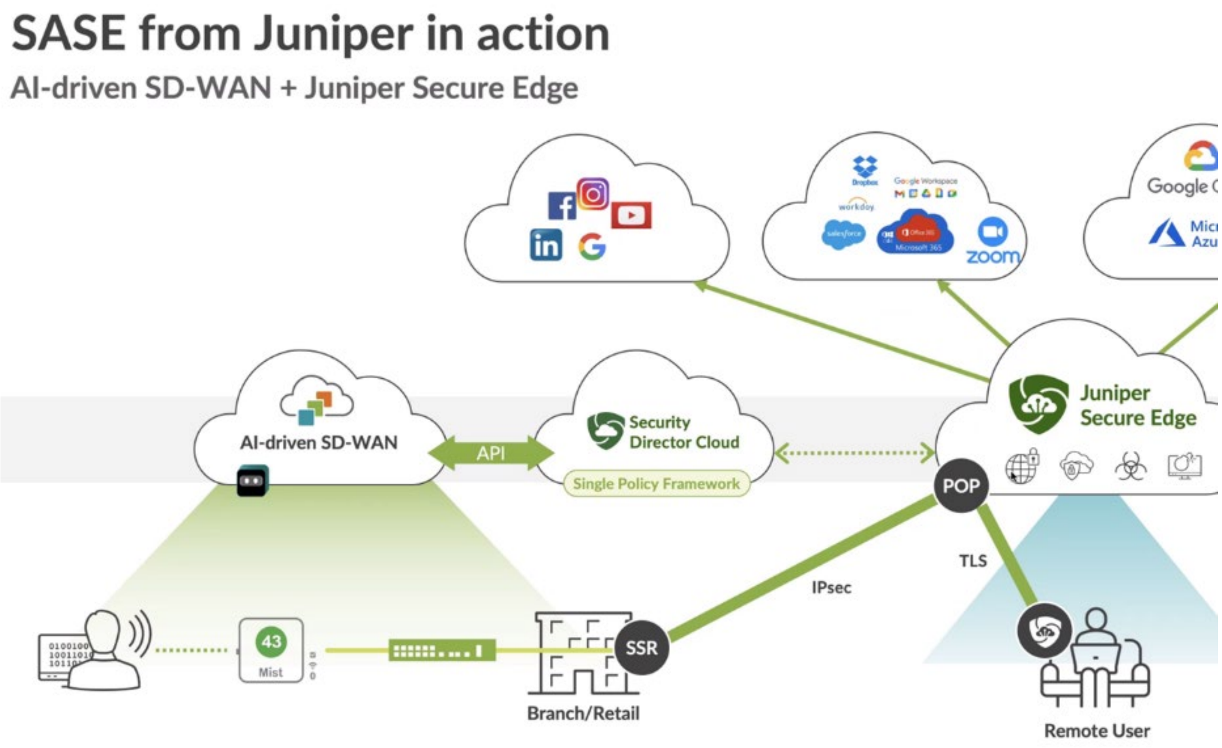
Mist works with Juniper Secure Edge by providing a Secure Edge Connector (SEC) that can establish a secure tunnel with the Juniper Secure Edge cloud service.

Figure127: Secure Edge


Simplify the SASE Experience
Single-vendor SASE
with continuous security, common config,
common policy & complete visibility
Juniper
Secure Edge
AI-driven SD-WAN
Marvis Virtual Assistant
FWaaS
SWG
CASB
DLP
ZTNA
Protect SaaS, web & private apps
Identity & access control
Secure the remote workforce
Traffic inspection
Threat Intelligence
Ease of use & cloud on
Adaptive encryption + application aware
Zero trust networking
Session vector micro-segmentation
WAN Assurance

Secure Edge capabilities are all managed by Juniper Security Director Cloud, Juniper's simple and seamless management experience delivered in a single user interface (UI).

Figure128: Traffic Inspection by Juniper Secure Edge



For more information, see Juniper Secure Edge.

Secure Edge Connector Overview

The Juniper Mist cloud works with Juniper® Secure Edge to perform traffic inspection from edge devices by using the Secure Edge connector feature. This feature allows the Juniper Networks® SRX Series Firewall, deployed as WAN edge device, to send a portion of traffic to Juniper Secure Edge for an inspection.

In this task, you send the Internet-bound traffic from the LAN side of a spoke or hub device to Secure Edge for an inspection before the traffic reaches Internet.

To perform traffic inspection by Secure Edge:

- In Security Director Cloud, create and configure the service locations, IPsec profiles, sites, and policies for Secure Edge. These are the cloud-based resources that provide security services and connectivity for the WAN edge devices.
- In Mist Cloud, create and configure the WAN edge devices, such as SRX Series Firewall that connect to the LAN networks. These are the devices that provide routing, switching, and SD-WAN capabilities for the branches or campuses.
- In Mist WAN edge, create and configure the Secure Edge tunnels that connect the WAN edge devices to the service locations. These are the IPsec tunnels that provide secure and reliable transport for the traffic that needs to be inspected by Secure Edge.
- In Mist Cloud, assign the Secure Edge tunnels to the sites or device profiles that correspond to the WAN edge devices. This enables the traffic steering from the LAN networks to the Secure Edge cloud based on the defined data policies and other match criteria.

Before You Begin

- Read about the Juniper® Secure Edge subscription requirements. See Juniper Secure Edge Subscriptions Overview.
- Ensure that you have completed the prerequisites to access the Juniper Security Director Cloud portal. See Prerequisites.
- Created Create Your Secure Edge Tenant. See Create Your Secure Edge Tenant.
- Be assumed that, in the Mist cloud, you have adopted and configured the WAN edge devices, such as SRX Series Firewall that connects to the LAN networks.

## Access Juniper Security Director Cloud and Check Active Subscriptions

A tenant in Juniper Secure Edge is an organization account that you create to access the Juniper Security Director Cloud portal and manage your Secure Edge services. A tenant is associated with a unique e-mail address and a subscription plan. A tenant can have multiple service locations, which are vSRX based WAN edge hosted in a public cloud for your organization.

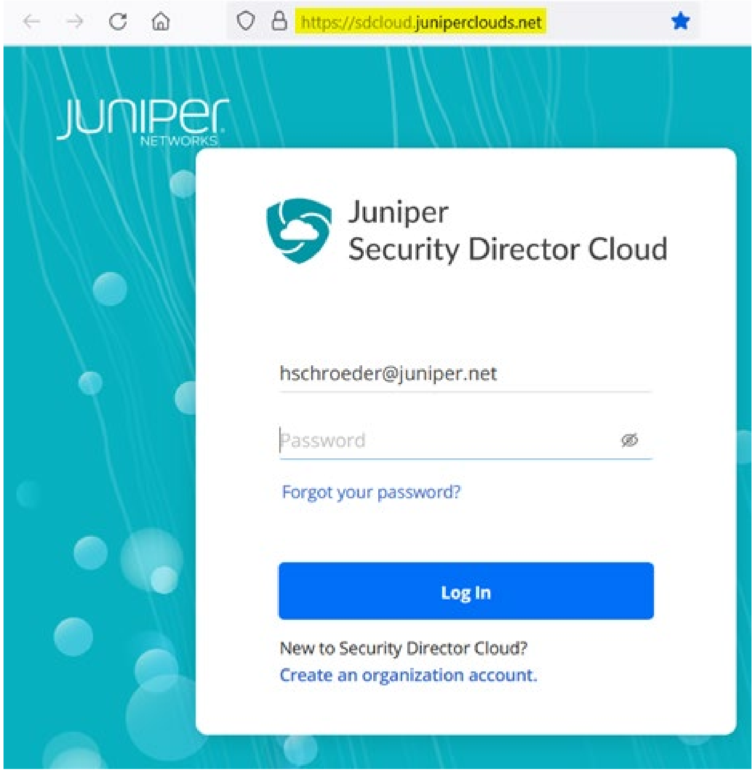
A tenant can have one or more service locations, which are the connection points for end users. To create a tenant, you need to have an account on Juniper Security Director Cloud. See Create Your Secure Edge Tenant for details.

After you create your Secure Edge tenant in the Juniper Security Director Cloud portal, access the portal and check your subscriptions.

To access Juniper Security Director Cloud and check active subscriptions:

- Open the URL to the Juniper Security Director Cloud. Enter your e-mail address and password to log in and start using the Juniper Security Director Cloud portal.

Figure129: Access Juniper Security Director Cloud



https://sdcloud.juniperclouds.net

Juniper
Security Director Cloud

hschroeder@juniper.net

Password

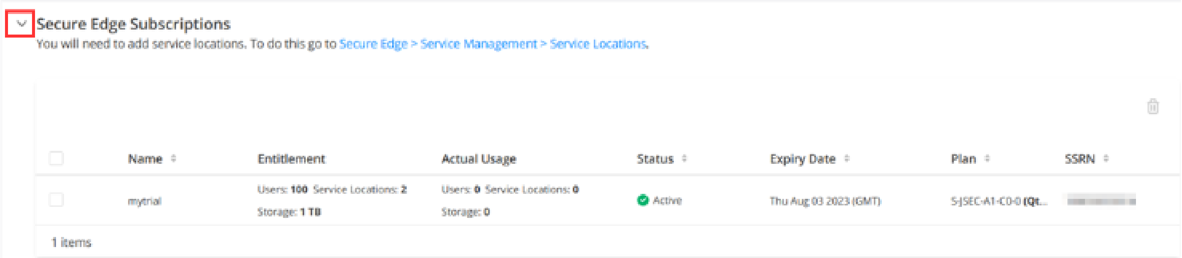
Forgot your password?

Log In

New to Security Director Cloud?
Create an organization account.

- Select the required tenant in the upper right corner of the portal to continue.
- Select **Administration** > **Subscriptions** to access the Juniper Security Director Cloud subscriptions page.

Figure130: Secure Edge Subscriptions



Secure Edge Subscriptions

You will need to add service locations. To do this go to Secure Edge > Service Management > Service Locations.

| □ | Name | Entitlement | Actual Usage | Status | Expiry Date | Plan | SSRN |
|---|---|---|---|---|---|---|---|
| □ | mytrial | Users: **100** Service Locations: **2**<br>Storage: **1 TB** | Users: **0** Service Locations: **0**<br>Storage: **0** | Active | Thu Aug 03 2023 (GMT) | S-JSEC-A1-C0-0 (Qt... | [redacted] |

1 items

- Scroll to the **Secure Edge Subscriptions** section to check whether you have an active subscription. For details, see About the Subscriptions Page. Assuming that you have active subscriptions, continue with next steps.

## Generate Device Certificates in Juniper Security Director Cloud

Now that you have configured service locations in Juniper Security Director Cloud, you generate device certificates to secure network traffic.

You use a Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificate to establish secure communications between Secure Edge and WAN edge devices. All the client browsers on your network must trust the certificates signed by the Juniper Networks and SRX Series Firewalls to use an SSL proxy.

In Juniper Security Director Cloud, you have the following choices for generating certificates:

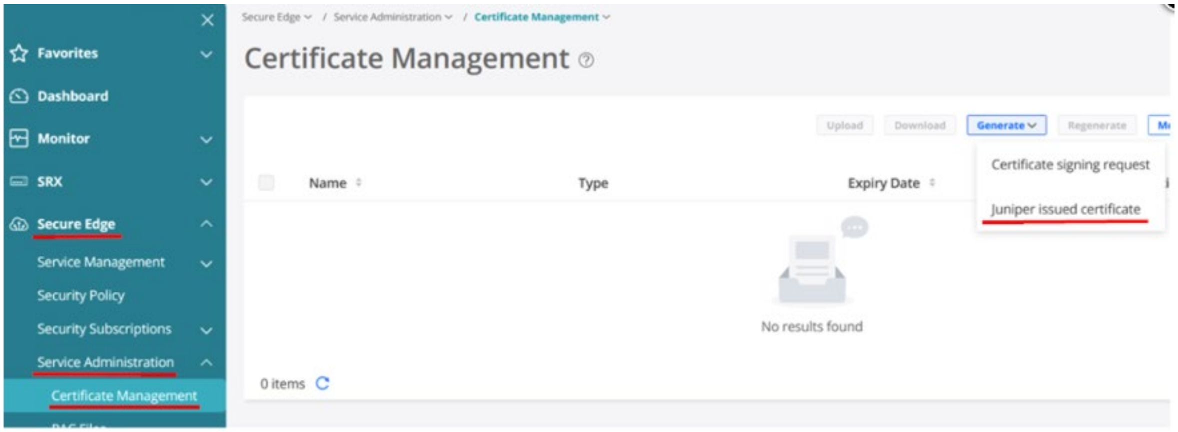
- Create a new certificate signing request (CSR), and your own certificate authority (CA) can use the CSR to generate a new certificate.
- Select the option to have Juniper Networks create a new certificate.

**Note**: This topic describes how to generate a TLS/SSL certificate. How you import and use the certificate depends on your company's client-management requirements and is beyond the scope of this topic.

To generate device certificates in Juniper Security Director Cloud:

- Select **Secure Edge > Service Management > Service Administration > Certificate Management**.
- The Certificate Management page appears.
  - From the Generate list, you can generate either a new Certificate signing request (CSR), or a Juniper issued certificate.

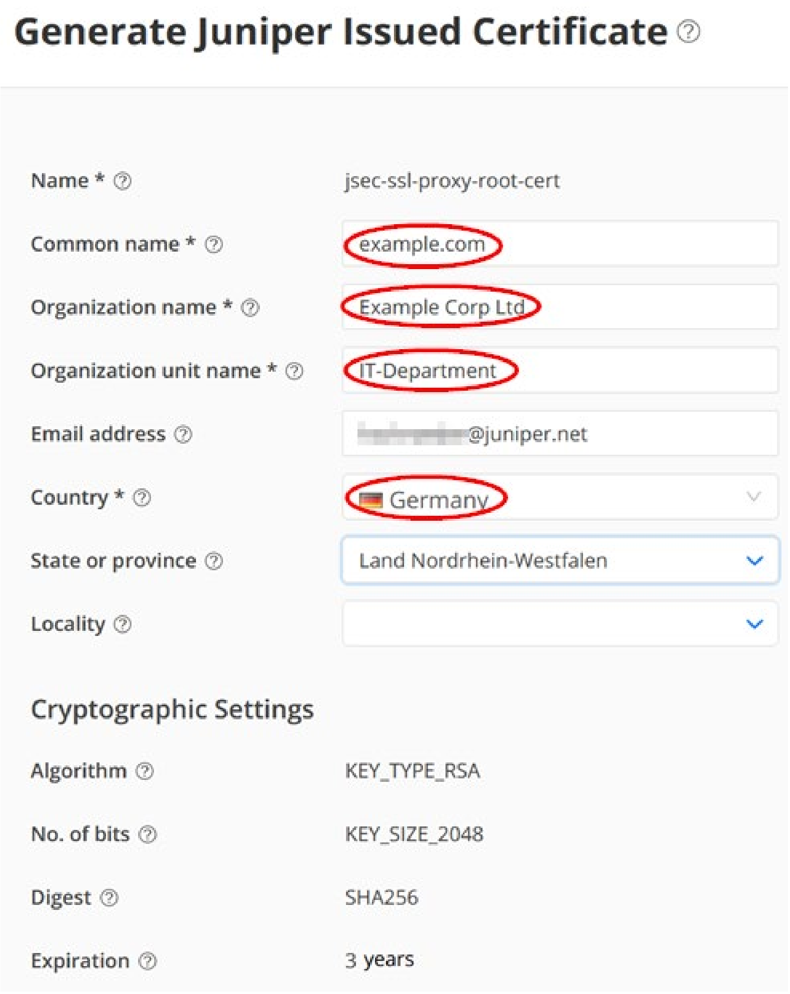
Figure131: Certificate Management



- Select the relevant option:
  - If your company has its own CA and you want to generate a CSR, click **Certificate signing request**.

    After Juniper Secure Edge generates CSR, download the CSR and submit it to your CA to generate a new certificate. Once generated, click Upload to upload the certificate on the Certificate Management page.
  - If your company does not have its own CA, click **Juniper issued certificate**, and then click **Generate** to generate the certificate. Juniper Networks will generate and keep the certificate on the system. In this task, select **Juniper issued certificate** and continue with next step.
- Enter the certificate details. In the **Common name** field, use the certificate's fully qualified domain name (FQDN).

Figure132: Generate a Juniper-Issued Certificate



## Generate Juniper Issued Certificate

| | |
|---|---|
| Name * | jsec-ssl-proxy-root-cert |
| Common name * | example.com |
| Organization name * | Example Corp Ltd |
| Organization unit name * | IT-Department |
| Email address | [redacted]@juniper.net |
| Country * | Germany |
| State or province | Land Nordrhein-Westfalen |
| Locality | |

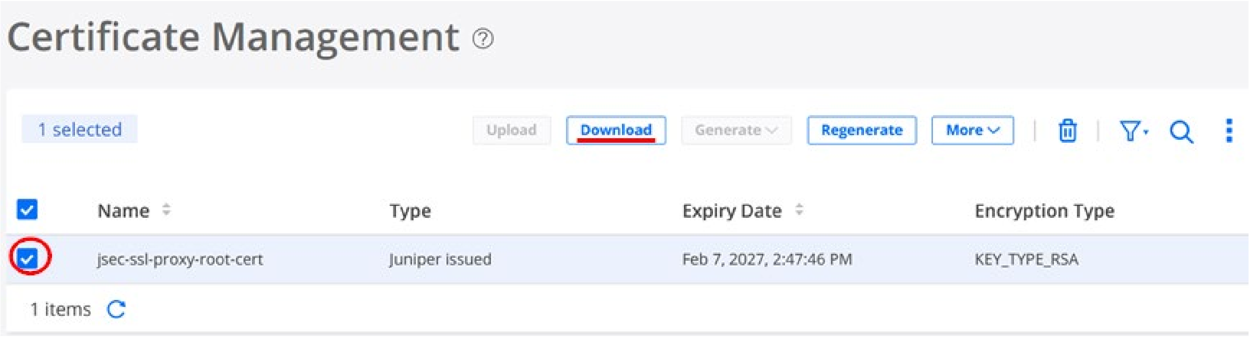
### Cryptographic Settings

| | |
|---|---|
| Algorithm | KEY_TYPE_RSA |
| No. of bits | KEY_SIZE_2048 |
| Digest | SHA256 |
| Expiration | 3 years |

The Certificate Management page opens with a message indicating that the certificate is created successfully.

- Download the generated certificate.

Figure133: Download the Certificate



## Certificate Management

| ☑ | Name | Type | Expiry Date | Encryption Type |
|---|---|---|---|---|
| ☑ | jsec-ssl-proxy-root-cert | Juniper issued | Feb 7, 2027, 2:47:46 PM | KEY_TYPE_RSA |

1 items

The following sample shows the downloaded certificate:

```
-----BEGIN CERTIFICATE-----
MIIG4jCCBMqgAwIBAgIIX3yPMZ7QT9MwDQYJKoZIhvcNAQEMBQAwgYgxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJDQTESMBAGA1UEBxMJU3Vubnl2YWxlMR4wHAYDVQQK
.
.
JwePvBrmKGPph8k+8gL9Gqw+wnfaARP3fqp4TXUcp6twDMyP0OJR8tRm51keplVw
RAfTzy91Bhf261E62+MzKeh8J0Wi8q8Amaw6+aNVj8TcA9T/zotCI5JSkqV6+Wap
btLaf5DXSYliXWnDgt72sURF3bmUYjfDTmPgwzeMi/dal4IWUqk=
-----END CERTIFICATE-----
```

After you download the certificate to your system, add the certificate to client browsers.

## Configure a Service Location in Juniper Security Director Cloud

After ensuring that you have an active license to Juniper Security Director Cloud, you configure a service location. This is your first main task in setting up a Secure Edge connector for SRX Series Firewalls.

A service location in Juniper Security Director Cloud is also known as POP (point of presence) and represents a Juniper® Secure Edge instance in a cloud location. The service location is the connection (access) point for both on-premises and roaming users.

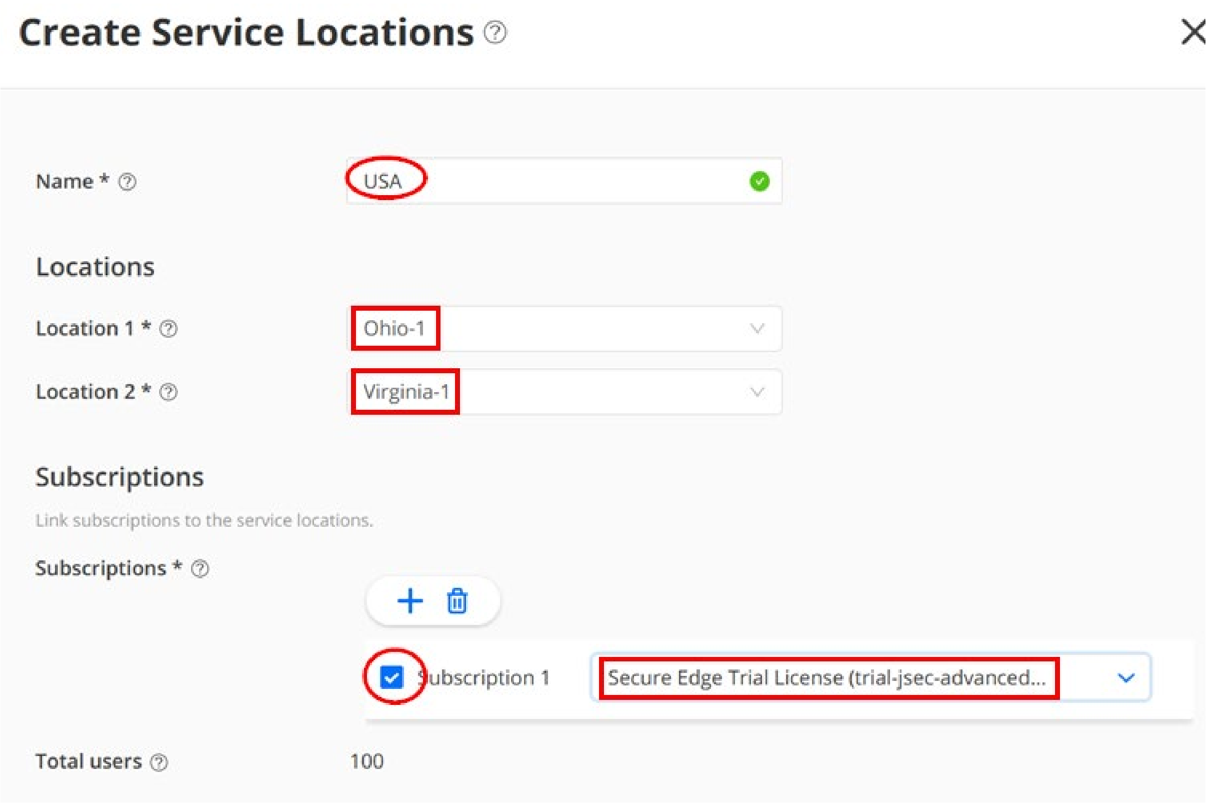
Service locations are places where vSRX creates secure connections between different networks using a public cloud service. The public IP address (unique per tenant and service location) is used to:

- Set up an IPsec tunnel between the branch device and the Juniper Security Director Cloud.
- Centrally distribute the traffic when the destination is on the Internet.

To configure a service location in Juniper Security Director Cloud:

- In Juniper Security Director Cloud menu, select **Secure Edge** > **Service Management** > **Service Locations**.
- The Service Locations page appears. Click the Add (**+**) icon to create a new service location. Enter the details for the following fields:
  - **Name**—Give a name like “USA” below.
  - **Location 1**—Select the location for the Secure Edge in the region.
  - **Location 2**—Select the location for the Secure Edge in the region. Ensure that it is not another instance in the same region as Location 1. You usually want a backup in case the entire region fails.
  - **Subscriptions**—Select at least one Subscription which has a minimum of 100 Users.

The Figure below shows examples of service locations.



**Create Service Locations**

Name * USA

Locations

Location 1 * Ohio-1

Location 2 * Virginia-1

Subscriptions

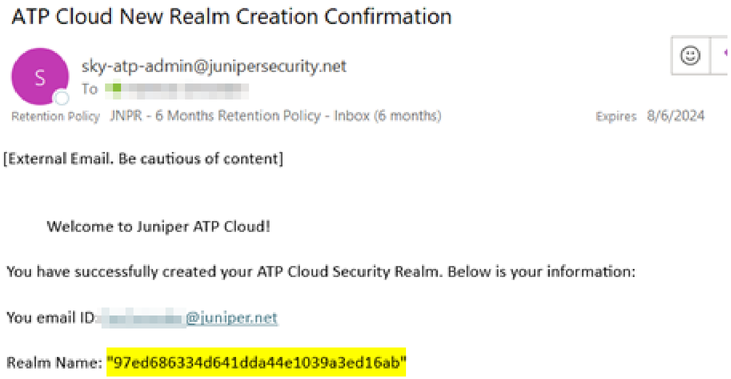
Link subscriptions to the service locations.

Subscriptions *

☑ Subscription 1 Secure Edge Trial License (trial-jsec-advanced...

Total users 100

- Click **OK**. Security Director Cloud creates a new service location and lists it on the Service Locations page.
- You will receive an Email confirming your action like the example below.



ATP Cloud New Realm Creation Confirmation

sky-atp-admin@junipersecurity.net

To [redacted]

Retention Policy JNPR - 6 Months Retention Policy - Inbox (6 months) Expires 8/6/2024

[External Email. Be cautious of content]

Welcome to Juniper ATP Cloud!

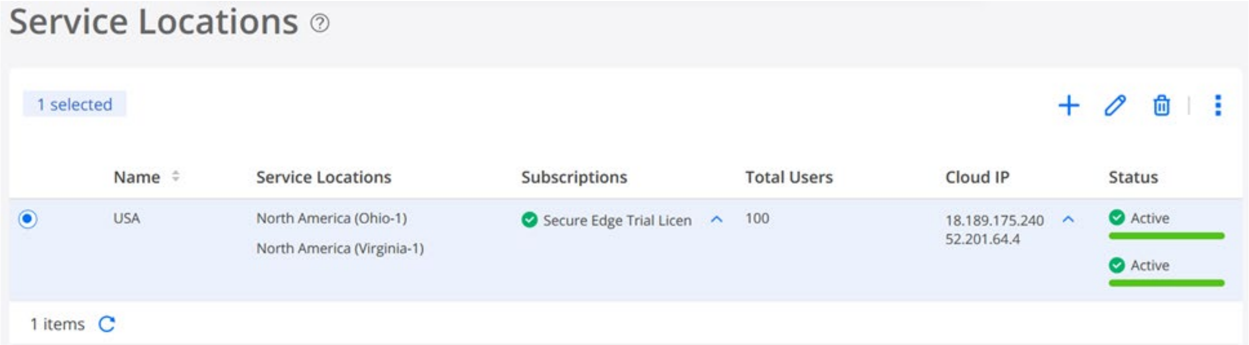
You have successfully created your ATP Cloud Security Realm. Below is your information:

You email ID:[redacted]@juniper.net

Realm Name: "97ed686334d641dda44e1039a3ed16ab"

The status of the service location shows **In Progress** until the Secure Edge instance is fully deployed, as shown in the Figure below.

Figure134: Service Location Status



Service Locations

1 selected

| | Name | Service Locations | Subscriptions | Total Users | Cloud IP | Status |
|---|---|---|---|---|---|---|
| ● | USA | North America (Ohio-1)<br>North America (Virginia-1) | ✓ Secure Edge Trial Licen | 100 | 18.189.175.240<br>52.201.64.4 | ✓ Active<br>✓ Active |

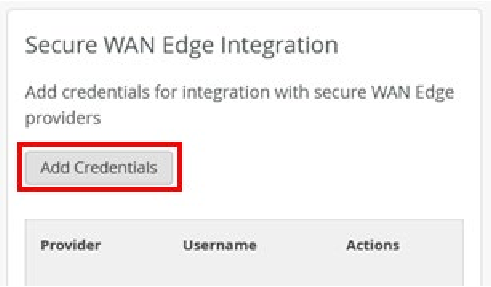
1 items

When you create a new service location, the system starts the deployment of two vSRX instances as WAN edges for your tenant system. In this deployment, vSRX instances are not shared with other tenants.

It is suggested that you review the Security Policies [https://sdcloud.juniperclouds.net/secure-edge/secure-edge-policy](https://sdcloud.juniperclouds.net/secure-edge/secure-edge-policy) of your Tenant. You may need to make changes to allow/deny certain Traffic forward to the Internet. For example, for simple debugging, we recommend allowing ICMP-Ping to be allowed towards Internet so that we can easy measure reachability and Path-Latency from a Client connected at the Branch to the destination Internet service he wants to reach via Secure Edge re-direction to the Juniper Security Director Cloud environment. An example of such configuration is given here.

Add Juniper Security Director Cloud Account Credentials to the Mist Cloud Organization

- Go to Organization > Settings
- Click on **Add Credentials**

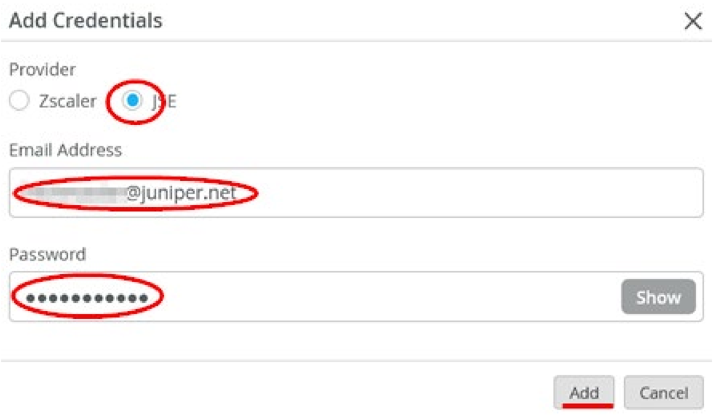


Secure WAN Edge Integration

Add credentials for integration with secure WAN Edge providers

| Provider | Username | Actions |
|---|---|---|

- Fill in your Credentials
  - Set Provider: “JSE”
  - Add your own Email Address on the Juniper Security Director Cloud instance
  - Add your own Password on the Juniper Security Director Cloud instance



Add Credentials

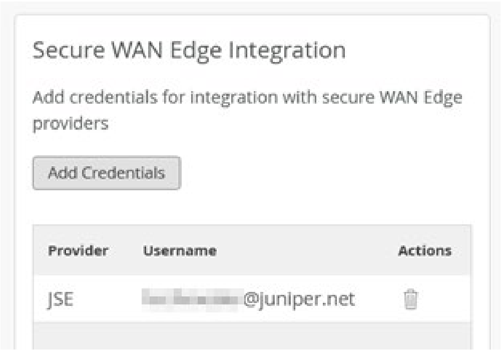
Provider

○ Zscaler [✓ ● JSE]

Email Address: [redacted]@juniper.net

Password: ●●●●●●●●●●●

The result of your adds should now look similar to the below Figure.



Secure WAN Edge Integration

Add credentials for integration with secure WAN Edge providers

| Provider | Username | Actions |
|---|---|---|
| JSE | [redacted]@juniper.net | 🗑 |

Create Secure Edge Connectors in the Juniper Mist Cloud Portal

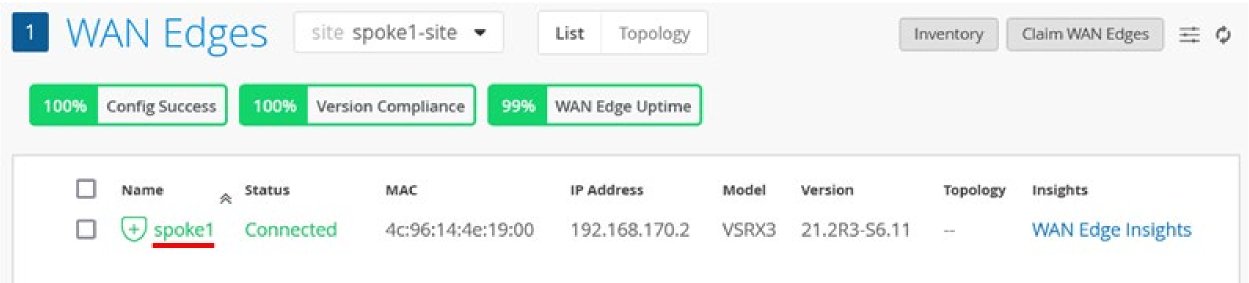
You create Secure Edge connectors in the Juniper Mist cloud portal. This task completes the configuration on the Mist cloud side of the tunnels to establish an IPsec tunnel between WAN edge devices managed by Mist and Security Director Cloud. Before you create the connectors, ensure that your site has a deployed SRX Series Firewall.

To create Secure Edge connectors:

- In the Juniper Mist cloud portal, click **WAN Edges**.

  The WAN Edges page displays site details.

Figure135: Configure WAN Edge



1 WAN Edges

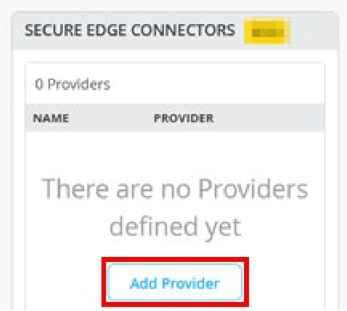
site spoke1-site

100% Config Success | 100% Version Compliance | 99% WAN Edge Uptime

| □ | Name | Status | MAC | IP Address | Model | Version | Topology | Insights |
|---|---|---|---|---|---|---|---|---|
| □ | spoke1 | Connected | 4c:96:14:4e:19:00 | 192.168.170.2 | VSRX3 | 21.2R3-S6.11 | -- | WAN Edge Insights |

- Select a site with a deployed branch device.
- In the **Secure Edge Connectors** pane, click **Add Provider**.

