Engineering
Simplicity

Juniper Mist WAN Assurance Configuration Guide

Published
2024-12-15

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Mist WAN Assurance Configuration Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

About This Guide

Use this guide to learn about key features of Juniper Mist WAN Assurance and to understand the configuration choices that are available through the Juniper Mist™ cloud portal.

1

CHAPTER

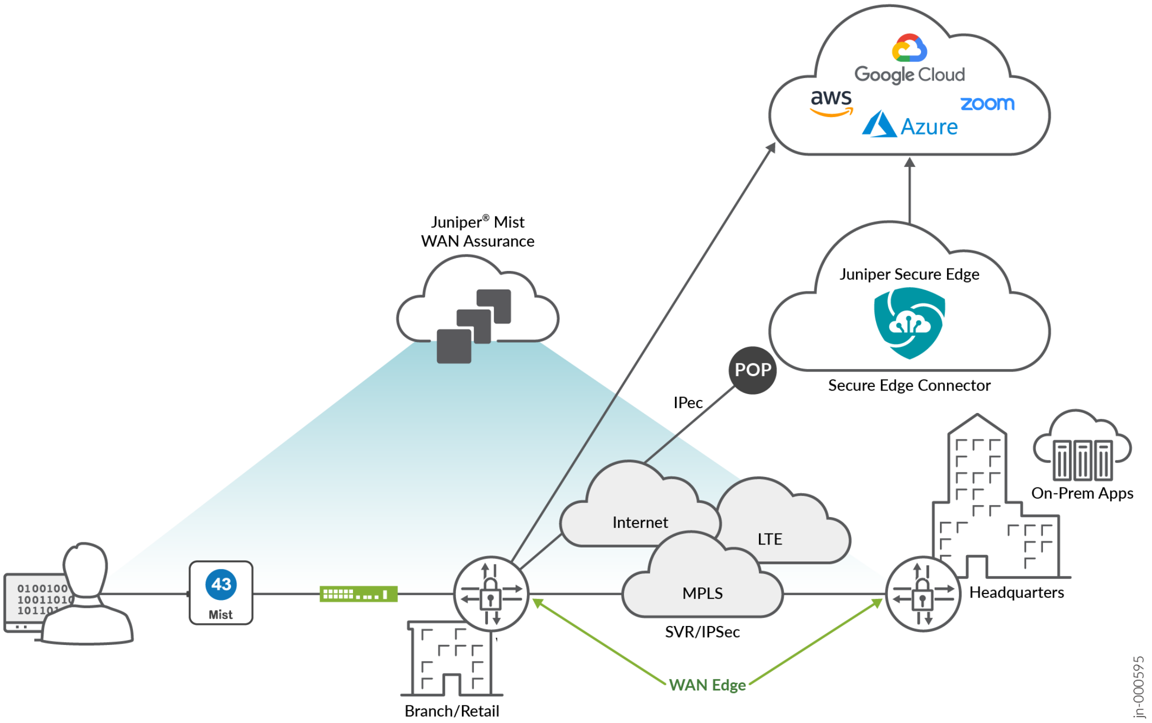
Overview

Introduction to Juniper Mist WAN Assurance

IN THIS SECTION

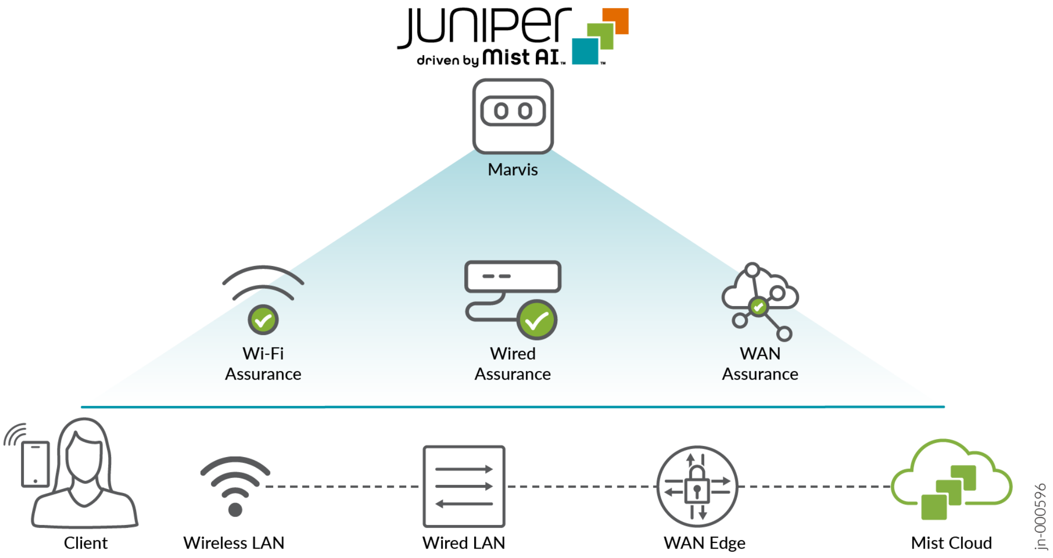
The WAN edge references the demarcation point for your enterprise network to reach the outside world. This boundary is a crucial security and troubleshooting hotspot. The WAN edge can be a simple border between your enterprise network and the outside world. However, the WAN edge can also be a Juniper®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

Figure 1: Juniper Mist WAN Assurance



The WAN edge transforms with Juniper's AI-driven SD-WAN solution and acts as your centralized policy enforcement point. Combined with the Juniper Mist WAN Assurance cloud service, the Juniper SD-WAN solves many of the legacy SD-WAN solutions' security, monitoring, and troubleshooting challenges. 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® Session Smart™ Routers or Juniper® SRX Series Firewalls across a software-defined WAN.

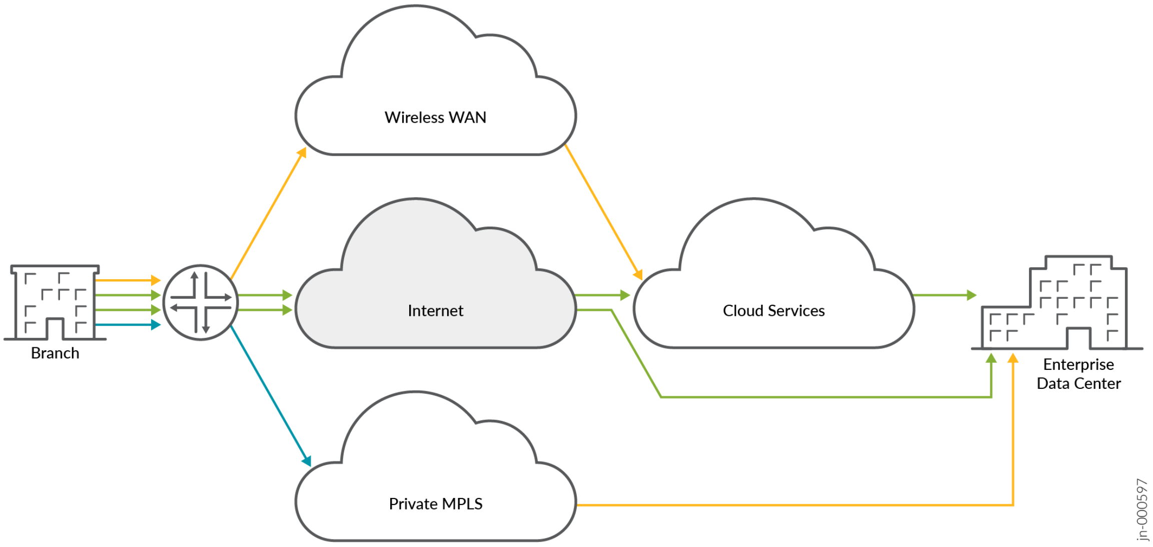
Figure 2: Juniper AI-Driven SD-WAN Solution



Intersite 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. Software-defined WAN traffic from remote sites travels through an abstracted overlay across less expensive broadband service providers. This connectivity design replaces expensive legacy MPLS solutions. Edge devices deliver stateful failovers across various connection types, including MPLS, broadband, satellite, and LTE. This real-time switch for critical applications is imperceptible to the user. Juniper Mist WAN Assurance also brings 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 for access and security.

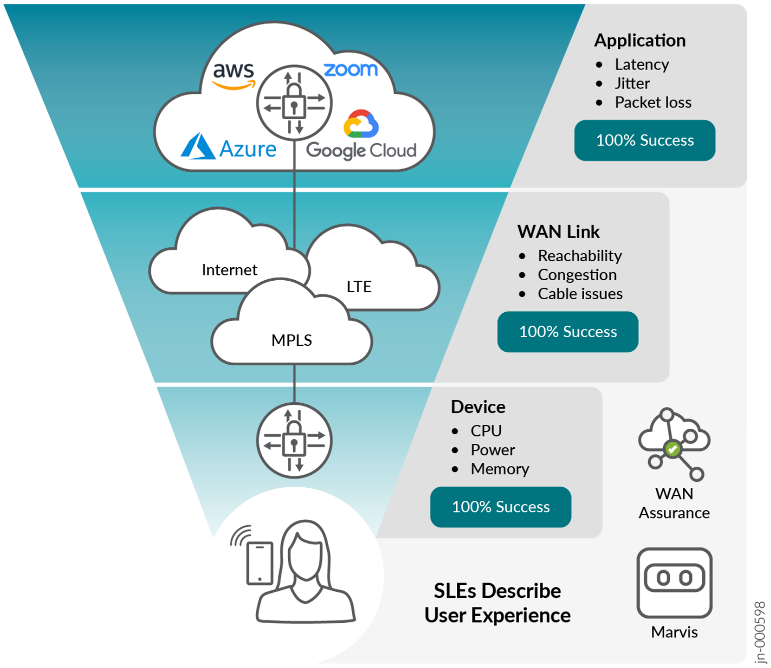
Figure 3: SD_WAN Intersite Connectivity



Juniper Mist WAN Assurance Service Level Expectations (SLEs)

Mist's Predictive Analytics and Correlation Engine (PACE) provides data science and machine learning to 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 impacting user experiences. Service-level expectations enable simpler operations, better visibility into end-user experiences, and simplify monitoring and troubleshooting your network.

Figure 4: Juniper Mist WAN Assurance Service Level Expectations (SLEs)



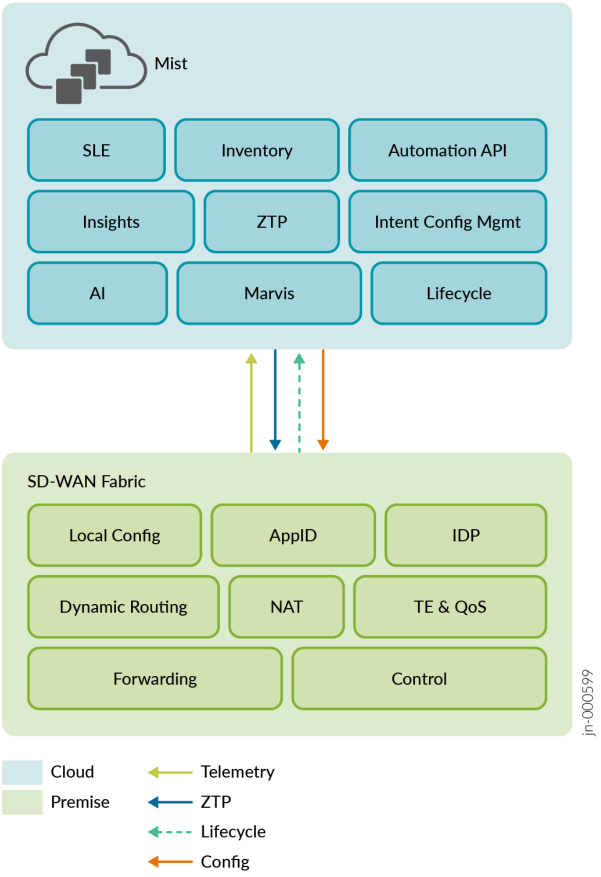
AIOps for SD-WAN

✓ Gain insights to user experience
✓ Get immediate root cause discovery
✓ Surface and ID anomalies

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, life cycle, and configuration are done through a single Mist dashboard.

Figure 5: Mist Management Model



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

Video: WAN Assurance - How's user experience? Really?

RELATED DOCUMENTATION

Juniper Mist WAN Assurance Platform Considerations | 10

Request Help with a New Deployment of Juniper Mist Devices

SUMMARY

If you need help with a new deployment of Juniper Mist™ devices, follow these steps to submit your request.

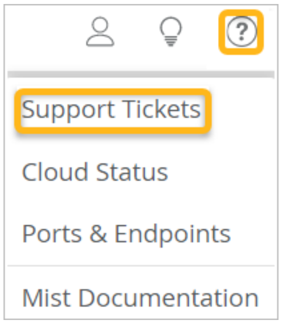
The Juniper Mist™ Support team provides onboarding assistance to help customers with new deployments. You'll get assistance with initial setup, configuration, and basic troubleshooting.

NOTE:

- These services do not include network design.
- Submit your request at least 48 hours in advance of your preferred appointment time.
- Available only for wireless, switching, and SD-WAN deployments.

To request help with a new deployment:

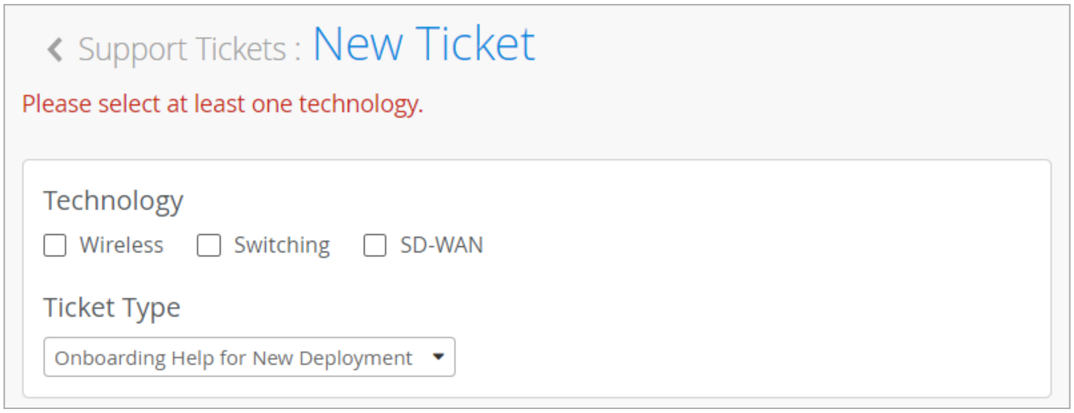
1. Click the question icon near the top-right corner of the Juniper Mist™ portal, and then click **Support Tickets**.



2. Click **Create a Ticket**.
3. For **Technology**, select the relevant technologies for your deployment:
   - **Wireless**
   - **Switching**

- SD-WAN

4. For **Ticket Type**, select **Onboarding Help for New Deployment**.



‹ Support Tickets : New Ticket

Please select at least one technology.

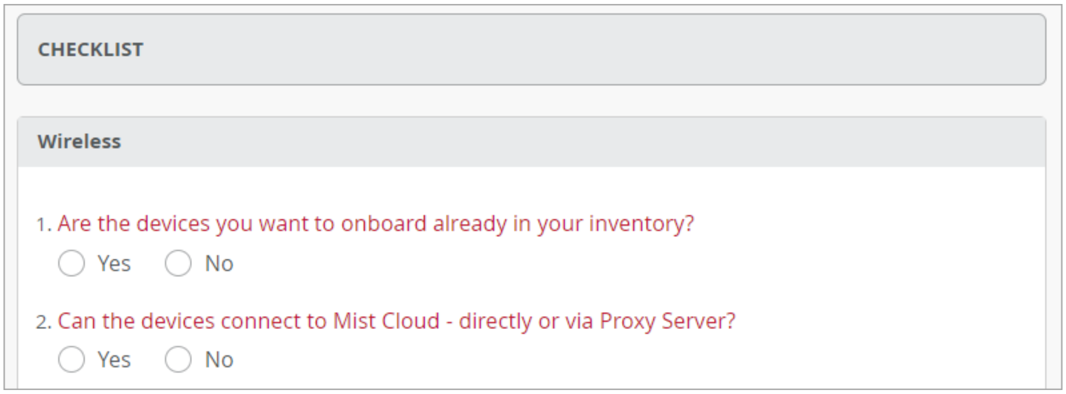
Technology

□ Wireless □ Switching □ SD-WAN

Ticket Type

Onboarding Help for New Deployment ▾

5. Enter a short **Ticket Summary** and a detailed **Description**.
6. Under **Checklist**, answer all the questions.



CHECKLIST

Wireless

1. Are the devices you want to onboard already in your inventory?

○ Yes ○ No

2. Can the devices connect to Mist Cloud - directly or via Proxy Server?

○ Yes ○ No

> **NOTE**: The checklist includes each technology that you selected at the top. Complete all questions in all sections that appear.
>
> As you complete the checklist, you can use suggested hyperlinks for self-help. If you find your answers in these links, you can cancel submitting this ticket.

7. Under **Schedule**, select the date, time, and time zone for your onboarding help session.

> **NOTE**: If you need to change your appointment after you submit your ticket, you can go to your list of open tickets, select this ticket, and reschedule.

8. Click **Submit** at the top right corner of the page.

   If this button is unavailable, ensure that you've entered all required information. Required fields have red labels.

The support team will contact you to conduct the help session.

2

CHAPTER

Platform Considerations

Juniper Mist WAN Assurance Platform Considerations

IN THIS SECTION

Introduction

Juniper Mist WAN Assurance is a comprehensive SD-WAN solution to streamline your operations and optimize your end user experience. It does so using tunnel-free overlay technology, integrated security, cloud management with zero-touch provisioning, and AI-driven operations. Choosing the right WAN Edge platform is crucial for leveraging the full benefits of Juniper Mist WAN Assurance. This topic aims to assist organizations in making informed decisions aligned with their specific needs, current network architecture, and future goals.

Platform Selection Criteria

For WAN edge devices in Mist WAN Assurance, Juniper Networks® Session Smart™ Routers and Juniper Networks® SRX Series Firewalls can be used as platform in a deployment.

When selecting a WAN Edge platform, it's essential to consider how each option fits with your organization's requirements:

- **Session Smart Routers** are recommended for deployments aiming to maximize network efficiency and performance, particularly in dynamic environments.
- **SRX Series Firewalls** are suited for organizations seeking to maintain strong security postures while gradually transitioning to SD-WAN.

Session Smart™ Router in WAN Assurance

When selecting a platform to use as WAN edge in Juniper Mist, generally the Session Smart Routers are recommended for most SD-WAN deployments. The Session Smart Routers excels in several areas which are key to the successful implementation and operation of SD-WAN:

- Network efficiency—By forming overlays using secure vector routing (SVR) technology, an open standard for tunnel-free forwarding between router peers, Session Smart Routers ensures your bandwidth is used as efficiently as possible. It maximizes performance for users and applications without unnecessary overhead.

- Rapid Failover—During instances of network failure or poor network quality, the Session Smart Routers gives the fastest possible failover, minimizing downtime and maintaining connectivity for critical applications and services.

- Rich Telemetry and Insights—The session-based architecture of the Session Smart Routers not only facilitates efficient data forwarding but also provides a wealth of telemetry data. This offers deep insights into the performance of users, applications, and the network itself. It serves as the foundation for Marvis and AI models in the Mist cloud, enabling continuous improvement and optimization of your network.

- Integrated Security—A router with security at its foundation, the Session Smart Routers provides Layer 3-Layer 4 security policy by default, and optional Layer 5-Layer 7 where advanced security at the branch is needed. Integrations with Security Service Edge (SSE) providers and the Session Smart Routers are simplified using Mist driven orchestration for simplicity. This offers a seamless transition to a modern cloud based Secure Access Service Edge (SASE) architecture.

SRX Series in Juniper Mist WAN Assurance

While the Session Smart Routers Series is recommended for most deployments, the Juniper Networks SRX Series presents an ideal alternative for environments where traditional security mechanisms and transitional benefits are prioritized.

Key features include:

- Enhancing Existing Deployments—If your current infrastructure already utilizes SRX Series Firewalls, integrating them with Mist WAN Assurance can amplify their capabilities through the addition of cloud and AI technologies. This not only extends the life and utility of your current investments but does so in a way that aligns with modern, intelligent network management practices.

- Evolutionary Transition to SD-WAN—For organizations looking to transition to SD-WAN at a measured pace, starting with SRX Series as your WAN edge platform within Mist WAN Assurance can offer a familiar yet powerful stepping stone. This allows your team to gradually adapt to SD-

WAN technologies and principles while still gaining immediate benefits from AI and cloud management features.

Ultimately, your WAN Edge platform decision within Juniper Mist WAN Assurance should align with your organization's specific needs, current network architecture, and future goals. Under Mist, both platforms provide simplified management and Zero Touch Provisioning (ZTP) for easy setup, ideal for branches with limited IT support, ensuring a reliable and scalable network. The platform portfolio supports a variety of WAN types (MPLS, broadband, 3G/4G LTE) and speeds (1/10/25/40/100 Gbps). Whether you prioritize the cutting-edge routing capabilities, application performance and efficiency of the Session Smart Routers or the traditional security and transitional benefits of the SRX Series, both paths lead to a more intelligent, responsive, and user experience centric network.

For Juniper Mist WAN Assurance related information, see

- Juniper Mist WAN Assurance
- Secure Access Service Edge (SASE)
- Juniper SD-WAN, Driven by Juniper Mist AI™
- Juniper Session Smart™ Routing
- Juniper SRX Series Firewalls
- Juniper Mist Wired Assurance
- Juniper Mist Wireless Assurance
- Secure Access Service Edge (SASE)

RELATED DOCUMENTATION

Introduction to Juniper Mist WAN Assurance | 2

Juniper Mist WAN Assurance Configuration Hierarchy

IN THIS SECTION

Introduction to Configuration Hierarchy

Juniper Mist WAN Assurance Configuration

For network administrators, it's essential to understand that each piece of the puzzle builds your network's policies, security, and connectivity in Juniper Mist WAN Assurance cloud service. A full SD-WAN deployment requires each part to complete intersite connectivity. Mist automatically translates your traffic intent to configurations for WAN edge devices using Mist's intent-based networking model. Each part works together to build complex interface assignments, security, routing policies, and—depending on the platform—destination zones. Therefore, understanding the Mist intent model is crucial as we dive into the configuration hierarchy for Juniper Mist WAN Assurance.

Intent-Based Routing

Intent-based networking solves several problems. For example, consider the need for secure communication between two networks. An intent model states that secure communication requires a secure tunnel between Network A and Network B. In this scenario, a network administrator identifies which traffic uses the tunnel and describes other desired general properties. But an operator wouldn't specify or even know how to build a tunnel. To implement a tunnel, you must know how many devices to secure, how to make BGP advertisements, and which features and parameters to turn on. By contrast, an intent-based networking system automatically generates an entire configuration of all devices based on the service description. It then provides ongoing assurance checks between the intended and operational state of the network, using closed-loop validation to continuously verify the configuration's correctness. Intent-based networking is a declarative network operation model. It contrasts with traditional imperative networking, which requires network engineers to specify the sequence of actions needed on individual network elements and creates significant potential for error.

Intent-based model key characteristics:

- Do not require as much explicit direction as traditional network models require.
- Build policies based on which network goes to which application.
- Configure Juniper Mist WAN Assurance **Networks** and **Applications** organization-wide.
- Push relevant configurations only.
- Configure only the **Applications** that a device uses. If a device doesn't use an **Application**, the intent-based network doesn't configure it on that device.

Let's look at the example of configuring DHCP on a LAN and assume that the interface is already configured and assigned to a zone.

Required steps in the Junos CLI:

- Navigate to the Junos system services level and enable the DHCP-local-server for your interface.
- Navigate to the Junos system address assignment and create an address pool specifying the target network, the range of addresses for the pool, the default gateway, and any other DHCP attributes.
- Navigate to your security zone and enable host-inbound traffic for the DHCP system service to allow the SRX Series to process DHCP requests from clients.

This requires multiple configuration lines spread across three configuration hierarchies at a minimum.

The same workflow is significantly streamlined in Mist:

- First, navigate to your LAN configuration and open it for Editing.
- Next, enable the DHCP Server radio button to unlock the configuration and populate the required fields (IP Start, IP End, and gateway).
- Save the LAN configuration and then Save the device configuration.

Configuration Hierarchy Elements

Organization-Wide Configuration Elements

The top of the Mist configuration is called your Mist Organization. These elements impact your entire software-defined wide area network (SD-WAN) deployment. The different components at this configuration level become building blocks for sources and destinations across your deployment. Once identified, traffic requests associate a sender and the desired destination appropriately. The elements help build different Juniper Mist WAN Assurance deployment components depending on your platform. Identifying the source and destination will build IPsec tunnels across the WAN and associated security zones on the Juniper® SRX Series Firewall. These components on the Juniper® Networks Session Smart™ Router become the corresponding source and destination to help build the Secure Vector Routing (SVR) metadata exchange. The two platforms approach the challenge of SD-WAN uniquely, which makes it important to know your Juniper Mist WAN Assurance platform.

Networks

The Juniper Mist WAN Assurance **Network** is the "who" in the Mist intent-driven paradigm. **Networks** are sources of the request in your network. Networks enable you to define groups of "Users." Once you create this element in your Mist design, the network is defined for use across the entire organization.

Characteristics of Networks on the Juniper® Networks Session Smart™ Router:

- Mist **Networks** create Tenants in the background for SVR.
- The Session Smart Router identifies Tenants at the logical interface (Network Interface).
- LAN and WAN interface configurations identify your Tenant (request source).

Characteristics of Networks on the Juniper® SRX Series Firewall:

- **Networks** create Address books used as the source for **Security Policies** and Advanced Policy Based Routing (APBR) Policies.
- Configurations are applied to the device if an **Application Policy** is configured.
- For the LAN, the zone's name is derived from the name of the specified network.
- For the WAN, the zone's name is based on the name of the WAN.

Route Advertisement (Advertise via Overlay)

WAN Assurance is about the abstraction of the transport network into the SD-WAN. You can advertise networks via SD-WAN for control and reachability with route advertisement. This is how established networks in your LAN segments can be advertised across the overlay. Setting up these networks generates the source addresses for service policies. Network Address Translation (NAT) for the source and destination can route traffic to your users if needed.

The purpose of SD-WAN is intersite connectivity. Therefore, networks can be advertised via overlay to enable reachability between your SD-WAN devices. With this setting, your network will share the address across the WAN so other devices know how to reach it.

Access to Mist Cloud

Mist is a full-stack solution. Only some of your devices are WAN edge or SD-WAN routers. Specific devices will want access to the Mist Cloud to leverage other solutions like Wireless and Wired Assurance on Wireless APs and switches. **Access to Mist Cloud** will automatically generate specific firewall/policy rules enabling the devices to phone home to Mist without needing an explicit **Application Policy**. You don't want this on all devices behind the WAN edge in an SD-WAN deployment, as it can pose a policy challenge for routers. **Access to Mist Cloud** is excellent for Mist APs or switches, as you can monitor and troubleshoot them from the Mist dashboard. See Juniper Mist Wireless Assurance and Wired Assurance.

Enabling access to the Mist cloud ensures that anything sitting behind the WAN edge can reach the Mist cloud without needing to express policies for connectivity manually. Ports and protocols for this setting include the following:

- TCP/443
- DNS/53
- SSH/2200
- NTP/123
- Syslog/6514
- ICMP

Users

Don't let the label fool you. **Users** does not represent a single user on your network. **Users** are subsets of subnets or indirectly connected subnets. Since **Networks** are "who," think of **Users** as a subdivision of that network identity. There are often universal rules to treat networks the same. For example, for 99% of your traffic, you want sessions to do the same thing. But what about when you're blocking access to a corporate network from a guest network, but you need one specific IP to have printer access? This is your use case for **Users**. For those familiar with the Session Smart Routing platform, consider this the child to the parent network "Tenant." Alternatively, **Users** have a second use case defining indirect prefixes on the network.

- **Users** can define granular permissions. For example, your LAN segment may need Internet access, but you must restrict it to a particular network device. So here, you'd create an access policy around that desktop.
- You sometimes need to reach indirectly connected prefixes behind a router on the LAN segment. For example, picture a router behind a device that connects multiple devices to an outside application.

Applications

Applications comprise the "what" in the Mist intent-driven model paradigm. **Applications** are what your network delivers. **Applications** represent traffic destinations and are named for what a client would access, like a "database" or the "Internet." Once you create this element in your Mist design, the **Application** is defined for use across the entire organization.

Characteristics of **Applications** on the Juniper® Networks Session Smart™ Router

- Mist applications create services in the background for SVR.
- **Applications** can be ports, protocols, prefixes, custom domains, or app names from the built-in AppID library.

Ports, protocols, and prefixes are where all the policy revolves.

- **Custom Apps** are a set of ports, protocols, or prefixes.
- **Apps** map to the Internet app-id.
- **URL Categories** are force-point URLs.

Characteristics of Applications on the Juniper® SRX Series Firewall

- **Applications** determine the destination used in a security policy.
  - A prefix of 0.0.0.0/0 with protocol "any", is resolved to *any* within the Juniper Mist WAN Assurance policy. No address book or application is necessary.
- **Custom Apps** on the WAN edge use the SRX Series on-box engine "type" and are a combination of an address book and applications.
- **Apps** map to the SRX Series Layer 7 AppID engine.
- **URL Categories** are force-point URLs.

Traffic Steering

Traffic Steering is the "how" in the Mist intent-driven model paradigm. **Traffic Steering** is how you define the different paths traffic can take to reach its destination. If traffic to an application has multiple paths, you can restrict the paths to a subset of paths and configure an order of preference. You can also load and balance numerous streams across the available paths.

Characteristics of **Traffic Steering** on the Juniper® Networks Session Smart™ Router:

- The Juniper® Session Smart Router™ has a proprietary solution for **Traffic Steering** that determines the next hop and vector to the destination leveraging SVR.
- Blocklist items interfere with the establishment of the next hops for SVR.

You'll only want **Traffic Steering** rules on a Session Smart Router

- Traditional steering strategies like Ordered, Weighted, and ECMP do not apply to the Session Smart Router.
- Blocking **Applications** in the **Application Policy** is unnecessary and undermines the Session Smart next-hop selection process.

The Session Smart Router chooses the next hops using a proprietary hello mechanism. This bidirectional forwarding detection (BFD) message between peer Session Smart Routers checks for liveness and path health.

Characteristics of **Traffic Steering** on the Juniper® SRX Series Firewall:

- The Juniper® SRX Series Firewall is zone-based, and the destination zone is determined by the paths configured within a **Traffic Steering** policy.
- **Traffic Steering** configures forwarding-type routing instances and the relevant routing policy to import routes. For your SRX Series, this routing instance is used in APBR.
- There are several steering strategies for the SRX Series:
    - Ordered: Default, go in order of the list. The top takes priority, then failover to the next. Creates an ordered list.
    - Weighted: Allows you to set your desired order based on weight. For example, two weighted paths, both set to 5 results in ECMP across the two paths. On the other hand, two weighted paths with one set to 5 and the other set to 10 results in ordered steering with traffic taking lower weight path first.
    - ECMP: Fully load balance traffic with an equal-cost multipath algorithm. Traffic will be split evenly across all available paths.

Application Policy

The "who," "what," and "how" come together with **Application Policy**. The Mist intent-driven model simplifies manually generating routes and security policies through Junos OS on the SRX Series with thousands of lines of code. It also simplifies deploying a Session Smart Router for those transitioning from a Conductor-based Session Smart deployment to WAN Assurance. You no longer need explicit permissions and interface assignments to get up and running. WAN Assurance is zero-trust. This is both implied and part of the intent-driven model. You must explicitly grant permission to a **Network** for access to an **Application**, or it will not route.

Order only matters when egressing your local network on the Juniper® Networks Session Smart™ Router. The Session Smart Router is a router that uses the most specific matches. This means that using Mist Traffic Steering isn't necessary for local traffic. Importantly, using a block in your **Traffic Steering** does not work with SVR, as it undermines the proprietary process. If a device, subnet, or network shouldn't have access to an **Application**, do not create traffic steering for it.

Characteristics of **Application Policy** on the Juniper® SRX Series Firewall:

The steering path determines the destination zone in the SRX series. Please ensure that policies have **Traffic Steering** assigned because the order of policies matters when working with the SRX Series. As a traditional zone-based firewall, it uses a list of rules that generate filters and policies. Most specific rules should be at the top of the Application Policy list on the SRX Series.

Scaling Your Network: Automation in Mist

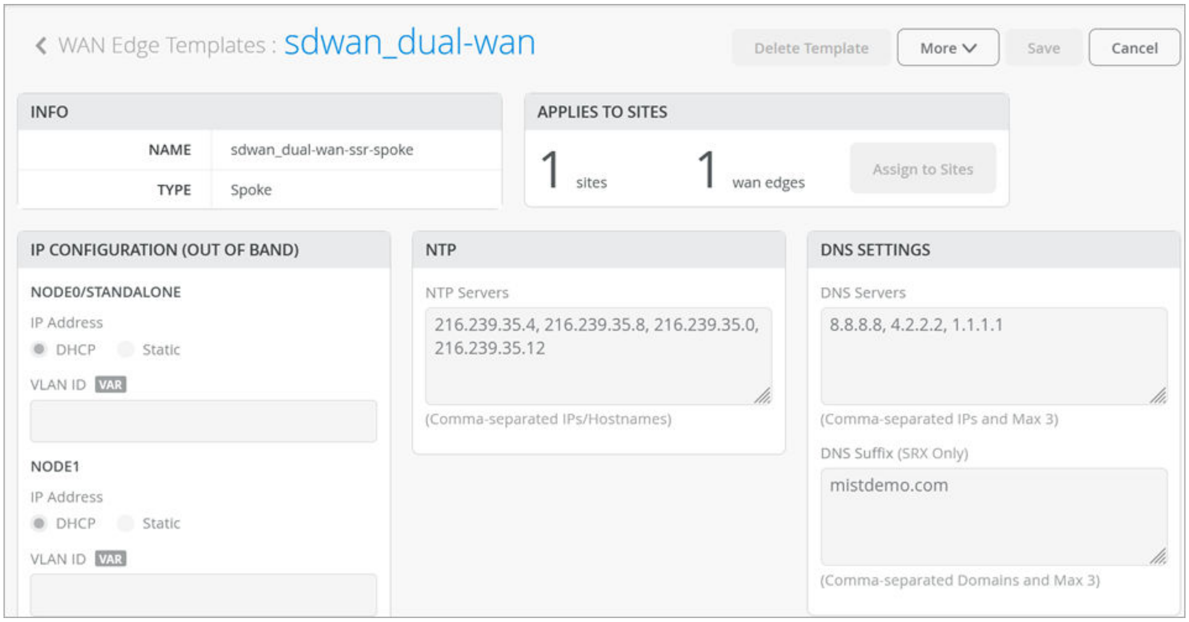
WAN Edge Templates

Once basic configuration elements of SD-WAN are in place, Mist enables you to deploy new WAN edge devices through WAN edge templates. All that previous configuration can be templated with WAN edge templates. These templates work for a standalone edge device to a full SD-WAN deployment with hundreds of sites. The automation process removes errors and simplifies deploying multiple spoke sites and headends.

Templates reduce or eliminate common configuration tasks and remove human error when configuring multiple devices. WAN edge templates:

- Enforce standards across a deployment.
- Ensure that all your network devices point to the same DNS (8.8.8.8).
- Provide predictable behavior because they use the same Network Time Protocol (NTP) for synchronization and logging. (This also affects specific certificates.)
- Simplify troubleshooting and management.

Figure 6: WAN Edge Template



WAN Edge Templates : sdwan_dual-wan

INFO

NAME	sdwan_dual-wan-ssr-spoke
TYPE	Spoke

APPLIES TO SITES

1 sites 1 wan edges

IP CONFIGURATION (OUT OF BAND)

NODE0/STANDALONE

IP Address

● DHCP ○ Static

VLAN ID VAR

NODE1

IP Address

● DHCP ○ Static

VLAN ID VAR

NTP

NTP Servers

216.239.35.4, 216.239.35.8, 216.239.35.0, 216.239.35.12

(Comma-separated IPs/Hostnames)

DNS SETTINGS

DNS Servers

8.8.8.8, 4.2.2.2, 1.1.1.1

(Comma-separated IPs and Max 3)

DNS Suffix (SRX Only)

mistdemo.com

(Comma-separated Domains and Max 3)

However, WAN edge templates do more than automate tasks and may contain things you don't often use and apply to all sites or a subset of sites. For example, not every site may have a guest network, but you could reserve that interface.

These templates also allow for:

- Bulk orders of hardware for ports and site groups through specific models.
- Specific use cases and traffic flows.
- Different corporate LAN networks.
- Guest networks.

WAN edge templates automatically configure repetitive information like an IP, gateway, or VLAN. In addition, WAN edge templates can include traffic steering, access policies, routing preferences, and any additional configuration you'd like standardized. Remember that you'll need a prefix, NAT, or other local information for WAN and LAN connectivity.

Hub Profiles

Hub profiles work with WAN edge templates. Hubs are not at the edge and are universally unique throughout your network. It's impossible to define their deployment fully within a template. Hubs affect how Mist builds the overlay network. Each branch and remote office build the SD-WAN communication to the hub. Topology is determined by overlay endpoints that make up a single overlay. Every hub WAN interface creates an overlay endpoint for spokes. Spoke WAN interfaces map the appropriate hub WAN interfaces, defining the topology. This is the abstraction of the transport network. Because the two platforms for WAN Assurance solve the abstraction differently, it's essential to understand their nuances when building that overlay network.

Juniper® SRX Series Firewall

The SRX Series overlay SD-WAN combines a virtual router for route separation and IPsec tunnels for secure transit traffic. WAN configurations determine the topology and build the overlay network. One thing to note is that you can implement only one overlay per organization. However, you can have many paths within this overlay across multiple types of transport and securely isolate and forward traffic. For SRX Series devices, the overlay combines a security zone, virtual router, and IPsec tunnels.

Juniper® Networks Session Smart™ Router

The Session Smart overlay SD-WAN is your neighborhood, which involves proprietary communication via BFD on port 1280 for liveness and jitter, latency, and loss between Session Smart peers. When you configure a WAN interface on a hub profile, it creates an overlay hub endpoint. On the Session Smart Router, the endpoint is the receiving end of the SVR.

A few things happen when you map a spoke WAN Interface to the overlay hub endpoint. The spoke will establish peer connectivity and identify the neighborhoods and vectors for SVR, which is the Session Smart abstraction of the transport network.

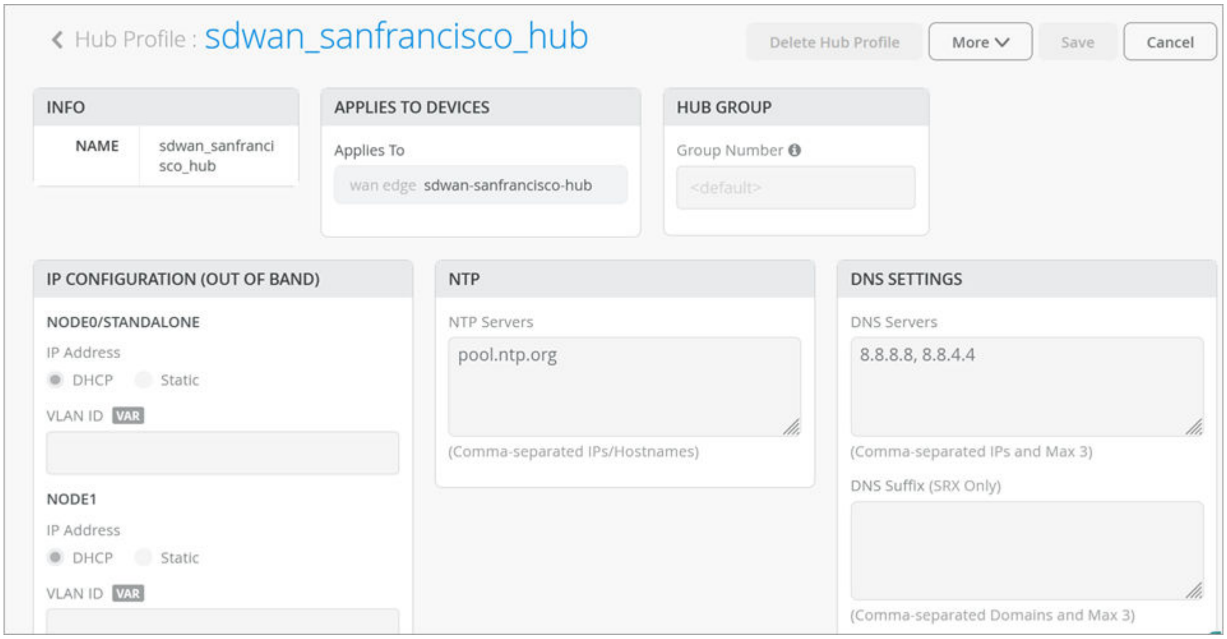
A final note on the overlay: The SRX Series and Session Smart Routers cannot exist in a single overlay. They can be paired via BGP at the hub, but their solutions to create intersite connectivity are unique and cannot work in concert. This means those with migration plans should identify which routes need advertisement and advertise at the hub.

Keep the following hub profile considerations in mind:

- Hub profiles must be built first, so spoke templates know where to connect.
  - Hubs must have static IPs for overlay endpoints.
  - The overlay endpoint configuration is exposed in the WAN edge spoke template.
- There is no limit to the number of hubs you can incorporate within these guidelines:
  - One hub per datacenter
  - Two hubs for redundancy (HA clusters)

Spokes choose the primary hub via traffic steering and an **Application Policy**. Zero-touch-provisioning (ZTP) requires DHCP (for physical implementation) unless ZTP is done and then migrated to the destination network. You can pre-stage the devices manually, too.

Figure 7: Hub Profile



Hub Profile : sdwan_sanfrancisco_hub

INFO

NAME: sdwan_sanfrancisco_hub

APPLIES TO DEVICES

Applies To: wan edge sdwan-sanfrancisco-hub

HUB GROUP

Group Number: <default>

IP CONFIGURATION (OUT OF BAND)

NODE0/STANDALONE

IP Address: ● DHCP ○ Static

VLAN ID VAR

NODE1

IP Address: ● DHCP ○ Static

VLAN ID VAR

NTP

NTP Servers: pool.ntp.org

(Comma-separated IPs/Hostnames)

DNS SETTINGS

DNS Servers: 8.8.8.8, 8.8.4.4

(Comma-separated IPs and Max 3)

DNS Suffix (SRX Only)

(Comma-separated Domains and Max 3)

Site Variables

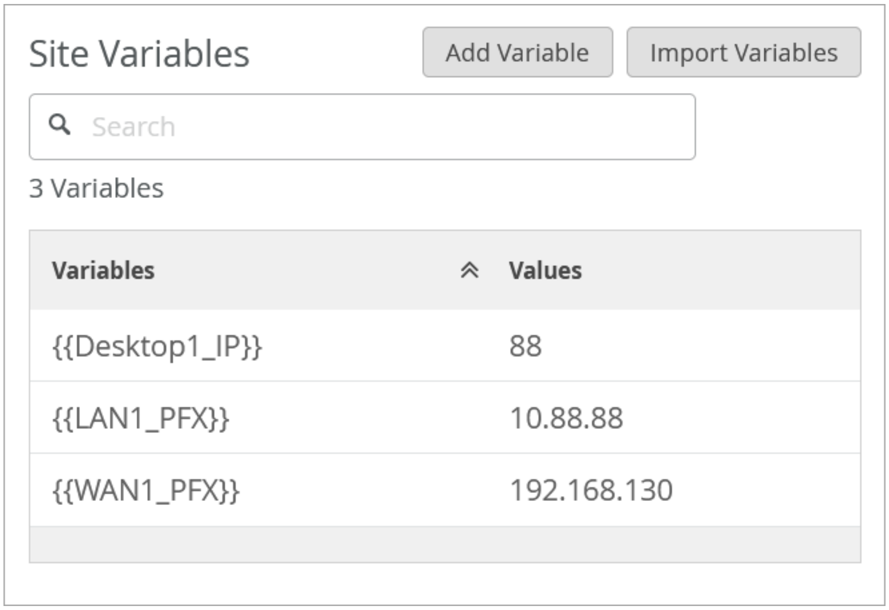
Site variables are configured on a per-site basis. When planning a network holistically, you can create standard templates for specific WAN edges and WAN edge clusters. Ideally, you have only one WAN edge device per site (or a single logical WAN edge if the device is clustered). Since variables can differ per site, administrators use them in templates or the WAN edge configuration page. The transformation happens when the configuration is rendered and pushed to the device.

Keep the following site variable considerations in mind:

- The syntax for variables matches Jinja2 and is contained within double curly brackets, like this: {{variableName}}
- The UI enforces the leading and trailing curly brackets as part of the name.
- Site variable limitations:
  - No spaces in the variable.
  - No special characters (except underscore) within the variable field.
  - Variables can be used only in one field and cannot specify an entire prefix.

  For example, 10.88.88.88/24 would need at least two variables, one for the IP address (10.88.88.88) and another for the prefix length (24).

Figure 8: Site Variables



3 Variables

Variables	Values
{{Desktop1_IP}}	88
{{LAN1_PFX}}	10.88.88
{{WAN1_PFX}}	192.168.130

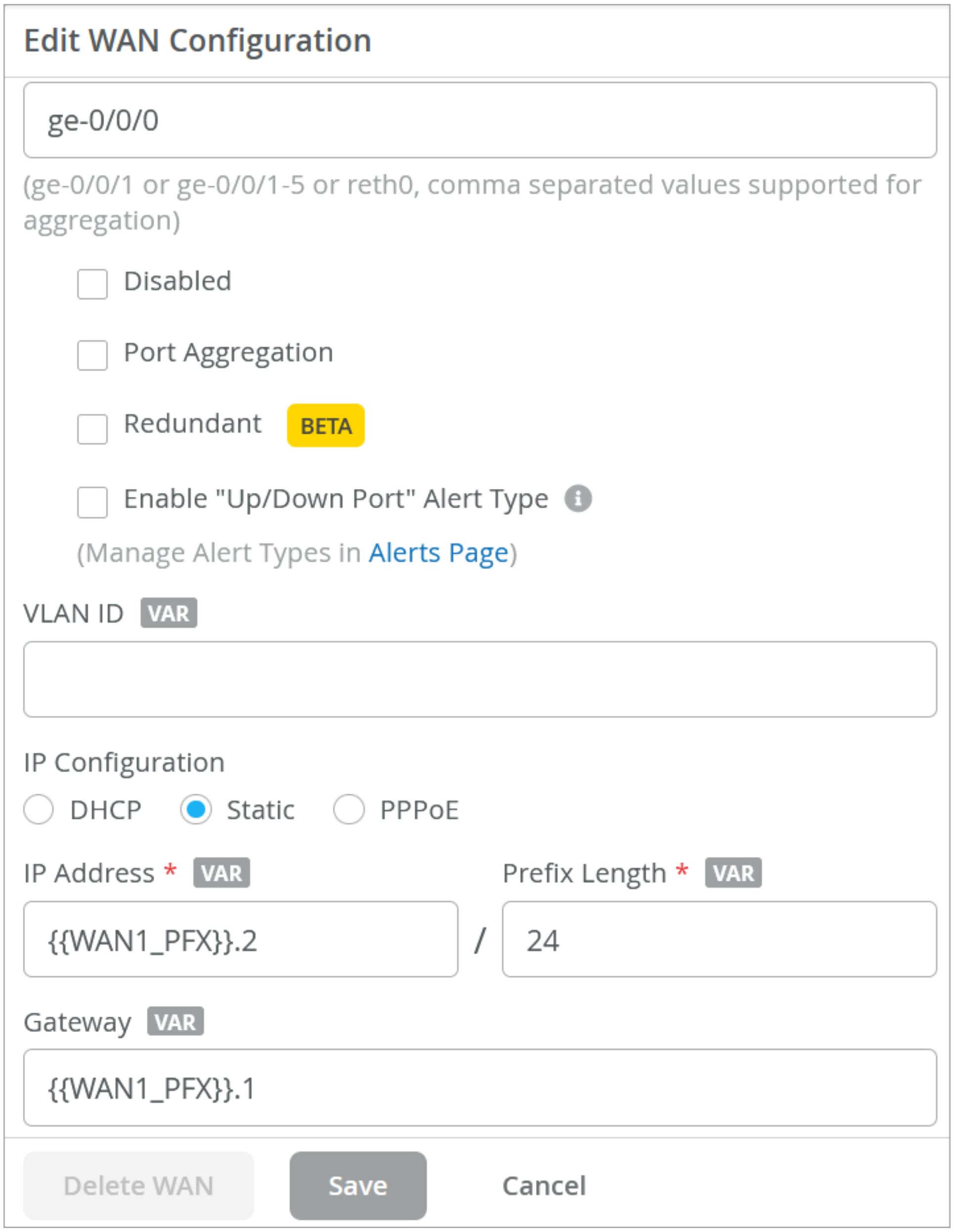
The best way to use the real power of templates is with site variables. Many configuration items are required to deploy the hardware. It makes sense to combine the WAN edge templates and site variables. Consider the following situation where you can define entire IP subnets of the first three octets, leaving minimal configuration at each device:

Create standard templates and place variables in standard interfaces like your WAN in either of these ways:

- With a WAN1PFX variable, let’s say {{192.168.170}}, and in the WAN field on the Configuration page, it would be {{WAN1PFX}}.1 for the local IP and {{WAN1PFX}}.2 for the gateway.

- You could define a {{WAN1IP}} and {{WAN1_GW}} pair of variables; however, there are places where the subnet may be reused but not the specific IP.

Figure 9: Site Variables in WAN Configuration



Edit WAN Configuration

ge-0/0/0

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

□ Disabled

□ Port Aggregation

□ Redundant BETA

□ Enable "Up/Down Port" Alert Type

(Manage Alert Types in Alerts Page)

VLAN ID VAR

IP Configuration

○ DHCP ● Static ○ PPPoE

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

Gateway VAR: {{WAN1_PFX}}.1

Another robust use case is the magic octet, where the third octet becomes a variable, and that variable may also apply to multiple fields. For example, a {{SITEID}} variable may be used for both the third octet and a VLAN tag. In that case, the network prefix may be 192.168.{{SITEID}}.1/24 with the {{SITE_ID}} VLAN ID. Remember that although WAN edge templates apply only to the WAN edge, site variables also apply to switches and APs. The purpose of the automation is to simplify deployments and increase reusability.

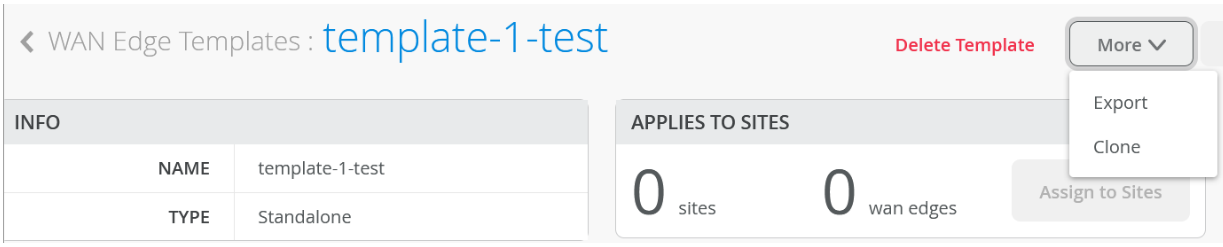
Introduction to Applying Templates

Remember that a site is a collection of all your assets in a single location. It is implied that there will only be a single WAN edge. A key feature of Mist management through the Juniper Mist AI is your ability to use configuration templates to group WAN edges and make bulk updates. Templates provide uniformity and convenience, while the hierarchy provides scale and granularity.

Import and Export Templates

There is no one-size-fits-all solution. You can have multiple templates. To save time, clone a template and modify it in the UI or export it for offline/programmatic modification to be imported later.

Figure 10: Export or Clone Template



NAME	template-1-test
TYPE	Standalone

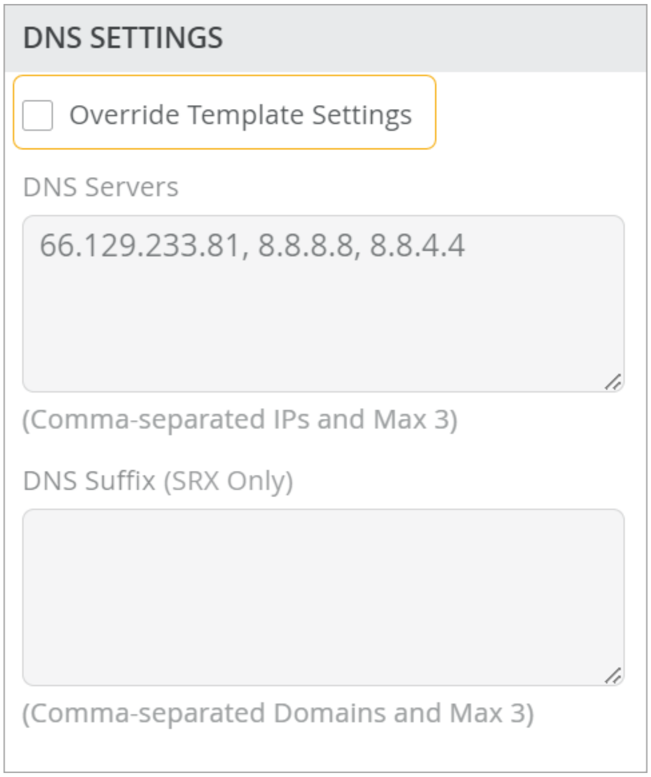
Modifying Template Sample

```
{
"type": "standalone",
"ip_configs": {
  "LAN": {
    "type": "static"
    "ip":
"{{LAN1_PFX}}.1" ,
      "netmask": "/24*
     }
  },
  "dhcpd_config" : {},
  "dns_servers" : [
    "8.8.8.8"
   ],
....
}
```

Overriding the Template

Templates apply to sites, which apply to devices. Templates are used to standardize configurations, but exceptions always exist. Rather than create a slightly different template for one site, you override the template configuration on the device.

Figure 11: Override Template Settings



DNS SETTINGS

☐ Override Template Settings

DNS Servers

66.129.233.81, 8.8.8.8, 8.8.4.4

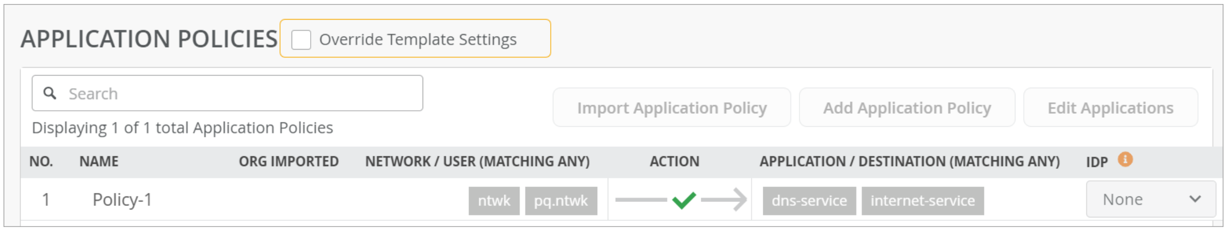
(Comma-separated IPs and Max 3)

DNS Suffix (SRX Only)

(Comma-separated Domains and Max 3)

If you need to override the template, you can enable the Override Template Settings option for the required configuration blocks on a per-device basis. Figure 12 on page 26 shows how you can override the DNS and the **Application Policy** but none of the other settings, such as WANs, LANs, or NTP servers.

Figure 12: Application Policy



APPLICATION POLICIES ☐ Override Template Settings

Displaying 1 of 1 total Application Policies

NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP
1	Policy-1		ntwk pq.ntwk	✓	dns-service internet-service	None

The screenshot illustrates an all-or-nothing action. Enabling override template settings means the configuration block will no longer inherit any configurations from the WAN edge template. Changes to that configuration block of your template no longer apply to this device. Future changes must be done manually in both places (per configuration block, no mixing and matching).

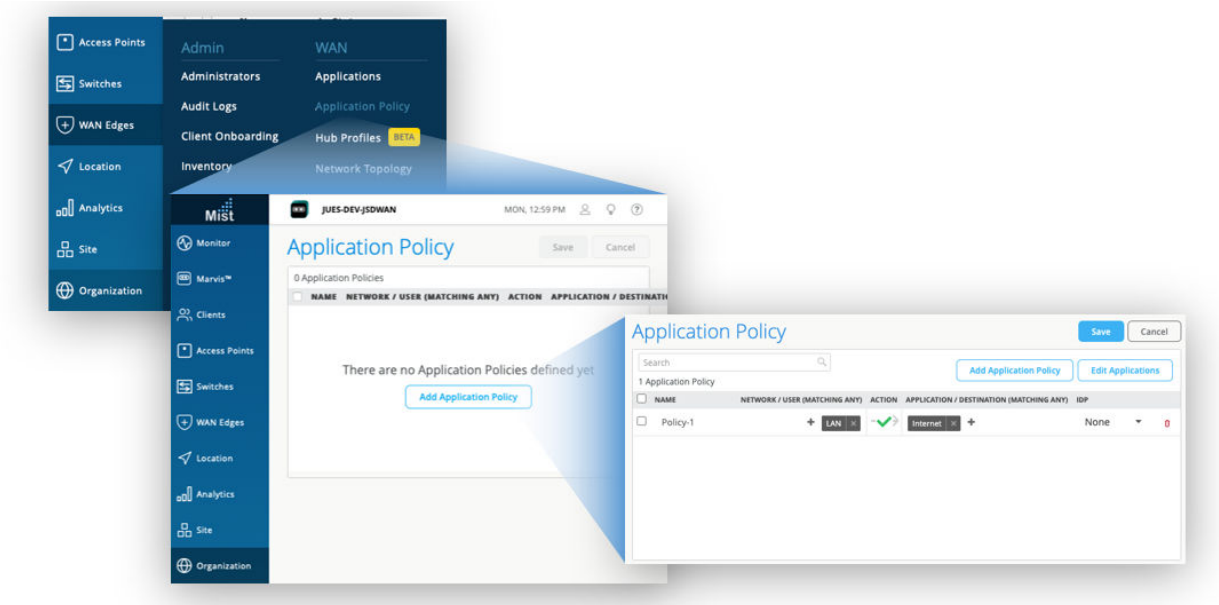
You need to have one of the following role assigned to you in order to override the configuration:

- Super User
- Network Admin (All Sites Access)
- Network Admin (Site Group or Specific Sites Access)

Organizational-Level Application Policy

Figure 13: Organizational-Level Application Policy

Figure 13 on page 27 shows **Application Policy** configuration option at the organization level.



0 Application Policies

□	NAME	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATI

There are no Application Policies defined yet

1 Application Policy

□	NAME	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP
□	Policy-1	+ LAN ×	✓	Internet × +	None

Although templates save time on deploying multiple devices, you may have various templates to account for different device models or slightly different configurations. You can create the same **Application Policy** on each template, but there is a shortcut to using an organizational-level **Application Policy**. With an organizational-level **Application Policy**, you can create importable application rules into WAN edge templates and hub profiles for large-scale network topologies.

Let's explore some best practices and restrictions for using an organizational-level **Application Policy**. Each organizational-level **Application Policy** requires a globally unique name, or you run into errors when saving the configuration. The imported policy has all the fields dimmed because it is not meant to be modified. There's no organizational-level **traffic steering**, which makes sense, because traffic steering applies to local connections and intent.

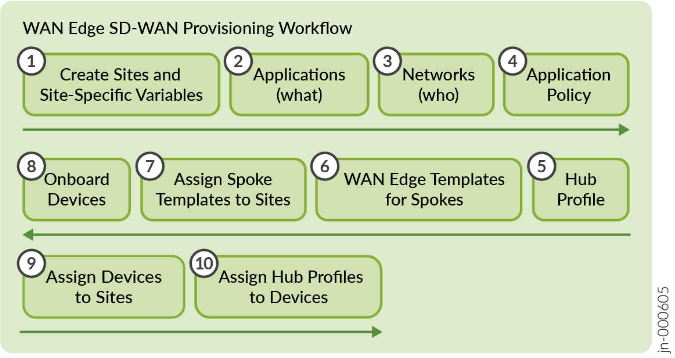
Consider applying an organizational-level **Application Policy** to a LAN block or one subnet. If you create a LAN "supernet" of a 10/8, the policy will allow anything sourced from 10/any to reach the Internet, meaning it would work for all your sites. This is why planning is crucial. Design your network to streamline troubleshooting with similar traffic patterns regardless of deployment. For example, some sites have LTE, and traffic must egress there on that site instead of others. In addition, some sites are standalone, and others are SD-WAN. A universal policy could apply to both by telling traffic steering on standalone sites to go out the WAN to the underlay, whereas the sites are going to the overlay for the SD-WAN spokes.

In summary, the use case for an organizational-level policies is to describe network-wide traffic patterns regardless of the site; as a policy, you define what is and is not allowed. Then, when applied to the site or template (which applies to places), you add the steering portion giving you the final piece of the puzzle.

WAN Design Considerations

Figure 14 on page 28 shows the workflow for WAN edge provisioning.

Figure 14: WAN Edge Provisioning 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

Reviewing the blocks that make up the completed project is essential to deploy an SD-WAN, as follows:

1. Think about "who" (**Network**) makes up the source of requests in your organization.

2. Consider "what" destinations (**Applications**) users access.

3. Where do those elements go in your organization? Consider site types.

4. Finally, consider "how" (**Traffic Steering**) those users get and gain access to their traffic destinations.

5. Now you can use the power of Mist AI, templates, and variables for scale.

SD-WAN Provisioning

The order of operations matters. When preparing to implement SD-WAN provisioning, complete tasks in this order:

1. First, plan your network with templates, thinking about the deployment holistically.

2. Hub profiles must come before WAN edge spoke templates.

3. Design with your **Applications** (destinations of traffic) first, and then **Networks** (who).

You can analyze apps and become more granular later.

1. Make sure you know your networks (sources of traffic).

Networks inform policy and traffic steering.

- Apply the appropriate **Application Policy** to both ends (spokes and hubs).

Strive for end-to-end reachability when establishing overlay endpoints. Keep in mind that you can't connect an isolated MPLS endpoint to an Internet endpoint.

RELATED DOCUMENTATION

Juniper Mist WAN Assurance Platform Considerations | 10

Introduction to Juniper Mist WAN Assurance | 2

3

CHAPTER

WAN Configuration for Session Smart Routers

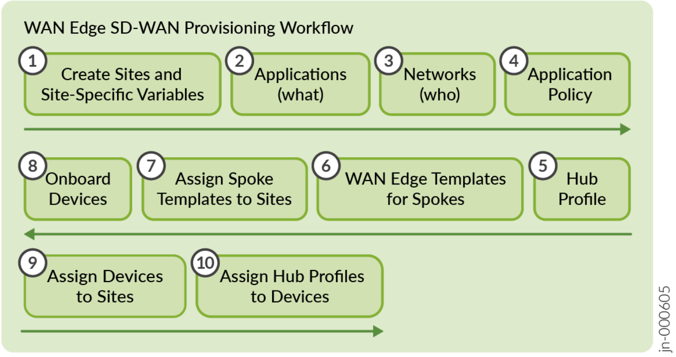
WAN Assurance Configuration Overview

This overview illustrates how to use the Juniper Mist™ cloud console (the GUI) to provision a simple hub-and-spoke network using Juniper® Session Smart™ Routers. 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. We also assume and that the physical connections (cabling) needed to support the configuration are in place and that you know the interfaces, and VLANs are valid for your sandbox.

Figure 15 on page 31 illustrates the workflow for configuring WAN using the Juniper Mist cloud portal.

Figure 15: 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
5 Hub Profile
6 WAN Edge Templates for Spokes
7 Assign Spoke Templates to Sites
8 Onboard Devices
9 Assign Devices to Sites
10 Assign Hub Profiles to Devices
jn-000605

The sequence of configuration tasks in this example:

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. See "Configure Sites and Variables" on page 33.

2. Setup Networks—Define the Networks. Networks are the source of traffic defined through IP prefixes. See "Configure Networks" on page 38.

3. Configure Applications—Applications are destinations that you define using IP prefixes. Applications represent traffic destinations. See "Configure Applications" on page 48.

4. Create Application Policies— Application policies determine which networks or users can access which applications, and according to which traffic steering policy. See "Configure Application Policies" on page 58.

5. Create hub profiles—You assign hub profile to standalone or clustered devices to automate overlay path creation. See "Configure Hub Profiles" on page 66.

6. Create WAN edge templates—WAN edge templates automatically configure repetitive information such as an IP address, gateway, or VLAN when applied to sites. See "Configure WAN Edge Templates" on page 92.

7. Onboard devices—Onboard your devices by assigning them to a site. 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. See "Assign Templates to Sites" on page 132.

You can perform the following tasks on your devices for providing additional security measures:

- Setup Secure Edge Connectors—Perform traffic inspection by Secure Edge for the WAN edge devices managed by Juniper Mist Cloud portal. See Set Up Secure Edge Connectors

  .

- Configure IDP-Based Threat Detection—Monitor the events occurring on your network and proactively stop attacks and prevent future attacks. See "IDP-Based Threat Detection" on page 138.

Upgrade software on your device to take advantage of new enhancements.

- Upgrade Software—Upgrade the software on your device through the Juniper Mist portal in a few simple steps. See "Upgrade WAN Edge Device" on page 150.

RELATED DOCUMENTATION

Introduction to Juniper Mist WAN Assurance | **2**

Juniper Mist WAN Assurance Platform Considerations | **10**

Juniper Mist WAN Assurance Configuration Hierarchy | **13**

Configure Sites and Variables for Session Smart Routers

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. Users with required privileges can configure and modify sites. The configuration changes in the sites are automatically applied to (or at least available to) all your Juniper® Session Smart™ Routers included in the site.

Site variable 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.

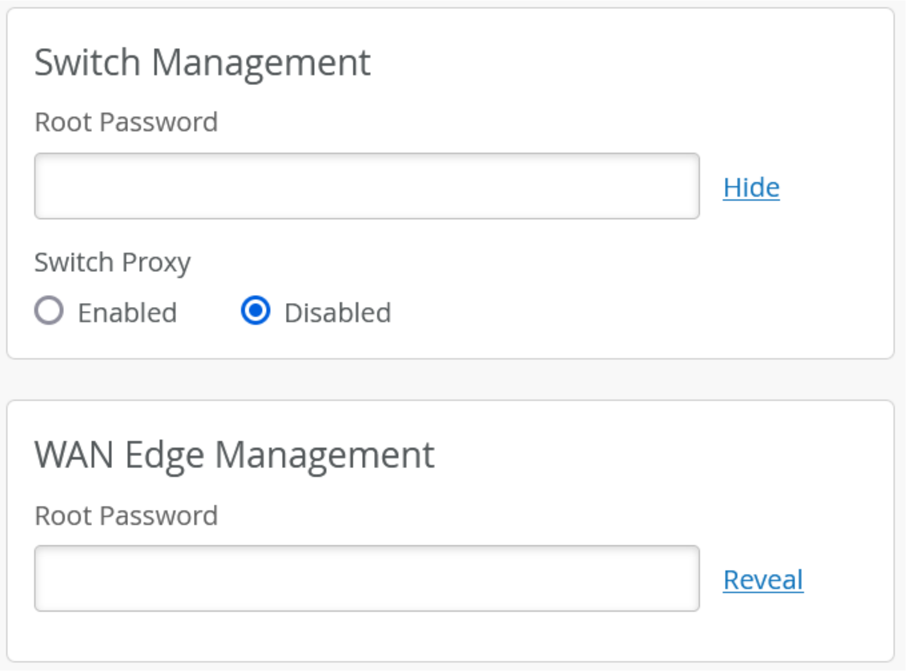
You can define the site variable by using double brackets to format the variable name. Example: {{SPOKE_LAN1_PFX}}

To configure sites:

1. In the Juniper Mist cloud portal, click **Organization** > **Admin** > **Site Configuration**.
   A list of existing sites, if any, appears.
2. Click **Create Sites** in the upper right corner. The New Site window appears.
   a. 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).

   b. Enter the street address of your site, or use the map to locate it.
3. Scroll down the page to the **Switch Management** and **WAN Edge Management** settings pane, and configure the root password.

Figure 16: Setting Root Password



Switch Management

Root Password

Hide

Switch Proxy

○ Enabled ● Disabled

WAN Edge Management

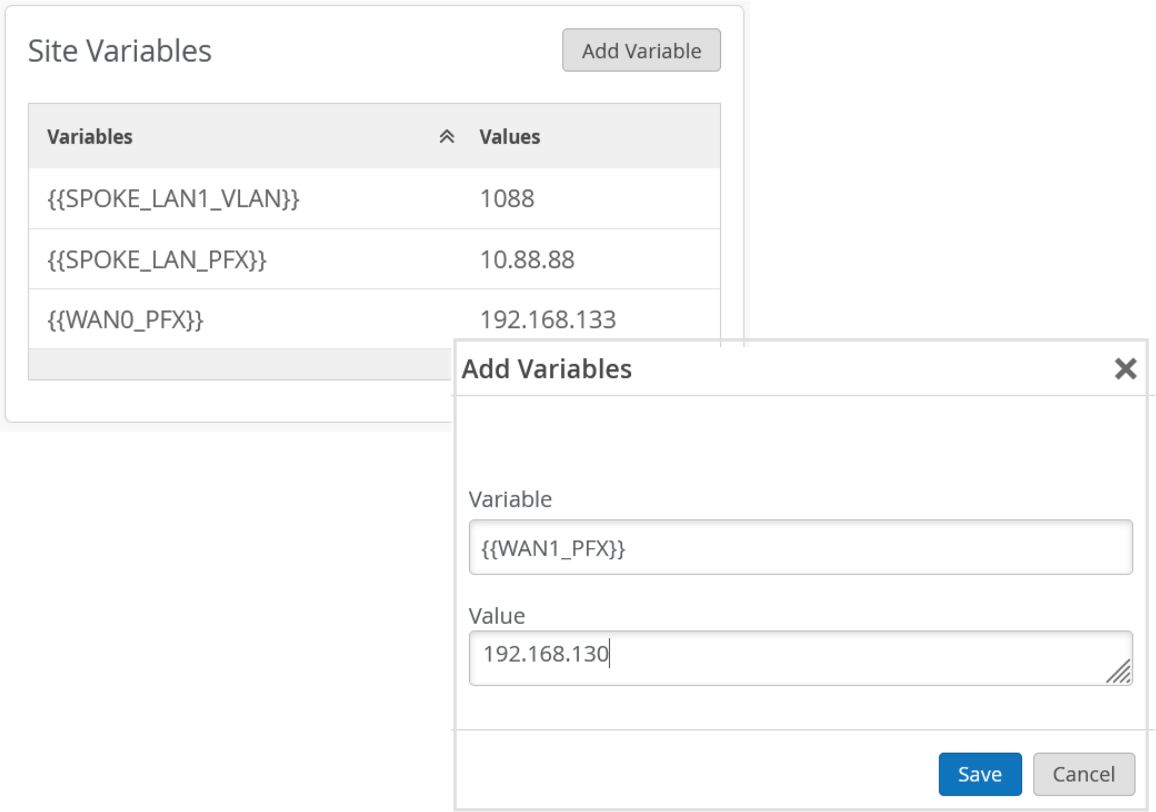
Root Password

Reveal

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.

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

Figure 17: 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

6. Use Figure 17 on page 35 to complete the list of variables 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

Table 1: Variable Settings for Sites *(Continued)*

Site Name	Variable	Value
	{{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

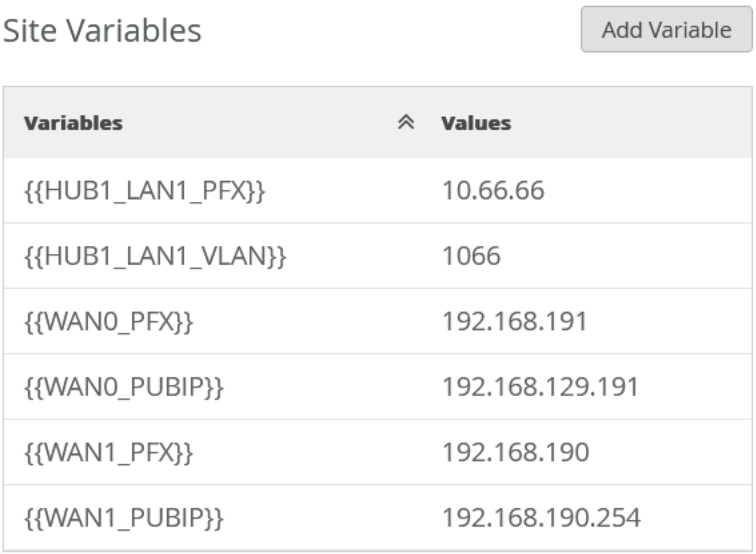
NOTE:

- 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 in 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.

7. Click **Save** to add the variable to the list.
   Figure 18 on page 37 shows the list of newly created variables.

Figure 18: Site Variables Sample



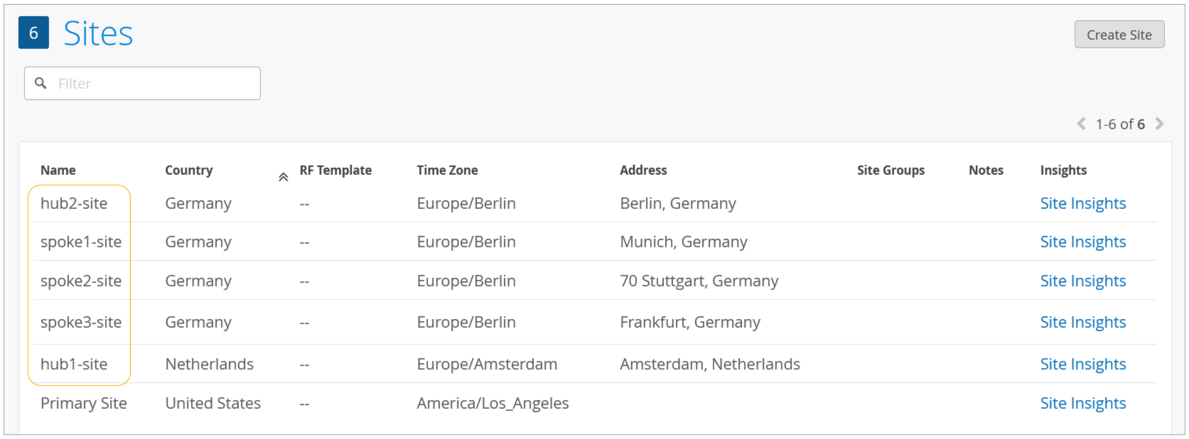
Site Variables

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

8. Click **Save** to save your changes for the site

Figure 19 on page 38 shows the list of newly created sites.

Figure 19: Newly Created Sites



Name	Country	RF Template	Time Zone	Address	Site Groups	Notes	Insights
hub2-site	Germany	--	Europe/Berlin	Berlin, Germany			Site Insights
spoke1-site	Germany	--	Europe/Berlin	Munich, Germany			Site Insights
spoke2-site	Germany	--	Europe/Berlin	70 Stuttgart, Germany			Site Insights
spoke3-site	Germany	--	Europe/Berlin	Frankfurt, Germany			Site Insights
hub1-site	Netherlands	--	Europe/Amsterdam	Amsterdam, Netherlands			Site Insights
Primary Site	United States	--	America/Los_Angeles				Site Insights

RELATED DOCUMENTATION

Juniper Mist WAN Assurance Configuration Hierarchy | 13
WAN Assurance Configuration Overview | 31
Configure Networks for Session Smart Routers | 38

Configure Networks for Session Smart Routers

IN THIS SECTION

Networks are sources of the request in your Juniper WAN Assurance design. On the Juniper® Session Smart™ Router, networks create tenants in the background for SVR and the Session Smart Router identifies tenants at the logical interface (network interface). LAN and WAN interface configurations identify your tenant (request source).

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 a Network:

Site Variables

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 on page 39 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. If your device is using an untagged interface, you should use 1 as the VLAN ID instead of the variable.
Access to Mist Cloud	Check the option to allow Session Smart Router services to access the Juniper Mist cloud.

Table 2: Network Options *(Continued)*

Fields	Description
Advertised to the Overlay	Check the option to advertise the network to the hub devices through the overlay tunnels. When you select this option, the system displays following additional options for advertising: • **Advertise to Other Spokes**—Network to advertise the network prefix to other spokes (default option). If you want the network to advertise the prefix only to hubs (not other spokes), disable the default option. • **Advertise to Hub LAN BGP Neighbor**—Network to advertise the network prefix to any LAN BGP neighbor at the hub (default option). If you do not want to advertise, disable the default option. • **Advertise to Hub LAN OSPF Neighbor (SRX Only)**—Network to advertise the network prefix to any LAN OSPF neighbor at the hub (default option). If you do not want to advertise, disable the default option. • **Override Prefix to Advertise**— Enable this option when the prefix to advertise to the Hubs is not the original network but a different prefix. This is typically used when enabling NAT options. When you select this option, enter IP Address and Prefix Length. The portal also displays following route summarization options: • **Hub Overlay Summarization**—Enable the network to summarize the network prefix advertised to the overlay. For example: Juniper Mist portal can summarize 192.168.1.0/24 to 192.168.0.0/16. This feature limits the number of BGP updates received by a hub from each spoke and sent by the hub back to all the other spokes.

Table 2: Network Options *(Continued)*

Fields	Description
	- **Hub LAN BGP Summarization**—Enable the network to summarize the network prefix advertised to the LAN BGP neighbor. For example: Juniper Mist portal can summarize 192.168.1.0/24 to 192.168.0.0/16. - **Hub LAN OSPF Summarization**—Enable the network to summarize the network prefix advertised to the LAN OSPF neighbor. For example: Juniper Mist portal can summarize 192.168.1.0/24 to 192.168.0.0/16. - **Route Summarization**—Summarize local routes towards overlay. You can specify the IP addresses and prefix length of the summarized routes. Session Smart Routers support summarization when the network is attached to the spoke only.
Networks not directly attached (SSR Only)	Select the networks that are not directly connected networks that arrive on this network assigned to a LAN.
Users	(Optional) Additional networks or users. Example: remote networks or users connected to the main network. 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. Click the **Add Static NAT** option and enter the **Name** , **Internal IP**, **External IP** and select option to apply to outgoing traffic on **Underlay** or **Overlay**. Enter **WAN Name** for SRX Series Devices.

Table 2: Network Options *(Continued)*

Fields	Description
Destination NAT	(Optional) Translate the destination IP address of a packet. Click the **Add Destination NAT** option and enter the **Name** , **Internal IPInternal Port**, **External IP**, **External Port** and select option to apply to outgoing traffic on **Underlay** or **Overlay**. Enter **WAN Name** for SRX Series Devices.

3. Complete the configuration according to the details available in Table 3 on page 42. 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: Values for Network Configuration

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

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 Session Smart Router in hubs can use the same username (All) and IP prefix (10.0.0.8) to identify all spoke LAN interfaces using a single rule.

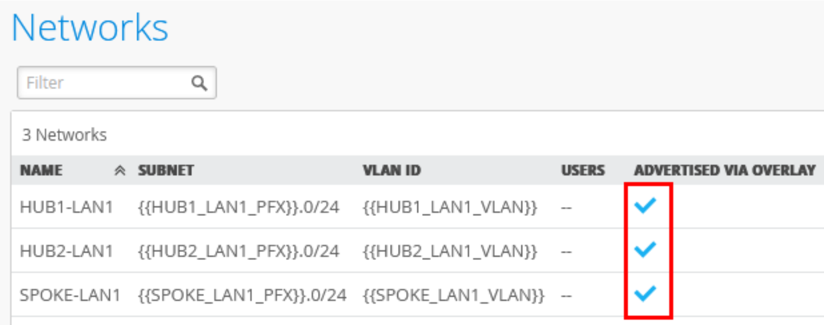
NOTE: When you use variables, do not assume that the system imports all LAN segments on the hub site automatically. Sometimes, the system may apply an Any netmask, which has a wide scope and may generate security issues.

NOTE:

4. Click **Add**.

   Figure 20 on page 43 shows the list of newly created networks.

Figure 20: Networks Summary



Networks

Filter

3 Networks

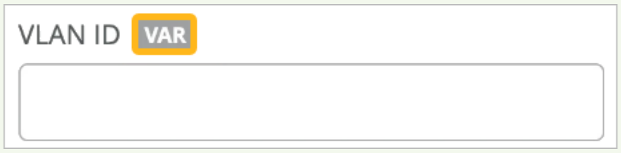
NAME	SUBNET	VLAN ID	USERS	ADVERTISED VIA OVERLAY
HUB1-LAN1	{{HUB1_LAN1_PFX}}.0/24	{{HUB1_LAN1_VLAN}}	--	✓
HUB2-LAN1	{{HUB2_LAN1_PFX}}.0/24	{{HUB2_LAN1_VLAN}}	--	✓
SPOKE-LAN1	{{SPOKE_LAN1_PFX}}.0/24	{{SPOKE_LAN1_VLAN}}	--	✓

Site Variables

You can configure the site variables on a per-site basis. When planning a network holistically, you can configure specific WAN edge devices and WAN edge clusters using templates.

Site variables allow you to use the same network definition with different values for each site without having to define multiple networks. Variables have the format {{variable_name}}.

TIP: The fields with this label also display the matching variables (if configured) as you start typing a specific variable in it. This field lists variables from all sites within the organization.

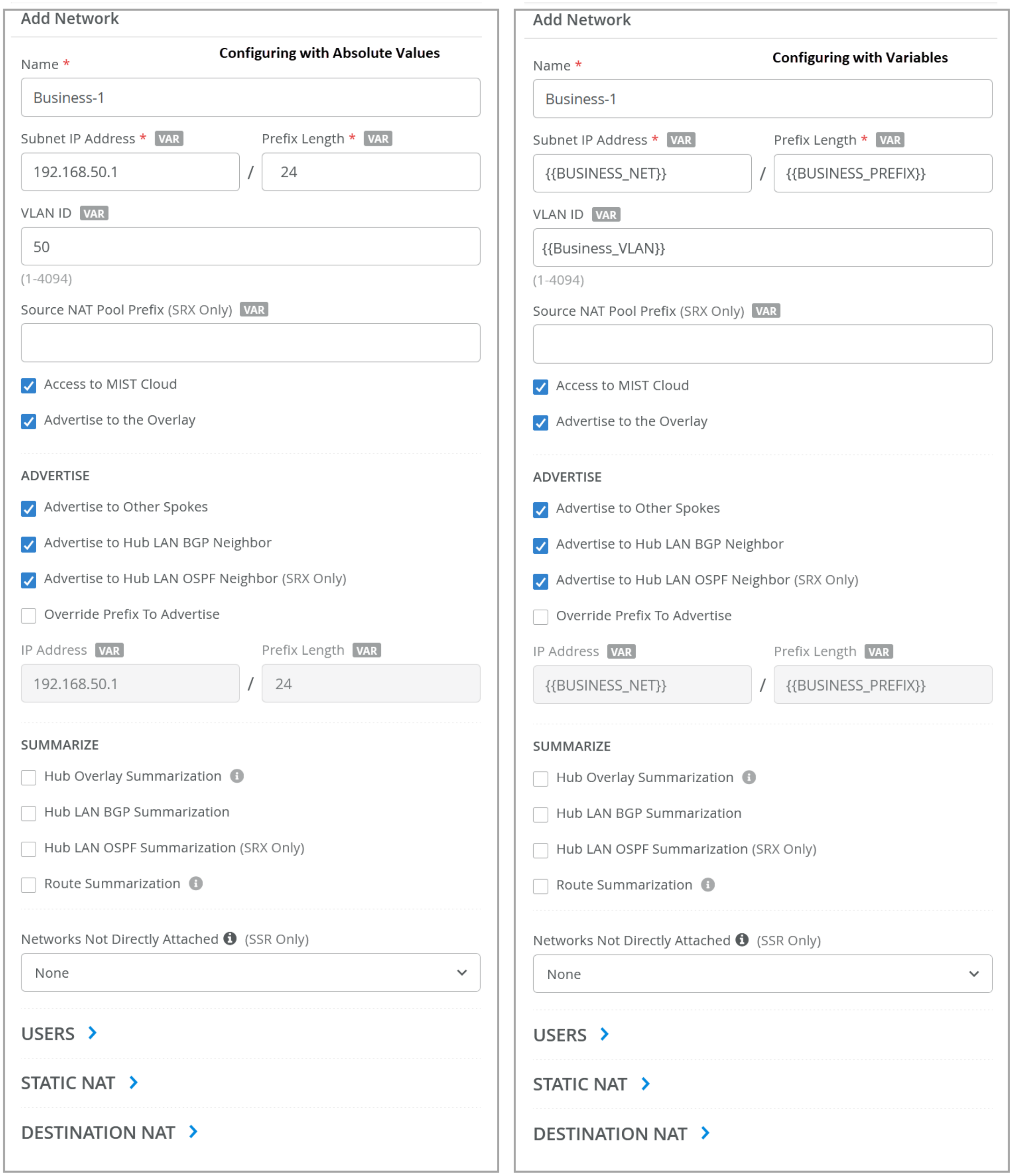


The organization-wide list of variables can be viewed using **GET /api/v1/orgs/:org_id/vars/search?var=***. This list is populated as variables are added under site settings.

Defining networks with variables is common practice in WAN edge template configuration.

Figure 21 on page 45 shows two samples of configuration of a network using absolute values and using site variables.

Figure 21: Configuring Networks with Absolute Values and Variables



Add Network

Configuring with Absolute Values

Name *
Business-1

Subnet IP Address * VAR: 192.168.50.1 / Prefix Length * VAR: 24

VLAN ID VAR: 50
(1-4094)

Source NAT Pool Prefix (SRX Only) VAR:

☑ Access to MIST Cloud

☑ Advertise to the Overlay

ADVERTISE

☑ Advertise to Other Spokes

☑ Advertise to Hub LAN BGP Neighbor

☑ Advertise to Hub LAN OSPF Neighbor (SRX Only)

□ Override Prefix To Advertise

IP Address VAR: 192.168.50.1 / Prefix Length VAR: 24

SUMMARIZE

□ Hub Overlay Summarization

□ Hub LAN BGP Summarization

□ Hub LAN OSPF Summarization (SRX Only)

□ Route Summarization

Networks Not Directly Attached (SSR Only): None

USERS >

STATIC NAT >

DESTINATION NAT >

Add Network

Configuring with Variables

Name *
Business-1

Subnet IP Address * VAR: {{BUSINESS_NET}} / Prefix Length * VAR: {{BUSINESS_PREFIX}}

VLAN ID VAR: {{Business_VLAN}}
(1-4094)

Source NAT Pool Prefix (SRX Only) VAR:

☑ Access to MIST Cloud

☑ Advertise to the Overlay

ADVERTISE

☑ Advertise to Other Spokes

☑ Advertise to Hub LAN BGP Neighbor

☑ Advertise to Hub LAN OSPF Neighbor (SRX Only)

□ Override Prefix To Advertise

IP Address VAR: {{BUSINESS_NET}} / Prefix Length VAR: {{BUSINESS_PREFIX}}

SUMMARIZE

□ Hub Overlay Summarization

□ Hub LAN BGP Summarization

□ Hub LAN OSPF Summarization (SRX Only)

□ Route Summarization

Networks Not Directly Attached (SSR Only): None

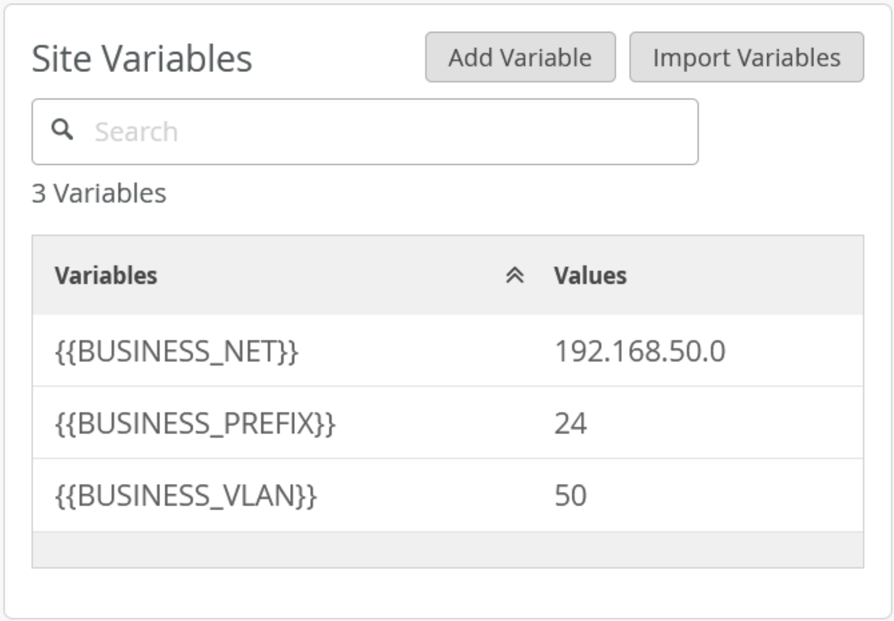
USERS >

STATIC NAT >

DESTINATION NAT >

You can define the site variables in **Organization** > **Admin**> **Site Configuration** pane.

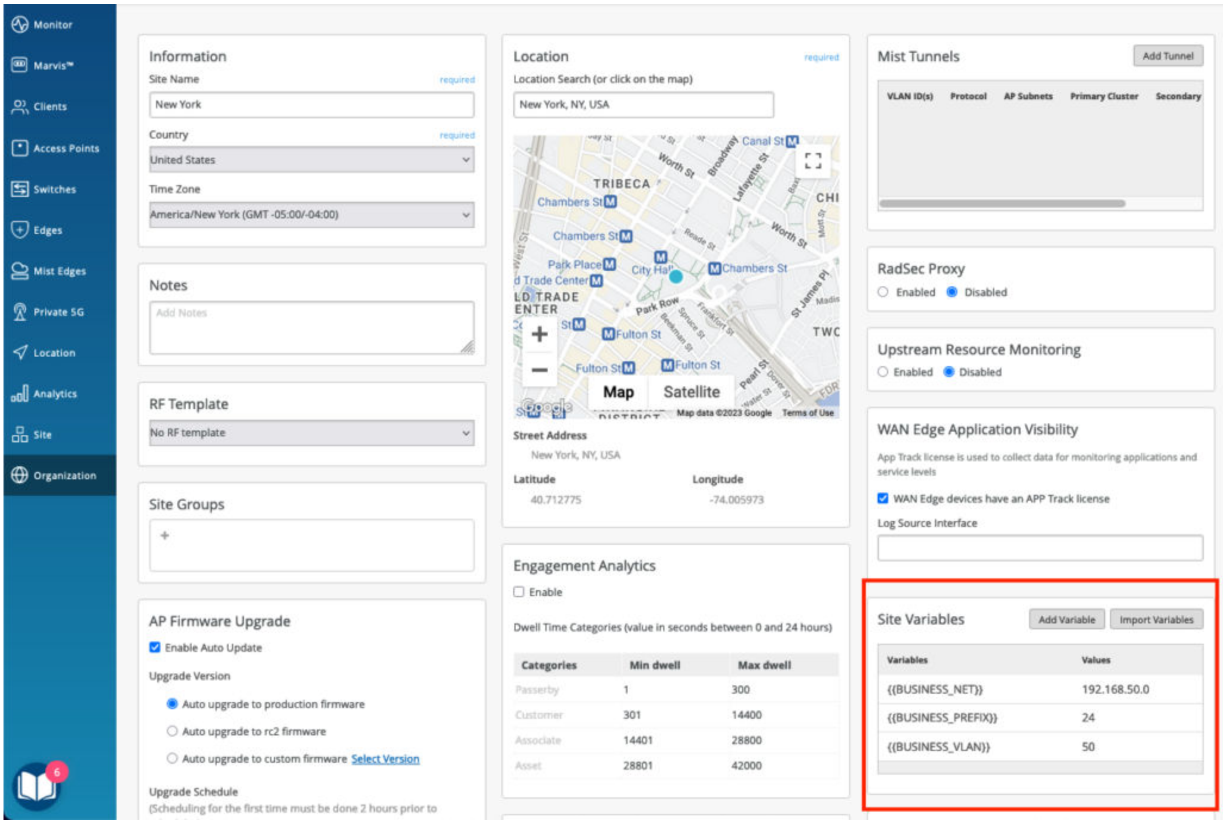
Figure 22: Site Variables Settings Pane



Variables	Values
{{BUSINESS_NET}}	192.168.50.0
{{BUSINESS_PREFIX}}	24
{{BUSINESS_VLAN}}	50

This task uses variables for the VLAN ID and subnet IP address. Site variables that contain the first three octets substitute the subnet IP address variable values as shown in Figure 23 on page 47.

Figure 23: Site Variables Displayed in Site Configuration Page



Information

Site Name: New York

Country: United States

Time Zone: America/New York (GMT -05:00/-04:00)

Notes: Add Notes

RF Template: No RF template

Site Groups

AP Firmware Upgrade

☑ Enable Auto Update

Upgrade Version

● Auto upgrade to production firmware

○ Auto upgrade to rc2 firmware

○ Auto upgrade to custom firmware Select Version

Upgrade Schedule
(Scheduling for the first time must be done 2 hours prior to

Location

Location Search (or click on the map): New York, NY, USA

Street Address: New York, NY, USA

Latitude: 40.712775

Longitude: -74.005973

Engagement Analytics

☐ Enable

Dwell Time Categories (value in seconds between 0 and 24 hours)

Categories	Min dwell	Max dwell
Passerby	1	300
Customer	301	14400
Associate	14401	28800
Asset	28801	42000

Mist Tunnels — Add Tunnel

VLAN ID(s)	Protocol	AP Subnets	Primary Cluster	Secondary

RadSec Proxy: ○ Enabled ● Disabled

Upstream Resource Monitoring: ○ Enabled ● Disabled

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

Site Variables — Add Variable — Import Variables

Variables	Values
{{BUSINESS_NET}}	192.168.50.0
{{BUSINESS_PREFIX}}	24
{{BUSINESS_VLAN}}	50

RELATED DOCUMENTATION

- Juniper Mist WAN Assurance Configuration Hierarchy | 13
- WAN Assurance Configuration Overview | 31
- Configure Sites and Variables for Session Smart Routers | 33
- Configure Applications for Session Smart Routers | 48
- Configure Application Policies on Session Smart Routers | 58

Configure Applications for Session Smart Routers

IN THIS SECTION

Applications represent traffic destinations. On the Juniper® Session Smart™ Router, applications create services in the background for SVR. Applications can be ports, protocols, prefixes, custom domains, or app names from the built-in AppID library.

Applications are the services or apps that your network users will 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).

Configure Applications

To configure applications:

1. In the Juniper Mist portal, click **Organization** > **WAN**> **Applications**.
   A list of existing applications, if any, appears.
2. Click the **Add Applications** button in the upper right corner.

   The Add Application window appears.

   Table 4 on page 49 summarizes the options you can set in an application configuration.

TIP: The fields with this label also display the matching variables (if configured) as you start typing a specific variable in it. This field lists variables from all sites within the organization.

The organization-wide list of variables can be viewed using **GET /api/v1/orgs/:org_id/vars/search?var=***. This list is populated as variables are added under site settings.

Table 4: Applications Options

Fields	Description
Name	Enter a unique name for the application. You can use upto 32 characters for naming the application including alphanumerics, underscores, and dashes.
Description	Enter a description of the application and context.
Type	Enter the application type: • Custom Applications. See "Configure Applications with Custom Applications" on page 53. • Predefined Applications. See "Configure Applications with Predefined Applications" on page 54. • URL Categories. See "Configure Applications with URL Categories" on page 55. • Custom URLs. See "Configure Applications with Custom URLs" on page 57.
IP Address	(For custom applications) Enter the network IP address, including prefix (if any) of the application.

Table 4: Applications Options *(Continued)*

Fields	Description
Domain Name	Enter the domain name of the application. The domain name is used in cloud breakout profiles to generate the fully qualified domain name (FQDN). The cloud security providers use the FQDN to identify the IPsec tunnels. For example, juniper.example.com.
Protocol and Port Ranges	(For custom applications) Enter details about protocols, protocol numbers, and port ranges (start and end ports) that the application is using. **NOTE**: Click the blue Add (+) icon to select multiple protocols.

Table 4: Applications Options *(Continued)*

Fields	Description
Advanced Settings	Configure the optional advanced traffic type settings that includes: • Traffic type—Select the type of traffic (example: voice, video, data). The portal provides a list of predefined traffic type. When you select any of the defined traffic types such as gaming or video streaming, all the below parameters will be selected automatically. If you select **Custom**, you can configure the following values: • Failover policy (Session Smart Routers only)—Revertible or Non-revertible. ◦ **Revertible**: Traffic automatic switches back to the primary link when the primary link recovers. ◦ **Non-Revertible**: Requires manual intervention to revert to the primary link. When traffic switches to the secondary link due to primary link failure, it does not automatically revert back to the primary link. ◦ **None**: Disable session failover. If the primary link on your device fails to meet the Service Level Agreement (SLA), existing sessions remain on the primary link, while new sessions will be redirected to the secondary link. When the primary link recovers and meets the SLA, existing sessions on the secondary link will continue, and any new sessions will start on the primary link. This behavior remains consistent even if the entire link goes down. • Traffic class—Best effort, High,Medium, and Low. ◦ **Best Effort**: No special treatment, suitable for non-critical data.

Table 4: Applications Options *(Continued)*

Fields	Description
	- **Medium**: Prioritized over **Best Effort**, used for non-latency-sensitive applications. - **High**: Critical applications with low latency requirements. - **Low**: Background or non-urgent traffic . - DSCP class—DSCP Class in the range 0-63. When you select a traffic class (Best Effort, High, Medium, or Low), the applicable default DSCP Class value is displayed as a help text. You can choose to override it. By configuring DSCP classes, you can map specific traffic types to appropriate QoS levels. - Maximum latency—Maximum latency in the range 0-4294967295. Setting a maximum latency threshold ensures that SD-WAN avoids links with excessive delay - Maximum jitter—Maximum jitter in the range 0-4294967295. By specifying a maximum jitter threshold, SD-WAN selects stable links to maintain predictable performance - Maximum loss—Maximum loss in the range 0-100. Configuring a maximum loss threshold helps SD-WAN avoid links with high packet loss rates.

3. Complete the configuration as per details provided in "Configure Applications with Custom Applications" on page 53 to configure applications with custom applications.

   If you want to create applications using predefined applications or URL categories, see the following sections:

   - "Configure Applications with Predefined Applications" on page 54
   - "Configure Applications with URL Categories" on page 55
   - "Configure Applications with Custom URLs" on page 57

Configure Applications with Custom Applications

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.

To define custom applications:

1. In the Juniper Mist cloud portal, under the **Add Application** pane, select the **Type** as **Custom Apps**.
2. Create a custom application using IP prefixes. Refer to the details in Table 5 on page 53. 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 5: 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 10.0.0.8). A wildcard match allows easy extensions without a need to change the ruleset in your environment.

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

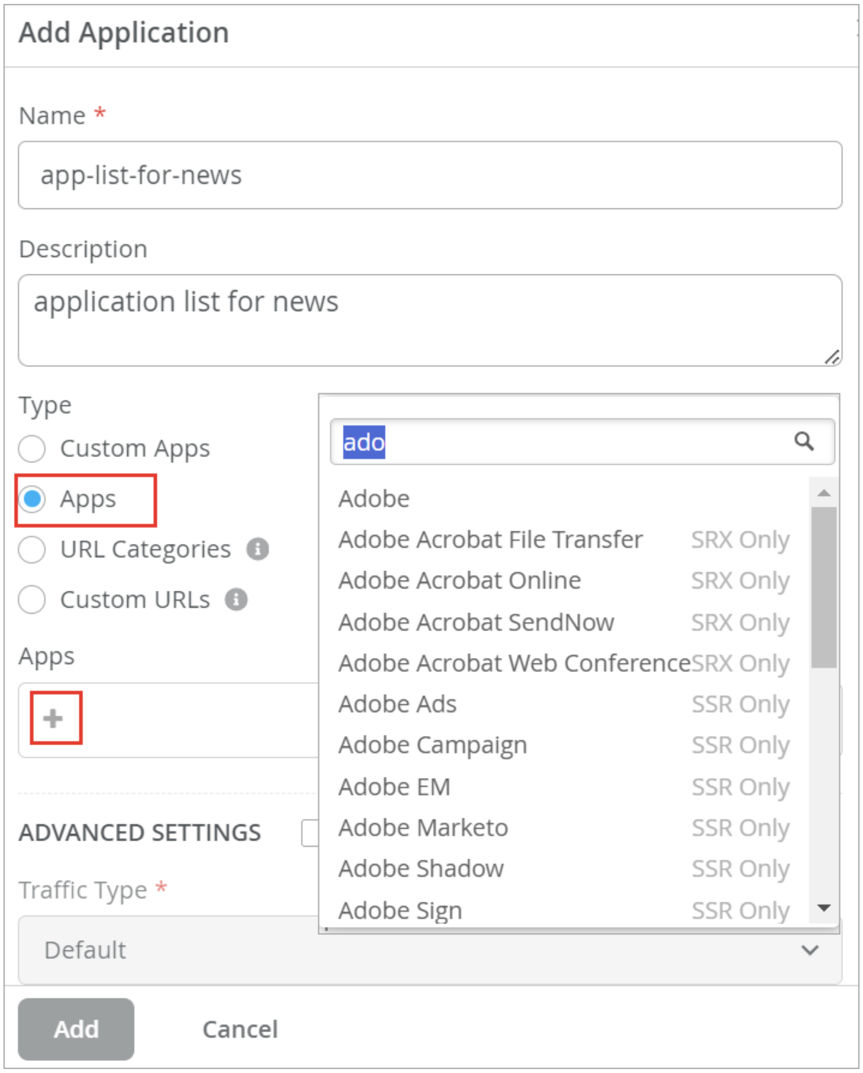
Configure Applications with Predefined Applications

Juniper Mist cloud provides a list of known applications that you can use to define an Application.

To configure predefined applications:

1. In the Mist portal, in the **Add Application** pane, select the **Type** as **Apps**.
2. Click the Add (**+**) icon to display the list of available predefined applications.

Figure 24: Predefined Applications



Add Application

Name *

app-list-for-news

Description

application list for news

Type

○ Custom Apps

● Apps

○ URL Categories

○ Custom URLs

Apps

ADVANCED SETTINGS

Traffic Type *

Default

ado

Adobe	
Adobe Acrobat File Transfer	SRX Only
Adobe Acrobat Online	SRX Only
Adobe Acrobat SendNow	SRX Only
Adobe Acrobat Web Conference	SRX Only
Adobe Ads	SSR Only
Adobe Campaign	SSR Only
Adobe EM	SSR Only
Adobe Marketo	SSR Only
Adobe Shadow	SSR Only
Adobe Sign	SSR Only

Applications that are specific to only SSRs are marked as 'SSR Only'.

3. Select one or more applications from the drop-down menu.
4. Click **Add** to save your changes.

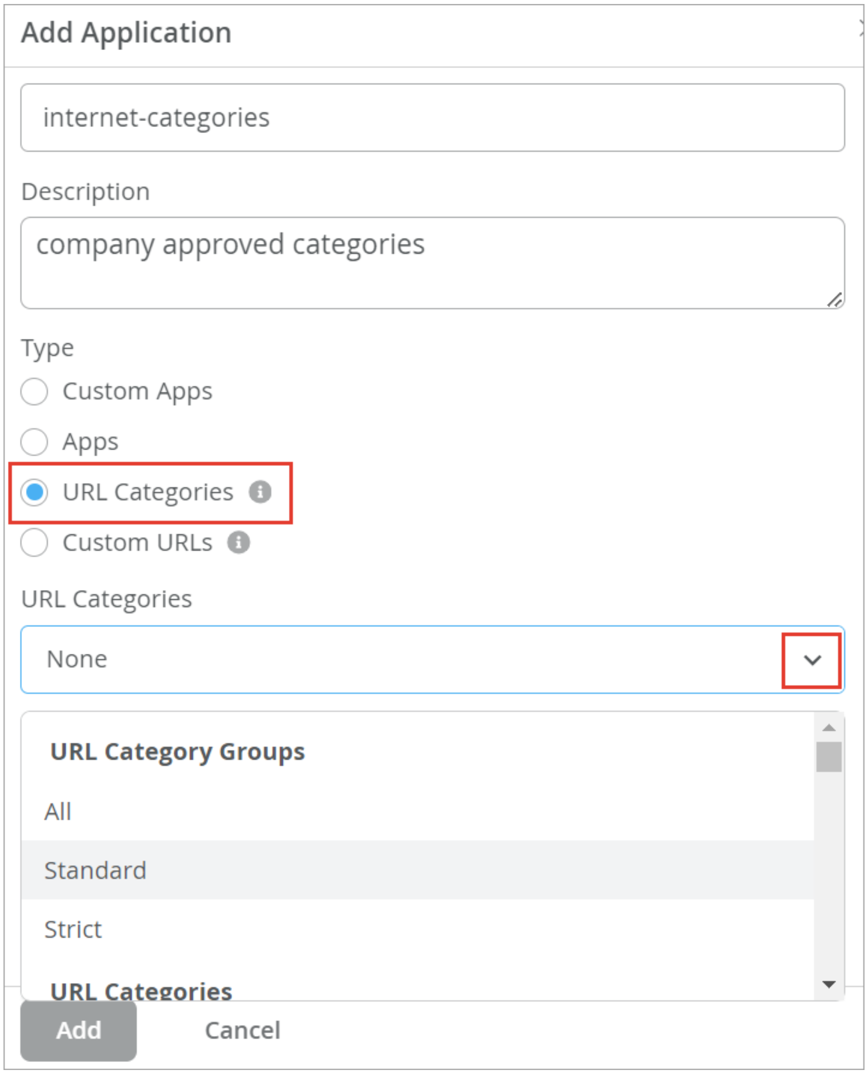
Configure Applications with URL Categories

Juniper Mist cloud provides a list of URL categories based on types (example: shopping, sports) and grouped by severity (all, standard, 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:

1. In the Mist portal, in the **Add Application** pane, select the **Type** as **URL Categories**.
2. Click the Add (+) icon to display the list of available URL categories

Figure 25: URL Categories



Add Application

internet-categories

Description

company approved categories

Type

○ Custom Apps

○ Apps

● URL Categories

○ Custom URLs

URL Categories

None

3. Select one or more URL category groups or URL categories.
4. Click **Add** to save your changes.

Configure Applications with Custom URLs

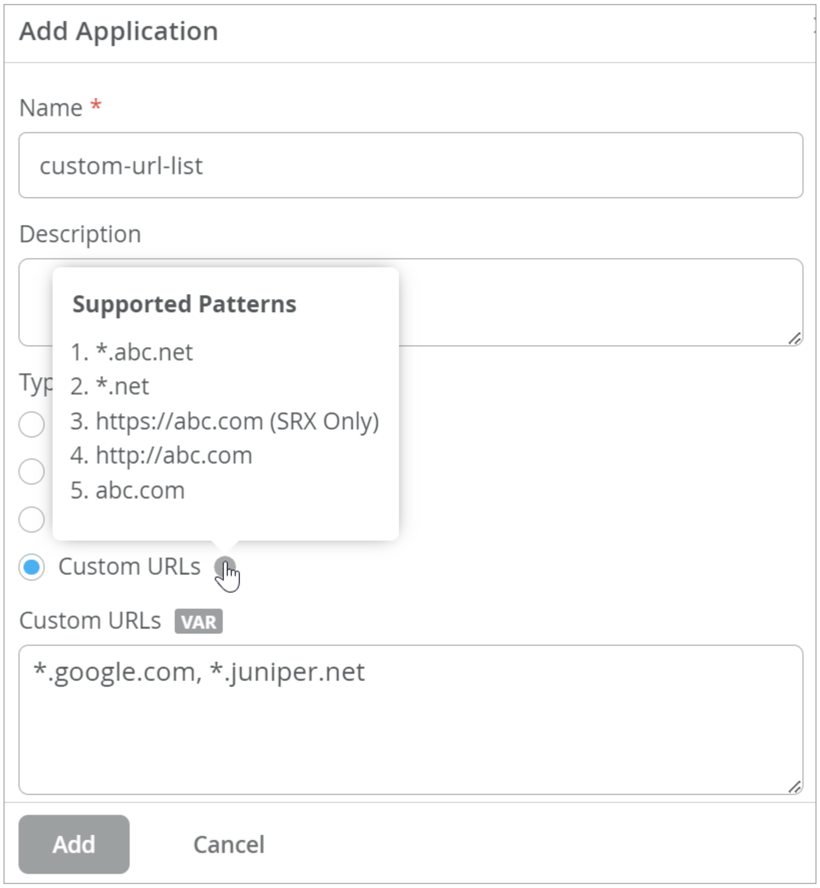
Juniper Mist allows you to create custom URL-based applications. With custom URLs, you can create a wildcard domains list, which can be used to permit or block traffic.

To define custom URLs:

1. In the Mist portal, in the **Add Application** pane, select the **Type** as **Custom URLs**.
2. Enter the custom URLs. Use a comma separator if you need to specify multiple URLs.

   Mist supports only the asterisk(*) wildcard pattern. You can specify up to 15 URL patterns for an application. You can view the supported patterns by hovering the mouse over the tooltip icon. Note that you can use the *https://abc.com* pattern only for SRX Series devices.

   Figure 26: Custom URLs

   Add Application

   Name *

   custom-url-list

   Description

   Supported Patterns

   1. *.abc.net
   2. *.net
   3. https://abc.com (SRX Only)
   4. http://abc.com
   5. abc.com

   Typ

   ● Custom URLs

   Custom URLs VAR

   *.google.com, *.juniper.net

3. Click **Add** to save your changes.

> **NOTE**: You can also edit an existing application to include custom URL patterns.

SEE ALSO

Juniper Mist WAN Assurance Configuration Hierarchy | 13

WAN Assurance Configuration Overview | 31

Configure Networks for Session Smart Routers | 38

Configure Application Policies on Session Smart Routers | 58

Configure Application Policies on Session Smart Routers

IN THIS SECTION

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.

Notes about the application policies on the Juniper® Session Smart™ Routers :

- 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:

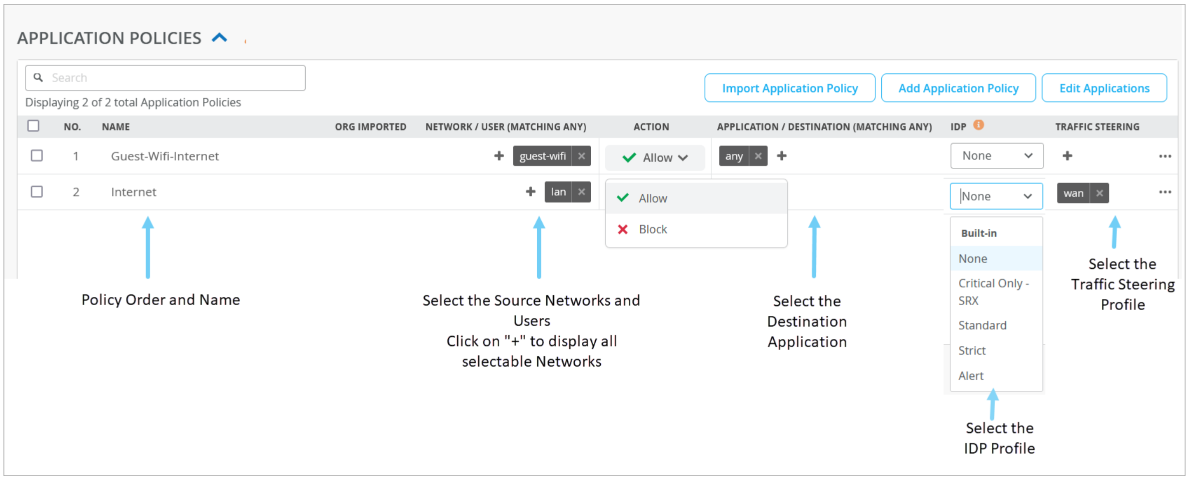
1. In Juniper Mist cloud portal, select **Organization** > **WAN** > **Application Policy** to create a policy at the organization level.

   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 the **Add Application Policy** button.

   > **NOTE**: You can import a global policy into the WAN Edge template or hub profile by clicking the **Import Application Policy** option.
   >
   > Juniper Mist Cloud portal displays the imported policies in gray color to differentiate from local policies defined in the template/profile.
3. Click the new field under the **Name** column and give the policy a name and then click the blue check mark to apply your changes.

   Figure 27 on page 60 shows the options that are available to you when you configure an application policy.

Figure 27: Application Policy Configuration Options



APPLICATION POLICIES

Search

Displaying 2 of 2 total Application Policies

□	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
□	1	Guest-Wifi-Internet		guest-wifi	✓ Allow	any	None	
□	2	Internet		lan			None	wan

Policy Order and Name

Select the Source Networks and Users
Click on "+" to display all selectable Networks

Select the Destination Application

Select the IDP Profile

Select the Traffic Steering Profile

Table 6 on page 60 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. For Session Smart Routers, policy order is not important. As good practice, you place the global policies at the end of the policy list.
Name	Name of the application policy. You can use upto 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 an user to the network, the Mist portal displays the detail as *user.network* format in the dropdown menu.

Table 6: Application Policies Options *(Continued)*

Field	Description
Action	Policy actions. Select one of these policy actions: • Allow • Block
Application / Destination	Destination end point. Applications determine the destinations used in a policy You can select applications from the list of already defined applications.

Table 6: Application Policies Options *(Continued)*

Field	Description
IDP	(Optional) Intrusion Detection and Prevention (IDP) profiles. Select one of the IDP profiles: • **Standard**—Standard profile is the default profile and represents the set of IDP signatures and rules recommended by Juniper Networks. The actions include: Close the client and server TCP connection. Drop current packet and all subsequent packets • **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. • **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. • **None**—No IDP profile applied. The IDP profile applied 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. 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 Table 7 on page 63 .

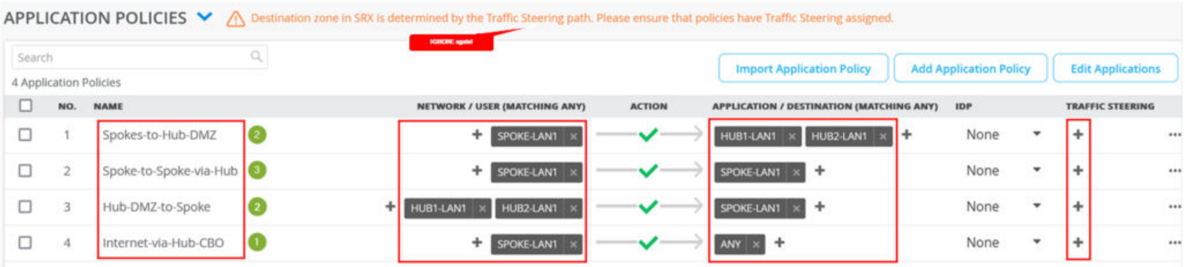
Table 7: Application Policy Examples

No.	Policy Name	Network/User	Application/ Destination	Action
1	Spoke-to-Hub-DMZ	SPOKE-LAN1	HUB1-LAN1 and HUB2-LAN1	Allow
2	Spoke-to-Spoke-via-hub	SPOKE-LAN1	SPOKE-LAN1	Allow
3	Hub-DMZ-to-Spoke	HUB1-LAN1 and HUB2-LAN1	SPOKE-LAN1	Allow
4	Internet-via-Hub-CBO	SPOKE-LAN1	Any	Allow

5. Click **Save**.

   Figure 28 on page 63 shows the list of newly created application policies.

Figure 28: Application Policies Summary



APPLICATION POLICIES

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

Search

4 Application Policies

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

Reordering and Deleting Application Policies

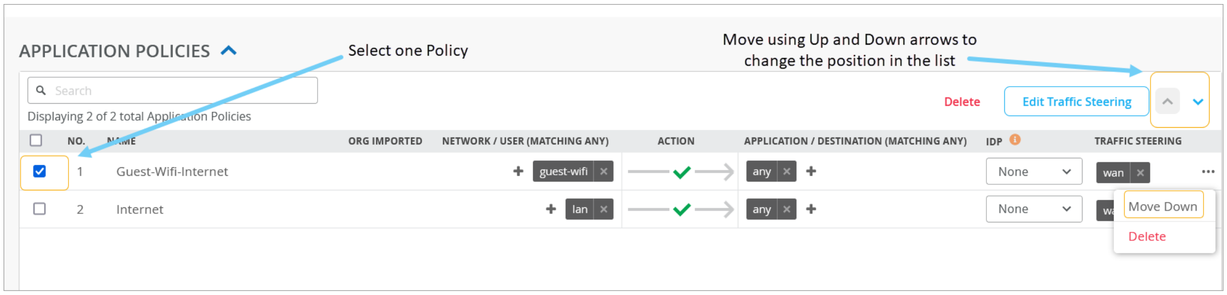
Reordering application policy allows you to move the policies around after they have been created.

Mist evaluates policies and executes policies in the order of their appearance in the policies list, you should be aware of 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 29: Changing Policy Order



Select one Policy

Move using Up and Down arrows to change the position in the list

Displaying 2 of 2 total Application Policies

☐	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
☑	1	Guest-Wifi-Internet		guest-wifi	✓	any	None	wan
☐	2	Internet		lan	✓	any	None	wa

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

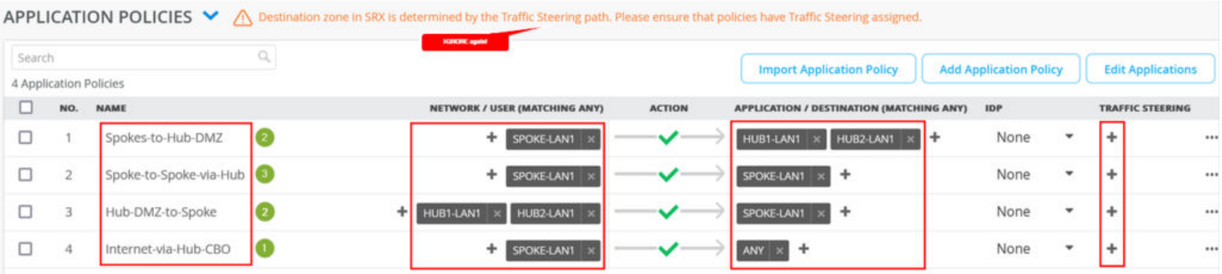
Using Same IP Addresses/Prefixes in Networks and Applications

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.

Consider the policies in Figure 30 on page 65.

Figure 30: Application Policies Details



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

Search

4 Application Policies

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

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.

Monitoring Breakout Paths (Beta)

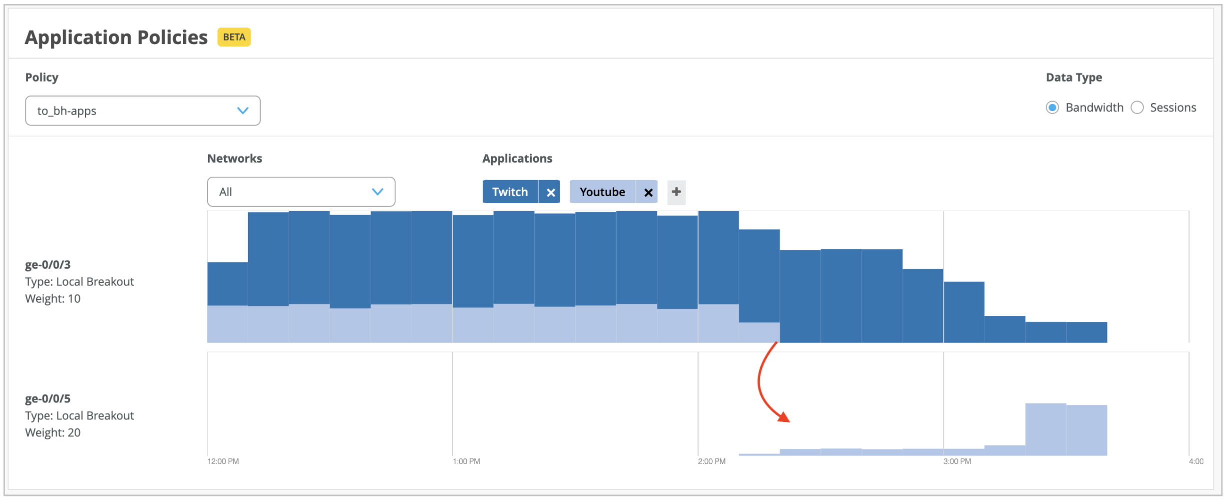
You can monitor breakout paths with the Application Routing Visibility graph on the Application Policy dashboard.

NOTE: This feature is available to Beta participants only.

To improve your network monitoring experience with SSR devices, Juniper Mist switches local breakout traffic from one path to another when the path doesn't meet the associated SLA requirements for the link latency, jitter, and loss parameters.

The SSR devices compare the SLA parameters (latency, jitter, and loss) for all the local breakout paths against the thresholds configured for these parameters for each application. Whenever a set threshold is breached (that is, a local breakout path fails to meet the associated SLA requirements), the traffic shifts to another path based on the traffic steering configuration. Any such shifts in traffic are displayed on the Application Routing Visibility graph on the Application Policy dashboard.

In the following example, you see a traffic shift from the ge-0/0/3 interface to the ge-0/0/5 interface due to an SLA threshold breach.



Application Policies BETA

Policy: to_bh-apps

Data Type: ● Bandwidth ○ Sessions

Networks: All

Applications: Twitch × Youtube × +

ge-0/0/3
Type: Local Breakout
Weight: 10

ge-0/0/5
Type: Local Breakout
Weight: 20

Configure Hub Profile for Session Smart Routers

IN THIS SECTION

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® Session Smart™ Routers, the 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.

   > **NOTE**: You can also create a hub profile by importing a JavaScript Object Notation (JSON file) using the **Import Profile** option.

3. Enter the name of the profile and click **Create**.

   Table 8 on page 67 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	The 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.

Table 8: Hub Profile Options *(Continued)*

Field	Description
Hub Group	Configure a hub group by specifying a hub group identifier (number). Hub groups are used to group hub devices logically. Hub groups help you scale your hub architecture horizontally. By assigning a set of devices to a hub group, spokes can form overlay paths to hub endpoints within the group. Each hub group is limited to 31 hub endpoints.
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. Secure Edge performs traffic inspection for the WAN edge devices managed by Juniper Mist Cloud portal.
WAN	WAN interfaces details. 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 "Add WAN Interfaces to the Hub Profile" on page 69.
LAN	LAN interfaces details. Hub-side of LAN interfaces that connect hub to the LAN segment. You assign the networks, create VLANs, and setup IP addresses and DHCP options (none, or relay, or server). See "Add a LAN Interface to the Hub Profile" on page 71.
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 "Configure Traffic-Steering Policies" on page 72.

Table 8: Hub Profile Options *(Continued)*

Field	Description
Application Policies	Policies to enforce rules for traffic. Define network (source), application (destination), traffic steering policies, and policy action. See "Configure an Application Policy" on page 74.
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 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.

4. Click **Save**.

Add WAN Interfaces to the Hub Profile

IN THIS SECTION

Create WAN interfaces for the hub profile. WAN interfaces become the connection across the SD-WAN. The hub profile automatically creates an overlay endpoints 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:

Hub-to-spoke Traffic Steering

The hub profiles let you control t

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 in Table 9 on page 70.

Table 9: WAN Interface Configuration

Fields	WAN Interface 1	WAN Interface 2
Name (a label and not a technology)	INET	MPLS
Overlay Hub Endpoint (generated automatically) Also see "Configure Path Selection from Hub-to-Spoke with Traffic Steering" on page 86	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** • Provide Public IP={{WAN0_PUBIP} }	• Check **Override for Public IP** • Provide Public IP={{WAN1_PUBIP} }
Public IP	{{WAN0_PUBIP}}	{{WAN1_PUBIP}}

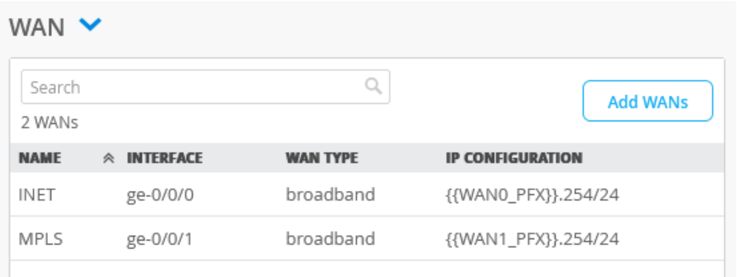
NOTE: Use Network Address Translation (NAT) along with advertising the public IP address unless the WAN address is a publicly routable address.

3. Click **Save**.

Figure 31 on page 71 shows the list of WAN interfaces you created.

shows the list of WAN interfaces you created.

Figure 31: Configured WAN Interfaces



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:

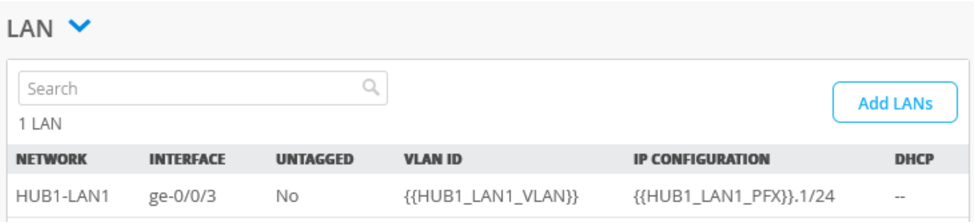
1. Under the LAN section, click the **Add LAN** button to open the Add LAN Configuration panel.
2. Complete the configuration according to the details provided in Table 10 on page 71

   Table 10: LAN Interface Configuration

Fields	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**.
4. Figure 32 on page 72 shows the LAN interface you created.

Figure 32: Configured LAN Interfaces



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
- 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 Table 11 on page 73 .

Table 11: Traffic-Steering Policy Configuration

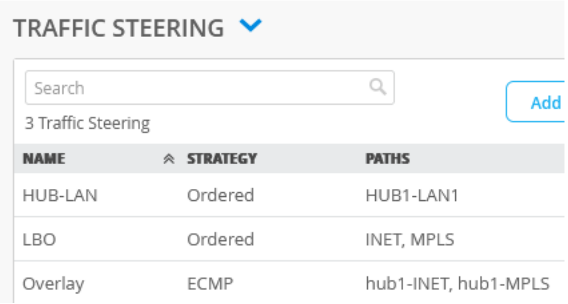
Fields	Traffic Steering Policy 1	Traffic Steering Policy 2	Traffic Steering Policy 3
Name	HUB-LAN	Overlay	Central Breakout
Strategy	Ordered	ECMP	Ordered
PATHS For path types, LAN and WAN networks created already are made available for selection as endpoints.	• **Type**—LAN • **Network**—HUB1-LAN1	• **Type**—WAN • **Network** —hub1-INET and hub1-MPLS	• **Type**—WAN • **Network**—WAN: INET and WAN: MPLS

NOTE:

- Order of application policies do not have any effect on Session Smart Router configuration. As good practice, we recommend you to place global rules towards the end of the policy rules list.
- Associating traffic steering policy on each application rule is not a requirement for Session Smart Router. When you use Session Smart Routers, the system announces all the routes on each LAN interface using the iBGP-based route distribution.
- For the Session Smart Router deployments, for the traffic to traverse between a hub and spoke, you must use the same name for networks on both sides. The network name for Session Smart Router is identical to a security tenant used for traffic isolation. So, the name must match on both the sides.

Figure 33 on page 74 shows the list of the traffic-steering policies that you created.

Figure 33: Traffic Steering Policies



TRAFFIC STEERING

Search

Add

3 Traffic Steering

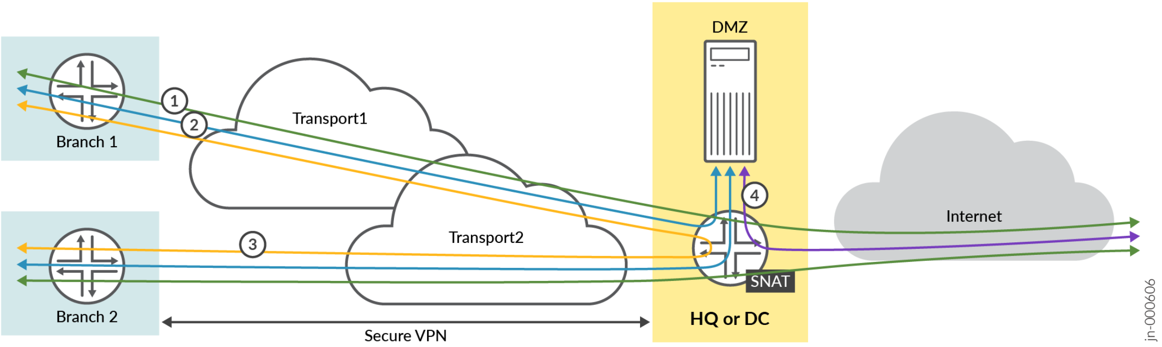
NAME	STRATEGY	PATHS
HUB-LAN	Ordered	HUB1-LAN1
LBO	Ordered	INET, MPLS
Overlay	ECMP	hub1-INET, hub1-MPLS

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 arrow to change the order of policies.

Figure 34 on page 74 shows different traffic-direction requirements in this task (third spoke device and second hub device are not shown in the image).

Figure 34: Traffic Direction Topology



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

-

- Rule 1—Allows traffic from spoke sites to reach the hub (and to a server in the DMZ attached to the hub device).

- Rule 2—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.

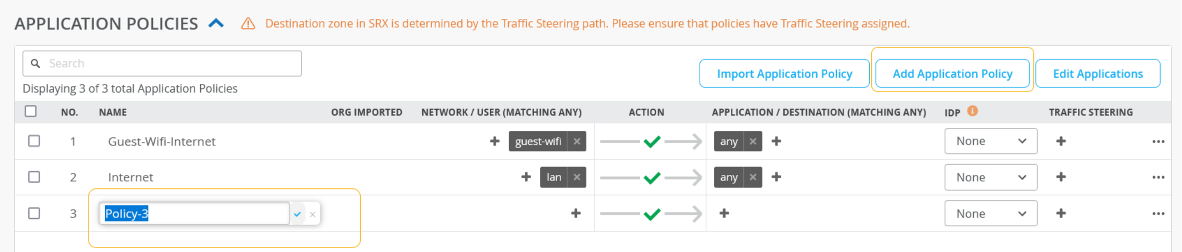
- **NOTE**: Avoid creating rules with same destination name and IP address 0.0.0.0/0. If required, create destinations with different names using IP address 0.0.0.0/0.

- 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.

To configure an application policy:

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

Figure 35: Adding a New Application Policy



APPLICATION POLICIES

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

Displaying 3 of 3 total Application Policies

☐	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
☐	1	Guest-Wifi-Internet		guest-wifi	✓	any	None	
☐	2	Internet		lan	✓	any	None	
☐	3	Policy-3			✓		None	

3. Create application rules according to the details provided in Table 12 on page 75.

Table 12: Application Policy Rule Configuration

S.No.	Rule Name	Network	Action	Destination	Steering
1	Spoke-to-Hub-DMZ	SPOKE-LAN1	Pass	HUB1-LAN1	NA

Table 12: Application Policy Rule Configuration *(Continued)*

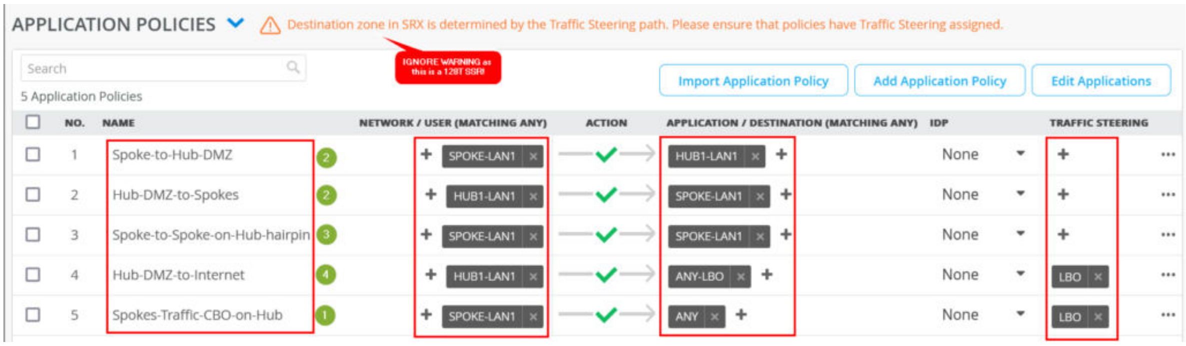
S.No.	Rule Name	Network	Action	Destination	Steering
2	Hub-DMZ-to-Spokes	HUB1-LAN1	Pass	SPOKE-LAN1	NA
3	Spoke-to-Spoke-on-Hub-Hairpin	SPOKE-LAN1	Pass	SPOKE-LAN1	NA
4	Hub-DMZ-to-Internet	HUB1-LAN1	Pass	ANY-LBO	LBO
5	Spokes-Traffic-CBO-on-Hub	ALL.SPOKE-LAN1	Pass	ANY	LBO

NOTE:

If you are configuring application policies for Session Smart Router, associating a traffic steering for each application policy is not a requirement. Table 12 on page 75 shows application policies configured without any traffic steering profiles. The reason is - when you use Session Smart Router, the system acts as a routing device and announces all routes on each LAN interface. The system automatically applies traffic steering using iBGP-based route distribution when you build the hub and spoke VPN.

Figure 36 on page 76 shows a list of the application policies that you created.

Figure 36: Application Policies Summary



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

5 Application Policies

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

In the above illustration, the green counter marks indicates the policies you have created for the traffic requirements in Figure 34 on page 74.

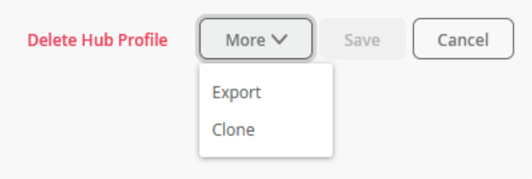
Create a Second Hub by Cloning the Existing Hub Profile

Hubs devices are unique throughout your network. You have to create individual profile for each hub device. Juniper Mist provides you an option 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:

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

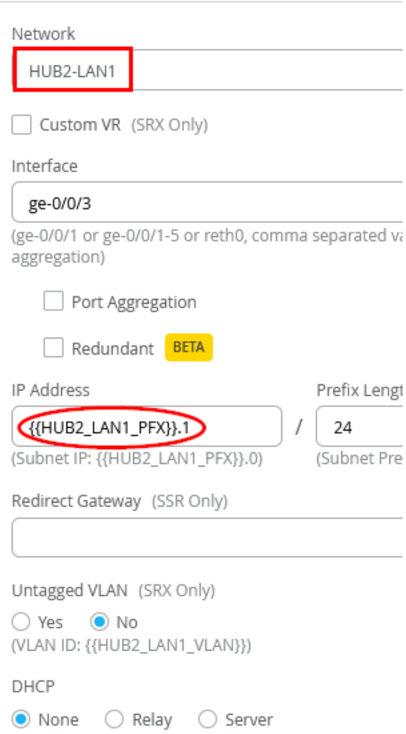
   Figure 37: Creating a New Hub Profile By using Clone Option

4. Name the new profile as hub2 and click **Clone**

   If you see any errors while naming the profile, refresh your browser.
5. 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.

Figure 38: Edit a Cloned Profile



Network

HUB2-LAN1

□ Custom VR (SRX Only)

Interface

ge-0/0/3

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

□ Port Aggregation

□ Redundant BETA

IP Address / Prefix Lengt

{{HUB2_LAN1_PFX}}.1 / 24

(Subnet IP: {{HUB2_LAN1_PFX}}.0) (Subnet Pre

Redirect Gateway (SSR Only)

Untagged VLAN (SRX Only)

○ Yes ● No

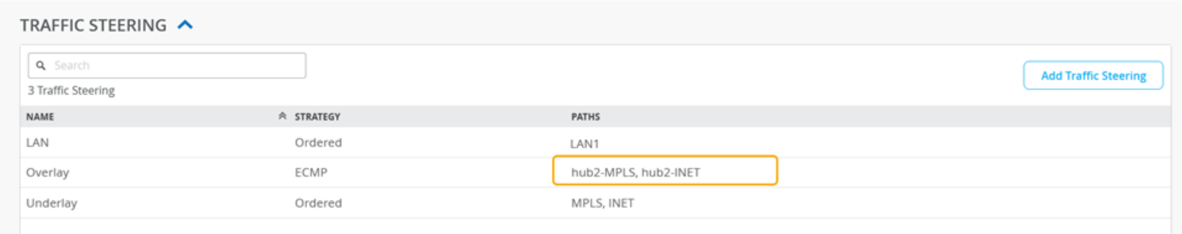
(VLAN ID: {{HUB2_LAN1_VLAN}})

DHCP

● None ○ Relay ○ Server

6. Change the LAN interface to include HUB2. Example: HUB2-LAN1 and {{HUB2_LAN1_PFX}}.1
7. 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.

Figure 39: Updated Traffic Steering Policy



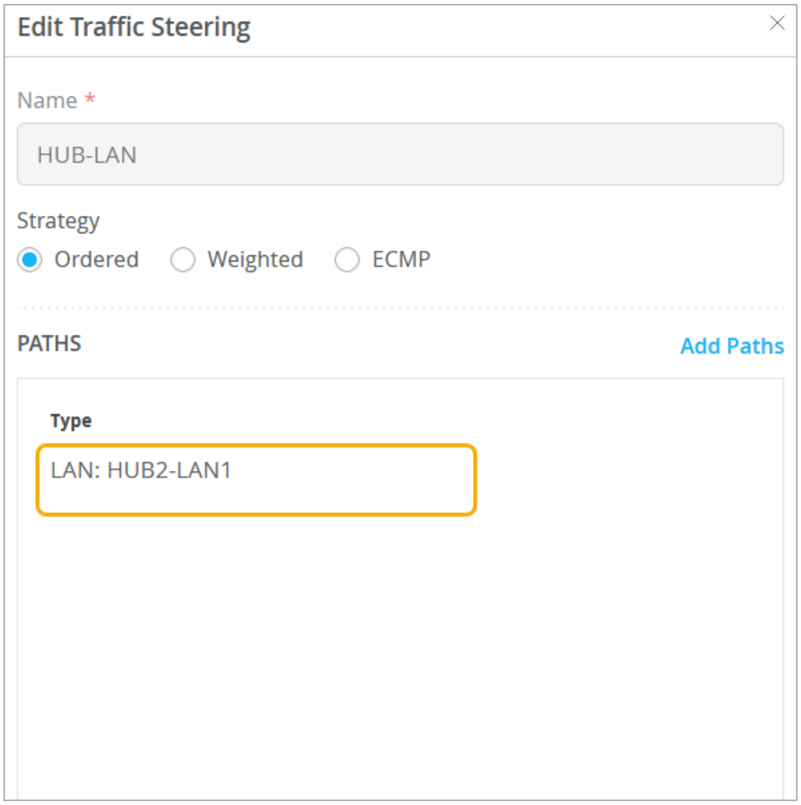
TRAFFIC STEERING

3 Traffic Steering

NAME	STRATEGY	PATHS
LAN	Ordered	LAN1
Overlay	ECMP	hub2-MPLS, hub2-INET
Underlay	Ordered	MPLS, INET

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

Figure 40: Update Paths in a Traffic-Steering Policy



Edit Traffic Steering

Name *

HUB-LAN

Strategy

● Ordered ○ Weighted ○ ECMP

PATHS

Type

LAN: HUB2-LAN1

9. Update the application rules according to the details provided in Table 13 on page 79. For example, wherever applicable, change HUB1-LAN to HUB2-LAN.

Table 13: Application Rules Configuration

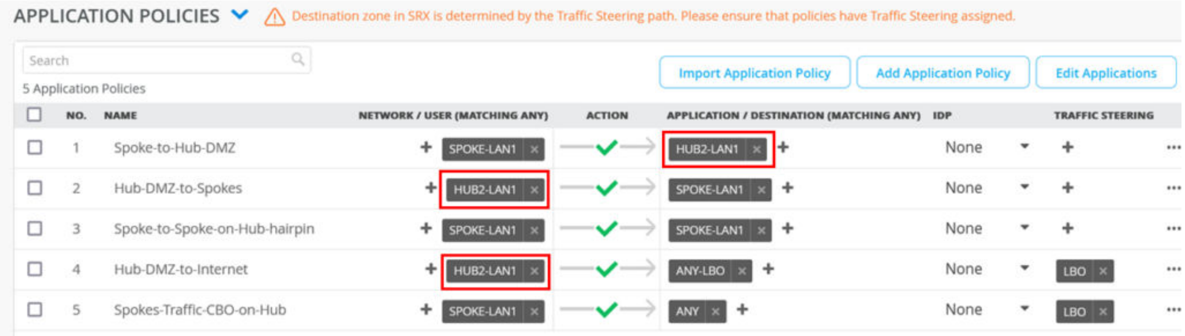
S.No.	Rule Name	Network	Action	Destination	Steering
1	Spoke-to-Hub-DMZ	SPOKE-LAN1	Pass	HUB2-LAN1	N/A
1	Hub-DMZ-to-Spokes	HUB2-LAN1	Pass	SPOKE-LAN1	N/A
3	Spoke-to-Spoke-on-Hub-Hairpin	SPOKE-LAN1	Pass	SPOKE-LAN1	N/A
4	Hub-DMZ-to-Internet	HUB2-LAN1	Pass	ANY-LBO	LBO

Table 13: Application Rules Configuration *(Continued)*

S.No.	Rule Name	Network	Action	Destination	Steering
5	Spokes-Traffic-CBO-on-Hub	SPOKE-LAN1	Pass	ANY	LBO

Figure 41 on page 80 shows the details of the updated application policies after you save your changes.

Figure 41: Updated Application Policy Summary



APPLICATION POLICIES

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

5 Application Policies

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

Hub-to-Hub Overlay

IN THIS SECTION

The Hub-to-hub overlay feature allows a you to form a peer path between two hub devices. You can utilize the hub-to-hub overlay path as a preferred route for data center traffic originating from sites. Additionally, these hub-to-hub overlays can serve as failover paths in scenarios involving hub-to-spoke connections.

Configure Hub-to-Hub Overlay

To create Hub-to-Hub overlay, the WAN interfaces of one hub map to the WAN interfaces of another hub, thus forming an overlay and designating a traffic pathway.

> **NOTE**: Hub-to-Hub overlay can utilize different WAN interfaces on both hub devices. It is not mandatory for the overlay to form between identical WAN interfaces on the two hubs.

Consider you have two hubs, Hub device A and Hub device B, and you wish to establish an overlay between them.

Hub device A is equipped with two WAN interfaces: WAN-1-A and WAN-2-A. You must pair these WAN interfaces with the WAN interfaces of Hub device B, which are WAN-1-B and WAN-2-B, marking them as hub endpoints.

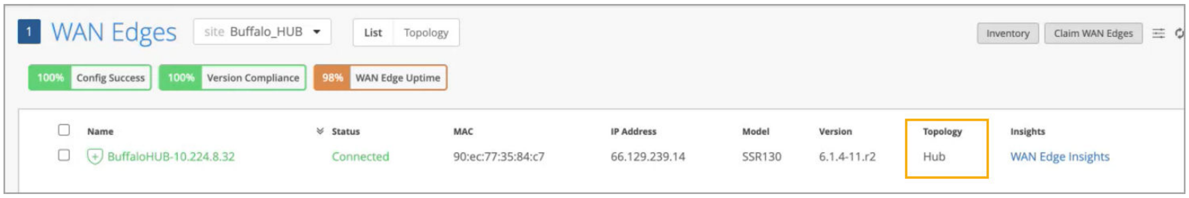
Similarly, for Hub device B:

It features two WAN Interfaces: WAN-1-B and WAN-2-B. These should be linked to the WAN Interfaces of Hub Device A (WAN-1-A and WAN-2-A) to complete the setup as hub endpoints.

Use the following steps to create hub endpoints:

1. On Juniper Mist portal, select **WAN Edges** and click the hub device. Ensure that the hub device you select must be part of hub topology.

Figure 42: Hub Device in Hub Topology



□	Name	Status	MAC	IP Address	Model	Version	Topology	Insights
□	BuffaloHUB-10.224.8.32	Connected	90:ec:77:35:84:c7	66.129.239.14	SSR130	6.1.4-11.r2	Hub	WAN Edge Insights

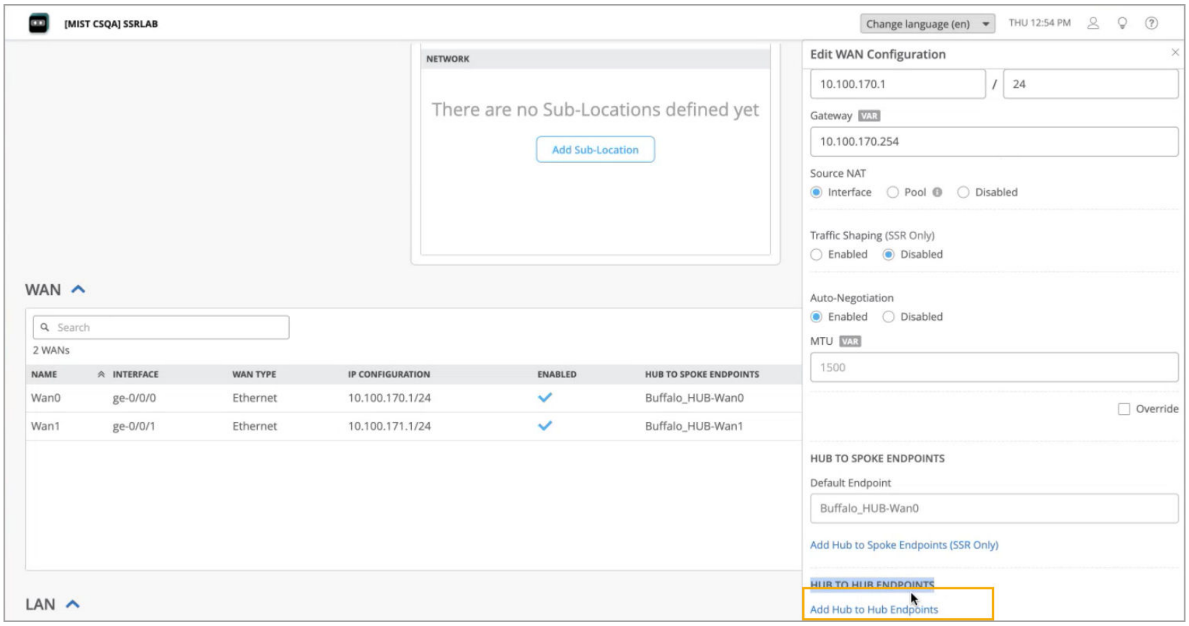
2. On the **WAN Edge >** ***Device-Name*** page, go to Properties section and scroll down to Hub Profile.