Figure136: Secure Edge Connector Configuration



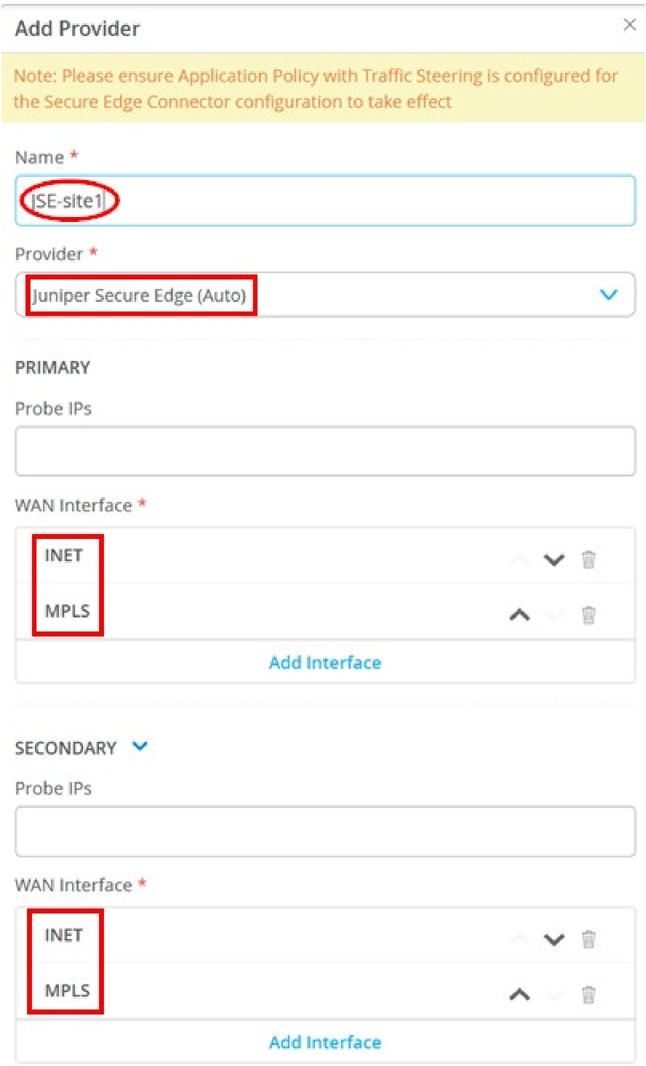
SECURE EDGE CONNECTORS [redacted]

0 Providers

| NAME | PROVIDER |
|---|---|

There are no Providers defined yet

- Enter Secure Edge connector details according to the Figure below. We just need to select the automatic JSE Provide and add the WAN-Interfaces that shall be used towards the two Service Locations. It’s very similar to the definition of two hubs we use for regular VPN-Connections.



Add Provider

Note: Please ensure Application Policy with Traffic Steering is configured for the Secure Edge Connector configuration to take effect

Name *: JSE-site1

Provider *: Juniper Secure Edge (Auto)

PRIMARY

Probe IPs:

WAN Interface *: INET, MPLS

SECONDARY

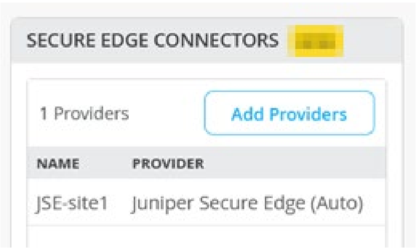
Probe IPs:

WAN Interface *: INET, MPLS

Note: You don't need to enter the probe IP values. IPsec tunnels do not need additional monitoring like GRE needs.

- Verify that the Mist cloud portal has added the Secure Edge connector you just configured.

Figure137: Secure Edge Connector Added

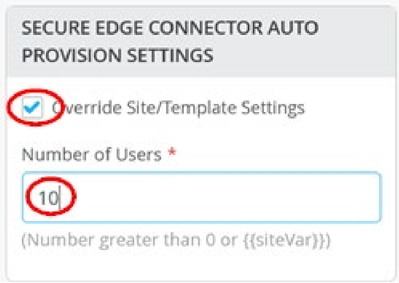


SECURE EDGE CONNECTORS [redacted]

1 Providers

| NAME | PROVIDER |
|---|---|
| JSE-site1 | Juniper Secure Edge (Auto) |

- Next add a few User sessions to your Secure Edge Connector



SECURE EDGE CONNECTOR AUTO PROVISION SETTINGS

☑ Override Site/Template Settings

Number of Users *

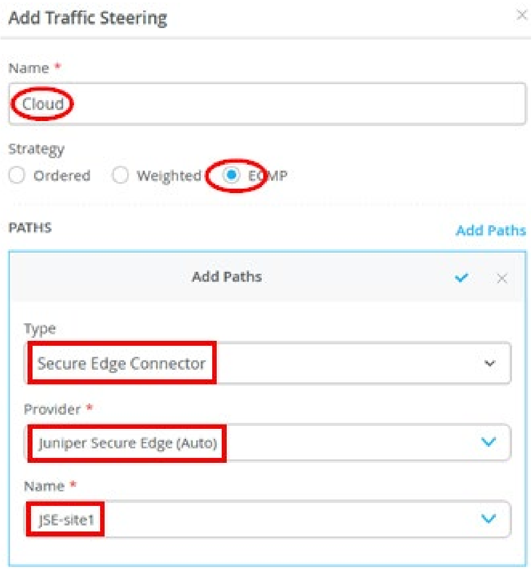
10

(Number greater than 0 or {{siteVar}})

- Add the traffic steering paths.

  Add a new traffic steering path on the WAN edge template or WAN edge device, according to the values provided in below Figure and Table.

Figure138: Add Traffic Steering Options for Secure Edge



Add Traffic Steering

Name *

Cloud

Strategy

○ Ordered ○ Weighted ● ECMP

PATHS

Add Paths ✓ ×

Type

Secure Edge Connector

Provider *

Juniper Secure Edge (Auto)

Name *

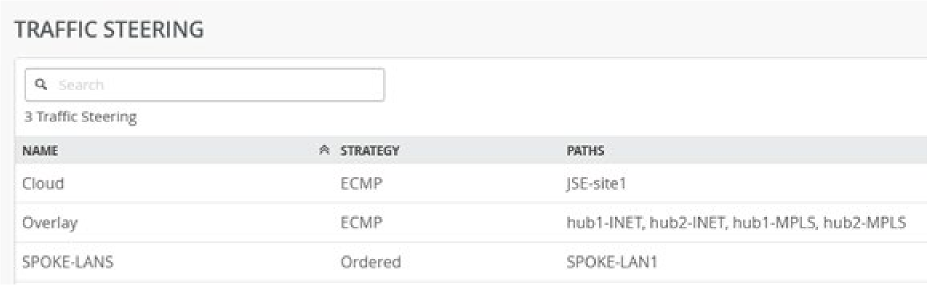
JSE-site1

Table 28: Traffic Steering Path Configuration

| Fields | Value |
|---|---|
| Name | Cloud |
| Strategy | ECMP |
| Paths | Select Type and Destination |
| Type | Secure Edge Connector |
| Provider | Juniper Secure Edge (Auto) |
| Name | JSE-site1 |

- Below Figure displays the configured traffic steering paths.

Figure139: Traffic Steering Paths



TRAFFIC STEERING

Search

3 Traffic Steering

| NAME | STRATEGY | PATHS |
|---|---|---|
| Cloud | ECMP | JSE-site1 |
| Overlay | ECMP | hub1-INET, hub2-INET, hub1-MPLS, hub2-MPLS |
| SPOKE-LANS | Ordered | SPOKE-LAN1 |

Modify an Application Policy

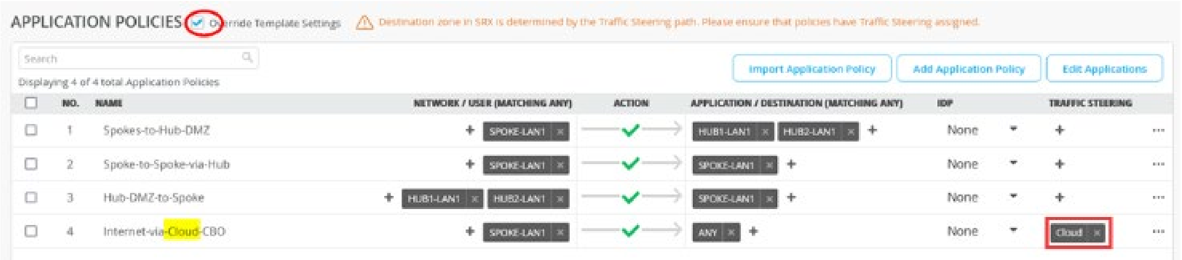
After you create Secure Edge connectors in the Juniper Mist cloud portal, next step is to modify application policies on the branch device. For example, you can allow traffic from a spoke device to a hub device. You can also allow traffic from a spoke device to another spoke device in the VPN tunnel. After that, you can send traffic from spokes to the Internet through Juniper Security Director Cloud instead of sending traffic from spokes to a hub for central breakout.

To modify an application policy:

- In the Juniper Mist cloud portal, select **Organization** > **WAN** > **Application Policy**.

  The Application Policies page opens.

Figure140: Change Application Policies



APPLICATION POLICIES ☑ Override Template Settings ⚠ Destination zone in SRX is determined by the Traffic Steering path. Please ensure that policies have Traffic Steering assigned.

Search

Displaying 4 of 4 total Application Policies

| □ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| □ | 1 | Spokes-to-Hub-DMZ | + SPOKE-LAN1 × | ✓ | HUB1-LAN1 × HUB2-LAN1 × + | None | + |
| □ | 2 | Spoke-to-Spoke-via-Hub | + SPOKE-LAN1 × | ✓ | SPOKE-LAN1 × + | None | + |
| □ | 3 | Hub-DMZ-to-Spoke | + HUB1-LAN1 × HUB2-LAN1 × | ✓ | SPOKE-LAN1 × + | None | + |
| □ | 4 | Internet-via-Cloud-CBO | + SPOKE-LAN1 × | ✓ | ANY × + | None | Cloud × |

- Select the policy that you want to modify, and apply the following changes
  - Check the Override Template Settings option.
  - Change the **Traffic Steering** to **Cloud** in the last rule (Internet-via-Cloud-CBO).
- Save your changes.

Juniper Mist cloud builds new tunnels to Juniper Security Director Cloud.

Verify the Configuration

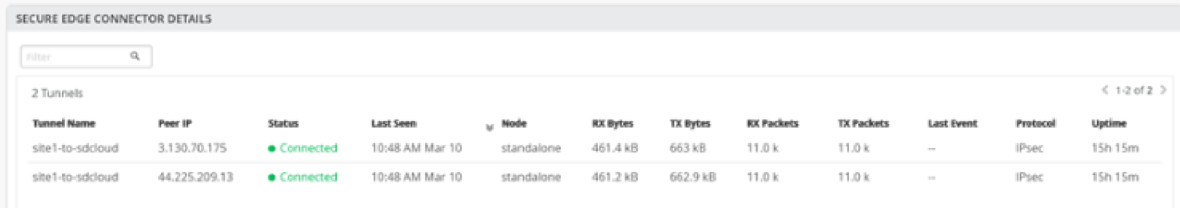
After you modify the application policy, now it is time to confirm that your configuration is working as expected.

With the desired configuration saved, you can verify if Juniper Mist cloud routes the Internet-bound traffic from spokes to Juniper Security Director Cloud instead of routing it to a hub for central breakout.

To verify the configuration:

- Verify the established tunnels details WAN Insights of the device in Juniper Mist cloud portal.

Figure141: Secure Edge Connector with Tunnel Details



SECURE EDGE CONNECTOR DETAILS

2 Tunnels

1-2 of 2

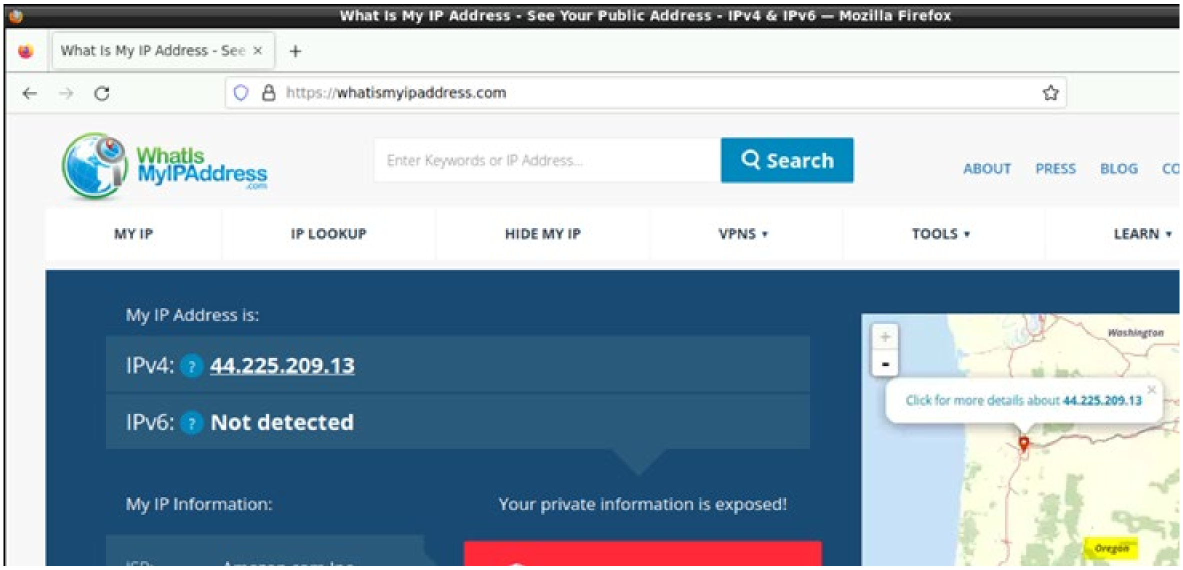
| Tunnel Name | Peer IP | Status | Last Seen | Node | RX Bytes | TX Bytes | RX Packets | TX Packets | Last Event | Protocol | Uptime |
|---|---|---|---|---|---|---|---|---|---|---|---|
| site1-to-sdcloud | 3.130.70.175 | ● Connected | 10:48 AM Mar 10 | standalone | 461.4 kB | 663 kB | 11.0 k | 11.0 k | -- | IPsec | 15h 15m |
| site1-to-sdcloud | 44.225.209.13 | ● Connected | 10:48 AM Mar 10 | standalone | 461.2 kB | 662.9 kB | 11.0 k | 11.0 k | -- | IPsec | 15h 15m |

You can also check the established tunnels in the Juniper Security Director Cloud dashboard and in the service location.

- Check the new traffic flow using a client attached at the LAN-Interface of the spoke. Open a browser on client attached at the LAN-Interface of the spoke and navigate to https://whatismyipaddress.com/ to view details about the source IP address used to route the Juniper Mist network traffic from a service location towards the Internet.

The two Figures below show traffic from the primary and secondary service locations.

Figure142: Traffic from Primary Service Location



What Is My IP Address - See Your Public Address - IPv4 & IPv6 — Mozilla Firefox

https://whatismyipaddress.com

My IP Address is:

IPv4: ? 44.225.209.13

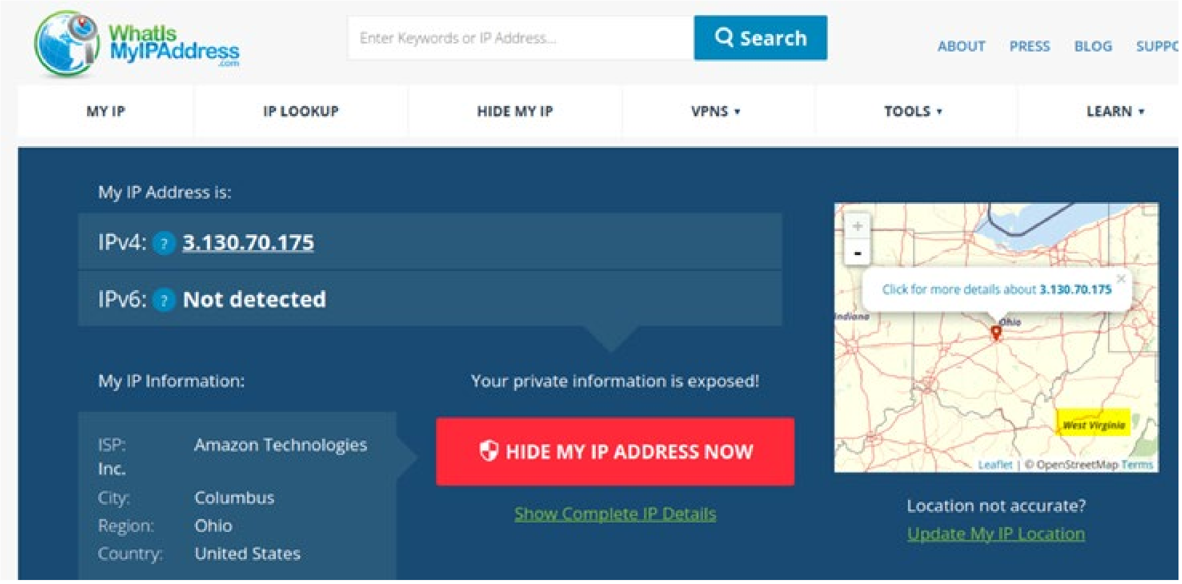
IPv6: ? Not detected

My IP Information:

Your private information is exposed!

Click for more details about 44.225.209.13

Figure143: Traffic from Secondary Service Location



My IP Address is:

IPv4: 3.130.70.175

IPv6: Not detected

My IP Information:

Your private information is exposed!

ISP: Amazon Technologies Inc.
City: Columbus
Region: Ohio
Country: United States

One of the two IP addresses of the service location is a public IP address and serves two purposes:

- Terminates the IPsec tunnel hence the Spoke uses it to establish the Tunnel with Juniper Security Director Cloud.
- Act as a new Source IP address for Traffic leaving the VPN which we can detect with the above.

Remember that a service location in Juniper Security Director Cloud is also known as POP and represents a Juniper Secure Edge instance in a cloud location. The service location is the connection (access) point for both on-premises and roaming users.

# Additional Features Valid for All Topologies

In this chapter, we are sharing more information about the other aspects and features tested for this JVD.

## Advanced Application Steering

**Applications** represent traffic destinations. On Juniper SRX Series Firewall, applications determine the destination used in a security policy.

Applications are the services or applications that your network users connect to in a Juniper Mist WAN Assurance design. You can define these applications manually in the Juniper Mist cloud portal. You define applications by selecting the category (such as Social Media) or selecting individual applications (such as Microsoft Teams) from a list. Another option is to use the predefined list of common traffic types. You can also create a custom application.

> Note: When you define how to build your internal VPN, then use IP prefixes through a custom rule to define the basic rules of forwarding traffic. After you have tested those, you can be more specific and use other types to detect applications and steer them.

For users to access applications, you must first define the applications and then use application policies to permit or deny access. That is, you associate these applications with users and networks and then assign a traffic steering policy and access rule (allow or deny).

When defining applications, you have the following options defined by their Types:

- Using Custom Apps application:
    - IP address or IP prefix. You can add multiple using comma-separated in the field.
    - Domain Names. Ensure to use FQDN. You can add multiple using comma-separated in the field.
    - IP-Protocol. TCP, UDP, GRE, or a Custom value are allowed.
    - Destination Start and End Ports (if the IP-Protocol supports it).
- Using Apps application the device leverages its **DPI-Engine** with presently more than >7000 known applications to identify them.
    - You can select each known application individually from the drop-down menu or search for them.
    - When you have your VPN up and running for a while, the system reports automatically detected applications and display them as a Learned Application. This is quite useful as one can learn by that what is really in use by the clients and then decide what to do with this traffic.

Using a URL Categories application that has a table of known websites that are mapped into categories, you can  define an application. This is an additional licensed feature same as IDP. You can use the URL Category Groups, URL Categories, and URL Subcategories as shown in the table below.

| | |
|---|---|
| URL Category Groups | All |
| URL Category Groups | Standard |
| URL Category Groups | Strict |
| URL Categories | Adult |
| URL Categories | Advertisement |
| URL Categories | Arts and Entertainment |
| URL Categories | Business |
| URL Categories | Career and Education |
| URL Categories | Collaboration |
| URL Categories | Conferencing |
| URL Categories | Device IOT |
| URL Categories | File Sharing |
| URL Categories | Financial |
| URL Categories | Games |
| URL Categories | Government |
| URL Categories | Images |
| URL Categories | Infrastructure |

| | |
|---|---|
| URL Categories | Malware |
| URL Categories | Networking |
| URL Categories | News and Reference |
| URL Categories | Recreation |
| URL Categories | Religion |
| URL Categories | Remote Desktop |
| URL Categories | Search Engines |
| URL Categories | Security |
| URL Categories | Shopping |
| URL Categories | Social Media |
| URL Categories | Software Updates |
| URL Categories | Sports |
| URL Categories | Streaming Media |
| URL Categories | Technology |
| URL Categories | Violence |
| URL Subcategories | Abortion |
| URL Subcategories | Adult Content |
| URL Subcategories | Adult Material |
| URL Subcategories | Advanced Malware Command and Control |
| URL Subcategories | Advanced Malware Payloads |
| URL Subcategories | Advertisements |
| URL Subcategories | Alcohol and Tobacco |
| URL Subcategories | Alternative Journals |
| URL Subcategories | Application and Software Download |
| URL Subcategories | Bandwidth |
| URL Subcategories | Blog Commenting |
| URL Subcategories | Blog Posting |
| URL Subcategories | Blogs and Personal Sites |

| | |
|---|---|
| URL Subcategories | Bot Networks |
| URL Subcategories | Business and Economy |
| URL Subcategories | Classifieds Posting |
| URL Subcategories | Collaboration Office |
| URL Subcategories | Compromised Websites |
| URL Subcategories | Computer Security |
| URL Subcategories | Content Delivery Networks |
| URL Subcategories | Cultural Institutions |
| URL Subcategories | Education |
| URL Subcategories | Educational Institutions |
| URL Subcategories | Educational Materials |
| URL Subcategories | Educational Video |
| URL Subcategories | Emerging Exploits |
| URL Subcategories | Entertainment |
| URL Subcategories | File Download Servers |
| URL Subcategories | Files Containing Passwords |
| URL Subcategories | Financial Data and Services |
| URL Subcategories | Freeware and Software Download |
| URL Subcategories | Games |
| URL Subcategories | Gay or Lesbian or Bisexual Interest |
| URL Subcategories | Government |
| URL Subcategories | Hacking |
| URL Subcategories | Hobbies |
| URL Subcategories | Hosted Business Applications |
| URL Subcategories | Image Servers |
| URL Subcategories | Images Media |
| URL Subcategories | Information Technology |
| URL Subcategories | Internet Auctions |

| | |
|---|---|
| URL Subcategories | Internet Radio and TV |
| URL Subcategories | Internet Telephony |
| URL Subcategories | Intolerance |
| URL Subcategories | Job Search |
| URL Subcategories | Keyloggers |
| URL Subcategories | Lingerie and Swimsuit |
| URL Subcategories | Malicious Embedded iFrame |
| URL Subcategories | Malicious Embedded Link |
| URL Subcategories | Malicious Web Sites |
| URL Subcategories | Media File Download |
| URL Subcategories | Militancy and Extremist |
| URL Subcategories | Military |
| URL Subcategories | Mobile Malware |
| URL Subcategories | Network Errors |
| URL Subcategories | News and Media |
| URL Subcategories | Non Traditional Religions |
| URL Subcategories | Non Traditional Religions and Occult and Folklore |
| URL Subcategories | Nudity |
| URL Subcategories | Office Apps |
| URL Subcategories | Office Documents |
| URL Subcategories | Office Drive |
| URL Subcategories | Office Mail |
| URL Subcategories | Online Brokerage and Trading |
| URL Subcategories | Parked Domain |
| URL Subcategories | Peer to Peer File Sharing |
| URL Subcategories | Personal Network Storage and Backup |
| URL Subcategories | Personals and Dating |
| URL Subcategories | Phishing and Other Frauds |

| | |
|---|---|
| URL Subcategories | Political Organizations |
| URL Subcategories | Potentially Exploited Documents |
| URL Subcategories | Potentially Unwanted Software |
| URL Subcategories | Private IP Addresses |
| URL Subcategories | Pro Choice |
| URL Subcategories | Pro Life |
| URL Subcategories | Professional and Worker Organizations |
| URL Subcategories | Proxy Avoidance |
| URL Subcategories | Real Estate |
| URL Subcategories | Reference Materials |
| URL Subcategories | Religion |
| URL Subcategories | Restaurants and Dining |
| URL Subcategories | Search Engines and Portals |
| URL Subcategories | Security |
| URL Subcategories | Service and Philanthropic Organizations |
| URL Subcategories | Sex |
| URL Subcategories | Sex Education |
| URL Subcategories | Shopping |
| URL Subcategories | Social and Affiliation Organizations |
| URL Subcategories | Social Organizations |
| URL Subcategories | Social Web Facebook |
| URL Subcategories | Social Web LinkedIn |
| URL Subcategories | Social Web Twitter |
| URL Subcategories | Social Web YouTube |
| URL Subcategories | Society and Lifestyles |
| URL Subcategories | Special Events |
| URL Subcategories | Sport Hunting and Gun Clubs |
| URL Subcategories | Sports |

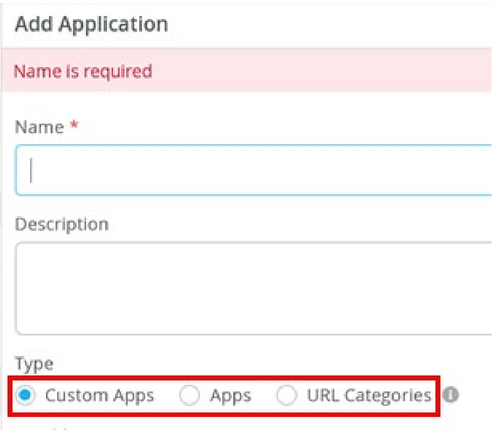
| | |
|---|---|
| URL Subcategories | Spyware |
| URL Subcategories | Streaming Media |
| URL Subcategories | Surveillance |
| URL Subcategories | Suspicious Content |
| URL Subcategories | Suspicious Embedded Link |
| URL Subcategories | Tasteless |
| URL Subcategories | Traditional Religions |
| URL Subcategories | Unauthorized Mobile Marketplaces |
| URL Subcategories | Violence |
| URL Subcategories | Viral Video |
| URL Subcategories | Web Analytics |
| URL Subcategories | Web and Email Marketing |
| URL Subcategories | Web and Email Spam |
| URL Subcategories | Web Hosting |
| URL Subcategories | Web Images |
| URL Subcategories | Web Infrastructure |
| URL Subcategories | Website Translation |

Note: In the Advanced Settings tab, you cannot select Traffic Types for SRX Series devices.

To configure applications:

1. In the Juniper Mist portal, click **Organization** > **WAN**> **Applications**. A list of existing applications, if any, appears.

2. Click **Add Applications** in the top-right corner. The **Add Application** window appears.
   Beside setting an application name and an optional description, you can then select between the three major types as shown below.



Add Application

Name is required

Name *

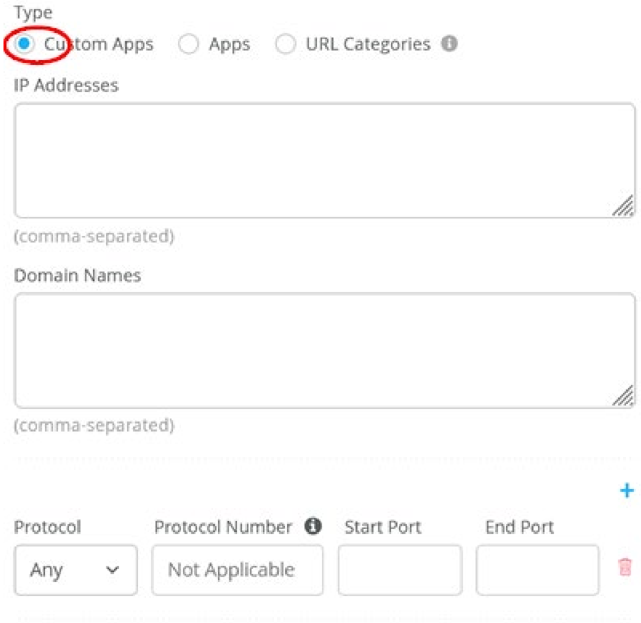
Description

Type

● Custom Apps ○ Apps ○ URL Categories

Define Custom Applications

Juniper Mist cloud enables you to define your own custom applications with IP addresses/prefixes, domain names, IP protocols and destination port/port ranges. Select the appropriate type and fill in the fields you want to use.



Type

● Custom Apps ○ Apps ○ URL Categories

IP Addresses

(comma-separated)

Domain Names

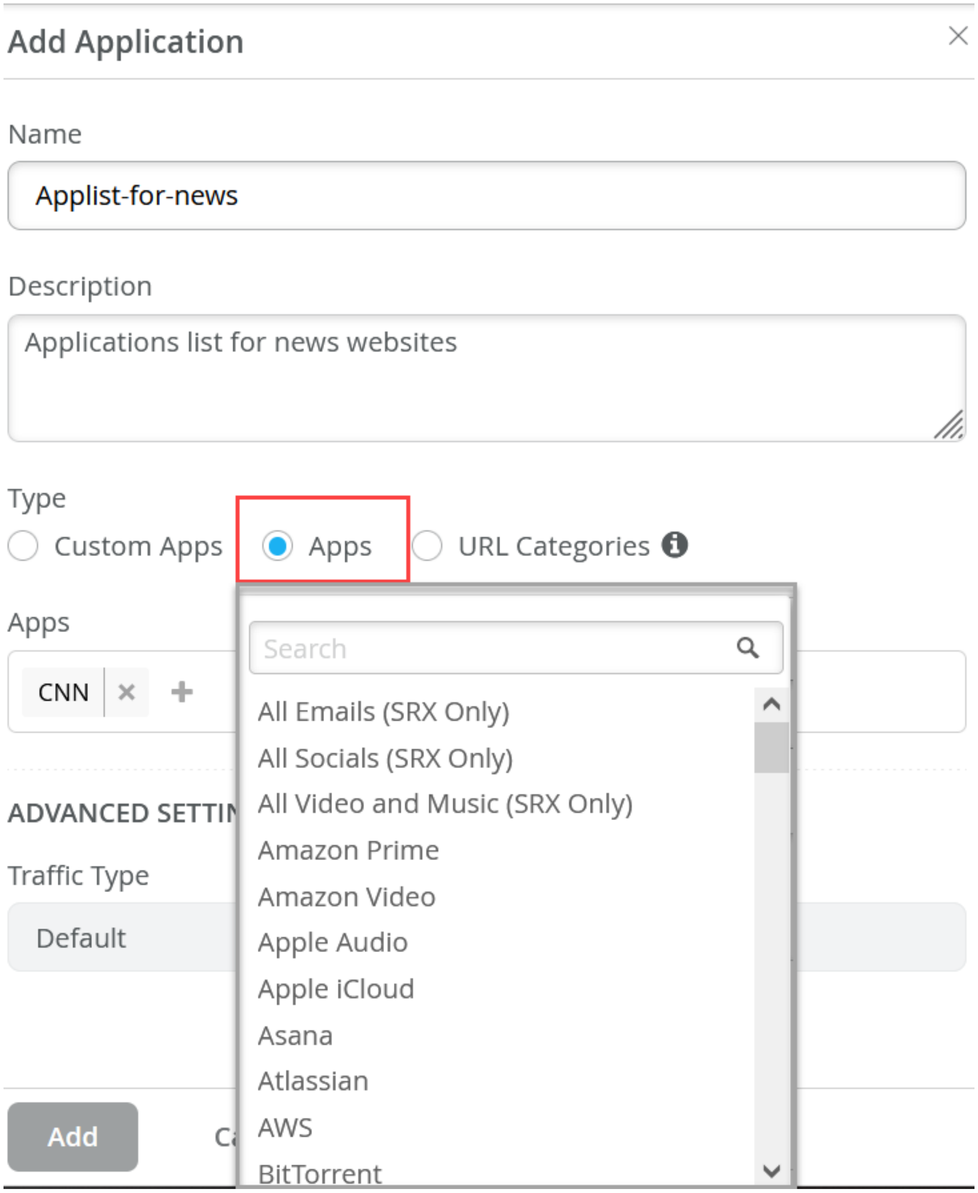
(comma-separated)

| Protocol | Protocol Number | Start Port | End Port |
|---|---|---|---|
| Any | Not Applicable | | |

Configure Predefined Applications

Juniper Mist cloud provides a list of known applications (>7000) that you can use to define an application.

Select the appropriate type and select the application from the drop-down menu or search for it.



Add Application

Name

Applist-for-news

Description

Applications list for news websites

Type

○ Custom Apps ● Apps ○ URL Categories

Apps

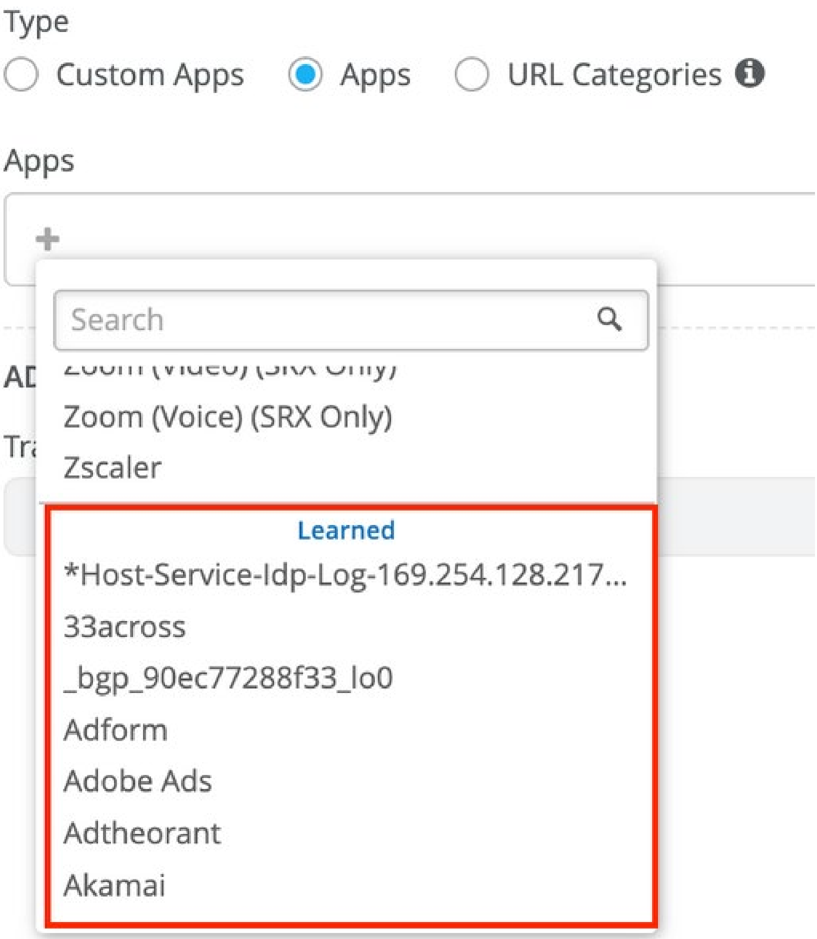
CNN

ADVANCED SETTI

Traffic Type

Default

Learned Applications, which are detected by running traffic for a while, should appear automatically at the end of the selection list as shown below.



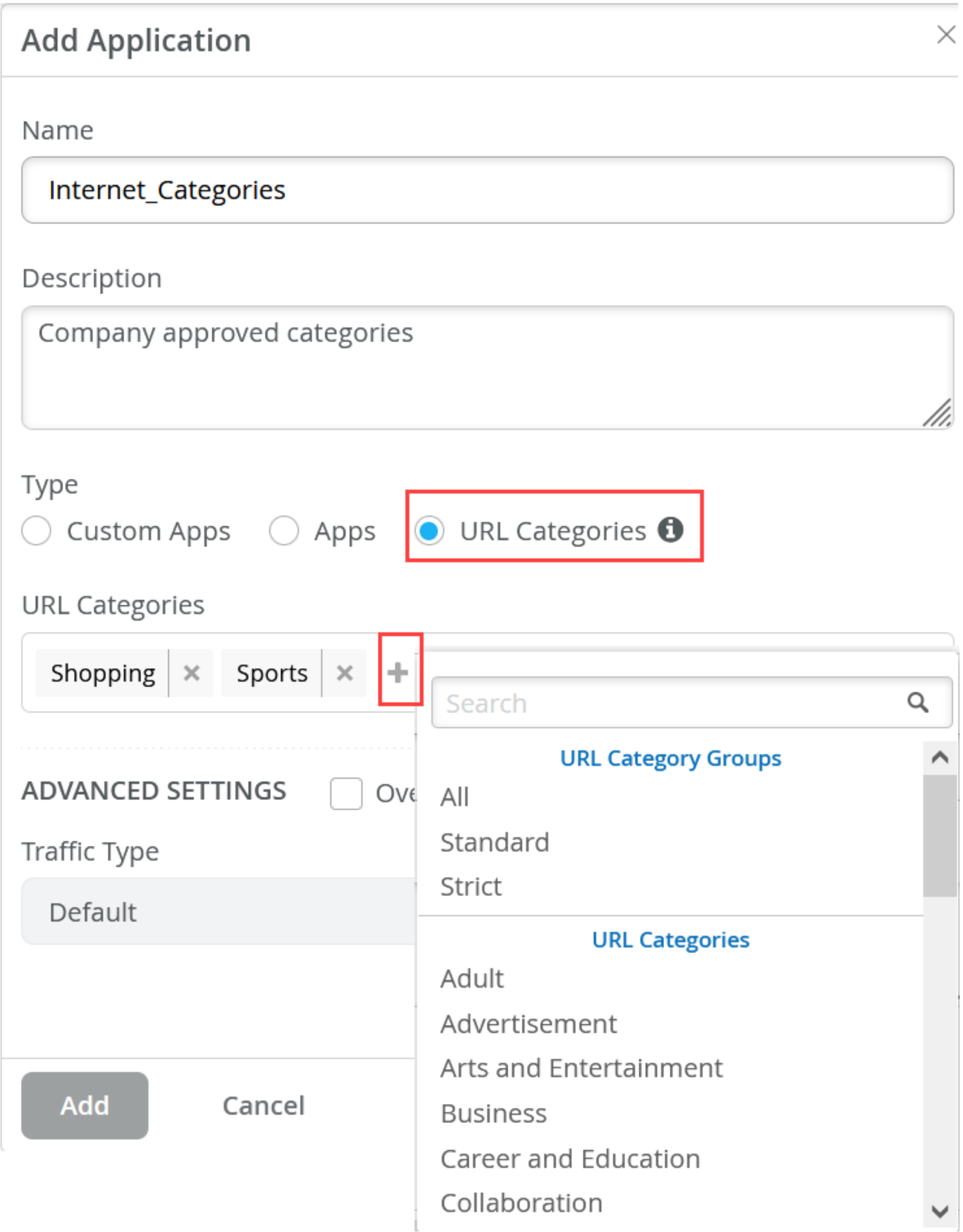
Using URL Categories

Juniper Mist cloud provides a list of URL categories based on types (for example, shopping and sports) and grouped by severity (all, standard, and strict). You can use the URL categories to define an application. URL categories offer granular filtering for application creation. You can select a single or multiple URL categories for an application.

To define URL categories:

- In the Mist portal, in the **Add Application** pane, select the **Type** as **URL Categories**.
- Click the Add (**+**) icon to display the list of available URL categories.

Figure144: URL Categories



Name: Internet_Categories

Description: Company approved categories

Type: ○ Custom Apps ○ Apps ● URL Categories

URL Categories: Shopping × Sports × +

ADVANCED SETTINGS □ Ove

Traffic Type: Default

## IDP-Based Threat Detection for SRX Series Firewalls

An Intrusion Detection and Prevention (IDP) policy lets you selectively enforce various attack detection and prevention techniques on network traffic. You can enable IDP on the Juniper Networks SRX Series Firewall operating as a spoke device in your Juniper Mist network by activating it in an application policy.

Intrusion detection is the process of monitoring the events occurring on your network and analyzing them for signs of incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. For more details, see Intrusion Detection and Prevention Overview.

> Note: You must install the IDP signature database update license key on your Juniper Mist device. For details about licenses, see **Junos OS Feature License Keys**. The Juniper Mist cloud portal manages downloading of signatures and enabling the IDP features on your firewall if you have a valid license.

Juniper Mist cloud supports the following IDP profiles:

- Standard—The Standard profile is the default profile and represents the set of IDP signatures and rules that we recommend. Each attack type and severity have a Juniper-defined, non-configurable action that the IDP engine enforces when it detects an attack. The possible actions are as follows:
  - Close the client and server TCP connection.
  - Drop the current packet and all subsequent packets
  - Send an alert only (no additional action).
- Alert—The Alert profile is suitable only for low-severity attacks. When the IDP engine detects malicious traffic on the network, the system generates an alert, but it does not take additional measures to prevent the attack. The IDP signature and rules are the same as in the standard profile.
- Strict—The Strict profile contains a similar set of IDP signatures and rules as the standard profile. When the system detects an attack, this profile actively blocks any malicious traffic or other attacks detected on the network.
- Critical Only—This loads a reduced rule set with only about 300 critical patterns on the device. This often used on devices such as SRX300/SRX320 to reduce the CPU-load IDP causes.

You can apply an IDP profile to an application policy. Each profile has an associated traffic action, and these actions define how to apply a rule set to a service or an application policy. You cannot configure the actions in the IDP profile that are preconfigured.

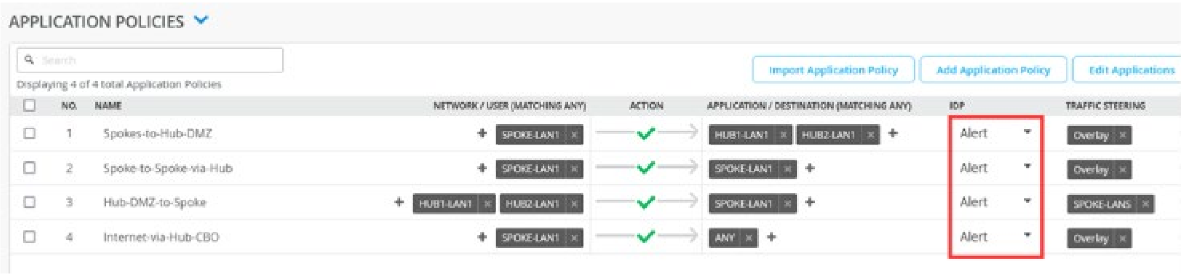
To configure IDP-based threat detection:

1. In the Juniper Mist cloud portal, click **Organization** > **WAN Edge Templates** and select a template for your spoke device.

2. On the WAN Edge Templates spoke page, scroll down to the **Applications Policies** pane. The pane displays the list of existing application policies.

3. Under the **IDP** column, select an IDP profile. For example, select the **Alert** profile for all application policies.

Figure145: Configure an IDP Profile (Alert)



APPLICATION POLICIES

Search

Import Application Policy | Add Application Policy | Edit Applications

Displaying 4 of 4 total Application Policies

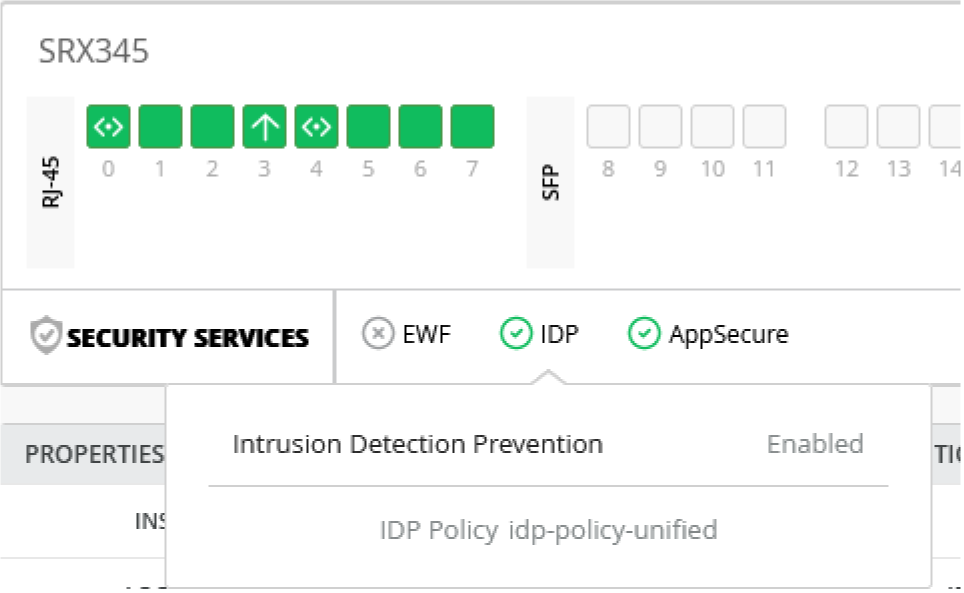
| ☐ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| ☐ | 1 | Spokes-to-Hub-DMZ | + SPOKE-LAN1 × | ✓ | HUB1-LAN1 × HUB2-LAN1 × + | Alert | Overlay × |
| ☐ | 2 | Spoke-to-Spoke-via-Hub | + SPOKE-LAN1 × | ✓ | SPOKE-LAN1 × + | Alert | Overlay × |
| ☐ | 3 | Hub-DMZ-to-Spoke | + HUB1-LAN1 × HUB2-LAN1 × | ✓ | SPOKE-LAN1 × + | Alert | SPOKE-LANS × |
| ☐ | 4 | Internet-via-Hub-CBO | + SPOKE-LAN1 × | ✓ | ANY × + | Alert | Overlay × |

4. Click **Save**. The Juniper Mist cloud applies the configured IDP profile on all spoke devices.

Note: Ensure that you set the policy action to PERMIT. Else, the IDP settings might override the DENY statement.

5. After you apply an IDP profile, the spoke devices download the IDP policy and display the status of IDP as **Enabled**, as shown below.

Figure146: Activated IDP Policy



Intrusion Detection Prevention Enabled

IDP Policy idp-policy-unified

You can test the effects of the IDP-based security scanner by launching sample attacks. You can use tools such as Nikto in Kali Linux, which has a variety of options available for security-penetration testing.

Use a Client in your environment (VM recommended), and install a simple security scanner for web servers, such as Nikto. Nikto is an open-source web server and web application scanner. For example, you can run Nikto against an unhardened Apache Tomcat web server (or its equivalent) that is local to your lab. In this test, you can send plain or unencrypted HTTP requests for IDP inspection.

The following sample shows a process where you install the tool, check the presence of the HTTP server, and then launch the attacks. Here we used an Ubuntu based desktop VM attached to the LAN interface of a spoke.

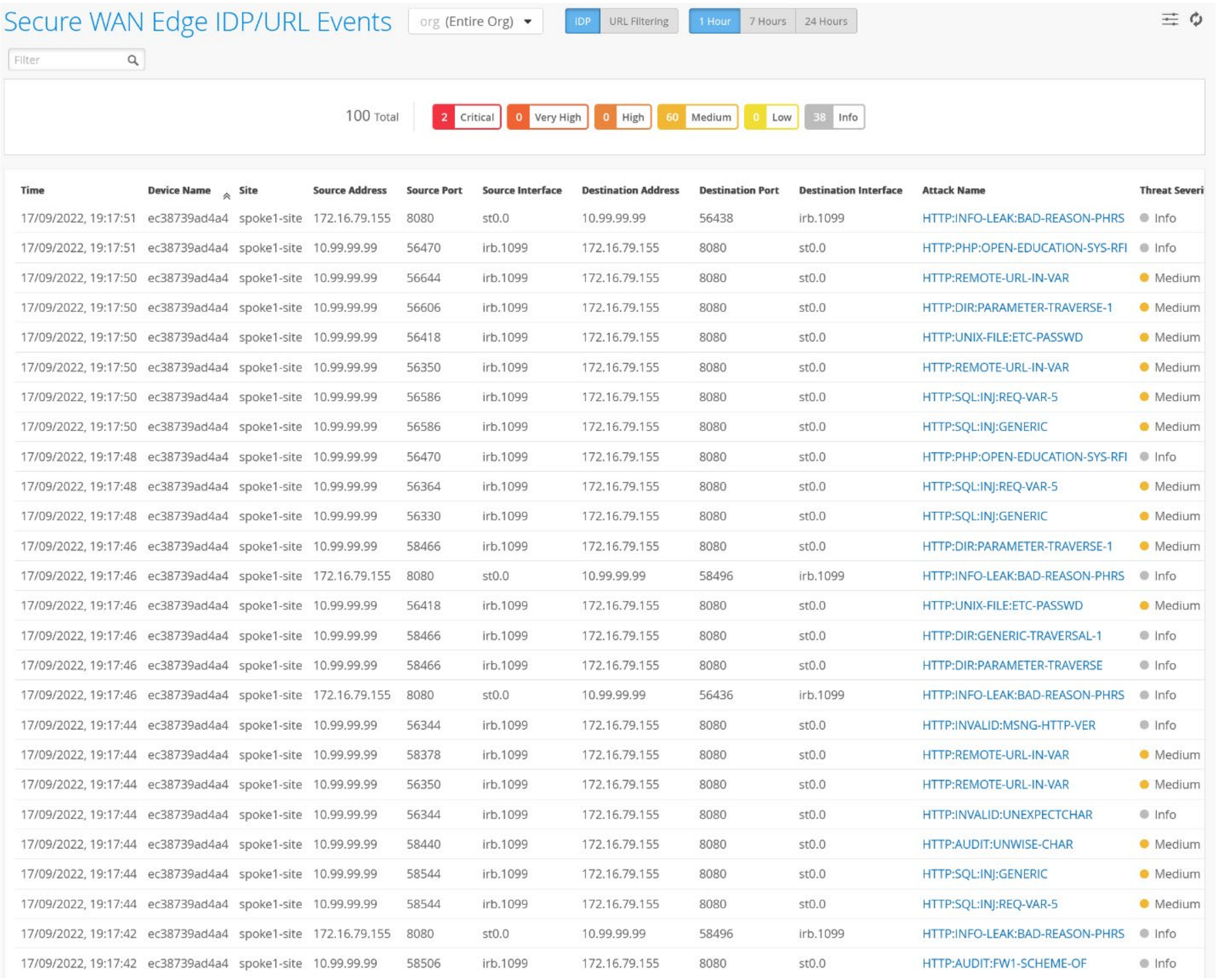
```
apt-get update

apt-get install -y nikto

# Check the Apache Tomcat Server of the local lab
wget http://172.16.77.155:8080
--2022-09-16 15:47:32--  http://172.16.77.155:8080/
Connecting to 172.16.77.155:8080... connected.
HTTP request sent, awaiting response... 200
Length: unspecified [text/html]
Saving to: 'index.html'

index.html              [ <=>                  ]  10.92K  --.-KB/s    in 0s
```

```
2022-09-16 15:47:32 (85.3 MB/s) - 'index.html' saved [11184]

# Now start our security scanner for the first time
nikto -h http://172.16.77.155:8080
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          172.16.77.155
+ Target Hostname:    172.16.77.155
+ Target Port:        8080
+ Start Time:         2022-09-16 15:48:22 (GMT0)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /favicon.ico, fields:
0xW/21630 0x1556961512000
+ OSVDB-39272: favicon.ico file identifies this server as: Apache Tomcat
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save
files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files
on the web server.
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
+ Cookie JSESSIONID created without the httponly flag
+ OSVDB-3720: /examples/jsp/snp/snoop.jsp: Displays information about page retrievals,
including other users.
+ OSVDB-3233: /manager/manager-howto.html: Tomcat documentation found.
+ /manager/html: Default Tomcat Manager interface found
+ 6544 items checked: 1 error(s) and 10 item(s) reported on remote host
+ End Time:           2022-09-16 15:50:03 (GMT0) (101 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- You can view the generated events by navigating to **Site** > **Secure WAN Edge IDP/URL Events**.

The figure below shows detected events generated for an SRX Series Firewall.

Figure147: IDP Events Generated for an Alert IDP Profile



Secure WAN Edge IDP/URL Events

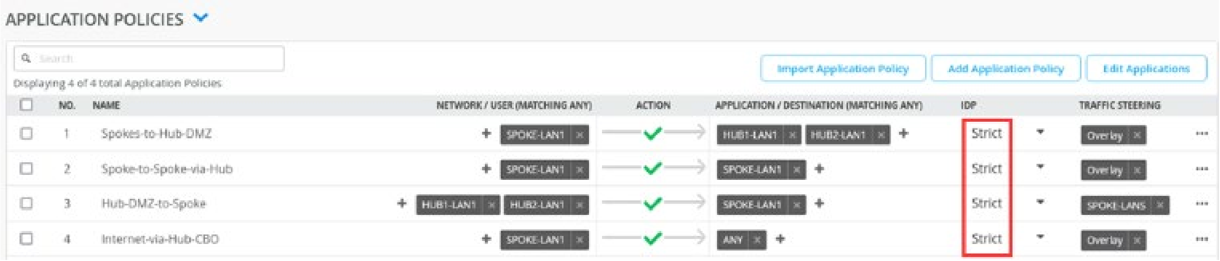
100 Total | 2 Critical | 0 Very High | 0 High | 60 Medium | 0 Low | 38 Info

| Time | Device Name | Site | Source Address | Source Port | Source Interface | Destination Address | Destination Port | Destination Interface | Attack Name | Threat Severi |
|---|---|---|---|---|---|---|---|---|---|---|
| 17/09/2022, 19:17:51 | ec38739ad4a4 | spoke1-site | 172.16.79.155 | 8080 | st0.0 | 10.99.99.99 | 56438 | irb.1099 | HTTP:INFO-LEAK:BAD-REASON-PHRS | ● Info |
| 17/09/2022, 19:17:51 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56470 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:PHP:OPEN-EDUCATION-SYS-RFI | ● Info |
| 17/09/2022, 19:17:50 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56644 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:REMOTE-URL-IN-VAR | ● Medium |
| 17/09/2022, 19:17:50 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56606 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:DIR:PARAMETER-TRAVERSE-1 | ● Medium |
| 17/09/2022, 19:17:50 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56418 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:UNIX-FILE:ETC-PASSWD | ● Medium |
| 17/09/2022, 19:17:50 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56350 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:REMOTE-URL-IN-VAR | ● Medium |
| 17/09/2022, 19:17:50 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56586 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:SQL:INJ:REQ-VAR-5 | ● Medium |
| 17/09/2022, 19:17:50 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56586 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:SQL:INJ:GENERIC | ● Medium |
| 17/09/2022, 19:17:48 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56470 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:PHP:OPEN-EDUCATION-SYS-RFI | ● Info |
| 17/09/2022, 19:17:48 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56364 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:SQL:INJ:REQ-VAR-5 | ● Medium |
| 17/09/2022, 19:17:48 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56330 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:SQL:INJ:GENERIC | ● Medium |
| 17/09/2022, 19:17:46 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 58466 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:DIR:PARAMETER-TRAVERSE-1 | ● Medium |
| 17/09/2022, 19:17:46 | ec38739ad4a4 | spoke1-site | 172.16.79.155 | 8080 | st0.0 | 10.99.99.99 | 58496 | irb.1099 | HTTP:INFO-LEAK:BAD-REASON-PHRS | ● Info |
| 17/09/2022, 19:17:46 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56418 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:UNIX-FILE:ETC-PASSWD | ● Medium |
| 17/09/2022, 19:17:46 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 58466 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:DIR:GENERIC-TRAVERSAL-1 | ● Info |
| 17/09/2022, 19:17:46 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 58466 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:DIR:PARAMETER-TRAVERSE | ● Info |
| 17/09/2022, 19:17:46 | ec38739ad4a4 | spoke1-site | 172.16.79.155 | 8080 | st0.0 | 10.99.99.99 | 56436 | irb.1099 | HTTP:INFO-LEAK:BAD-REASON-PHRS | ● Info |
| 17/09/2022, 19:17:44 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56344 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:INVALID:MSNG-HTTP-VER | ● Info |
| 17/09/2022, 19:17:44 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 58378 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:REMOTE-URL-IN-VAR | ● Medium |
| 17/09/2022, 19:17:44 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56350 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:REMOTE-URL-IN-VAR | ● Medium |
| 17/09/2022, 19:17:44 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 56344 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:INVALID:UNEXPECTCHAR | ● Info |
| 17/09/2022, 19:17:44 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 58440 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:AUDIT:UNWISE-CHAR | ● Medium |
| 17/09/2022, 19:17:44 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 58544 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:SQL:INJ:GENERIC | ● Medium |
| 17/09/2022, 19:17:44 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 58544 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:SQL:INJ:REQ-VAR-5 | ● Medium |
| 17/09/2022, 19:17:42 | ec38739ad4a4 | spoke1-site | 172.16.79.155 | 8080 | st0.0 | 10.99.99.99 | 58496 | irb.1099 | HTTP:INFO-LEAK:BAD-REASON-PHRS | ● Info |
| 17/09/2022, 19:17:42 | ec38739ad4a4 | spoke1-site | 10.99.99.99 | 58506 | irb.1099 | 172.16.79.155 | 8080 | st0.0 | HTTP:AUDIT:FW1-SCHEME-OF | ● Info |

In the previous example, you used passive logging for the events by using IDP profile type Alerts. Next, use IDP profile type **Strict** to stop or mitigate the events. When you use the Strict profile, the IDP engine closes TCP connections against the detected attacks.

You can follow the same process as shown in the example. Now, you change the spoke device template and change the IDP profile from **Alert** to **Strict**, as shown below.

Figure148: IDP Profile Configuration (Strict Profile)



APPLICATION POLICIES

Displaying 4 of 4 total Application Policies

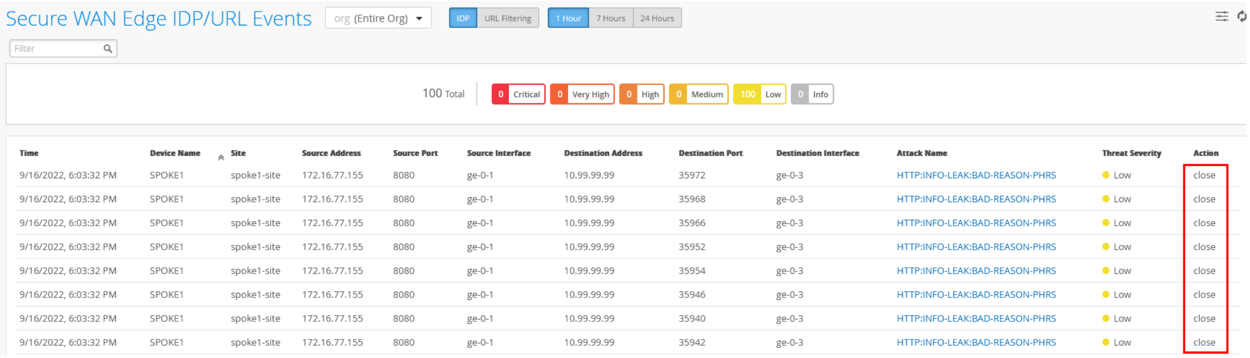
| ☐ | NO. | NAME | NETWORK / USER (MATCHING ANY) | ACTION | APPLICATION / DESTINATION (MATCHING ANY) | IDP | TRAFFIC STEERING |
|---|---|---|---|---|---|---|---|
| ☐ | 1 | Spokes-to-Hub-DMZ | SPOKE-LAN1 | ✓ | HUB1-LAN1<br>HUB2-LAN1 | Strict | Overlay |
| ☐ | 2 | Spoke-to-Spoke-via-Hub | SPOKE-LAN1 | ✓ | SPOKE-LAN1 | Strict | Overlay |
| ☐ | 3 | Hub-DMZ-to-Spoke | HUB1-LAN1<br>HUB2-LAN1 | ✓ | SPOKE-LAN1 | Strict | SPOKE-LANS |
| ☐ | 4 | Internet-via-Hub-CBO | SPOKE-LAN1 | ✓ | ANY | Strict | Overlay |

Run the security scanner again. You'll notice that the scanner takes longer to run because it detects more errors and less events.

```
nikto -h http://172.16.77.155:8080
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          172.16.77.155
+ Target Hostname:    172.16.77.155
+ Target Port:        8080
+ Start Time:         2022-09-16 16:01:51 (GMT0)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /favicon.ico, fields:
0xW/21630 0x1556961512000
+ OSVDB-39272: favicon.ico file identifies this server as: Apache Tomcat
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save
files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files
on the web server.
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
+ 6544 items checked: 5657 error(s) and 6 item(s) reported on remote host
+ End Time:           2022-09-16 16:05:27 (GMT0) (216 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

The figure below shows that for some events, the action is to close the session to mitigate the threats (under the **Action** field).

Figure 149: IDP Events Generated for the Strict IDP Profile

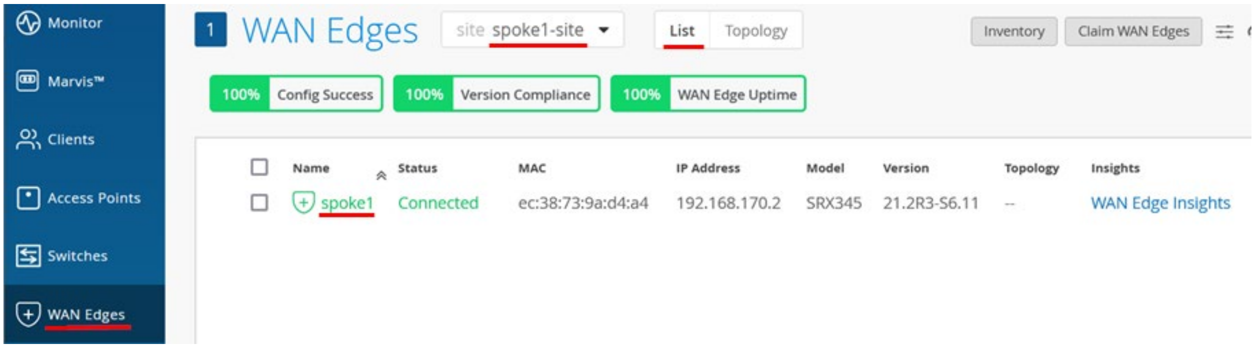


| Time | Device Name | Site | Source Address | Source Port | Source Interface | Destination Address | Destination Port | Destination Interface | Attack Name | Threat Severity | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 9/16/2022, 6:03:32 PM | SPOKE1 | spoke1-site | 172.16.77.155 | 8080 | ge-0-1 | 10.99.99.99 | 35972 | ge-0-3 | HTTP:INFO-LEAK:BAD-REASON-PHRS | ● Low | close |
| 9/16/2022, 6:03:32 PM | SPOKE1 | spoke1-site | 172.16.77.155 | 8080 | ge-0-1 | 10.99.99.99 | 35968 | ge-0-3 | HTTP:INFO-LEAK:BAD-REASON-PHRS | ● Low | close |
| 9/16/2022, 6:03:32 PM | SPOKE1 | spoke1-site | 172.16.77.155 | 8080 | ge-0-1 | 10.99.99.99 | 35966 | ge-0-3 | HTTP:INFO-LEAK:BAD-REASON-PHRS | ● Low | close |
| 9/16/2022, 6:03:32 PM | SPOKE1 | spoke1-site | 172.16.77.155 | 8080 | ge-0-1 | 10.99.99.99 | 35952 | ge-0-3 | HTTP:INFO-LEAK:BAD-REASON-PHRS | ● Low | close |
| 9/16/2022, 6:03:32 PM | SPOKE1 | spoke1-site | 172.16.77.155 | 8080 | ge-0-1 | 10.99.99.99 | 35954 | ge-0-3 | HTTP:INFO-LEAK:BAD-REASON-PHRS | ● Low | close |
| 9/16/2022, 6:03:32 PM | SPOKE1 | spoke1-site | 172.16.77.155 | 8080 | ge-0-1 | 10.99.99.99 | 35946 | ge-0-3 | HTTP:INFO-LEAK:BAD-REASON-PHRS | ● Low | close |
| 9/16/2022, 6:03:32 PM | SPOKE1 | spoke1-site | 172.16.77.155 | 8080 | ge-0-1 | 10.99.99.99 | 35940 | ge-0-3 | HTTP:INFO-LEAK:BAD-REASON-PHRS | ● Low | close |
| 9/16/2022, 6:03:32 PM | SPOKE1 | spoke1-site | 172.16.77.155 | 8080 | ge-0-1 | 10.99.99.99 | 35942 | ge-0-3 | HTTP:INFO-LEAK:BAD-REASON-PHRS | ● Low | close |

# Day-2 Device Information, Gateway Insights, WAN SLE and Alarms

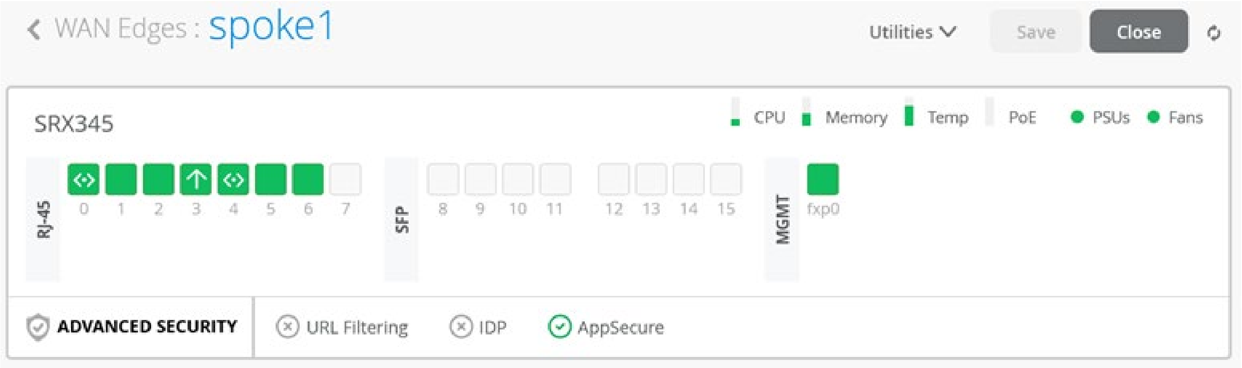
## Device Information Page

To get to the basic Device Monitoring page, click **WAN Edges**, select a site, and then click on the device as shown below.

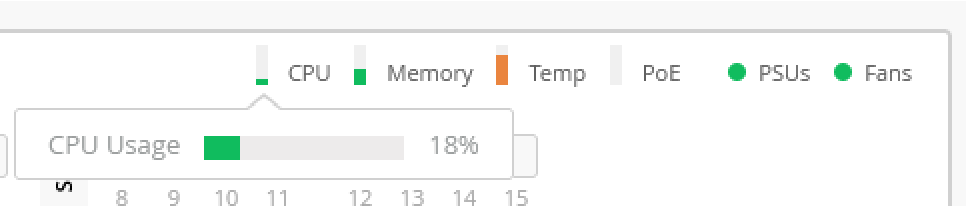


| ☐ | Name | Status | MAC | IP Address | Model | Version | Topology | Insights |
|---|---|---|---|---|---|---|---|---|
| ☐ | spoke1 | Connected | ec:38:73:9a:d4:a4 | 192.168.170.2 | SRX345 | 21.2R3-S6.11 | -- | WAN Edge Insights |

At the top of the Device information page, you see a graphical front view of the devices, its ports, and some baseline status information.