3. Click the hub profile link to open the **Hub Profile** page.

4. Scroll-down to WAN section and click a WAN interface which you want to use for overlay.

5. In the **Edit WAN Configuration** window, scroll down to **Hub-to-Hub Endpoints** and click **Add Hub-to-Hub Endpoints** option.

Figure 43: Adding Hub-to-Hub Endpoints



NAME	INTERFACE	WAN TYPE	IP CONFIGURATION	ENABLED	HUB TO SPOKE ENDPOINTS
Wan0	ge-0/0/0	Ethernet	10.100.170.1/24	✓	Buffalo_HUB-Wan0
Wan1	ge-0/0/1	Ethernet	10.100.171.1/24	✓	Buffalo_HUB-Wan1

Edit WAN Configuration

10.100.170.1 / 24

Gateway VAR

10.100.170.254

Source NAT

● Interface ○ Pool ○ Disabled

Traffic Shaping (SSR Only)

○ Enabled ● Disabled

Auto-Negotiation

● Enabled ○ Disabled

MTU VAR

1500

□ Override

HUB TO SPOKE ENDPOINTS

Default Endpoint

Buffalo_HUB-Wan0

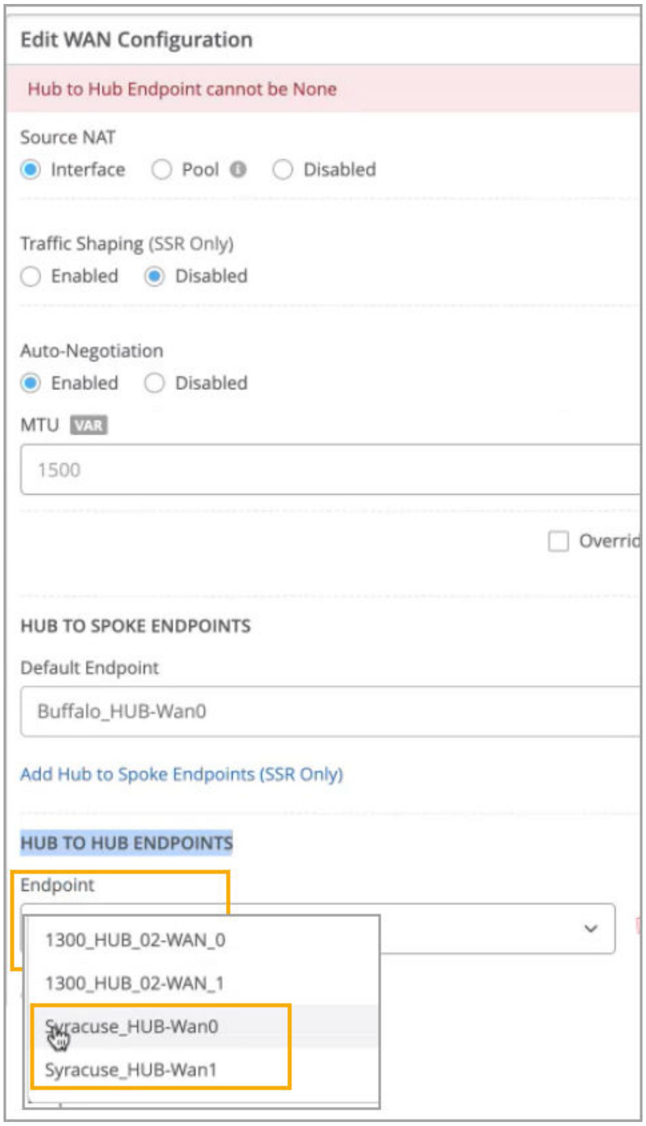
Add Hub to Spoke Endpoints (SSR Only)

HUB TO HUB ENDPOINTS

Add Hub to Hub Endpoints

6. a. Select a hub endpoint point (WAN interface) from the drop-down menu. Choose the WAN interface of the other hub device to establish an overlay connection.

Figure 44: Select WAN Interface for Overlay



Edit WAN Configuration

Hub to Hub Endpoint cannot be None

Source NAT

● Interface ○ Pool ○ Disabled

Traffic Shaping (SSR Only)

○ Enabled ● Disabled

Auto-Negotiation

● Enabled ○ Disabled

MTU VAR

1500

□ Overrid

HUB TO SPOKE ENDPOINTS

Default Endpoint

Buffalo_HUB-Wan0

Add Hub to Spoke Endpoints (SSR Only)

HUB TO HUB ENDPOINTS

Endpoint

1300_HUB_02-WAN_0

1300_HUB_02-WAN_1

Syracuse_HUB-Wan0

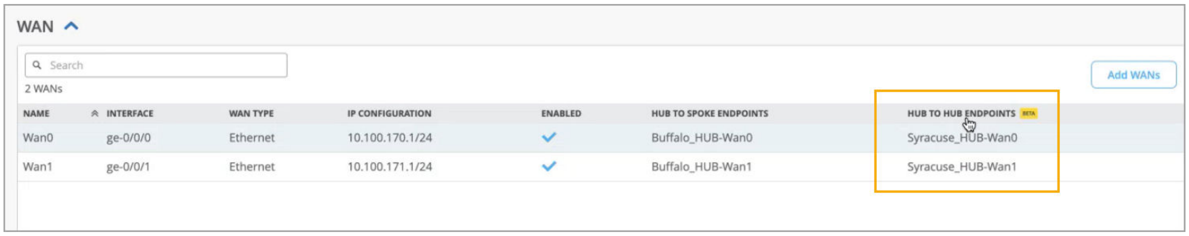
Syracuse_HUB-Wan1

b. Click **Save**. The selected hub endpoint appears under Hub to Hub Endpoints columns in WAN pane.

7. Select another WAN interface and repeat the same procedure to add another endpoint.

8. Now, both endpoints appear under **Hub to Hub Endpoints** columns in WAN pane.

Figure 45: Configured Hub to Hub Endpoints of First Hub Device



NAME	INTERFACE	WAN TYPE	IP CONFIGURATION	ENABLED	HUB TO SPOKE ENDPOINTS	HUB TO HUB ENDPOINTS BETA
Wan0	ge-0/0/0	Ethernet	10.100.170.1/24	✓	Buffalo_HUB-Wan0	Syracuse_HUB-Wan0
Wan1	ge-0/0/1	Ethernet	10.100.171.1/24	✓	Buffalo_HUB-Wan1	Syracuse_HUB-Wan1

9. Click **Save**.

Now, lets configure WAN interfaces of other hub device to complete the setup as hub endpoints.

1. On Juniper Mist portal, select **WAN Edges** and click the hub device. This is the hub device from which you earlier chose the WAN interface for establishing the overlay.

2. On the **WAN Edge >** ***Device-Name*** page, go to Properties section and scroll down to Hub Profile.

3. Click the hub profile link to open the **Hub Profile** page.

4. Scroll-down to WAN section and click a WAN interface which you want to use for overlay.

5. In the **Edit WAN Configuration** window, scroll down to **Hub-to-Hub Endpoints** and click **Add Hub-to-Hub Endpoints** option.

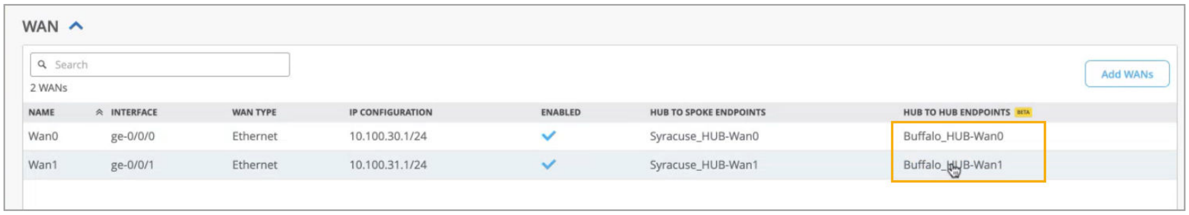
6. a. Select a hub endpoint point from the drop-down menu. Select the WAN interface of the same hub device that was configured in the prior procedure

   b. Click **Save**. The selected hub endpoint appears under Hub to Hub Endpoints columns in WAN pane.

7. Select another WAN interface and repeat the same procedure to add another endpoint.

8. Now, both endpoints appear under Hub yo Hub Endpoints columns in WAN pane.

Figure 46: Configured Hub to Hub Endpoints of Second Hub Device



NAME	INTERFACE	WAN TYPE	IP CONFIGURATION	ENABLED	HUB TO SPOKE ENDPOINTS	HUB TO HUB ENDPOINTS BETA
Wan0	ge-0/0/0	Ethernet	10.100.30.1/24	✓	Syracuse_HUB-Wan0	Buffalo_HUB-Wan0
Wan1	ge-0/0/1	Ethernet	10.100.31.1/24	✓	Syracuse_HUB-Wan1	Buffalo_HUB-Wan1

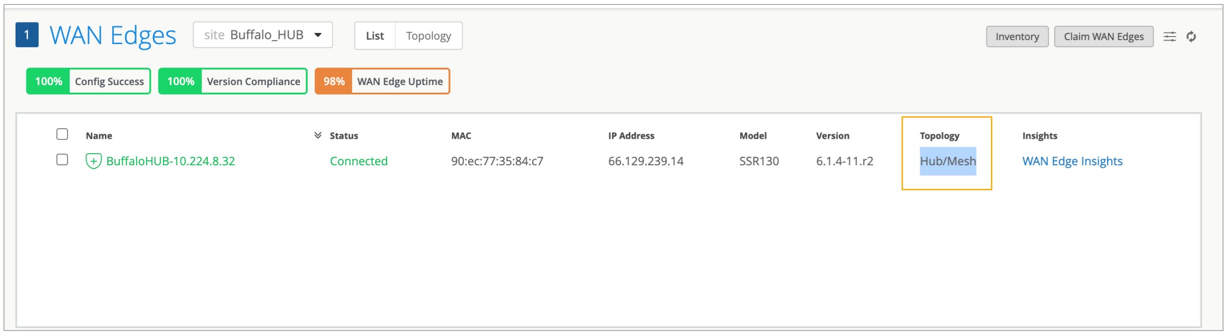
9. Click **Save**.

Verification

On Juniper Mist portal, you can verify the established hub-to-hub overlays by checking the topology of the WAN Edge device:

On the WAN Edge page, the **Topology** column displays **Hub/Mesh**.

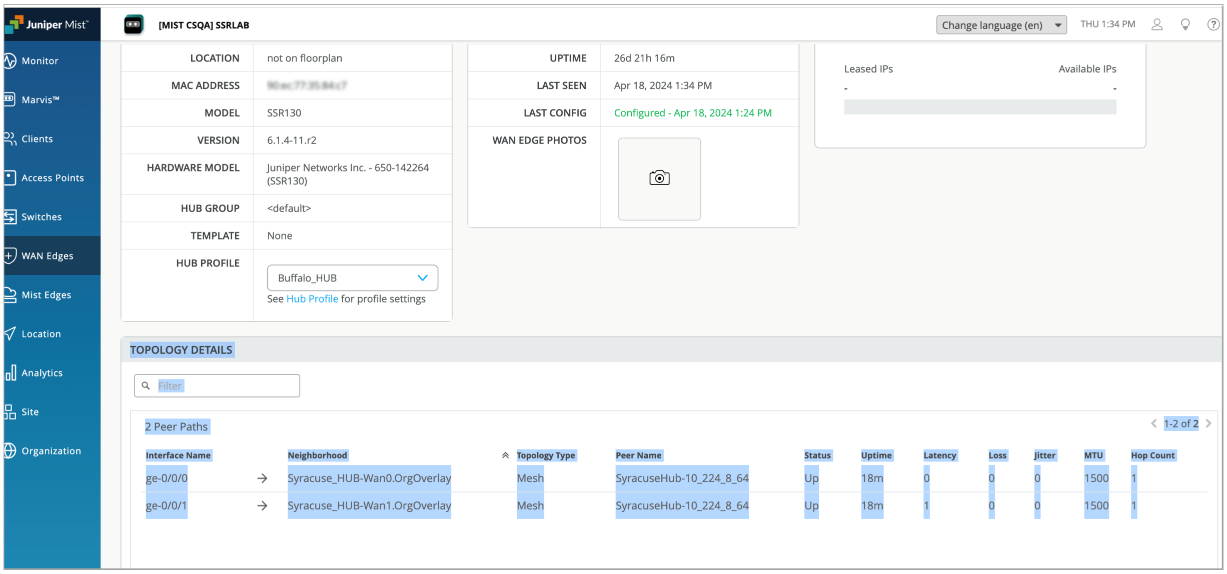
Figure 47: Topology Displaying as Hub/Mesh



Name	Status	MAC	IP Address	Model	Version	Topology	Insights
BuffaloHUB-10.224.8.32	Connected	90:ec:77:35:84:c7	66.129.239.14	SSR130	6.1.4-11.r2	Hub/Mesh	WAN Edge Insights

Go to WAN Edge page of the device and check **Topology Details** section. The portal displays peer details and also connection status.

Figure 48: Hub-to-Hub Overlay Topology Details



LOCATION	not on floorplan
MAC ADDRESS	[redacted]
MODEL	SSR130
VERSION	6.1.4-11.r2
HARDWARE MODEL	Juniper Networks Inc. - 650-142264 (SSR130)
HUB GROUP	<default>
TEMPLATE	None
HUB PROFILE	Buffalo_HUB See Hub Profile for profile settings

UPTIME	26d 21h 16m
LAST SEEN	Apr 18, 2024 1:34 PM
LAST CONFIG	Configured - Apr 18, 2024 1:24 PM
WAN EDGE PHOTOS	

TOPOLOGY DETAILS

Filter

2 Peer Paths

1-2 of 2

Interface Name		Neighborhood	Topology Type	Peer Name	Status	Uptime	Latency	Loss	Jitter	MTU	Hop Count
ge-0/0/0	→	Syracuse_HUB-Wan0.OrgOverlay	Mesh	SyracuseHub-10_224_8_64	Up	18m	0	0	0	1500	1
ge-0/0/1	→	Syracuse_HUB-Wan1.OrgOverlay	Mesh	SyracuseHub-10_224_8_64	Up	18m	1	0	0	1500	1

SEE ALSO

WAN Assurance Configuration Overview | 31

Configure Networks for Session Smart Routers | 38

Configure Applications for Session Smart Routers | 48

Configure Application Policies on Session Smart Routers | 58

Configure WAN Edge Templates for Session Smart Routers | 92

Onboard Session Smart Routers for WAN Configuration | 132

Configure Path Selection from Hub-to-Spoke with Traffic Steering

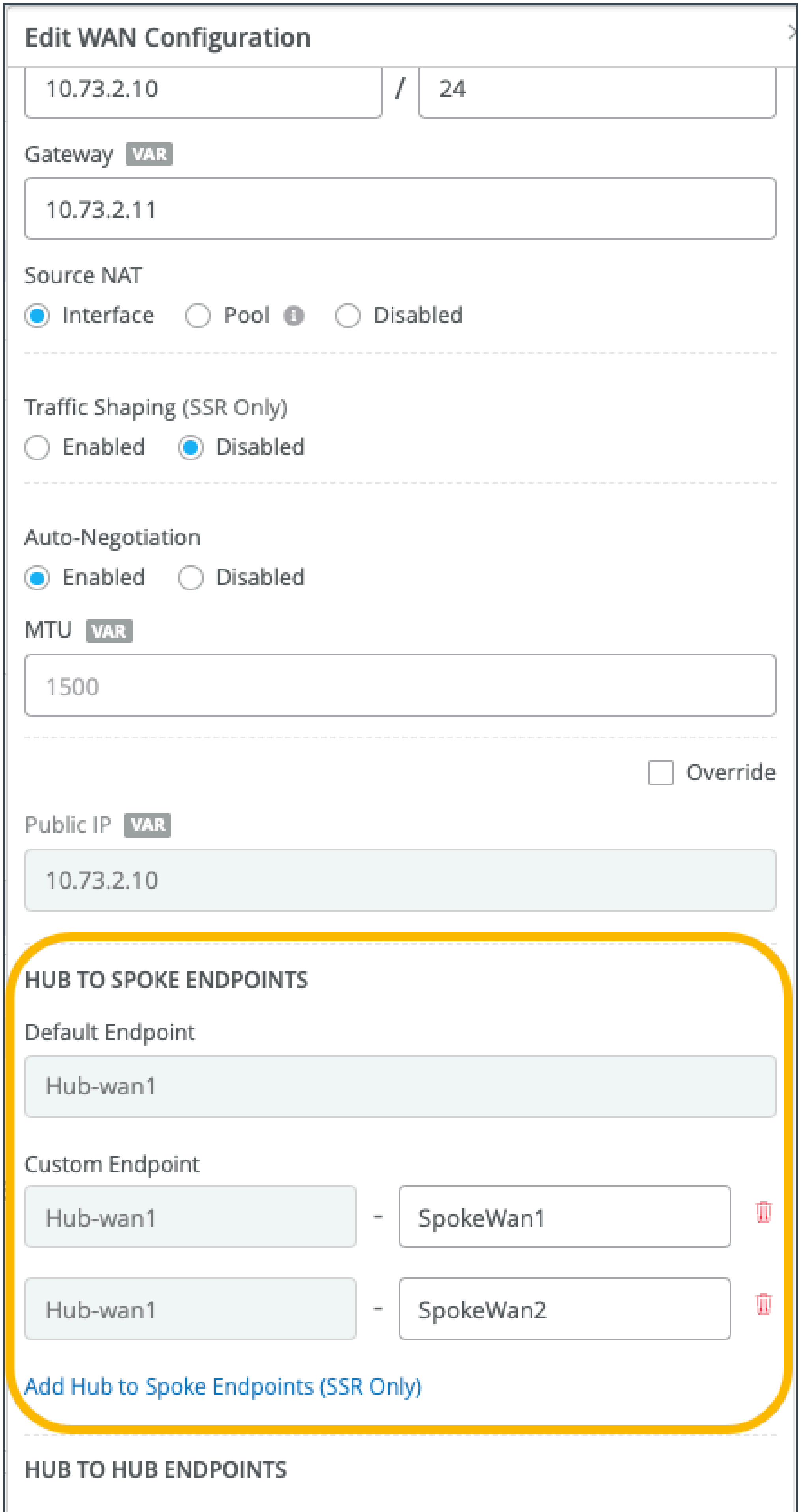
Juniper Mist™ allows you to influence path selection for traffic going from hub-to-spoke. This comes in handy when you have multiple spokes that the hub is trying to reach and you want to have granular control over which spoke interface traffic will arrive on. This configuration gives you full path control in both directions.

To configure Hub-to-Spoke Traffic Steering:

1. From the Mist portal, navigate to **Organization** > **Hub Profiles** and select the appropriate Hub Profile.
2. Select the WAN interface that you want to define the logical spoke endpoints for.
3. In the **Edit WAN Configuration** panel, under **HUB TO SPOKE ENDPOINTS**,

    a. Notice that the **Default Endpoint** has automatically been defined for you. This represents the endpoints you are connecting to on the hub.

    b. Define your **Custom Endpoints** in the field to the right to specify the spokes that you want traffic to arrive on. Configure as many as necessary by clicking **Add Hub to Spoke Endpoints (SSR Only)**.



Edit WAN Configuration

10.73.2.10 / 24

Gateway VAR

10.73.2.11

Source NAT

● Interface ○ Pool ○ Disabled

Traffic Shaping (SSR Only)

○ Enabled ● Disabled

Auto-Negotiation

● Enabled ○ Disabled

MTU VAR

1500

□ Override

Public IP VAR

10.73.2.10

HUB TO SPOKE ENDPOINTS

Default Endpoint

Hub-wan1

Custom Endpoint

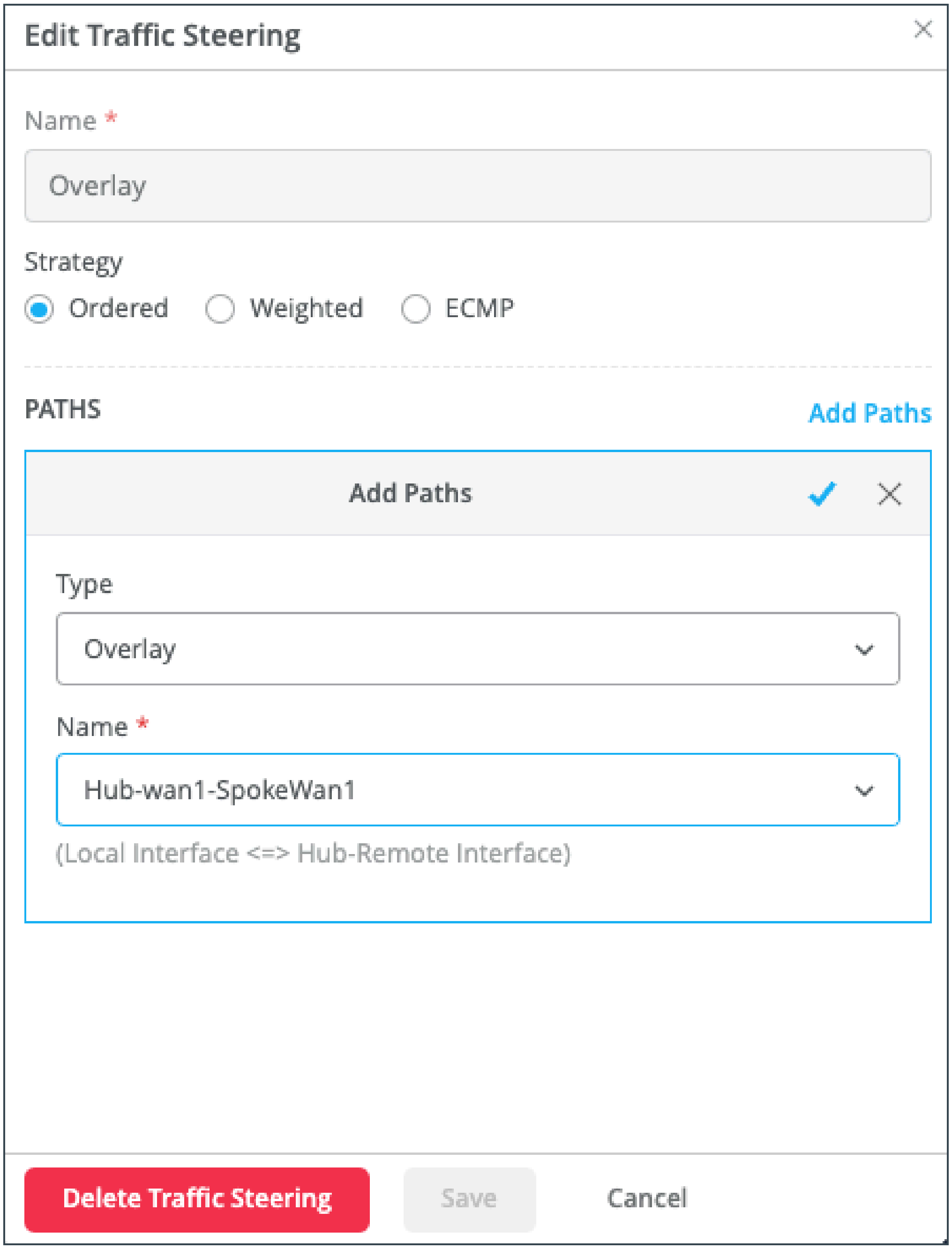
Hub-wan1 - SpokeWan1

Hub-wan1 - SpokeWan2

Add Hub to Spoke Endpoints (SSR Only)

HUB TO HUB ENDPOINTS

4. Select **Save** at the bottom of the **Edit WAN Configuration** panel.
5. Scroll down to **TRAFFIC STEERING** and select the **Overlay** traffic steering policy.
6. In the **Edit Traffic Steering** panel, select **Add Paths**. Keep the defaulted **Type** as **Overlay**, then under **Name**, select the name of the first hub-to-spoke endpoint you created in step 3 (Example: Hub-wan1-SpokeWan1).



Edit Traffic Steering

Name *

Overlay

Strategy

● Ordered ○ Weighted ○ ECMP

PATHS

Add Paths

Add Paths ✓ ×

Type

Overlay

Name *

Hub-wan1-SpokeWan1

(Local Interface <=> Hub-Remote Interface)

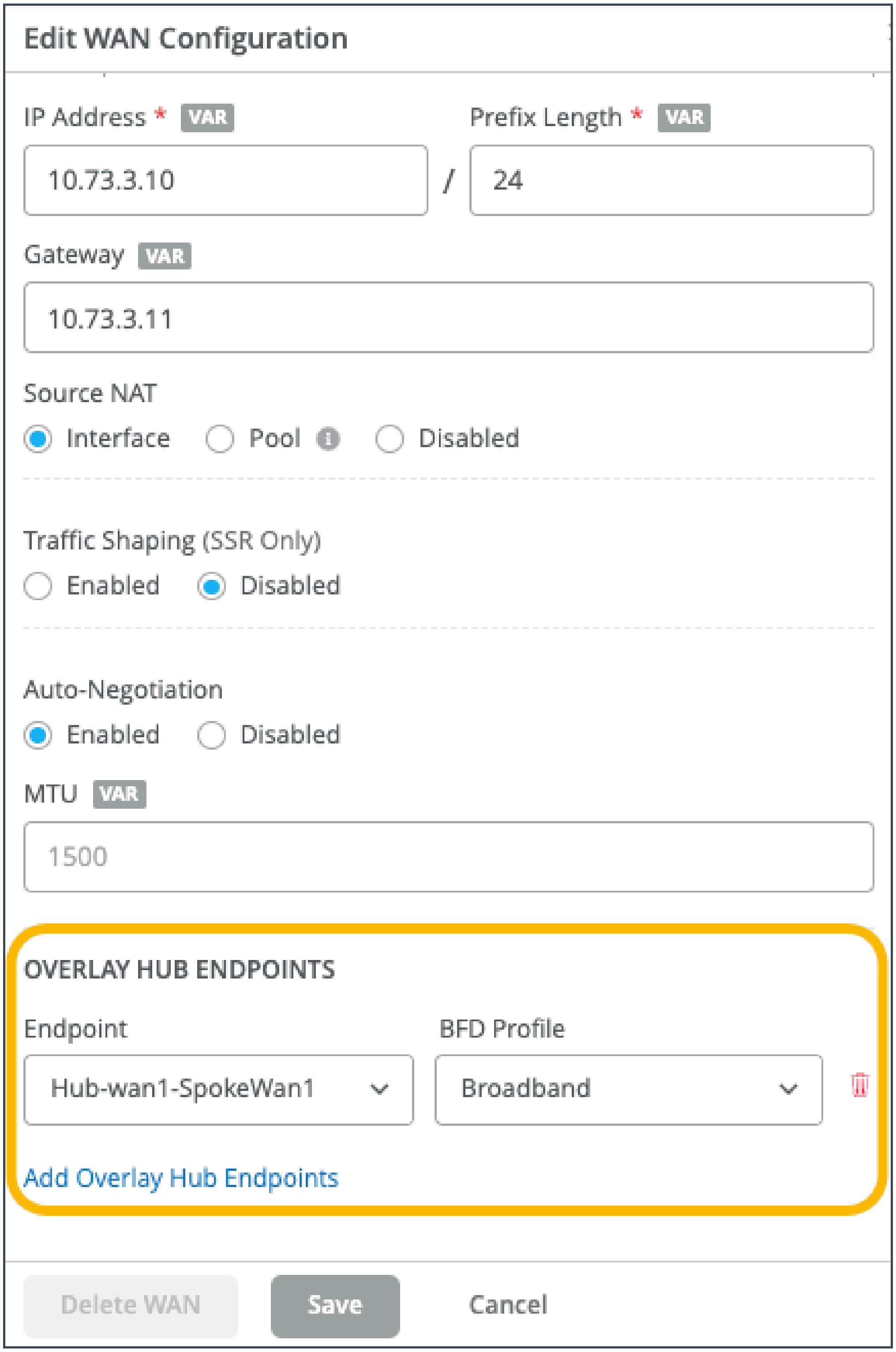
a. Select the blue checkmark to save the path.

b. Select **Add Paths** again and keep the defaulted **Type** as **Overlay**. Then, in the **Name** field, select the name of the second hub-to-spoke endpoint you created in step 3 (Example: Hub-wan1-SpokeWan2). Continue adding paths as needed.

c. Click **Save** at the bottom of the panel, then click **Save** in the top right corner of the Hub Profile.

You must now configure this on the spoke in order to accomplish hub-to-spoke traffic steering from end to end.

7. Navigate to **Organization** > **WAN Edge Templates** and select your spoke template.
8. On your spoke, select the appropriate WAN configuration (Example: WAN1), then in the **Edit WAN Configuration** panel, under **OVERLAY HUB ENDPOINTS**, select the **Endpoint** that corresponds with the WAN configuration you have selected (Example: Hub-wan1-SpokeWan1) to indicate that you are using this overlay endpoint to make the connection between hub and spoke. Click **Save**.



Edit WAN Configuration

IP Address * VAR: 10.73.3.10 / Prefix Length * VAR: 24

Gateway VAR: 10.73.3.11

Source NAT

● Interface ○ Pool ○ Disabled

Traffic Shaping (SSR Only)

○ Enabled ● Disabled

Auto-Negotiation

● Enabled ○ Disabled

MTU VAR: 1500

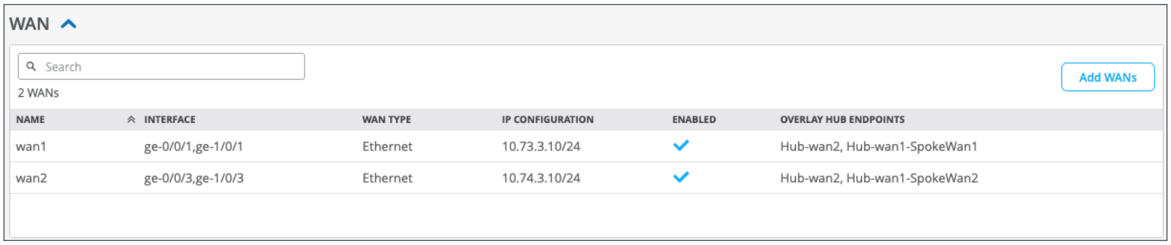
OVERLAY HUB ENDPOINTS

Endpoint: Hub-wan1-SpokeWan1

BFD Profile: Broadband

9. Select the second WAN configuration (Example: WAN2) and then set the corresponding endpoint (Example: Hub-wan1-SpokeWan2). Click **Save**.

   In the WAN tile, in the OVERLAY HUB ENDPOINTS column, you can see the endpoints you configured which indicate how you want your spokes to connect to the hub.



2 WANs

NAME	INTERFACE	WAN TYPE	IP CONFIGURATION	ENABLED	OVERLAY HUB ENDPOINTS
wan1	ge-0/0/1,ge-1/0/1	Ethernet	10.73.3.10/24	✓	Hub-wan2, Hub-wan1-SpokeWan1
wan2	ge-0/0/3,ge-1/0/3	Ethernet	10.74.3.10/24	✓	Hub-wan2, Hub-wan1-SpokeWan2

10. Scroll down to the **TRAFFIC STEERING**, select the **Overlay** traffic steering policy that you want to configure the path preferences on.
11. In the **Edit Traffic Steering** panel, select **Add Paths**.
12. Keep the defaulted **Type** as **Overlay**, then under **Name**, select the name of the first hub-to-spoke endpoint you created (Example: Hub-wan1-SpokeWan1).

    a. Select the blue checkmark to save the path.

    b. Select **Add Paths** again and keep the defaulted **Type** as **Overlay**. Then, in the **Name** field, select the name of the second hub-to-spoke endpoint you created (Example: Hub-wan1-SpokeWan2). Continue adding paths as needed.

    > **NOTE**: The order of path preference depends on what you configure for a Traffic Steering Strategy. You can configure a Strategy of Ordered, Weighted, or Equal-cost Multipath (ECMP). See "Configure Traffic-Steering Policies" on page 72.

    c. Click **Save** at the bottom of the panel, then click **Save** in the top right corner of the WAN Edge Template.

> **NOTE**: To accomplish the above behavior for spoke to hub traffic, simply configure Traffic Steering on the spoke.

RELATED DOCUMENTATION

Configure Hub Profile for Session Smart Routers | 66

Configure WAN Edge Templates for Session Smart Routers

IN THIS SECTION

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® Session Smart™ Router 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:

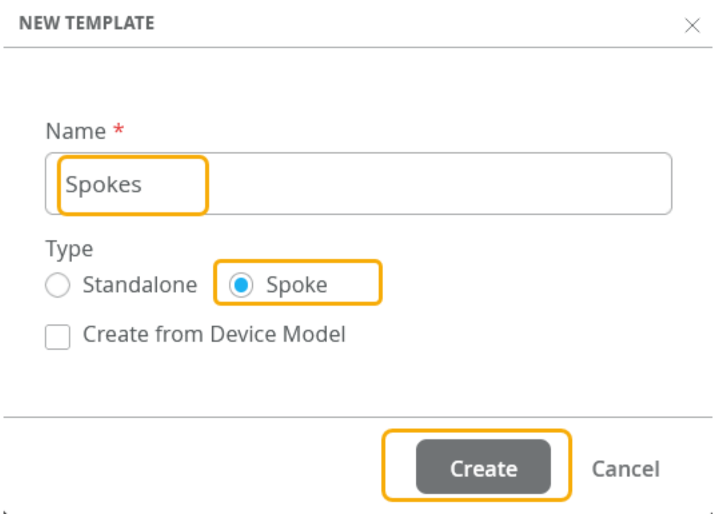
1. In the Juniper Mist cloud portal, click **Organization** > **WAN** > **WAN Edge Templates**. A list of existing templates, if any, appears.

2. 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.

3. In the box that appears, enter the name for the template, click **Type** and select Spoke, and then click **Create**.

Figure 49: Select the Template Type



NEW TEMPLATE

Name *

Spokes

Type

○ Standalone ● Spoke

□ Create from Device Model

> **NOTE**: You can also create a WAN Edge template by importing a JSON file by using the **Import Profile** option.

4. Complete the configurations according to the details provided in Table 14 on page 93

Table 14: WAN Edge Profile Options

Fields	Description
Name	Profile name. Enter a unique profile name with up to 64 characters.

Table 14: WAN Edge Profile Options *(Continued)*

Fields	Description
Type	WAN edge profile type. Select one of the following options: • Standalone—To manage a standalone device in your site. • Spoke—To manage a spoke device that is connecting to a hub device in your configuration.
NTP	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 hub to WAN interface on 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 "Add WAN Interfaces to the Template" on page 95.

Table 14: WAN Edge Profile Options *(Continued)*

Fields	Description
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 "Add a LAN Interface" on page 102.
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 "Configure Traffic-Steering Policies" on page 105.
Application Policies	Policies to enforce rules for traffic. Define network (source), application (destination), traffic steering policies, and policy action. See "Configure Application Policies" on page 106.
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	For any additional settings that are not available in the template's GUI, you can still configure them using CLI commands in the **set** format.

5. 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 hub to WAN interface on spoke. (Note that Mist can also automatically perform onboarding through an aggregated interface on the connected WAN edge cluster, but the interface must first be enabled or the connection will fail. See **Enable Force Up** in Table 2 for configuration details.)

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

To add WAN interfaces to the template:

1. Scroll down to the WAN section and click **Add WAN** to open the Add WAN Configuration pane.
2. Complete the configuration according to the details provided in Table 15 on page 96.

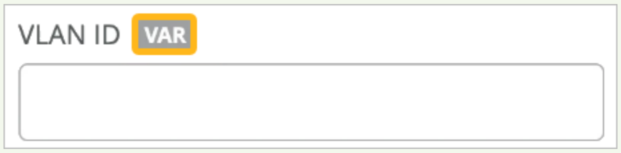
> **TIP**: The fields with this label also display the matching variables (if configured) as you start typing a specific variable in it. This field lists variables from all sites within the organization.
>
> 
>
>
> The organization-wide list of variables can be viewed using **GET /api/v1/orgs/:org_id/vars/search?var=***. This list is populated as variables are added under site settings.

Table 15: WAN Interface Configuration Options

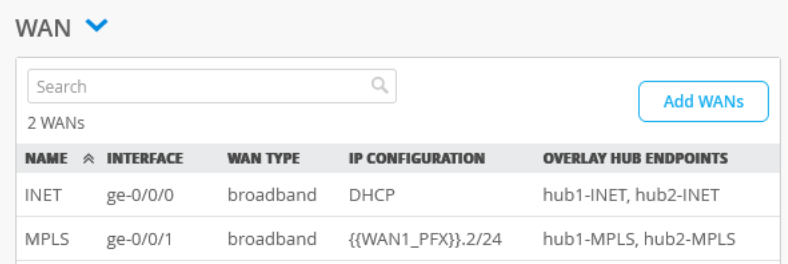
Fields	WAN Interface 1	WAN Interface 2
Name (a label and not a technology)	INET	MPLS
WAN Type	Ethernet	Ethernet
Interface	ge-0/0/0	ge-0/0/3
VLAN ID	-	-
Enable Force Up	Choose this option prior to onboarding a WAN edge device via Link Aggregation Control Protocol (LACP) interface. When enabled, **Enable Force Up** forces the first Ethernet interface in the cluster on the peer to the *up* state, thus allowing the zero-touch provisioning (ZTP) process to retrieve the configuration files needed to complete onboarding.	

Table 15: WAN Interface Configuration Options *(Continued)*

Fields	WAN Interface 1	WAN Interface 2
IP Configuration	DHCP	Static • • **IP Address**={{WAN1_PFX}}.2 • **Prefix Length**=24 • **Gateway**={{WAN1_PFX}}.1
Source NAT	Interface	Interface
Overlay Hub Endpoint (generated automatically).	hub1-INET, hub2-INET (BFD profile Broadband)	hub1-MPLS and hub2-MPLS
MTU	Enter an MTU value between 256 -9192. Default is 1500.	Enter an MTU value between 256 -9192. Default is 1500.

Figure 50 on page 97 shows list of WAN interfaces you created.

Figure 50: WAN Interfaces Summary



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

Configure LTE Interface

Juniper Mist SD-WAN allows organizations to integrate LTE connectivity seamlessly. LTE connectivity provides an alternate path for multipath routing; either as a primary path in locations that have no access to circuits or as a path of last resort in the event that the primary circuit has failed.

For example: In a retail store with a primary MPLS connection for business-critical applications. Juniper Mist SD-WAN can add an LTE link as a backup. If the MPLS link experiences issues, Juniper Mist dynamically switches traffic to the LTE link. This ensures continuous connectivity and minimizes disruptions.

On Session Smart Routers, the LTE support is provided through the in-built LTE module that operates on both 3G and 4G networks. See LTE and Dual LTE Configuration on setting up LTE on Session Smart Routers.

To have LTE link for Juniper Mist SD-WAN, you need an LTE interface setup on your Session Smart Routers and SRX Series Firewalls and insert the Subscriber Identity Module (SIM) in the LTE card.

To add an LTE interface as WAN link:

1. Scroll down to the WAN section and click **Add WAN** to open the Add WAN Configuration pane.
2. Enter the details for the interface configuration

Table 16: LTE Interface Configuration

Fields	Values
Name	Name of the LTE interface
Description	Description of the interface.
WAN Type	LTE
Interface	cl-1/0/0.
LTE APN	Enter the access point name (APN) of the gateway router. The name can contain alphanumeric characters and special characters. (Mandatory for Session Smart Routers).

Table 16: LTE Interface Configuration *(Continued)*

Fields	Values
LTE Authentication	Select the authentication method for the APN configuration: • PAP—Select this option to use Password Authentication Protocol (PAP) as the authentication method. Provide User name and Password. • CHAP—Select this option to use Challenge Handshake Authentication Protocol (CHAP) authentication as the authentication method. Provide User name and Password. • None (Default)—Select this option if you do not want to use any authentication method.
Source NAT	Select Source NAT options: • Interface—NAT using source interface. • Pool—NAT using defined IP address pool. • Disabled—Disable source NAT
Traffic Shaping	Select **Enabled** or **Disabled**. (Required for Session Smart Routers)
Auto Negotiation	Select **Enabled** or **Disabled**.
MTU	Enter an MTU value between 256 -9192. Default is 1500.

3. Click **Save**.

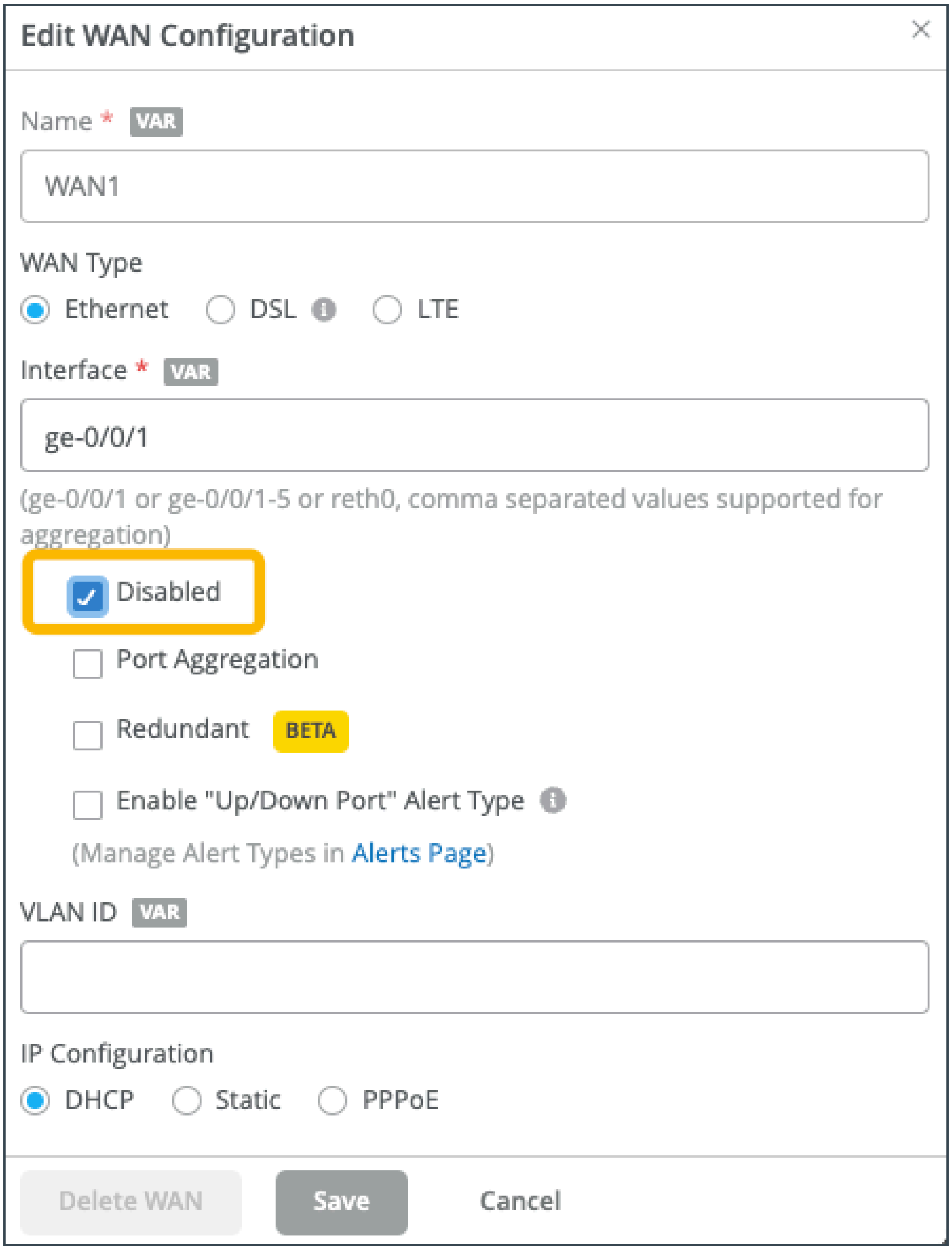
Disable WAN Edge Ports

There are many reasons why it might be necessary to disable a WAN Edge port. In debugging scenarios, for example, disabling a port and then enabling it again can trigger processes to reset, which can help resolve issues.

You may also want to disable a port when you are staging a connection, but are not quite ready to bring the connection into service, or if you've identified a malicious or problematic device, you can disable the port to quickly disable the device until the device can be removed or repaired.

To disable WAN Edge ports:

1. Navigate to **Organization** > **WAN Edge Templates**.
2. Click the appropriate WAN Edge Template.
3. Scroll down to the WAN or LAN section and click the appropriate WAN Edge.
4. In the **Interface** section of the window, select the **Disabled** checkbox. This will administratively disable the WAN Edge device port for the specified interface.



Edit WAN Configuration

Name * VAR

WAN1

WAN Type

● Ethernet ○ DSL ○ LTE

Interface * VAR

ge-0/0/1

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

☑ Disabled

□ Port Aggregation

□ Redundant BETA

□ Enable "Up/Down Port" Alert Type

(Manage Alert Types in Alerts Page)

VLAN ID VAR

IP Configuration

● DHCP ○ Static ○ PPPoE

5. Click **Save** at the bottom of the window to save the changes.
6. Click **Save** at the top right-corner of the template page.

   This option is part of interface configuration. If you use this option to disable an aggregated Ethernet (AE) interface or redundant Ethernet (reth) interface, all member links are disabled

Add a LAN Interface

LAN interface configuration identifies your request source from the name of the network you specify in the LAN configuration. (Note that Mist can automatically perform onboarding through an aggregated interface on the connected WAN edge cluster, but the interface must first be enabled or the connection will fail. See **Enable Force Up** for details.)

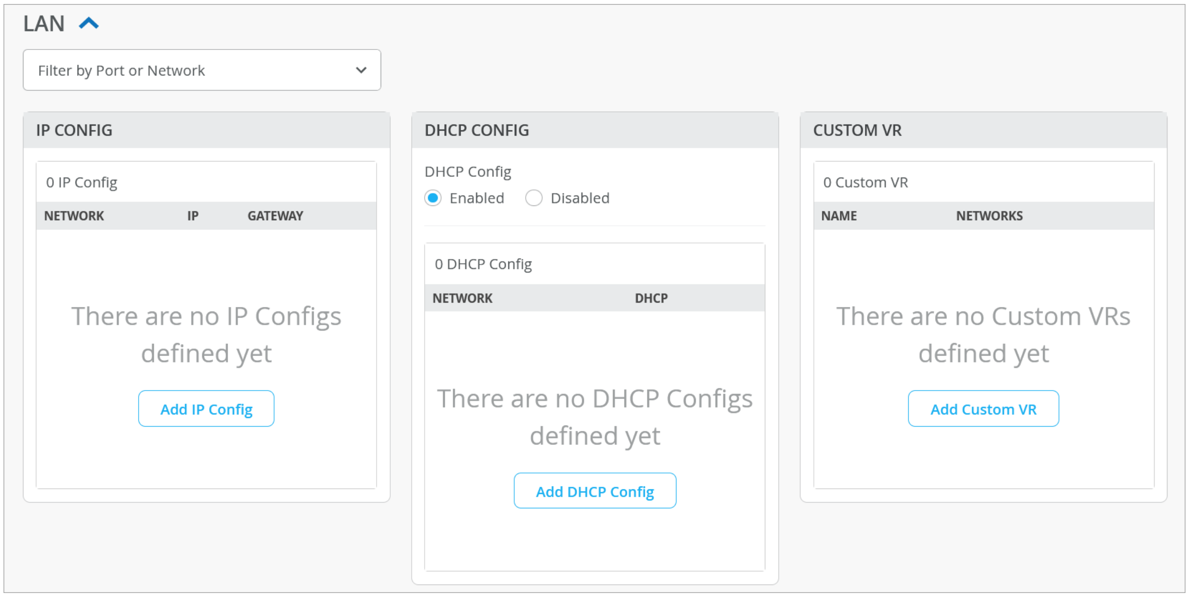
To add a LAN interface:

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

To add a LAN interface:

1. Scroll down to the LAN pane and click **Add LAN** to open the Add LAN Configuration panel.

Figure 51: Add LAN Interfaces to the Template


LAN
Filter by Port or Network

IP CONFIG

0 IP Config

NETWORK	IP	GATEWAY

There are no IP Configs defined yet

DHCP CONFIG

DHCP Config
● Enabled ○ Disabled

0 DHCP Config

NETWORK	DHCP

There are no DHCP Configs defined yet

CUSTOM VR

0 Custom VR

NAME	NETWORKS

There are no Custom VRs defined yet

2. Configure LAN interfaces.

   The LAN configuration section includes the components for IP Configuration, DHCP Configuration, and Custom VR. The LAN configuration section enables more flexibility by allowing you to override each configuration component (such as IP configuration) separately without touching other components.

   The LAN Configuration section also provides a filter for you to easily search for configurations per port or network.

   - IP configuration

    - **Network**—Select an available network from the drop-down.
    - **IP Address**—IPv4 address and prefix length for the interface.
    - **Prefix Length**—Prefix length for the interface.
    - **Redirect Gateway**—IP address of redirect gateway for Session Smart Routers.
  - DHCP configuration—Select **Enabled** option to use DHCP service for assigning IP addresses to the LAN interface.
    - **Network**—Select the network from the list of available networks.
    - **DHCP type**—Select DHCP Server or DHCP Relay. If you chose DHCP server, enter the following options:
      - **IP Start**—Enter the beginning IP address of the desired IP address range.
      - **IP End**—Enter the ending IP address.
      - **Gateway**—Enter the IP address of the network gateway.
      - **Maximum Lease Time**—Specify a maximum lease time for the DHCP addresses. Supported DHCP lease duration ranges from 3600 seconds (1 hour) to 604800 seconds (1 week).
      - **DNS Servers**—Enter IP address of the Domain Name System (DNS) server.
      - **Server Options**—Add following options:
        - **Code**—Enter the DHCP option code you want to configure the server. The Type field will be populated with the associated value. For example: If you select Option 15 (domain-name), the **Type** field displays FQDN. You must enter the **Value** associated to the Type.
      - Static Reservations—Use this option if you want to statically reserve a DHCP address. Static DHCP IP address reservation involves binding a client MAC address to a static IP address from the DHCP address pool. The following options are available:
        - **Name**—A name that identifies the configuration.
        - **MAC Address**—The MAC address to be used in the reservation.
        - **IP Address**—The IP address to be reserved.
  - Custom VR configuration.
    - **Network**—Select an available network from the drop-down.
    - **Name**—Enter the name for the routing instance.

3. Complete the configuration according to the details provided in Table 17 on page 104.

TIP: The fields with this label also display the matching variables (if configured) as you start typing a specific variable in it. This field lists variables from all sites within the organization.

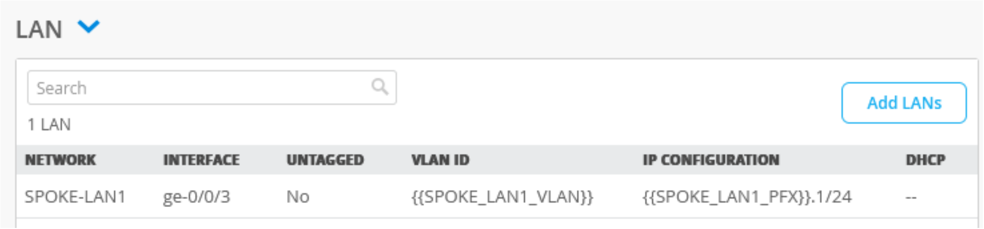
The organization-wide list of variables can be viewed using **GET /api/v1/orgs/:org_id/vars/search?var=***. This list is populated as variables are added under site settings.

Table 17: Sample LAN Interface Configuration

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	
Enable Force Up	Choose this option prior to onboarding a device that is connected to the LAN port via Link Aggregation Control Protocol (LACP). For example, if you are onboarding a new switch to the Mist cloud, the switch will not already be provisioned for LACP. Setting **Enable Force Up** will force the first Ethernet interface of the LACP on the WAN edge device to the *up* state, which in turn allows the switch to connect to the Mist cloud using zero-touch provisioning (ZTP), where it will retrieve the configuration files needed to complete the onboarding.	
DHCP	No	

Figure 52 on page 105 shows the list of LAN interface you created.

Figure 52: Summary of LAN Interface



LAN

1 LAN

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:

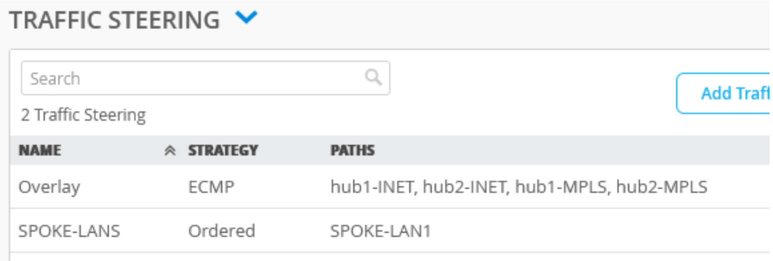
1. Scroll down to the Traffic Steering section, and click **Add Traffic Steering** to display the Traffic Steering configuration pane.
2. Complete the configuration according to the details provided in Table 18 on page 105.

Table 18: Traffic-Steering Policies Summary

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 • **Network** —SPOKE-LAN1	• **Type**— WAN • **Network** — • hub1-INET • hub2-INET • hub1-MPLS • hub2-MPLS

Figure 53 on page 106 shows the list of traffic steering policies you created.

Figure 53: Traffic-Steering Policies Summary



2 Traffic Steering

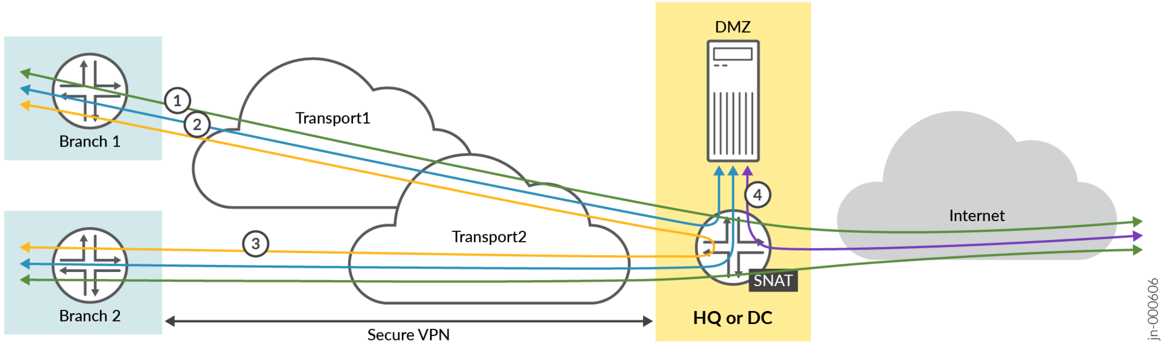
NAME	STRATEGY	PATHS
Overlay	ECMP	hub1-INET, hub2-INET, hub1-MPLS, hub2-MPLS
SPOKE-LANS	Ordered	SPOKE-LAN1

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 Figure 54 on page 106. The image depicts a basic initial traffic model for a corporate VPN setup (third spoke device and second hub device are not shown).

Figure 54: Traffic Flow and Distribution



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

- 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: This may not be feasible in the real world except on expensive MPLS networks with managed IPs. Managed IPs send traffic directly to the other spoke. This type of traffic usually flows through a hub device

- 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. Juniper Mist cloud evaluates and applies application policies in the order in which the policies are listed.

NOTE:

- Order of application policies do not have any effect on Session Smart Router configuration. As good practice, we recommend you to place global rules towards the end of the policy rules list.
- Traffic steering on each rule is not a mandatory for Session Smart Routers. When you use Session Smart Router, the system announces all routes on each LAN interface using the iBGP-based route distribution.
- Use the same name for network on both sides for Session Smart Router for traffic to traverse between a hub and a spoke. The network name for the Session Smart Router must be identical to the security tenant used for traffic isolation. Because of this, the network name must match on both sides.

To create an application policy:

1. Under the **Application Policy** pane, click the **Add Policy** button to add a new rule in the policy list.
2. Complete the configuration according to the details provided in Table 19 on page 107

Table 19: Application Policies Configuration

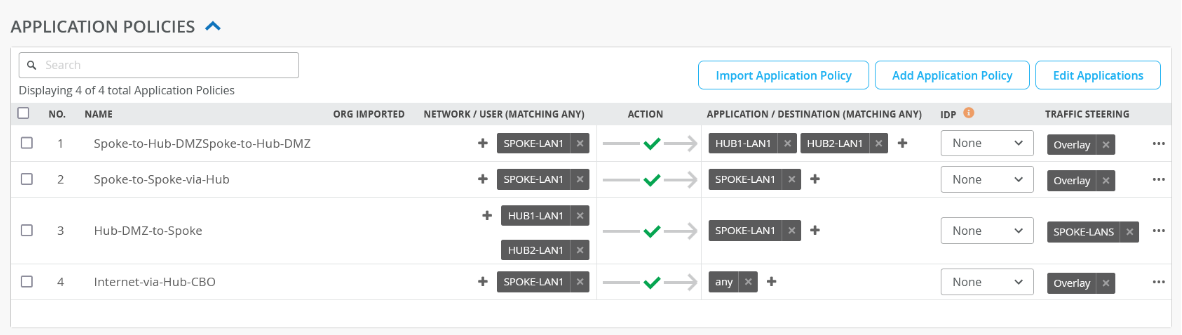
S.No	Rule Name	Network	Action	Destination	Steering
1	Spoke-to-Hub-DMZ	SPOKE-LAN1	Pass	HUB1-LAN1 + HUB2-LAN1	Overlay
2	Spoke-to-Spoke-via-Hub	SPOKE-LAN1	Pass	SPOKE-LAN1	Overlay

Table 19: Application Policies Configuration *(Continued)*

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

Figure 55 on page 108 shows the list of application policies you created.

Figure 55: Application Policies Summary



Displaying 4 of 4 total Application Policies

□	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
□	1	Spoke-to-Hub-DMZSpoke-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

Assign Spoke Templates to Sites

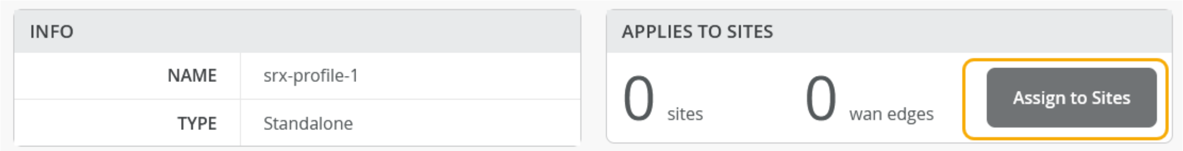
The template now exists in the Juniper Mist cloud as an object that can be attached to one or more sites.

- You can apply the same template to multiple sites.
- If a site already has a template assigned to it, assigning another template will replace the existing template (in other words, one site cannot have two templates).

To assign the spoke template to site:

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

Figure 56: Assign Spoke Templates to Sites



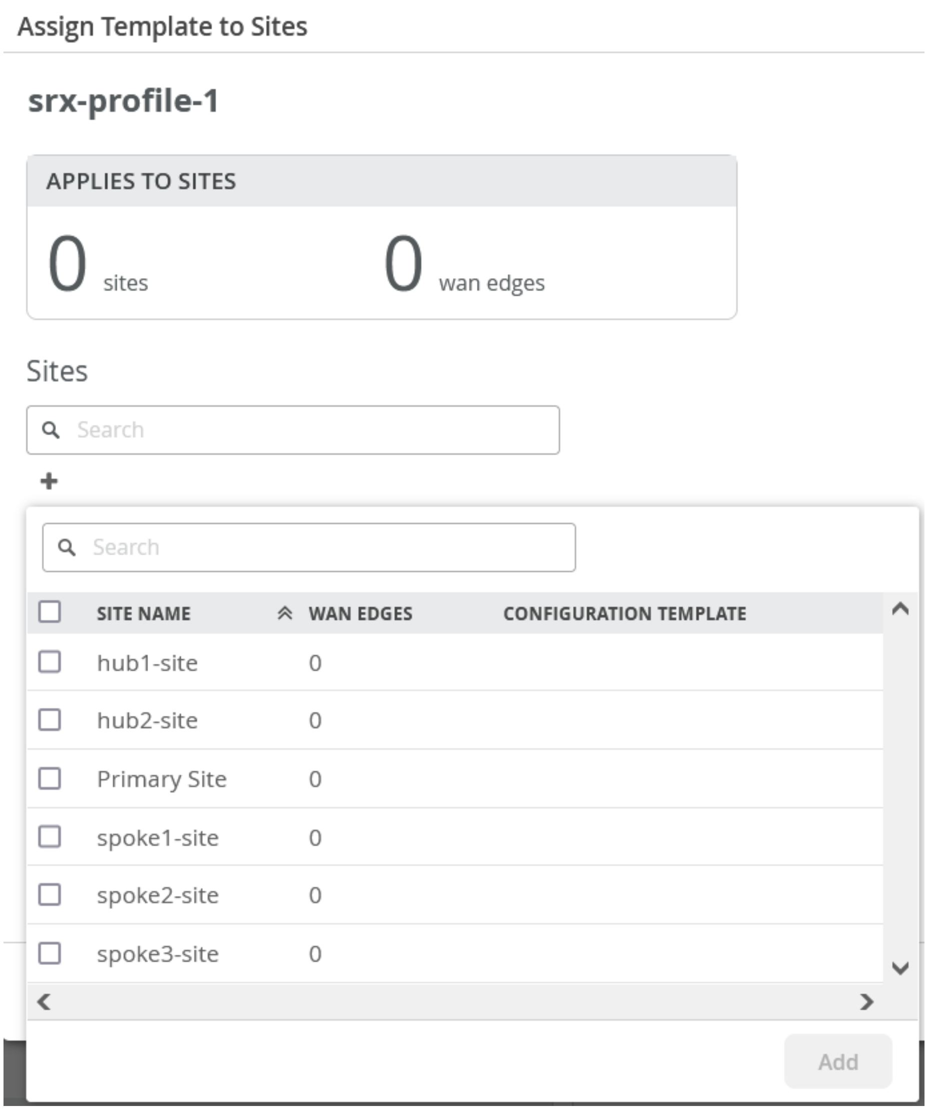
INFO	
NAME	srx-profile-1
TYPE	Standalone

APPLIES TO SITES

0 sites 0 wan edges

2. In the **Assign Template to Sites**, select the required sites.

Figure 57: Select Sites to Assign Spoke Templates



Assign Template to Sites

srx-profile-1

APPLIES TO SITES

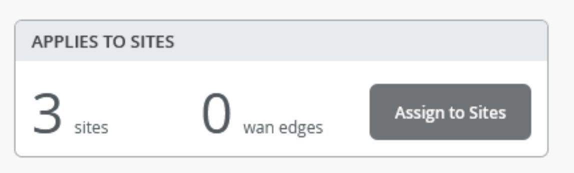
0 sites 0 wan edges

Sites

□	SITE NAME	WAN EDGES	CONFIGURATION TEMPLATE
□	hub1-site	0	
□	hub2-site	0	
□	Primary Site	0	
□	spoke1-site	0	
□	spoke2-site	0	
□	spoke3-site	0	

3. Click **Apply**.

Figure 58: WAN Edge Templates Applied to Sites


APPLIES TO SITES

3 sites

0 wan edges

Configure Device-Specific WAN Edge Templates

IN THIS SECTION

Device configuration is simplified with WAN Edge Templates following your device onboarding process. These WAN Edge templates can be customized to unique deployments across all edge devices. Juniper Networks Mist AI is positioned uniquely in the industry as Mist AI WAN Edge templates can be applied to any model, regardless of vendor. Additionally, WAN Edge templates can mix and match different models under a single template, streamlining your configuration and deployment phase.

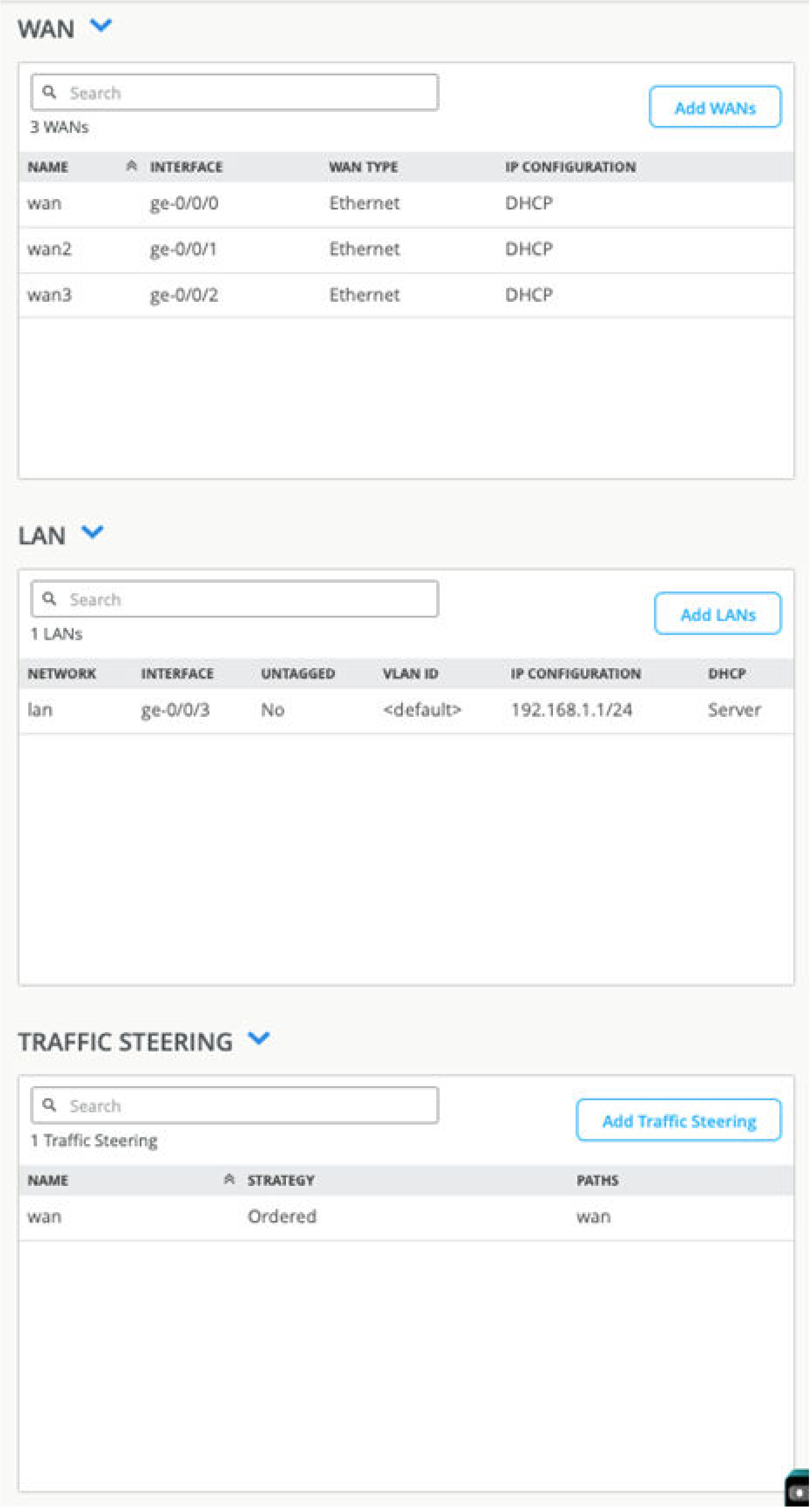
To manually configure your WAN Edge templates for the Session Smart Router, see "Configure a WAN Edge Template" on page 92.

Device-Specific WAN Edge Templates

There is a significant benefit to leveraging select Juniper Networks hardware with Mist AI SD-WAN. Configuration is simplified for many Juniper Networks® Session Smart™ Routers, and Juniper Networks® SRX Series Firewalls, which have device-specific templates that automatically assign WAN and LAN interfaces and define LAN Networks for connectivity.

These templates are unique for each device model. With zero manual input after device selection and naming the WAN Edge, a user’s specified WAN Edge device is pre-populated with the values.

Figure 59: Sample of SSR120 WAN Edge Template



WAN

3 WANs

NAME	INTERFACE	WAN TYPE	IP CONFIGURATION
wan	ge-0/0/0	Ethernet	DHCP
wan2	ge-0/0/1	Ethernet	DHCP
wan3	ge-0/0/2	Ethernet	DHCP

LAN

1 LANs

NETWORK	INTERFACE	UNTAGGED	VLAN ID	IP CONFIGURATION	DHCP
lan	ge-0/0/3	No	<default>	192.168.1.1/24	Server

TRAFFIC STEERING

1 Traffic Steering

NAME	STRATEGY	PATHS
wan	Ordered	wan

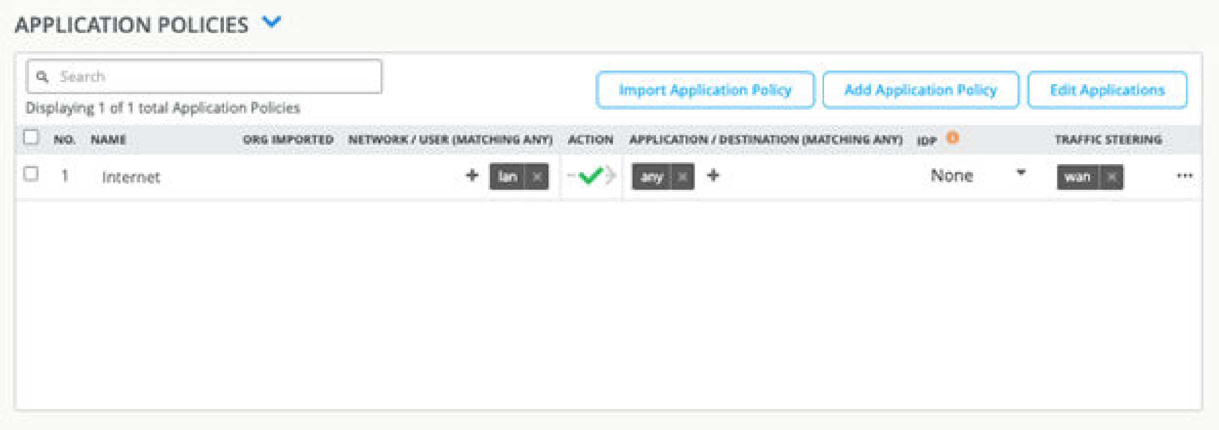
For example, Figure 59 on page 111 shows that the SSR120 WAN Edge template generates several values, including Ethernet interfaces for **LAN** and **WAN** with relevant **DHCP** and **IP** values:

- wan ge-0/0/0
- wan2 ge-0/0/1
- wan3 ge-0/0/2
- lan ge-0/03

Additionally, we see in Figure 59 on page 111 that the Juniper Mist portal populates a traffic steering policy. This enables Juniper Mist to send traffic over our **wan** connection to an **any** Mist Application with a quad zero catch-all destination.

Upon applying a WAN Edge template, application policies, networks, and applications receive automatic updates as shown in Figure 60 on page 112, Figure 61 on page 113, and Figure 62 on page 113.

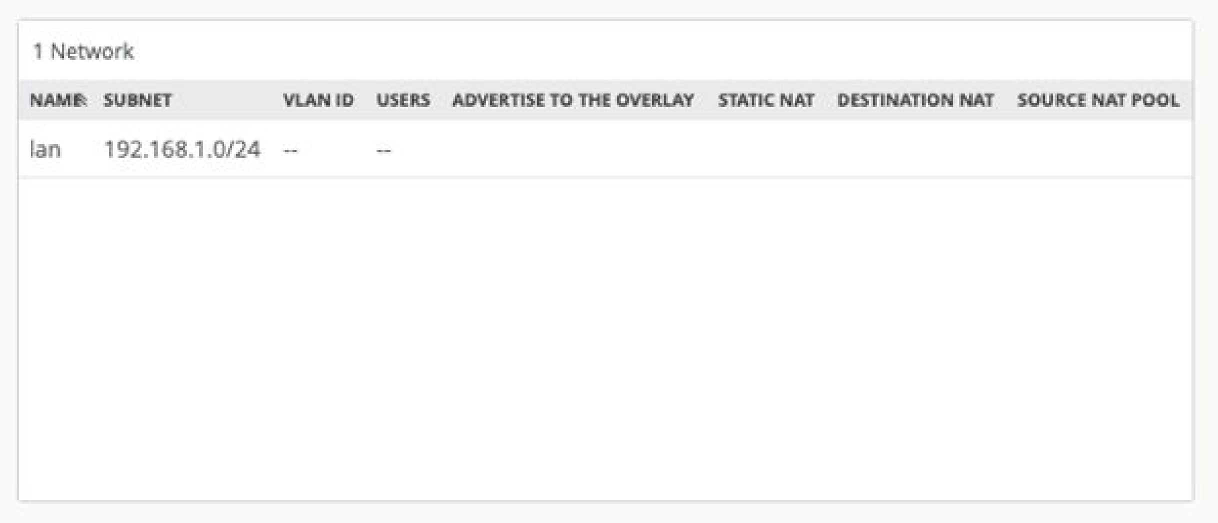
Figure 60: Application Policies After Applying WAN Edge Template for SSR120



Displaying 1 of 1 total Application Policies

□	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
□	1	Internet		+ lan	✓	any +	None	wan

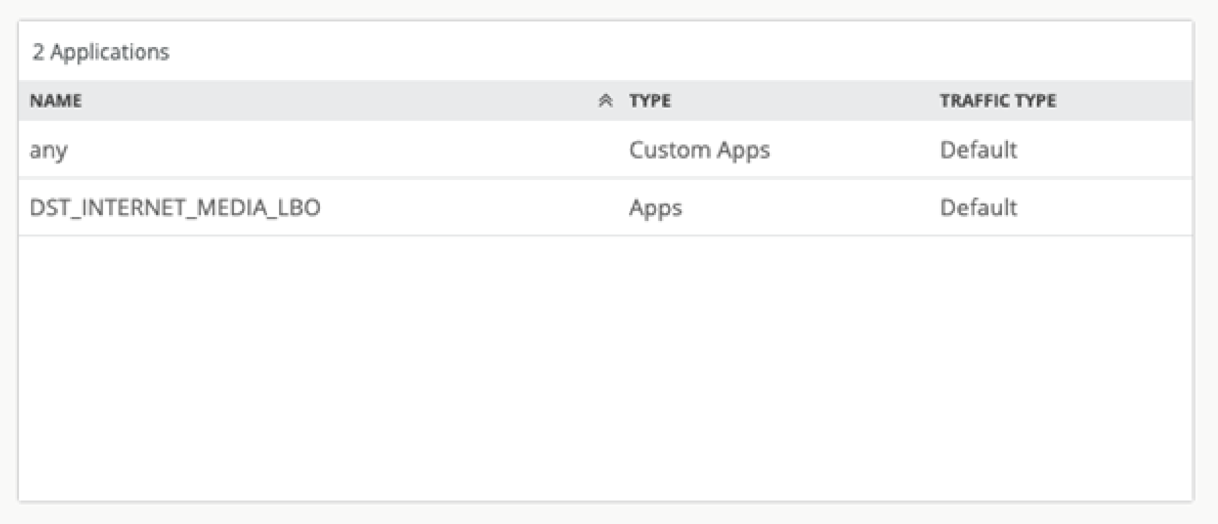
Figure 61: Networks After Applying WAN Edge Template for SSR120



1 Network

NAME	SUBNET	VLAN ID	USERS	ADVERTISE TO THE OVERLAY	STATIC NAT	DESTINATION NAT	SOURCE NAT POOL
lan	192.168.1.0/24	--	--				

Figure 62: Applications After Applying WAN Edge Template for SSR120



2 Applications

NAME	TYPE	TRAFFIC TYPE
any	Custom Apps	Default
DST_INTERNET_MEDIA_LBO	Apps	Default

Juniper Mist AI SD-WAN includes the following device models with pre-configured WAN Edge templates for Session Smart Routers:

- SSR120
- SSR130
- SSR1200
- SSR1300

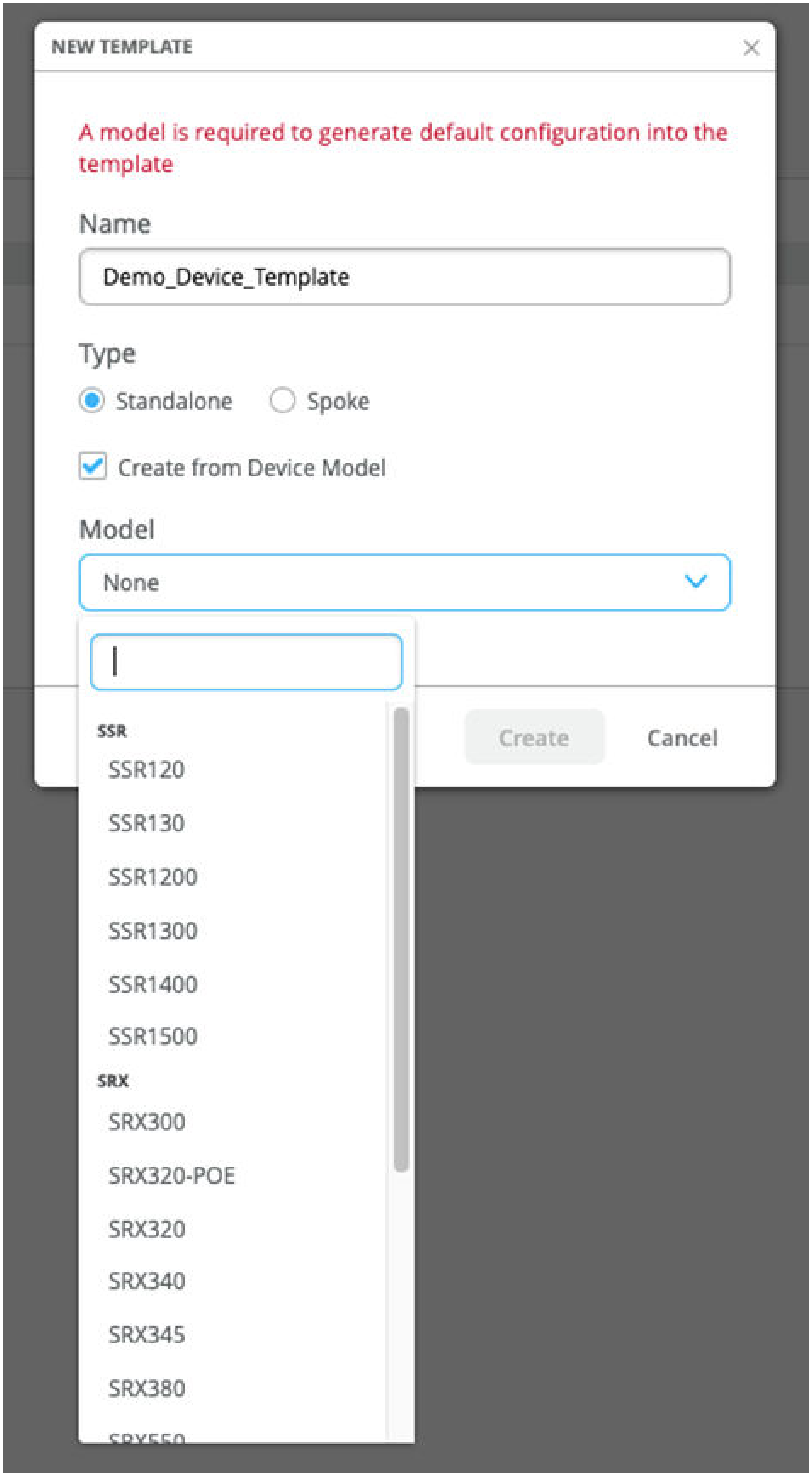
- SSR1400
- SSR1500

The WAN Edge device specific templates provide basic network configuration in a single step and allow for re-usable and consistent configuration for Session Smart Router and SRX Series Firewall device you deploy. The template provides device-specific, pre-configured WAN interfaces, LAN interfaces, a traffic steering policy, and an application policy. All you have to do is name the template and select the device type.

To select a device-specific WAN Edge template:

1. In the Juniper Mist portal, select **Organization > WAN > WAN Edge Templates**.
2. Select **Create Template** in the upper right corner to open a new template page.
3. Enter the name for the template.
4. Click the **Create from Device Model** check-box.
5. Select your device model from the drop-down box.

Figure 63: Configure Device-Specific WAN Edge Template



NEW TEMPLATE

A model is required to generate default configuration into the template

Name

Demo_Device_Template

Type

● Standalone ○ Spoke

☑ Create from Device Model

Model

None

6. Click **Create**.

Juniper Mist UI displays the completed device template. You now have a working WAN Edge template that you can apply to many sites and devices across your organization.

Assign to Site

With your template set up, you need to save and assign it to the site where your WAN edge device will be deployed.

1. Click the **Assign to Site** button at the top of the template page.
2. Select a site from the list where you want the template applied.
3. Click **Apply**.
4. Finally, all that remains is to associate the device with your Site: "Onboard Session Smart Routers for WAN Configuration" on page 132

SEE ALSO

WAN Assurance Configuration Overview | 31

Configure Networks for Session Smart Routers | 38

Configure Applications for Session Smart Routers | 48

Configure Application Policies on Session Smart Routers | 58

Configure Hub Profile for Session Smart Routers | 66

Onboard Session Smart Routers for WAN Configuration | 132

Routing Configuration on Session Smart Routers

IN THIS SECTION

Configure BGP Groups

You can configure BGP (Border Gateway Protocol) and add their BGP neighbors. You can also add and modify peer-based advertisement and redistribution rules

To configure a BGP group:

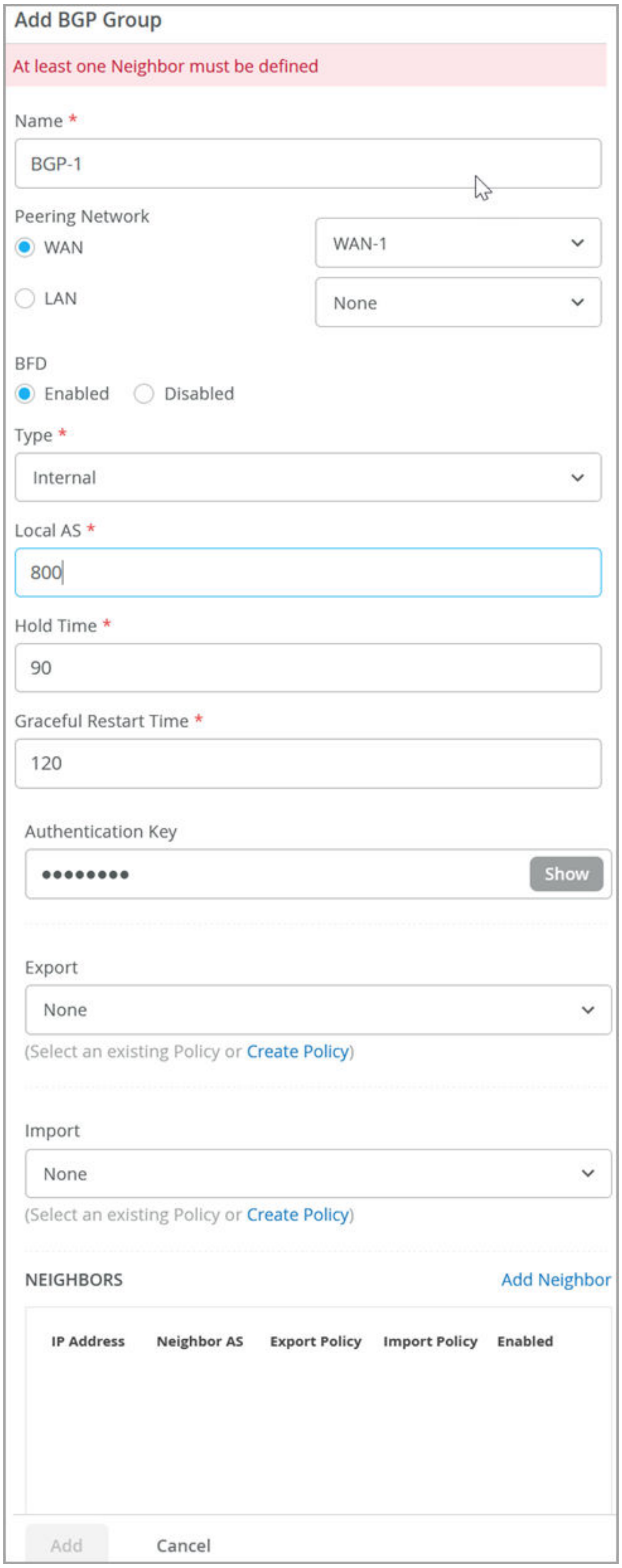
1. In the Juniper Mist™ portal, click **Organization** > **WAN** > **WAN Edge Templates**.

2. Create a new template or click an existing template to modify it.

3. In the Templates page, scroll down to Routing pane and click **Add BGP Group**.

4. In the Add BGP Group window, add details for the BGP group.

Figure 64: Add BGP Group



Add BGP Group

At least one Neighbor must be defined

Name *

BGP-1

Peering Network

● WAN — WAN-1

○ LAN — None

BFD

● Enabled ○ Disabled

Type *

Internal

Local AS *

800

Hold Time *

90

Graceful Restart Time *

120

Authentication Key

●●●●●●●●

Export

None

(Select an existing Policy or Create Policy)

Import

None

(Select an existing Policy or Create Policy)

NEIGHBORS

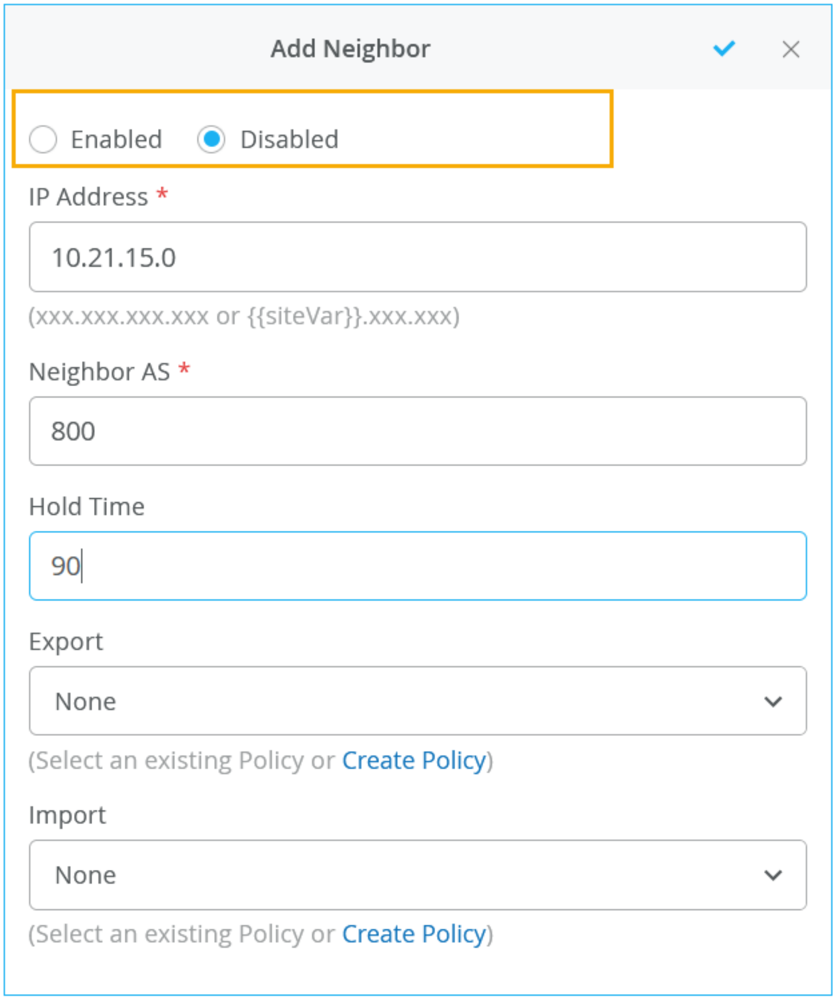
IP Address	Neighbor AS	Export Policy	Import Policy	Enabled

- Name—Name of the BGP group.
- Peering Network —Select Peering Network as **WAN** or **LAN**.
- BFD —Select **Enabled** or **Disabled**.
- Type —Select **Internal** or **External**.
- Local AS —Specify the local autonomous system (AS) number.
- Hold Time —Specify the hold-time value to use when negotiating a connection with the peer.
- Graceful Restart Time —Specify graceful restart for BGP. Graceful restart allows a routing device undergoing a restart to inform its adjacent neighbors and peers of its condition
- Authentication Key —Configure an MD5 authentication key (password). Neighboring routing devices use the same password to verify the authenticity of BGP packets sent from this system
- Click drop-down for **Export** or **Import** and select an existing routing policy or click **Create Policy**.
    - In the Routing Policy window,you can add or edit the policy for the overlay path preference.
        - **Name**—Enter the name of the policy.
        - **Add Terms**—Enter the policy conditions such as prefix, autonomous system [AS] path regular expressions, protocols, and community.
        - **Then**—Select an action (Accept or Reject) to apply when the condition is fulfilled. Enable one of the following preference for the accepted path:
            - Append Community
            - Exclude Community
            - Set Community
            - Prepend AS Path
            - Exclude AS Path
            - Set Local Preference
            - Add Target VRs
        - Click **Add** to add to save the routing policy.

5. On the Add BGP Group window, for the **Export** or **Import** field, select the routing policy you created from the drop-down.

6. In **Neighbors** pane, click **Add Neighbors**

Figure 65: BGP Group- Add Neighbors



Add Neighbor

○ Enabled ● Disabled

IP Address *

10.21.15.0

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

Neighbor AS *

800

Hold Time

90

Export

None

(Select an existing Policy or Create Policy)

Import

None

(Select an existing Policy or Create Policy)

.

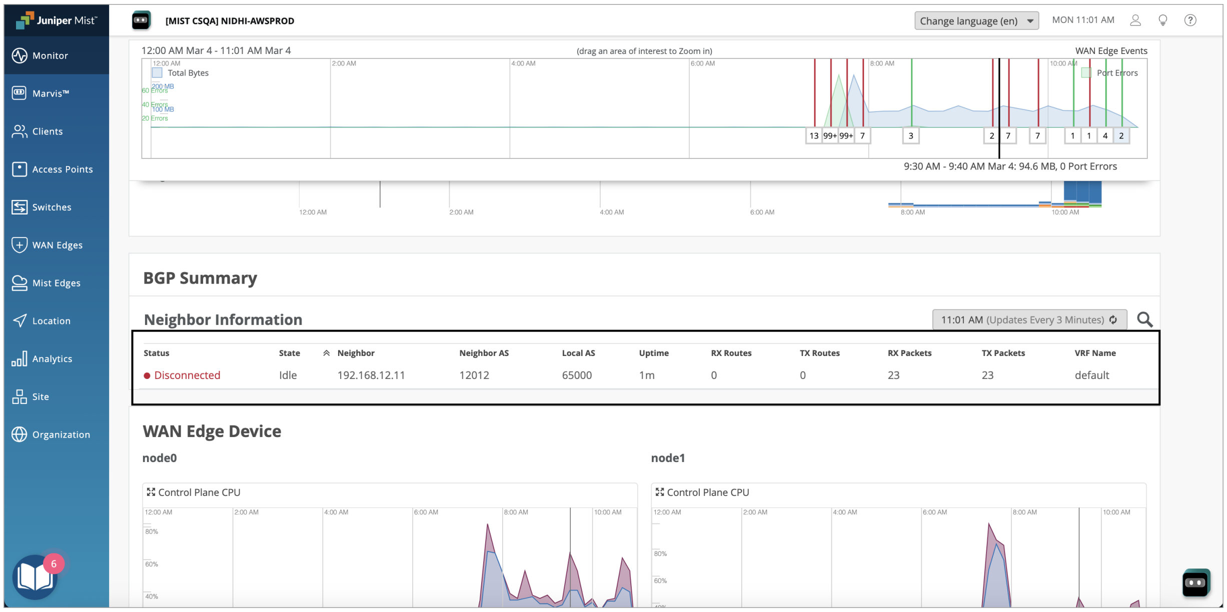
- Select **Enabled** or **Disabled** to administratively enable or disable a BGP neighbor.
- IP address —Enter the IP address of the neighbor device.
- Neighbor AS —Enter the neighbor node AS.
- Hold Time —Specify the hold-time value to use when negotiating a connection with the neighbor device.
- Type —Click drop-down for **Export** or **Import** and select an existing routing policy or click **Create Policy**.

7. Select the check-box in **Add Neighbors** pane to add the neighbor.

8. Click **Save**.

You can view the BGP neighbors details in **BGP Summary** section of **Monitor > Insights** page.

Figure 66: BGP Neighbor Information



BGP Summary

Neighbor Information

11:01 AM (Updates Every 3 Minutes)

Status	State	Neighbor	Neighbor AS	Local AS	Uptime	RX Routes	TX Routes	RX Packets	TX Packets	VRF Name
● Disconnected	Idle	192.168.12.11	12012	65000	1m	0	0	23	23	default

Configure BFD for BGP Sessions

The Bidirectional Forwarding Detection (BFD) protocol is a simple Hello mechanism that detects failures or faults between network forwarding elements that share a link. Hello packets are sent at a specified, regular interval. When the routing device stops receiving a reply after a specified interval, a neighbor failure is detected . The failure detection timers for BFD provide faster detection, as they have shorter time limits than that of the default failure detection mechanisms for BGP.

To enable or disable BFD for the BGP sessions on a Session Smart Router deployed as a WAN Edge device:

1. In the Mist portal, navigate to **Organization** > **WAN Edge Templates** > ***WAN Edge Name***.
2. From the **BGP** section, click on an existing BGP Group, or click **Add BGP Group** to add a new one.
3. In the **Add BGP Group** window, Under **BFD**, select **Enabled** or **Disabled** depending on your network needs.
4. Configure any other necessary setting for your BGP group, then click **Add** at the bottom of the window.

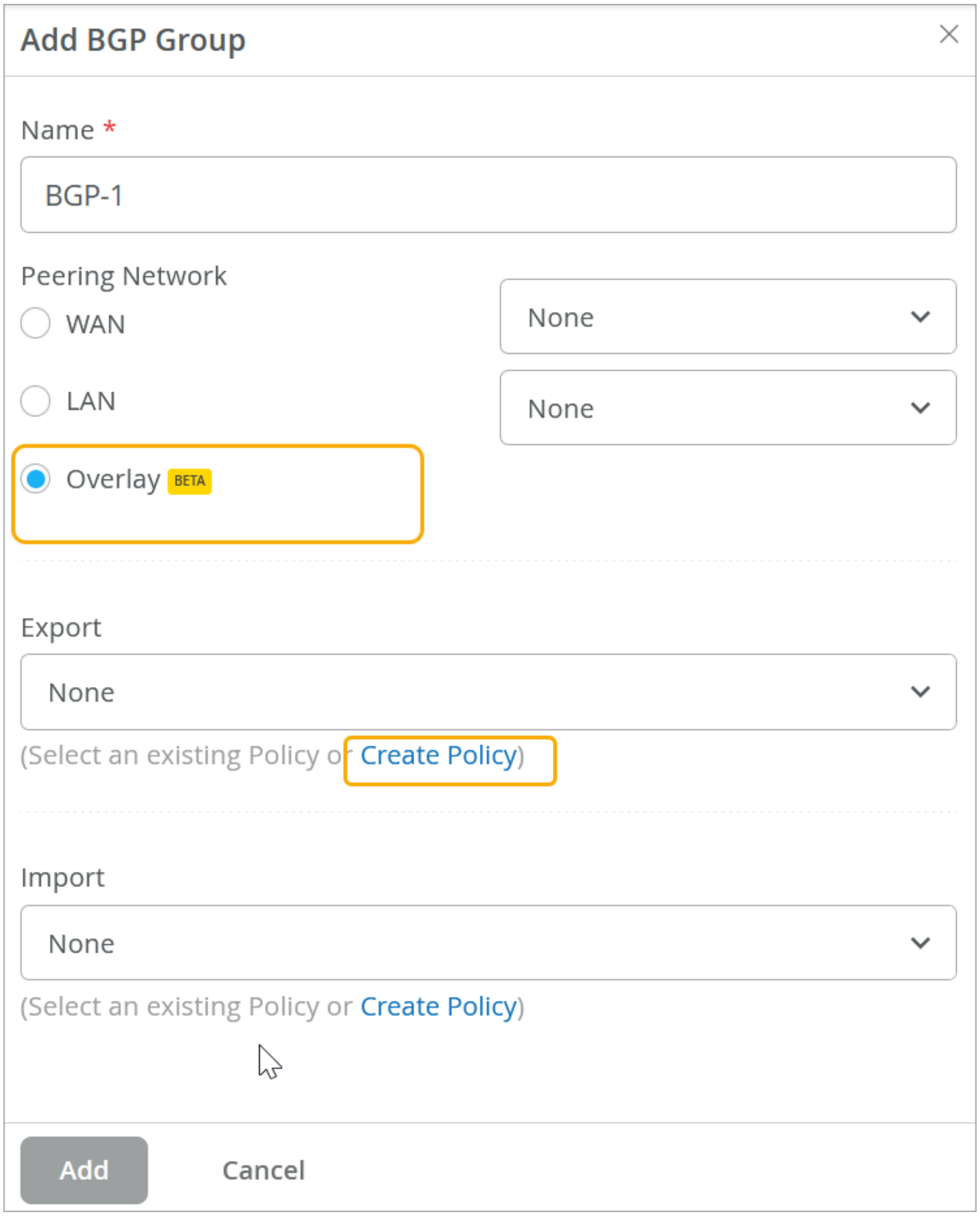
Overlay Traffic Steering for BGP-Learned Prefixes

You can specify a preferred path for the traffic traversing from a spoke device to the BGP-learned prefixes by configuring overlay path preferences. You can configure path preferences in the routing policies on the spoke devices. This feature allows you to determine which hub the traffic should pass through.

To configure path preferences:

1. In the Add BGP Group window, enter the details for the BGP group:

Figure 67: Add BGP Group



Add BGP Group

Name * BGP-1

Peering Network

○ WAN — None

○ LAN — None

● Overlay BETA

Export: None

(Select an existing Policy or Create Policy)

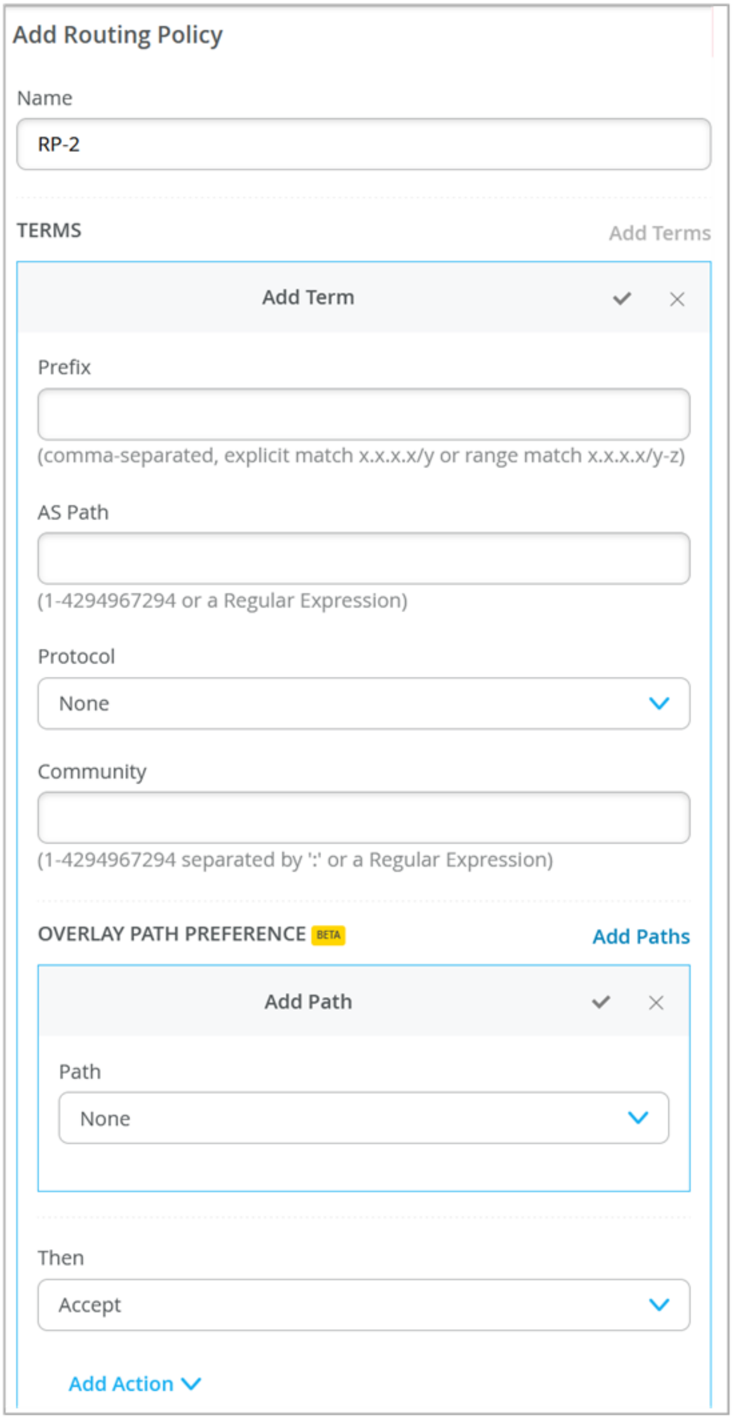
Import: None

(Select an existing Policy or Create Policy)

2. Enter the following details:

   - Enter a name of the BGP group.
   - Select Peering Network as **Overlay**.
   - Click drop-down for **Export** and select an existing routing policy or click **Create Policy**.
   - In the Routing Policy window,you can add or edit the policy for the overlay path preference.

Figure 68: Add Routing Policy



Add Routing Policy

Name

RP-2

TERMS

Add Terms

Add Term

Prefix

(comma-separated, explicit match x.x.x.x/y or range match x.x.x.x/y-z)

AS Path

(1-4294967294 or a Regular Expression)

Protocol

None

Community

(1-4294967294 separated by ':' or a Regular Expression)

OVERLAY PATH PREFERENCE BETA

Add Paths

Add Path

Path

None

Then

Accept

Add Action

- **Name**—Enter the name of the policy.
- **Add Terms**—Enter the policy conditions such as prefix, autonomous system [AS] path regular expressions, protocols, and community.

- **Overlay Path Preference**—Enter overlay path preference. Click **Add Paths** and select an existing overlay hub endpoint.
- **Then**—Select an action (Accept or Reject) to apply when the condition is fulfilled. Enable one of the following preference for the accepted path:
  - **Append Community**—Add a BGP community to the route. A BGP community is a group of destinations that share a common property.
  - **Exclude Community**—Exclude a BGP communities to the route.
  - **Set Community**—Set a BGP community in the route. The set option replaces the current communities on a route with the specified community
  - **Prepend AS Path**—Prepend a AS number to the start of a BGP AS path.
  - **Exclude AS Path**—Exclude a AS number from the start of a BGP AS path.
  - **Set Local Preference**—Set preference to assign to routes that are advertised to the group or peer.
  - **Add Target VRs**— Add virtual Routing and Forwarding (VRF) instances for the intentional sharing of route information across VRF instances.
- Click **Add** to add to save the routing policy.
- On the Add BGP Group window, for the **Export** field, select the routing policy you created from the drop-down.

3. Click **Save**.

> **NOTE**: You can create overlay traffic steering for BGP-learned prefixes by selecting **WAN Edges** in Juniper Mist Portal.

Configure OSPF

Open Shortest Path First (OSPF) is a link-state routing protocol used in IP networks to determine the best path for forwarding IP packets. OSPF divides a network into areas to improve scalability and control the flow of routing information. The following steps explain how you can configure OSPF for your Session Smart Router deployed as a WAN Edge device.

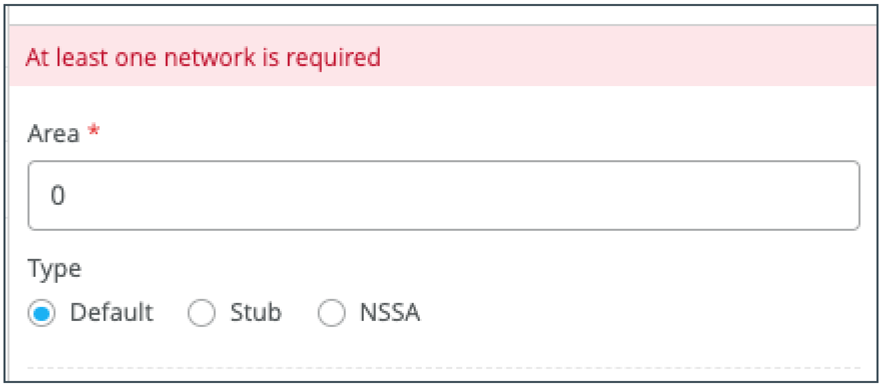
You must first define an OSPF Area from the **OSPF AREAS** tile, then apply that area to the WAN Edge device from the **OSPF CONFIGURATION** tile.

NOTE: You can configure OSPF from the Routing section on WAN Edge templates (**Organization** > **WAN Edge Templates**), hub profiles (**Organization** > **Hub Profiles**), or the WAN Edge device configuration page (**WAN Edges** > **WAN Edges** > ***WAN Edge Name***). The following steps show how to configure OSPF from the WAN Edge Template.

1. From the Mist portal, navigate to **Organization** > **WAN Edge Templates**.
2. In the **ROUTING** section, from the **OSPF AREAS** tile, click **Add OSPF Area**.
3. In the **Add OSPF Area** window, add the following information:

Table 20: Add OSPF Area Options

Field	Description
Area	This number indicates the identification area that your OSPF network or Session Smart Router belongs to.
Type	This is the OSPF Area type. Select one of the following options: **a.** Default (Area 0) — This represents the core of an OSPF network. **b.** Stub — Using this OSPF area type blocks external routes. **c.** Not So Stubby Area (NSSA) — Using this OSPF area type allows redistribution of some external routes and not others. For a more in depth explanation of the different area types, see Configuring OSPF Areas.



At least one network is required

Area *

0

Type

● Default ○ Stub ○ NSSA

4. Click **Add OSPF Network**, then, in the **Add OSPF Network** section of the window, enter the following information:

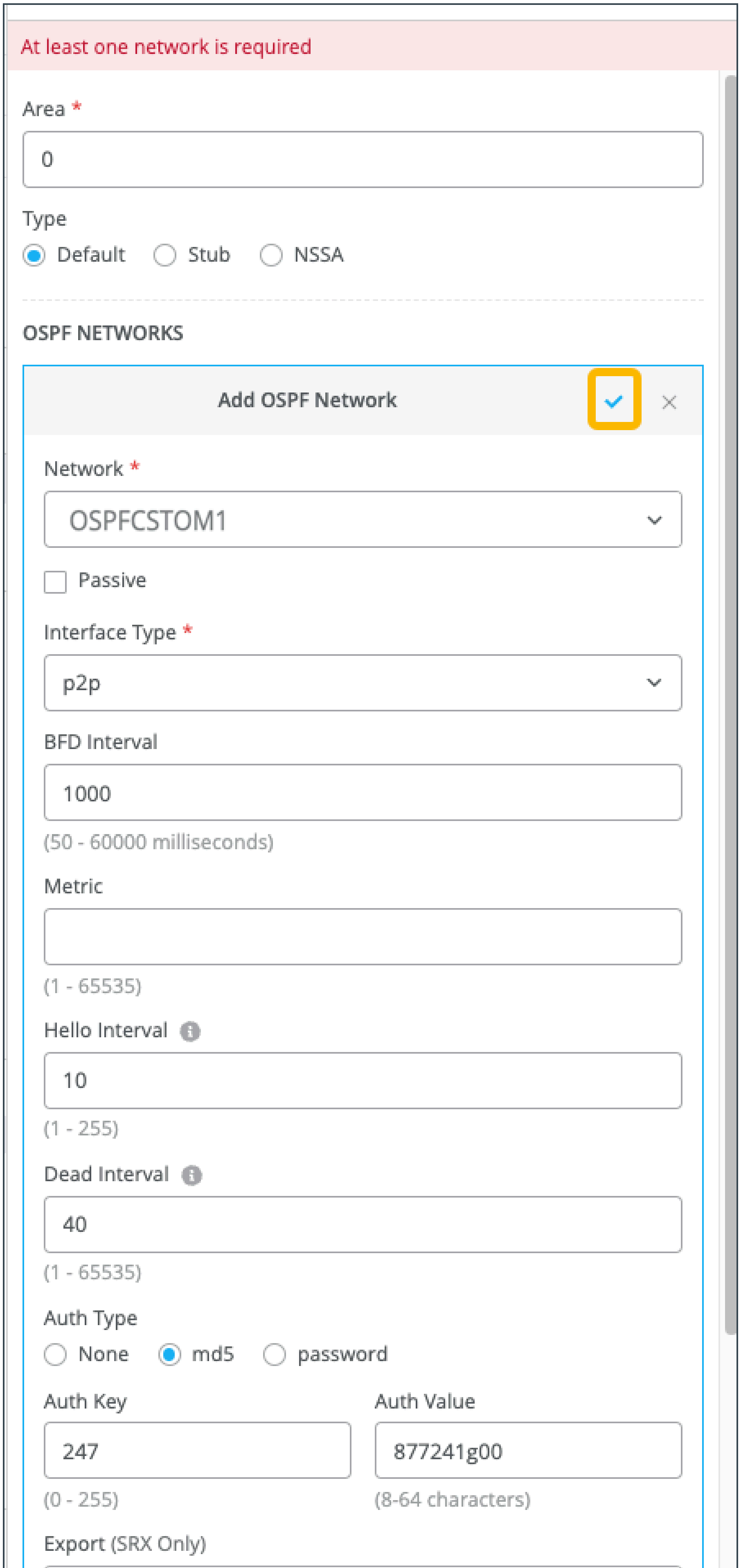
Table 21: Add OSPF Network Options

Field	Description
Network	This is the name of your OSPF network. **NOTE**: Check the **Passive** checkbox if you do not want OSPF to send Hello packets on an interface. This prevents the interface from forming unnecessary neighor relationships, which reduces overhead on routers and ensures that only the crucial connections are being made.
Interface Type	• Broadcast — This is the default interface type for an OSPF ethernet interface. • p2p (point to point) — This represents a connection between two OSPF routers (one router has one recipient).
BFD Interval	This value determines how frequently BFD packets will be sent to BFD peers (in milliseconds).
Metric	This is the cost metric used by OSPF to determine the best path between two OSPF-enabled devices.

Table 21: Add OSPF Network Options *(Continued)*

Field	Description
Hello Interval	This interval specifies the length of time, in seconds, before the routing device sends a hello packet out an interface. By default, the routing device sends Hello packets every 10 seconds.
Dead Interval	This interval specifies the length of time, in seconds, that the routing device waits before declaring a neighboring routing device as unavailable. By default, the routing device waits 40 seconds (four times the Hello interval).
Auth Type	• None — Selecting this means you are selecting no authentication to be done. • md5 (message-digest algorithm) — This is a hashing algorithm that uses a one-way cryptographic function that acccepts a message of any length and returns it as a fixed-length output value to be used for authentication. • password — This means that a password will be required for authentication.
Export (SRX Only)	See "Routing Configuration on SRX Series Firewalls" on page 243.
Import (SRX Only)	See "Routing Configuration on SRX Series Firewalls" on page 243.

5. When you have entered in the appropriate information, click the checkbox at the top of the Add OSPF Network section.



At least one network is required

Area *

0

Type

● Default ○ Stub ○ NSSA

OSPF NETWORKS

Add OSPF Network ✓ ×

Network *

OSPFCSTOM1

□ Passive

Interface Type *

p2p

BFD Interval

1000

(50 - 60000 milliseconds)

Metric

(1 - 65535)

Hello Interval

10

(1 - 255)

Dead Interval

40

(1 - 65535)

Auth Type

○ None ● md5 ○ password

Auth Key

247

(0 - 255)

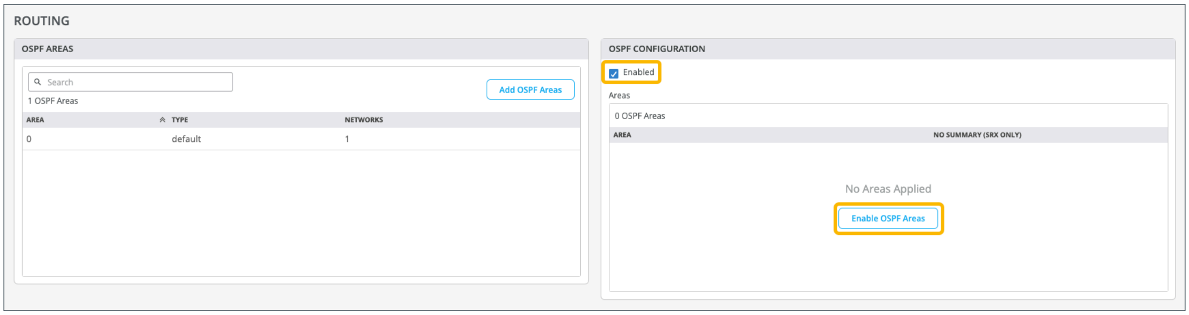
Auth Value

877241g00

(8-64 characters)

Export (SRX Only)

6. Click **Add** at the bottom of the window. You will now see your OSPF area listed in the **OSPF Areas** tile.
7. Now that you've created your OSPF area, you need to enable it. In the **OSPF CONFIGURATION** tile, check the **Enabled** checkbox. This causes the **Enable OSPF Areas** button to appear.
8. Click the **Enable OSPF Areas** button.



☑ Enabled

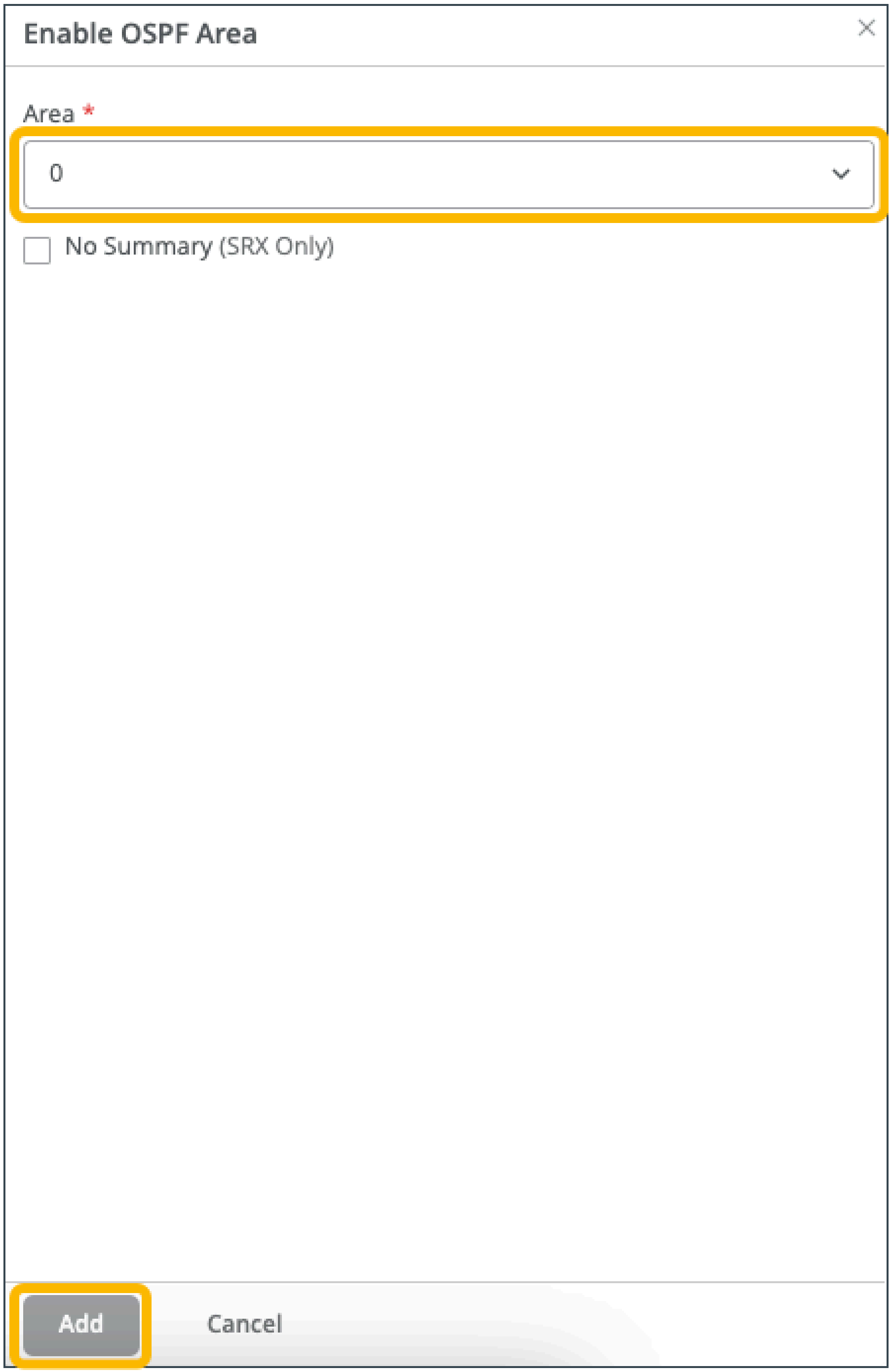
1 OSPF Areas

AREA	TYPE	NETWORKS
0	default	1

0 OSPF Areas

AREA	NO SUMMARY (SRX ONLY)

9. The **Enable OSPF Area** window appears. Select the **Area** you just created, then click **Add** at the bottom of the window.



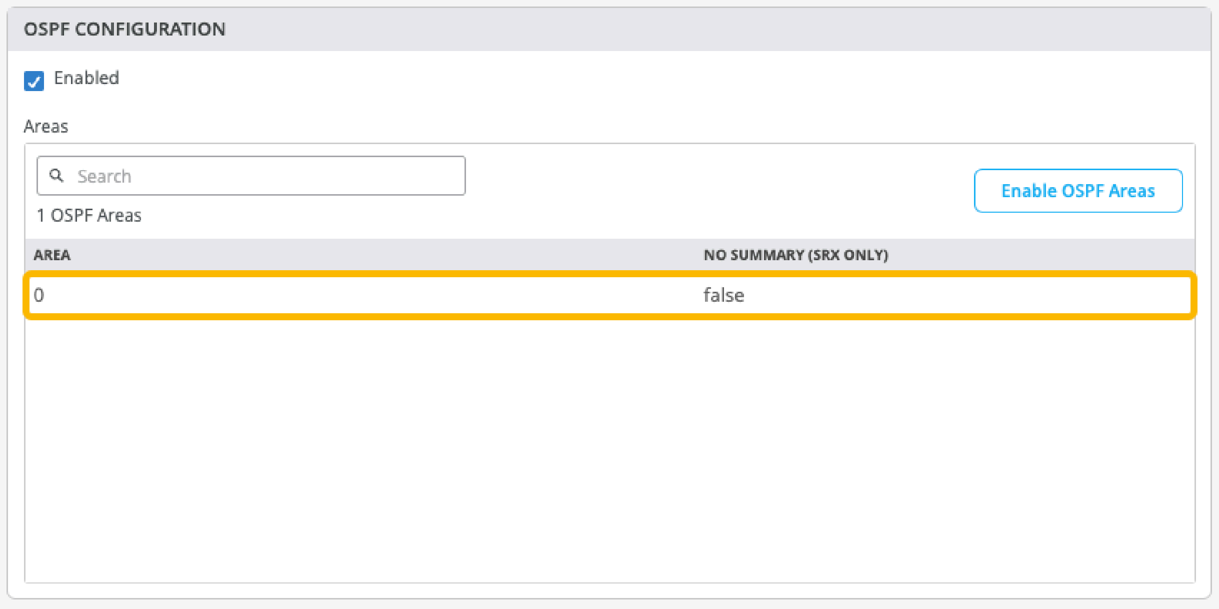
Enable OSPF Area

Area *

0

□ No Summary (SRX Only)

You will see your area listed in the **OSPF CONFIGURATION** tile.



OSPF CONFIGURATION

☑ Enabled

Areas

Search

1 OSPF Areas

AREA	NO SUMMARY (SRX ONLY)
0	false

SEE ALSO

Configuring OSPF Areas

Onboard Session Smart Routers for WAN Configuration

IN THIS SECTION

In a Juniper Mist™ network, you must onboard your Juniper® Session Smart™ Routers 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.

Before You Begin

We assume that you have your Session Smart Router 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 Session Smart Router up and running in the Mist cloud, see SSR Series Devices.

Assign Spoke Templates to Sites

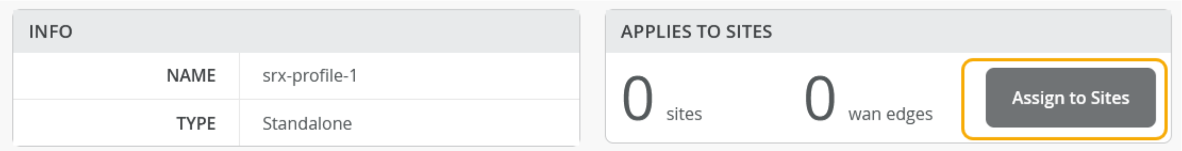
The template that you created in "Configure WAN Edge Templates" on page 92 now exists in the Juniper Mist cloud as an object that you can assign to one or more sites. WAN edge templates are a quick and easy way to group the common attributes of WAN edge spoke devices. You can apply a single template 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:

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

Figure 69: Assign Spoke Templates to Sites



INFO

NAME srx-profile-1

TYPE Standalone

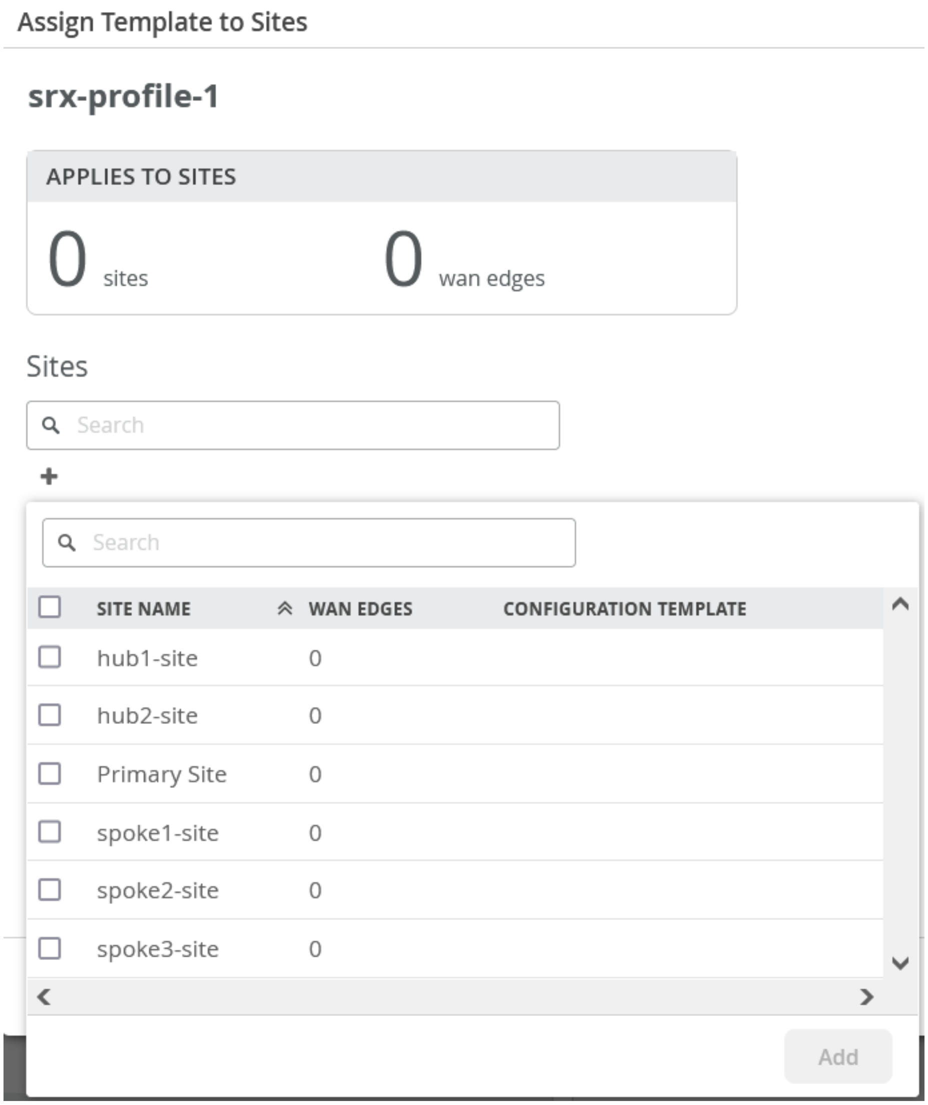
APPLIES TO SITES

0 sites

0 wan edges

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

Figure 70: Select Sites to Assign Spoke Templates



Assign Template to Sites

srx-profile-1

APPLIES TO SITES

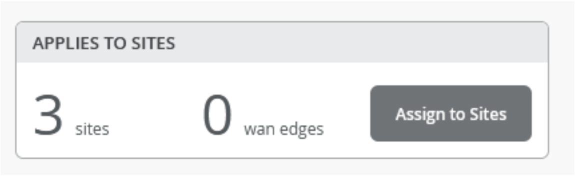
0 sites 0 wan edges

Sites

□	SITE NAME	WAN EDGES	CONFIGURATION TEMPLATE
□	hub1-site	0	
□	hub2-site	0	
□	Primary Site	0	
□	spoke1-site	0	
□	spoke2-site	0	
□	spoke3-site	0	

The WAN Edge Templates page reflects the updated status. Figure 71 on page 134 indicates that three sites are using the template.

Figure 71: WAN Edge Templates Applied to Sites



APPLIES TO SITES

3 sites 0 wan edges

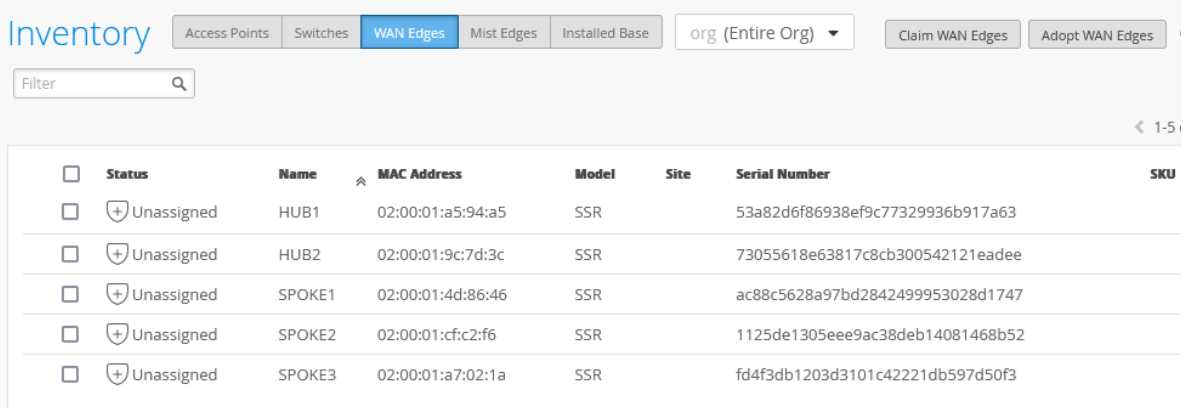
Assign a Session Smart Router to a Site

To assign your Session Smart Router to sites, the devices must be present in the Juniper Mist inventory. You can claim or adopt your Session Smart Router to onboard it in the Juniper Mist cloud. After the device is on board, the organization inventory shows the device. For details on onboarding, see Getting Started.

To assign a Session Smart Router to a site:

1. In the Juniper Mist portal. click **Organization** > **Admin** > **Inventory**.
2. Refresh your browser and check under **WAN Edges** to find out if your Session Smart Router is part of the inventory.

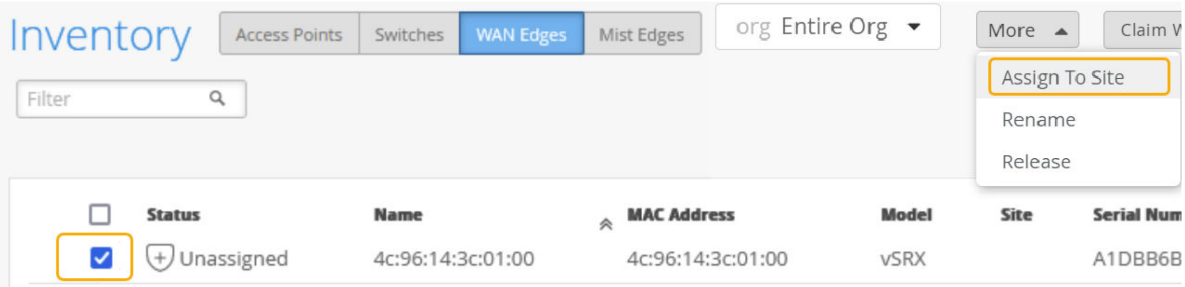
Figure 72: Session Smart Router in Inventory



☐	Status	Name	MAC Address	Model	Site	Serial Number	SKU
☐	Unassigned	HUB1	02:00:01:a5:94:a5	SSR		53a82d6f86938ef9c77329936b917a63	
☐	Unassigned	HUB2	02:00:01:9c:7d:3c	SSR		73055618e63817c8cb300542121eadee	
☐	Unassigned	SPOKE1	02:00:01:4d:86:46	SSR		ac88c5628a97bd2842499953028d1747	
☐	Unassigned	SPOKE2	02:00:01:cf:c2:f6	SSR		1125de1305eee9ac38deb14081468b52	
☐	Unassigned	SPOKE3	02:00:01:a7:02:1a	SSR		fd4f3db1203d3101c42221db597d50f3	

3. Assign Session Smart Router to an individual site using **Assign to Site** option.

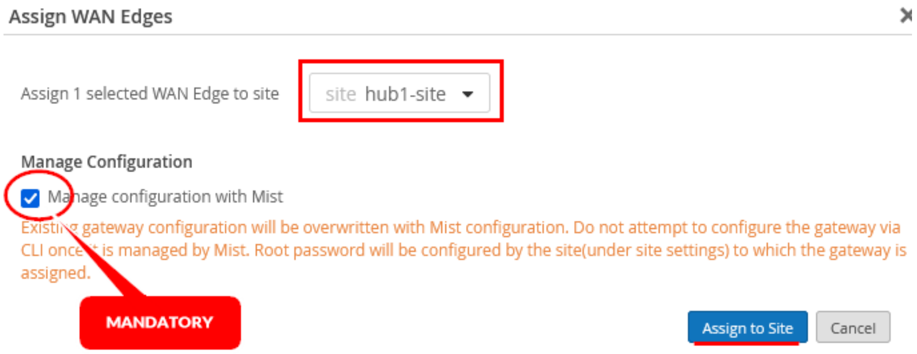
Figure 73: Assign Session Smart Router to Sites



☐	Status	Name	MAC Address	Model	Site	Serial Num
☑	Unassigned	4c:96:14:3c:01:00	4c:96:14:3c:01:00	vSRX		A1DBB6B

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

Figure 74: Selecting Sites for SSR Assignment



Assign WAN Edges

Assign 1 selected WAN Edge to site: site hub1-site

Manage Configuration

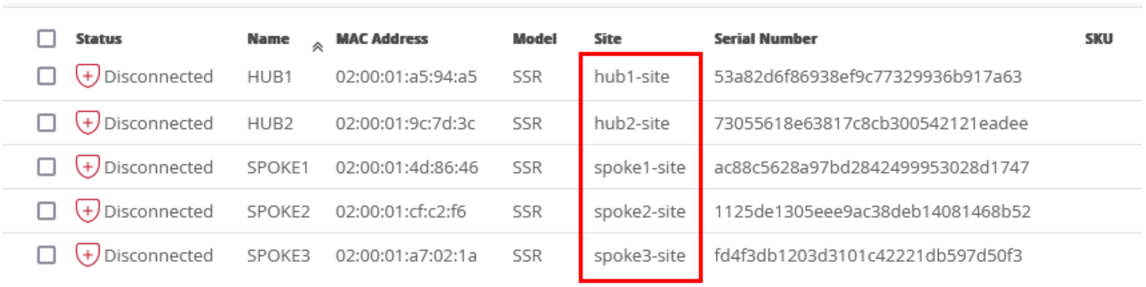
☑ Manage configuration with Mist

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 is assigned.

5. Enable the **Manage configuration with Mist** option.

   Figure 75 on page 136 shows changes in the inventory once you assign the device to the site.

Figure 75: Site Assignment Summary



□	Status	Name	MAC Address	Model	Site	Serial Number	SKU
□	Disconnected	HUB1	02:00:01:a5:94:a5	SSR	hub1-site	53a82d6f86938ef9c77329936b917a63	
□	Disconnected	HUB2	02:00:01:9c:7d:3c	SSR	hub2-site	73055618e63817c8cb300542121eadee	
□	Disconnected	SPOKE1	02:00:01:4d:86:46	SSR	spoke1-site	ac88c5628a97bd2842499953028d1747	
□	Disconnected	SPOKE2	02:00:01:cf:c2:f6	SSR	spoke2-site	1125de1305eee9ac38deb14081468b52	
□	Disconnected	SPOKE3	02:00:01:a7:02:1a	SSR	spoke3-site	fd4f3db1203d3101c42221db597d50f3	

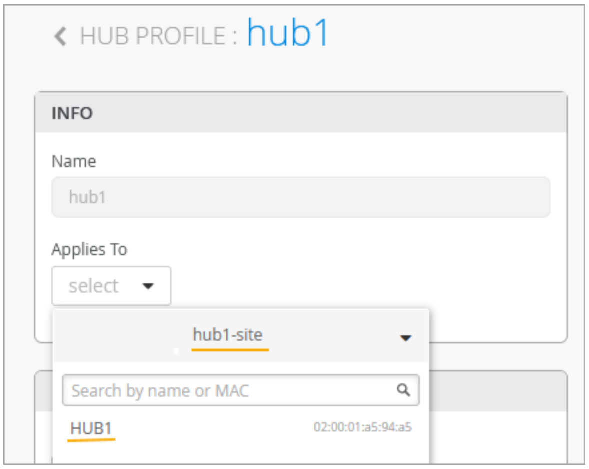
Assign a Hub Profile to the Session Smart Router

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 Session Smart Router, which is part of a hub site:

1. In the Juniper Mist portal, click **Organization** > **WAN** > **Hub Profiles**. The Hub Profile displays the list of existing profiles.
2. Click the hub profile that you want to assign to a site.
3. Under the **Applies To** option, select the site from the list of available sites.

Figure 76: Select Devices on Sites



HUB PROFILE : hub1

INFO

Name

hub1

Applies To

select

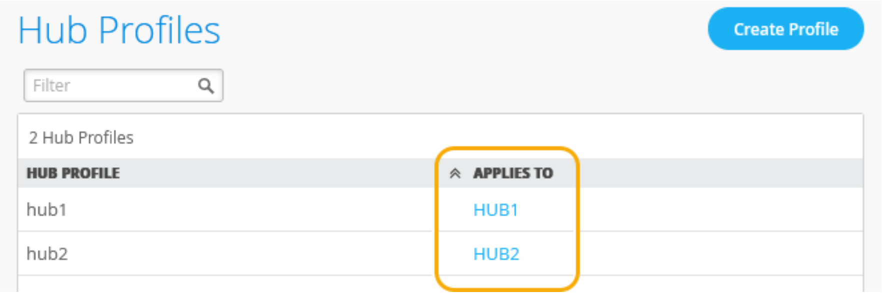
hub1-site

Search by name or MAC

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

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

Figure 77: Hub Profile Assignment Summary



Hub Profiles

2 Hub Profiles

HUB PROFILE	APPLIES TO
hub1	HUB1
hub2	HUB2

Revert Configuration Automatically for Session Smart Router

Once the Session Smart Router is adopted or claimed, it automatically receives new configurations from the Juniper Mist portal. If a new configuration is invalid, the device rejects it and returns to the last valid configuration. If valid, the configuration is applied to the router. The router then waits five minutes and checks the connection to the Mist cloud. If it loses connectivity after this period, the Mist portal rolls back to the previous configuration. This auto-rollback feature ensures the system quickly returns to a working configuration.

SEE ALSO

Configure WAN Edge Templates for Session Smart Routers | 92

Configure Hub Profile for Session Smart Routers | 66

Juniper Mist WAN Assurance Platform Considerations | 10

WAN Assurance Configuration Overview | 31

IDP-Based Threat Detection on Session Smart Routers

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 Session Smart™ Router operating as a spoke device in your Juniper Mist™ network by activating it in an application policy. IDP with an SSR device is useful for local breakout traffic.

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 details, see Intrusion Detection and Prevention Overview.

NOTE: IDP is a calculation-heavy feature. You will likely see performance degradation on entry-level SSRs such as the SSR120 if you enable IDP in your policies.

Watch the following video for IDP-based threat detection on Session Smart Routers.

Video: Deploying a Full Stack Branch with Mist AI

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 Juniper Networks recommends. Each attack type and severity has 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—Alert profiles are 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. However, when the system detects an attack, this profile actively blocks any malicious traffic or other attacks detected on the network.

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. Actions in the IDP profile are preconfigured and are not available for users to configure.

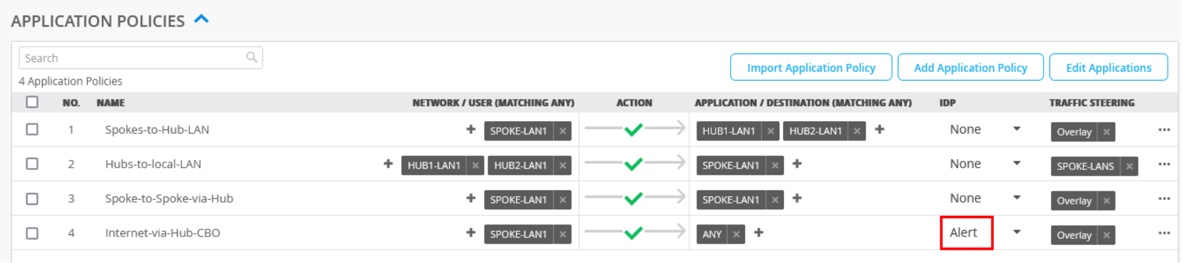
To configure IDP-based threat detection:

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 page, scroll down to the **Applications Policies** pane. The pane displays the list of existing application policies.

3. Under **IDP** column, select an IDP profile. For example, for the **Internet-via-Hub-CBO** policy, select the IDP profile **Alert**.

Figure 78: Configure an IDP Profile (Alert)



APPLICATION POLICIES

4 Application Policies

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

4. Click **Save**.

The selected IDP profile is applied on all spoke devices.

NOTE: Ensure that you set the policy action to PERMIT; otherwise, the IDP settings might override the DENY statement.

On all spoke devices, where the traffic is not steered to a local LAN or WAN interface (for LBO), you must add the IDP service on the hub device. In this example, you steer the traffic to an overlay VPN, so you must also let the remote site (the hub) know about the change.

In the following snippet, you can see the change of the forwarding path on the spoke device after activating IDP. On the LAN-interface side, there is no change, on the WAN-side, a new automatic service called: ANY-idp* and Tenant called: SPOKE-LAN1-idp* are created. Also, you can see two sessions inside the system. Other side, that is, the hub device expects a matching tenant name “SPOKE-LAN1-idp*” and no longer uses “SPOKE-LAN1” that was used earlier in application policies.

The following sample is from an Session Smart Router Programmable Command Line Interface (PCLI) accessible locally on the device.

```
show service

============================================== ====================
====================================================== =================
=========================== ======= ========== ============== ==============
Service Prefixes Transport Tenant Allowed Service-Policy State Sessions Tx Bandwidth Rx Bandwidth
============================================== ====================
====================================================== =================
=========================== ======= ========== ============== ==============
ANY 0.0.0.0/0 - SPOKE-LAN1 ANY-sp
.
.
ANY-idp* 0.0.0.0/0 - SPOKE-LAN1-idp* ANY-sp Up 0 0 bps 0 bps
.
.

show sessions

====================================== ===== =============================== =================
======================= ======================= ====== ======= ================= ==========
================= =========== =============== ========== =================== =========
=================
Session Id Dir Service Tenant Dev Name Intf Name VLAN Proto Src IP Src Port Dest IP Dest Port
NAT IP NAT Port Payload Encrypted Timeout Uptime
====================================== ===== =============================== =================
======================= ======================= ====== ======= ================= ==========
================= =========== =============== ========== =================== =========
=================
3e3bc1d9-3e6f-455b-87f8-902d459eec5e fwd ANY SPOKE-LAN1 ge-0-3 ge-0-3_1099 1099 ICMP 10.99.99.99
10 9.9.9.9 10 0.0.0.0 0 True 4 0 days 0:59:25
3e3bc1d9-3e6f-455b-87f8-902d459eec5e rev ANY SPOKE-LAN1 idp-in idp-in 0 ICMP 9.9.9.9 10
10.99.99.99 10 0.0.0.0 0 True 0 0 days 0:59:25
2d1251ac-1e3a-42b7-8d5b-83403be09677 fwd ANY-idp* SPOKE-LAN1-idp* idp-out idp-out 0 ICMP
```

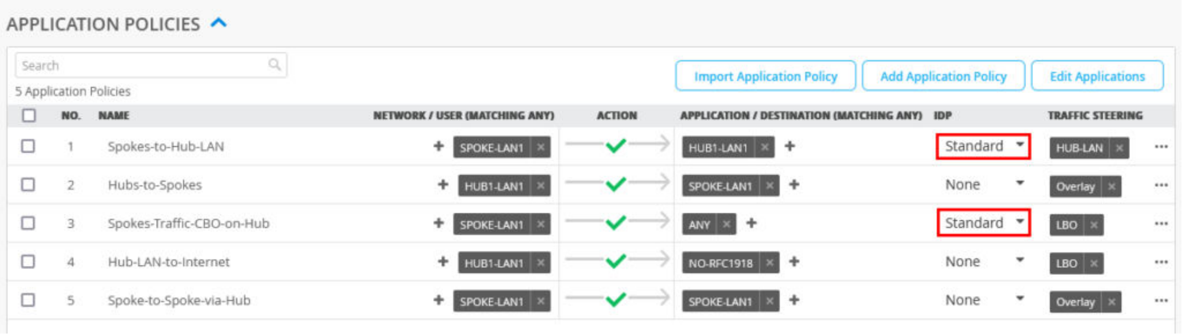
```
10.99.99.99 10 9.9.9.9 10 0.0.0.0 0 True 4 0 days 0:59:25
2d1251ac-1e3a-42b7-8d5b-83403be09677 rev ANY-idp* SPOKE-LAN1-idp* ge-0-0 ge-0-0 0 UDP
192.168.129.191 16405 192.168.173.114 16414 0.0.0.0 0 True 0 0 days 0:59:25
```

To setup a matching tenant name on the hub-device side for this example, use the following steps:

1. In Juniper Mist cloud portal, click **Organization** > **Hub Profiles** and select a profile. For example, select a profile named **hub1**.

2. Scroll down to the **Application Policies** section and set IDP profile as **Standard** for **Spokes-to-Hub-LAN** and **Spokes-Traffic-CBO-on-Hub**.

Figure 79: Setting IDP Profile on Hub Device Side



APPLICATION POLICIES

Search

5 Application Policies

□	NO.	NAME	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
□	1	Spokes-to-Hub-LAN	SPOKE-LAN1	✓	HUB1-LAN1	Standard	HUB-LAN
□	2	Hubs-to-Spokes	HUB1-LAN1	✓	SPOKE-LAN1	None	Overlay
□	3	Spokes-Traffic-CBO-on-Hub	SPOKE-LAN1	✓	ANY	Standard	LBO
□	4	Hub-LAN-to-Internet	HUB1-LAN1	✓	NO-RFC1918	None	LBO
□	5	Spoke-to-Spoke-via-Hub	SPOKE-LAN1	✓	SPOKE-LAN1	None	Overlay

3. Save the changes.

This procedure synchronizes the tenant-names on both sides enabling the communication between hub and spoke.

> **WARNING**: When you activate the IDP feature for the first time on a spoke-device, we recommend you to plan it in a maintenance window. The start of the IDP engine and inclusion into the path from LAN to WAN (that is, service-chaining) might take a few minutes and might also interrupt ongoing communications.