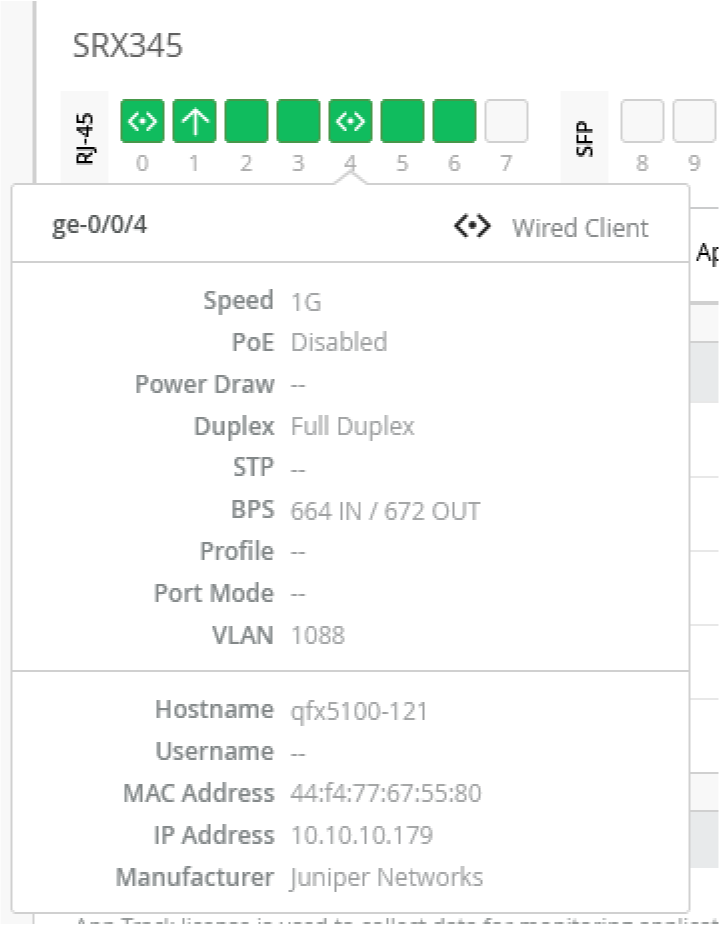


Hover- over with the mouse on each status information icon for CPU, Memory, Temperature, PoE, PSUs, and Fans to see how the device behaves.



CPU Usage 18%

Next, hover over with the mouse on some of the device ports  to review what is configured and detected. In this example, you see at the bottom that our lab switch is detected as a client attached to the Port.

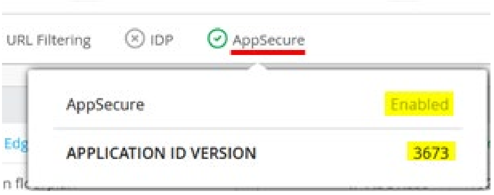


ge-0/0/4

Speed 1G
PoE Disabled
Power Draw --
Duplex Full Duplex
STP --
BPS 664 IN / 672 OUT
Profile --
Port Mode --
VLAN 1088

Hostname qfx5100-121
Username --
MAC Address 44:f4:77:67:55:80
IP Address 10.10.10.179
Manufacturer Juniper Networks

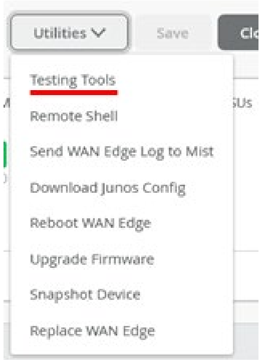
Below the Front Ports, hover over the mouse over each security service and review the reported information.



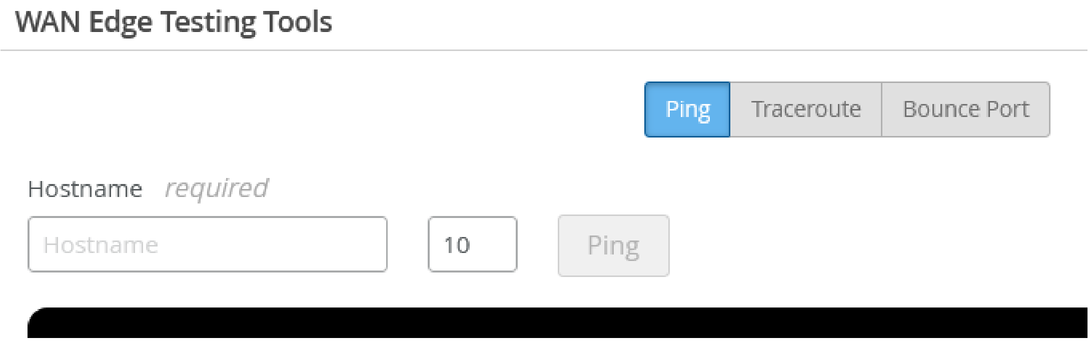
AppSecure Enabled

APPLICATION ID VERSION 3673

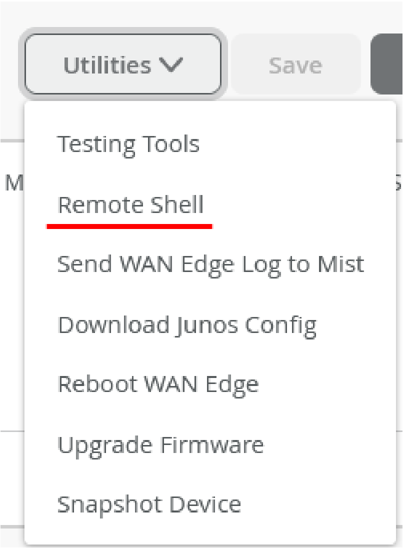
Then, check out the Utilities tab.  We've avail for the device and click on "Testing Tools" as there is more behind this one.



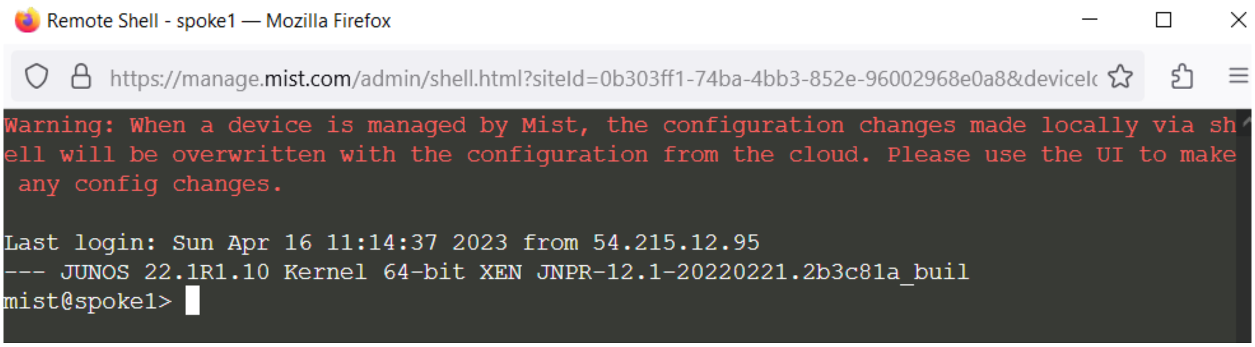
For example, the Testing Tools allow you to issue ICMP ping, Traceroutes, and Bounce a Port.



Besides the other Testing Tools, click Remote Shell to open a direct SSH-Shell to the device.

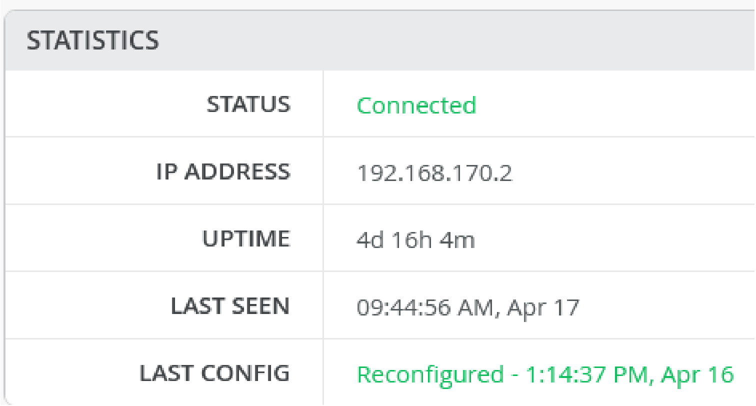


A new window appears with the ability to utilize the CLI on the device remotely.


Remote Shell - spoke1 — Mozilla Firefox
https://manage.mist.com/admin/shell.html?siteId=0b303ff1-74ba-4bb3-852e-96002968e0a8&deviceIc

```
Warning: When a device is managed by Mist, the configuration changes made locally via sh
ell will be overwritten with the configuration from the cloud. Please use the UI to make
 any config changes.

Last login: Sun Apr 16 11:14:37 2023 from 54.215.12.95
--- JUNOS 22.1R1.10 Kernel 64-bit XEN JNPR-12.1-20220221.2b3c81a_buil
mist@spoke1> 
```

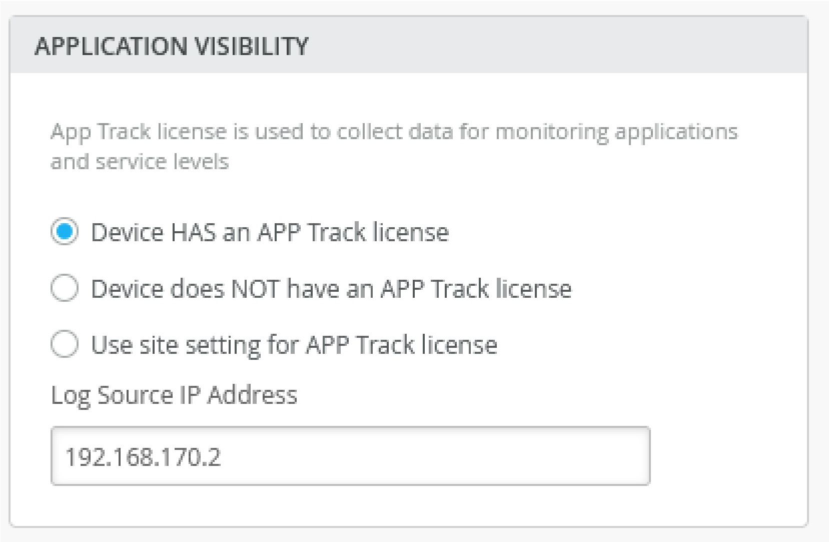
Back to the Device information page. Review the Statistics pane for information.



STATISTICS

| | |
|---|---|
| STATUS | Connected |
| IP ADDRESS | 192.168.170.2 |
| UPTIME | 4d 16h 4m |
| LAST SEEN | 09:44:56 AM, Apr 17 |
| LAST CONFIG | Reconfigured - 1:14:37 PM, Apr 16 |

Review the Application Visibility pane for information.



APPLICATION VISIBILITY

App Track license is used to collect data for monitoring applications and service levels

● Device HAS an APP Track license

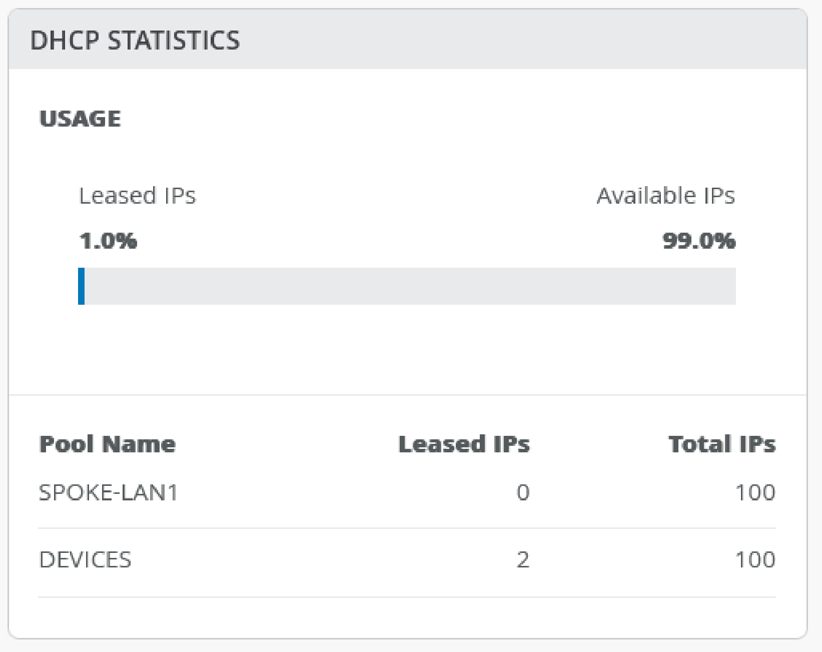
○ Device does NOT have an APP Track license

○ Use site setting for APP Track license

Log Source IP Address

192.168.170.2

In case you have configured DHCP servers on the WAN router, the DHCP Statistics pane displays the very useful information about the leases handed out.



DHCP STATISTICS

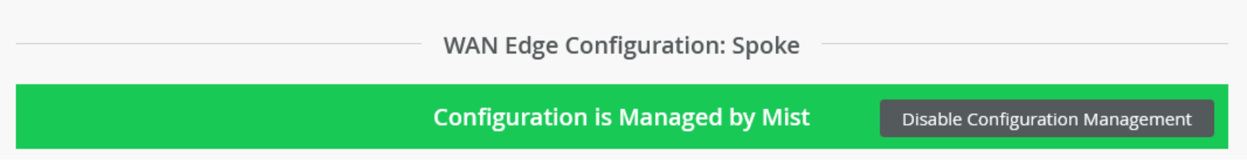
USAGE

Leased IPs 1.0%

Available IPs 99.0%

| Pool Name | Leased IPs | Total IPs |
|---|---|---|
| SPOKE-LAN1 | 0 | 100 |
| DEVICES | 2 | 100 |

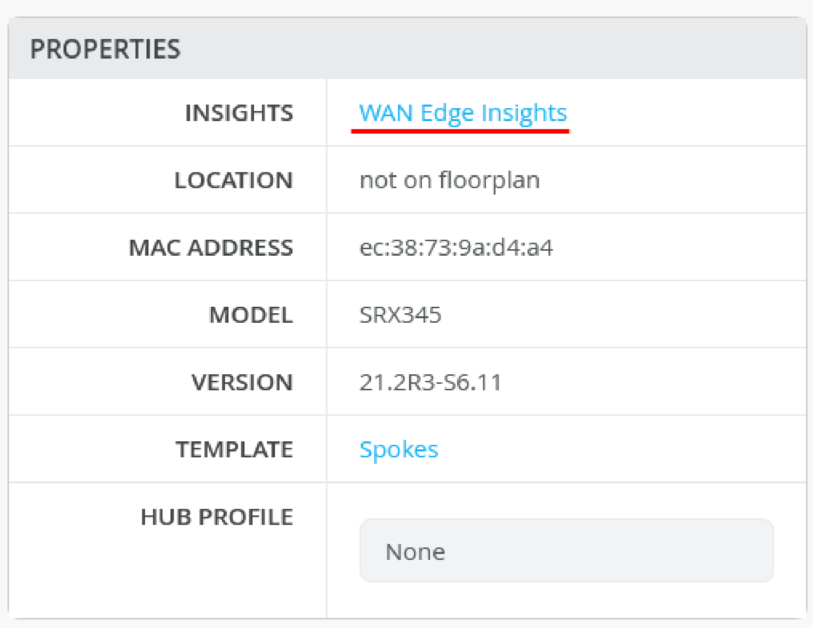
Then, review the device configuration. Usually, it should be inherited by the templates or profiles you have used. You can make **individual changes to the configuration** to be pushed to the device.



WAN Edge Configuration: Spoke

Configuration is Managed by Mist

Finally, review the Properties pane for information and then click **WAN Edge Insights** for the next-level of information about the device.

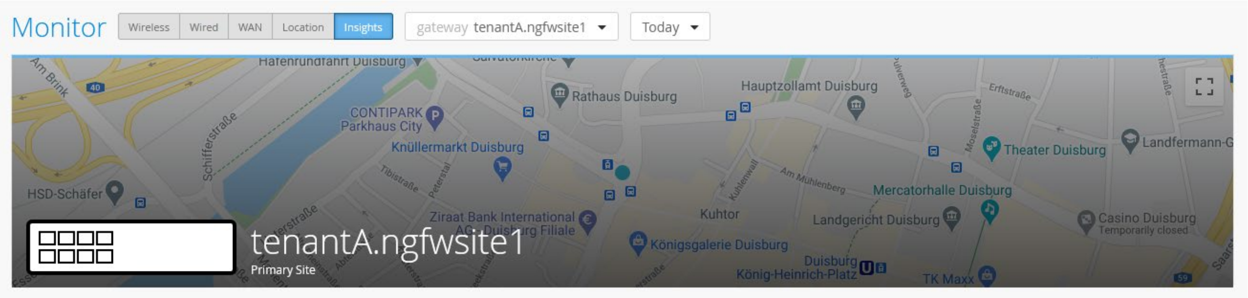


PROPERTIES

| | |
|---|---|
| INSIGHTS | WAN Edge Insights |
| LOCATION | not on floorplan |
| MAC ADDRESS | ec:38:73:9a:d4:a4 |
| MODEL | SRX345 |
| VERSION | 21.2R3-S6.11 |
| TEMPLATE | Spokes |
| HUB PROFILE | None |

## WAN Edge Insights Page

At the top of the WAN Edge Insight page, you must see the site location based information that you have configured, where this gateway is on the street map.



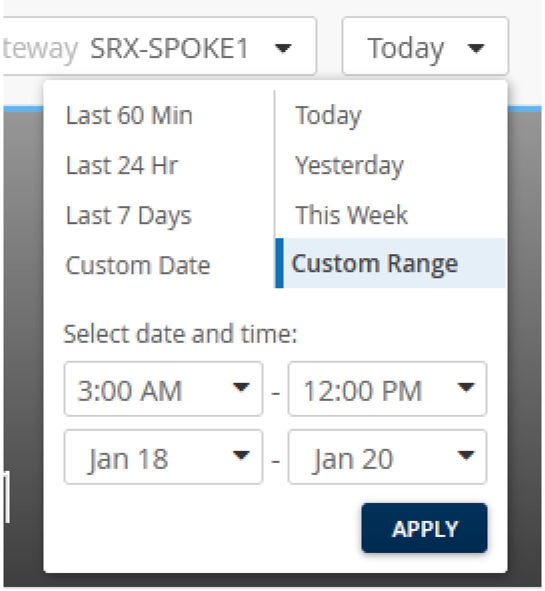
gateway tenantA.ngfwsite1

Today

tenantA.ngfwsite1

Primary Site

Also, at the top of the page, you can see the time period for information that you want to look. The default time period is **Today**.

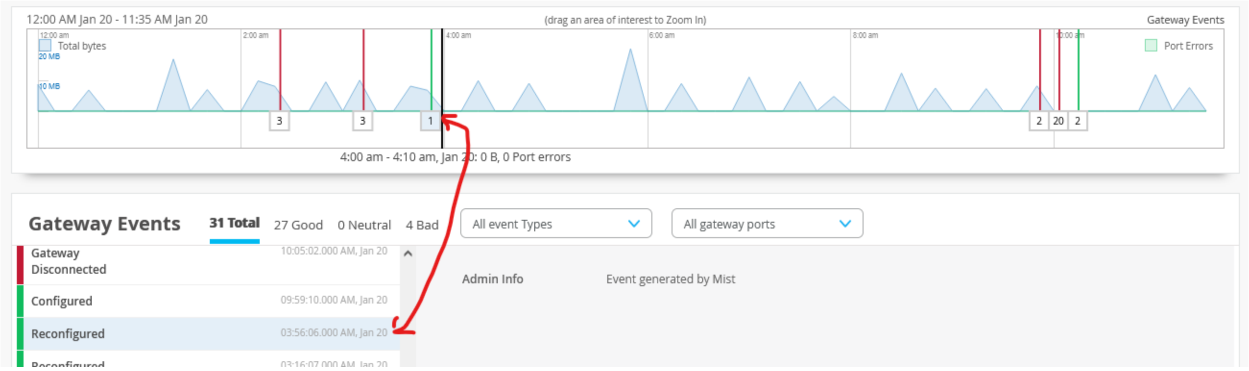


Select date and time:

3:00 AM - 12:00 PM

Jan 18 - Jan 20

Below the street map, you see the timeline for gateway events over time (and the traffic through the device at that time). With your mouse cursor, you can select an event to check, which is selected in the events reports as shown below.



Gateway Disconnected 10:05:02.000 AM, Jan 20

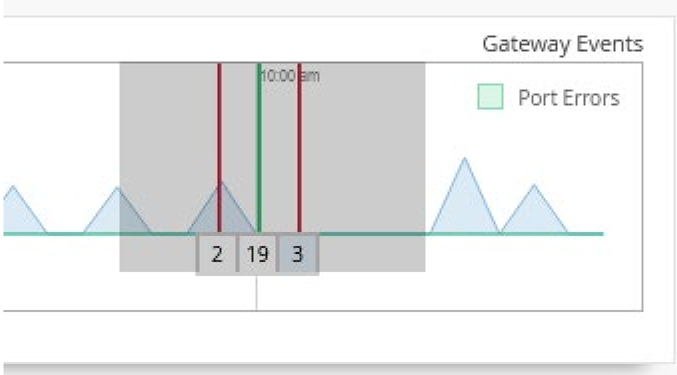
Configured 09:59:10.000 AM, Jan 20

Reconfigured 03:56:06.000 AM, Jan 20

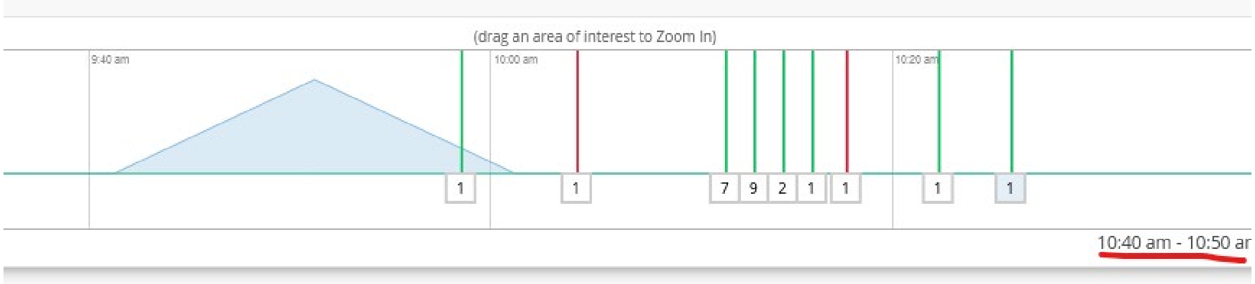
Reconfigured 03:16:07.000 AM, Jan 20

Admin Info Event generated by Mist

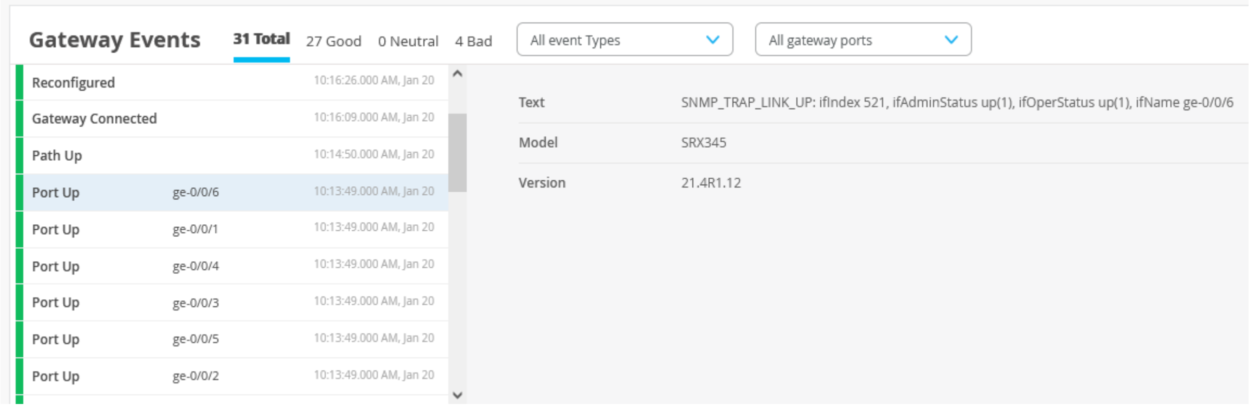
You can also zoom in by selecting an area in the timeline with your mouse cursor. Ensure the selected area is not too short).



Then, get to a more detailed view for the previous time period:



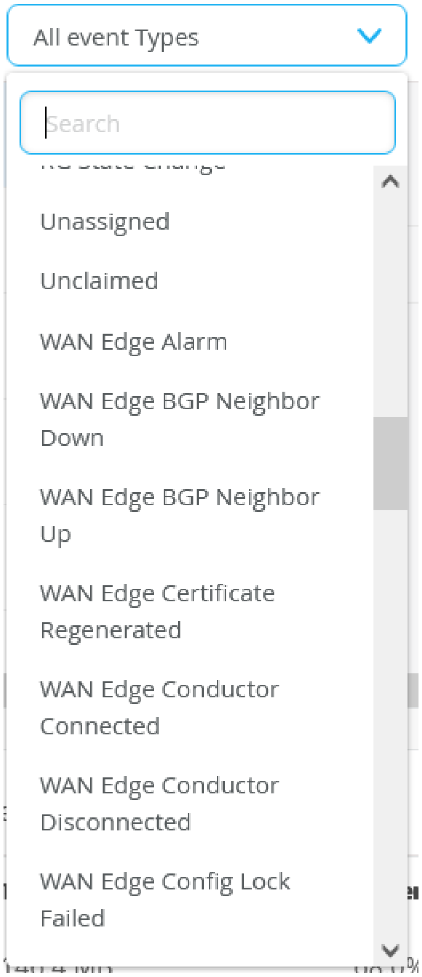
Then, review the Gateway Events Pane:



| | | |
|---|---|---|
| Reconfigured | | 10:16:26.000 AM, Jan 20 |
| Gateway Connected | | 10:16:09.000 AM, Jan 20 |
| Path Up | | 10:14:50.000 AM, Jan 20 |
| Port Up | ge-0/0/6 | 10:13:49.000 AM, Jan 20 |
| Port Up | ge-0/0/1 | 10:13:49.000 AM, Jan 20 |
| Port Up | ge-0/0/4 | 10:13:49.000 AM, Jan 20 |
| Port Up | ge-0/0/3 | 10:13:49.000 AM, Jan 20 |
| Port Up | ge-0/0/5 | 10:13:49.000 AM, Jan 20 |
| Port Up | ge-0/0/2 | 10:13:49.000 AM, Jan 20 |

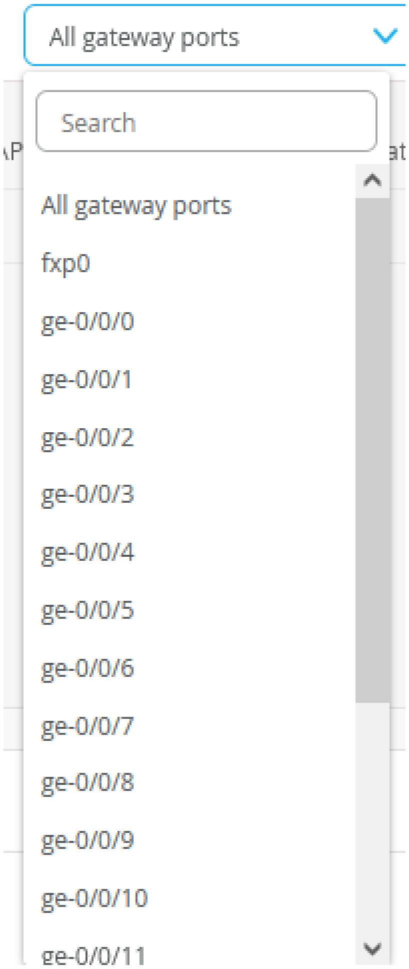
| | |
|---|---|
| Text | SNMP_TRAP_LINK_UP: ifIndex 521, ifAdminStatus up(1), ifOperStatus up(1), ifName ge-0/0/6 |
| Model | SRX345 |
| Version | 21.4R1.12 |

You can limit the event display looking after specific events as shown below:



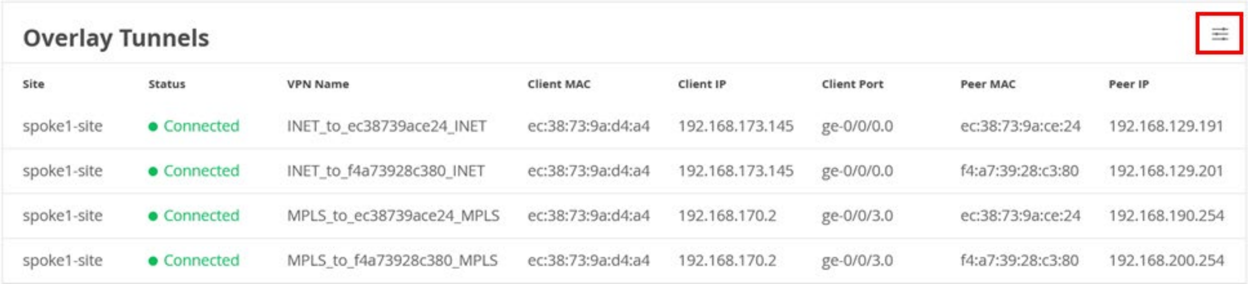
All event Types
Search
Unassigned
Unclaimed
WAN Edge Alarm
WAN Edge BGP Neighbor Down
WAN Edge BGP Neighbor Up
WAN Edge Certificate Regenerated
WAN Edge Conductor Connected
WAN Edge Conductor Disconnected
WAN Edge Config Lock Failed

You can limit the event display looking after specific ports as shown below:



Note: IPsec tunnels on a hub might show some in disconnected state due to technical reasons. You can ignore such wrong reports.

If there are IPsec based Overlay Tunnels configured on your device, they are visible in the Tunnels pane.



Overlay Tunnels

| Site | Status | VPN Name | Client MAC | Client IP | Client Port | Peer MAC | Peer IP |
|---|---|---|---|---|---|---|---|
| spoke1-site | ● Connected | INET_to_ec38739ace24_INET | ec:38:73:9a:d4:a4 | 192.168.173.145 | ge-0/0/0.0 | ec:38:73:9a:ce:24 | 192.168.129.191 |
| spoke1-site | ● Connected | INET_to_f4a73928c380_INET | ec:38:73:9a:d4:a4 | 192.168.173.145 | ge-0/0/0.0 | f4:a7:39:28:c3:80 | 192.168.129.201 |
| spoke1-site | ● Connected | MPLS_to_ec38739ace24_MPLS | ec:38:73:9a:d4:a4 | 192.168.170.2 | ge-0/0/3.0 | ec:38:73:9a:ce:24 | 192.168.190.254 |
| spoke1-site | ● Connected | MPLS_to_f4a73928c380_MPLS | ec:38:73:9a:d4:a4 | 192.168.170.2 | ge-0/0/3.0 | f4:a7:39:28:c3:80 | 192.168.200.254 |

You can have more individual information in the Tunnels Pane through the Table Settings dialog.

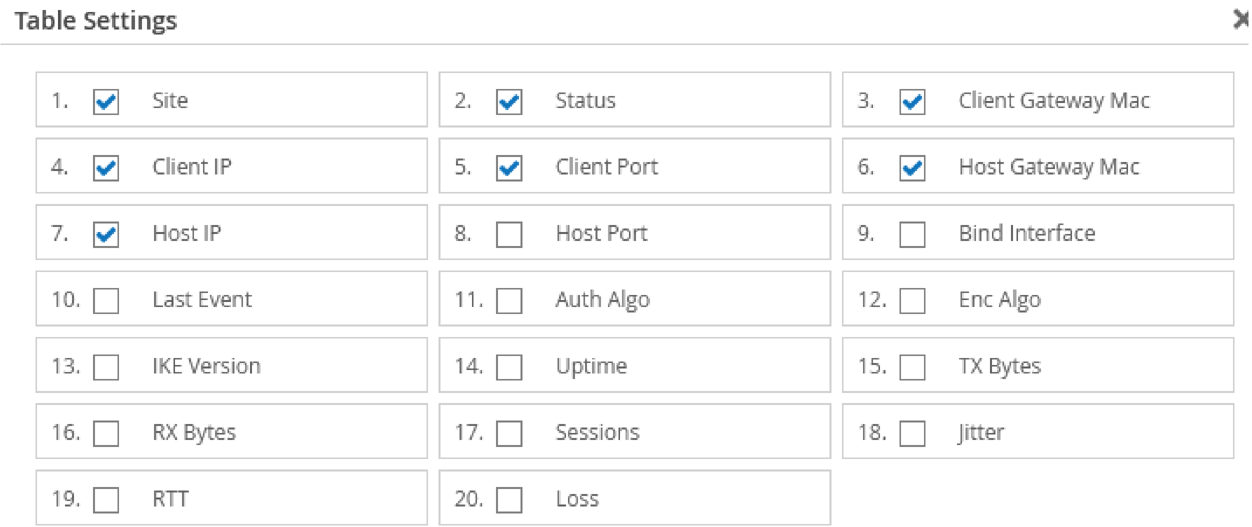
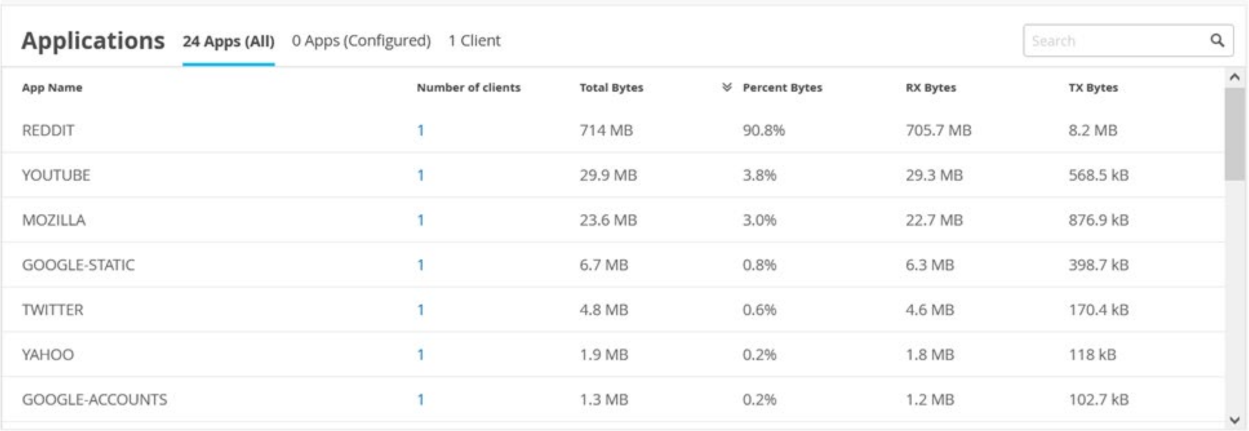


Table Settings

| | | |
|---|---|---|
| 1. ☑ Site | 2. ☑ Status | 3. ☑ Client Gateway Mac |
| 4. ☑ Client IP | 5. ☑ Client Port | 6. ☑ Host Gateway Mac |
| 7. ☑ Host IP | 8. □ Host Port | 9. □ Bind Interface |
| 10. □ Last Event | 11. □ Auth Algo | 12. □ Enc Algo |
| 13. □ IKE Version | 14. □ Uptime | 15. □ TX Bytes |
| 16. □ RX Bytes | 17. □ Sessions | 18. □ Jitter |
| 19. □ RTT | 20. □ Loss | |

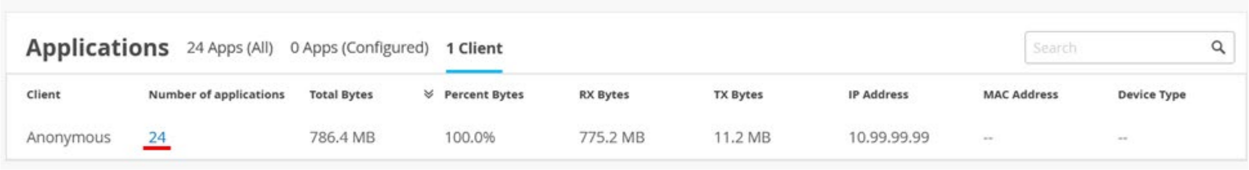
If your device is configured to send AppTrack information to the Mist cloud and you waited long enough (>1 hour after initial device adoption), you should see reports in the “Applications” Pane.