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 virtual machine (VM) desktop (desktop1) in a sandbox or lab environment, 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.

```
virsh console desktop1
apt-get update
apt-get install -y nikto
# Using your individual Lab-Access-IP we test if the labinternal
# Apache Tomcat Server of the Apache guacamole container is avail
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**.

Figure 80: Secure WAN Edge IDP Events

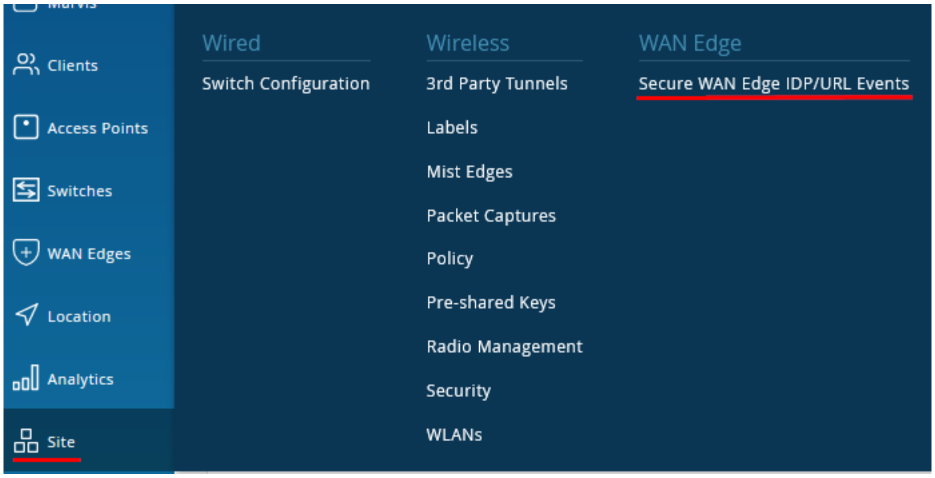
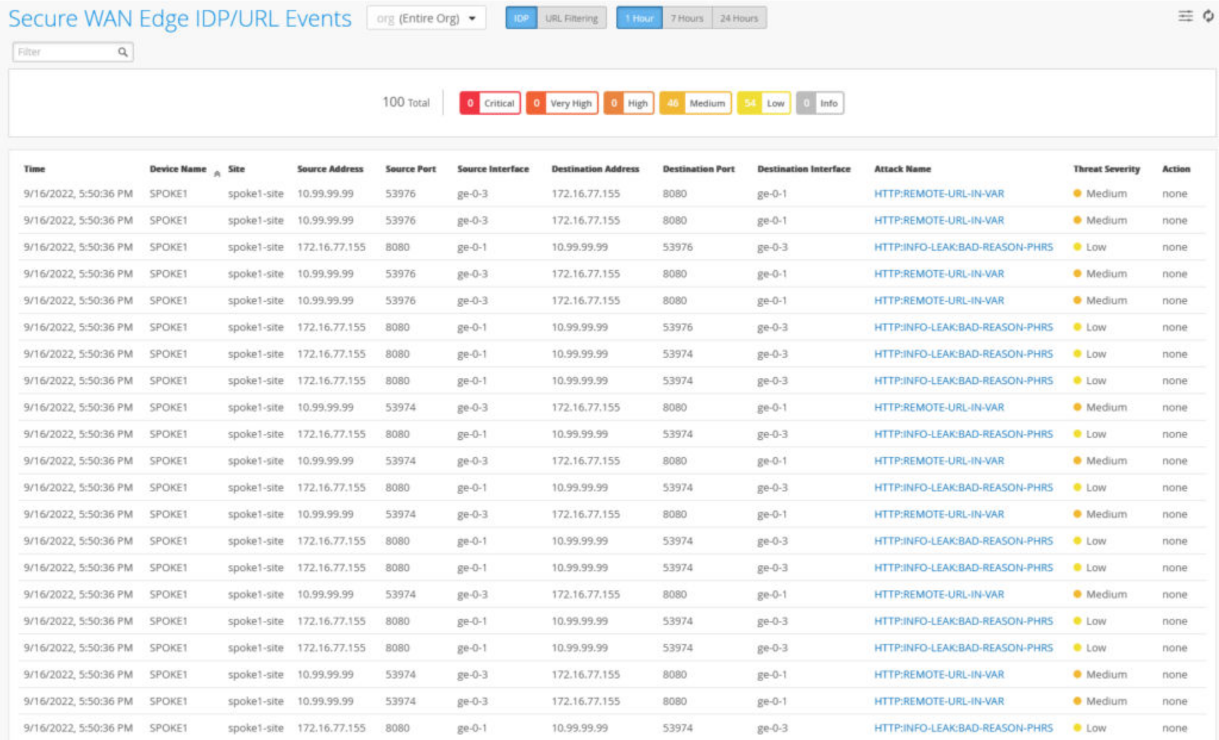


Figure 81 on page 144 shows IDP events generated for the Session Smart Router.

Figure 81: IDP Events Generated for an Alert IDP Profile



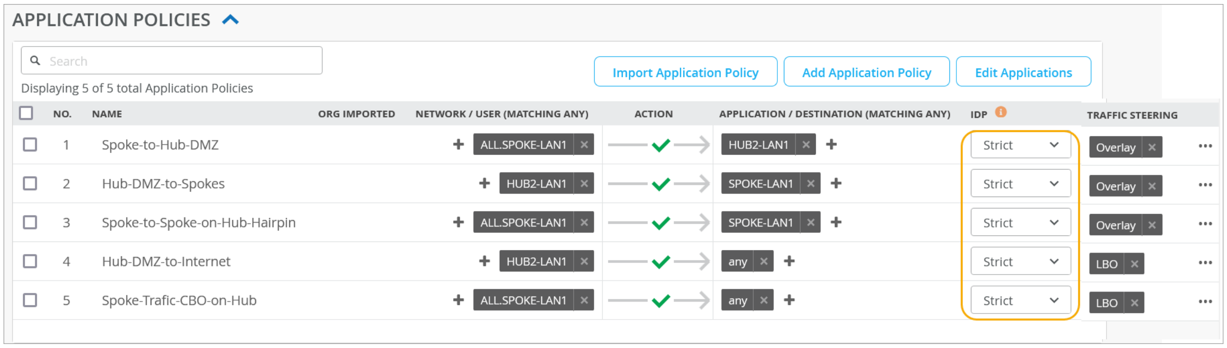
100 Total | 0 Critical | 0 Very High | 0 High | 46 Medium | 54 Low | 0 Info

Time	Device Name	Site	Source Address	Source Port	Source Interface	Destination Address	Destination Port	Destination Interface	Attack Name	Threat Severity	Action
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	10.99.99.99	53976	ge-0-3	172.16.77.155	8080	ge-0-1	HTTP:REMOTE-URL-IN-VAR	● Medium	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	10.99.99.99	53976	ge-0-3	172.16.77.155	8080	ge-0-1	HTTP:REMOTE-URL-IN-VAR	● Medium	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	172.16.77.155	8080	ge-0-1	10.99.99.99	53976	ge-0-3	HTTP:INFO-LEAK:BAD-REASON-PHRS	● Low	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	10.99.99.99	53976	ge-0-3	172.16.77.155	8080	ge-0-1	HTTP:REMOTE-URL-IN-VAR	● Medium	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	10.99.99.99	53976	ge-0-3	172.16.77.155	8080	ge-0-1	HTTP:REMOTE-URL-IN-VAR	● Medium	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	172.16.77.155	8080	ge-0-1	10.99.99.99	53976	ge-0-3	HTTP:INFO-LEAK:BAD-REASON-PHRS	● Low	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	172.16.77.155	8080	ge-0-1	10.99.99.99	53974	ge-0-3	HTTP:INFO-LEAK:BAD-REASON-PHRS	● Low	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	172.16.77.155	8080	ge-0-1	10.99.99.99	53974	ge-0-3	HTTP:INFO-LEAK:BAD-REASON-PHRS	● Low	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	10.99.99.99	53974	ge-0-3	172.16.77.155	8080	ge-0-1	HTTP:REMOTE-URL-IN-VAR	● Medium	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	172.16.77.155	8080	ge-0-1	10.99.99.99	53974	ge-0-3	HTTP:INFO-LEAK:BAD-REASON-PHRS	● Low	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	10.99.99.99	53974	ge-0-3	172.16.77.155	8080	ge-0-1	HTTP:REMOTE-URL-IN-VAR	● Medium	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	172.16.77.155	8080	ge-0-1	10.99.99.99	53974	ge-0-3	HTTP:INFO-LEAK:BAD-REASON-PHRS	● Low	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	10.99.99.99	53974	ge-0-3	172.16.77.155	8080	ge-0-1	HTTP:REMOTE-URL-IN-VAR	● Medium	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	172.16.77.155	8080	ge-0-1	10.99.99.99	53974	ge-0-3	HTTP:INFO-LEAK:BAD-REASON-PHRS	● Low	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	172.16.77.155	8080	ge-0-1	10.99.99.99	53974	ge-0-3	HTTP:INFO-LEAK:BAD-REASON-PHRS	● Low	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	10.99.99.99	53974	ge-0-3	172.16.77.155	8080	ge-0-1	HTTP:REMOTE-URL-IN-VAR	● Medium	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	172.16.77.155	8080	ge-0-1	10.99.99.99	53974	ge-0-3	HTTP:INFO-LEAK:BAD-REASON-PHRS	● Low	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	172.16.77.155	8080	ge-0-1	10.99.99.99	53974	ge-0-3	HTTP:INFO-LEAK:BAD-REASON-PHRS	● Low	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	10.99.99.99	53974	ge-0-3	172.16.77.155	8080	ge-0-1	HTTP:REMOTE-URL-IN-VAR	● Medium	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	10.99.99.99	53974	ge-0-3	172.16.77.155	8080	ge-0-1	HTTP:REMOTE-URL-IN-VAR	● Medium	none
9/16/2022, 5:50:36 PM	SPOKE1	spoke1-site	172.16.77.155	8080	ge-0-1	10.99.99.99	53974	ge-0-3	HTTP:INFO-LEAK:BAD-REASON-PHRS	● Low	none

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 sample. However, this time you change the spoke device template and change the IDP profile from **Alert** to **Strict**, as shown in Figure 82 on page 144.

Figure 82: IDP Profile Configuration (Strict Profile)



Displaying 5 of 5 total Application Policies

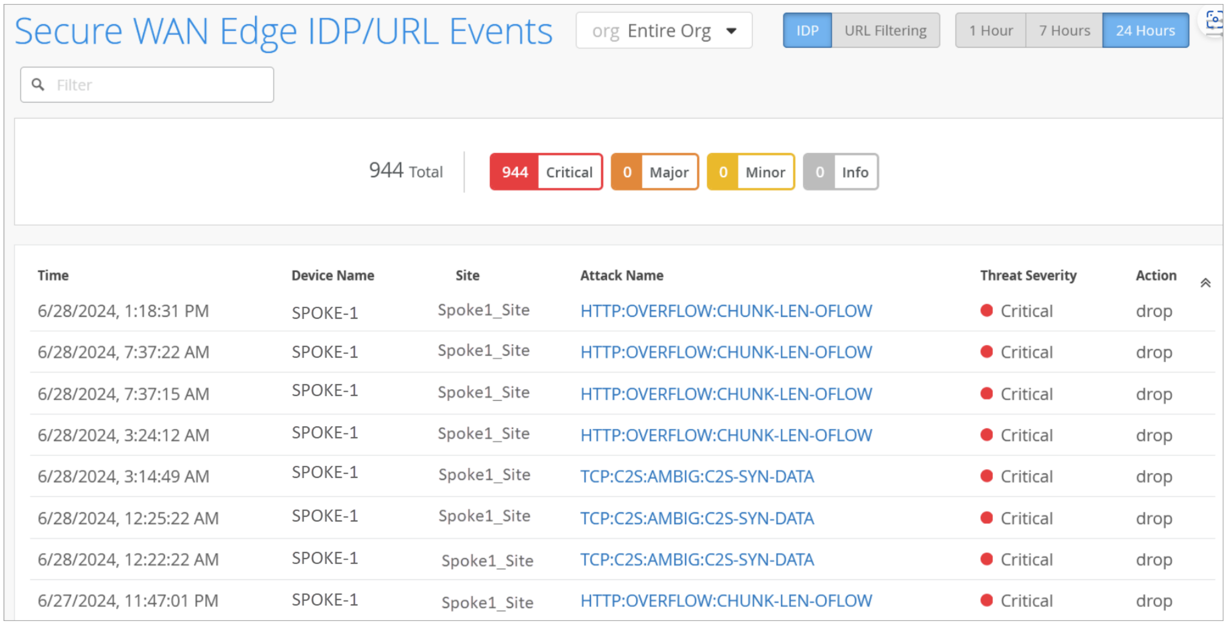
□	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
□	1	Spoke-to-Hub-DMZ		ALL.SPOKE-LAN1	✓	HUB2-LAN1	Strict	Overlay
□	2	Hub-DMZ-to-Spokes		HUB2-LAN1	✓	SPOKE-LAN1	Strict	Overlay
□	3	Spoke-to-Spoke-on-Hub-Hairpin		ALL.SPOKE-LAN1	✓	SPOKE-LAN1	Strict	Overlay
□	4	Hub-DMZ-to-Internet		HUB2-LAN1	✓	any	Strict	LBO
□	5	Spoke-Trafic-CBO-on-Hub		ALL.SPOKE-LAN1	✓	any	Strict	LBO

Run the security scanner. 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
```

Figure 83 on page 146 shows that for some events, the action is to close the session to mitigate the threats (under the **Action** field).

Figure 83: IDP Events Generated for Strict IDP Profile



944 Total | 944 Critical | 0 Major | 0 Minor | 0 Info

Time	Device Name	Site	Attack Name	Threat Severity	Action
6/28/2024, 1:18:31 PM	SPOKE-1	Spoke1_Site	HTTP:OVERFLOW:CHUNK-LEN-OFLOW	● Critical	drop
6/28/2024, 7:37:22 AM	SPOKE-1	Spoke1_Site	HTTP:OVERFLOW:CHUNK-LEN-OFLOW	● Critical	drop
6/28/2024, 7:37:15 AM	SPOKE-1	Spoke1_Site	HTTP:OVERFLOW:CHUNK-LEN-OFLOW	● Critical	drop
6/28/2024, 3:24:12 AM	SPOKE-1	Spoke1_Site	HTTP:OVERFLOW:CHUNK-LEN-OFLOW	● Critical	drop
6/28/2024, 3:14:49 AM	SPOKE-1	Spoke1_Site	TCP:C2S:AMBIG:C2S-SYN-DATA	● Critical	drop
6/28/2024, 12:25:22 AM	SPOKE-1	Spoke1_Site	TCP:C2S:AMBIG:C2S-SYN-DATA	● Critical	drop
6/28/2024, 12:22:22 AM	SPOKE-1	Spoke1_Site	TCP:C2S:AMBIG:C2S-SYN-DATA	● Critical	drop
6/27/2024, 11:47:01 PM	SPOKE-1	Spoke1_Site	HTTP:OVERFLOW:CHUNK-LEN-OFLOW	● Critical	drop

Intrusion Detection and Prevention (IDP) Bypass Profiles

The IDP Bypass works in conjunction with the intrusion prevention system (IPS) rules to prevent unnecessary alarms from being generated. You configure IDP profile when you want to exclude a specific destination, or attack type from matching an IDP rule. This prevents IDP from generating unnecessary alarms.

An IDP profile can have multiple bypass profiles, each with multiple bypass rules.

To create IDP bypass profile:

1. In the Juniper Mist cloud portal, select **Organization** > **WAN** > **Application Policy** > **IDP bypass profiles**.

   The page displays a list of IDP bypass profiles (if available)

2. Click **Add Bypass Profile** to create a profile.

3. In the Create Bypass Profile window:

   a. Add Name. Use alphanumerics, underscores, or dashes, and cannot exceed 63 characters.

   b. Select base profile. The supported base profiles are:

      - Standard

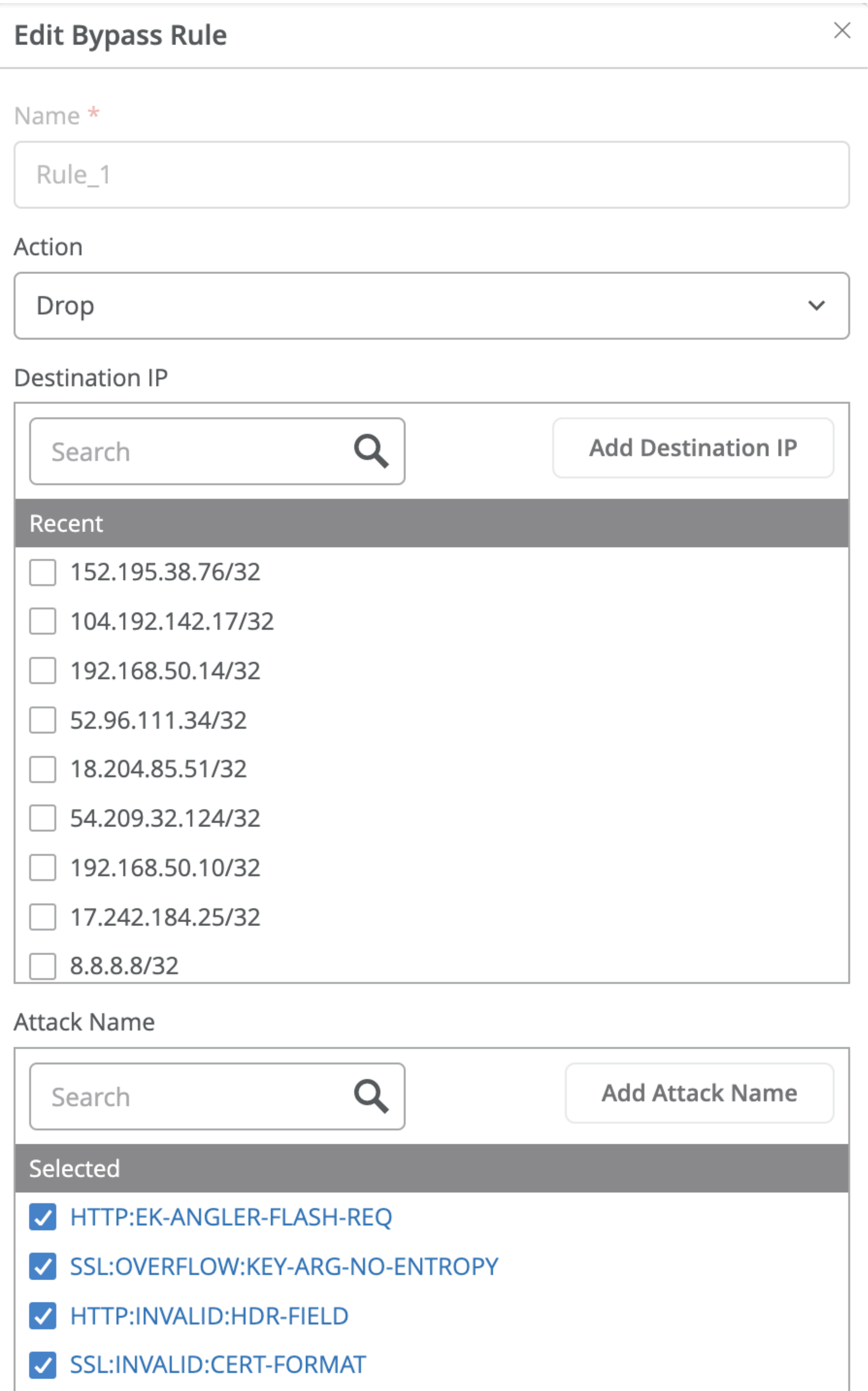
      - Strict

- Critical only– SRX

You need a base IDP profile to create an IDP bypass profile.

c. Click **Next**. The portal opens a rules page where you can define the rule for the IDP bypass profile.

Figure 84: IDP Bypass Profile Rule



Edit Bypass Rule

Name *

Rule_1

Action

Drop

Destination IP

Search

Add Destination IP

Recent

- □ 152.195.38.76/32
- □ 104.192.142.17/32
- □ 192.168.50.14/32
- □ 52.96.111.34/32
- □ 18.204.85.51/32
- □ 54.209.32.124/32
- □ 192.168.50.10/32
- □ 17.242.184.25/32
- □ 8.8.8.8/32

Attack Name

Search

Add Attack Name

Selected

- ☑ HTTP:EK-ANGLER-FLASH-REQ
- ☑ SSL:OVERFLOW:KEY-ARG-NO-ENTROPY
- ☑ HTTP:INVALID:HDR-FIELD
- ☑ SSL:INVALID:CERT-FORMAT

- Action – Select the associated traffic action. Available options are — **Alter**, **Drop**, or **Close**.

- Destination IP – IP address of the destination for traffic you want to exempt. You can select one or more destination IP address from the populated list or you can enter the destination IP address by clicking **Add Destination IP**.

- Attack Name – Select the attacks you want IDP to exempt for the specified destination addresses from the displayed list. Alternatively you can enter the attack by clicking **Add Attack Name**. The attack you enter must be of type supported by Juniper Networks IPS Signature.

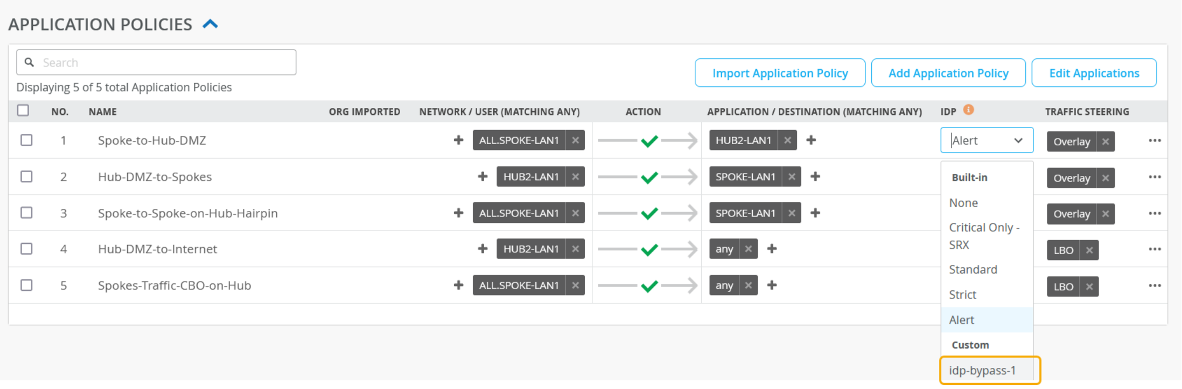
- Click **Save**.

The rule you created appears under IDP Bypass Profile pane. Next, you need to apply the IDP bypass profile in an application policy similar applying any IDP profile by using the following steps:

1. In the Juniper Mist cloud portal, click **Organization** > **WAN Edge Templates** and select a template for your spoke device.

2. Under the IDP column, select the IDP profile. For example, select the IDP bypass profile that you created in the previous step.

Figure 85: Apply IDP Bypass Profile in Application Policy



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	Alert	Overlay
☐	2	Hub-DMZ-to-Spokes		HUB2-LAN1	✓	SPOKE-LAN1		Overlay
☐	3	Spoke-to-Spoke-on-Hub-Hairpin		ALL.SPOKE-LAN1	✓	SPOKE-LAN1		Overlay
☐	4	Hub-DMZ-to-Internet		HUB2-LAN1	✓	any		LBO
☐	5	Spokes-Traffic-CBO-on-Hub		ALL.SPOKE-LAN1	✓	any		LBO

3. Click **Save** once you configure other options in application policy. See Configure Application Policies on Session Smart Routers.

You can view the generated events by navigating to **Site** > **Secure WAN Edge IDP/URL Events**.

RELATED DOCUMENTATION

Configure Application Policies on Session Smart Routers | 58

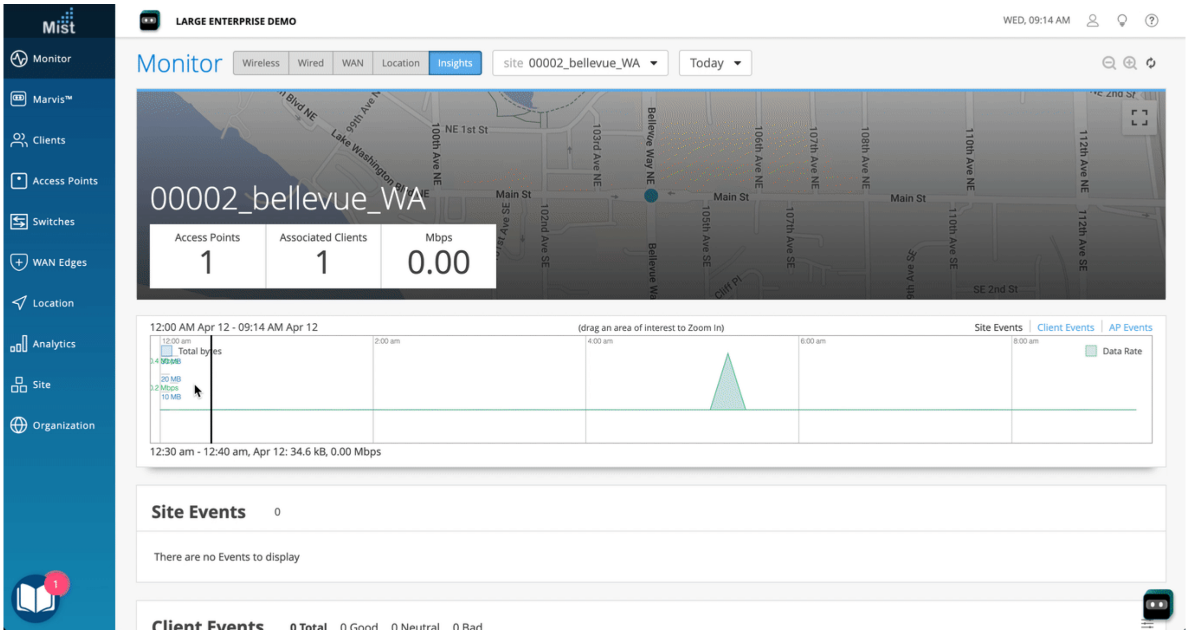
WAN Assurance Configuration Overview | 31

Upgrade a WAN Edge Session Smart Router

You can upgrade Juniper® Session Smart™ Routers deployed as a WAN edge device in the Juniper Mist™ cloud portal. Upgrading your device's operating system to a newer version can provide you with new features, enhancements, bug fixes, and compatibility improvements.

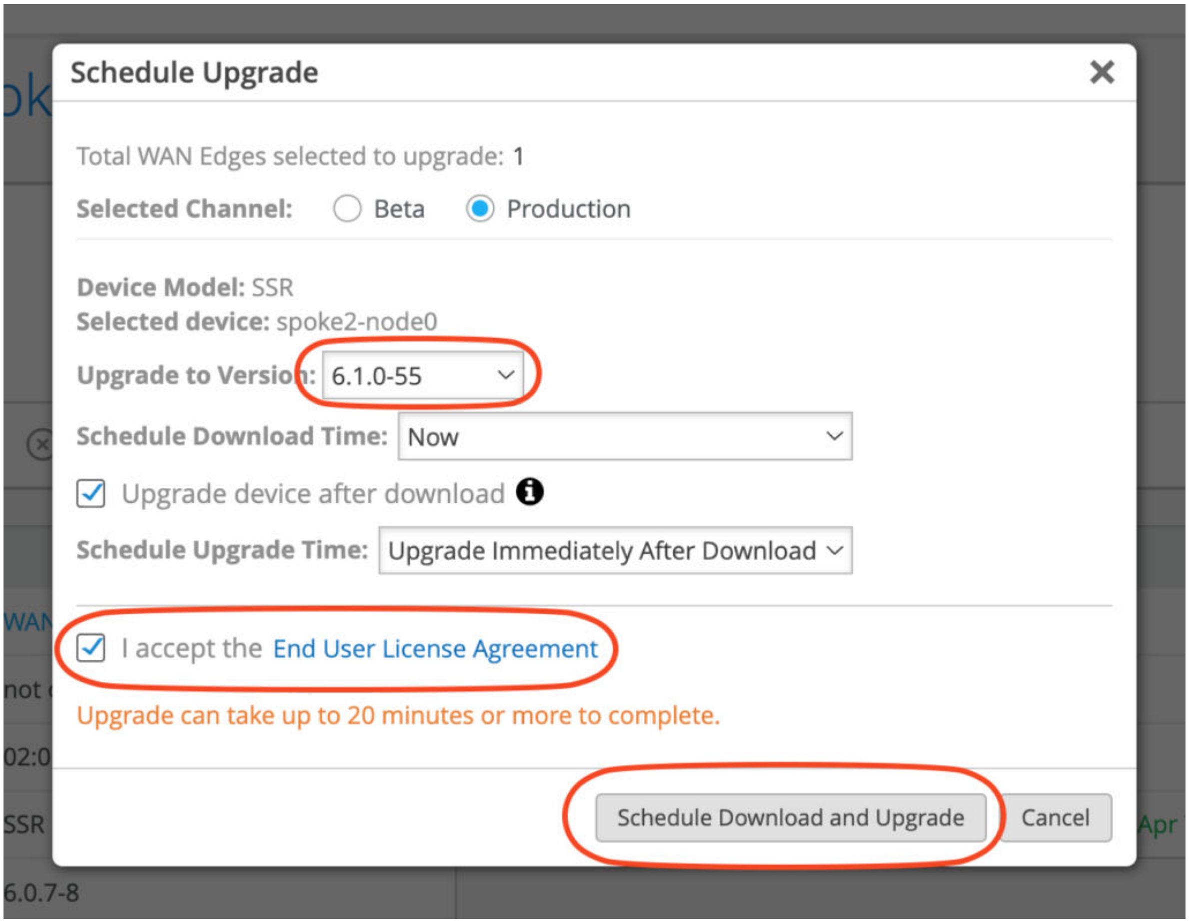
1. In the Juniper Mist cloud portal, select **WAN Edge** and select the device.
2. Click the device and select the **Upgrade Firmware** option from the utilities menu.

Figure 86: Upgrade Software



3. In the **Schedule Upgrade** screen, use the available options based on your requirements to download and upgrade the firmware for the Session Smart Routers.

Figure 87: Schedule Upgrade Option



Schedule Upgrade

Total WAN Edges selected to upgrade: 1

Selected Channel: ○ Beta ● Production

Device Model: SSR

Selected device: spoke2-node0

Upgrade to Version: 6.1.0-55

Schedule Download Time: Now

☑ Upgrade device after download

Schedule Upgrade Time: Upgrade Immediately After Download

☑ I accept the End User License Agreement

Upgrade can take up to 20 minutes or more to complete.

4. For **Selected Channel**, select **Production**. If you are testing new firmware builds in a non-production lab environment, you can select the **Beta** channel.
5. In the **Upgrade to Version** list, select the required version to upgrade. The list of available versions might vary based on the selected channel.
6. For the **Schedule Download Time** option, the portal displays **Now** by default. The download of the selected version starts when you submit the upgrade.

   If you want to schedule the download at your preferred date and time (ex: off-peak hours for the site), change the **Schedule Download Time** to **Later**. Then use the time picker to select a time for the download operation.
7. The **Upgrade device after download** option indicates that you can perform the upgrade immediately after download.

   If you want to perform the upgrade at a later time:

   a. Uncheck the **Upgrade device after download** option.

   b. Set the **Schedule Upgrade Time** setting to **Later**.

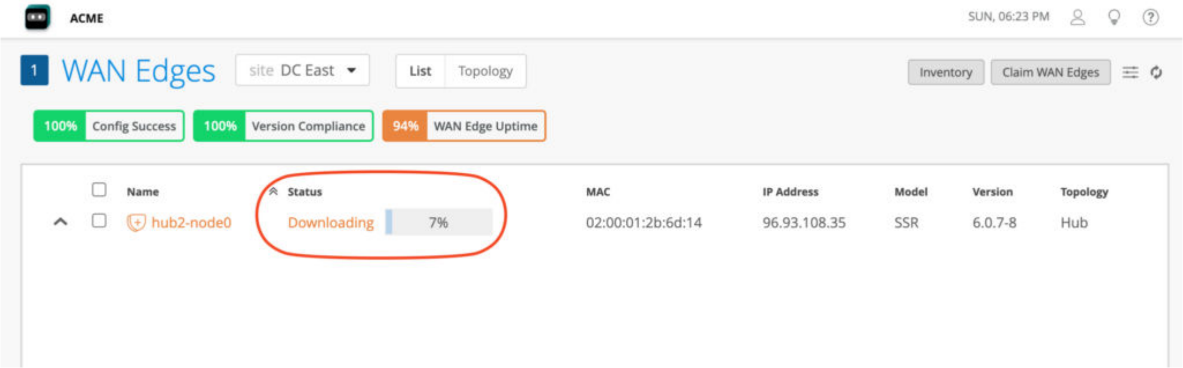
c. Use the time picker option to select a time for the upgrade operation.

d. Read and accept the **End User License Agreement** to continue.

e. Select the **Schedule Download and Upgrade** option. Mist cloud portal saves your scheduled download and upgrade operation.

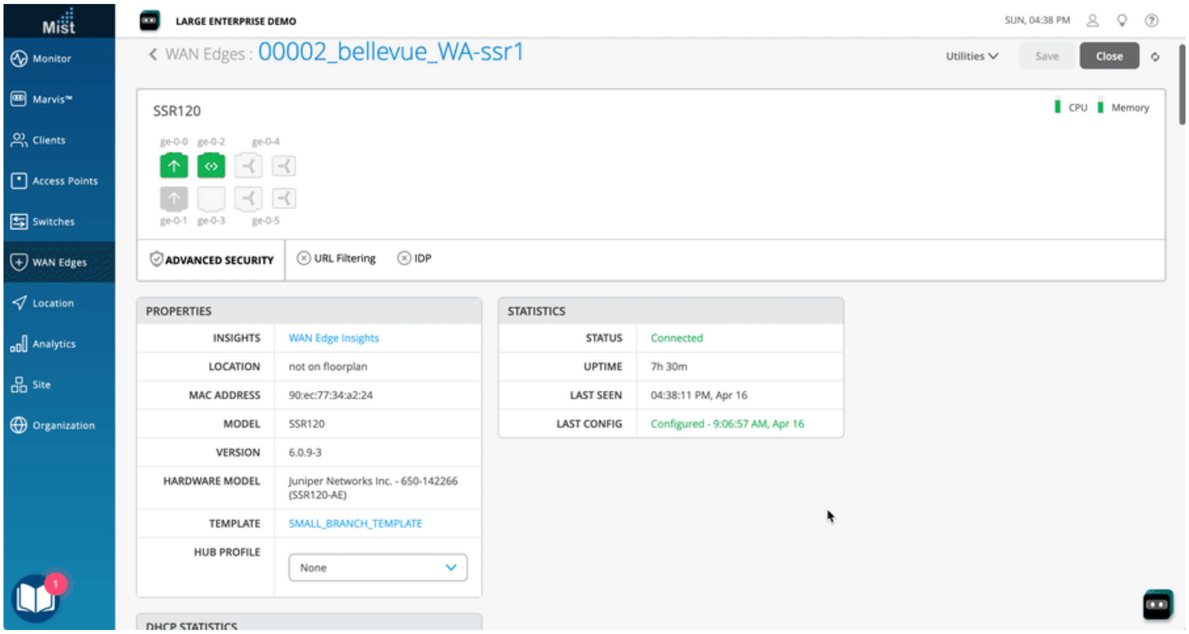
8. Select **Monitor** > **Insights** > **WAN Edge** to monitor the upgrade progress and get details on the events.

Figure 88: Monitor Progress of Firmware Download and Upgrade



	Name	Status	MAC	IP Address	Model	Version	Topology
□	hub2-node0	Downloading 7%	02:00:01:2b:6d:14	96.93.108.35	SSR	6.0.7-8	Hub

Figure 89: WAN Edge Insights



PROPERTIES	
INSIGHTS	WAN Edge Insights
LOCATION	not on floorplan
MAC ADDRESS	90:ec:77:34:a2:24
MODEL	SSR120
VERSION	6.0.9-3
HARDWARE MODEL	Juniper Networks Inc. - 650-142266 (SSR120-AE)
TEMPLATE	SMALL_BRANCH_TEMPLATE
HUB PROFILE	None

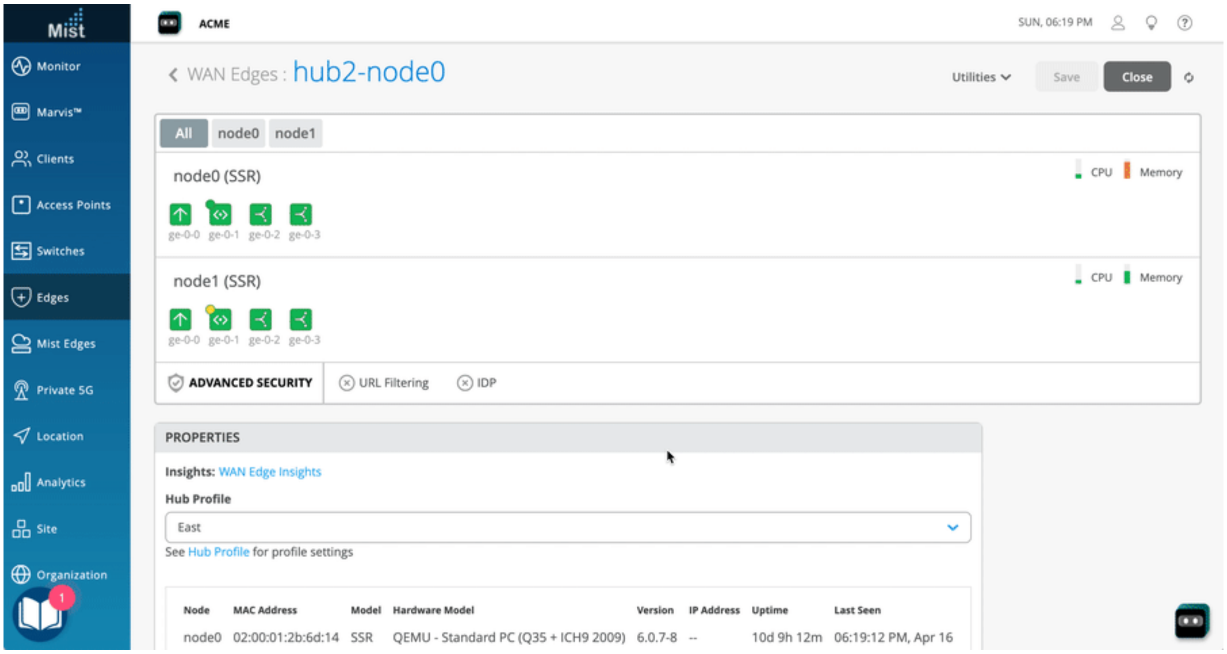
STATISTICS	
STATUS	Connected
UPTIME	7h 30m
LAST SEEN	04:38:11 PM, Apr 16
LAST CONFIG	Configured - 9:06:57 AM, Apr 16

You can see the following stages of firmware upgrade:

- Initiation of the upgrade operation
- Completion of firmware download
- Device reboot to complete the upgrade process
- Completion of firmware upgrade

High Availability Considerations: For WAN edge devices in a High Availability (HA) cluster, you can minimize the downtime by upgrading one node at a time.

Figure 90: Firmware Upgrade for WAN Edge Devices in High Availability



Insights: WAN Edge Insights

Hub Profile: East

See Hub Profile for profile settings

Node	MAC Address	Model	Hardware Model	Version	IP Address	Uptime	Last Seen
node0	02:00:01:2b:6d:14	SSR	QEMU - Standard PC (Q35 + ICH9 2009)	6.0.7-8	--	10d 9h 12m	06:19:12 PM, Apr 16

RELATED DOCUMENTATION

Introduction to Juniper Mist WAN Assurance | 2

Juniper Mist WAN Assurance Platform Considerations | 10

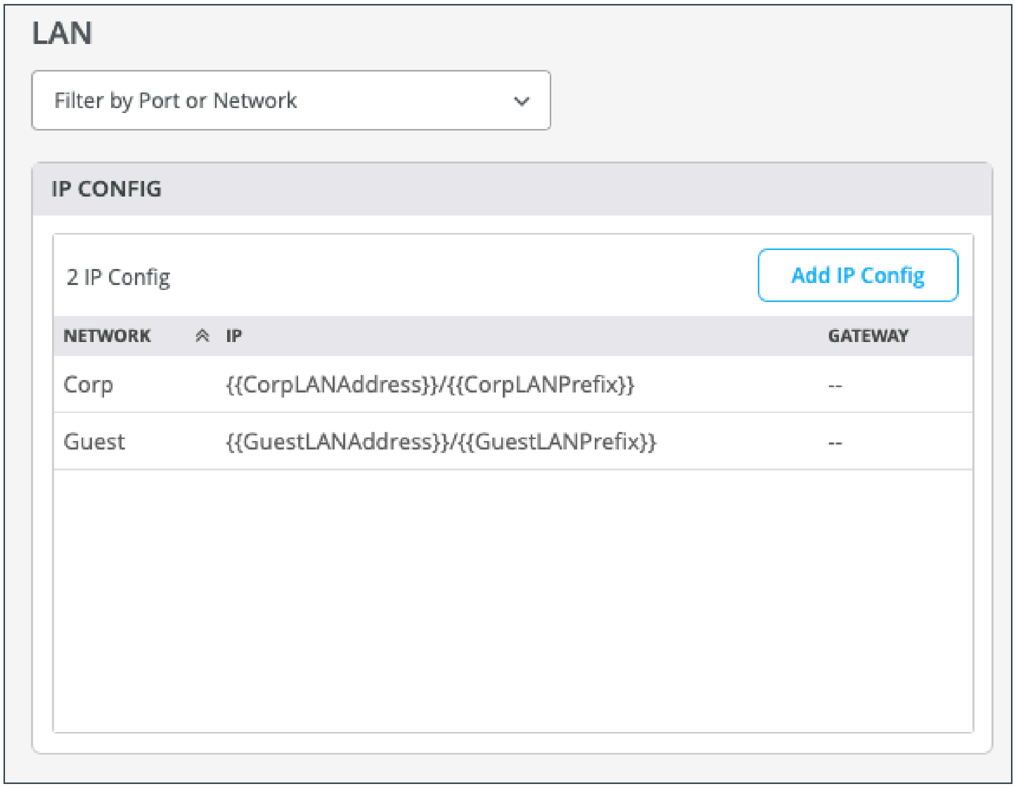
Configure VRF Route Leaking for Session Smart Routers

IN THIS SECTION

Virtual Routing and Forwarding (VRF) instances enable you to configure multiple routing instances for a single router. For a Session Smart Router deployed as a WAN Edge, you can configure VRF Route Leaking (propagation), which is the intentional sharing of route information across VRF instances. You may want to use VRF Route Leaking so that traffic can be shared or balanced across VRF instances, or maybe you want to share a default route to the internet that can be adopted by each VRF.

Configure VRF Route Leaking on the Session Smart Router

1. From the left menu of the Juniper Mist portal, select **Organization** > **WAN Edge Templates** and select the WAN Edge Template for the Session Smart Router hub device.
2. Configure your LAN segments if you have not already done so.



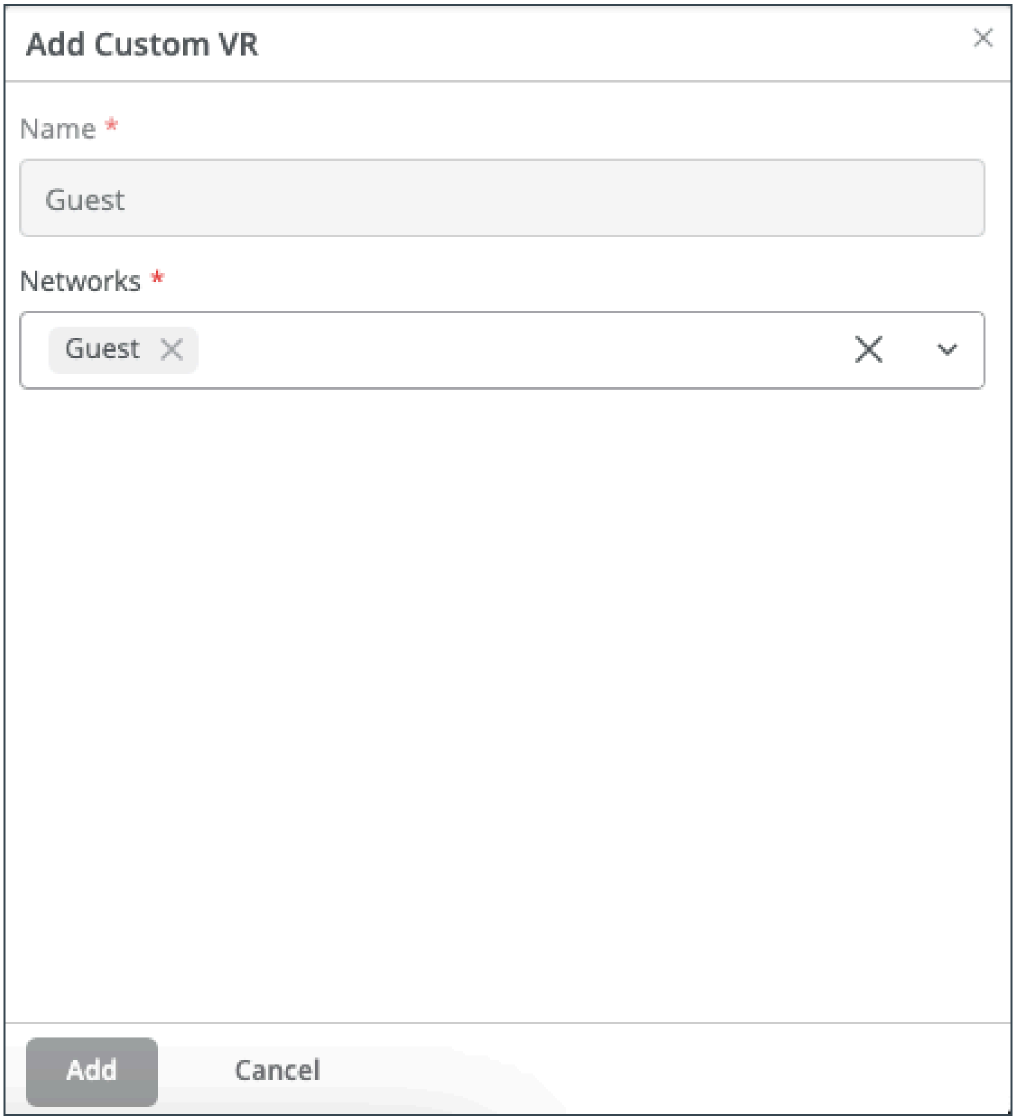
LAN

IP CONFIG

2 IP Config

NETWORK	IP	GATEWAY
Corp	{{CorpLANAddress}}/{{CorpLANPrefix}}	--
Guest	{{GuestLANAddress}}/{{GuestLANPrefix}}	--

3. From the **Custom VR** tile, select the **Add Custom VR** (virtual router) button.
4. Give your VR a **Name**, then, in the **Networks** field, select the appropriate LAN segment.



Add Custom VR

Name *

Guest

Networks *

Guest

5. Click **Add** at the bottom of the window.
6. Continue adding Custom VRs for any other LAN segments you wish to propogate routes to.
7. Repeat the above steps on the Spoke side.

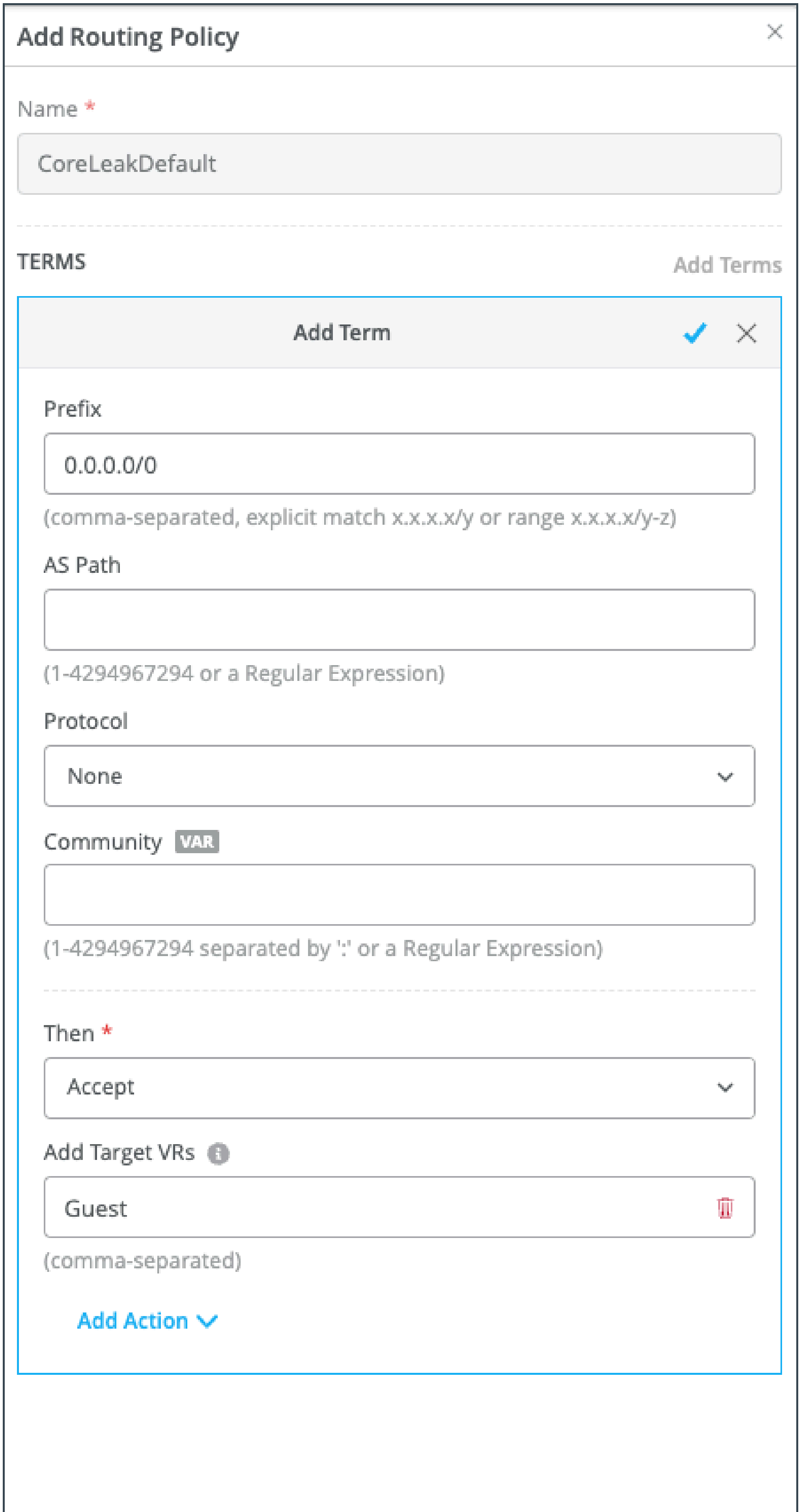
   Note that the above steps are all it takes to configure VRF route propagation across VRF instances.

Configure a Routing Policy to Propagate Routes from the Default Instance

If you want to propagate routes from the default instance to other instances, you must create a Routing Policy and then set that policy as the import policy on the BGP peer. Typically, this policy is associated with a hub (in a hub-to-spoke use case).

1. Navigate to the **ROUTING POLICIES** tile.
2. Select **Add Routing Policy**.
3. In the **Routing Policy** window, enter the appropriate information for route redistribution.
   - **Name** — Enter the name of the policy.
   - Select **Add Terms** from the righthand side of the window and enter the policy conditions.
     - **Prefix** — This is the route that you want to propagate to other instances from the default instance. For example, 0.0.0.0/0 will redistribute the default route only, while 0.0.0.0/0-32 will redistribute all routes.
     - **Protocol** — select **None**.

       Then — Select **Accept**. This is the action to apply when the condition is fulfilled.
     - **Add Action** — Select **Add Target VRs** to enable route propagation based on the target VR. Select the Custom VR you created earlier, or select multiple target VRs separated by a comma.



Add Routing Policy

Name *

CoreLeakDefault

TERMS

Add Term ✓ ×

Prefix

0.0.0.0/0

(comma-separated, explicit match x.x.x.x/y or range x.x.x.x/y-z)

AS Path

(1-4294967294 or a Regular Expression)

Protocol

None

Community VAR

(1-4294967294 separated by ':' or a Regular Expression)

Then *

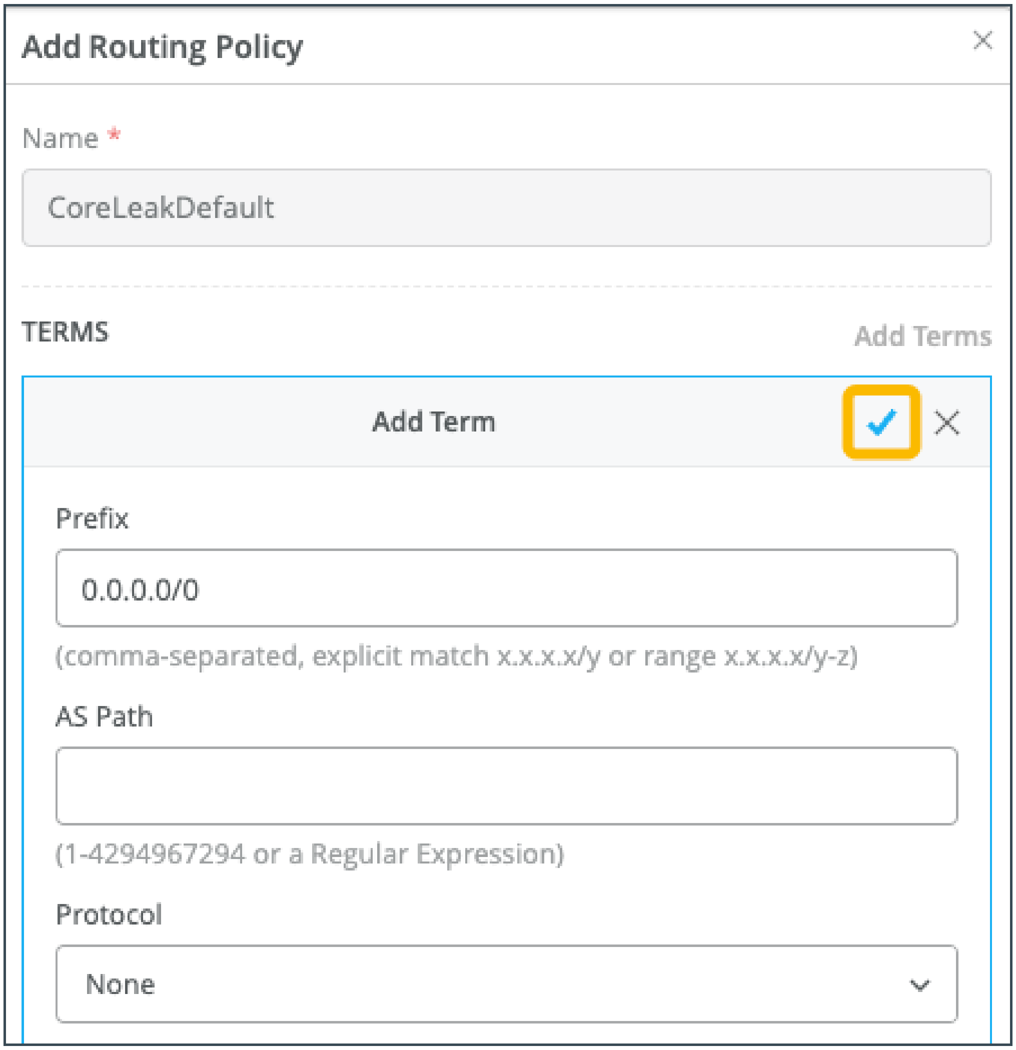
Accept

Add Target VRs

Guest

(comma-separated)

- Select the **checkbox** at the top righthand corner of the **Add Terms** section of the window.



Add Routing Policy

Name *

CoreLeakDefault

TERMS

Add Terms

Add Term ✓ ×

Prefix

0.0.0.0/0

(comma-separated, explicit match x.x.x.x/y or range x.x.x.x/y-z)

AS Path

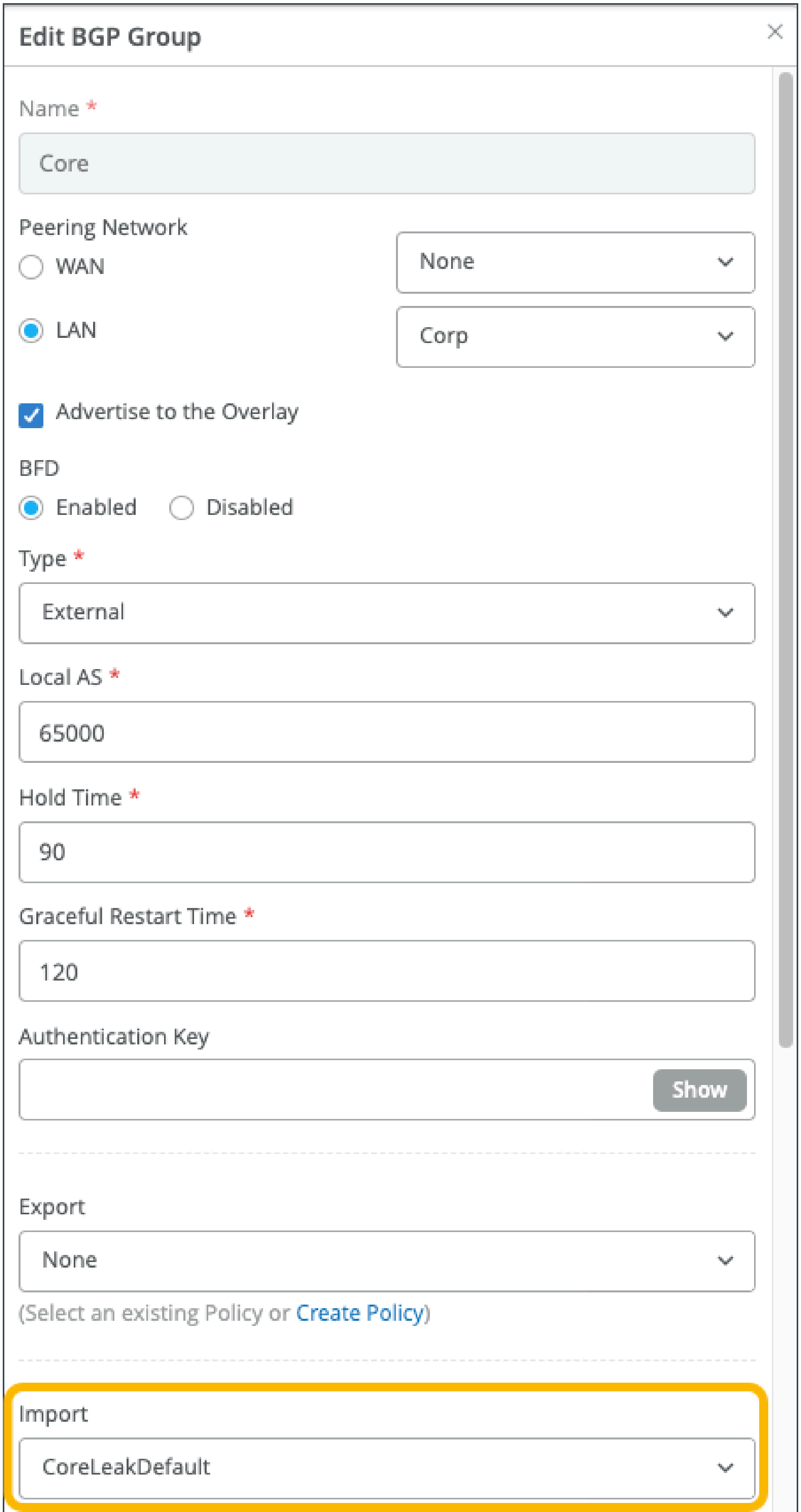
(1-4294967294 or a Regular Expression)

Protocol

None

- Click **Add** at the bottom of the window to save the routing policy.

4. Navigate to the **BGP** tile and select the BGP neighbor (peer) that you want to assign the routing policy you just created to.
5. In the **Edit BGP Group** window, scroll down for the **Import** field, then select the routing policy you just created. This assigns the import policy to the BGP peer. When routes are received from the peer, they will be leaked to the target VRFs defined in the policy.
6. Click **Save**.



Edit BGP Group

Name *

Core

Peering Network

○ WAN None

● LAN Corp

☑ Advertise to the Overlay

BFD

● Enabled ○ Disabled

Type *

External

Local AS *

65000

Hold Time *

90

Graceful Restart Time *

120

Authentication Key

Export

None

(Select an existing Policy or Create Policy)

Import

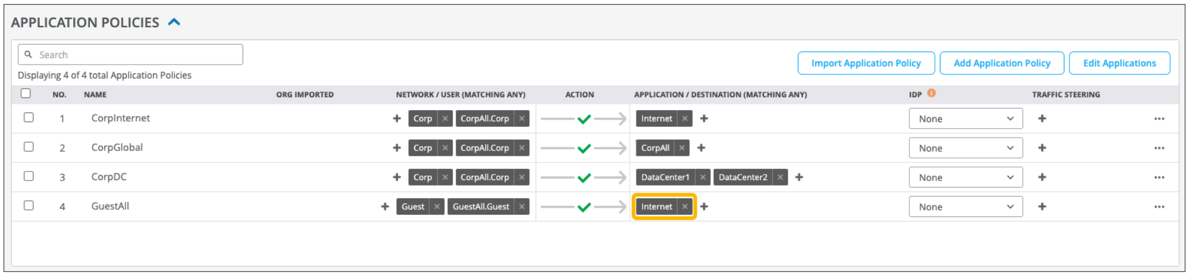
CoreLeakDefault

At this point, the routes will be propagated so that all other sites in the VRFs learn them. Note that the export policy can be configured here in the BGP Group configuration or can be configured separately.

Configure an Application Policy to Steer Traffic

In order to steer traffic from the VRF tenant toward the selected gateway (to create the forwarding plane), you must create an Application Policy. This policy allows the traffic to flow from the VRF toward the next hop of the leaked route.

1. Navigate to the **WAN Edge Template** of the hub device.
2. From the **APPLICATION POLICIES** tile, select **Add Application Policy**.
3. In the **Application/Destination** field, add the destination application matching the **prefix** you entered in the **routing policy** previously. For example, if the default route was leaked to the VRF, then the application assigned should include the 0.0.0.0/0 prefix for steering.



APPLICATION POLICIES

Search

Displaying 4 of 4 total Application Policies

□	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
□	1	CorpInternet		Corp, CorpAll.Corp	✓	Internet	None	
□	2	CorpGlobal		Corp, CorpAll.Corp	✓	CorpAll	None	
□	3	CorpDC		Corp, CorpAll.Corp	✓	DataCenter1, DataCenter2	None	
□	4	GuestAll		Guest, GuestAll.Guest	✓	Internet	None	

NOTE: The spoke may also need an application policy configured to allow traffic to flow toward the leaked targets.

For more information on how to configure application policies for the Session Smart Router, see "Configure Application Policies on Session Smart Routers" on page 58.

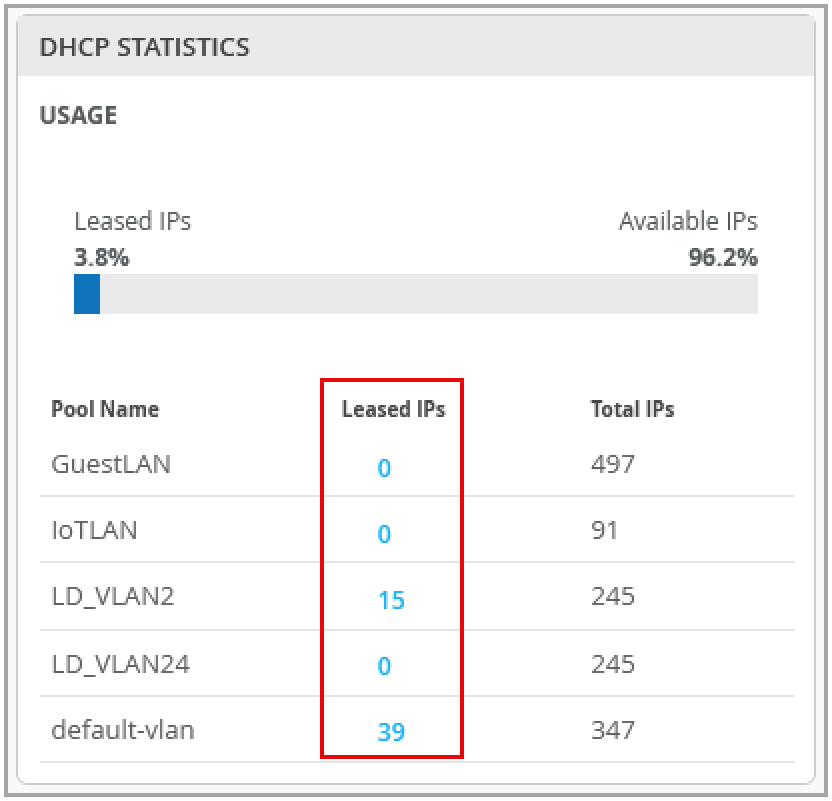
Revoke DHCP Lease on a WAN Edge Device

A DHCP server is assigned to a given network (for example, Guest_LAN). And then when a user device comes online in that specific network and requests a lease, the server in that network provides the device with a DHCP lease. And that lease is associated with the network.

You can view and revoke the DHCP lease on a WAN Edge device from the WAN Edge details page. The revoke option lets you release client devices from their current DHCP lease.

To view and revoke the DHCP lease information:

1. Click **WAN Edges** > *WAN Edges Name* to navigate to a WAN Edge details page.
2. In the DHCP Statistics section on the WAN Edge details page, click the hyperlinked value in the Leased IPs column to navigate to the Leased IPs window.



DHCP STATISTICS

USAGE

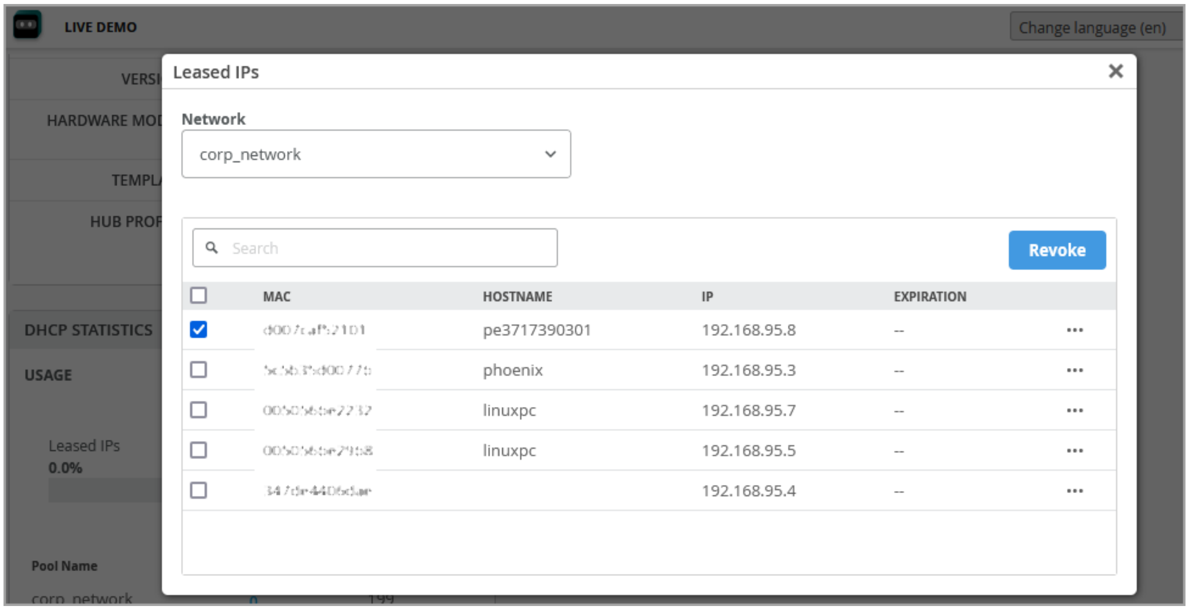
Leased IPs
3.8%

Available IPs
96.2%

Pool Name	Leased IPs	Total IPs
GuestLAN	0	497
IoTLAN	0	91
LD_VLAN2	15	245
LD_VLAN24	0	245
default-vlan	39	347

On the Leased IPs window, you can view the client devices (MAC Addresses or hostnames) along with the leased IP addresses and the lease expiry dates.

3. To revoke the DHCP lease, select a DHCP lease record from the Leased IP window and click **Revoke**.



Network: corp_network

☐	MAC	HOSTNAME	IP	EXPIRATION	
☑	[illegible]	pe3717390301	192.168.95.8	--	•••
☐	[illegible]	phoenix	192.168.95.3	--	•••
☐	[illegible]	linuxpc	192.168.95.7	--	•••
☐	[illegible]	linuxpc	192.168.95.5	--	•••
☐	[illegible]		192.168.95.4	--	•••

Reserve DHCP IP Address

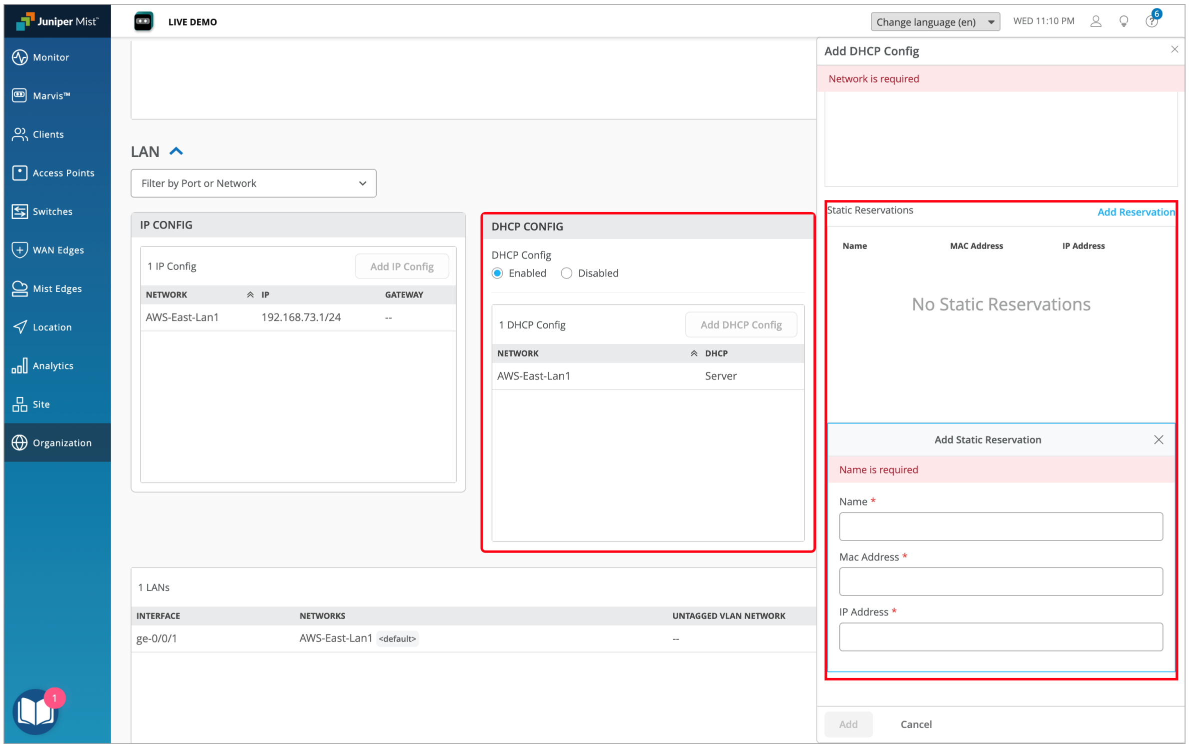
For a WAN Edge LAN interface, you can statically reserve a DHCP address provided that the interface has a DHCP server configured. Static DHCP IP address reservation involves binding a client MAC address to a static IP address from the DHCP address pool.

To reserve a DHCP IP address:

1. To create static DHCP address reservation at the device level, click **WAN Edges** > *WAN Edge Name*.

   If you want to create static DHCP address reservation at the template level, click **Organization** > **WAN Edge Templates** to open the WAN Edge template.
2. Navigate to the **LAN** configuration section.
3. In the DHCP Config box, click a configuration item to open the Edit DHCP Config page.

   Or, if you are creating a new DHCP configuration, click **Add DHCP Config** to open the Add DHCP Config page.



1 IP Config

NETWORK	IP	GATEWAY
AWS-East-Lan1	192.168.73.1/24	--

DHCP Config
● Enabled

1 DHCP Config

NETWORK	DHCP
AWS-East-Lan1	Server

1 LANs

INTERFACE	NETWORKS	UNTAGGED VLAN NETWORK
ge-0/0/1	AWS-East-Lan1 <default>	--

Network is required

Static Reservations

Name	MAC Address	IP Address

No Static Reservations

Name is required

Name *

Mac Address *

IP Address *

4. Navigate to the Static Reservation section and then click **Add Reservation**.
5. Specify a configuration Name, MAC Address, and an IP Address.
6. Click **Add** and then save the configuration.

4
CHAPTER

WAN Configuration for SRX Series Firewalls

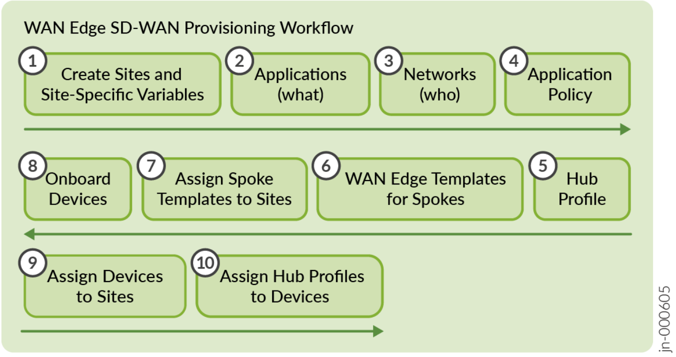
WAN Assurance Configuration Overview

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. We also assume that the physical connections (cabling) needed to support the configuration are in place. Finally, we assume that you know the interfaces and VLANs are valid for your sandbox.

Figure 91 on page 166 illustrates the workflow for configuring WAN using the Juniper Mist cloud portal.

Figure 91: 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
5 Hub Profile
6 WAN Edge Templates for Spokes
7 Assign Spoke Templates to Sites
8 Onboard Devices
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. See "Create Sites" on page 168.

2. Set Up Networks—Define the Networks. Networks are the source of traffic defined through IP prefixes. See "Setup Networks" on page 182.

3. Configure Applications—Applications are destinations that you define using IP prefixes. Applications represent traffic destinations. See "Configure Applications" on page 174

4. Create Application Policies— Application policies determine which networks or users can access which applications, and according to which traffic steering policy. See "Configure Application Policies" on page 191.

5. Create Hub Profiles—You assign hub profile to standalone or clustered devices to automate overlay path creation. See "Configure Hub Profiles" on page 197.

6. Create WAN Edge Templates—WAN edge templates automatically configure repetitive information such as an IP address, gateway, or VLAN when applied to sites. See "Configure WAN Edge Templates for SRX Series Firewalls" on page 217.

7. Onboard Devices—Onboard your devices by assigning them to a site. 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. See "Onboarding Devices" on page 259.

You can perform the following tasks on your devices to provide additional security measures:

- Set Up Secure Edge Connectors—Perform traffic inspection by Secure Edge for the WAN edge devices managed by Juniper Mist Cloud portal. See Configure Secure Edge Connectors

  .