Applications 24 Apps (All) 0 Apps (Configured) 1 Client

| App Name | Number of clients | Total Bytes | Percent Bytes | RX Bytes | TX Bytes |
|---|---|---|---|---|---|
| REDDIT | 1 | 714 MB | 90.8% | 705.7 MB | 8.2 MB |
| YOUTUBE | 1 | 29.9 MB | 3.8% | 29.3 MB | 568.5 kB |
| MOZILLA | 1 | 23.6 MB | 3.0% | 22.7 MB | 876.9 kB |
| GOOGLE-STATIC | 1 | 6.7 MB | 0.8% | 6.3 MB | 398.7 kB |
| TWITTER | 1 | 4.8 MB | 0.6% | 4.6 MB | 170.4 kB |
| YAHOO | 1 | 1.9 MB | 0.2% | 1.8 MB | 118 kB |
| GOOGLE-ACCOUNTS | 1 | 1.3 MB | 0.2% | 1.2 MB | 102.7 kB |

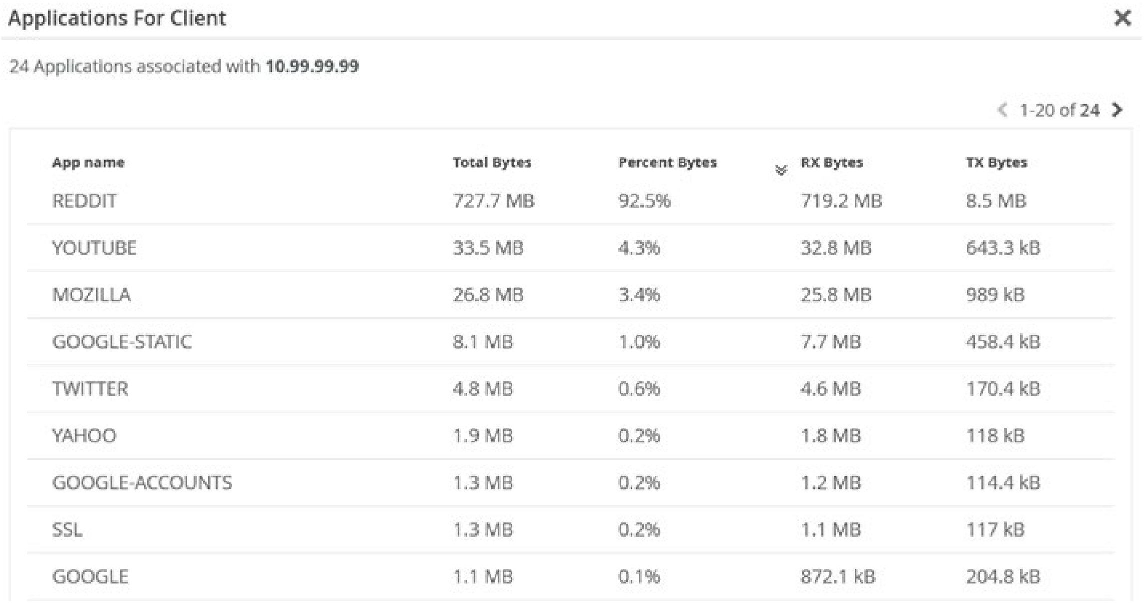
Through the Clients-tab, you can see who is using how much bandwidth.



Applications 24 Apps (All) 0 Apps (Configured) 1 Client

| Client | Number of applications | Total Bytes | Percent Bytes | RX Bytes | TX Bytes | IP Address | MAC Address | Device Type |
|---|---|---|---|---|---|---|---|---|
| Anonymous | 24 | 786.4 MB | 100.0% | 775.2 MB | 11.2 MB | 10.99.99.99 | -- | -- |

Click on the client to further drill down  to see which applications are used.



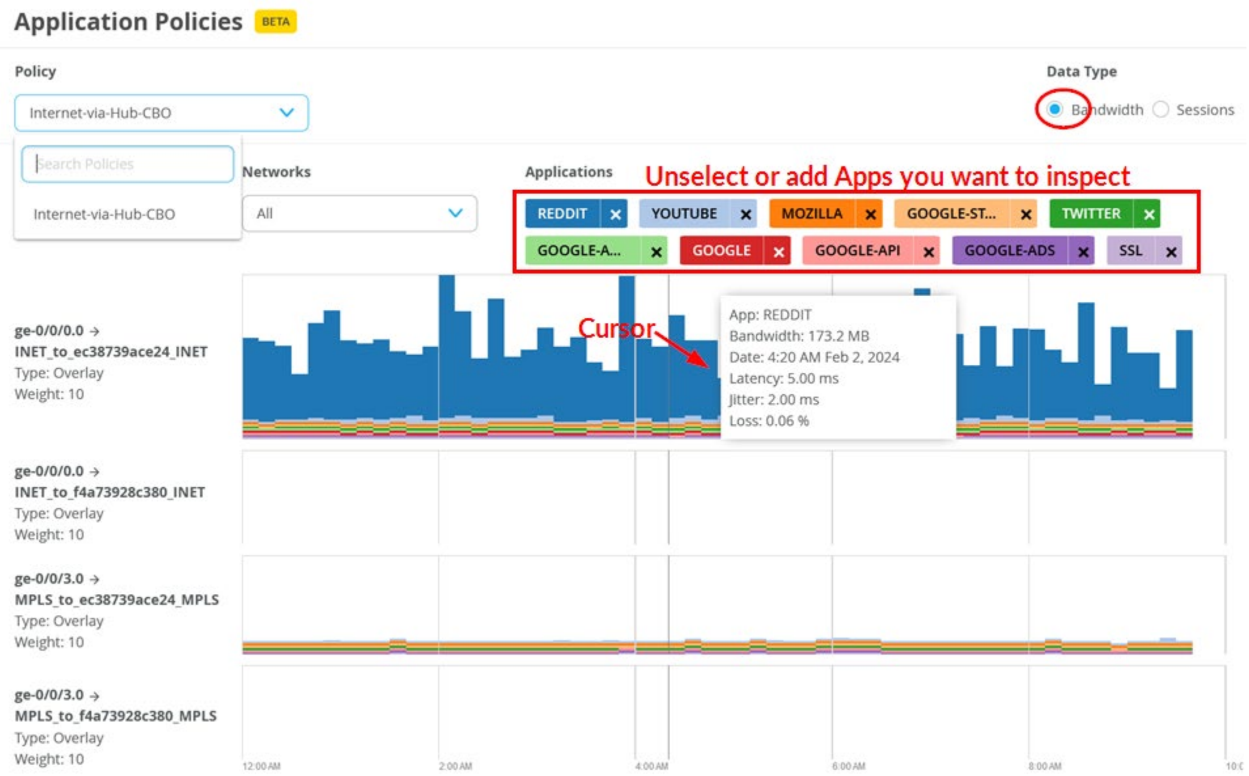
Applications For Client

24 Applications associated with **10.99.99.99**

| App name | Total Bytes | Percent Bytes | RX Bytes | TX Bytes |
|---|---|---|---|---|
| REDDIT | 727.7 MB | 92.5% | 719.2 MB | 8.5 MB |
| YOUTUBE | 33.5 MB | 4.3% | 32.8 MB | 643.3 kB |
| MOZILLA | 26.8 MB | 3.4% | 25.8 MB | 989 kB |
| GOOGLE-STATIC | 8.1 MB | 1.0% | 7.7 MB | 458.4 kB |
| TWITTER | 4.8 MB | 0.6% | 4.6 MB | 170.4 kB |
| YAHOO | 1.9 MB | 0.2% | 1.8 MB | 118 kB |
| GOOGLE-ACCOUNTS | 1.3 MB | 0.2% | 1.2 MB | 114.4 kB |
| SSL | 1.3 MB | 0.2% | 1.1 MB | 117 kB |
| GOOGLE | 1.1 MB | 0.1% | 872.1 kB | 204.8 kB |

Next is the new Application Policies pane with information about the usage of each application on the individual paths of your SD-WAN infrastructure:

- Policy allows you to set a filter on the configured application policies.
- Network allows to review all LAN networks or a single one.
- Applications allow you to deselect or add applications you are interested.
- Data Type allows you to review the application bandwidth , or the amount of session opened.
- Bubble allows you to view more details. You must move the cursor over the application in a path to get a bubble.

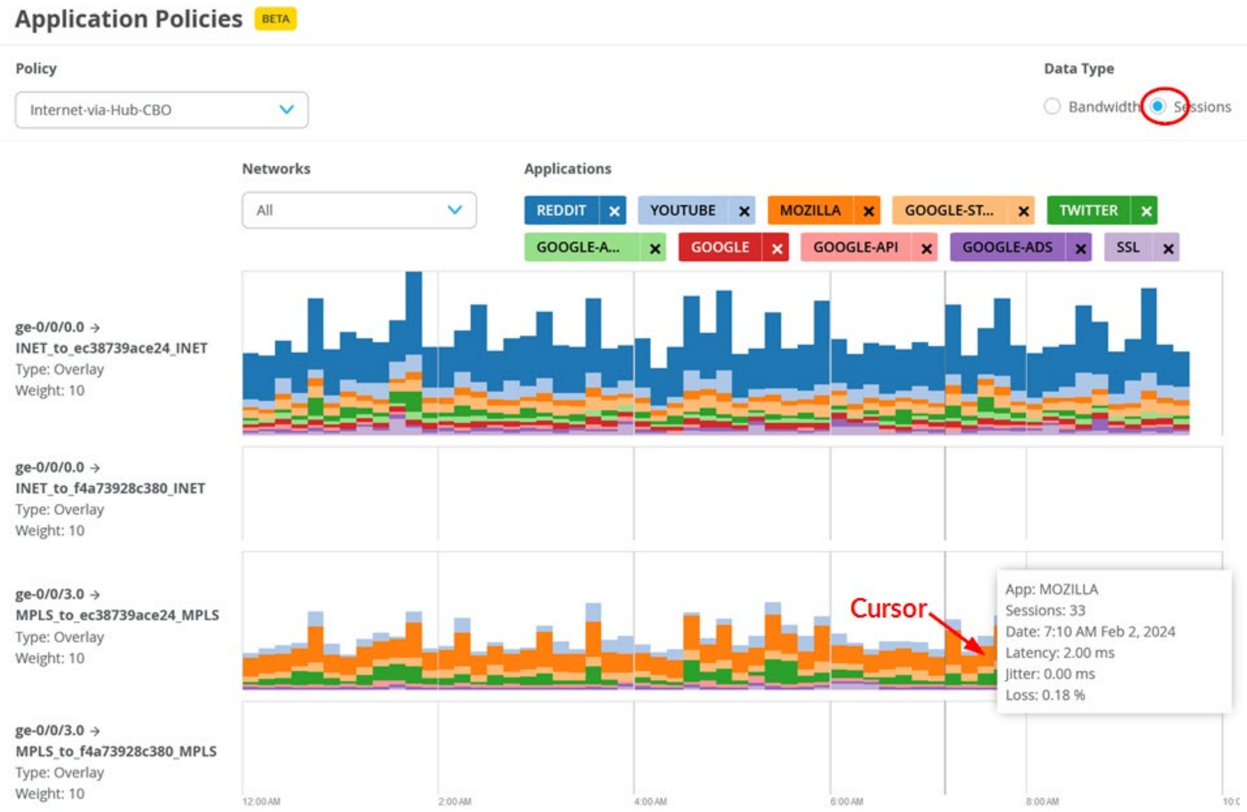


Unselect or add Apps you want to inspect

Cursor

App: REDDIT
Bandwidth: 173.2 MB
Date: 4:20 AM Feb 2, 2024
Latency: 5.00 ms
Jitter: 2.00 ms
Loss: 0.06 %

Here is the same view again. But we selected to review the session amount.

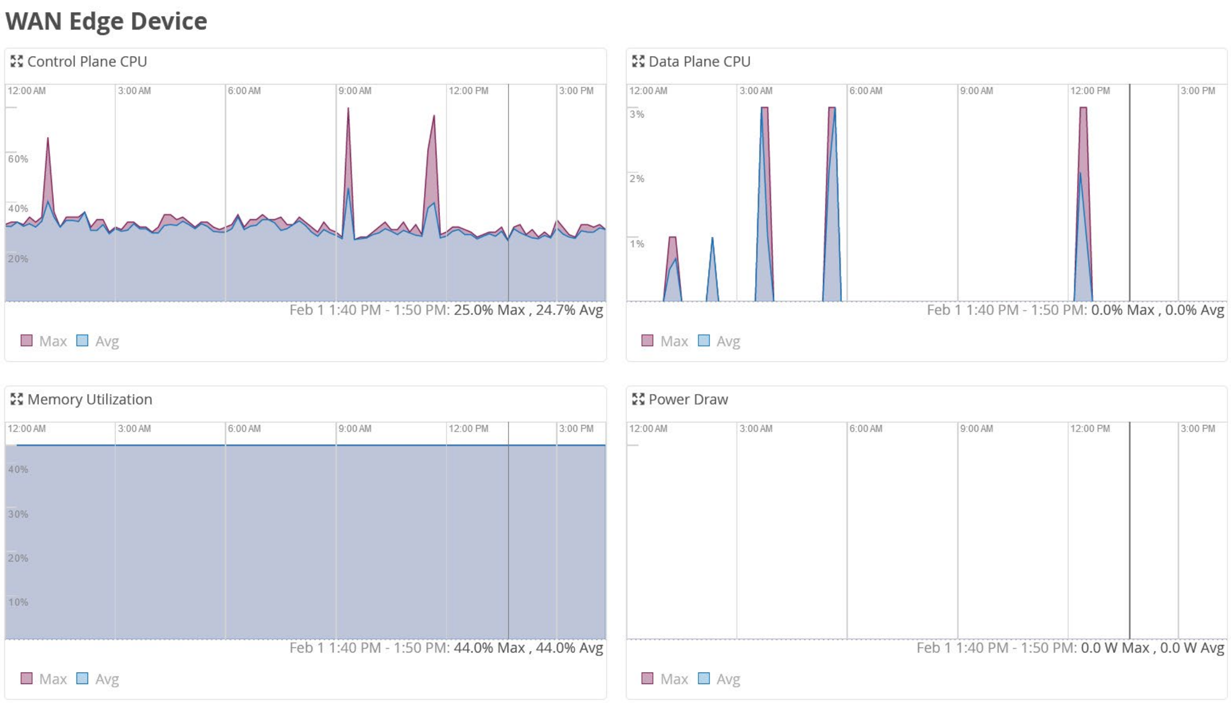


Cursor

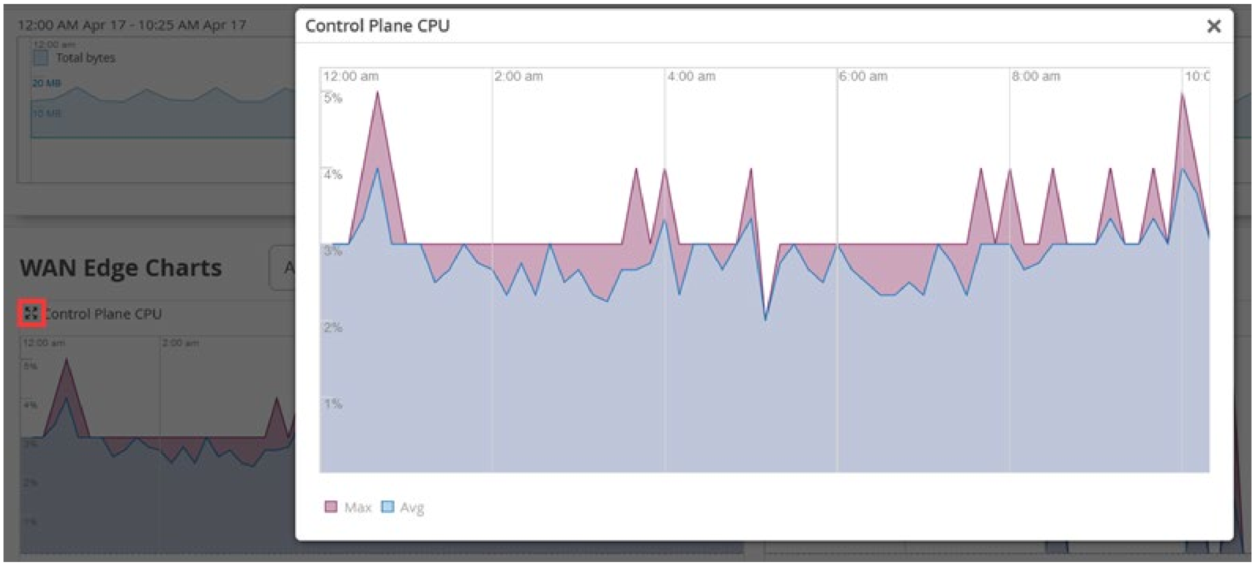
App: MOZILLA
Sessions: 33
Date: 7:10 AM Feb 2, 2024
Latency: 2.00 ms
Jitter: 0.00 ms
Loss: 0.18 %

Next is the WAN Edge Device pane with the four charts:

- Control Plane CPU
- Data Plane CPU
- Memory Utilization
- Power Draw

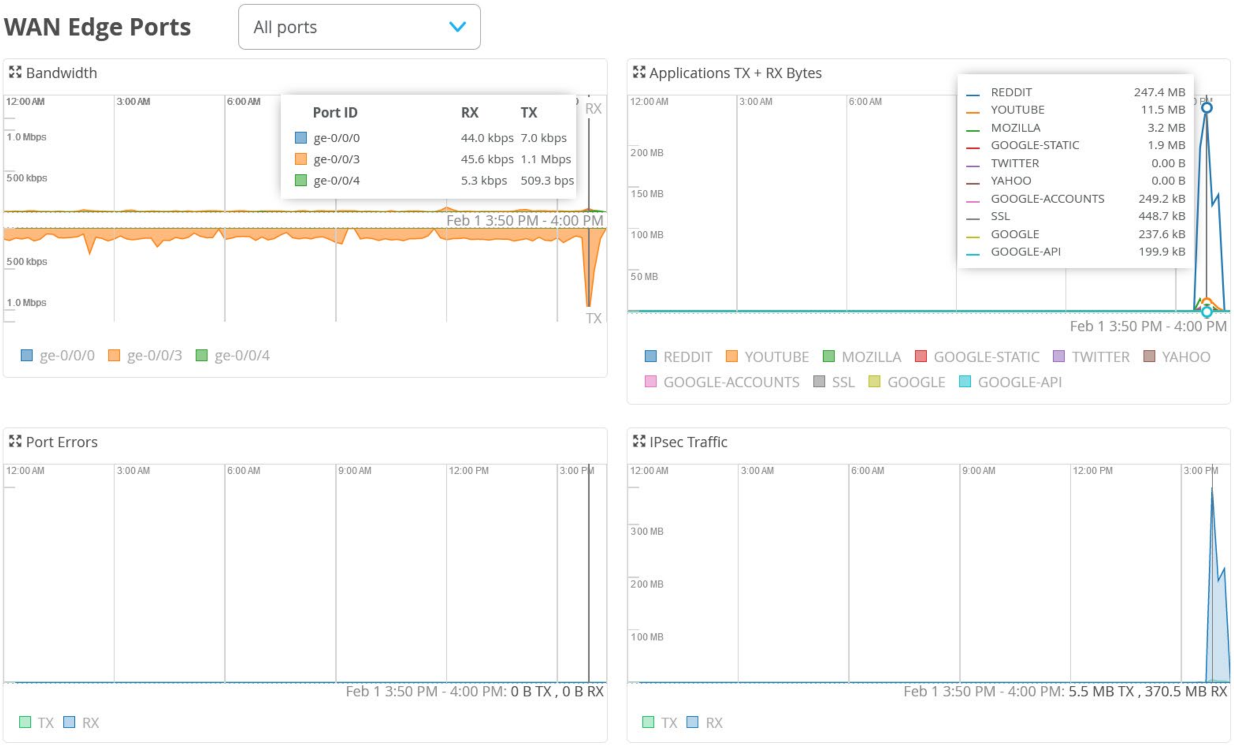

WAN Edge Device
Control Plane CPU
12:00 AM
3:00 AM
6:00 AM
9:00 AM
12:00 PM
3:00 PM
60%
40%
20%
Feb 1 1:40 PM - 1:50 PM: 25.0% Max , 24.7% Avg
Max
Avg
Data Plane CPU
3%
2%
1%
Feb 1 1:40 PM - 1:50 PM: 0.0% Max , 0.0% Avg
Max
Avg
Memory Utilization
40%
30%
20%
10%
Feb 1 1:40 PM - 1:50 PM: 44.0% Max , 44.0% Avg
Max
Avg
Power Draw
Feb 1 1:40 PM - 1:50 PM: 0.0 W Max , 0.0 W Avg
Max
Avg

Click on the highlighted icon to get a bigger chart as shown below:



Next is the WAN Edge Ports pane with the four charts about:

- Bandwidth
- Application TX + RX Bytes
- Port Errors
- IPsec Traffic



| | Port ID | RX | TX |
|---|---|---|---|
| 🟦 | ge-0/0/0 | 44.0 kbps | 7.0 kbps |
| 🟧 | ge-0/0/3 | 45.6 kbps | 1.1 Mbps |
| 🟩 | ge-0/0/4 | 5.3 kbps | 509.3 bps |

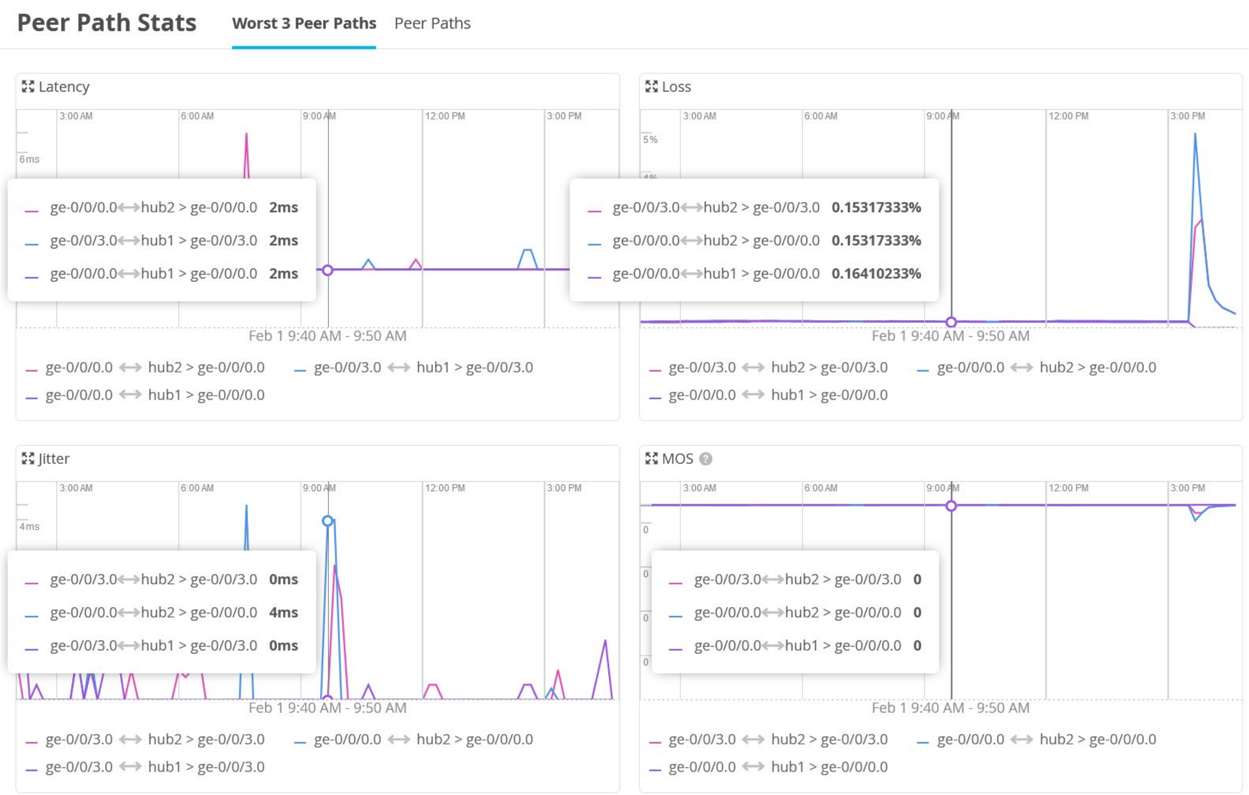
Feb 1 3:50 PM - 4:00 PM

| | | |
|---|---|---|
| — | REDDIT | 247.4 MB |
| — | YOUTUBE | 11.5 MB |
| — | MOZILLA | 3.2 MB |
| — | GOOGLE-STATIC | 1.9 MB |
| — | TWITTER | 0.00 B |
| — | YAHOO | 0.00 B |
| — | GOOGLE-ACCOUNTS | 249.2 kB |
| — | SSL | 448.7 kB |
| — | GOOGLE | 237.6 kB |
| — | GOOGLE-API | 199.9 kB |

Feb 1 3:50 PM - 4:00 PM

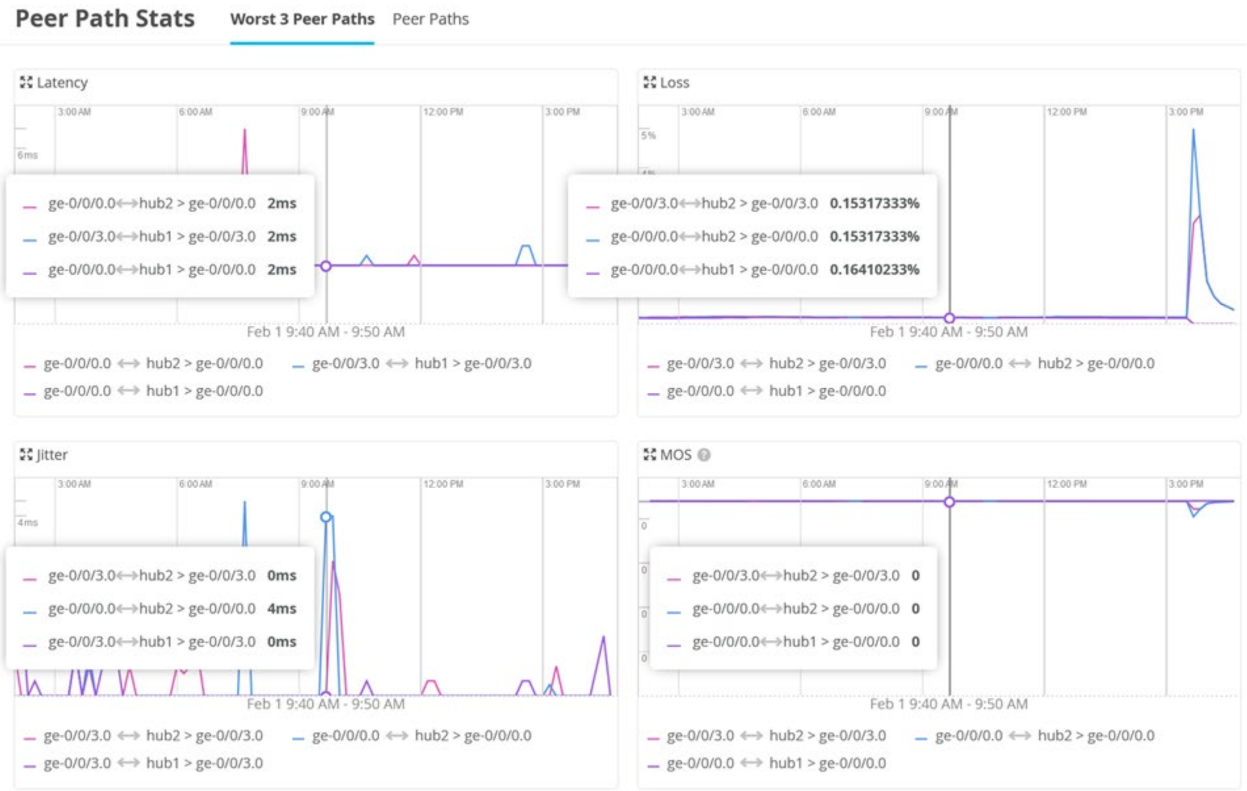
Feb 1 3:50 PM - 4:00 PM: 0 B TX , 0 B RX

Feb 1 3:50 PM - 4:00 PM: 5.5 MB TX , 370.5 MB RX

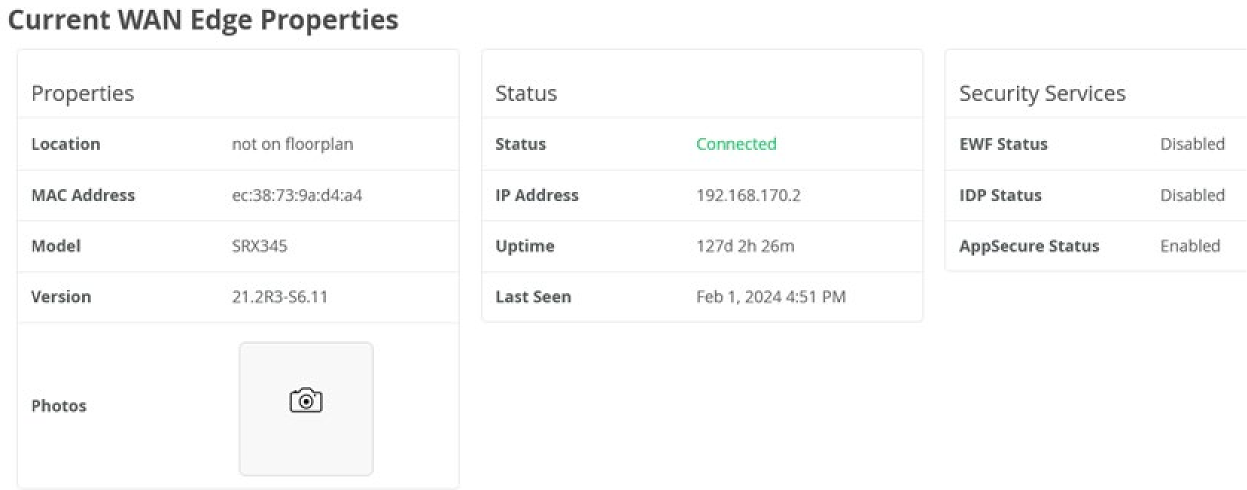

Peer Path Stats
Worst 3 Peer Paths
Peer Paths
Latency
6ms
3:00 AM
6:00 AM
9:00 AM
12:00 PM
3:00 PM
ge-0/0/0.0⟷hub2 > ge-0/0/0.0 2ms
ge-0/0/3.0⟷hub1 > ge-0/0/3.0 2ms
ge-0/0/0.0⟷hub1 > ge-0/0/0.0 2ms
Feb 1 9:40 AM - 9:50 AM
ge-0/0/0.0 ⟷ hub2 > ge-0/0/0.0
ge-0/0/3.0 ⟷ hub1 > ge-0/0/3.0
ge-0/0/0.0 ⟷ hub1 > ge-0/0/0.0
Loss
5%
ge-0/0/3.0⟷hub2 > ge-0/0/3.0 0.15317333%
ge-0/0/0.0⟷hub2 > ge-0/0/0.0 0.15317333%
ge-0/0/0.0⟷hub1 > ge-0/0/0.0 0.16410233%
Feb 1 9:40 AM - 9:50 AM
ge-0/0/3.0 ⟷ hub2 > ge-0/0/3.0
ge-0/0/0.0 ⟷ hub2 > ge-0/0/0.0
ge-0/0/0.0 ⟷ hub1 > ge-0/0/0.0
Jitter
4ms
ge-0/0/3.0⟷hub2 > ge-0/0/3.0 0ms
ge-0/0/0.0⟷hub2 > ge-0/0/0.0 4ms
ge-0/0/3.0⟷hub1 > ge-0/0/3.0 0ms
Feb 1 9:40 AM - 9:50 AM
ge-0/0/3.0 ⟷ hub2 > ge-0/0/3.0
ge-0/0/0.0 ⟷ hub2 > ge-0/0/0.0
ge-0/0/3.0 ⟷ hub1 > ge-0/0/3.0
MOS
0
0
0
0
ge-0/0/3.0⟷hub2 > ge-0/0/3.0 0
ge-0/0/0.0⟷hub2 > ge-0/0/0.0 0
ge-0/0/0.0⟷hub1 > ge-0/0/0.0 0
Feb 1 9:40 AM - 9:50 AM
ge-0/0/3.0 ⟷ hub2 > ge-0/0/3.0
ge-0/0/0.0 ⟷ hub2 > ge-0/0/0.0
ge-0/0/0.0 ⟷ hub1 > ge-0/0/0.0

Next is the Peer Path Stats pane with the four charts about:

- Latency
- Loss
- Jitter
- MOS (Mean Opinion Score)



Then, the last pane on this page with information is **Current WAN Edge Properties**.