- Configure IDP-Based Threat Detection—Monitor the events occurring on your network and proactively stop attacks and prevent future attacks. See "Configure IDP-Based Threat Detection" on page 266.

- Enable Application Visibility —Get visibility and control over the applications traversing your networks so that you can make informed decisions about permitting, denying, or redirecting traffic. See "Enable Application Visibility" on page 276.

- View Service Status —Monitor the status of services such as intrusion detection and prevention (IDP), URL filtering, and application visibility on your device. See "View Service Status" on page 285.

Upgrade software on your device to take advantage of new enhancements.

- Upgrade Software—Upgrade the software on your device through the Juniper Mist portal in a few simple steps. See "Upgrading WAN Edge SRX Series Firewall" on page 294.

Watch the following video to get an overview of WAN Assurance configuration:

Video: WAN Assurance

RELATED DOCUMENTATION

Introduction to Juniper Mist WAN Assurance | 2

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. Users with required privileges can configure and modify sites. 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:

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

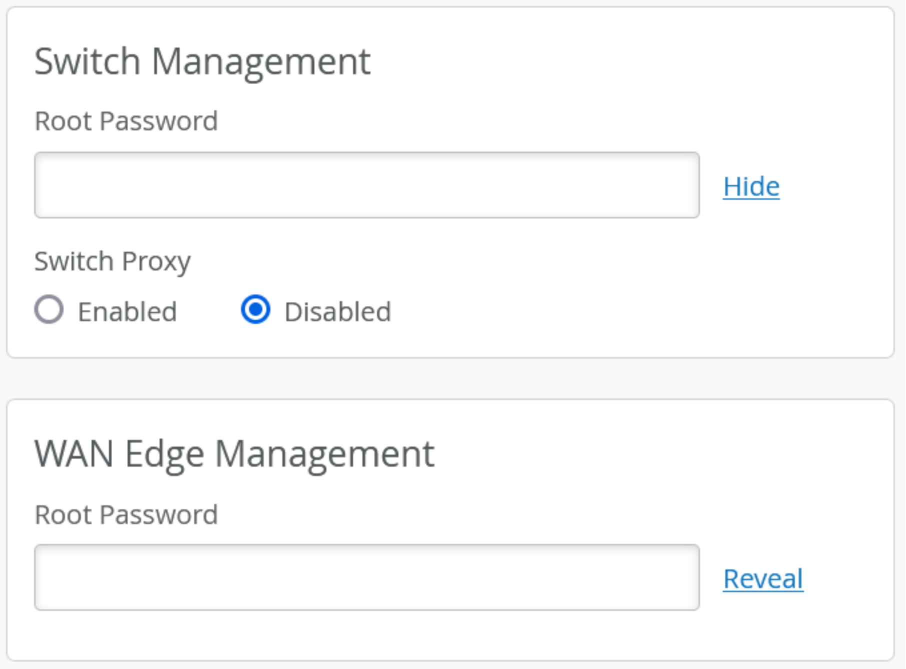
   A list of existing sites, if any, appears.
2. Click **Create Sites** in the upper right corner. The New Site window appears.

a. 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).

b. Enter the street address of your site, or use the map to locate it.

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

Figure 92: Setting Root Password



Switch Management

Root Password

Hide

Switch Proxy

○ Enabled ● Disabled

WAN Edge Management

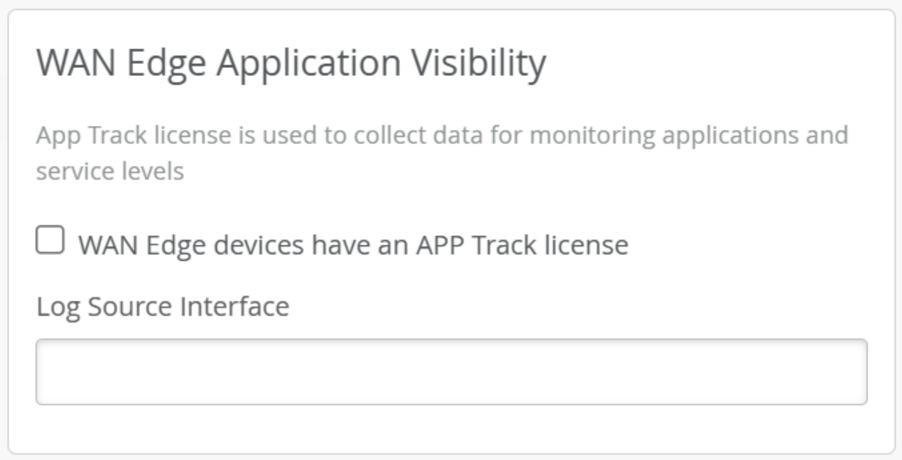
Root Password

Reveal

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.

4. Scroll down the page to the **WAN Edge Application Visibility section**, and then enable the **WAN Edge devices have an APP Track license** option.

Figure 93: 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

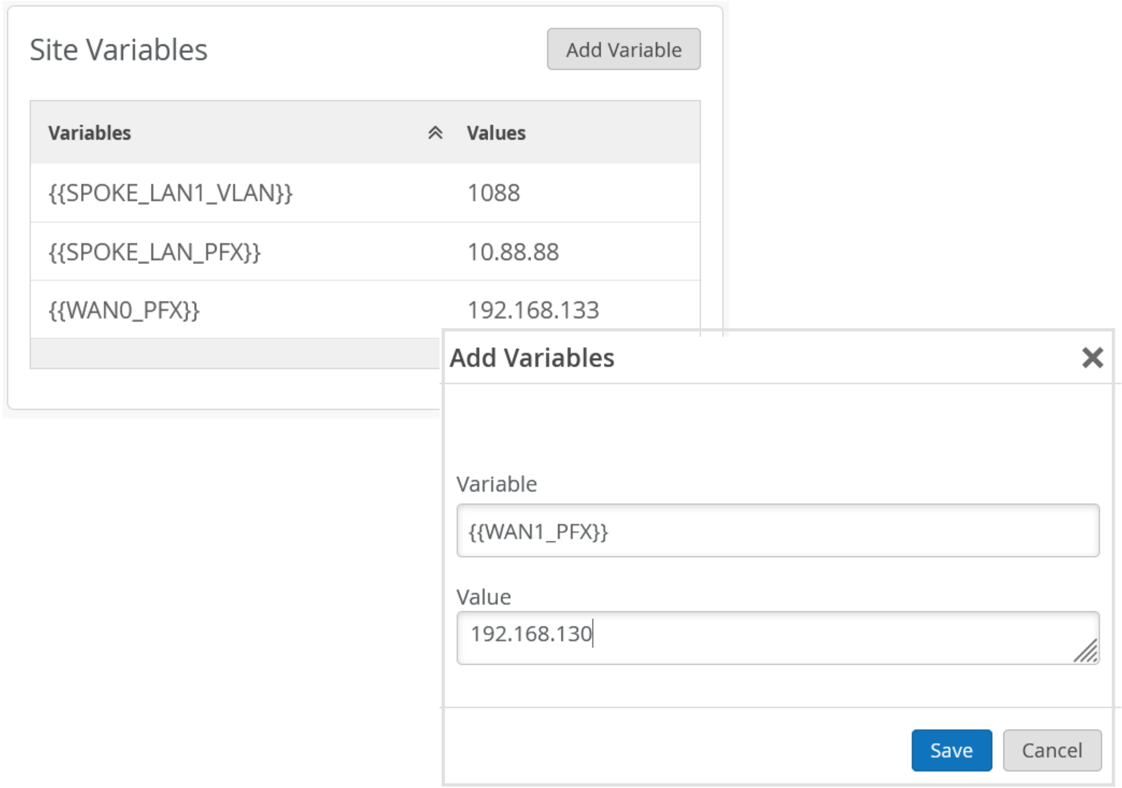
NOTE: An application security license is mandatory for all software-defined WAN (SD-WAN) SRX Series Firewall devices. Ensure that you have a valid license installed on the device.

5. Scroll down the screen to the **Site Variables** settings pane.

   a. Click the **Add Variable** button.

   b. In the pop-up screen that appears, type a name for the variable and specify the value it represents.

Figure 94: 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

Use Table 22 on page 171 to complete the list of variables you need to add.

Table 22: 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

Table 22: Variable Settings for Sites *(Continued)*

Site Name	Variable	Value
	{{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.

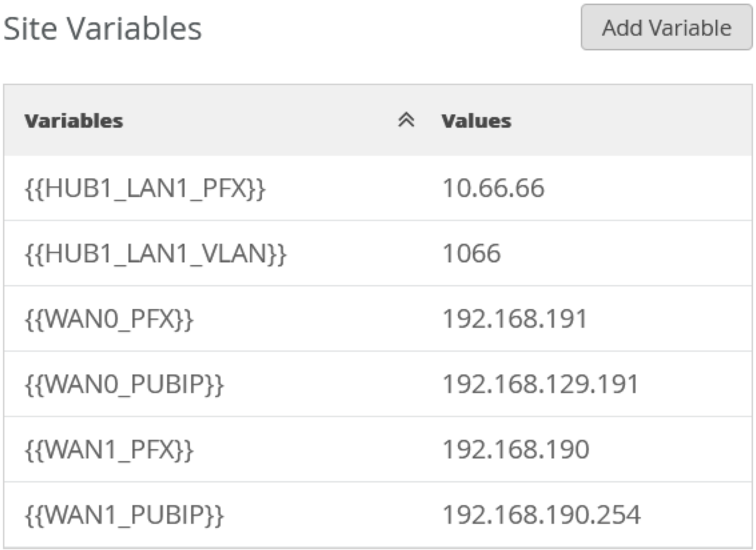
- The variables such as {{SPOKE_LAN1_VLAN}}, {{HUB1_LAN1_VLAN}}, {{HUB2_LAN1_VLAN}} contain the individual VLAN IDs. In this example, use VLAN tagging to break up the broadcast domain and separate the traffic.
- The variables {{WAN0_PUBIP}} and {{WAN1_PUBIP}} defined for the WAN interfaces of hubs use 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 in 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.

6. Click **Save** to add the variable to the list.

   Figure 95 on page 173 shows the list of newly created variables.

Figure 95: Site Variables Sample

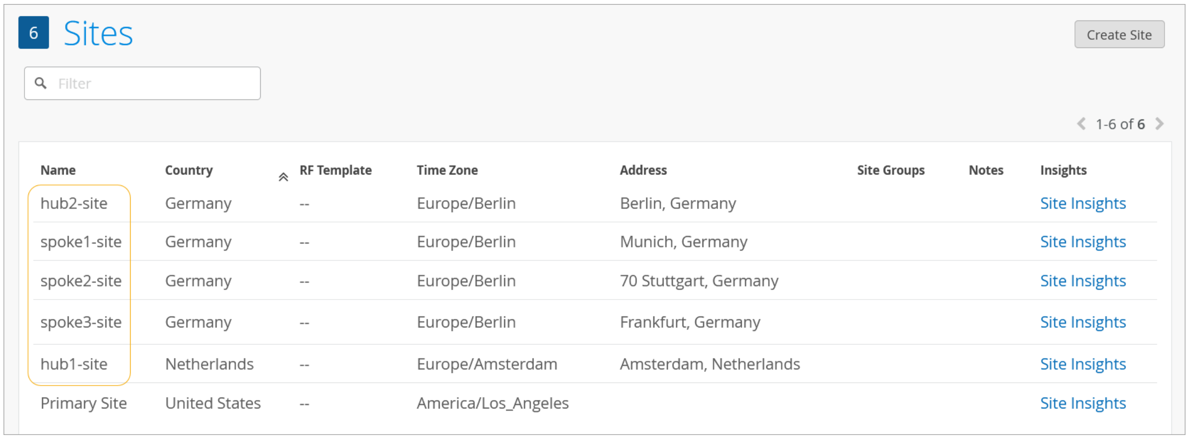


Variables	Values
{{HUB1_LAN1_PFX}}	10.66.66
{{HUB1_LAN1_VLAN}}	1066
{{WAN0_PFX}}	192.168.191
{{WAN0_PUBIP}}	192.168.129.191
{{WAN1_PFX}}	192.168.190
{{WAN1_PUBIP}}	192.168.190.254

7. Click **Save** to save your changes for the site.

   Figure 96 on page 174 shows the list of newly created sites.

Figure 96: Newly Created Sites



Name	Country	RF Template	Time Zone	Address	Site Groups	Notes	Insights
hub2-site	Germany	--	Europe/Berlin	Berlin, Germany			Site Insights
spoke1-site	Germany	--	Europe/Berlin	Munich, Germany			Site Insights
spoke2-site	Germany	--	Europe/Berlin	70 Stuttgart, Germany			Site Insights
spoke3-site	Germany	--	Europe/Berlin	Frankfurt, Germany			Site Insights
hub1-site	Netherlands	--	Europe/Amsterdam	Amsterdam, Netherlands			Site Insights
Primary Site	United States	--	America/Los_Angeles				Site Insights

RELATED DOCUMENTATION

Juniper Mist WAN Assurance Configuration Hierarchy | 13

WAN Assurance Configuration Overview | 166

Configure Networks for SRX Series Firewalls | 182

Configure Applications for SRX Series Firewalls | 174

Configure Applications for SRX Series Firewalls

IN THIS SECTION

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 will 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).

Configure Applications

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 upper right corner.
   The **Add Application** window appears.

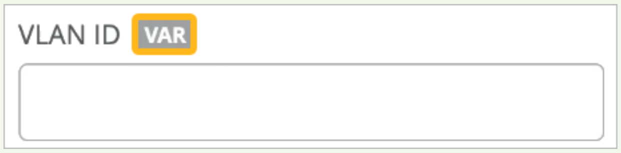
   > **TIP**: The fields with this label also display the matching variables (if configured) as you start typing a specific variable in it. This field lists variables from all sites within the organization.
   >
   > 
   >
   >
   > The organization-wide list of variables can be viewed using **GET /api/v1/orgs/:org_id/vars/search?var=***. This list is populated as variables are added under site settings.

   Table 23 on page 175 summarizes the options you can set in an application configuration.
   Table 23: Application Options

Fields	Description
Name	Enter a unique name for the application. You can use upto 32 characters for naming the application including alphanumerics, underscores, and dashes.

Table 23: Application Options *(Continued)*

Fields	Description
Description	Enter a description of the application and context.
Type	Select the application type: • Custom applications • Predefined applications • URL categories • Custom URLs
IP Address	(For custom applications) Enter the network IP address, including prefix (if any) of the application.
Domain Name	Enter the domain name of the application. The domain name is used in cloud breakout profiles to generate the fully qualified domain name (FQDN). The cloud security providers use the FQDN to identify the IPsec tunnels. For example, juniper.example.com.
Protocol and Port Ranges	(For custom applications) Enter details about protocols, protocol numbers, and port ranges (start and end ports) that the application is using. **NOTE**: Click the blue Add (+) icon to select multiple protocols.
Traffic Type	Configure the optional advanced traffic type settings that includes: • Traffic type • Failover policy • Traffic class • Maximum latency • Maximum jitter

3. Complete the configuration according to the details provided in "Configure Applications with Custom Applications" on page 177.

   If you want to create applications with predefined applications, URL categories, or custom URLs, go to the following sections:

   - "Configure Applications with Predefined Applications" on page 178
   - "Configure Applications with URL Categories" on page 179
   - "Configure Applications with Custom URLs" on page 181

Configure Applications with Custom Applications

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.

To define custom applications:

1. In the Juniper Mist cloud portal, under the **Add Application** pane, select the **Type** as **Custom Apps**.
2. Create a custom application using IP prefixes. Complete the configuration according to the details provided in "Configure Applications with Custom Applications" on page 177.

   Table 24: 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.

Table 24: Custom Application Configuration *(Continued)*

Custom Application	IP Address	Description
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.

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).

TIP: The Juniper Mist cloud portal assigns an IP address directly or indirectly to all LAN interfaces of hub-and-spoke. 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 10.0.0.8). A wildcard match allows easy extensions without a need to change the ruleset in your environment.

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

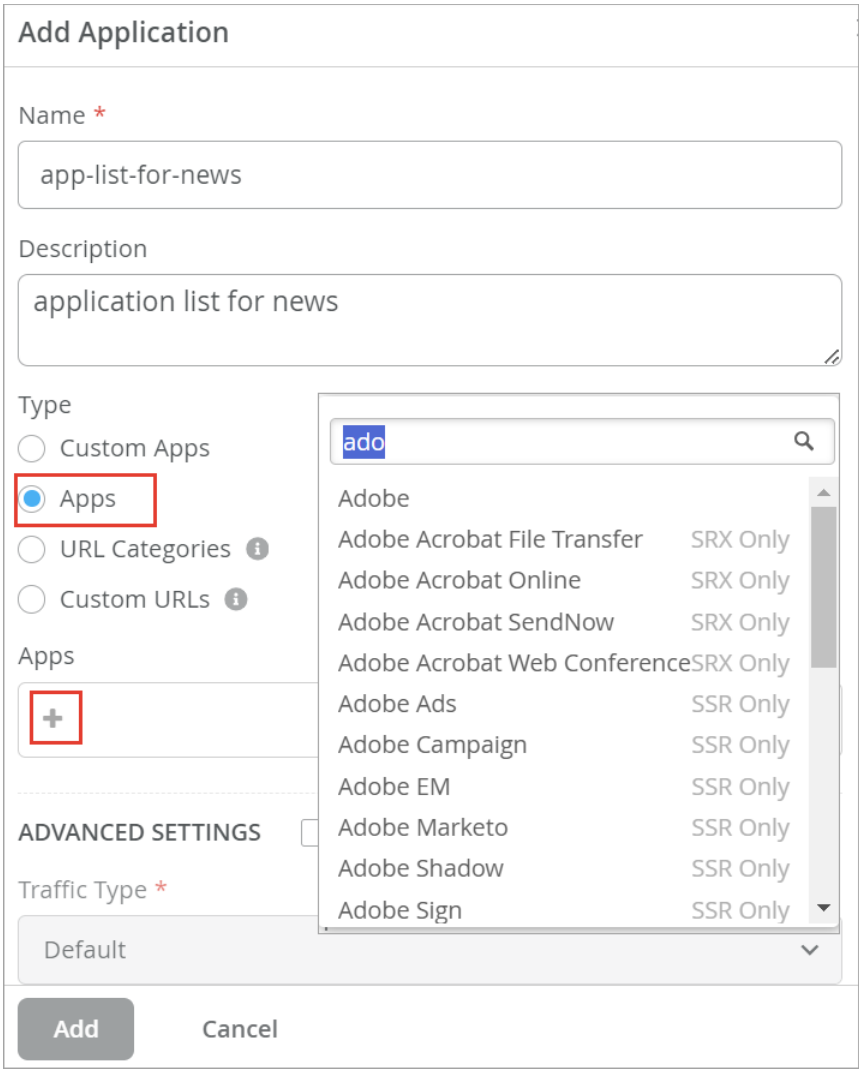
Configure Applications with Predefined Applications

Juniper Mist cloud provides a list of known applications that you can use to define an application.

To configure predefined applications:

1. In the Mist portal, in the **Add Application** pane, select the **Type** as **Apps**.
2. Click the Add (+) icon to display the list of available predefined applications.

Figure 97: Predefined Applications



Add Application

Name * app-list-for-news

Description application list for news

Type
○ Custom Apps
● Apps
○ URL Categories
○ Custom URLs

Applications that are specific only to SRX Series devices are marked as 'SRX Only'.

3. Select one or more applications from the drop-down menu.
4. Click **Add** to save your changes.

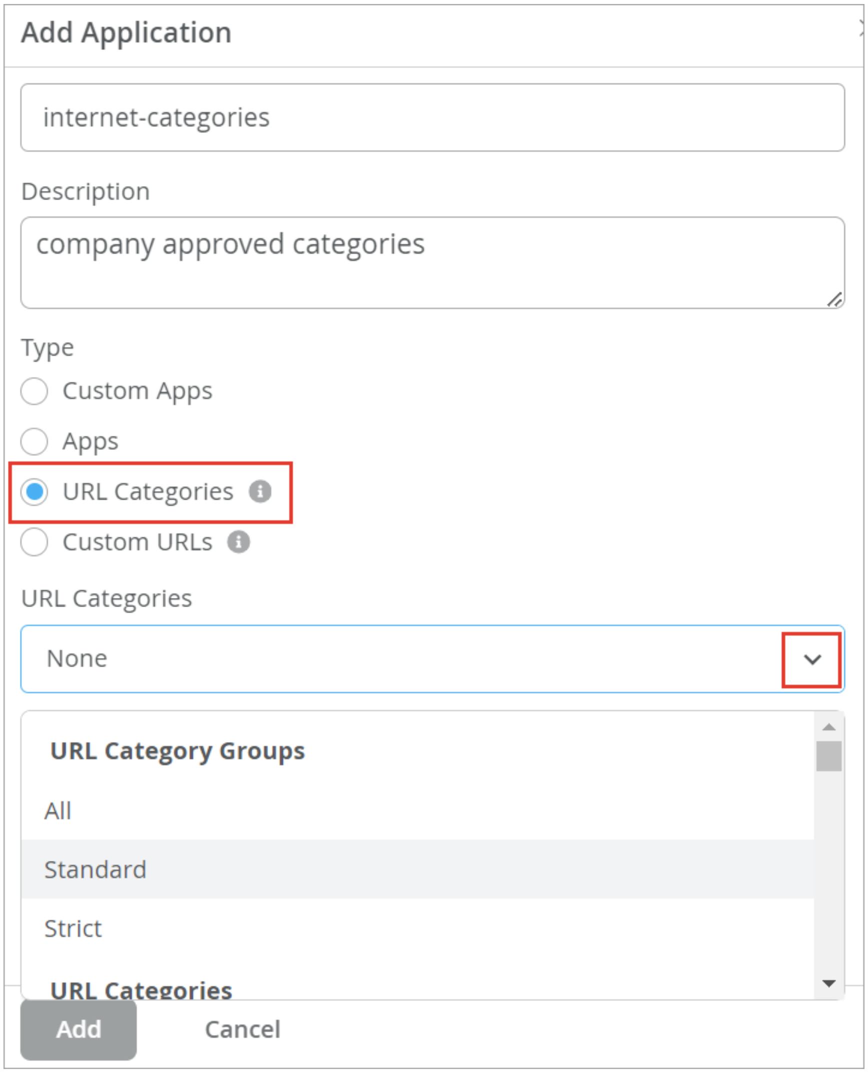
Configure Applications with URL Categories

Juniper Mist cloud provides a list of URL categories based on types (example: shopping, sports) and grouped by severity (all, standard, 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:

1. In the Mist portal, in the **Add Application** pane, select the **Type** as **URL Categories**.
   a. Click the Add (+) icon to display the list of available URL categories.

Figure 98: URL Categories



Add Application

internet-categories

Description

company approved categories

Type

○ Custom Apps

○ Apps

● URL Categories

○ Custom URLs

URL Categories

None

Select one or more URL category groups or URL categories.

2. Click **Add** to save your changes.

Configure Applications with Custom URLs

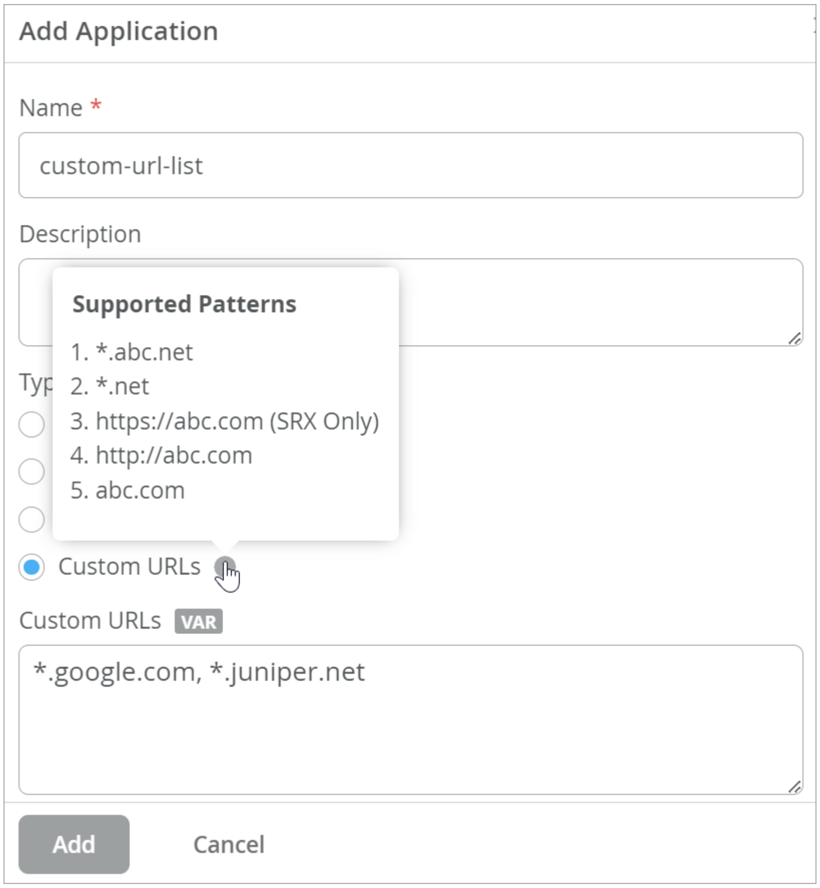
Juniper Mist allows you to create custom URL-based applications. With custom URLs, you can create a wildcard domains list, which can be used to permit or block traffic.

To define custom URLs:

1. In the Mist portal, in the **Add Application** pane, select the **Type** as **Custom URLs**.
2. Enter the custom URLs. Use a comma separator if you need to specify multiple URLs.

   Mist supports only the asterisk(*) wildcard pattern. You can specify up to 15 URL patterns for an application. You can view the supported patterns by hovering the mouse over the tooltip icon. Note that you can use the *https://abc.com* pattern only for SRX Series devices.

Figure 99: Custom URLs



Add Application

Name *

custom-url-list

Description

Supported Patterns

1. *.abc.net
2. *.net
3. https://abc.com (SRX Only)
4. http://abc.com
5. abc.com

Typ

○

○

○

● Custom URLs

Custom URLs VAR

*.google.com, *.juniper.net

3. Click **Add** to save your changes.

NOTE: You can also edit an existing application to include custom URL patterns.

SEE ALSO

WAN Assurance Configuration Overview | 166
Juniper Mist WAN Assurance Configuration Hierarchy | 13
Configure Networks for SRX Series Firewalls | 182
Configure Application Policies on SRX Series Firewalls | 191

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 25 on page 182 summarizes the options you can set in a network.
   Table 25: 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).

Table 25: Network Options *(Continued)*

Fields	Description
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. 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.

Table 25: Network Options *(Continued)*

Fields	Description
Advertise to the Overlay	Check the option to advertise the network to the hub devices through the overlay tunnels. When you select this option, the system displays following additional options for advertising: • Advertise to Other Spokes—Network to advertise the network prefix to other spokes (default option). If you want the network to advertise the prefix only to hubs (not other spokes), disable the default option. • Advertise to Hub LAN BGP Neighbor—Network to advertise the network prefix to any LAN BGP neighbor at the hub (default option). If you do not want to advertise, disable the default option. • Advertise to Hub LAN OSPF Neighbor (SRX Only)—Network to advertise the network prefix to any LAN OSPF neighbor at the hub (default option). If you do not want to advertise, disable the default option. • Override Prefix to Advertise— Enable this option when the prefix to advertise to the Hubs is not the original network but a different prefix. This is typically used when enabling NAT options. When you select this option, enter IP Address and Prefix Length. The portal also displays following route summarization options: • Hub Overlay Summarization—Enable the network to summarize the network prefix advertised to the overlay. For example: Juniper Mist portal can summarize 192.168.1.0/24 to 192.168.0.0/16. This feature limits the number of BGP updates received by a hub from each spoke and sent by the hub back to all the other spokes.

Table 25: Network Options *(Continued)*

Fields	Description
	• Hub LAN BGP Summarization—Enable the network to summarize the network prefix advertised to the LAN BGP neighbor. For example: Juniper Mist portal can summarize 192.168.1.0/24 to 192.168.0.0/16. • Hub LAN OSPF Summarization—Enable the network to summarize the network prefix advertised to the LAN OSPF neighbor. For example: Juniper Mist portal can summarize 192.168.1.0/24 to 192.168.0.0/16. • Route Summarization—Summarize local routes towards overlay. You can specify the IP addresses and prefix length of the summarized routes. For Session Smart Routers support summarization when the network is attached to the spoke only.
Networks Donot directly attached (SSR Only)	Select the networks that are not directly connected networks that arrive on this network assigned to a LAN.
Users	(Optional) Additional networks or users. Example: remote networks or users connected to the main network. 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. Click the **Add Static NAT** option and enter the **Name** , **Internal IP**, **External IP** and select option to apply to outgoing traffic on **Underlay** or **Overlay**. Enter **WAN Name** for SRX Series Devices.

Table 25: Network Options *(Continued)*

Fields	Description
Destination NAT	(Optional) Translate the destination IP address of a packet. Click the **Add Destination NAT** option and enter the **Name** , **Internal IPInternal Port**, **External IP**, **External Port** and select option to apply to outgoing traffic on **Underlay** or **Overlay**. Enter **WAN Name** for SRX Series Devices.

3. Complete the configuration according to the details available in Table 26 on page 186.

   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 26: 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 • IP-Prefixes=10.0.0.0/8	-	-

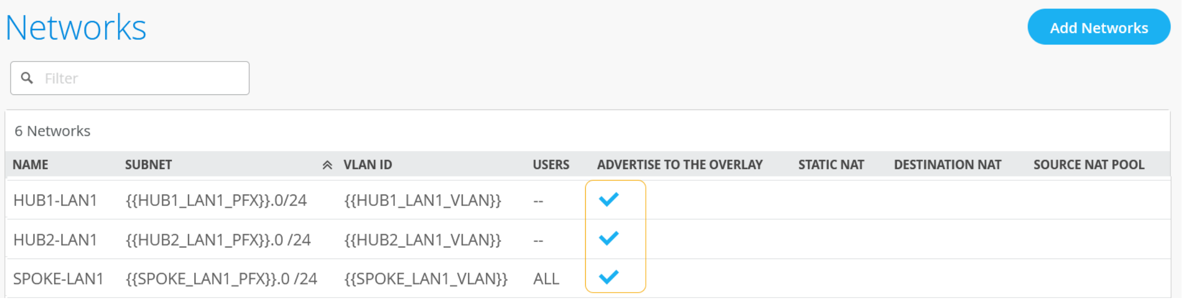
NOTE: The user "All" with IP prefix 10.0.0.0/8 serves as a wildcard for all the future LAN segments in the range. The SRX Series Firewall in hubs can use the same username (All) and IP prefix (10.0.0.8) to identify all spoke LAN interfaces using a single rule.

NOTE: When you use variables, do not assume that the system imports all LAN segments on the hub site automatically. Sometimes, the system may apply an Any netmask, which has a wide scope and may generate security issues.

4. Click **Add**.

   Figure 100 on page 187 shows the list of newly created networks.

Figure 100: Networks Summary



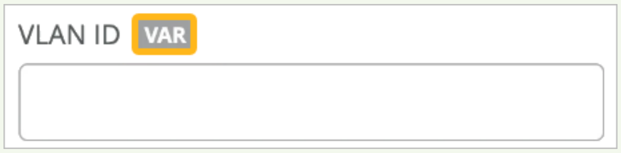
6 Networks

NAME	SUBNET	VLAN ID	USERS	ADVERTISE TO THE OVERLAY	STATIC NAT	DESTINATION NAT	SOURCE NAT POOL
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	✓			

Site Variables

You can configure the site variables on a per-site basis. Site variables allow you to use the same network definition with different values for each site without having to define multiple networks. Variables have the format {{variable_name}}. Defining networks with variables is common practice in WAN edge template configuration.

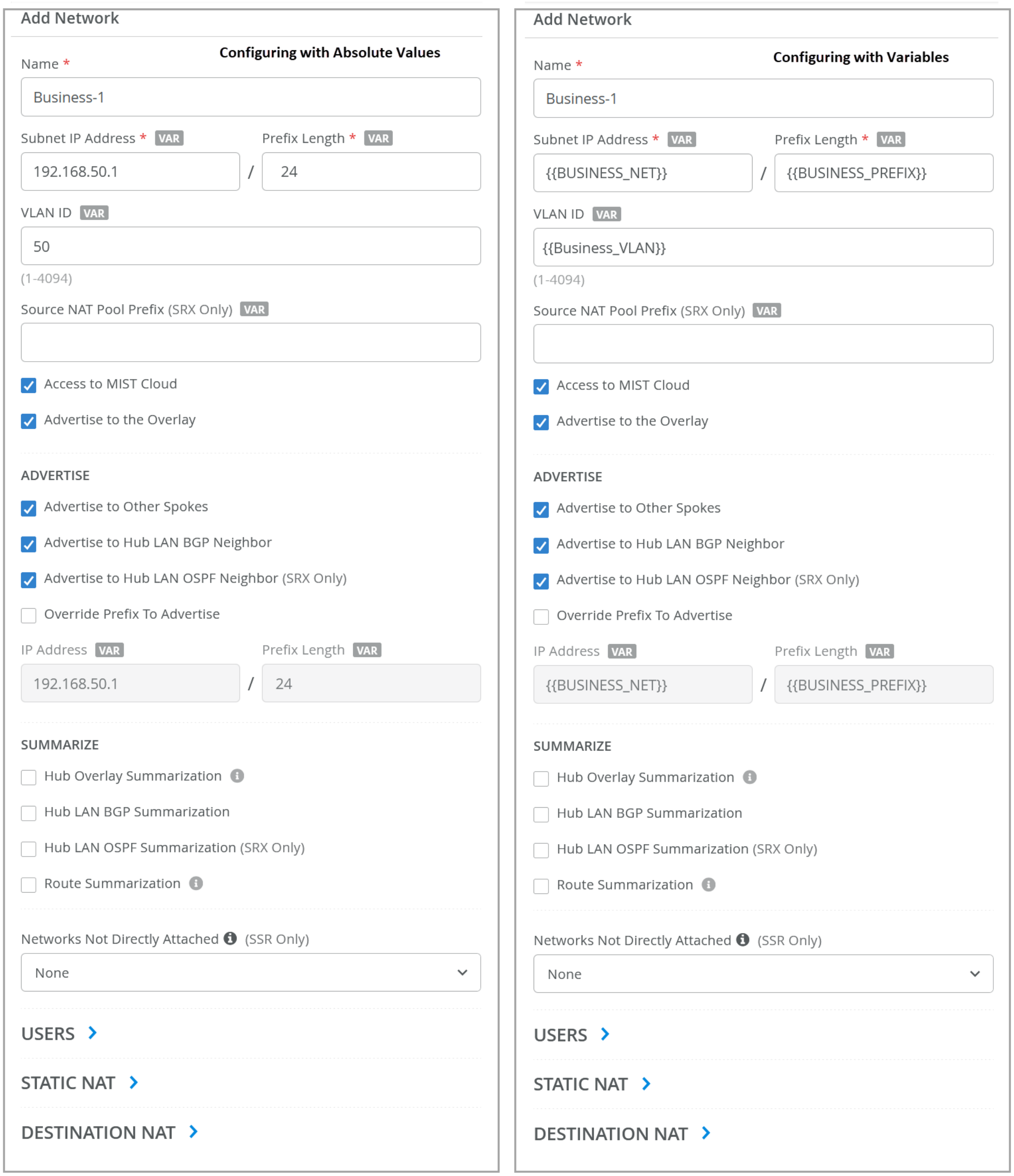
TIP: The fields with this label also display the matching variables (if configured) as you start typing a specific variable in it. This field lists variables from all sites within the organization.



The organization-wide list of variables can be viewed using **GET /api/v1/orgs/:org_id/vars/search?var=***. This list is populated as variables are added under site settings.

Figure 101 on page 188 shows two samples of configuring a network using absolute values and site variables.

Figure 101: Configuring Networks with Absolute Values and Variables



Add Network

Configuring with Absolute Values

Name *

Business-1

Subnet IP Address * VAR / Prefix Length * VAR

192.168.50.1 / 24

VLAN ID VAR

50

(1-4094)

Source NAT Pool Prefix (SRX Only) VAR

☑ Access to MIST Cloud

☑ Advertise to the Overlay

ADVERTISE

☑ Advertise to Other Spokes

☑ Advertise to Hub LAN BGP Neighbor

☑ Advertise to Hub LAN OSPF Neighbor (SRX Only)

☐ Override Prefix To Advertise

IP Address VAR / Prefix Length VAR

192.168.50.1 / 24

SUMMARIZE

☐ Hub Overlay Summarization

☐ Hub LAN BGP Summarization

☐ Hub LAN OSPF Summarization (SRX Only)

☐ Route Summarization

Networks Not Directly Attached (SSR Only)

None

USERS >

STATIC NAT >

DESTINATION NAT >

Add Network

Configuring with Variables

Name *

Business-1

Subnet IP Address * VAR / Prefix Length * VAR

{{BUSINESS_NET}} / {{BUSINESS_PREFIX}}

VLAN ID VAR

{{Business_VLAN}}

(1-4094)

Source NAT Pool Prefix (SRX Only) VAR

☑ Access to MIST Cloud

☑ Advertise to the Overlay

ADVERTISE

☑ Advertise to Other Spokes

☑ Advertise to Hub LAN BGP Neighbor

☑ Advertise to Hub LAN OSPF Neighbor (SRX Only)

☐ Override Prefix To Advertise

IP Address VAR / Prefix Length VAR

{{BUSINESS_NET}} / {{BUSINESS_PREFIX}}

SUMMARIZE

☐ Hub Overlay Summarization

☐ Hub LAN BGP Summarization

☐ Hub LAN OSPF Summarization (SRX Only)

☐ Route Summarization

Networks Not Directly Attached (SSR Only)

None

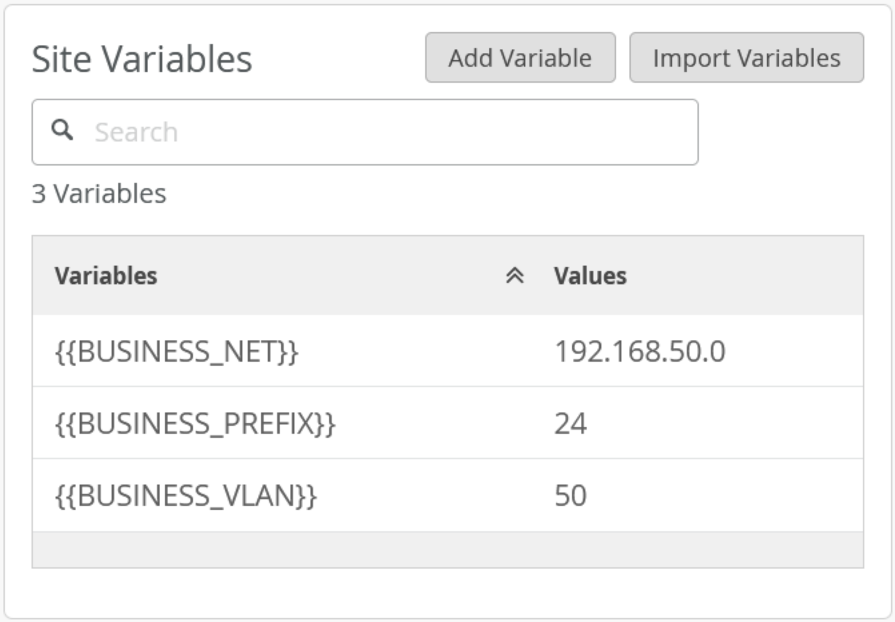
USERS >

STATIC NAT >

DESTINATION NAT >

You can define the site variables in the **Organization** > **Admin**> **Site Configuration** pane.

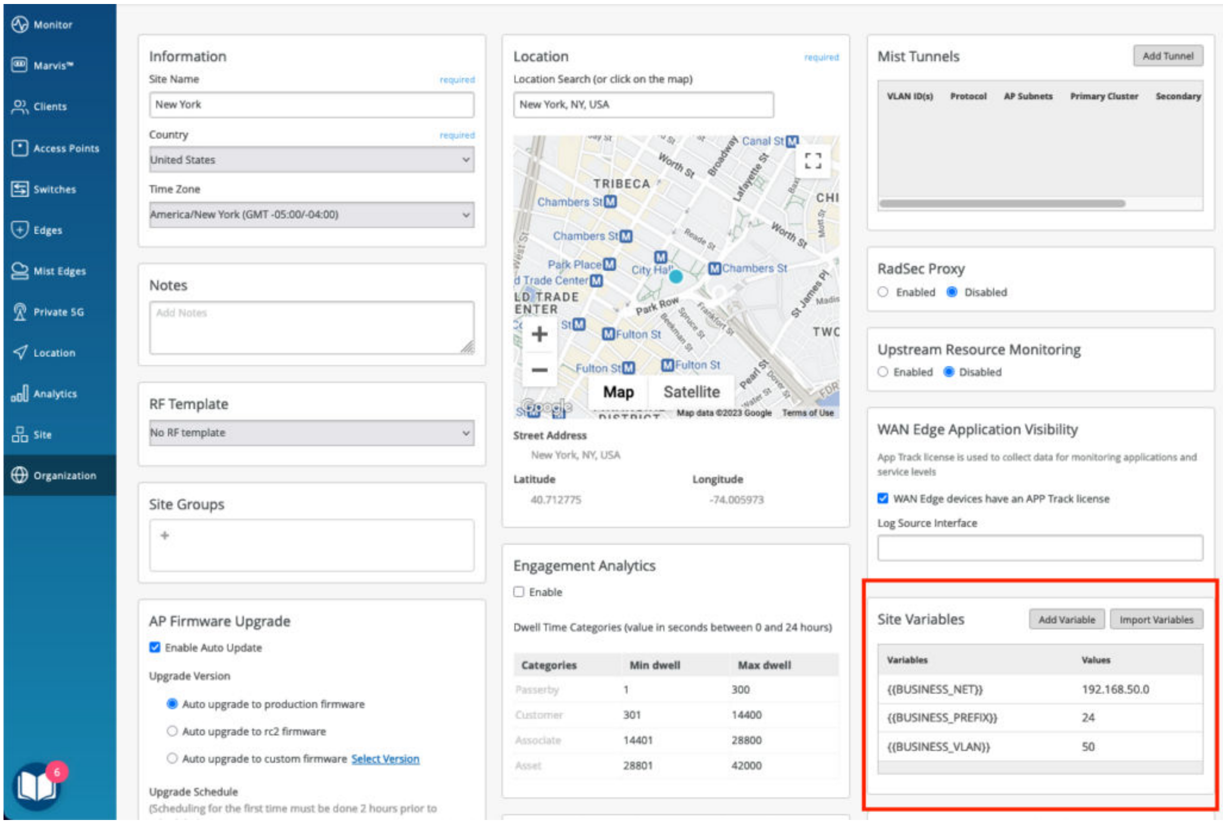
Figure 102: Site Variables Settings Pane



Variables	Values
{{BUSINESS_NET}}	192.168.50.0
{{BUSINESS_PREFIX}}	24
{{BUSINESS_VLAN}}	50

This task uses variables for the VLAN ID and subnet IP address. Site variables that contain the first three octets substitute the subnet IP address variable values as shown in Figure 103 on page 190.

Figure 103: Site Variables Displayed on the Site Configuration Page



Information

Site Name (required): New York

Country (required): United States

Time Zone: America/New York (GMT -05:00/-04:00)

Notes

Add Notes

RF Template

No RF template

Site Groups

+

AP Firmware Upgrade

☑ Enable Auto Update

Upgrade Version

● Auto upgrade to production firmware

○ Auto upgrade to rc2 firmware

○ Auto upgrade to custom firmware Select Version

Upgrade Schedule

(Scheduling for the first time must be done 2 hours prior to

Location (required)

Location Search (or click on the map): New York, NY, USA

Street Address: New York, NY, USA

Latitude: 40.712775

Longitude: -74.005973

Engagement Analytics

☐ Enable

Dwell Time Categories (value in seconds between 0 and 24 hours)

Categories	Min dwell	Max dwell
Passerby	1	300
Customer	301	14400
Associate	14401	28800
Asset	28801	42000

Mist Tunnels

Add Tunnel

VLAN ID(s)	Protocol	AP Subnets	Primary Cluster	Secondary

RadSec Proxy

○ Enabled ● Disabled

Upstream Resource Monitoring

○ Enabled ● Disabled

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

Site Variables

Add Variable | Import Variables

Variables	Values
{{BUSINESS_NET}}	192.168.50.0
{{BUSINESS_PREFIX}}	24
{{BUSINESS_VLAN}}	50

RELATED DOCUMENTATION

Juniper Mist WAN Assurance Configuration Hierarchy | 13

WAN Assurance Configuration Overview | 166

Configure Application Policies on SRX Series Firewalls | 191

Configure Applications for SRX Series Firewalls | 174

Configure Sites and Variables for SRX Series Firewalls | 168

Configure Application Policies on SRX Series Firewalls

IN THIS SECTION

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 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.

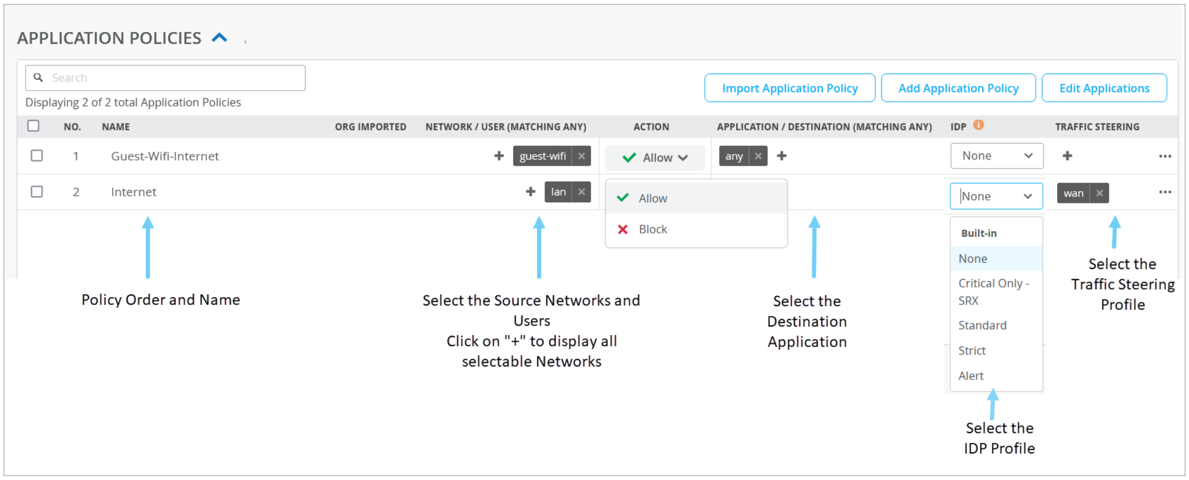
2. Scroll down to the **Application Policies** section, and click **Add Application Policy**.

   > **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 check mark to apply your changes.

   The following figure (Figure 104 on page 192) shows the options that are available to you when you configure an application policy.

Figure 104: Application Policy Configuration Options



APPLICATION POLICIES

Displaying 2 of 2 total Application Policies

NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
1	Guest-Wifi-Internet		guest-wifi	Allow	any	None	
2	Internet		lan			None	wan

Search
Import Application Policy
Add Application Policy
Edit Applications
Allow
Block
Built-in
None
Critical Only - SRX
Standard
Strict
Alert
Policy Order and Name
Select the Source Networks and Users
Click on "+" to display all selectable Networks
Select the Destination Application
Select the Traffic Steering Profile
Select the IDP Profile

The following table (Table 27 on page 193) explains the configuration options available for an application policy.

Table 27: 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 upto 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 an user to the network, the Mist portal displays the detail as ***user.network*** format in the drop-down menu.
Action	Policy actions. Select one of these policy actions: • Allow • Block
Application / Destination	Destination end point. Applications determine the destinations used in a policy You can select applications from the list of already defined applications.

Table 27: Application Policies Options *(Continued)*

Field	Description
IDP	(Optional) Intrusion Detection and Prevention (IDP) profiles. Select one of the IDP profiles: • **Standard**—Standard profile is the default profile and represents the set of IDP signatures and rules recommended by Juniper Networks. The actions include: Close the client and server TCP connection. Drop current packet and all subsequent packets • **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. • **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. • **None**—No IDP profile applied. 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. Steering profiles are required for deploying the policy to the WAN edge spoke device or to a hub device.
Hit Count	Application policy hit count (allow/block/filter) displays the number of times traffic has hit a given Application Policy.

> **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 Table 28 on page 195.

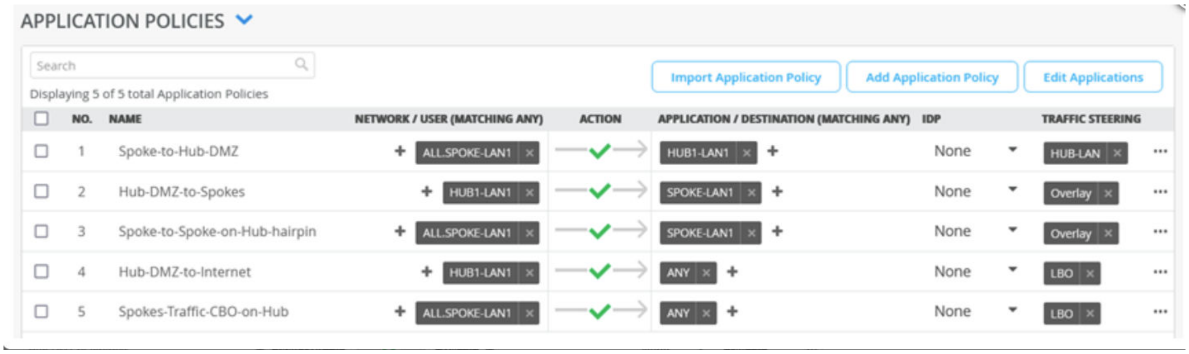
Table 28: Application Policy Examples

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**.

   Figure 105 on page 195 shows the list of newly created application policies.

Figure 105: Application Policies Summary



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

Reorder and Delete Application Policies

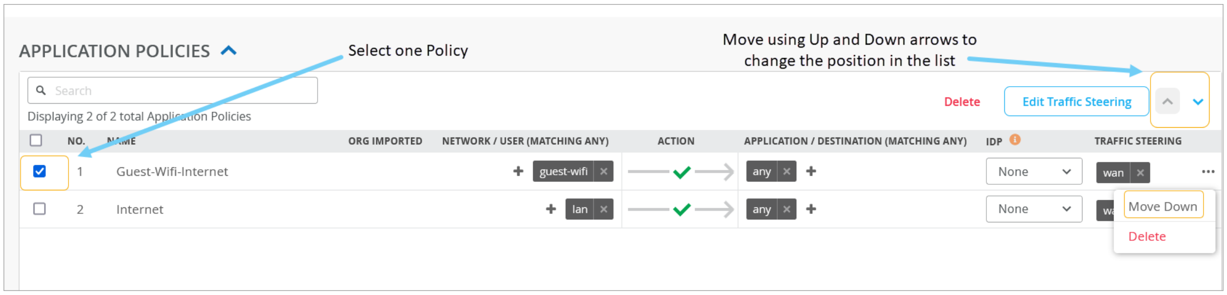
Reordering application policy allows you to move the policies around after they have been created.

Mist evaluates policies and executes policies in the order of their appearance in the policies list, you should be aware of 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 106: Changing Policy Order



APPLICATION POLICIES

Select one Policy

Move using Up and Down arrows to change the position in the list

Search

Displaying 2 of 2 total Application Policies

Delete   Edit Traffic Steering

☐	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
☑	1	Guest-Wifi-Internet		guest-wifi	✓	any	None	wan
☐	2	Internet		lan	✓	any	None	wa

Move Down
Delete

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

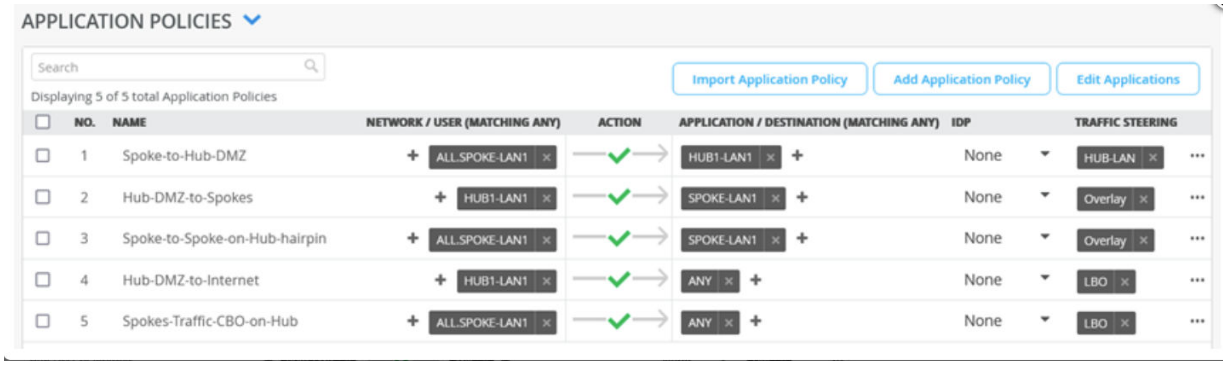
Using Same IP Addresses and Prefixes in Networks and Applications

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.

Consider the policies in Figure 107 on page 197.

Figure 107: Application Policies Details



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

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.

SEE ALSO

WAN Assurance Configuration Overview | 166
Juniper Mist WAN Assurance Configuration Hierarchy | 13
Configure Networks for SRX Series Firewalls | 182
Configure Applications for SRX Series Firewalls | 174

Configure Hub Profiles for SRX Series Firewalls

IN THIS SECTION

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 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

IN THIS SECTION

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.

> **NOTE**: You can also create a hub profile by importing a JavaScript Object Notation (JSON file) using the **Import Profile** option.

3. Enter the name of the profile and click **Create**.

   Table 29 on page 199 summarizes the options you can set in a hub profile.

Table 29: 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.
Hub Group	Configure a hub group by specifying a hub group identifier (number). Hub groups are used to group hub devices logically. Hub groups help you scale your hub architecture horizontally. By assigning a set of devices to a hub group, spokes can form overlay paths to hub endpoints within the group. Each hub group is limited to 31 hub endpoints.
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.
Secure Edge Connectors	Secure Edge connector details. Secure Edge performs traffic inspection for the WAN edge devices that the Juniper Mist cloud portal manages.

Table 29: Hub Profile Options *(Continued)*

Field	Description
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 "Add WAN Interfaces to the Hub Profile" on page 201.
LAN	LAN interface details. This section lists the hub side of the LAN interfaces that connect the hub to the LAN segment. You assign the networks, create VLANs, and set up IP addresses and DHCP options (none, relay, or server). See "Add a LAN Interface to the Hub Profile" on page 202.
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 "Configure Traffic-Steering Policies" on page 203.
Application Policies	Policies to enforce rules for traffic. Define network (source), application (destination), traffic steering policies, and policy action. See "Configure an Application Policy" on page 204.
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. See
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.

4. 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 endpoints 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 in Table 30 on page 201.

Table 30: WAN Interface Configuration

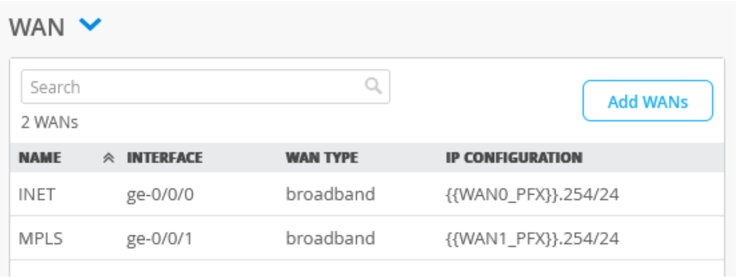
Field	WAN Interface 1	WAN Interface 2
Name (a label and not a technology)	INET	MPLS
Overlay Hub Endpoint (generated automatically)	hub1-INET	hub1-MPLS
WAN Type	Ethernet	Ethernet
Interface	ge-0/0/0	ge-0/0/1
VLAN ID	-	-
IP Address	{{WAN0_PFX}}.254	{{WAN1_PFX}}.254
Prefix Length	24	24
Gateway	{{WAN0_PFX}}.1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

   Figure 108 on page 202 shows the list of WAN interfaces you created.

Figure 108: Configured WAN Interfaces



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 Table 31 on page 202.

Table 31: 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

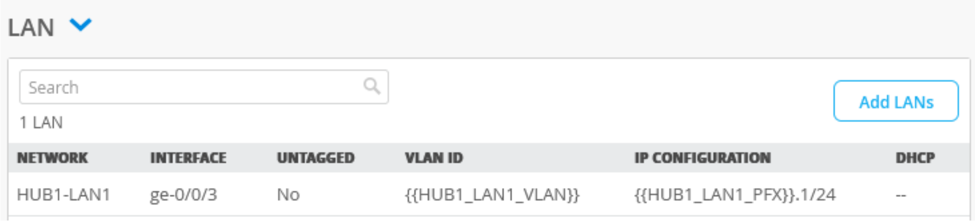
Table 31: LAN Interface Configuration *(Continued)*

Field	LAN Interface
Untagged VLAN	No
DHCP	No

3. Click **Save**.

   Figure 109 on page 203 shows the LAN interface you created.

Figure 109: Configured LAN Interfaces



LAN

Search

Add LANs

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
- 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.

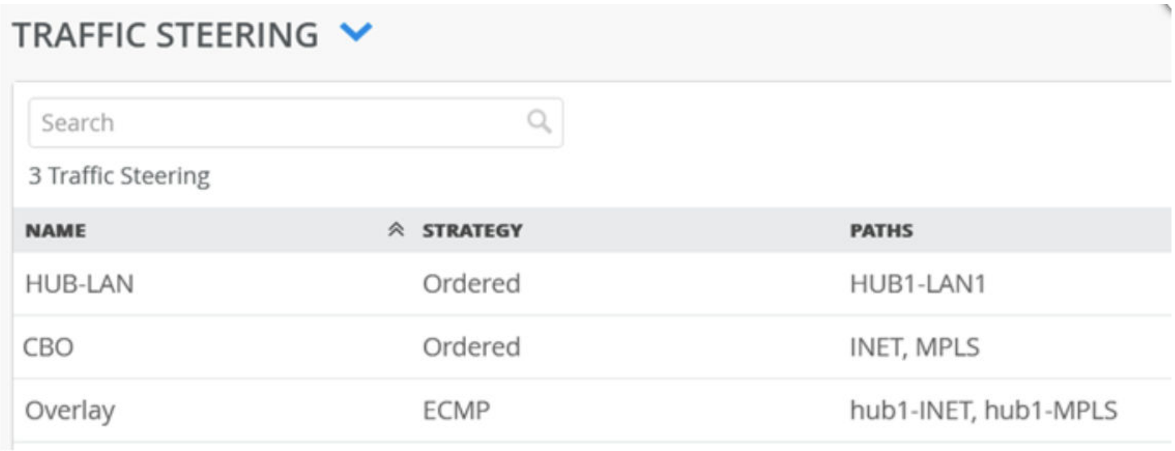
2. Configure three traffic-steering policies: one for the overlay, one for the underlay, and one for the central breakout, according to the details provided in Table 32 on page 204.

   Table 32: 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 • Network —HUB1-LAN1	• Type—WAN • Network —hub1-INET and hub1-MPLS	• Type—WAN • Network —WAN: INET and WAN: MPLS

   Figure 110 on page 204 shows the list of the traffic-steering policies that you created.

   Figure 110: Traffic-Steering Policies



TRAFFIC STEERING

Search

3 Traffic Steering

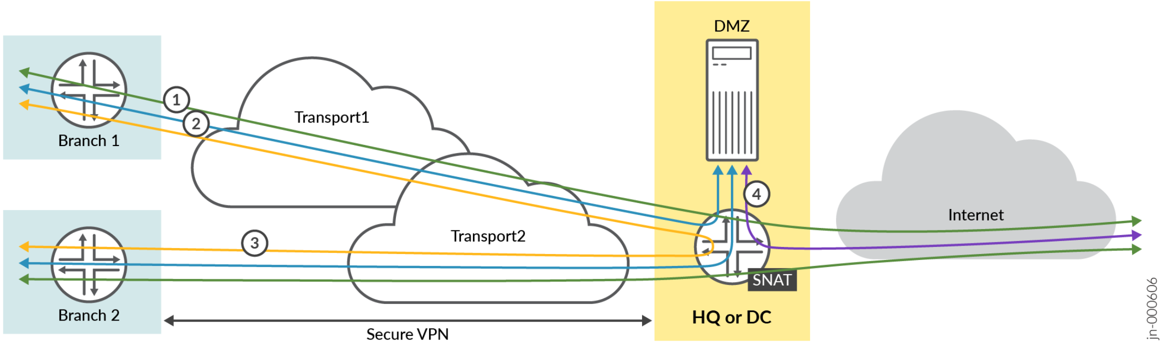
NAME	STRATEGY	PATHS
HUB-LAN	Ordered	HUB1-LAN1
CBO	Ordered	INET, MPLS
Overlay	ECMP	hub1-INET, hub1-MPLS

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.

Figure 111 on page 205 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 111: Traffic-Direction Topology



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

-

- Rule 1—Allows traffic from spoke sites to reach the hub (and to a server in the DMZ attached to the hub device).

- Rule 2—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.

- 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.

To configure an application policy:

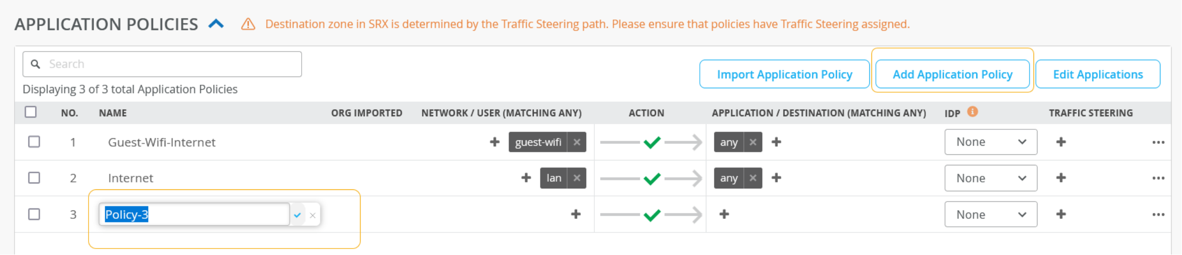
1. Scroll down to the **Application Policy** section, click **Add Policy** to create a new rule in the policy list.

   NOTE:

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

2. Click the **Name** column and give the policy a name, and then click the blue checkmark to apply your changes.

Figure 112: Adding a New Application Policy



APPLICATION POLICIES

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

Displaying 3 of 3 total Application Policies

□	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
□	1	Guest-Wifi-Internet		+ guest-wifi ×	✓	any × +	None	+
□	2	Internet		+ lan ×	✓	any × +	None	+
□	3	Policy-3		+	✓	+	None	+

3. Create application rules according to the details provided in Table 33 on page 206.

Table 33: Application Policy Rule Configuration

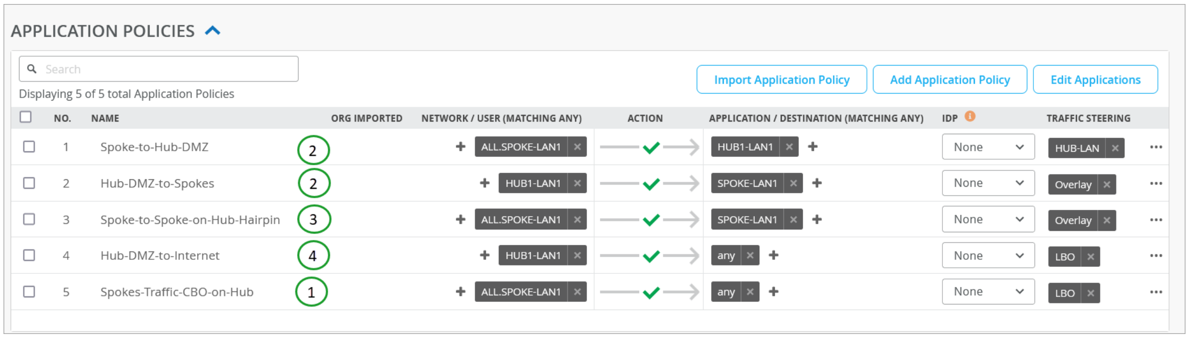
No. (Policy Order)	Rule Name	Network	Action	Destination	Steering
1	Spoke-to-Hub-DMZ	ALL.SPOKE-LAN1	Pass	HUB1-LAN1	HUB-LAN
2	Hub-DMZ-to-Spokes	HUB1-LAN1	Pass	SPOKE-LAN1	Overlay
3	Spoke-to-Spoke-on-Hub-Hairpin	ALL.SPOKE-LAN1	Pass	SPOKE-LAN1	Overlay

Table 33: Application Policy Rule Configuration *(Continued)*

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

Figure 113 on page 207 shows a list of the application policies that you created.

Figure 113: Application Policy Summary



APPLICATION POLICIES

Search

Displaying 5 of 5 total Application Policies

Import Application Policy | Add Application Policy | Edit Applications

☐	NO.	NAME	ORG IMPORTED	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 marks indicates the policies you have created for the traffic requirements in Figure 111 on page 205.

4. 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.

```
[edit]
user@host# set security zones security-zone HUB1-LAN1 host-inbound-traffic system-services
ping
```

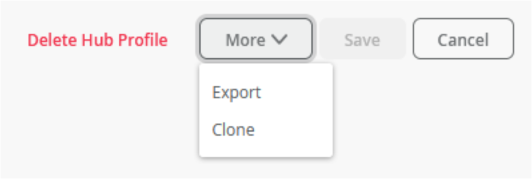
Create a Second Hub Profile by Cloning the Existing Hub Profile

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:

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

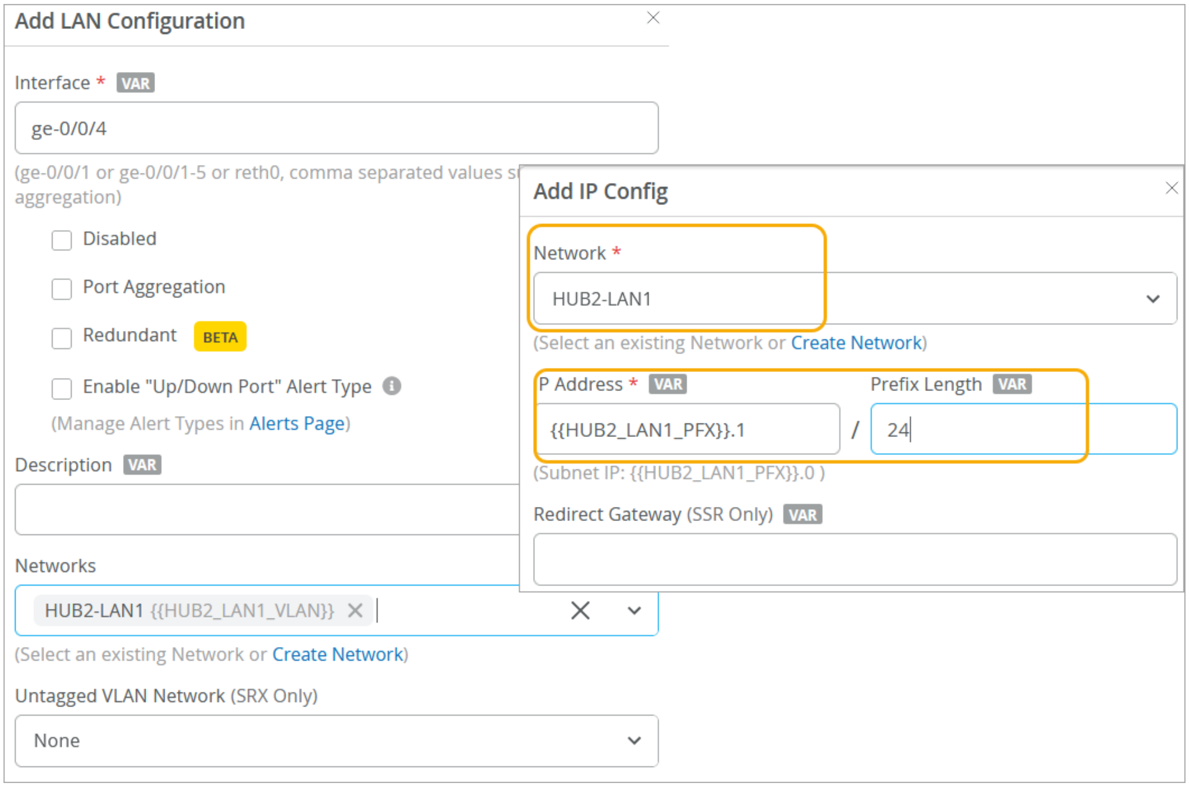
   Figure 114: Create a New Hub Profile By Using the Clone Option

4. Name the new profile (example: hub2) and click **Clone**.

   If you see any errors while naming the profile, refresh your browser.
5. 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.

Figure 115: Edit a Cloned Profile



Add LAN Configuration

Interface * VAR

ge-0/0/4

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

□ Disabled

□ Port Aggregation

□ Redundant BETA

□ Enable "Up/Down Port" Alert Type

(Manage Alert Types in Alerts Page)

Description VAR

Networks

HUB2-LAN1 {{HUB2_LAN1_VLAN}}

(Select an existing Network or Create Network)

Untagged VLAN Network (SRX Only)

None

Add IP Config

Network *

HUB2-LAN1

(Select an existing Network or Create Network)

P Address * VAR

{{HUB2_LAN1_PFX}}.1

Prefix Length VAR

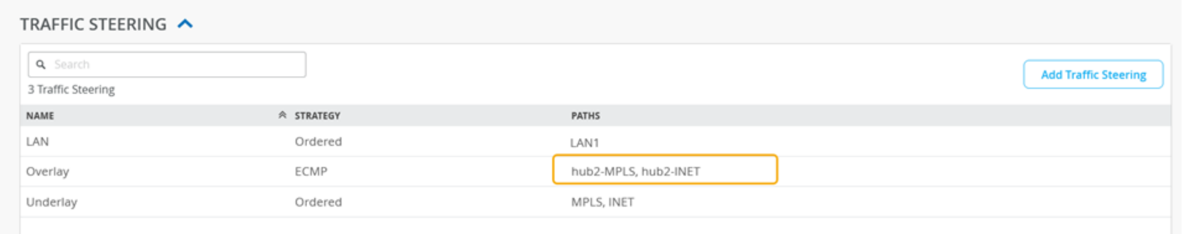
24

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

Redirect Gateway (SSR Only) VAR

6. Change the LAN interface to include HUB2. Example: HUB2-LAN1 and {{HUB2_LAN1_PFX}}.1
7. 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.

Figure 116: Updated Traffic-Steering Policy



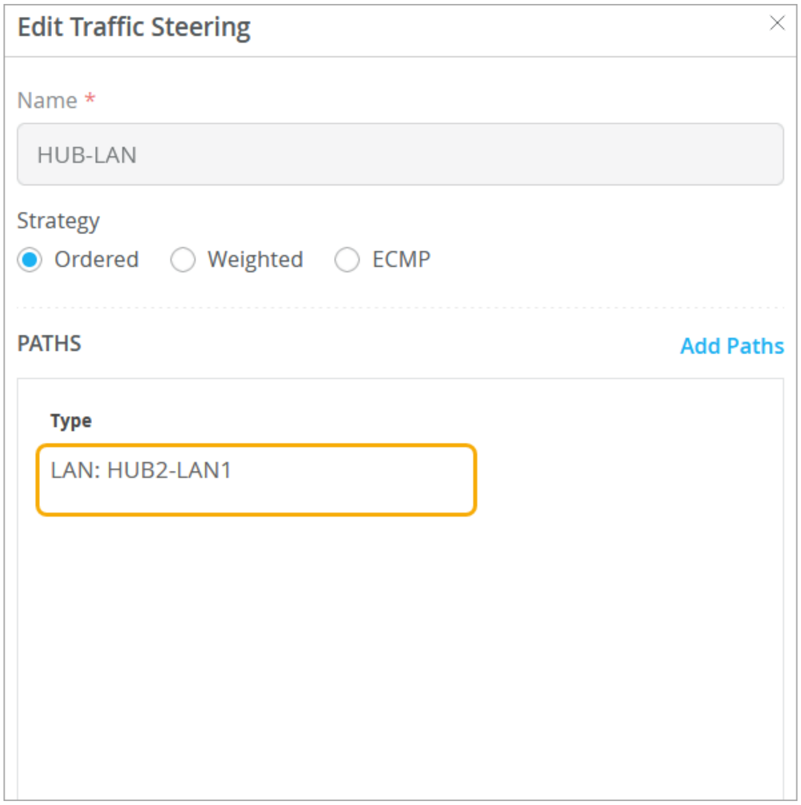
TRAFFIC STEERING

3 Traffic Steering

NAME	STRATEGY	PATHS
LAN	Ordered	LAN1
Overlay	ECMP	hub2-MPLS, hub2-INET
Underlay	Ordered	MPLS, INET

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

Figure 117: Update Paths in a Traffic-Steering Policy



Edit Traffic Steering

Name *

HUB-LAN

Strategy

● Ordered ○ Weighted ○ ECMP

PATHS

Type

LAN: HUB2-LAN1

9. Update the application rules according to the details provided in Table 34 on page 210. For example, wherever applicable, change HUB1-LAN to HUB2-LAN.