Current WAN Edge Properties

Properties

| | |
|---|---|
| Location | not on floorplan |
| MAC Address | ec:38:73:9a:d4:a4 |
| Model | SRX345 |
| Version | 21.2R3-S6.11 |
| Photos | |

Status

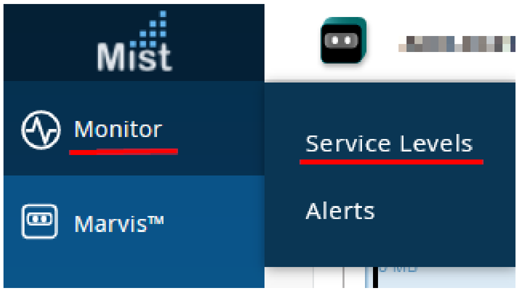
| | |
|---|---|
| Status | Connected |
| IP Address | 192.168.170.2 |
| Uptime | 127d 2h 26m |
| Last Seen | Feb 1, 2024 4:51 PM |

Security Services

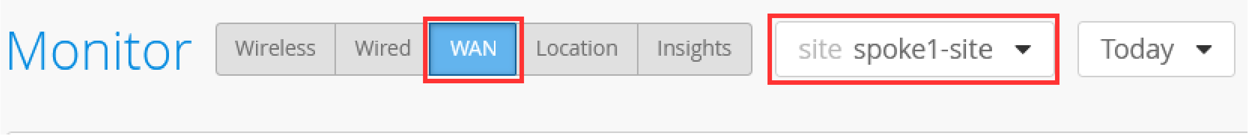
| | |
|---|---|
| EWF Status | Disabled |
| IDP Status | Disabled |
| AppSecure Status | Enabled |

## WAN SLE Monitor Page

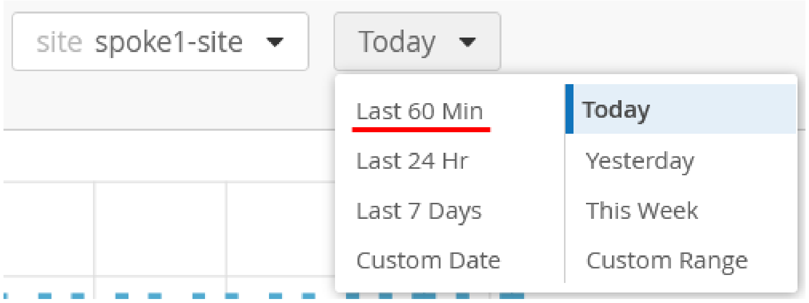
The next level of information is regarding WAN SLE monitoring. To review the information, click **Monitor** > **Service Levels**.



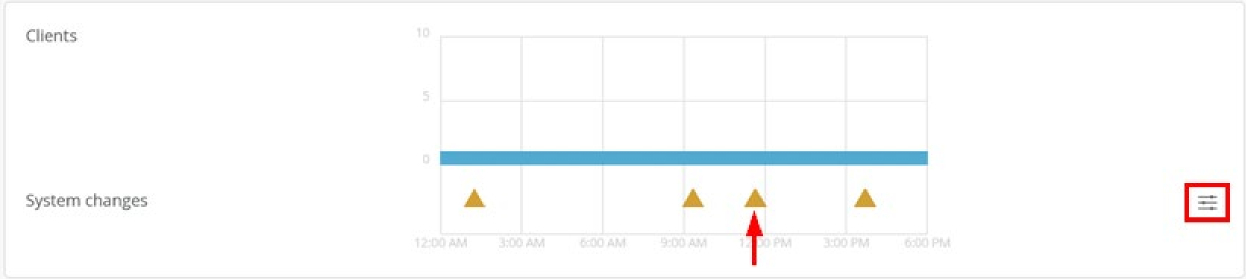
Then select a site for inspection and select “WAN”.



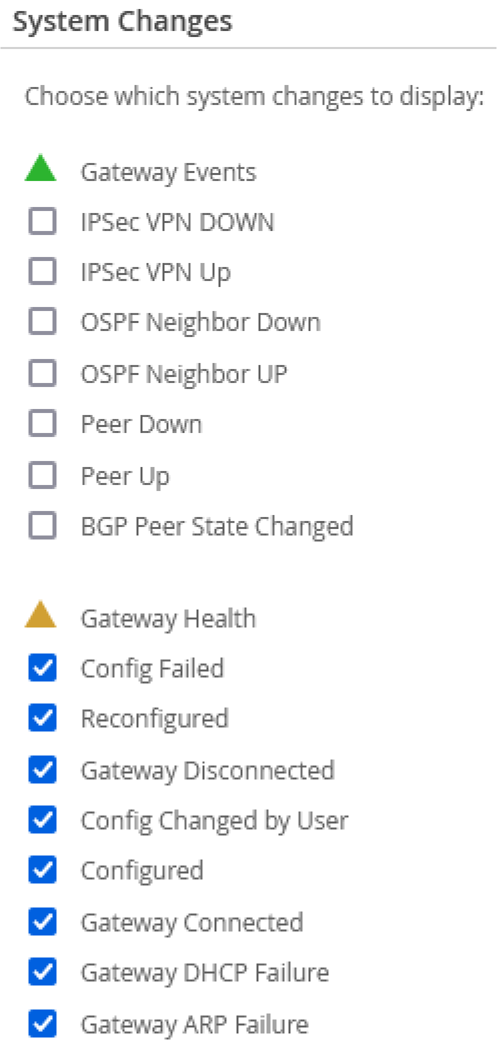
Ensure that **all WAN SLE metrics are about monitoring a device for a long period of time**! They may not display much after you’ve just onboarded the device. In a production environment, it is expected to have a full week of information about the device! You can try to change the period, for example **Last 60 Min**. But it might not represent much information yet.



The first pane gives you a relationship about number of collected clients at a point in time and system events that occurred then. You can see the amber triangle when something is changed. Also, make yourself familiar with the ability to see what is reported at the lower-right corner of the pane.



You can select which system changes should be used and displayed.



System Changes

Choose which system changes to display:

▲ Gateway Events

□ IPSec VPN DOWN

□ IPSec VPN Up

□ OSPF Neighbor Down

□ OSPF Neighbor UP

□ Peer Down

□ Peer Up

□ BGP Peer State Changed

▲ Gateway Health

☑ Config Failed

☑ Reconfigured

☑ Gateway Disconnected

☑ Config Changed by User

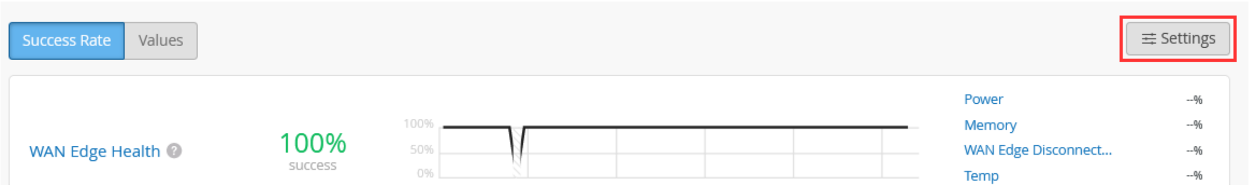
☑ Configured

☑ Gateway Connected

☑ Gateway DHCP Failure

☑ Gateway ARP Failure

Back to the WAN SLE page also make yourself familiar with the **Settings** at the top-right corner.

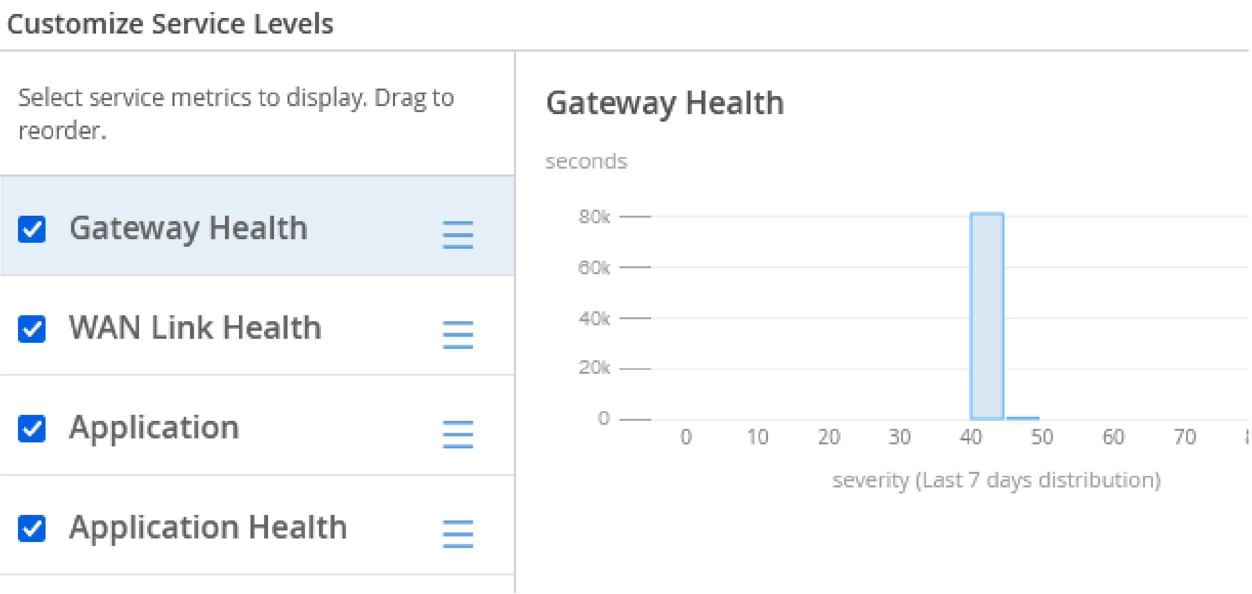


WAN Edge Health

100%
success

| | |
|---|---|
| Power | --% |
| Memory | --% |
| WAN Edge Disconnect... | --% |
| Temp | --% |

The most important customization you can do after you click  Settings is to set applications for Application SLE. For more information on setting applications using Application SLE, see **Application SLE**.



Customize Service Levels

Select service metrics to display. Drag to reorder.

☑ Gateway Health

☑ WAN Link Health

☑ Application

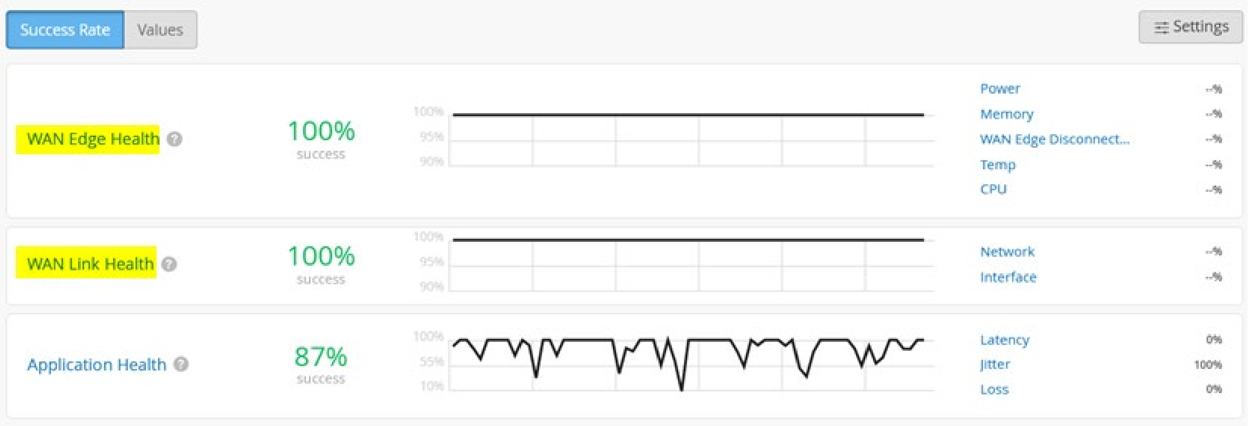
☑ Application Health

Note: It is critical to understand that the metrics and reports for WAN Edge Health, WAN Link Health, and Application Health are based on Mist AI utilizing a TensorFlow-Network. This means:

1. As with all AIs, it needs large portions of data for analysis to be trained about your network and make good choices. We recommend you wait a week after the spoke is installed and run traffic though it before you inspect.

2. Unlike a traditional monitoring tool displaying you a chart and then you must determine if something is good or bad the system, through AI, gathers a sense of the healthiness of your network and only display items that are at risk. If you do not see any report, the network health is good, and you do not need to review.

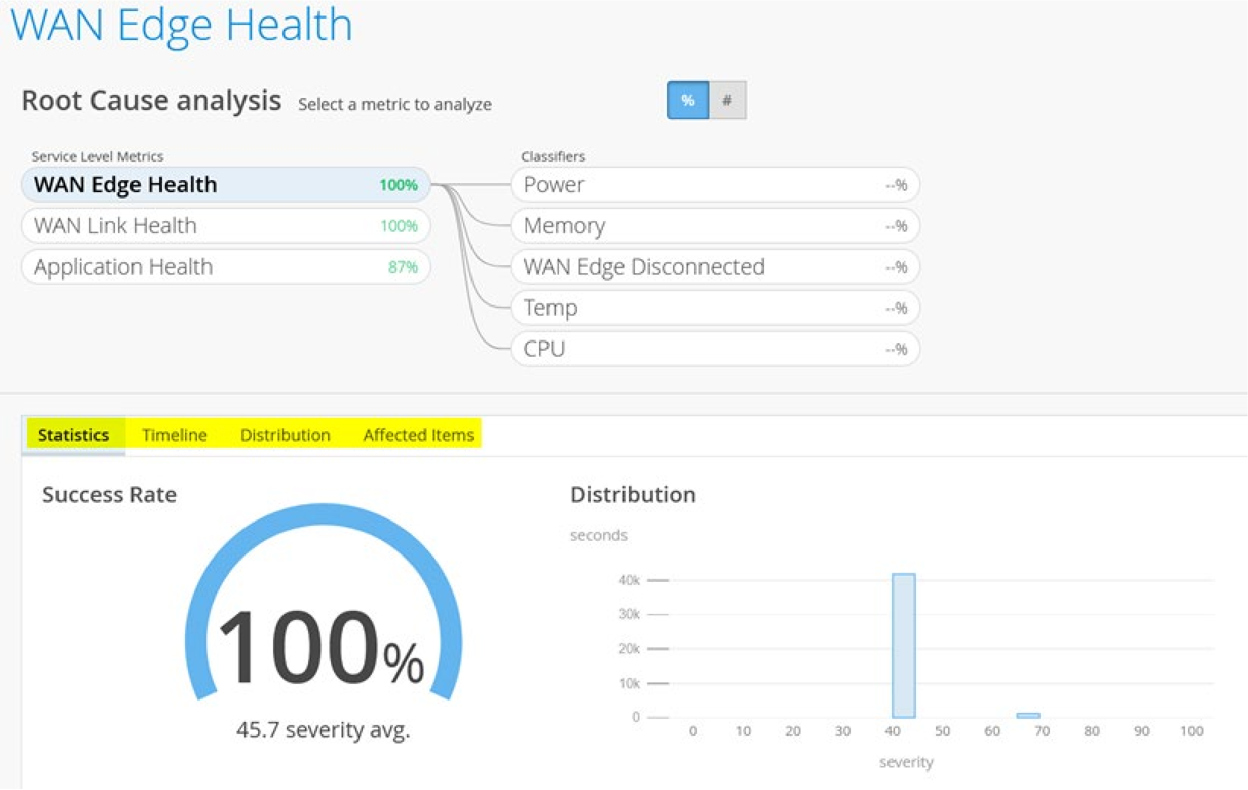
Let’s focus on the reports you can get through WAN Edge Health and WAN Link Health in this chapter.



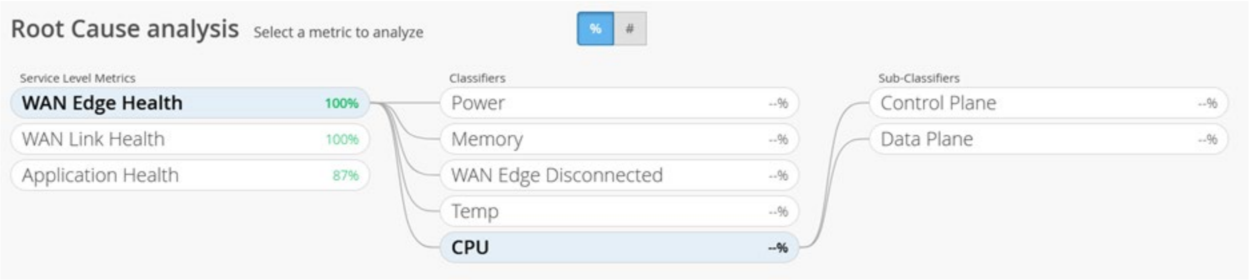
WAN Edge Health reports the health check of the SRX Series device deployed with metrics/classifiers such as:

- Power draw
- Memory usage
- WAN Edge Disconnected
- Temperature
- CPU utilization

Below you see an example chart. Look at the tabs for more granular information.

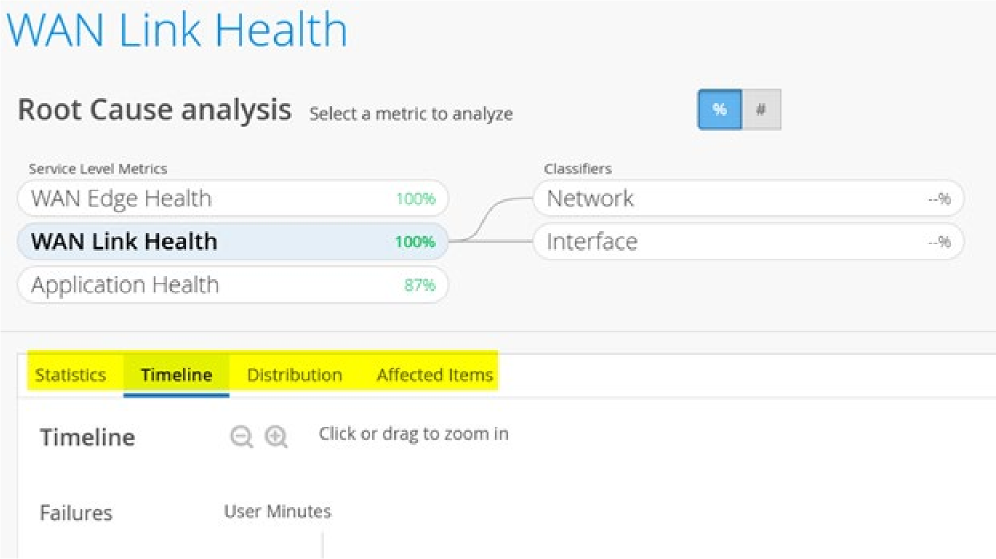


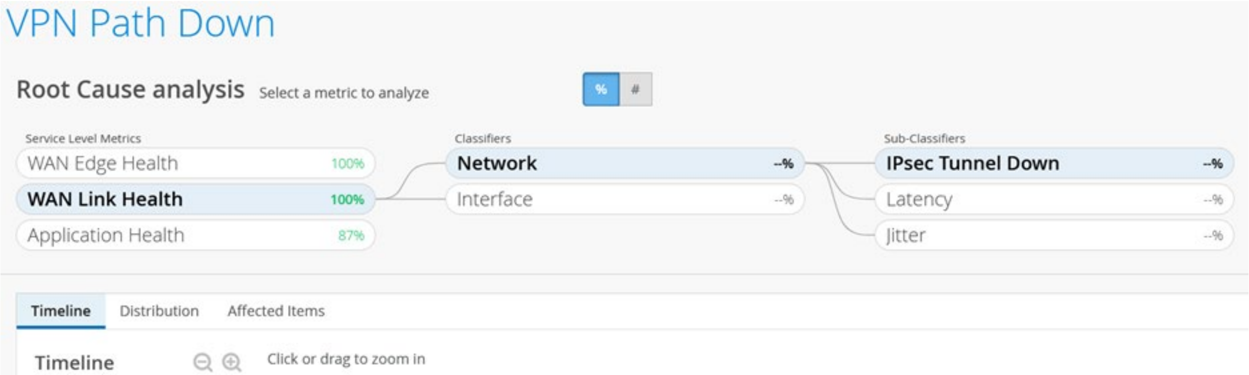
Temperature and CPU utilization have sub-classifiers as shown in the example below.



WAN Link Health reports the health check of the SRX Series device deployed with metrics/classifiers such as:

- Network
  - IPsec Tunnel Down
  - Latency
  - Jitter
- Interface
  - Cable Issues
  - Congestion
  - VPN





VPN Path Down

Root Cause analysis Select a metric to analyze

Service Level Metrics

- WAN Edge Health 100%
- **WAN Link Health 100%**
- Application Health 87%

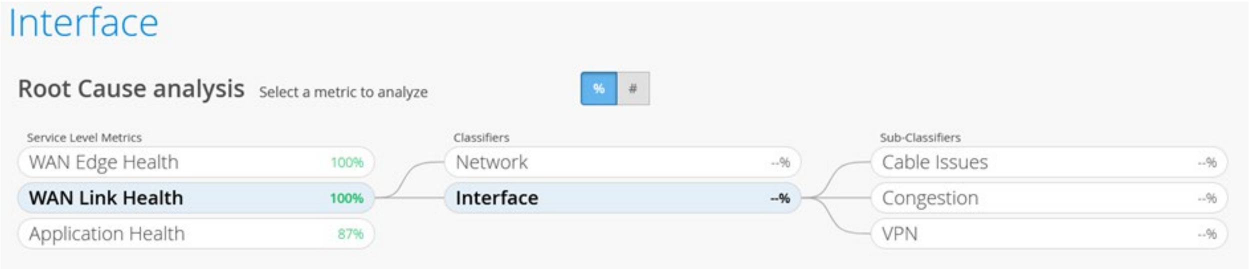
Classifiers

- **Network --%**
- Interface --%

Sub-Classifiers

- **IPsec Tunnel Down --%**
- Latency --%
- Jitter --%

Timeline Click or drag to zoom in



Interface

Root Cause analysis Select a metric to analyze

Service Level Metrics

- WAN Edge Health 100%
- **WAN Link Health 100%**
- Application Health 87%

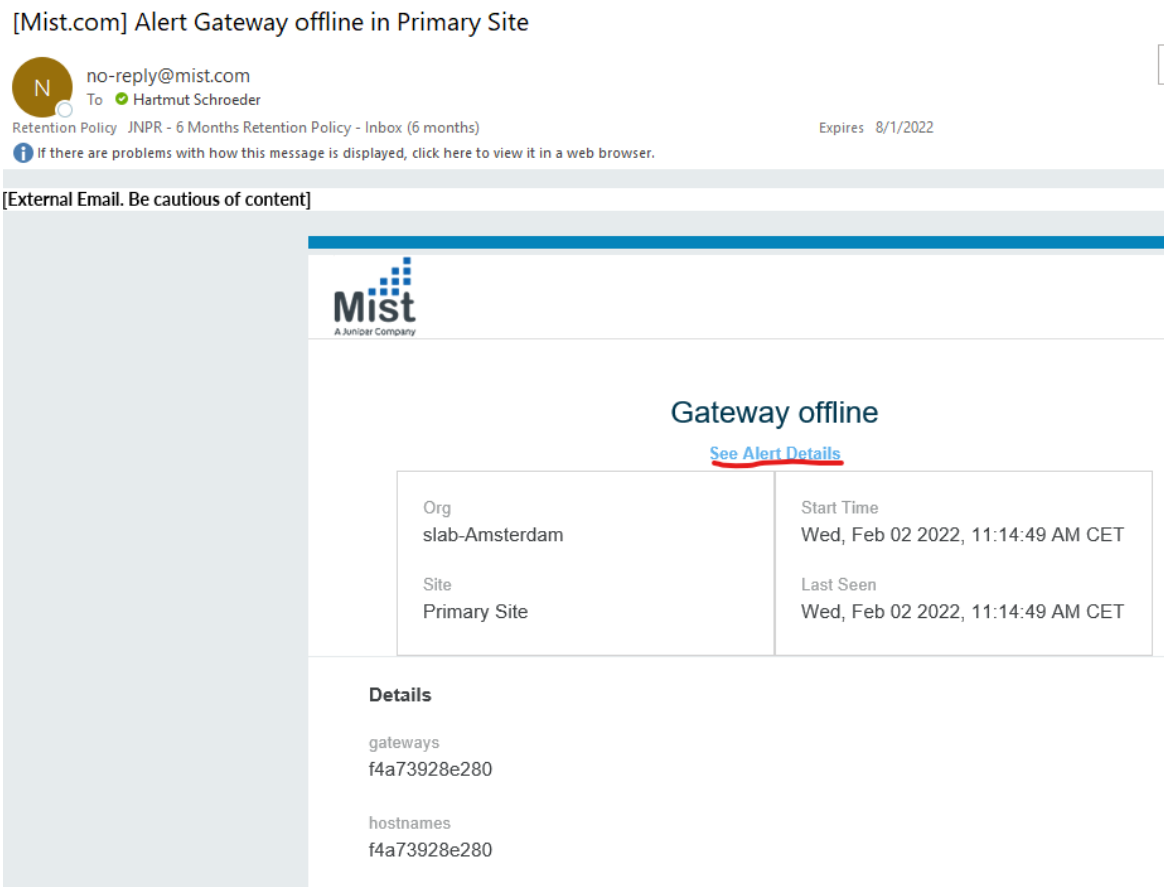
Classifiers

- Network --%
- **Interface --%**

Sub-Classifiers

- Cable Issues --%
- Congestion --%
- VPN --%

NOTE: Reports on SLEs are only made visible if there is a concern and you need to review. If you want charts on raw data without the benefit of an AI based analysis, see the Device page for **WAN Edge Insights Page**.



[Mist.com] Alert Gateway offline in Primary Site

no-reply@mist.com

To Hartmut Schroeder

Retention Policy JNPR - 6 Months Retention Policy - Inbox (6 months) Expires 8/1/2022

If there are problems with how this message is displayed, click here to view it in a web browser.

[External Email. Be cautious of content]

Gateway offline

See Alert Details

Org
slab-Amsterdam

Site
Primary Site

Start Time
Wed, Feb 02 2022, 11:14:49 AM CET

Last Seen
Wed, Feb 02 2022, 11:14:49 AM CET

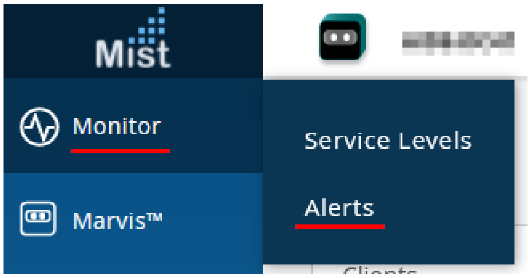
Details

gateways
f4a73928e280

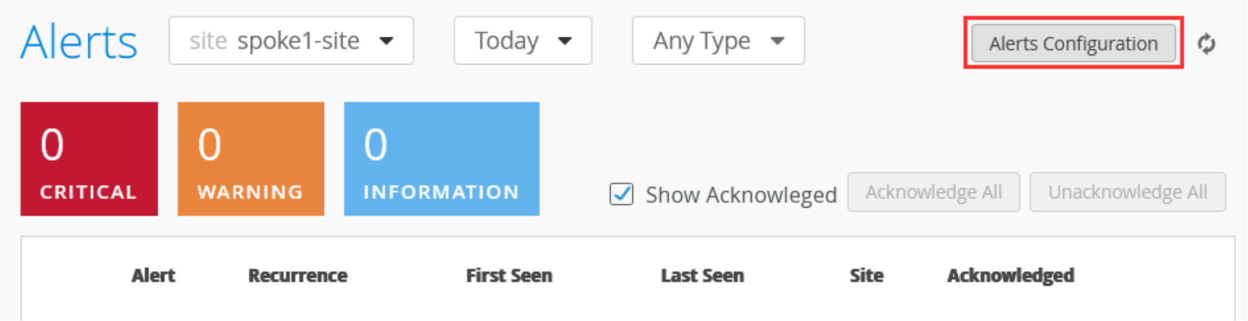
hostnames
f4a73928e280

## Alerts Page

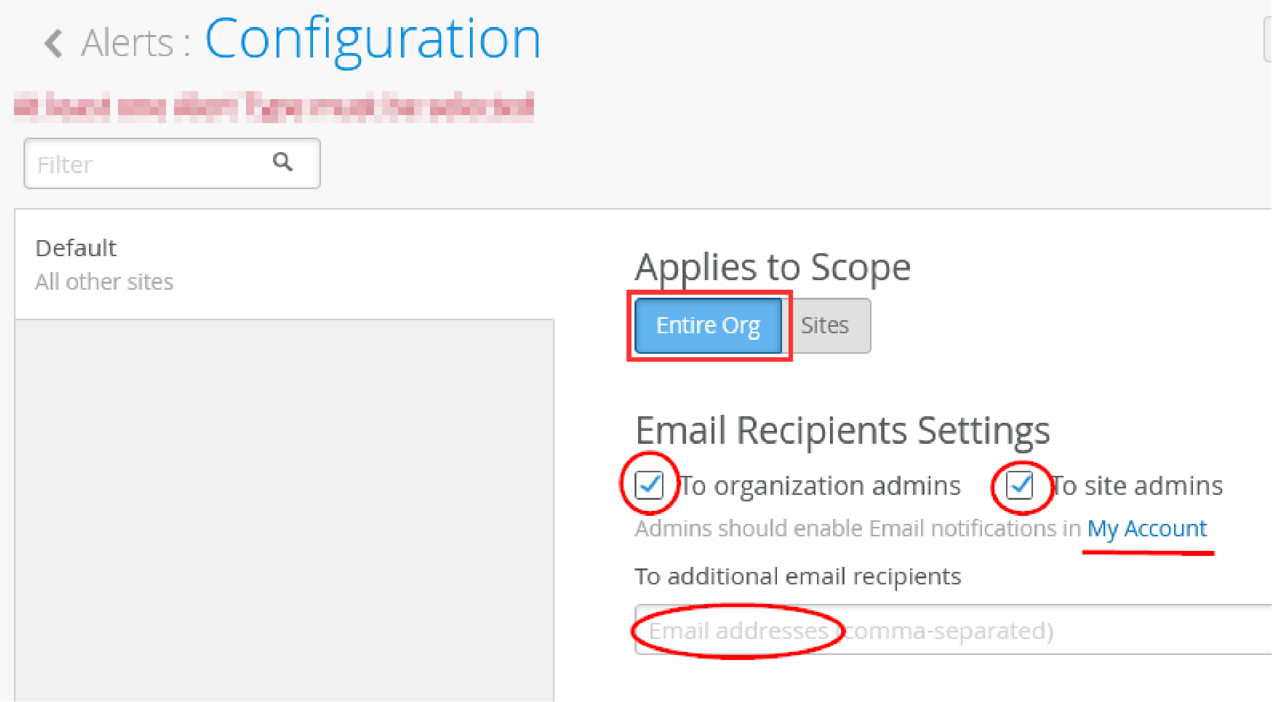
With this test case, we demonstrate the ability to see Alarms for gateways and get those as E-mail to the Administrator. To do this, go to **Monitor** > **Alerts**.



Review the current page and click Alerts Configuration.



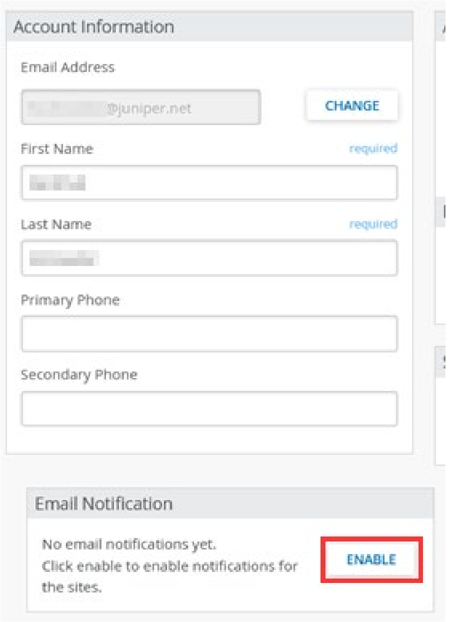
Under Configuration, enable the reporting default for Scope=**Entire Org**, **To Organization admins**, and To **site admins**. You can either add your E-mail address to the To additional email recipients field or click **My Account** to verify your settings.



Alerts : Configuration
[redacted]
Filter
Default
All other sites
Applies to Scope
Entire Org
Sites
Email Recipients Settings
☑ To organization admins
☑ To site admins
Admins should enable Email notifications in My Account
To additional email recipients
Email addresses (comma-separated)

> Note: If you are an admin, the default setting is not to send you any E-mails. Enable to receive the E-mails.

If you have followed the My Account link, click **Enable** under Email Notification.