Table 34: Application Rules Configuration

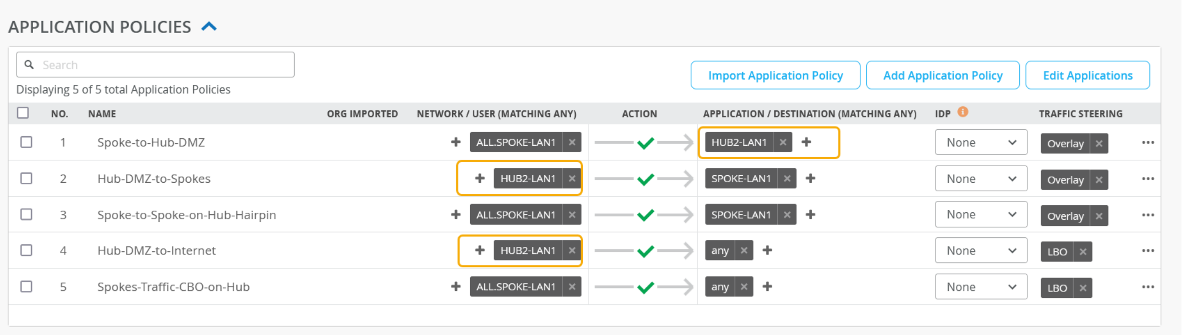
S.No.	Rule Name	Network	Action	Destination	Steering
1	Spoke-to-Hub-DMZ	ALL.SPOKE-LAN1	Pass	HUB2-LAN1	HUB-LAN
2	Hub-DMZ-to-Spokes	**HUB2-LAN1**	Pass	SPOKE-LAN1	Overlay
3	Spoke-to-Spoke-on-Hub-Hairpin	ALL.SPOKE-LAN1	Pass	SPOKE-LAN1	Overlay
4	Hub-DMZ-to-Internet	**HUB2-LAN1**	Pass	ANY	LBO

Table 34: Application Rules Configuration *(Continued)*

S.No.	Rule Name	Network	Action	Destination	Steering
5	Spokes-Traffic-CBO-on-Hub	ALL.SPOKE-LAN1	Pass	ANY	LBO

Figure 118 on page 211 shows the details of the updated application policies after you save your changes.

Figure 118: Updated Application Policy Summary



APPLICATION POLICIES

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	Overlay
☐	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

Hub-to-Hub Overlay

IN THIS SECTION

The Hub-to-hub overlay feature allows a you to form a peer path between two hub devices. You can utilize the hub-to-hub overlay path as a preferred route for data center traffic originating from sites. Additionally, these hub-to-hub overlays can serve as failover paths in scenarios involving hub-to-spoke connections.

Configure Hub-to-Hub Overlay

To create Hub-to-Hub overlay, the WAN interfaces of one hub map to the WAN interfaces of another hub, thus forming an overlay and designating a traffic pathway.

> **NOTE**: Hub-to-Hub overlay can utilize different WAN interfaces on both hub devices. It is not mandatory for the overlay to form between identical WAN interfaces on the two hubs.

Consider you have two hubs, Hub device A and Hub device B, and you wish to establish an overlay between them.

Hub device A is equipped with two WAN interfaces: WAN-1-A and WAN-2-A. You must pair these WAN interfaces with the WAN interfaces of Hub device B, which are WAN-1-B and WAN-2-B, marking them as hub endpoints.

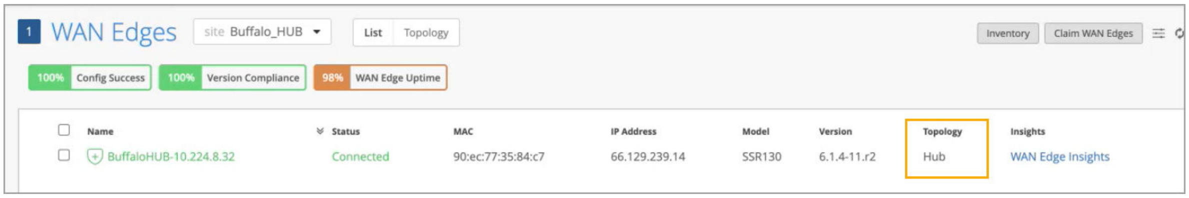
Similarly, for Hub device B:

It features two WAN Interfaces: WAN-1-B and WAN-2-B. These should be linked to the WAN Interfaces of Hub Device A (WAN-1-A and WAN-2-A) to complete the setup as hub endpoints.

Use the following steps to create hub endpoints:

1. On Juniper Mist portal, select **WAN Edges** and click the hub device. Ensure that the hub device you select must be part of hub topology.

   Figure 119: Hub Device in Hub Topology

   1 WAN Edges   site Buffalo_HUB   List   Topology   Inventory   Claim WAN Edges

   100% Config Success   100% Version Compliance   98% WAN Edge Uptime

□	Name	Status	MAC	IP Address	Model	Version	Topology	Insights
□	BuffaloHUB-10.224.8.32	Connected	90:ec:77:35:84:c7	66.129.239.14	SSR130	6.1.4-11.r2	Hub	WAN Edge Insights

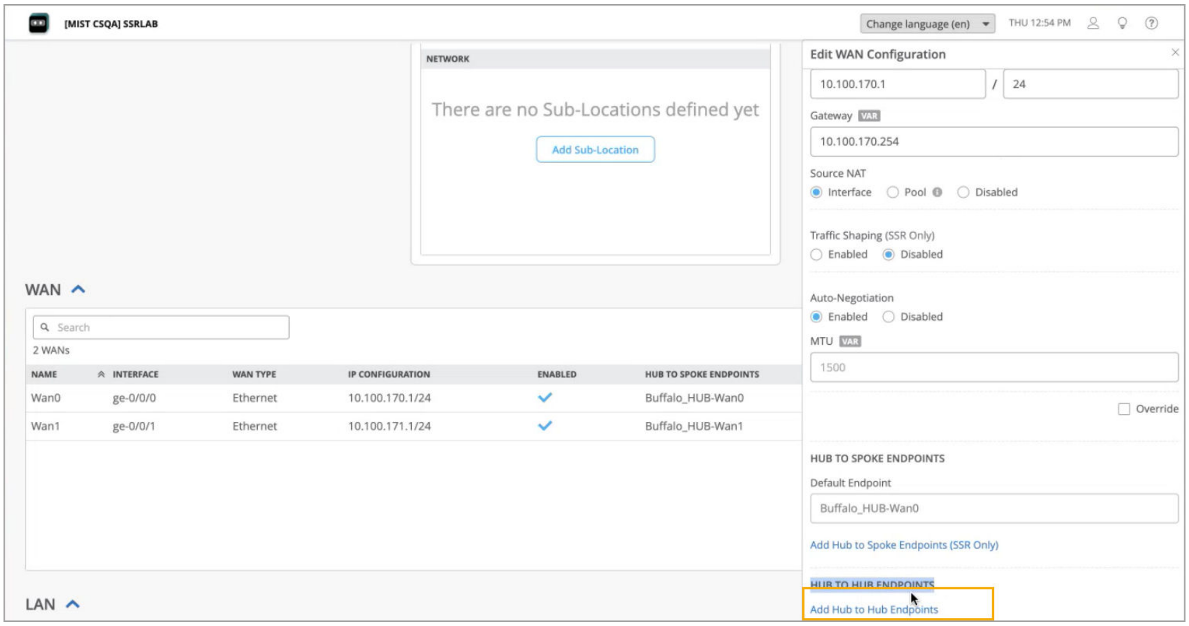
2. On the **WAN Edge >** ***Device-Name*** page, go to Properties section and scroll down to Hub Profile.

3. Click the hub profile link to open the **Hub Profile** page.

4. Scroll-down to WAN section and click a WAN interface which you want to use for overlay.

5. In the **Edit WAN Configuration** window, scroll down to **Hub-to-Hub Endpoints** and click **Add Hub-to-Hub Endpoints** option.

Figure 120: Adding Hub-to-Hub Endpoints



[MIST CSQA] SSRLAB

Change language (en) ▾ THU 12:54 PM

NETWORK

There are no Sub-Locations defined yet

Add Sub-Location

WAN

Search

2 WANs

NAME	INTERFACE	WAN TYPE	IP CONFIGURATION	ENABLED	HUB TO SPOKE ENDPOINTS
Wan0	ge-0/0/0	Ethernet	10.100.170.1/24	✓	Buffalo_HUB-Wan0
Wan1	ge-0/0/1	Ethernet	10.100.171.1/24	✓	Buffalo_HUB-Wan1

LAN

Edit WAN Configuration

10.100.170.1 / 24

Gateway VAR

10.100.170.254

Source NAT

● Interface ○ Pool ○ Disabled

Traffic Shaping (SSR Only)

○ Enabled ● Disabled

Auto-Negotiation

● Enabled ○ Disabled

MTU VAR

1500

□ Override

HUB TO SPOKE ENDPOINTS

Default Endpoint

Buffalo_HUB-Wan0

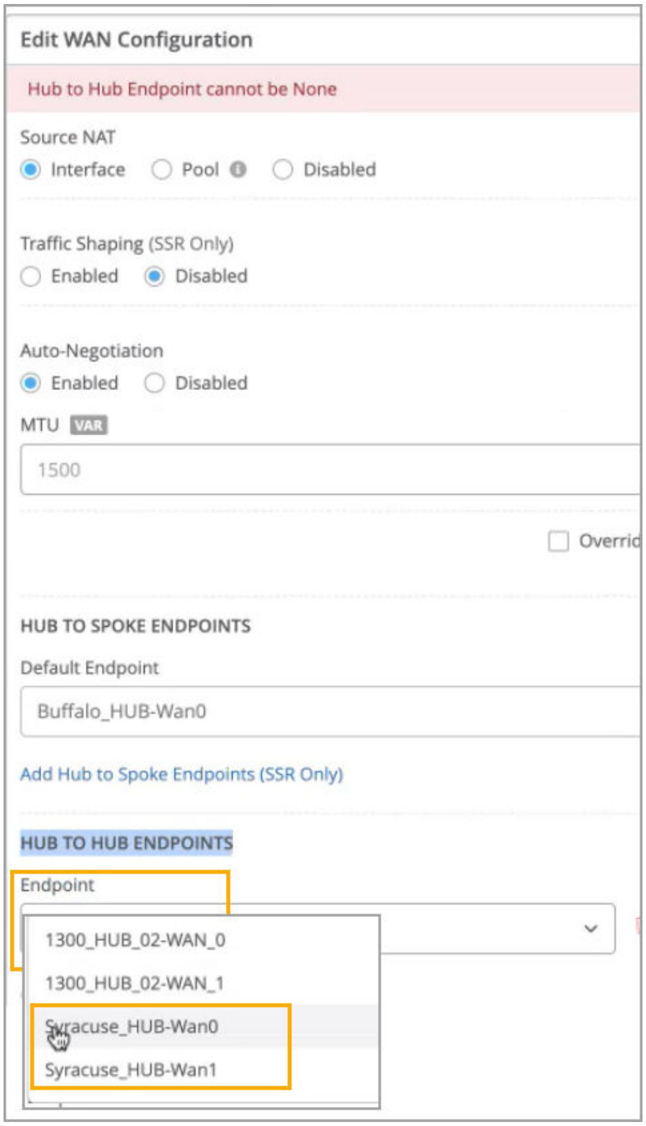
Add Hub to Spoke Endpoints (SSR Only)

HUB TO HUB ENDPOINTS

Add Hub to Hub Endpoints

6. a. Select a hub endpoint point (WAN interface) from the drop-down menu. Choose the WAN interface of the other hub device to establish an overlay connection.

Figure 121: Select WAN Interface for Overlay



Edit WAN Configuration

Hub to Hub Endpoint cannot be None

Source NAT

● Interface ○ Pool ○ Disabled

Traffic Shaping (SSR Only)

○ Enabled ● Disabled

Auto-Negotiation

● Enabled ○ Disabled

MTU VAR

1500

□ Overrid

HUB TO SPOKE ENDPOINTS

Default Endpoint

Buffalo_HUB-Wan0

Add Hub to Spoke Endpoints (SSR Only)

HUB TO HUB ENDPOINTS

Endpoint

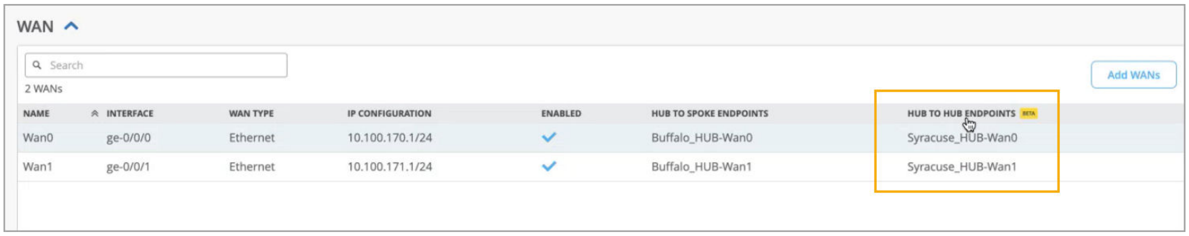
- 1300_HUB_02-WAN_0
- 1300_HUB_02-WAN_1
- Syracuse_HUB-Wan0
- Syracuse_HUB-Wan1

b. Click **Save**. The selected hub endpoint appears under Hub to Hub Endpoints columns in WAN pane.

7. Select another WAN interface and repeat the same procedure to add another endpoint.

8. Now, both endpoints appear under **Hub to Hub Endpoints** columns in WAN pane.

Figure 122: Configured Hub to Hub Endpoints of First Hub Device



NAME	INTERFACE	WAN TYPE	IP CONFIGURATION	ENABLED	HUB TO SPOKE ENDPOINTS	HUB TO HUB ENDPOINTS
Wan0	ge-0/0/0	Ethernet	10.100.170.1/24	✓	Buffalo_HUB-Wan0	Syracuse_HUB-Wan0
Wan1	ge-0/0/1	Ethernet	10.100.171.1/24	✓	Buffalo_HUB-Wan1	Syracuse_HUB-Wan1

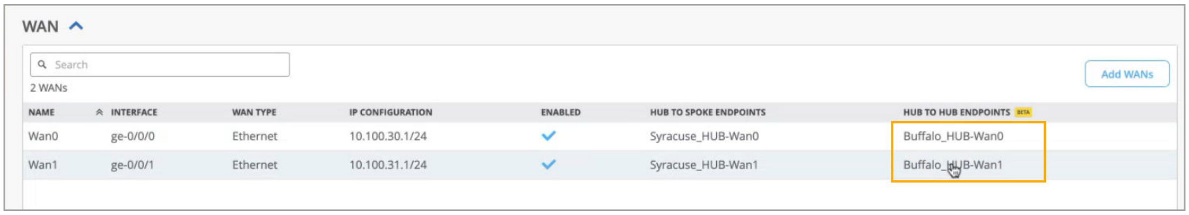
9. Click **Save**.

Now, lets configure WAN interfaces of other hub device to complete the setup as hub endpoints.

1. On Juniper Mist portal, select **WAN Edges** and click the hub device. This is the hub device from which you earlier chose the WAN interface for establishing the overlay.
2. On the **WAN Edge >** ***Device-Name*** page, go to Properties section and scroll down to Hub Profile.
3. Click the hub profile link to open the **Hub Profile** page.
4. Scroll-down to WAN section and click a WAN interface which you want to use for overlay.
5. In the **Edit WAN Configuration** window, scroll down to **Hub-to-Hub Endpoints** and click **Add Hub-to-Hub Endpoints** option.
6. a. Select a hub endpoint point from the drop-down menu. Select the WAN interface of the same hub device that was configured in the prior procedure

   b. Click **Save**. The selected hub endpoint appears under Hub to Hub Endpoints columns in WAN pane.
7. Select another WAN interface and repeat the same procedure to add another endpoint.
8. Now, both endpoints appear under Hub yo Hub Endpoints columns in WAN pane.

Figure 123: Configured Hub to Hub Endpoints of Second Hub Device



NAME	INTERFACE	WAN TYPE	IP CONFIGURATION	ENABLED	HUB TO SPOKE ENDPOINTS	HUB TO HUB ENDPOINTS
Wan0	ge-0/0/0	Ethernet	10.100.30.1/24	✓	Syracuse_HUB-Wan0	Buffalo_HUB-Wan0
Wan1	ge-0/0/1	Ethernet	10.100.31.1/24	✓	Syracuse_HUB-Wan1	Buffalo_HUB-Wan1

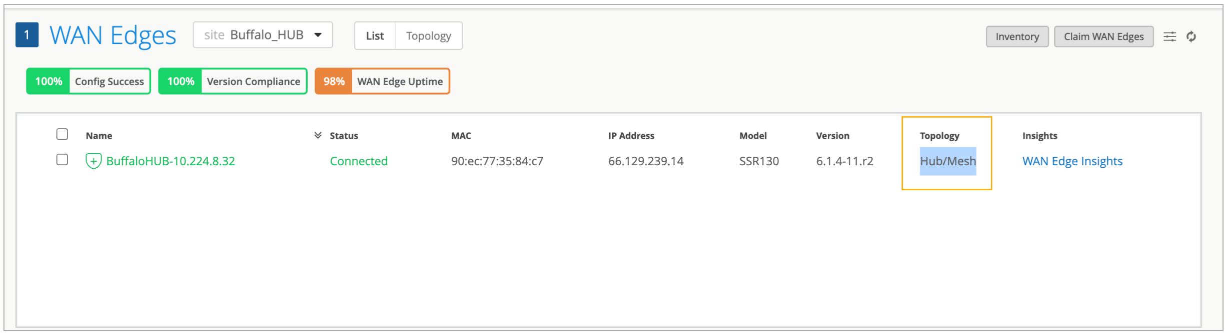
9. Click **Save**.

Verification

On Juniper Mist portal, you can verify the established hub-to-hub overlays by checking the topology of the WAN Edge device:

On the WAN Edge page, the **Topology** column displays **Hub/Mesh**.

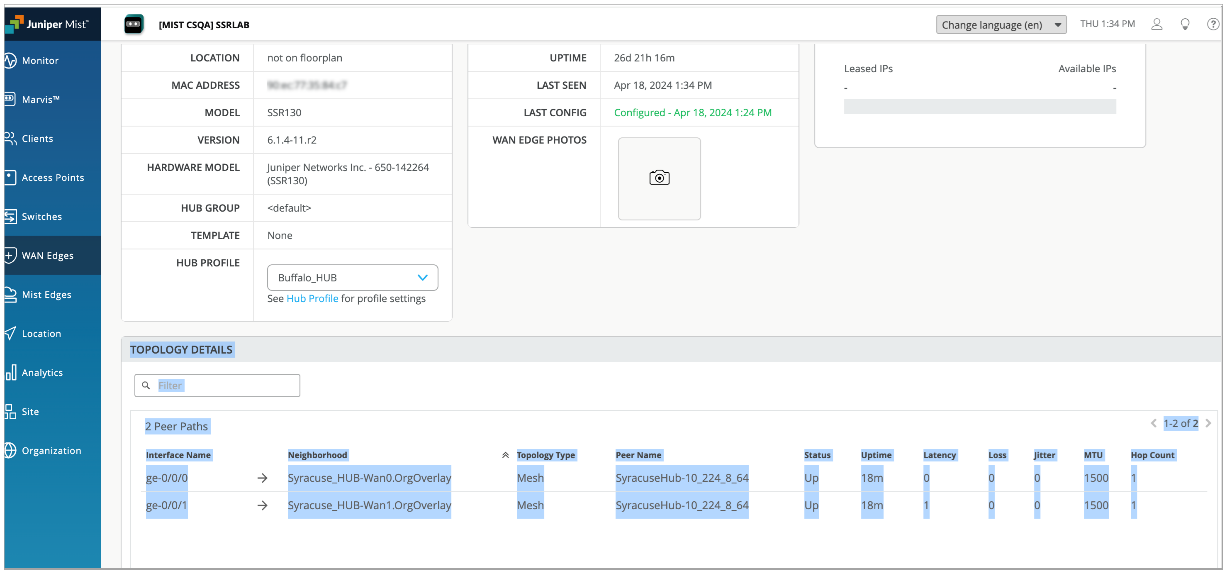
Figure 124: Topology Displaying as Hub/Mesh



Name	Status	MAC	IP Address	Model	Version	Topology	Insights
BuffaloHUB-10.224.8.32	Connected	90:ec:77:35:84:c7	66.129.239.14	SSR130	6.1.4-11.r2	Hub/Mesh	WAN Edge Insights

Go to WAN Edge page of the device and check **Topology Details** section. The portal displays peer details and also connection status.

Figure 125: Hub-to-Hub Overlay Topology Details



LOCATION	not on floorplan
MAC ADDRESS	[redacted]
MODEL	SSR130
VERSION	6.1.4-11.r2
HARDWARE MODEL	Juniper Networks Inc. - 650-142264 (SSR130)
HUB GROUP	<default>
TEMPLATE	None
HUB PROFILE	Buffalo_HUB See Hub Profile for profile settings

UPTIME	26d 21h 16m
LAST SEEN	Apr 18, 2024 1:34 PM
LAST CONFIG	Configured - Apr 18, 2024 1:24 PM
WAN EDGE PHOTOS	

Leased IPs	Available IPs
-	-

TOPOLOGY DETAILS

Filter

2 Peer Paths

1-2 of 2

Interface Name		Neighborhood	Topology Type	Peer Name	Status	Uptime	Latency	Loss	Jitter	MTU	Hop Count
ge-0/0/0	→	Syracuse_HUB-Wan0.OrgOverlay	Mesh	SyracuseHub-10_224_8_64	Up	18m	0	0	0	1500	1
ge-0/0/1	→	Syracuse_HUB-Wan1.OrgOverlay	Mesh	SyracuseHub-10_224_8_64	Up	18m	1	0	0	1500	1

SEE ALSO

WAN Assurance Configuration Overview | 166

Juniper Mist WAN Assurance Configuration Hierarchy | 13

Configure Networks for SRX Series Firewalls | 182

Configure Applications for SRX Series Firewalls | 174

Configure Application Policies on SRX Series Firewalls | 191

Configure WAN Edge Templates for SRX Series Firewalls | 217

Onboard SRX Series Firewalls for WAN Configuration | 259

Configure WAN Edge Templates for SRX Series Firewalls

IN THIS SECTION

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.

NOTE: Configuration done on the WAN edge device through the Mist dashboard overrides any configuration done through the device CLI.

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

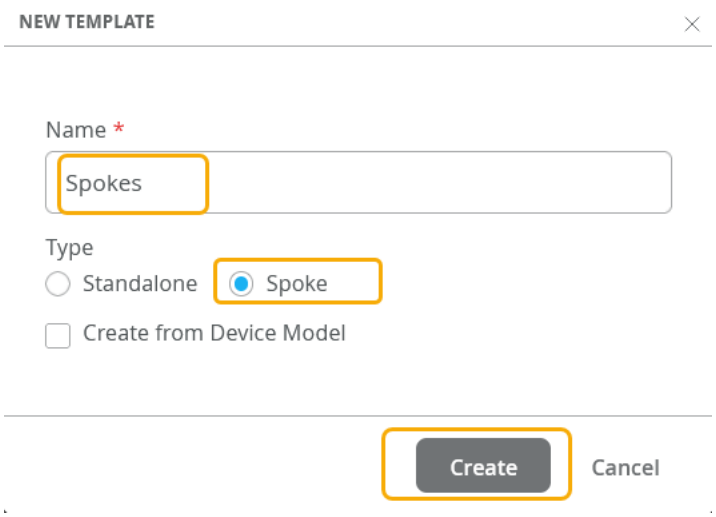
To configure a WAN edge template:

1. In the Juniper Mist™ portal, click **Organization** > **WAN** > **WAN Edge Templates**. A list of existing templates, if any, appears.
2. 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.

3. In the box that appears, enter the name for the template, click **Type** and select Spoke, and then click **Create**.

Figure 126: Select the Template Type



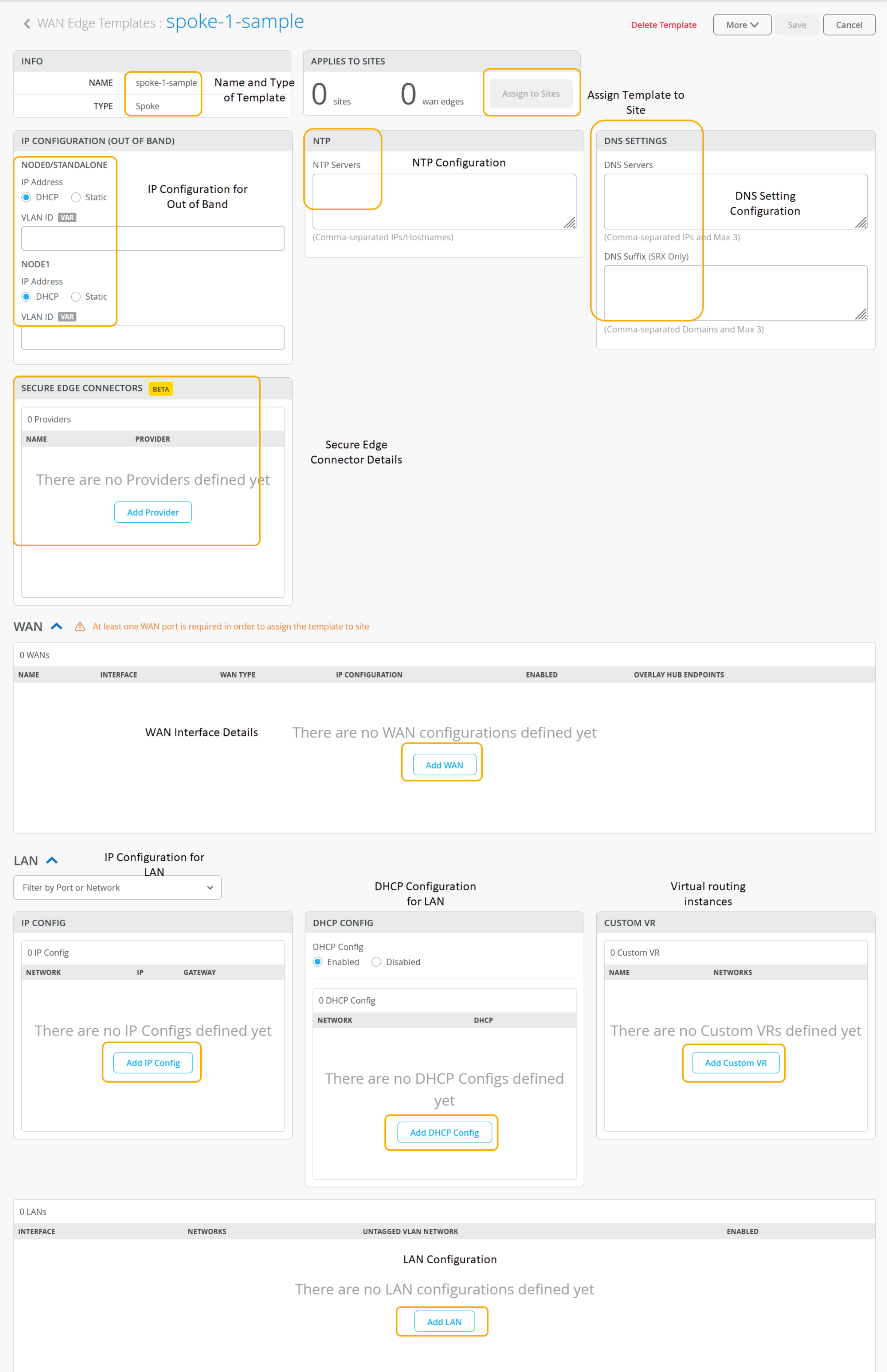
Name *
Spokes

Type
○ Standalone ● Spoke

□ Create from Device Model

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

Figure 127: WAN Edge Template Configuration Options



WAN Edge Templates : spoke-1-sample

INFO

NAME: spoke-1-sample

TYPE: Spoke

Name and Type of Template

APPLIES TO SITES

0 sites 0 wan edges

Assign Template to Site

IP CONFIGURATION (OUT OF BAND)

NODE0/STANDALONE

IP Address: ● DHCP ○ Static

VLAN ID VAR

NODE1

IP Address: ● DHCP ○ Static

VLAN ID VAR

IP Configuration for Out of Band

NTP

NTP Servers

(Comma-separated IPs/Hostnames)

NTP Configuration

DNS SETTINGS

DNS Servers

(Comma-separated IPs and Max 3)

DNS Suffix (SRX Only)

(Comma-separated Domains and Max 3)

DNS Setting Configuration

SECURE EDGE CONNECTORS BETA

0 Providers

NAME	PROVIDER

There are no Providers defined yet

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	ENABLED	OVERLAY HUB ENDPOINTS

There are no WAN configurations defined yet

WAN Interface Details

LAN

IP Configuration for LAN

Filter by Port or Network

DHCP Configuration for LAN

Virtual routing instances

IP CONFIG

0 IP Config

NETWORK	IP	GATEWAY

There are no IP Configs defined yet

DHCP CONFIG

DHCP Config: ● Enabled ○ Disabled

0 DHCP Config

NETWORK	DHCP

There are no DHCP Configs defined yet

CUSTOM VR

0 Custom VR

NAME	NETWORKS

There are no Custom VRs defined yet

0 LANs

INTERFACE	NETWORKS	UNTAGGED VLAN NETWORK	ENABLED

LAN Configuration

There are no LAN configurations defined yet

4. Complete the configurations according to the details provided in Table 35 on page 220.

   Table 35: 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: • Standalone—To manage a standalone device in your site. • 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 "Add WAN Interfaces to the Template" on page 221.

Table 35: WAN Edge Profile Options *(Continued)*

Fields	Description
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 "Add a LAN Interface" on page 228.
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 "Configure Traffic-Steering Policies" on page 234.
Application Policies	Policies to enforce rules for traffic. Define network (source), application (destination), traffic steering policies, and policy action. See "Configure Application Policies" on page 235.
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.

5. Click **Save**.

Add WAN Interfaces to the Template

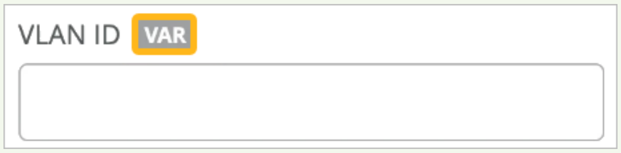
The WAN interface on the spoke corresponds to the WAN interface on hub. That is—Mist creates an IPsec VPN tunnel between WAN interface on the hub to WAN interface on the spoke.
In this task, add two WAN interfaces to the WAN edge template.

To add WAN interfaces to the template:

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

2.

TIP: The fields with this label also display the matching variables (if configured) as you start typing a specific variable in it. This field lists variables from all sites within the organization.



The organization-wide list of variables can be viewed using **GET /api/v1/orgs/:org_id/vars/search?var=***. This list is populated as variables are added under site settings.

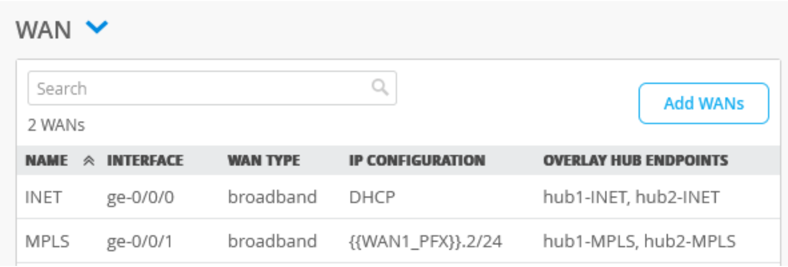
Complete the configuration according to the details provided in Table 36 on page 222.

Table 36: 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 • • **IP Address**={{WAN1_PFX}}.2 • **Prefix Length**=24 • **Gateway**={{WAN1_PFX}}.1
Source NAT	Interface	Interface
Overlay Hub Endpoint (generated automatically).	hub1-INET, hub2-INET (BFD profile Broadband)	hub1-MPLS and hub2-MPLS
MTU	Enter an MTU value between 256 -9192. Default is 1500.	Enter an MTU value between 256 -9192. Default is 1500.

Figure 128 on page 223 shows list of WAN interfaces you created.

Figure 128: WAN Interfaces Summary



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

Configure LTE Interface

Juniper Mist SD-WAN allows organizations to integrate LTE connectivity seamlessly. LTE connectivity provides an alternate path for multipath routing; either as a primary path in locations that have no access to circuits or as a path of last resort in the event that the primary circuit has failed.

For example: In a retail store with a primary MPLS connection for business-critical applications. Juniper Mist SD-WAN can add an LTE link as a backup. If the MPLS link experiences issues, Juniper Mist dynamically switches traffic to the LTE link. This ensures continuous connectivity and minimizes disruptions.

On SRX Series Firewalls, the LTE Mini-Physical Interface Module (Mini-PIM) provides wireless WAN support on the SRX300 Series and SRX550 High Memory Services Gateways. The Mini-PIM contains an integrated modem and operates over 3G and 4G networks. The Mini-PIM can be installed in any of the Mini-PIM slots on the devices. See https://www.juniper.net/documentation/us/en/hardware/lte-mpim-install/topics/task/lte-mpim-hardware-intalling.html for installing LTE Mini-PIM on an SRX Series Firewall.

To have LTE link for Juniper Mist SD-WAN, you need an LTE interface setup on your Session Smart Routers and SRX Series Firewalls and insert the Subscriber Identity Module (SIM) in the LTE card.

To add an LTE interface as WAN link:

1. Scroll down to the WAN section and click **Add WAN** to open the Add WAN Configuration pane.
2. Enter the details for the interface configuration

Table 37: LTE Interface Configuration

Fields	Values
Name	Name of the LTE interface
Description	Description of the interface.
WAN Type	LTE
Interface	cl-1/0/0. Use the interface `cl-1/0/0` when the LTE Mini-PIM module is inserted in slot 1.
LTE APN	Enter the access point name (APN) of the gateway router. The name can contain alphanumeric characters and special characters. (Optional for SRX Series Firewalls and mandatory for Session Smart Routers)
LTE Authentication	Select the authentication method for the APN configuration: • PAP—Select this option to use Password Authentication Protocol (PAP) as the authentication method. Provide User name and Password. • CHAP—Select this option to use Challenge Handshake Authentication Protocol (CHAP) authentication as the authentication method. Provide User name and Password. • None (Default)—Select this option if you do not want to use any authentication method.
Source NAT	Select Source NAT options: • Interface—NAT using source interface. • Pool—NAT using defined IP address pool. • Disabled—Disable source NAT

Table 37: LTE Interface Configuration *(Continued)*

Fields	Values
Traffic Shaping	Select **Enabled** or **Disabled**. (Required for Session Smart Routers only)
Auto Negotiation	Select **Enabled** or **Disabled**.
MTU	Enter an MTU value between 256 -9192. Default is 1500.

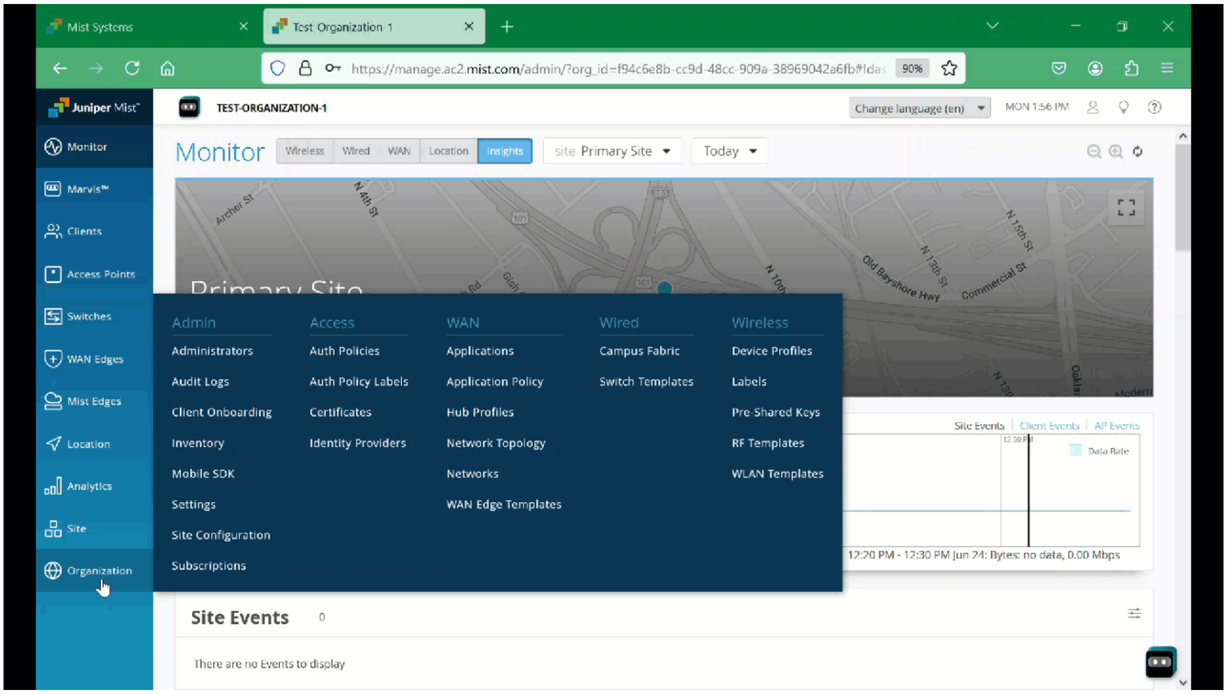
3. Click **Save**.

NOTE: On SRX Series Firewalls, when you create a WAN Edge template using device-specific WAN Edge templates option, the LTE interface configuration is included by default in the template.

The template provides device-specific, pre-configured WAN interfaces, LAN interfaces, a traffic steering policy, and an application policy. All you have to do is name the template and select the device type.

Figure 129 on page 226shows a sample of SRX320 template that includes default LTE configuration in WAN section of the template.

Figure 129: WAN Edge Template Sample



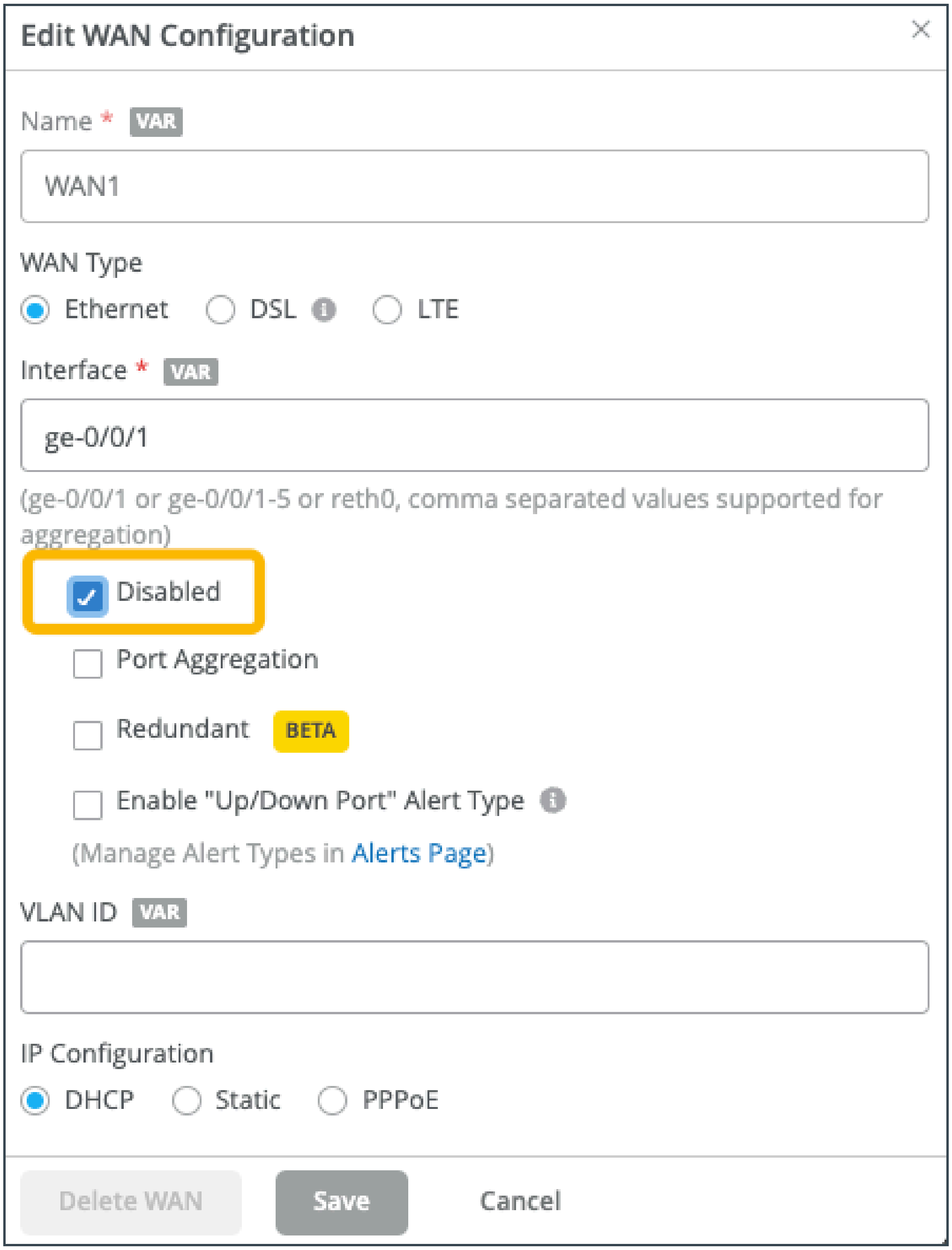
Disable WAN Edge Ports

There are many reasons why it might be necessary to disable a WAN Edge port. In debugging scenarios, for example, disabling a port and then enabling it again can trigger processes to reset, which can help resolve issues.

You may also want to disable a port when you are staging a connection, but are not quite ready to bring the connection into service, or if you've identified a malicious or problematic device, you can disable the port to quickly disable the device until the device can be removed or repaired.

To disable WAN Edge ports:

1. Navigate to **Organization** > **WAN Edge Templates**.
2. Click the appropriate WAN Edge Template.
3. Scroll down to the WAN or LAN section and click the appropriate WAN Edge.
4. In the **Interface** section of the window, select the **Disabled** checkbox. This will administratively disable the WAN Edge device port for the specified interface.



Edit WAN Configuration

Name * VAR

WAN1

WAN Type

● Ethernet ○ DSL ○ LTE

Interface * VAR

ge-0/0/1

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

☑ Disabled

□ Port Aggregation

□ Redundant BETA

□ Enable "Up/Down Port" Alert Type

(Manage Alert Types in Alerts Page)

VLAN ID VAR

IP Configuration

● DHCP ○ Static ○ PPPoE

5. Click **Save** at the bottom of the window to save the changes.
6. Click **Save** at the top right-corner of the template page.

   This option is part of interface configuration. If you use this option to disable an aggregated Ethernet (AE) interface or redundant Ethernet (reth) interface, all member links are disabled

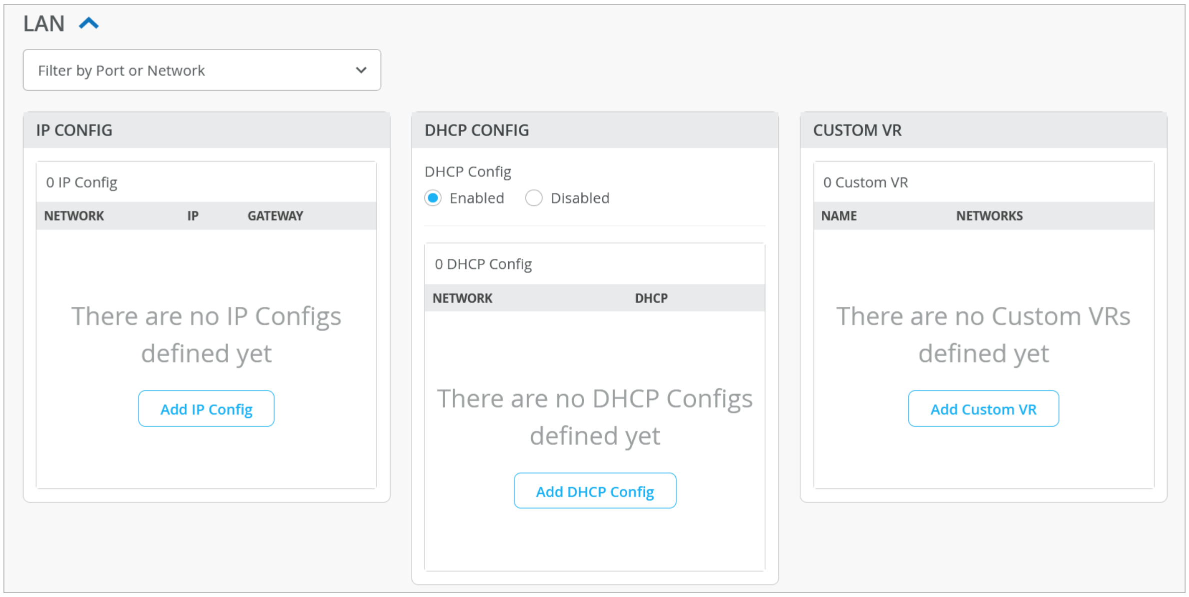
Add a LAN Interface

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

To add a LAN interface:

1. Scroll down to the LAN pane and click **Add LAN** to open the Add LAN Configuration panel.

Figure 130: Add LAN Interfaces to the Template



LAN

Filter by Port or Network

IP CONFIG

0 IP Config

NETWORK	IP	GATEWAY

There are no IP Configs defined yet

DHCP CONFIG

DHCP Config
● Enabled ○ Disabled

0 DHCP Config

NETWORK	DHCP

There are no DHCP Configs defined yet

CUSTOM VR

0 Custom VR

NAME	NETWORKS

There are no Custom VRs defined yet

2. Configure LAN interfaces.

   The LAN configuration section includes the components for IP Configuration, DHCP Configuration, and Custom VR. The LAN configuration section enables more flexibility by allowing you to override each configuration component (such as IP configuration) separately without touching other components.

   The LAN Configuration section also provides a filter for you to easily search for configurations per port or network.

   - IP configuration
     - **Network**—Select an available network from the drop-down.
     - **IP Address**—IPv4 address and prefix length for the interface.
     - **Prefix Length**—Prefix length for the interface.
     - **Redirect Gateway**—IP address of redirect gateway for Session Smart Routers only.

- DHCP configuration—Select **Enabled** option to use DHCP service for assigning IP addresses to the LAN interface.
  - **Network**—Select the network from the list of available networks.
  - **DHCP type**—Select DHCP Server or DHCP Relay. If you chose DHCP server, enter the following options:
    - **IP Start**—Enter the beginning IP address of the desired IP address range.
    - **IP End**—Enter the ending IP address.
    - **Gateway**—Enter the IP address of the network gateway.
    - **Maximum Lease Time**—Specify a maximum lease time for the DHCP addresses. Supported DHCP lease duration ranges from 3600 seconds (1 hour) to 604800 seconds (1 week).
    - **DNS Servers**—Enter IP address of the Domain Name System (DNS) server.
    - **Server Options**—Add following options:
      - **Code**—Enter the DHCP option code you want to configure the server. The Type field will be populated with the associated value. For example: If you select Option 15 (domain-name), the **Type** field displays FQDN. You must enter the **Value** associated to the Type.
    - Static Reservations—Use this option if you want to statically reserve a DHCP address. Static DHCP IP address reservation involves binding a client MAC address to a static IP address from the DHCP address pool. The following options are available:
      - **Name**—A name that identifies the configuration.
      - **MAC Address**—The MAC address to be used in the reservation.
      - **IP Address**—The IP address to be reserved.
- Custom VR configuration.
  - **Network**—Select an available network from the drop-down.
  - **Name**—Enter the name for the routing instance.

3. Complete the configuration according to the details provided in Table 38 on page 230.

> **TIP**: The fields with this label also display the matching variables (if configured) as you start typing a specific variable in it. This field lists variables from all sites within the organization.

VLAN ID VAR

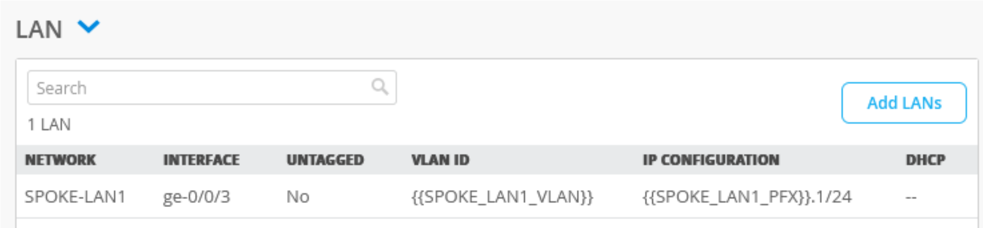
The organization-wide list of variables can be viewed using **GET /api/v1/orgs/:org_id/vars/search?var=***. This list is populated as variables are added under site settings.

Table 38: Sample LAN Interface Configuration

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

Figure 131 on page 230 shows the list of LAN interface you created.

Figure 131: Summary of LAN Interface



1 LAN

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

Configure LACP on Redundant Ethernet Interfaces (BETA)

Link Aggregation Control Protocol (LACP) is an IEEE standard protocol that defines how a group of interfaces operate. With LACP, devices send LACP data units to eachother to establish connection. The devices do not attempt to establish a connection if they are unable to do so, which prevents issues from occuring during the link aggregation setup process such as misconfigured Link Aggregation Group (LAG) settings. You can configure LACP on the Redundant Ethernet (Reth) Interfaces on your SRX Series Firewalls.

To configure LACP on Redundant Ethernet Interfaces:

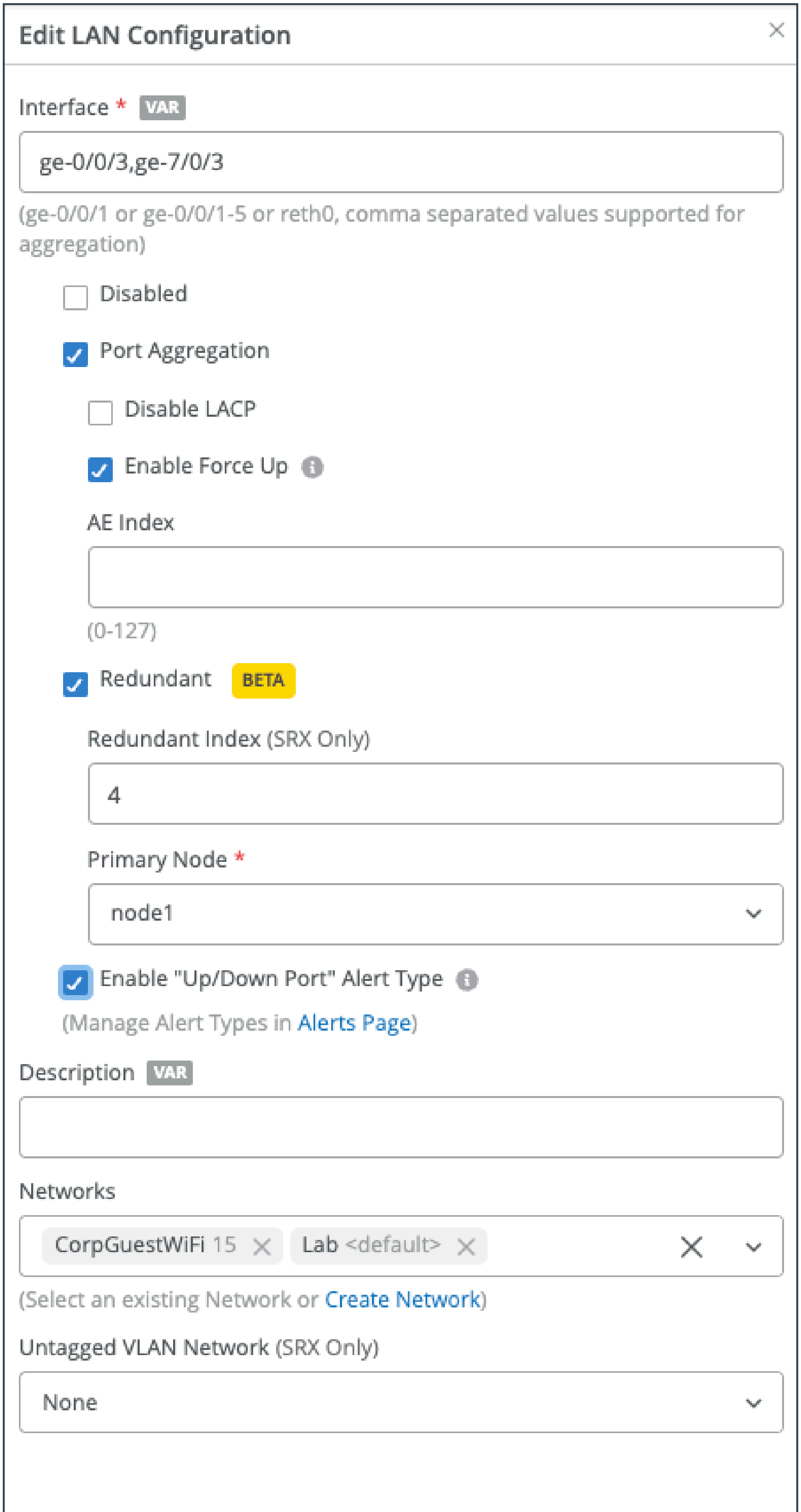
1. From the left menu of the Juniper Mist portal, select **Organization** > **WAN Edge Templates.**
2. Select the WAN Edge Template containing the Redundant Ethernet Interfaces you want to configure LACP for.
3. Scroll down to the LAN pane and click **Add LAN** to open the **Add LAN Configuration** panel, or click on an existing LAN to open the **Edit LAN Configuration** panel.
4. Configure the following fields:

Table 39: Sample LACP on Redundant Ethernet Interfaces Configuration

Fields	LAN Interface Configuration
Interface	List the redundant interfaces, separated by a comma.
Port Aggregation	Select this checkbox to enable LACP on the Reth interfaces.
Enable Force Up	Selecting this checkbox sets the state of the interface as "up" when the peer has limited LACP capacity. Use Case: When a device connected to this aggregate ethernet (AE) interface port is using Zero-Touch Provisioning (ZTP) for the first time, it will not have LACP configured on the other end. **NOTE**: Selecting this enables Force Up on one of the interfaces in the bundle only.
Redundant (BETA)	Select this checkbox to enable redundancy. The physical interfaces mentioned in the LAN configuration will be configured into a redundancy group and under a reth interface (redundant parent).

Table 39: Sample LACP on Redundant Ethernet Interfaces Configuration *(Continued)*

Fields	LAN Interface Configuration
Redundant Index (SRX) Only	This is the index for the reth interface. For example, an index of 4 would configure the redundant interface reth4.
Primary Node	This indicates which node is the primary node in a redundancy group, where one of the nodes is primary and the other is secondary so that a node can take over for the other in the event of interface failover.
Enable "Up/Down Port" Alert Type	Enable this alert type to allow the user to receive alerts when the port transitions from up to down or vice-versa. This also requires the user to enable **Critical WAN Edge Port Up/Down** under **Monitor** > **Alerts** > **Alerts Configuration**.



Edit LAN Configuration

Interface * VAR

ge-0/0/3,ge-7/0/3

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

□ Disabled

☑ Port Aggregation

□ Disable LACP

☑ Enable Force Up

AE Index

(0-127)

☑ Redundant BETA

Redundant Index (SRX Only)

4

Primary Node *

node1

☑ Enable "Up/Down Port" Alert Type

(Manage Alert Types in Alerts Page)

Description VAR

Networks

CorpGuestWiFi 15 ✕ Lab <default> ✕

(Select an existing Network or Create Network)

Untagged VLAN Network (SRX Only)

None

5. At the bottom of the panel, click **Add** or **Save** to save the configuration.

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:

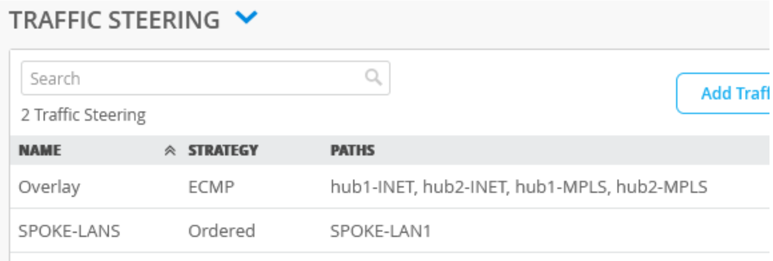
1. In the Juniper Mist portal, scroll down to the Traffic Steering section, and click **Add Traffic Steering** to display the Traffic Steering configuration pane.
2. Complete the configuration according to the details provided in Table 40 on page 234.

   Table 40: 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 • **Network**—SPOKE-LAN1	• **Type**— WAN • **Network** — • hub1-INET • hub2-INET • hub1-MPLS • hub2-MPLS

   Figure 132 on page 235 shows the list of traffic-steering policies you created.

Figure 132: Traffic-Steering Policies Summary



TRAFFIC STEERING

2 Traffic Steering

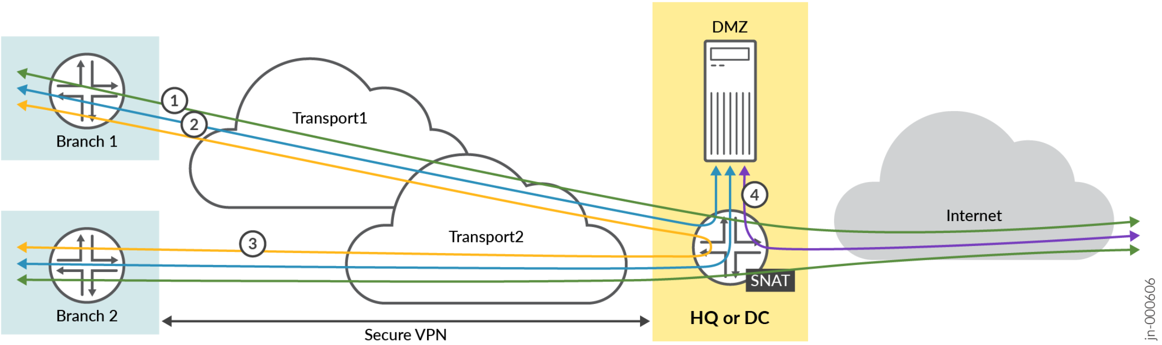
NAME	STRATEGY	PATHS
Overlay	ECMP	hub1-INET, hub2-INET, hub1-MPLS, hub2-MPLS
SPOKE-LANS	Ordered	SPOKE-LAN1

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 Figure 133 on page 235. The image depicts a basic initial traffic model for a corporate VPN setup (third spoke device and second hub device are not shown).

Figure 133: 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: This may not be feasible in the real world except on expensive MPLS networks with managed IPs. Managed IPs send traffic directly to the other spoke. This type of traffic usually flows through a hub device

- 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:

1. In the Juniper Mist portal, scroll down to Application Policy section, click **Add Policy** to add a new policy in the policy list.
2. Complete the configuration according to the details provided in Table 41 on page 236.

Table 41: 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

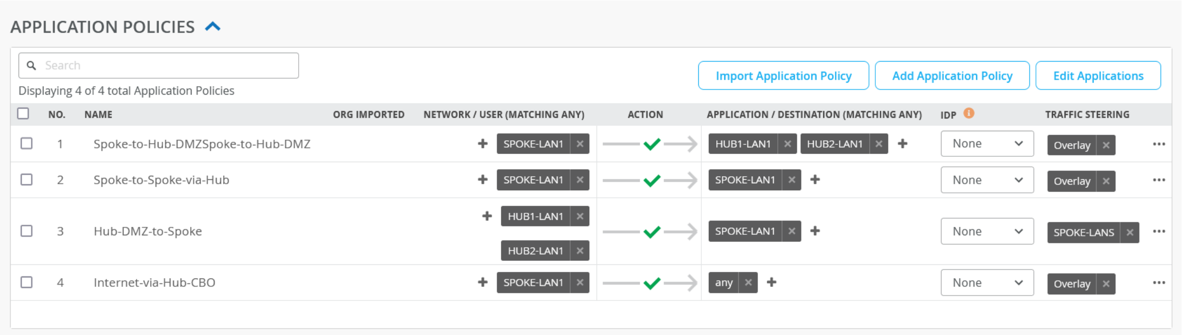
NOTE:

- Juniper Mist cloud evaluates and applies application policies in the order in which the policies are listed. You can move a given policy up or down in the order by clicking the ellipsis (...) button.

- You must create steering policies to use with SRX Series Firewalls.

Figure 134 on page 237 shows the list of application policies you created.

Figure 134: Application Policy Summary



Displaying 4 of 4 total Application Policies

☐	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
☐	1	Spoke-to-Hub-DMZSpoke-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

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

   The default security configuration 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:

```
[edit]
user@host# set security zones security-zone HUB1-LAN1 host-inbound-traffic system-services
ping
```

Configure Device-Specific WAN Edge Templates

IN THIS SECTION

Device configuration is simplified with WAN Edge Templates following your device onboarding process. These WAN Edge templates can be customized to unique deployments across all edge devices. Juniper Networks Mist AI is positioned uniquely in the industry as Mist AI WAN Edge templates can be applied to any model, regardless of vendor. Additionally, WAN Edge templates can mix and match different models under a single template, streamlining your configuration and deployment phase.

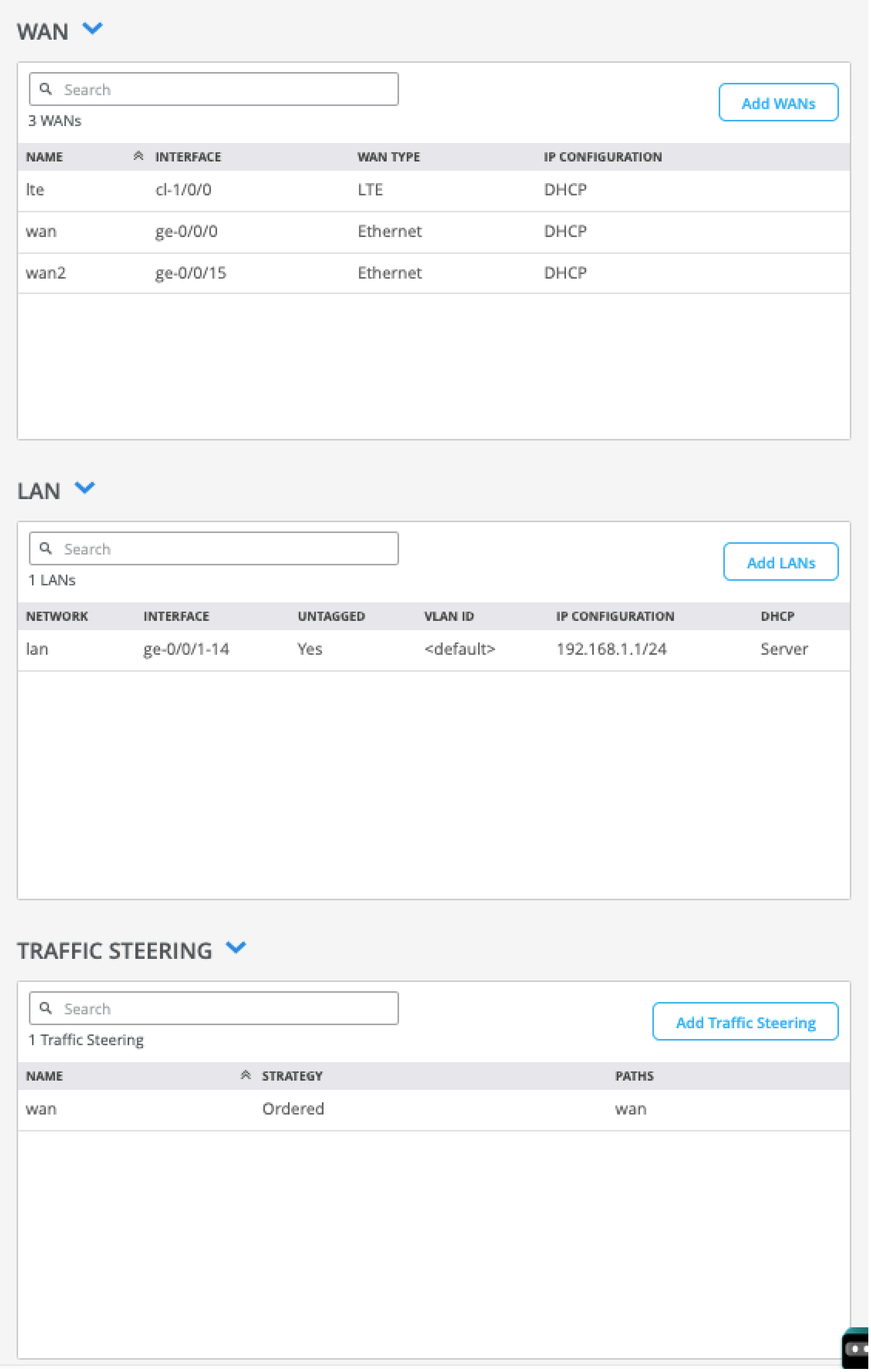
To manually configure your WAN Edge templates for the SRX Series Firewalls, see "Configure a WAN Edge Template" on page 218.

Device-Specific WAN Edge Templates

There is a significant benefit to leveraging select Juniper Networks hardware with Mist AI SD-WAN. Configuration is simplified for many Juniper Networks® SRX Series Firewalls, which have device-specific templates that automatically assign WAN and LAN interfaces and define LAN Networks for connectivity.

These templates are unique for each device model. With zero manual input after device selection and naming the WAN Edge, a user's specified WAN Edge device is pre-populated with the values. Figure 135 on page 239 shows that the SRX Series WAN Edge template generating several values, including Ethernet interfaces for **LAN** and **WAN** with relevant **DHCP** and **IP** values.

Figure 135: Sample of SRX Series WAN Edge Template



WAN

3 WANs

NAME	INTERFACE	WAN TYPE	IP CONFIGURATION
lte	cl-1/0/0	LTE	DHCP
wan	ge-0/0/0	Ethernet	DHCP
wan2	ge-0/0/15	Ethernet	DHCP

LAN

1 LANs

NETWORK	INTERFACE	UNTAGGED	VLAN ID	IP CONFIGURATION	DHCP
lan	ge-0/0/1-14	Yes	<default>	192.168.1.1/24	Server

TRAFFIC STEERING

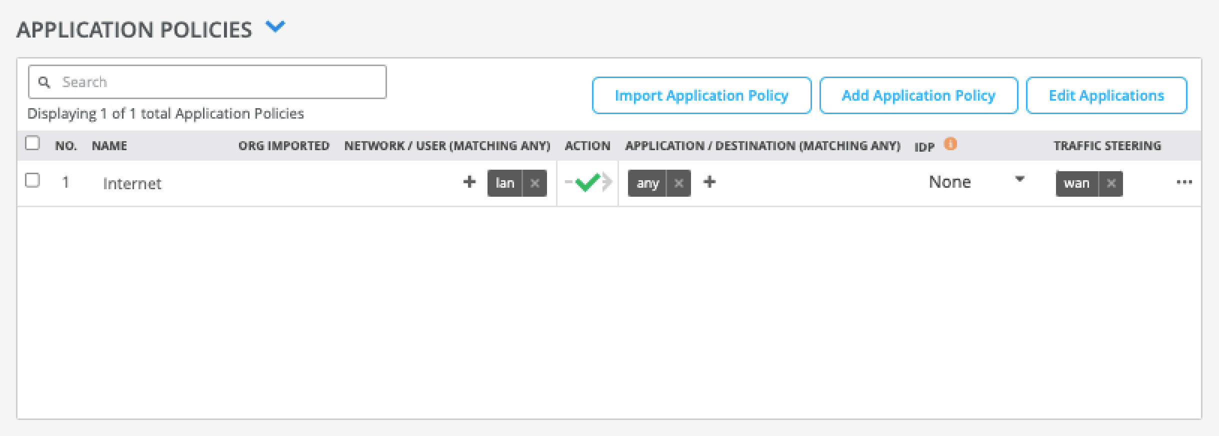
1 Traffic Steering

NAME	STRATEGY	PATHS
wan	Ordered	wan

Additionally, the Juniper Mist portal populates a traffic steering policy. This enables Juniper Mist to send traffic over our **wan** connection to an **any** Mist Application with a quad zero catch-all destination.

When you apply a WAN Edge template, you can notice that application policies, networks, and applications receive automatic updates. Figure 136 on page 240 shows a sample of application policies.

Figure 136: Application Policies After Applying WAN Edge Template



Displaying 1 of 1 total Application Policies

□	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
□	1	Internet		+ lan ×	✓	any × +	None	wan ×

Juniper Mist AI SD-WAN includes the following device models with pre-configured WAN Edge templates for SRX Series Firewalls:

- SRX300
- SRX320-POE
- SRX320
- SRX340
- SRX345
- SRX380
- SRX550M
- SRX1500
- SRX1600*
- SRX4100
- SRX4200
- SRX4600

- SRX2300*
- SRX4300*

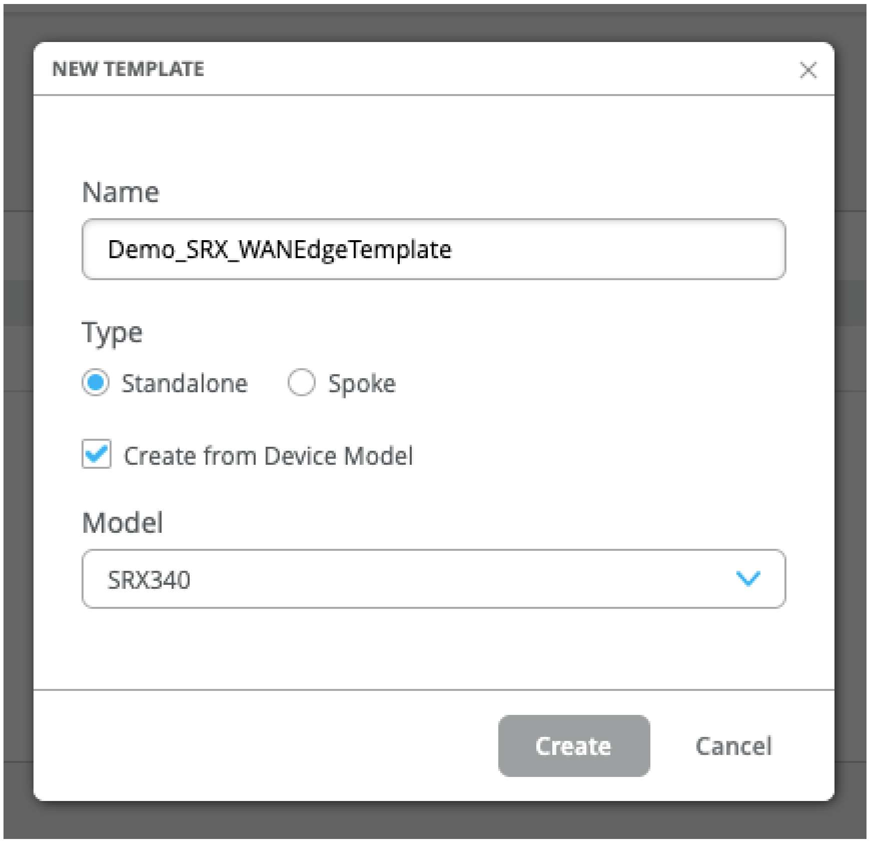
* Indicates planned Juniper Mist AI WAN support for new model later in 2024.

The WAN Edge device specific templates provide basic network configuration in a single step and allow for re-usable and consistent configuration for each Session Smart Router and SRX Series Firewall device you deploy. The template provides device-specific, pre-configured WAN interfaces, LAN interfaces, a traffic steering policy, and an application policy. All you have to do is name the template and select the device type.

To select a device-specific WAN Edge template:

1. In the Juniper Mist portal, select **Organization > WAN > WAN Edge Templates**.
2. Select **Create Template** in the upper right corner to open a new template page.
3. Enter the name for the template.
4. Click the **Create from Device Model** check-box.
5. Select your device model from the drop-down box.

Figure 137: Configure Device-Specific WAN Edge Template



NEW TEMPLATE

Name

Demo_SRX_WANEdgeTemplate

Type

● Standalone ○ Spoke

☑ Create from Device Model

Model

SRX340

6. Click **Create**.

Juniper Mist UI displays the completed device template. You now have a working WAN Edge template that you can apply to many sites and devices across your organization.

Assign to Site

With your template set up, you need to save and assign it to the site where your WAN edge device will be deployed.

1. Click the **Assign to Site** button at the top of the template page.
2. Select a site from the list where you want the template applied.
3. Click **Apply**.
4. Finally, all that remains is to associate the device with your site, see "Onboard SRX Series Firewalls for WAN Configuration" on page 259.