Account Information

Email Address

[redacted]@juniper.net

CHANGE

First Name required

[redacted]

Last Name required

[redacted]

Primary Phone

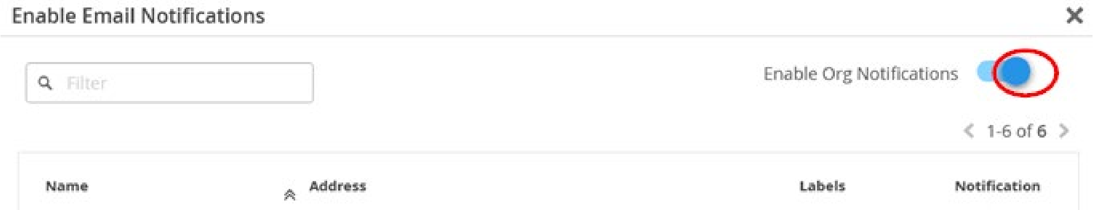
Secondary Phone

Email Notification

No email notifications yet. Click enable to enable notifications for the sites.

ENABLE

You can enable notifications on a site-by-site basis. But for now, enable **Enable Org Notifications** as shown below.



Enable Email Notifications ✕

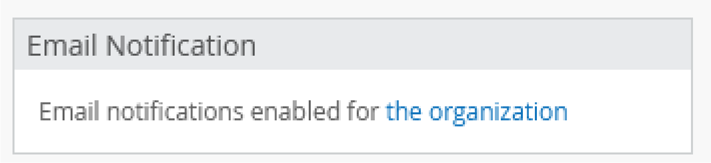
Filter

Enable Org Notifications ●

‹ 1-6 of 6 ›

| Name | Address | Labels | Notification |
|---|---|---|---|

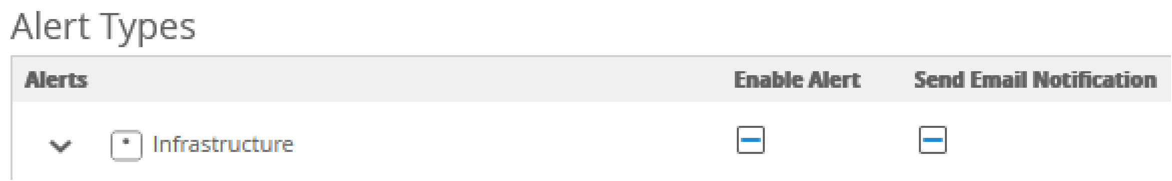
Your account E-mail notification setting might look as shown below.



Email Notification

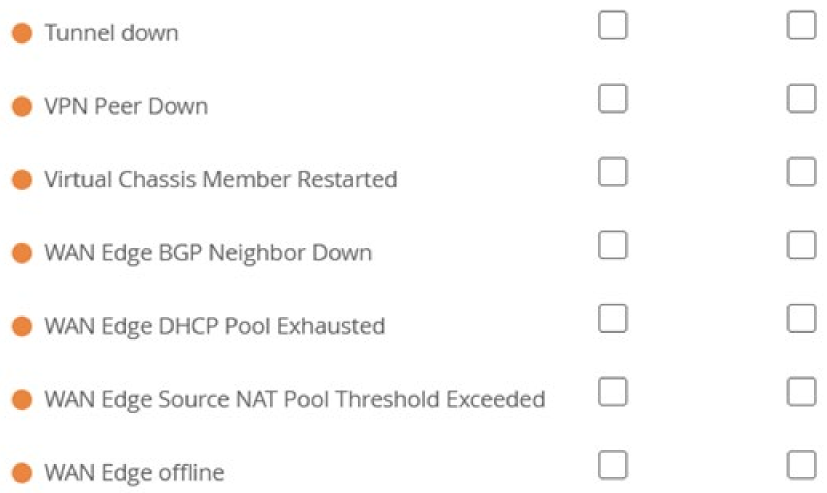
Email notifications enabled for the organization

Now, enable the Gateway Alerts and E-mail notifications for Infrastructure as the options shown below.



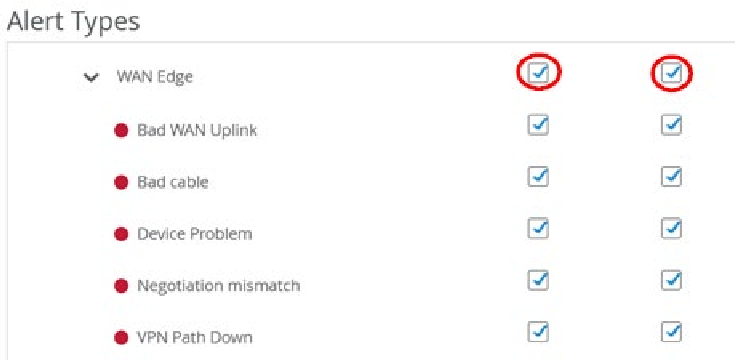
Alert Types

| Alerts | Enable Alert | Send Email Notification |
|---|---|---|
| Infrastructure | ⊟ | ⊟ |



| | | |
|---|---|---|
| ● Tunnel down | □ | □ |
| ● VPN Peer Down | □ | □ |
| ● Virtual Chassis Member Restarted | □ | □ |
| ● WAN Edge BGP Neighbor Down | □ | □ |
| ● WAN Edge DHCP Pool Exhausted | □ | □ |
| ● WAN Edge Source NAT Pool Threshold Exceeded | □ | □ |
| ● WAN Edge offline | □ | □ |

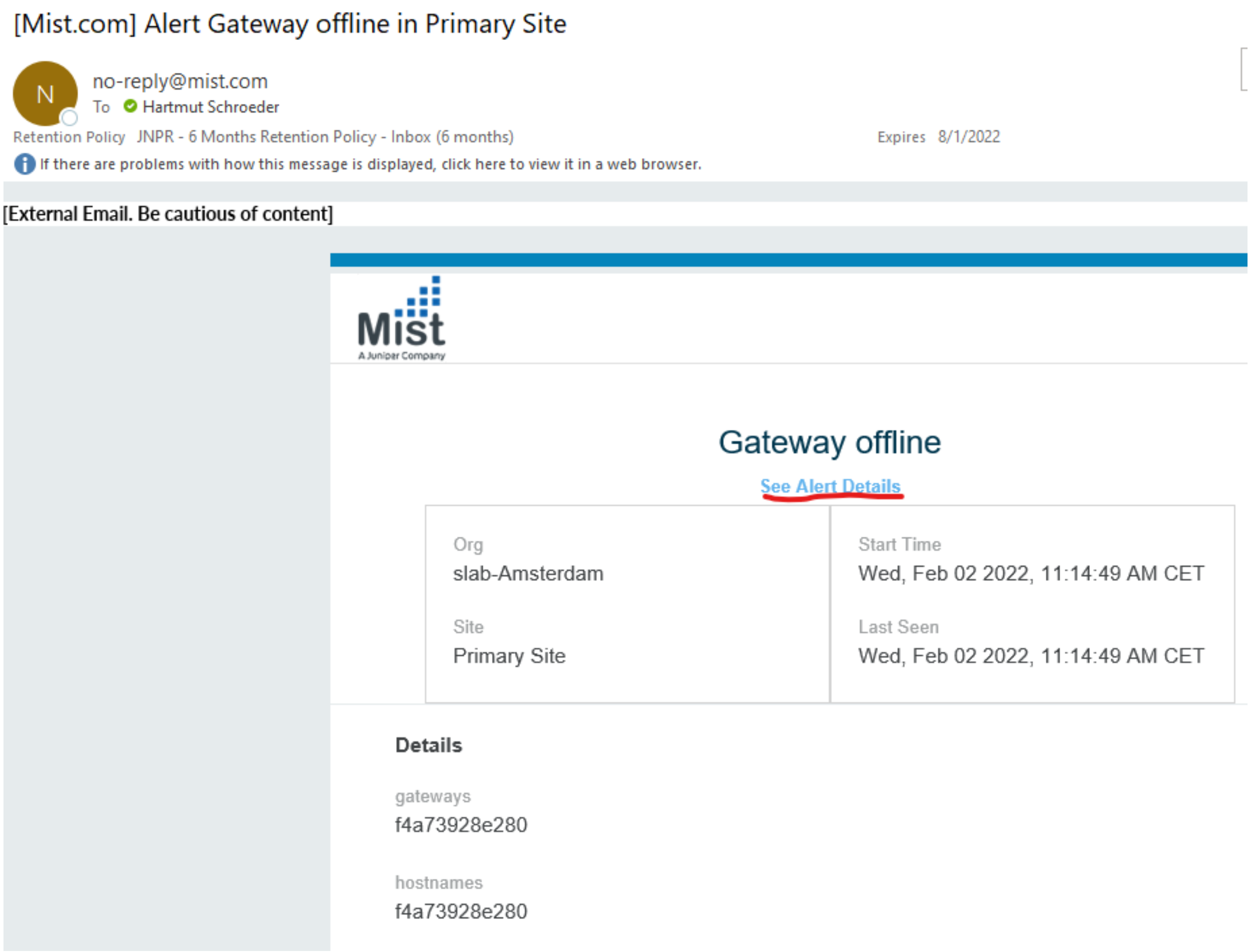
In addition, we recommend you to enable the Marvis WAN Edge Alerts and E-mail notifications.



Alert Types

| | | |
|---|---|---|
| WAN Edge | ☑ | ☑ |
| ● Bad WAN Uplink | ☑ | ☑ |
| ● Bad cable | ☑ | ☑ |
| ● Device Problem | ☑ | ☑ |
| ● Negotiation mismatch | ☑ | ☑ |
| ● VPN Path Down | ☑ | ☑ |

As an example, if you lose the connection of a device now to a Juniper Mist cloud, you might receive an E-mail after a couple of minutes. See an example below:



[Mist.com] Alert Gateway offline in Primary Site

no-reply@mist.com
To Hartmut Schroeder

Retention Policy JNPR - 6 Months Retention Policy - Inbox (6 months) Expires 8/1/2022

If there are problems with how this message is displayed, click here to view it in a web browser.

[External Email. Be cautious of content]

Gateway offline

See Alert Details

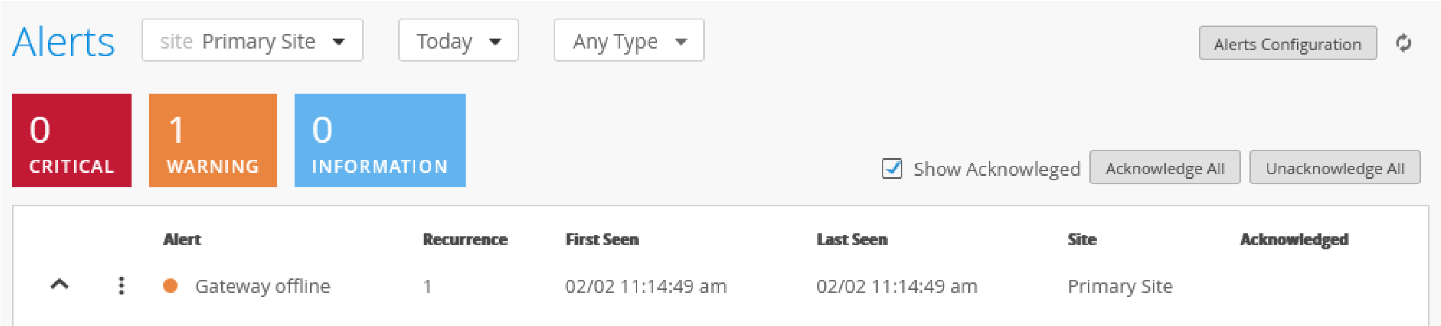
| | |
|---|---|
| Org<br>slab-Amsterdam | Start Time<br>Wed, Feb 02 2022, 11:14:49 AM CET |
| Site<br>Primary Site | Last Seen<br>Wed, Feb 02 2022, 11:14:49 AM CET |

Details

gateways
f4a73928e280

hostnames
f4a73928e280

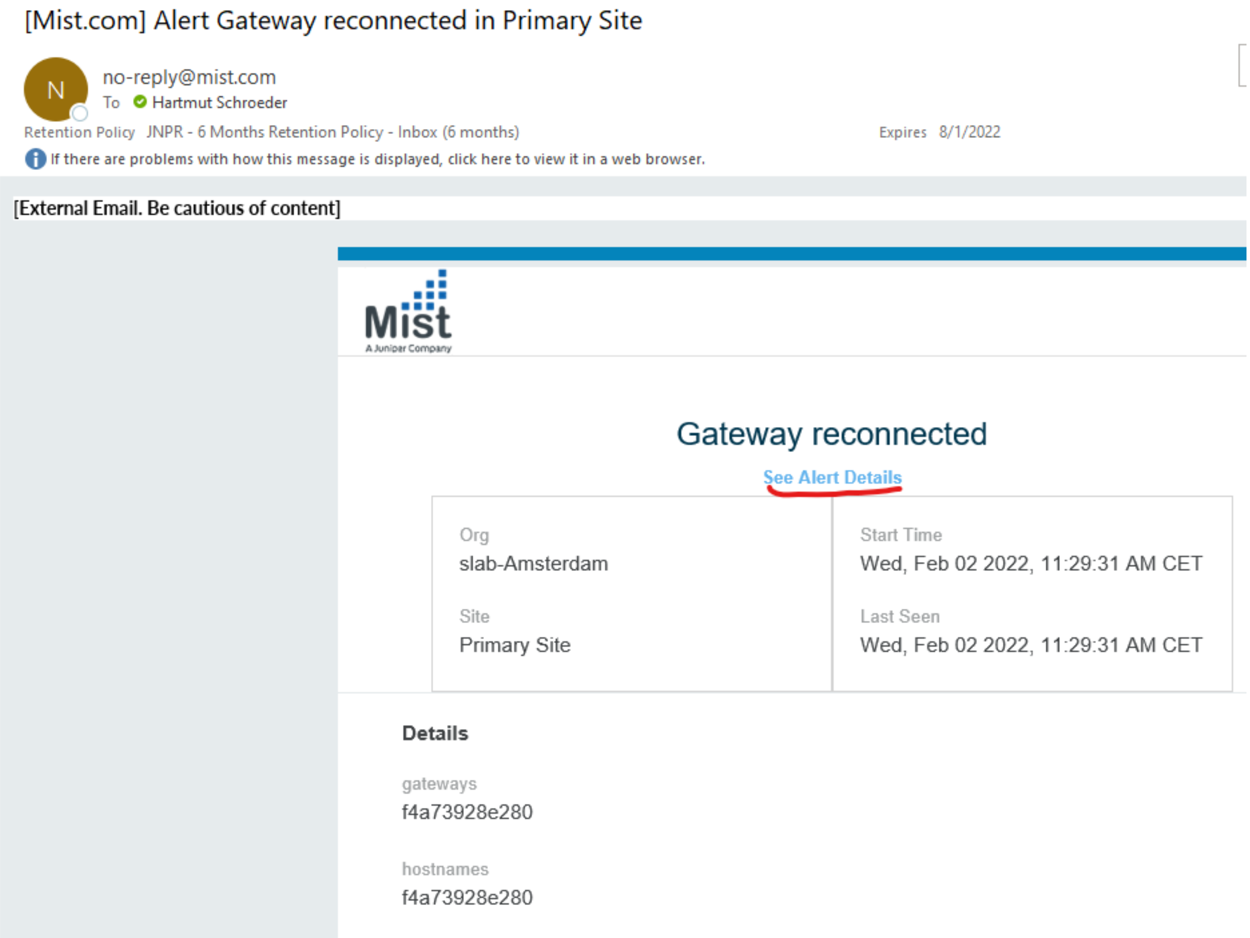
When you click **See Alert Details,** the link redirects you to the Alerts page. You can also navigate directly to the Alerts page to view the event reported as shown below.



| Alert | Recurrence | First Seen | Last Seen | Site | Acknowledged |
|---|---|---|---|---|---|
| ● Gateway offline | 1 | 02/02 11:14:49 am | 02/02 11:14:49 am | Primary Site | |

Let's assume that the connection to the Juniper Mist cloud is restored and you get another E-mail with a status change. When such an e-mail arrives, the alert details are as shown below.

And another example:



[Mist.com] Alert Gateway reconnected in Primary Site

no-reply@mist.com
To Hartmut Schroeder

Retention Policy JNPR - 6 Months Retention Policy - Inbox (6 months) Expires 8/1/2022

If there are problems with how this message is displayed, click here to view it in a web browser.

[External Email. Be cautious of content]

Mist
A Juniper Company

Gateway reconnected

See Alert Details

Org
slab-Amsterdam

Site
Primary Site

Start Time
Wed, Feb 02 2022, 11:29:31 AM CET

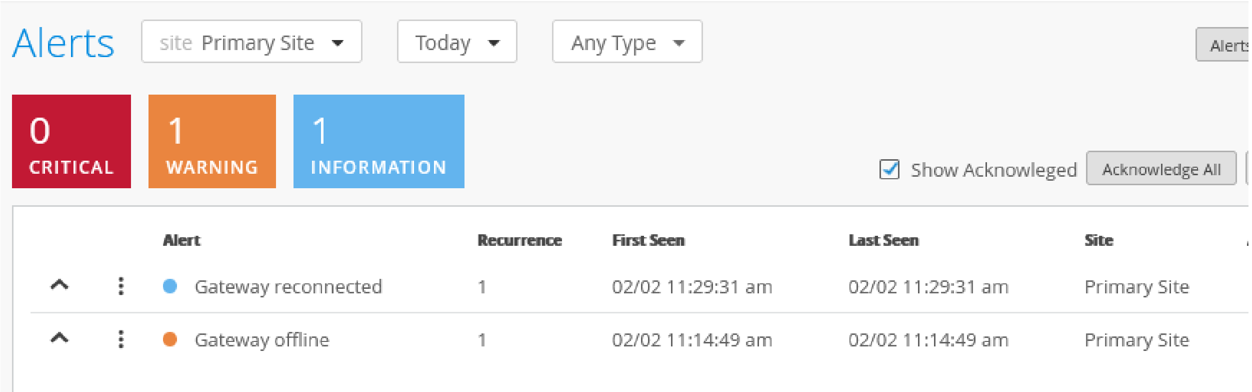
Last Seen
Wed, Feb 02 2022, 11:29:31 AM CET

Details

gateways
f4a73928e280

hostnames
f4a73928e280

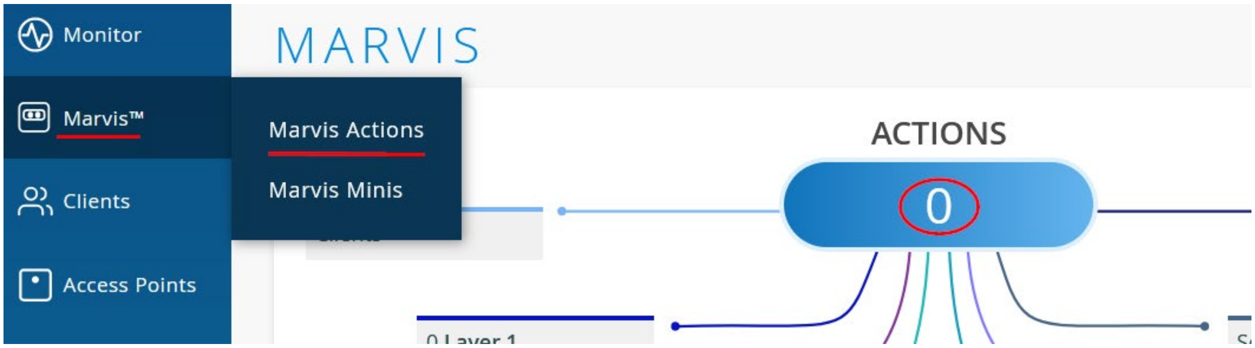
Again, on the Alerts page you should see the second event reported.



| Alert | Recurrence | First Seen | Last Seen | Site |
|---|---|---|---|---|
| ● Gateway reconnected | 1 | 02/02 11:29:31 am | 02/02 11:29:31 am | Primary Site |
| ● Gateway offline | 1 | 02/02 11:14:49 am | 02/02 11:14:49 am | Primary Site |

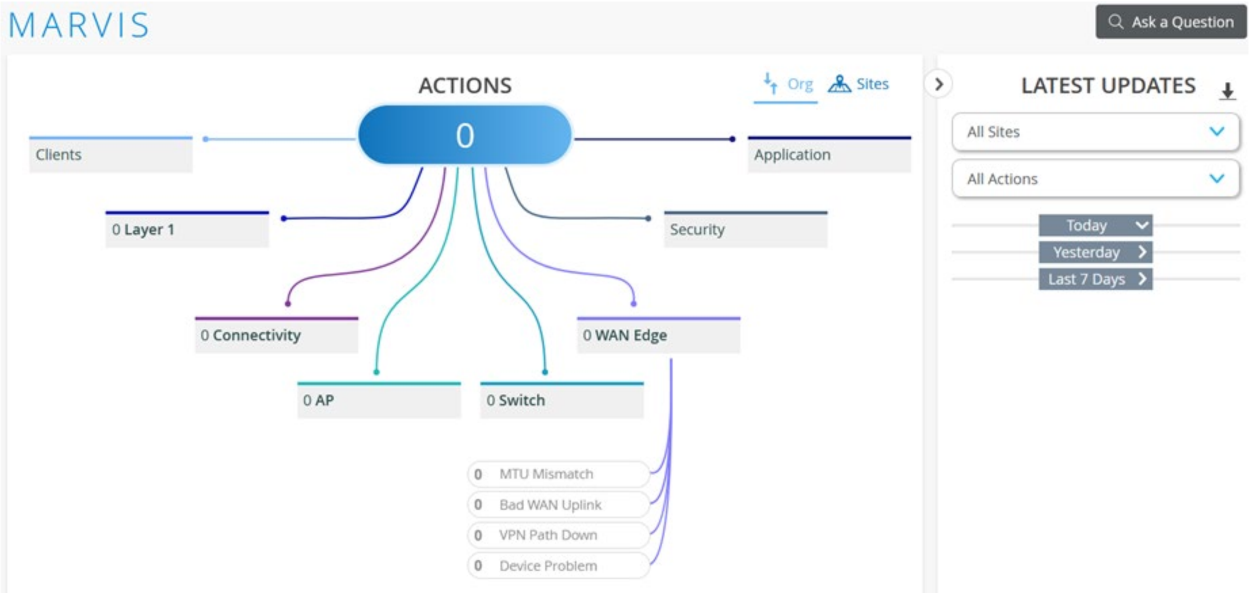
## Marvis Actions

Marvis Actions are reachable through **Marvis > Marvis Actions**.



The Marvis Actions you may see with concerns to WAN edge are:

- MTU Mismatch
- Bad WAN Uplink
- VPN Path Down
- Device Problem



# Day-2 Application SLE and Marvis Conversational Assistant

Feature in this chapter need more time to display meaningful data after you did the initial onboarding of the device. First, you need to define the probes using Application SLE and then consider the devices data after a weeks' time.

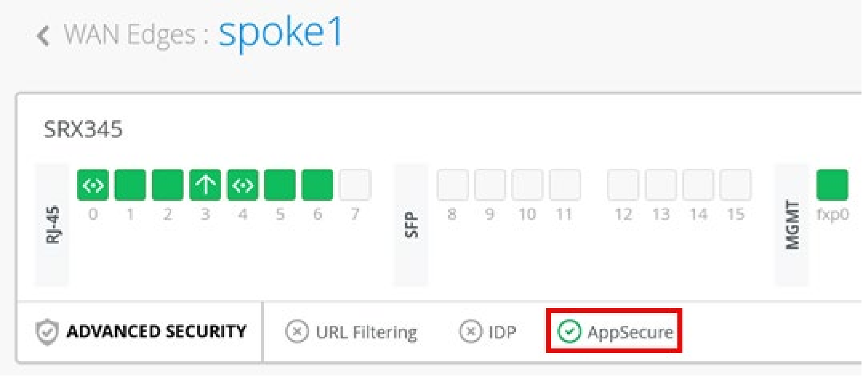
## Application SLE

Application SLE is used to monitor the reachability of applications through probes that are installed on the SRX Series device. Collecting monitoring reports and upstreaming this telemetry data to the Juniper Mist cloud enables you to review the data.

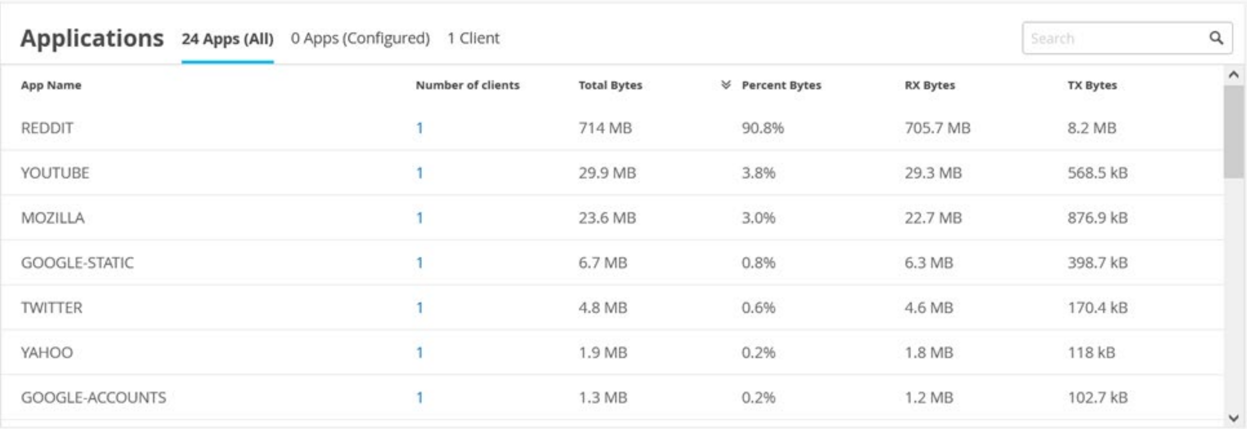
The number of maximum probes is limited to ten per SRX Series device. Looking at the applications utilized through its traffic analysis system and then automatically using the first ten to automatically install the probes is however seldom efficient. There might be application traffic appearing as a top ten application which is not critical for you to know. Example: Google web search or YouTube is not a critical application but might be a popular one. As a result, one must specify the probes for the 10 most needed applications to ensure that the probes really collect the right data.

**Prepare Application SLE Probes**

To ensure that this feature work as expected, check that AppSecure is enabled and running by reviewing the Device Page as shown below.

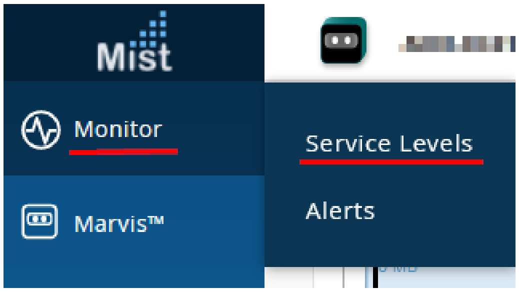


In this example, we already know which applications that we want to monitor through Application SLE. If you don't know, wait until you see them as detected applications under Gateway Insights as shown below.

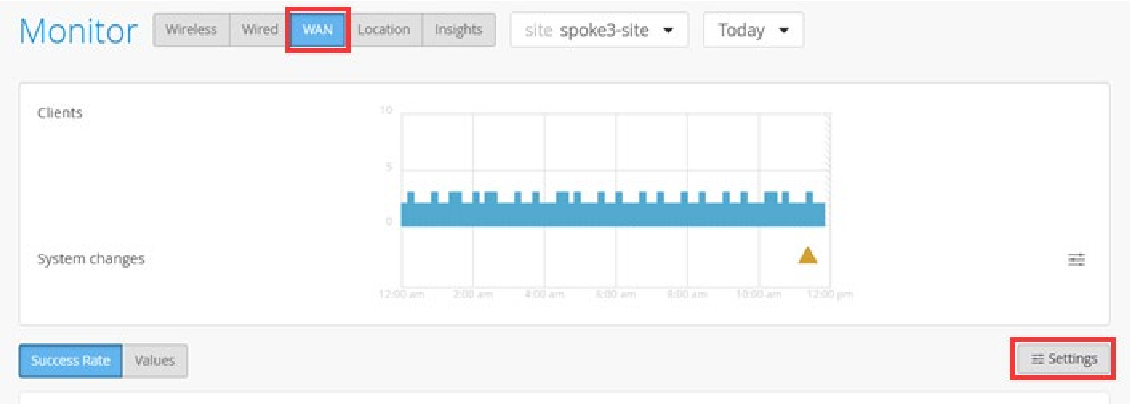


| App Name | Number of clients | Total Bytes | Percent Bytes | RX Bytes | TX Bytes |
|---|---|---|---|---|---|
| REDDIT | 1 | 714 MB | 90.8% | 705.7 MB | 8.2 MB |
| YOUTUBE | 1 | 29.9 MB | 3.8% | 29.3 MB | 568.5 kB |
| MOZILLA | 1 | 23.6 MB | 3.0% | 22.7 MB | 876.9 kB |
| GOOGLE-STATIC | 1 | 6.7 MB | 0.8% | 6.3 MB | 398.7 kB |
| TWITTER | 1 | 4.8 MB | 0.6% | 4.6 MB | 170.4 kB |
| YAHOO | 1 | 1.9 MB | 0.2% | 1.8 MB | 118 kB |
| GOOGLE-ACCOUNTS | 1 | 1.3 MB | 0.2% | 1.2 MB | 102.7 kB |

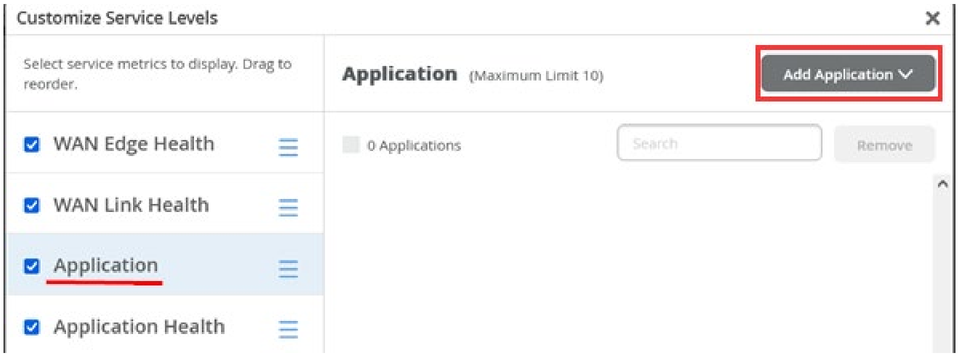
Select **Monitor** > **Service Levels** to configure the applications that you want to monitor through Application SLE.



Ensure you are on the correct Site. Select **WAN** and then click **Settings** available at the right-down corner to configure the settings.



Select **Application > Add Application** to add your first monitored application.


Customize Service Levels

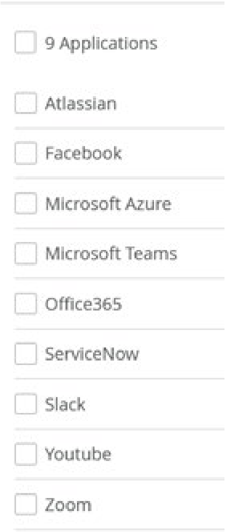
Select service metrics to display. Drag to reorder.

☑ WAN Edge Health
☑ WAN Link Health
☑ Application
☑ Application Health

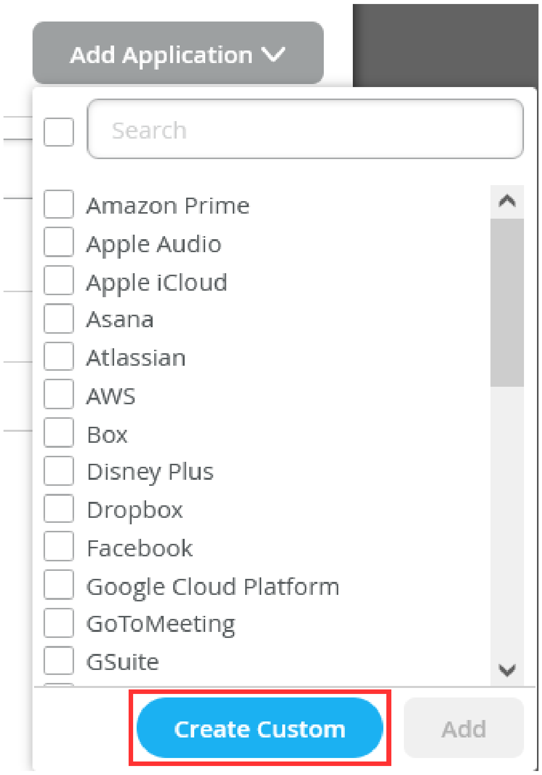
Application (Maximum Limit 10)

□ 0 Applications

We have configured the following nine applications that are known to the system already.

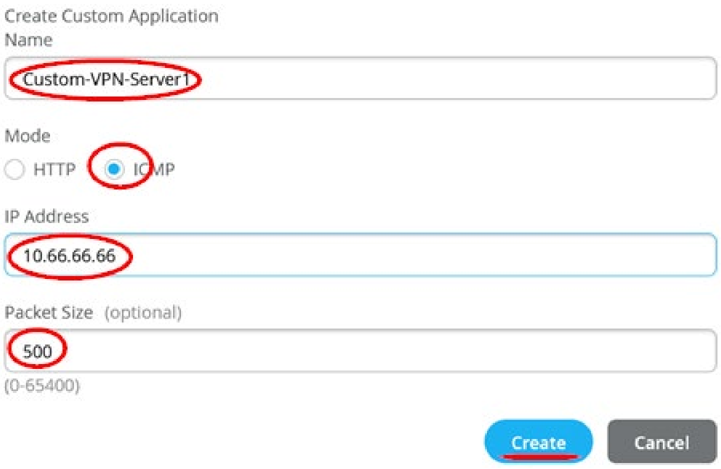


If an application is not on the pre-defined list, use **Create Custom** instead.



- In this example, we create a custom application to monitor a server in the VPN that is configured as follows:
  - Name: **Custom-VPN-Server1**
  - Mode: **ICMP**
  - IP Address: **10.66.66.66**

- Packet Size: **500**



Create Custom Application

Name: Custom-VPN-Server1

Mode

○ HTTP ● ICMP

IP Address: 10.66.66.66

Packet Size (optional): 500

(0-65400)

Exit the dialogue when all the required configurations are done.

> Note: As most websites today offer https encrypted pages, ensure the URL begins with “https://” even if the mode is called HTTP. For the ICMP method, you cannot configure a DNS-FQDN and must set an IP address instead.

The system now configures local RPM probes on the device for later traffic analysis.

Optional. On devices such as SRX340 or higher, you can review that installation and what is received through remote shell using the following Junos OS CLI:

```
show configuration services rpm | display inheritance no-comments | display set
```

```
show services rpm probe-results
```

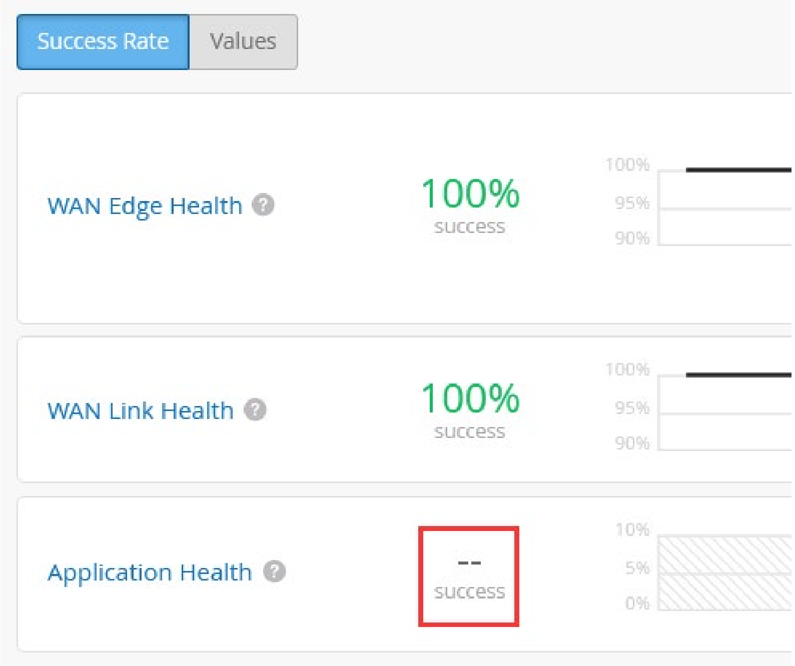
> Note: On SRX300 and SRX320, the probes are executed through local scripts for technical reasons. Hence, they won’t be seen in the local Junos OS configuration of the device.

After everything is prepared the LONG SAMPLE TIME of a minimum of 8 hours starts for the AI to adjust and “know” what is normal. Remember not every WAN-Link has the same behavior. A DSL-Broadband connection may have a ~30ms latency before you can reach any service on the Internet caused by the error-checking of the last mile copper.

> Note: Additionally, the probes that are installed now start collecting data utilizing the WAN-Link. This helps to collect enough samples for the SLE measurement.

In a lab situation, it might be appropriate to utilize scripts that generate real user traffic. In a production environment to see the real usage, it is better to allow traffic. Then, check through application visibility what is in use and adapt the required probes.

When collecting data for WAN-SLE, ensure that there is some value displayed for WAN-SLE. In the below screen, this is still not the case. Remember that you must configure the probes of the applications you want to monitor and cause traffic utilizing those applications. Else, the system does not get enough data for analysis.



WAN Edge Health 100% success

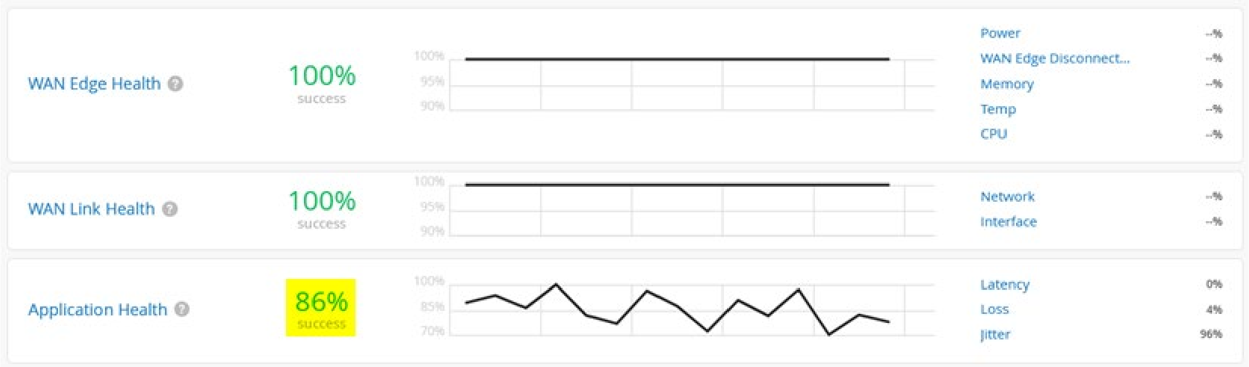
WAN Link Health 100% success

Application Health -- success

Check Application SLE metrics.

> Note: We recommend that after you install the Probes and run traffic, wait a week for the AI system to collect some data. The first coarse metrics takes about 8 hours to display the data.

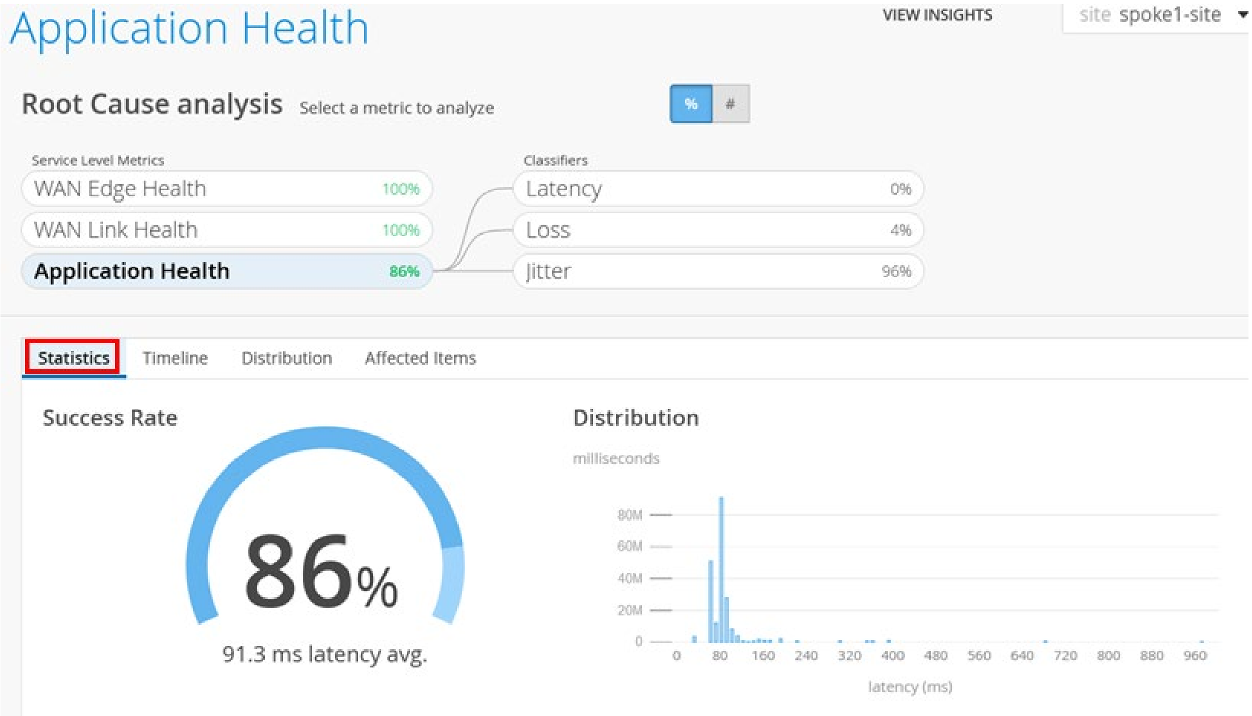
Now, we can check the Application Health SLE. IA percentage value represents that all in configured, traffic is running, and we collected enough data from the probes.



| | | |
|---|---|---|
| WAN Edge Health | 100% success | Power --%<br>WAN Edge Disconnect... --%<br>Memory --%<br>Temp --%<br>CPU --% |
| WAN Link Health | 100% success | Network --%<br>Interface --% |
| Application Health | 86% success | Latency 0%<br>Loss 4%<br>Jitter 96% |

In our case, we see 86%. Let’s inspect these reports to see who or what is impacted.

Review the Application Health Statistics tab for the sampled distribution of latency as shown below:



Application Health

VIEW INSIGHTS

site spoke1-site

Root Cause analysis Select a metric to analyze

| Service Level Metrics | | Classifiers | |
|---|---|---|---|
| WAN Edge Health | 100% | Latency | 0% |
| WAN Link Health | 100% | Loss | 4% |
| Application Health | 86% | Jitter | 96% |

Success Rate

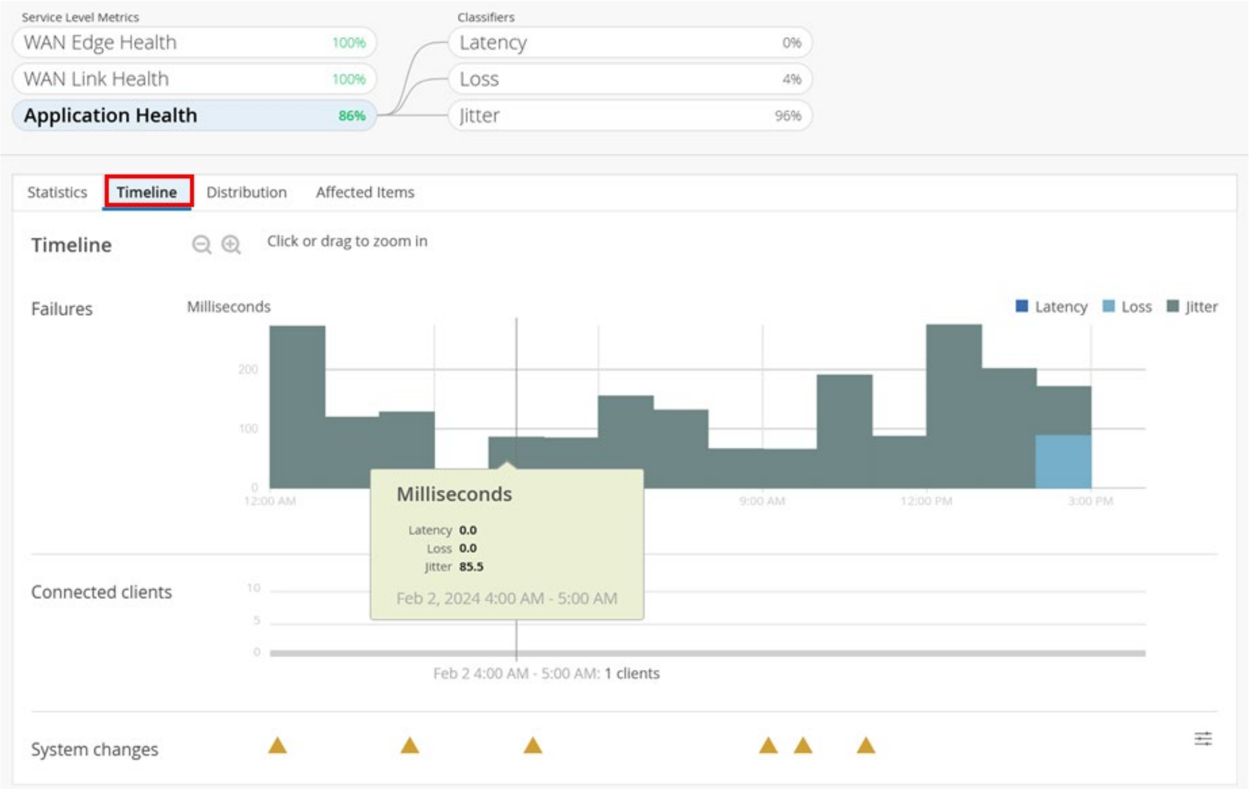
86%

91.3 ms latency avg.

Distribution

milliseconds

Then, check the Timeline tab to see what the impact is and when.



Service Level Metrics

| | |
|---|---|
| WAN Edge Health | 100% |
| WAN Link Health | 100% |
| Application Health | 86% |

Classifiers

| | |
|---|---|
| Latency | 0% |
| Loss | 4% |
| Jitter | 96% |

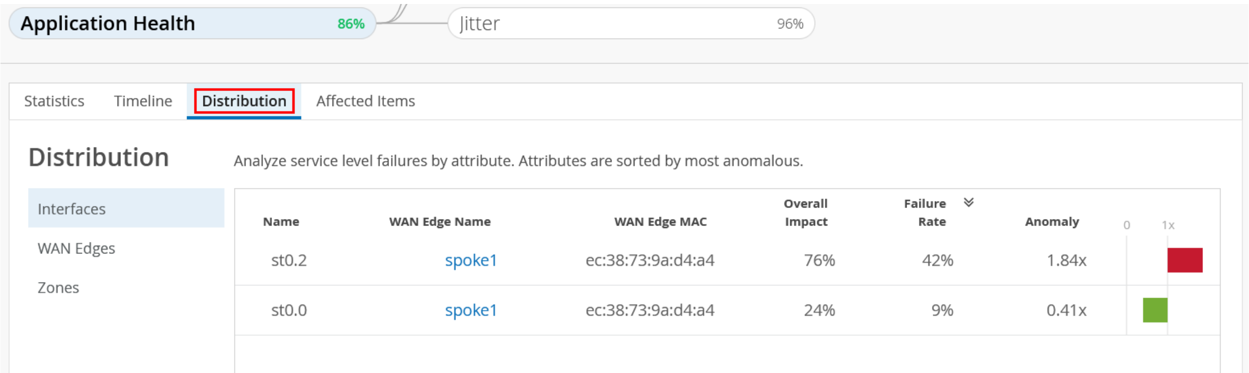
Milliseconds

Latency 0.0
Loss 0.0
Jitter 85.5

Feb 2, 2024 4:00 AM - 5:00 AM

Feb 2 4:00 AM - 5:00 AM: 1 clients

Next is to check the Distribution tab. Interfaces already provides us with data on the anomaly. All interfaces called st0.x are IPsec overlay tunnels similar to Central Breakout at Hub in the base Topology.

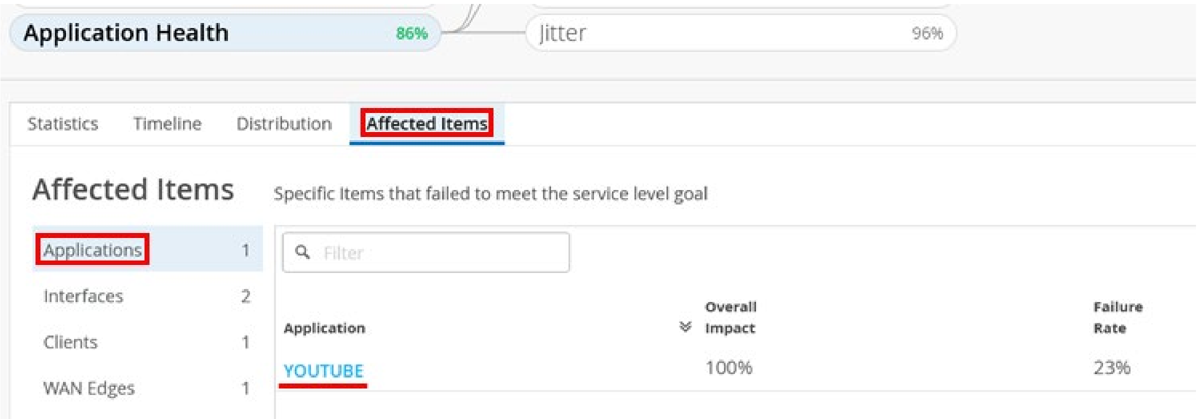


Distribution

Analyze service level failures by attribute. Attributes are sorted by most anomalous.

| Name | WAN Edge Name | WAN Edge MAC | Overall Impact | Failure Rate | Anomaly | 0 1x |
|---|---|---|---|---|---|---|
| st0.2 | spoke1 | ec:38:73:9a:d4:a4 | 76% | 42% | 1.84x | 🟥 |
| st0.0 | spoke1 | ec:38:73:9a:d4:a4 | 24% | 9% | 0.41x | 🟩 |

Finally, check the **Affected Items** > Applications, you see in our example that we have issues with YouTube.

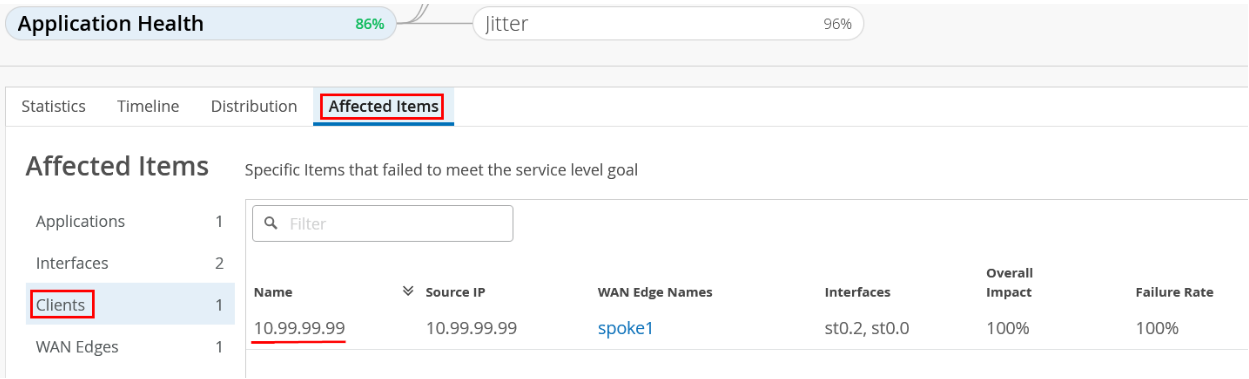


Affected Items Specific Items that failed to meet the service level goal

| | |
|---|---|
| Applications | 1 |
| Interfaces | 2 |
| Clients | 1 |
| WAN Edges | 1 |

| Application | Overall Impact | Failure Rate |
|---|---|---|
| YOUTUBE | 100% | 23% |

Finally let us check who are the affected users.



Affected Items Specific Items that failed to meet the service level goal

| | |
|---|---|
| Applications | 1 |
| Interfaces | 2 |
| Clients | 1 |
| WAN Edges | 1 |

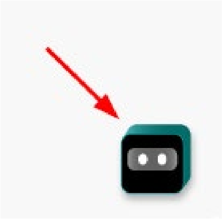
| Name | Source IP | WAN Edge Names | Interfaces | Overall Impact | Failure Rate |
|---|---|---|---|---|---|
| 10.99.99.99 | 10.99.99.99 | spoke1 | st0.2, st0.0 | 100% | 100% |

You can also inspect Interfaces and WAN edges.

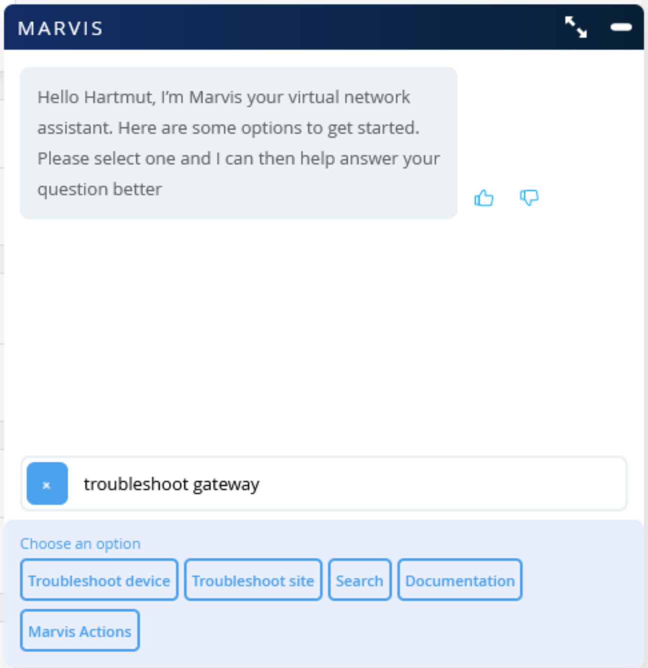
## Marvis Conversational Assistant

Note: We  recommend you to have traffic running at least a week for the AI system to collect some data.

The Marvis Conversational Assistant is in the lower-right corner of your browser window.



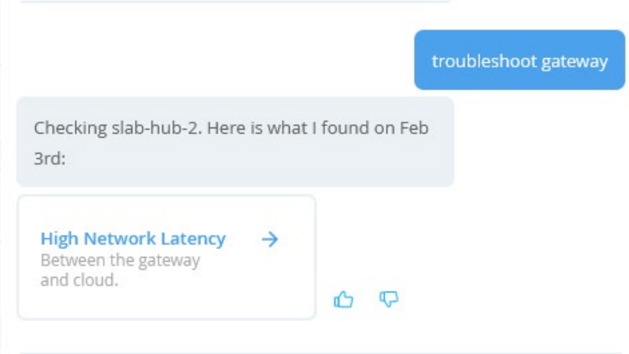
The window s that appears  already has some predefined ones. Enter **troubleshoot gateway** to limit the search only related to WAN-router.



Hello Hartmut, I'm Marvis your virtual network assistant. Here are some options to get started. Please select one and I can then help answer your question better

troubleshoot gateway

In our case (might be different in your environment) we get a report about High Network Latency for router "slab-hub-2"

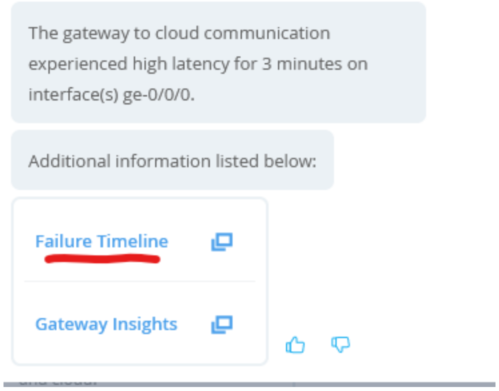


troubleshoot gateway

Checking slab-hub-2. Here is what I found on Feb 3rd:

High Network Latency
Between the gateway and cloud.

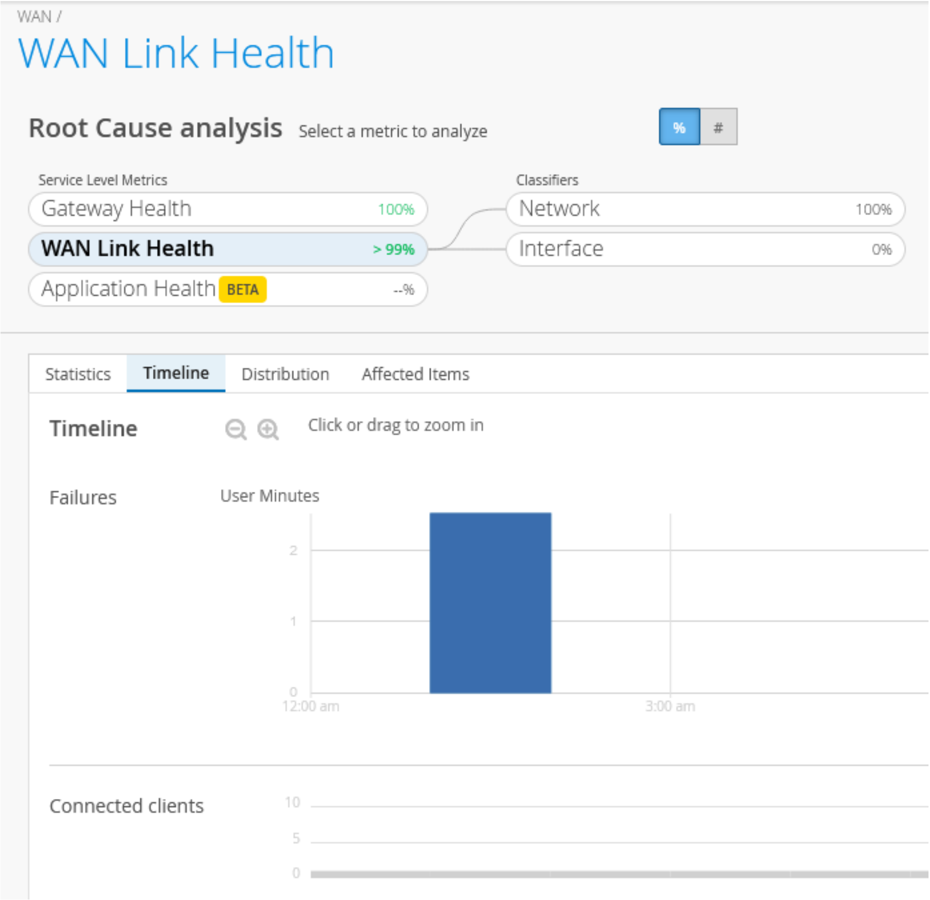
Clicking further provides you with more options to click. In our case, the next item is "Failure Timeline"



The gateway to cloud communication experienced high latency for 3 minutes on interface(s) ge-0/0/0.

Additional information listed below:

Clicking Failure Timeline link directs you to the WAN SLE page. The WAN SLE page displays when your traffic got impacted. For more information, see WAN SLE Monitor Page.



WAN /

WAN Link Health

Root Cause analysis Select a metric to analyze

Service Level Metrics
Gateway Health 100%
WAN Link Health > 99%
Application Health BETA --%

Classifiers
Network 100%
Interface 0%

The second link navigates you to the Gateway Insights Page. For more information, see “WAN Edge Insights Page“.

# Day-2 Upgrade a WAN Edge SRX Series Firewalls

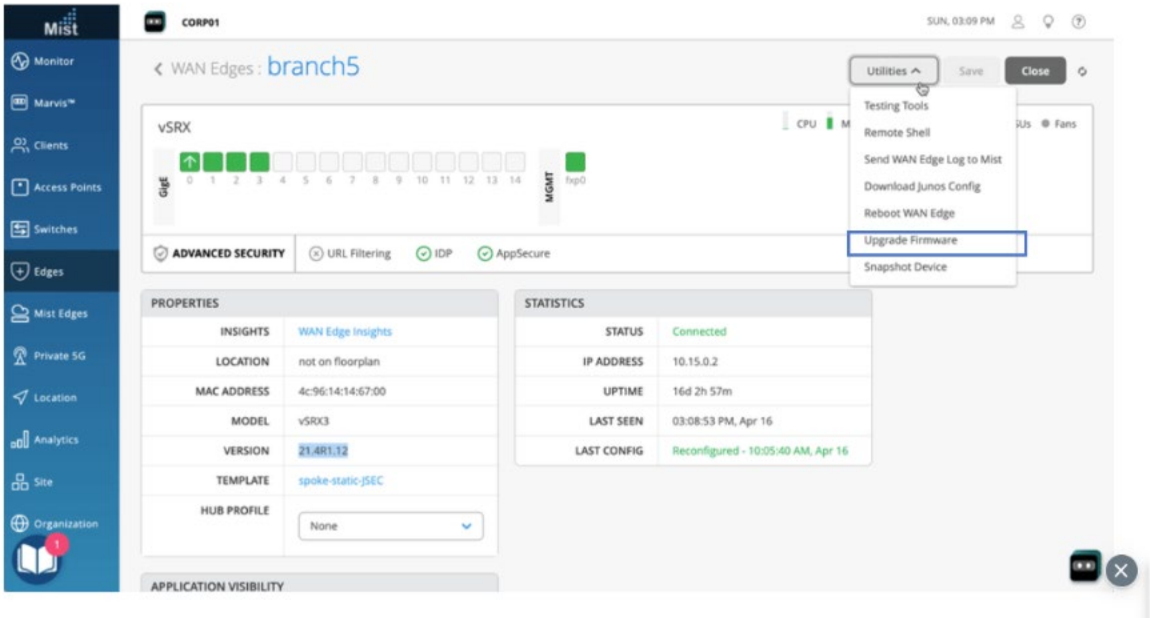
You can upgrade a Juniper Networks SRX Series Firewall deployed as a WAN edge device in the Juniper Mist cloud portal. Upgrading your device’s operating system to a newer version provides you with new features, enhancements, bug fixes, and compatibility improvements.

To upgrade a WAN edge SRX Series Firewall:

1. In the Juniper Mist cloud portal, select **WAN Edge** and select the device.

2. Click the device and select the **Upgrade Firmware** option from the utilities menu to initiate the upgrade.

Figure150: Upgrade Software

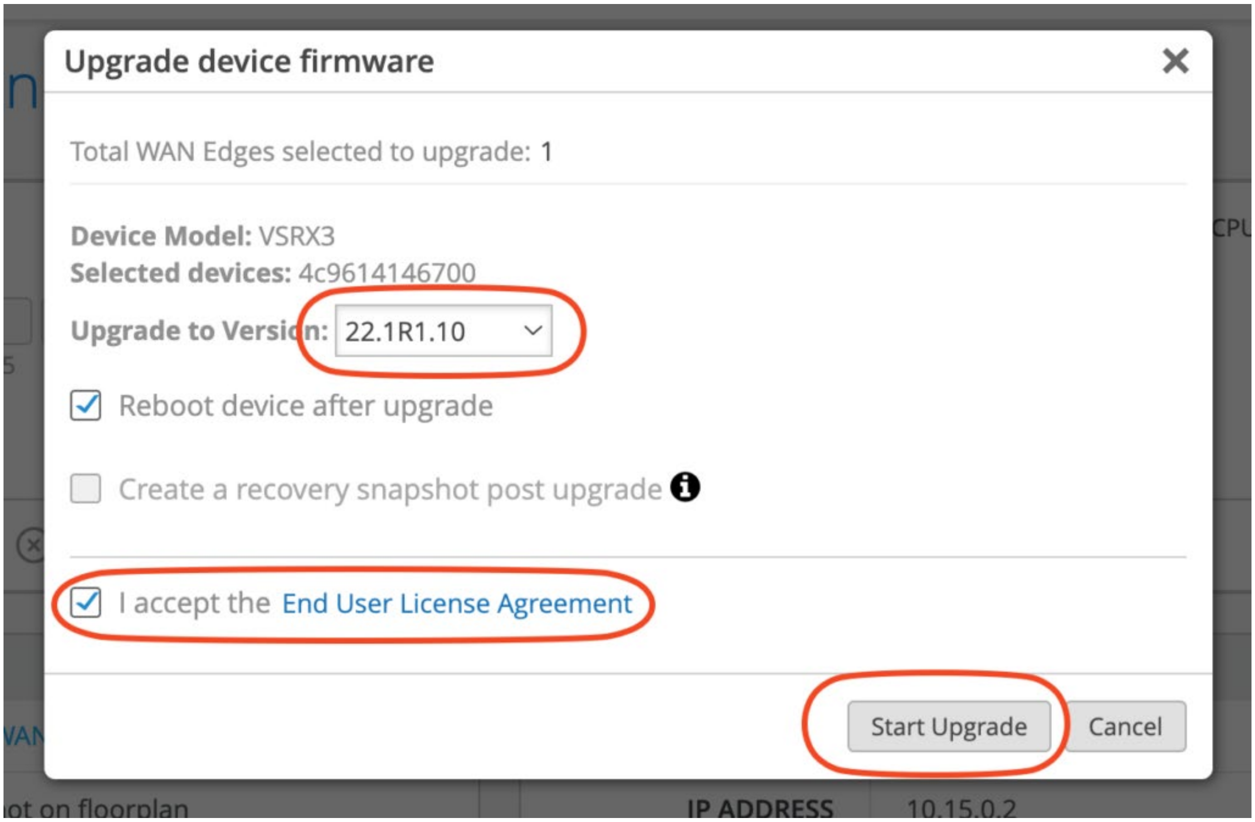


| PROPERTIES | |
|---|---|
| INSIGHTS | WAN Edge Insights |
| LOCATION | not on floorplan |
| MAC ADDRESS | 4c:96:14:14:67:00 |
| MODEL | vSRX3 |
| VERSION | 21.4R1.12 |
| TEMPLATE | spoke-static-JSEC |
| HUB PROFILE | None |

| STATISTICS | |
|---|---|
| STATUS | Connected |
| IP ADDRESS | 10.15.0.2 |
| UPTIME | 16d 2h 57m |
| LAST SEEN | 03:08:53 PM, Apr 16 |
| LAST CONFIG | Reconfigured - 10:05:40 AM, Apr 16 |

3. In the Upgrade device firmware window, select the required version from the **Upgrade to Version** list.

Figure151: Schedule the Upgrade Option



Upgrade device firmware

Total WAN Edges selected to upgrade: 1

**Device Model:** VSRX3
**Selected devices:** 4c9614146700
**Upgrade to Version:** 22.1R1.10

☑ Reboot device after upgrade

□ Create a recovery snapshot post upgrade

☑ I accept the End User License Agreement

4. Clear the **Reboot device after upgrade** option to manually reboot the device. You must reboot the device after you upgrade the software.

5. Read and accept the **End User License Agreement** and click **Start Upgrade** to initiate the upgrade.

6. From the Juniper Mist cloud menu, select **Monitor** > **Insights** > **WAN Edge** to monitor the upgrade progress.

Note: High Availability Considerations: For WAN edge devices in a High Availability cluster, you can minimize the downtime by upgrading one node at a time.

For more information visit the Data Center Design Center:
https://www.juniper.net/documentation/solutions/us/en/data-center/

**Corporate and Sales Headquarters**
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
**www.juniper.net**

**APAC and EMEA Headquarters**
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701