SEE ALSO

WAN Assurance Configuration Overview | 166
Juniper Mist WAN Assurance Configuration Hierarchy | 13
Configure Networks for SRX Series Firewalls | 182
Configure Applications for SRX Series Firewalls | 174
Configure Application Policies on SRX Series Firewalls | 191
Configure Hub Profiles for SRX Series Firewalls | 197
Onboard SRX Series Firewalls for WAN Configuration | 259

Routing Configuration on SRX Series Firewalls

IN THIS SECTION

Configure BGP Groups

You can configure BGP (Border Gateway Protocol) and add their BGP neighbors. You can also add and modify peer-based advertisement and redistribution rules

To configure a BGP group:

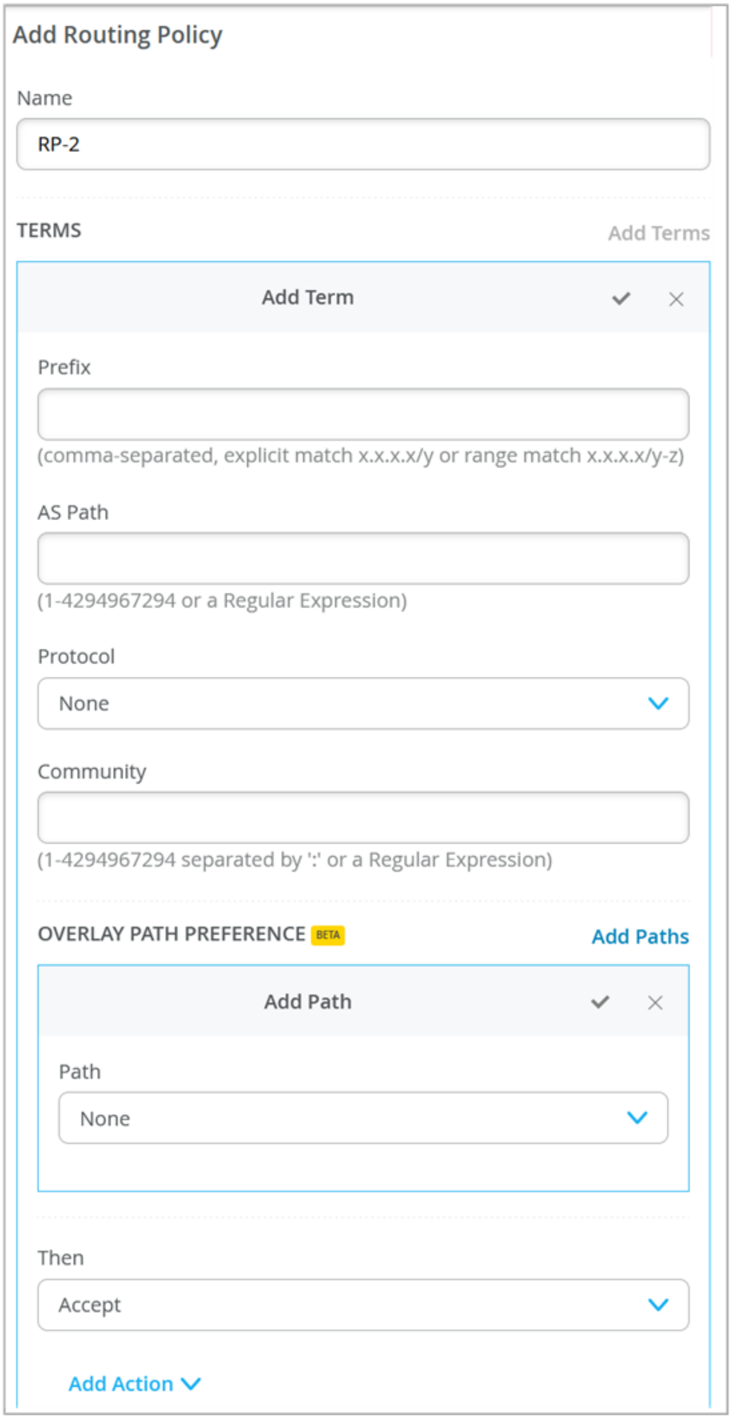
1. In the Juniper Mist™ portal, click **Organization** > **WAN** > **WAN Edge Templates**.

2. Create a new template or click an existing template to modify it.

3. In the Templates page, scroll down to Routing pane and click **Add BGP Group**.

4. In the Add BGP Group window, add details for the BGP group.

Figure 138: Add BGP Group



Add Routing Policy

Name

RP-2

TERMS

Add Term

Prefix

(comma-separated, explicit match x.x.x.x/y or range match x.x.x.x/y-z)

AS Path

(1-4294967294 or a Regular Expression)

Protocol

None

Community

(1-4294967294 separated by ':' or a Regular Expression)

OVERLAY PATH PREFERENCE BETA

Add Path

Path

None

Then

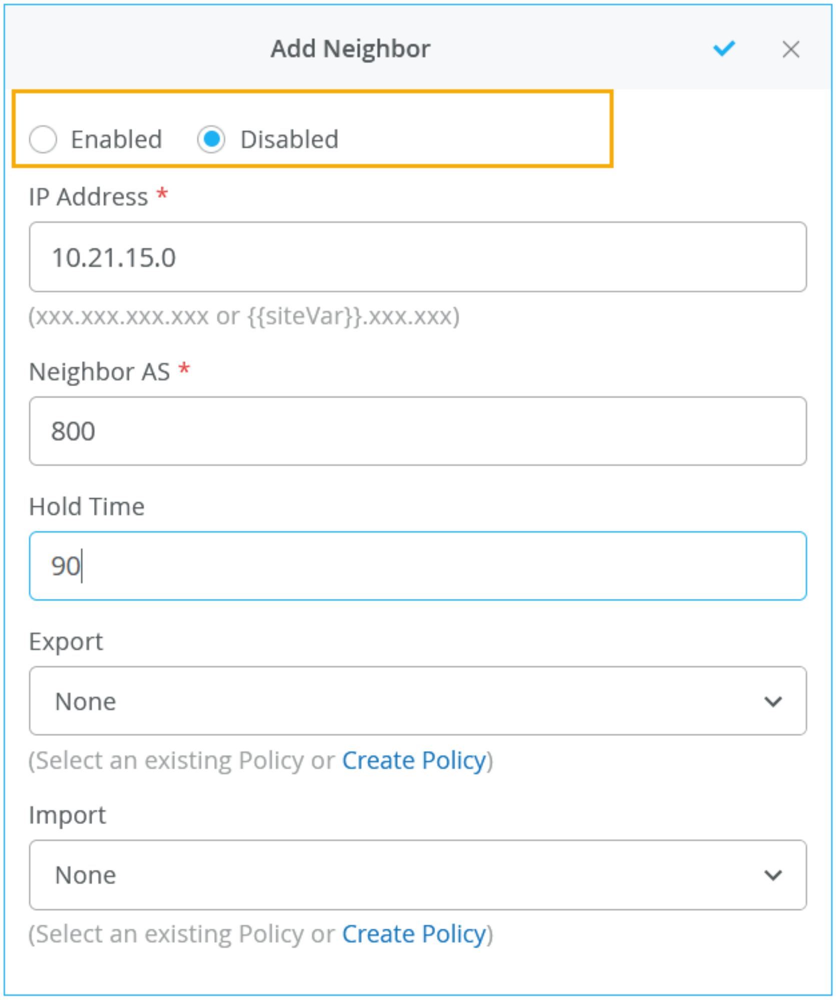
Accept

- Name—Name of the BGP group.
- Peering Network —Select Peering Network as **WAN** or **LAN**.
- BFD —Select **Enabled** or **Disabled**.

- Type —Select **Internal** or **External**.
- Local AS —Specify the local autonomous system (AS) number.
- Hold Time —Specify the hold-time value to use when negotiating a connection with the peer.
- Graceful Restart Time —Specify graceful restart for BGP. Graceful restart allows a routing device undergoing a restart to inform its adjacent neighbors and peers of its condition
- Authentication Key —Configure an MD5 authentication key (password). Neighboring routing devices use the same password to verify the authenticity of BGP packets sent from this system
- Click drop-down for **Export** or **Import** and select an existing routing policy or click **Create Policy**.
  - In the Routing Policy window,you can add or edit the policy for the overlay path preference.
    - **Name**—Enter the name of the policy.
    - **Add Terms**—Enter the policy conditions such as prefix, autonomous system [AS] path regular expressions, protocols, and community.
    - **Then**—Select an action (Accept or Reject) to apply when the condition is fulfilled. Enable one of the following preference for the accepted path:
      - Append Community
      - Exclude Community
      - Set Community
      - Prepend AS Path
      - Exclude AS Path
      - Set Local Preference
      - Add Target VRs
    - Click **Add** to add to save the routing policy.

5. On the Add BGP Group window, for the **Export** or **Import** field, select the routing policy you created from the drop-down.
6. In **Neighbors** pane, click **Add Neighbors**

Figure 139: BGP Group- Add Neighbors



Add Neighbor ✓ ×

○ Enabled ● Disabled

IP Address *

10.21.15.0

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

Neighbor AS *

800

Hold Time

90

Export

None

(Select an existing Policy or Create Policy)

Import

None

(Select an existing Policy or Create Policy)

.

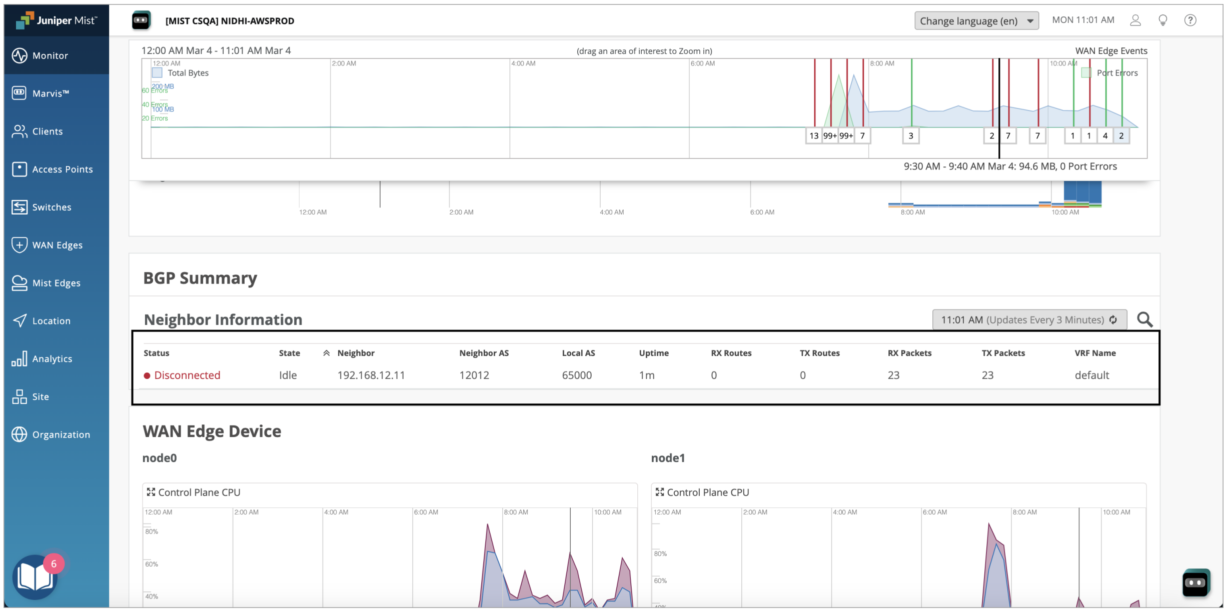
- Select **Enabled** or **Disabled** to administratively enable or disable a BGP neighbor.
- IP address —Enter the IP address of the neighbor device.
- Neighbor AS —Enter the neighbor node AS.
- Hold Time —Specify the hold-time value to use when negotiating a connection with the neighbor device.
- Type —Click drop-down for **Export** or **Import** and select an existing routing policy or click **Create Policy**.

7. Select the check-box in **Add Neighbors** pane to add the neighbor.

8. Click **Save**.

You can view the BGP neighbors details in **BGP Summary** section of **Monitor > Insights** page.

Figure 140: BGP Neighbor Information



BGP Summary

Neighbor Information

11:01 AM (Updates Every 3 Minutes)

Status	State	Neighbor	Neighbor AS	Local AS	Uptime	RX Routes	TX Routes	RX Packets	TX Packets	VRF Name
● Disconnected	Idle	192.168.12.11	12012	65000	1m	0	0	23	23	default

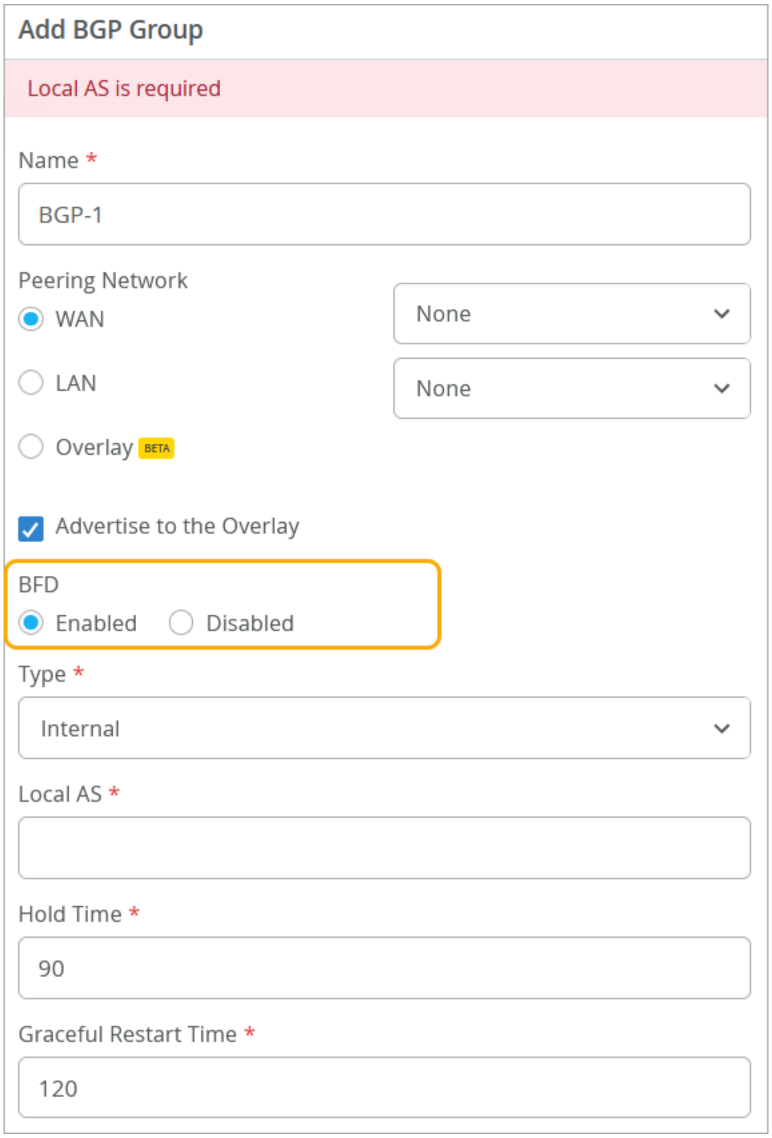
WAN Edge Device

Configure BFD for BGP Sessions

The Bidirectional Forwarding Detection (BFD) protocol is a simple Hello mechanism that detects failures or faults between network forwarding elements that share a link. Hello packets are sent at a specified, regular interval. When the routing device stops receiving a reply after a specified interval, a neighbor failure is detected . The failure detection timers for BFD provide faster detection, as they have shorter time limits than that of the default failure detection mechanisms for BGP.

To enable or disable BFD for the BGP sessions on a Session Smart Router deployed as a WAN Edge device:

1. In the Mist portal, navigate to **Organization** > **WAN Edge Templates** > ***WAN Edge Name***.
2. From the **BGP** section, click on an existing BGP Group, or click **Add BGP Group** to add a new one.
3. In the **Add BGP Group** window, Under **BFD**, select **Enabled** or **Disabled** depending on your network needs.



Add BGP Group

Local AS is required

Name *

BGP-1

Peering Network

● WAN — None

○ LAN — None

○ Overlay BETA

☑ Advertise to the Overlay

BFD

● Enabled ○ Disabled

Type *

Internal

Local AS *

Hold Time *

90

Graceful Restart Time *

120

4. Configure any other necessary setting for your BGP Group, such as the interval, then click **Add** at the bottom of the window.

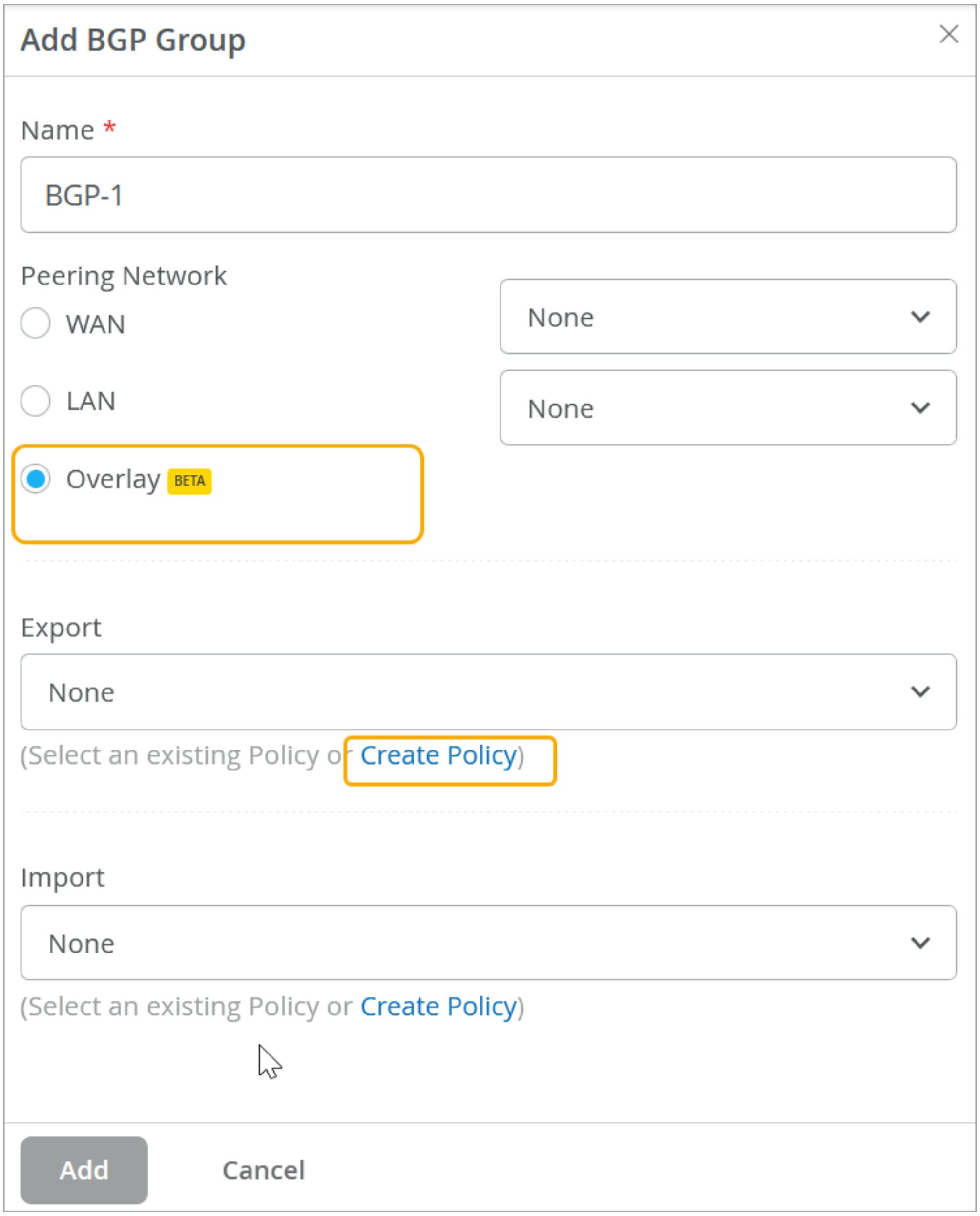
Overlay Traffic Steering for BGP-Learned Prefixes

You can specify a preferred path for the traffic traversing from a spoke device to the BGP-learned prefixes by configuring overlay path preferences. You can configure path preferences in the routing policies on the spoke devices. This feature allows you to determine which hub the traffic should pass through.

To configure path preferences:

1. In the Add BGP Group window, enter the details for the BGP group:

Figure 141: Add BGP Group



Add BGP Group

Name *

BGP-1

Peering Network

○ WAN — None

○ LAN — None

● Overlay BETA

Export

None

(Select an existing Policy or Create Policy)

Import

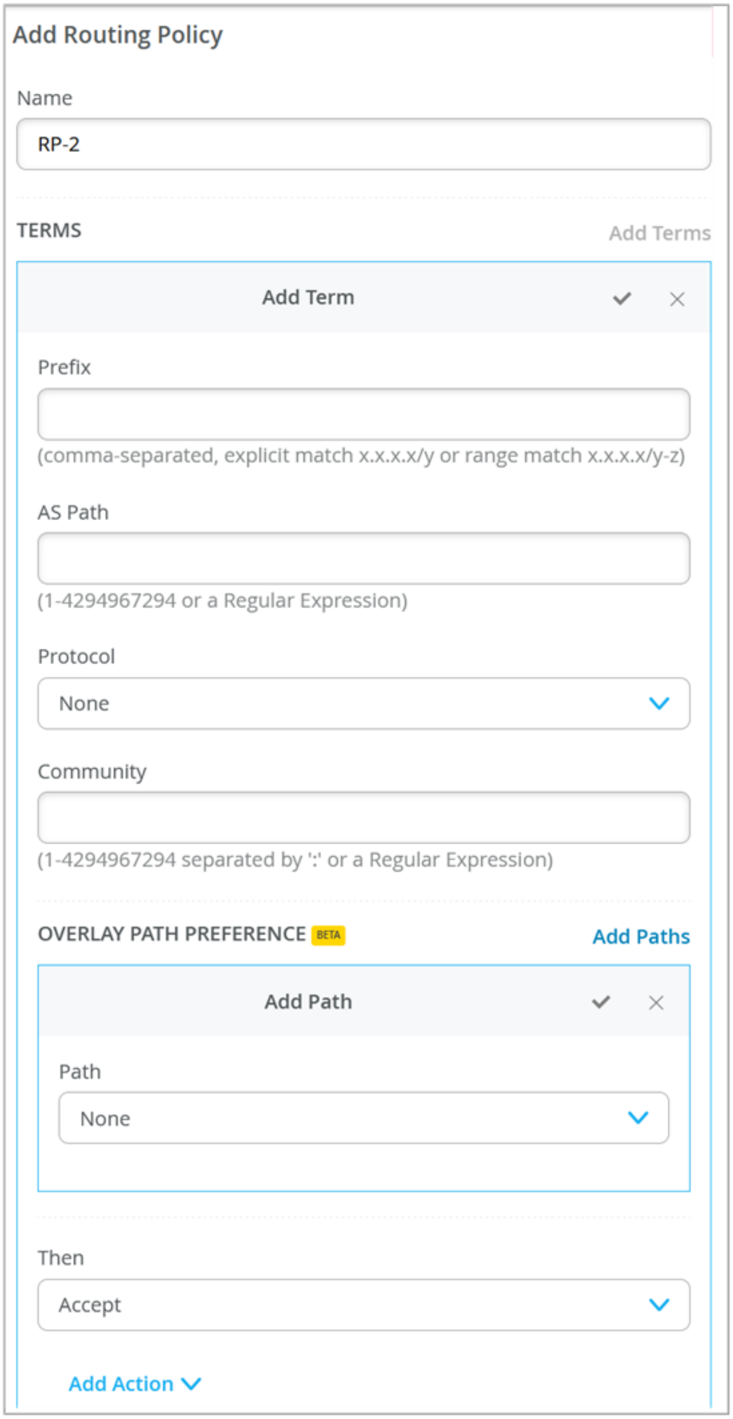
None

(Select an existing Policy or Create Policy)

2. Enter the following details:

   - Enter a name of the BGP group.
   - Select Peering Network as **Overlay**.
   - Click drop-down for **Export** and select an existing routing policy or click **Create Policy**.
   - In the Routing Policy window,you can add or edit the policy for the overlay path preference.

Figure 142: Add Routing Policy



Add Routing Policy

Name

RP-2

TERMS

Add Terms

Add Term ✓ ×

Prefix

(comma-separated, explicit match x.x.x.x/y or range match x.x.x.x/y-z)

AS Path

(1-4294967294 or a Regular Expression)

Protocol

None

Community

(1-4294967294 separated by ':' or a Regular Expression)

OVERLAY PATH PREFERENCE BETA

Add Paths

Add Path ✓ ×

Path

None

Then

Accept

Add Action

- **Name**—Enter the name of the policy.
- **Add Terms**—Enter the policy conditions such as prefix, autonomous system [AS] path regular expressions, protocols, and community.

- **Overlay Path Preference**—Enter overlay path preference. Click **Add Paths** and select an existing overlay hub endpoint.
- **Then**—Select an action (Accept or Reject) to apply when the condition is fulfilled. Enable one of the following preference for the accepted path:
  - **Append Community**—Add a BGP community to the route. A BGP community is a group of destinations that share a common property.
  - **Exclude Community**—Exclude a BGP communities to the route.
  - **Set Community**—Set a BGP community in the route. The set option replaces the current communities on a route with the specified community
  - **Prepend AS Path**—Prepend a AS number to the start of a BGP AS path.
  - **Exclude AS Path**—Exclude a AS number from the start of a BGP AS path.
  - **Set Local Preference**—Set preference to assign to routes that are advertised to the group or peer.
  - **Add Target VRs**— Add virtual Routing and Forwarding (VRF) instances for the intentional sharing of route information across VRF instances.
- Click **Add** to add to save the routing policy.
- On the Add BGP Group window, for the **Export** field, select the routing policy you created from the drop-down.

3. Click **Save**.

NOTE: You can create overlay traffic steering for BGP-learned prefixes by selecting **WAN Edges** in Juniper Mist Portal.

Configure OSPF

Open Shortest Path First (OSPF) is a link-state routing protocol used in IP networks to determine the best path for forwarding IP packets. OSPF divides a network into areas to improve scalability and control the flow of routing information. The following steps explain how you can configure OSPF for your SRX Series Firewall deployed as a WAN Edge device.

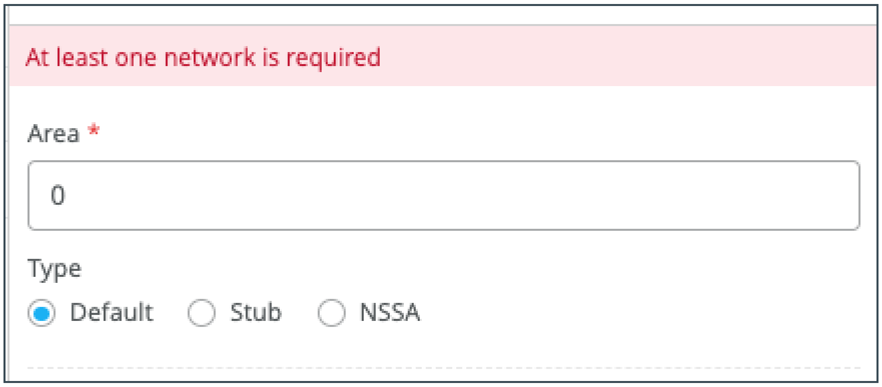
You must first define an OSPF Area from the **OSPF AREAS** tile, then apply that area to the WAN Edge device from the **OSPF CONFIGURATION** tile.

NOTE: You can configure OSPF from the Routing section on WAN Edge templates (**Organization** > **WAN Edge Templates**), hub profiles (**Organization** > **Hub Profiles**), or the WAN Edge device configuration page (**WAN Edges** > **WAN Edges** > ***WAN Edge Name***). The following steps show how to configure OSPF from the WAN Edge Template.

1. From the Mist portal, navigate to **Organization** > **WAN Edge Templates**.
2. In the **ROUTING** section, from the **OSPF AREAS** tile, click **Add OSPF Area**.
3. In the **Add OSPF Area** window, add the following information:

Table 42: Add OSPF Area Options

Field	Description
Area	This number indicates the identification area that your OSPF network or SRX Series Firewall belongs to.
Type	This is the OSPF Area type. Select one of the following options: a. Default (Area 0) — This represents the core of an OSPF network. b. Stub — Using this OSPF area type blocks external routes. c. Not So Stubby Area (NSSA) — Using this OSPF area type allows redistribution of some external routes and not others. For a more in depth explanation of the different area types, see Configuring OSPF Areas.



At least one network is required

Area *

0

Type

● Default ○ Stub ○ NSSA

4. Click **Add OSPF Network**, then, in the **Add OSPF Network** section of the window, enter the following information:

Table 43: Add OSPF Network Options

Field	Description
Network	This is the name of your OSPF network. **NOTE**: Check the **Passive** checkbox if you do not want OSPF to send Hello packets on an interface. This prevents the interface from forming unnecessary neighor relationships, which reduces overhead on routers and ensures that only the crucial connections are being made.
Interface Type	• Broadcast — This is the default interface type for an OSPF ethernet interface. • p2p (point to point) — This represents a connection between two OSPF routers (one router has one recipient).
BFD Interval	This value determines how frequently BFD packets will be sent to BFD peers (in milliseconds).
Metric	This is the cost metric used by OSPF to determine the best path between two OSPF-enabled devices.

Table 43: Add OSPF Network Options *(Continued)*

Field	Description
Hello Interval	This interval specifies the length of time, in seconds, before the routing device sends a hello packet out an interface. By default, the routing device sends Hello packets every 10 seconds.
Dead Interval	This interval specifies the length of time, in seconds, that the routing device waits before declaring a neighboring routing device as unavailable. By default, the routing device waits 40 seconds (four times the Hello interval).
Auth Type	• None — Selecting this means you are selecting no authentication to be done. • md5 (message-digest algorithm) — This is a hashing algorithm that uses a one-way cryptographic function that acccepts a message of any length and returns it as a fixed-length output value to be used for authentication. • password — This means that a password will be required for authentication.

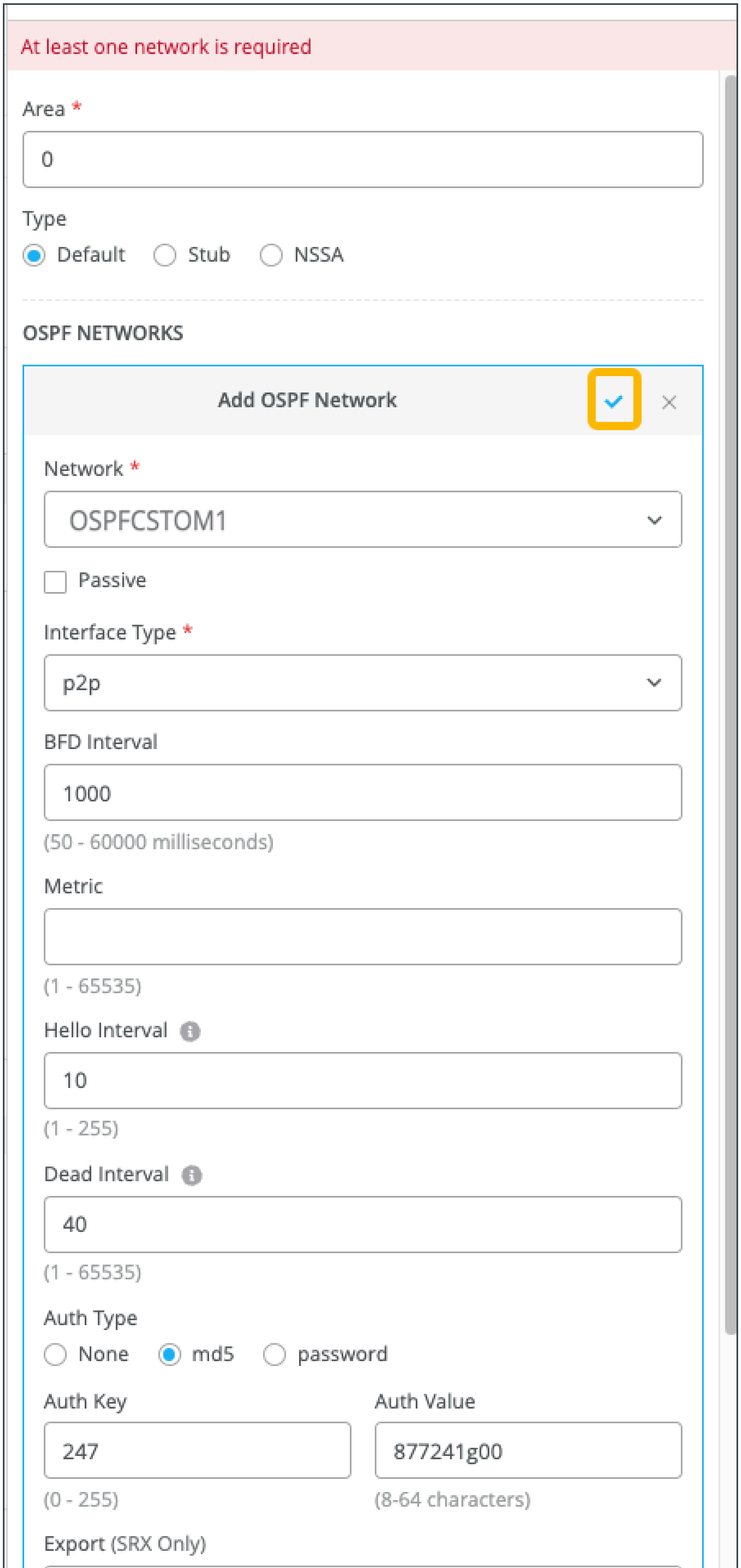
Table 43: Add OSPF Network Options *(Continued)*

Field	Description

Export (SRX Only)	• Click drop-down for **Export** and select an existing routing policy or click **Create Policy**.
	  ◦ In the Routing Policy window,you can add or edit the policy for the overlay path preference.
	    ▪ **Name**—Enter the name of the policy.
	    ▪ **Add Terms**—Enter the policy conditions such as prefix, autonomous system [AS] path regular expressions, protocols, and community.
	    ▪ **Then**—Select an action (Accept or Reject) to apply when the condition is fulfilled. Enable one of the following preferences for the accepted path by clicking **Add Action**:
	      – Append Community
	      – Exclude Community
	      – Set Community
	      – Prepend AS Path
	      – Exclude AS Path
	      – Set Local Preference
	      – Add Target VRs
	    ▪ Click the checkbox at the top of the Add Term section to save the routing policy.
	Click **Add** at the bottom of the window to return to the **Add OSPF Area** options.

Import (SRX Only)	See above.

5. When you have entered in the appropriate information, click the checkbox at the top of the Add OSPF Network section.



At least one network is required

Area *

0

Type

● Default ○ Stub ○ NSSA

OSPF NETWORKS

Add OSPF Network ✓ ×

Network *

OSPFCSTOM1

□ Passive

Interface Type *

p2p

BFD Interval

1000

(50 - 60000 milliseconds)

Metric

(1 - 65535)

Hello Interval

10

(1 - 255)

Dead Interval

40

(1 - 65535)

Auth Type

○ None ● md5 ○ password

Auth Key

247

(0 - 255)

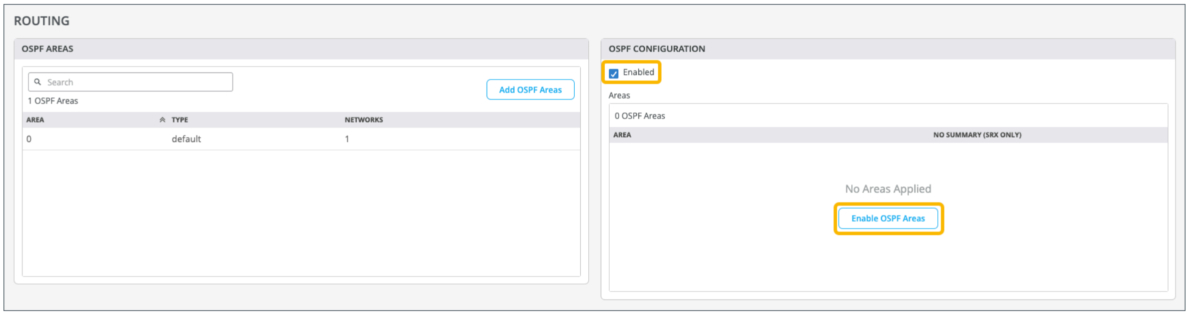
Auth Value

877241g00

(8-64 characters)

Export (SRX Only)

6. Click **Add** at the bottom of the window. You will now see your OSPF area listed in the **OSPF Areas** tile.
7. Now that you've created your OSPF area, you need to enable it. In the **OSPF CONFIGURATION** tile, check the **Enabled** checkbox. This causes the **Enable OSPF Areas** button to appear.
8. Click the **Enable OSPF Areas** button.



1 OSPF Areas

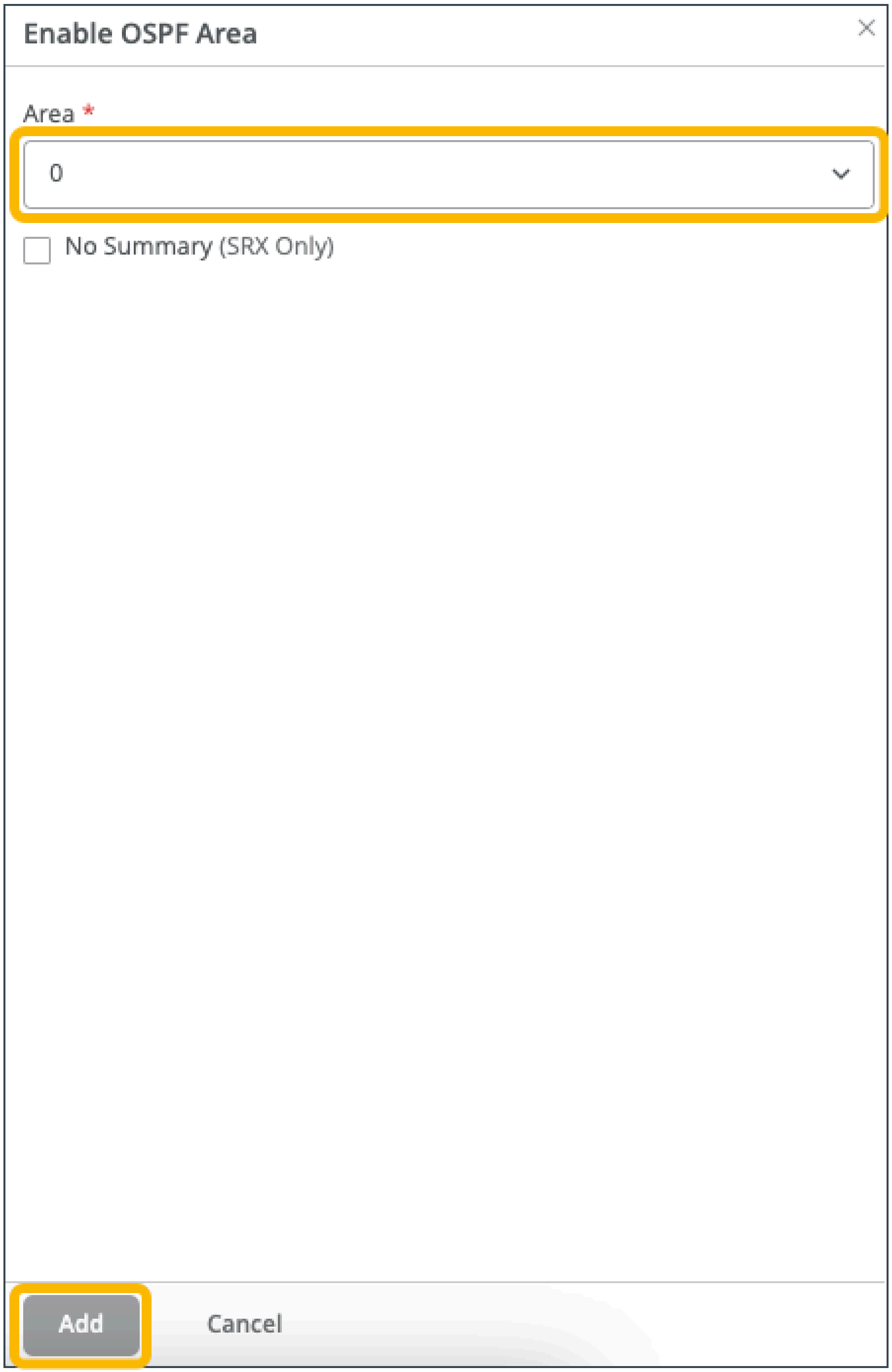
AREA	TYPE	NETWORKS
0	default	1

0 OSPF Areas

AREA	NO SUMMARY (SRX ONLY)

No Areas Applied

9. The **Enable OSPF Area** window appears. Select the **Area** you just created, then click **Add** at the bottom of the window.



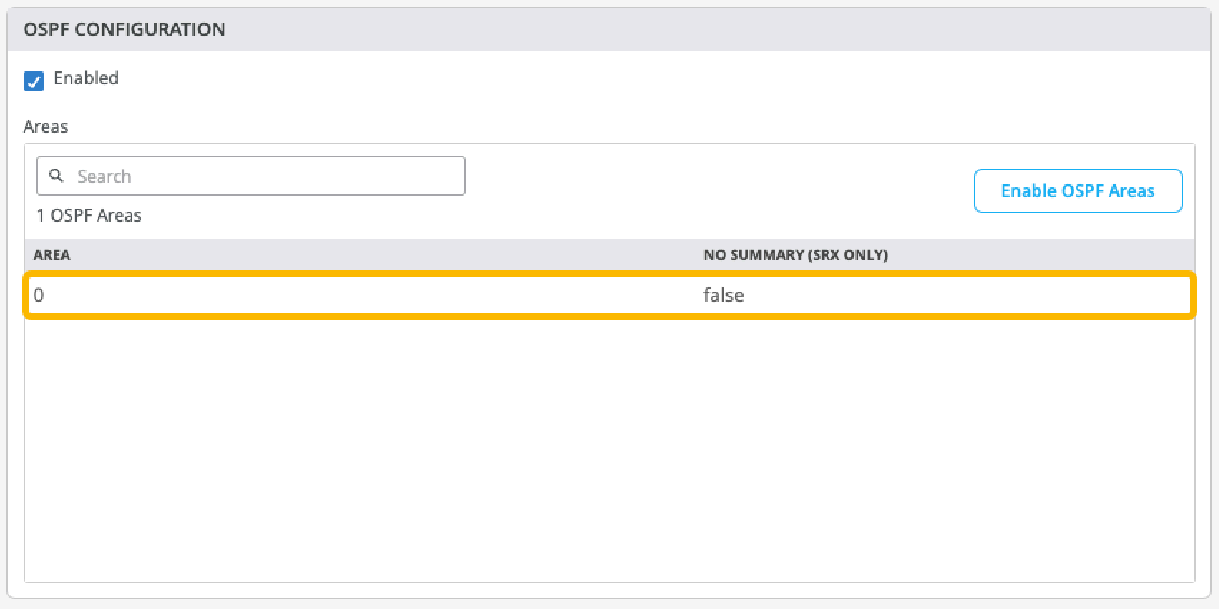
Enable OSPF Area

Area *

0

□ No Summary (SRX Only)

You will see your area listed in the **OSPF CONFIGURATION** tile.



OSPF CONFIGURATION

☑ Enabled

Areas

1 OSPF Areas

AREA	NO SUMMARY (SRX ONLY)
0	false

SEE ALSO

Configure OSPF | 125

Configuring OSPF Areas

Onboard SRX Series Firewalls for WAN Configuration

IN THIS SECTION

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.

Before You Begin

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 Cloud-Ready SRX Firewalls

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.

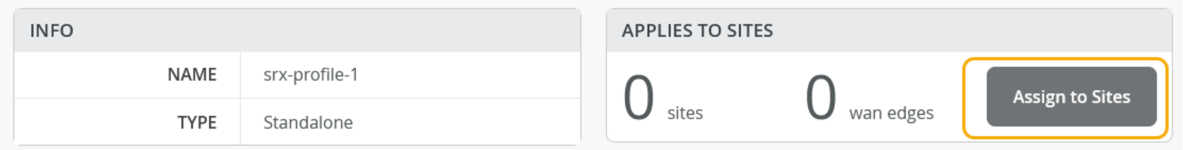
The template that you created in "Configure WAN Edge Templates for SRX Series Firewalls" on page 217 now exists in the Juniper Mist cloud as an object that you can assign to one or more sites. WAN edge templates are a quick and easy way to group the common attributes of WAN edge spoke devices. You can 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:

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

Figure 143: Assign Spoke Templates to Sites



INFO

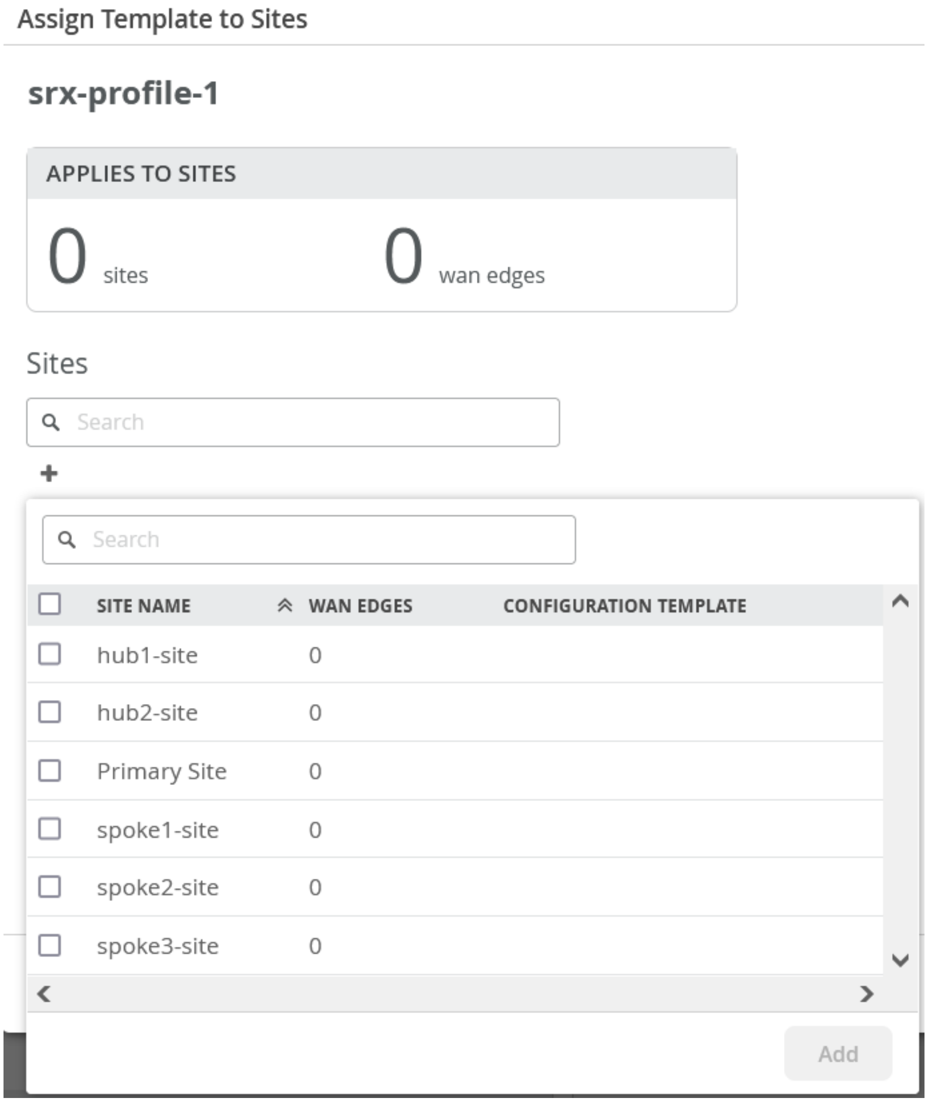
NAME	srx-profile-1
TYPE	Standalone

APPLIES TO SITES

0 sites 0 wan edges

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

Figure 144: Select Sites to Assign Spoke Templates



Assign Template to Sites

srx-profile-1

APPLIES TO SITES

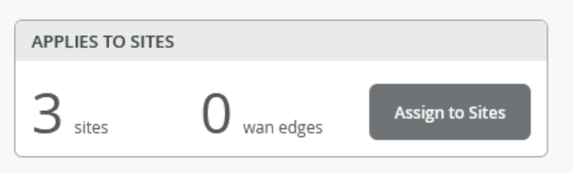
0 sites 0 wan edges

Sites

□	SITE NAME	WAN EDGES	CONFIGURATION TEMPLATE
□	hub1-site	0	
□	hub2-site	0	
□	Primary Site	0	
□	spoke1-site	0	
□	spoke2-site	0	
□	spoke3-site	0	

The WAN Edge Templates page reflects the updated status. Figure 145 on page 262 indicates that three sites are using the template.

Figure 145: WAN Edge Templates Applied to Sites



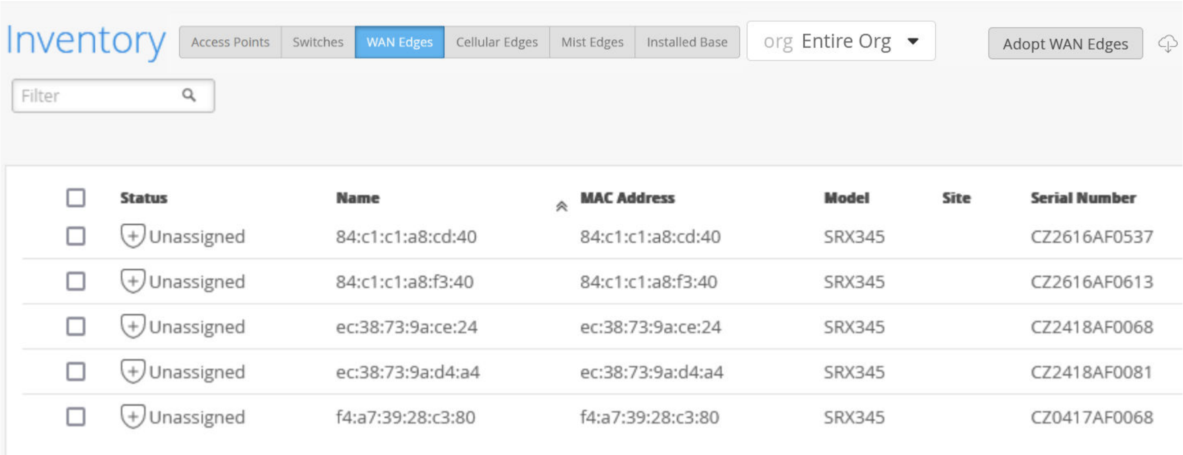
Assign an SRX Series Firewall to a Site

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. For details on onboarding, see SRX Adoption.

To assign an SRX Series Firewall to a site:

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

Figure 146: SRX Series Firewall in Inventory



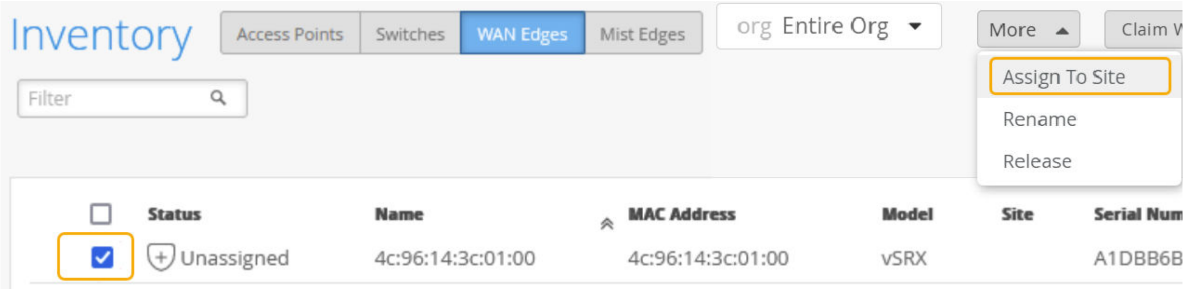
□	Status	Name	MAC Address	Model	Site	Serial Number
□	Unassigned	84:c1:c1:a8:cd:40	84:c1:c1:a8:cd:40	SRX345		CZ2616AF0537
□	Unassigned	84:c1:c1:a8:f3:40	84:c1:c1:a8:f3:40	SRX345		CZ2616AF0613
□	Unassigned	ec:38:73:9a:ce:24	ec:38:73:9a:ce:24	SRX345		CZ2418AF0068
□	Unassigned	ec:38:73:9a:d4:a4	ec:38:73:9a:d4:a4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

TIP: For virtual SRX Series Firewalls, you onboard the device and then assign it to the site. Alternatively, you can use the system MAC address or serial number for assigning the device to the site. Use the following CLI commands to get the device MAC address and serial number:

```
user@SPOKE1> show chassis mac-addresses
MAC address information:
Public base address 4c:96:14:b7:32:00
Public count 128
Private base address 4c:96:14:b7:32:80
Private count 0

user@SPOKE1> show chassis hardware
Hardware inventory:
Item Version Part number Serial number Description
Chassis 69e6b8d61b7e VSRX
Midplane
System IO
Routing Engine VSRX-2CPU-4G memory
FPC 0 BUILTIN BUILTIN FPC
PIC 0 VSRX DPDK GE
Power Supply 0
```

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

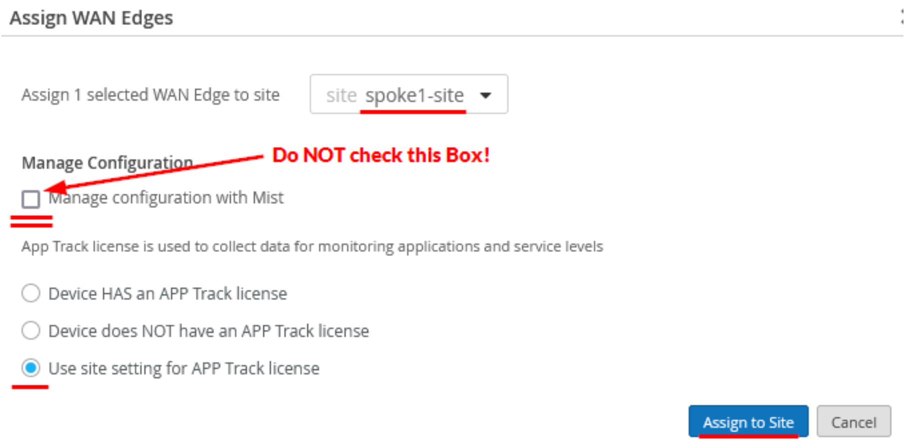
Figure 147: Assign SRX Series Firewalls to Sites



□	Status	Name	MAC Address	Model	Site	Serial Num
☑	Unassigned	4c:96:14:3c:01:00	4c:96:14:3c:01:00	vSRX		A1DBB6B

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

Figure 148: 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

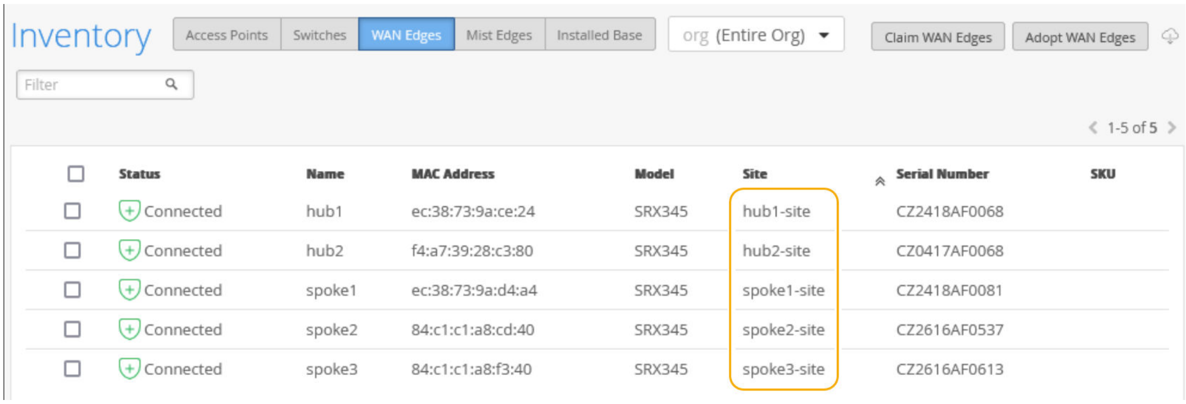
● Use site setting for APP Track license

- 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.

5. Check the **Use site setting for APP Track license** option if you have a valid Application Security license, and then click **Assign to Site**.

   Figure 149 on page 264 shows changes in the inventory once you assign the device to the site.

Figure 149: 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	

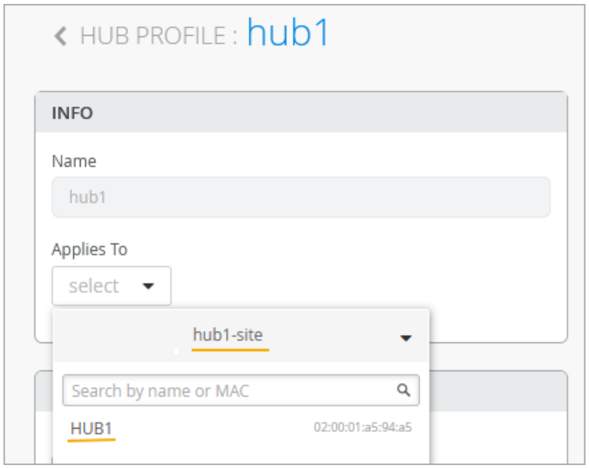
Assign a Hub Profile to the SRX Series Firewall

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:

1. In the Juniper Mist portal, click **Organization** > **WAN** > **Hub Profiles**. The Hub Profile displays the list of existing profiles.
2. Click the hub profile that you want to assign to a site.
3. Under the **Applies To** option, select the site from the list of available sites.

Figure 150: Select Devices on Sites



HUB PROFILE : hub1

INFO

Name: hub1

Applies To: select

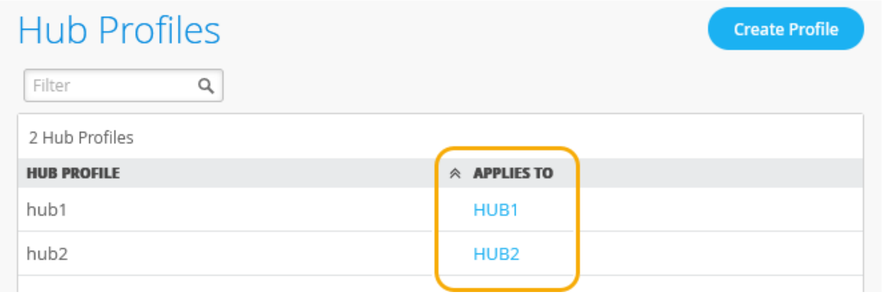
hub1-site

Search by name or MAC

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

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

Figure 151: Hub Profile Assignment Summary



Hub Profiles

2 Hub Profiles

HUB PROFILE	APPLIES TO
hub1	HUB1
hub2	HUB2

SEE ALSO

Configure WAN Edge Templates for SRX Series Firewalls | 217

Configure Hub Profiles for SRX Series Firewalls | 197

WAN Assurance Configuration Overview | 166
Juniper Mist WAN Assurance Configuration Hierarchy | 13

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 details, see Intrusion Detection and Prevention Overview.

> **NOTE**: You must install the IDP signature database update license key on your 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 Juniper Networks recommends. Each attack type and severity has 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. However, when the system detects an attack, this profile actively blocks any malicious traffic or other attacks detected on the network.

- Critical Only (SRX)—The Critical-Only profile is suitable for critical-severity attacks. When the system detects a critical attack, this profile takes appropriate action. We recommend the Critical – Only SRX profile for SRX300 line of firewalls.

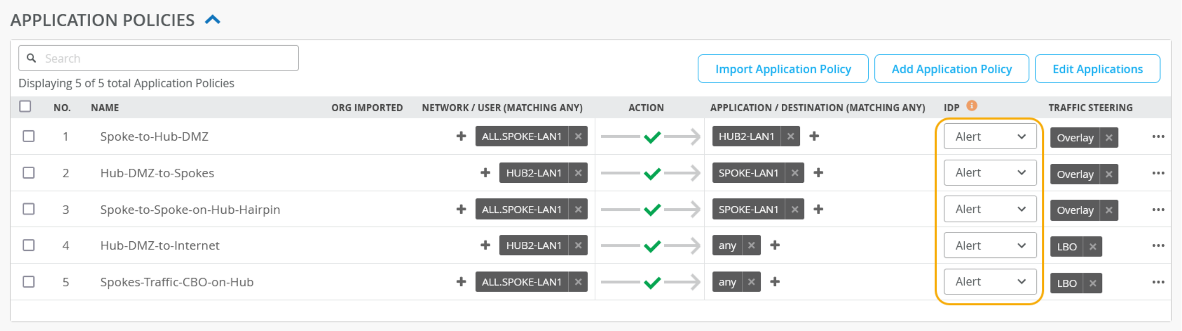
- None—No profile is applied when you select this option.

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. Actions in the IDP profile are preconfigured and are not available for users to configure.

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.

Figure 152: Configure an IDP Profile (Alert)



APPLICATION POLICIES

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	Alert	Overlay
☐	2	Hub-DMZ-to-Spokes		HUB2-LAN1	✓	SPOKE-LAN1	Alert	Overlay
☐	3	Spoke-to-Spoke-on-Hub-Hairpin		ALL.SPOKE-LAN1	✓	SPOKE-LAN1	Alert	Overlay
☐	4	Hub-DMZ-to-Internet		HUB2-LAN1	✓	any	Alert	LBO
☐	5	Spokes-Traffic-CBO-on-Hub		ALL.SPOKE-LAN1	✓	any	Alert	LBO

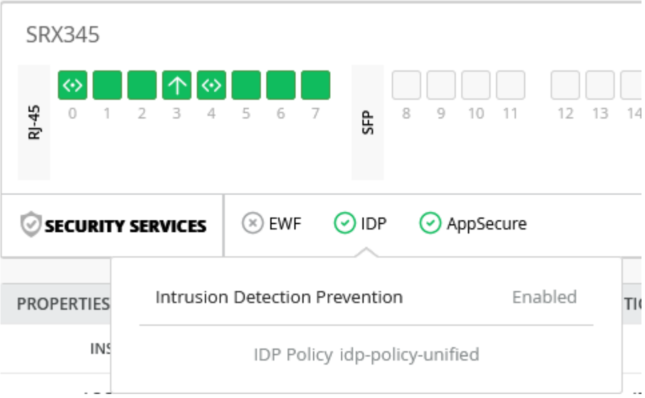
4. Click **Save**.

   The Juniper Mist cloud applies the configured IDP profile on all spoke devices.

> **NOTE**: Ensure that you set the policy action to PERMIT; otherwise, the IDP settings might override the DENY statement.

After you apply an IDP profile, the spoke devices download the IDP policy and display the status of IDP as **Enabled**, as shown in Figure 153 on page 268.

Figure 153: 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 virtual machine (VM) desktop (desktop1) in a sandbox or lab environment, 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.

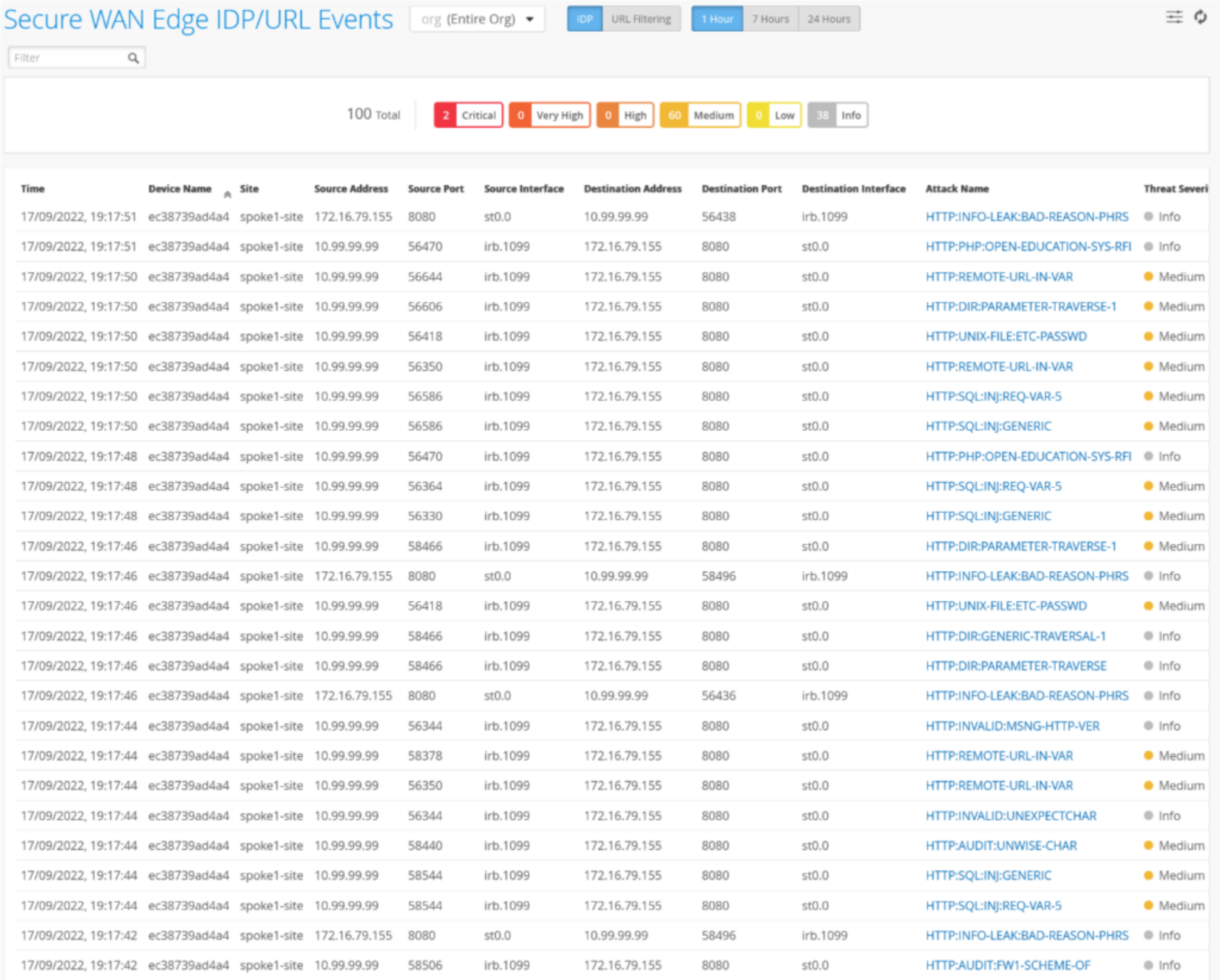
```
virsh console desktop1

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**.

Figure 154 on page 270 shows detected events generated for an SRX Series Firewall.

Figure 154: IDP Events Generated for an Alert IDP Profile



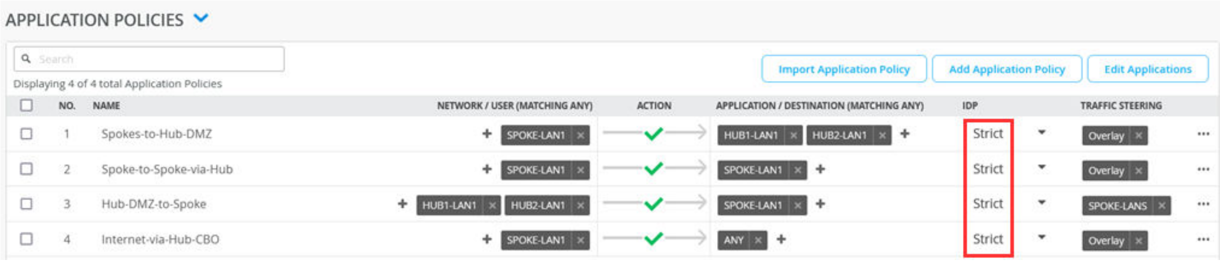
100 Total | 2 Critical | 0 Very High | 0 High | 60 Medium | 0 Low | 38 Info

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 sample. However, this time you change the spoke device template and change the IDP profile from **Alert** to **Strict**, as shown in Figure 155 on page 271.

Figure 155: IDP Profile Configuration (Strict Profile)



APPLICATION POLICIES

Displaying 4 of 4 total Application Policies

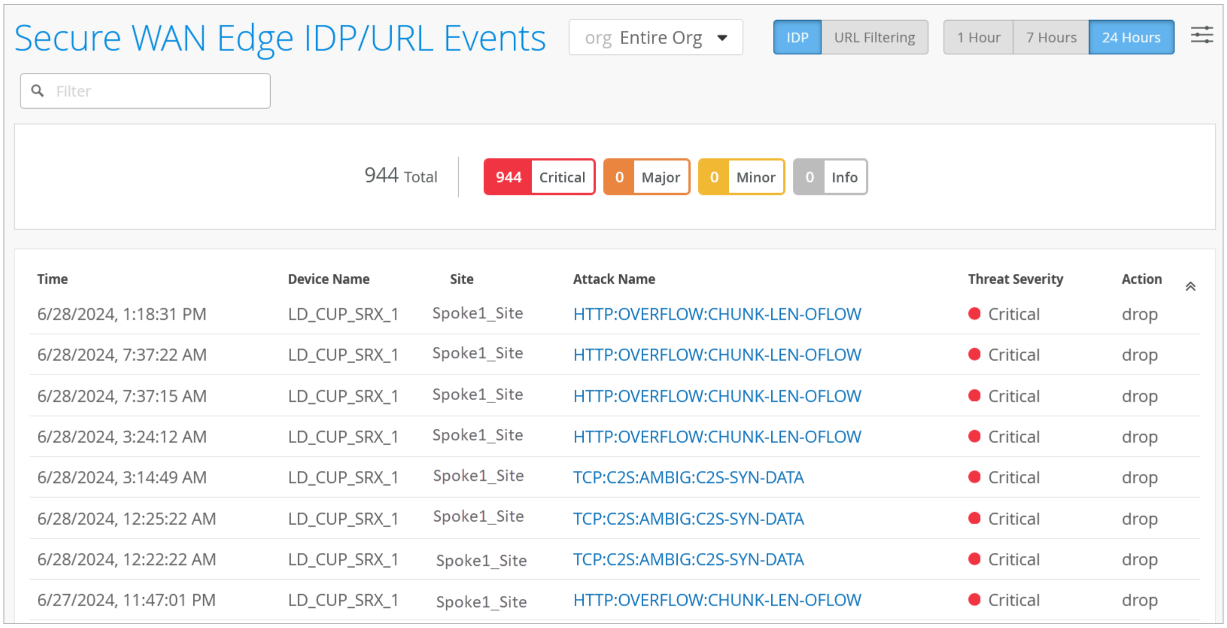
☐	NO.	NAME	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
☐	1	Spokes-to-Hub-DMZ	SPOKE-LAN1	✓	HUB1-LAN1 HUB2-LAN1	Strict	Overlay
☐	2	Spoke-to-Spoke-via-Hub	SPOKE-LAN1	✓	SPOKE-LAN1	Strict	Overlay
☐	3	Hub-DMZ-to-Spoke	HUB1-LAN1 HUB2-LAN1	✓	SPOKE-LAN1	Strict	SPOKE-LANS
☐	4	Internet-via-Hub-CBO	SPOKE-LAN1	✓	ANY	Strict	Overlay

Run the security scanner. 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
```

Figure 156 on page 272 shows that for some events, the action is to close the session to mitigate the threats (under the **Action** field).

Figure 156: IDP Events Generated for the Strict IDP Profile



Time	Device Name	Site	Attack Name	Threat Severity	Action
6/28/2024, 1:18:31 PM	LD_CUP_SRX_1	Spoke1_Site	HTTP:OVERFLOW:CHUNK-LEN-OFLOW	● Critical	drop
6/28/2024, 7:37:22 AM	LD_CUP_SRX_1	Spoke1_Site	HTTP:OVERFLOW:CHUNK-LEN-OFLOW	● Critical	drop
6/28/2024, 7:37:15 AM	LD_CUP_SRX_1	Spoke1_Site	HTTP:OVERFLOW:CHUNK-LEN-OFLOW	● Critical	drop
6/28/2024, 3:24:12 AM	LD_CUP_SRX_1	Spoke1_Site	HTTP:OVERFLOW:CHUNK-LEN-OFLOW	● Critical	drop
6/28/2024, 3:14:49 AM	LD_CUP_SRX_1	Spoke1_Site	TCP:C2S:AMBIG:C2S-SYN-DATA	● Critical	drop
6/28/2024, 12:25:22 AM	LD_CUP_SRX_1	Spoke1_Site	TCP:C2S:AMBIG:C2S-SYN-DATA	● Critical	drop
6/28/2024, 12:22:22 AM	LD_CUP_SRX_1	Spoke1_Site	TCP:C2S:AMBIG:C2S-SYN-DATA	● Critical	drop
6/27/2024, 11:47:01 PM	LD_CUP_SRX_1	Spoke1_Site	HTTP:OVERFLOW:CHUNK-LEN-OFLOW	● Critical	drop

Intrusion Detection and Prevention (IDP) Bypass Profiles

The IDP Bypass works in conjunction with the intrusion prevention system (IPS) rules to prevent unnecessary alarms from being generated. You configure IDP profile when you want to exclude a specific destination, or attack type from matching an IDP rule. This prevents IDP from generating unnecessary alarms.

An IDP profile can have multiple bypass profiles, each with multiple bypass rules.

To create IDP bypass profile:

1. In the Juniper Mist cloud portal, select **Organization** > **WAN** > **Application Policy** > **IDP bypass profiles**.

   The page displays a list of IDP bypass profiles (if available)

2. Click **Add Bypass Profile** to create a profile.

3. In the Create Bypass Profile window:

   a. Add Name. Use alphanumerics, underscores, or dashes, and cannot exceed 63 characters.

   b. Select base profile. The supported base profiles are:

      - Standard

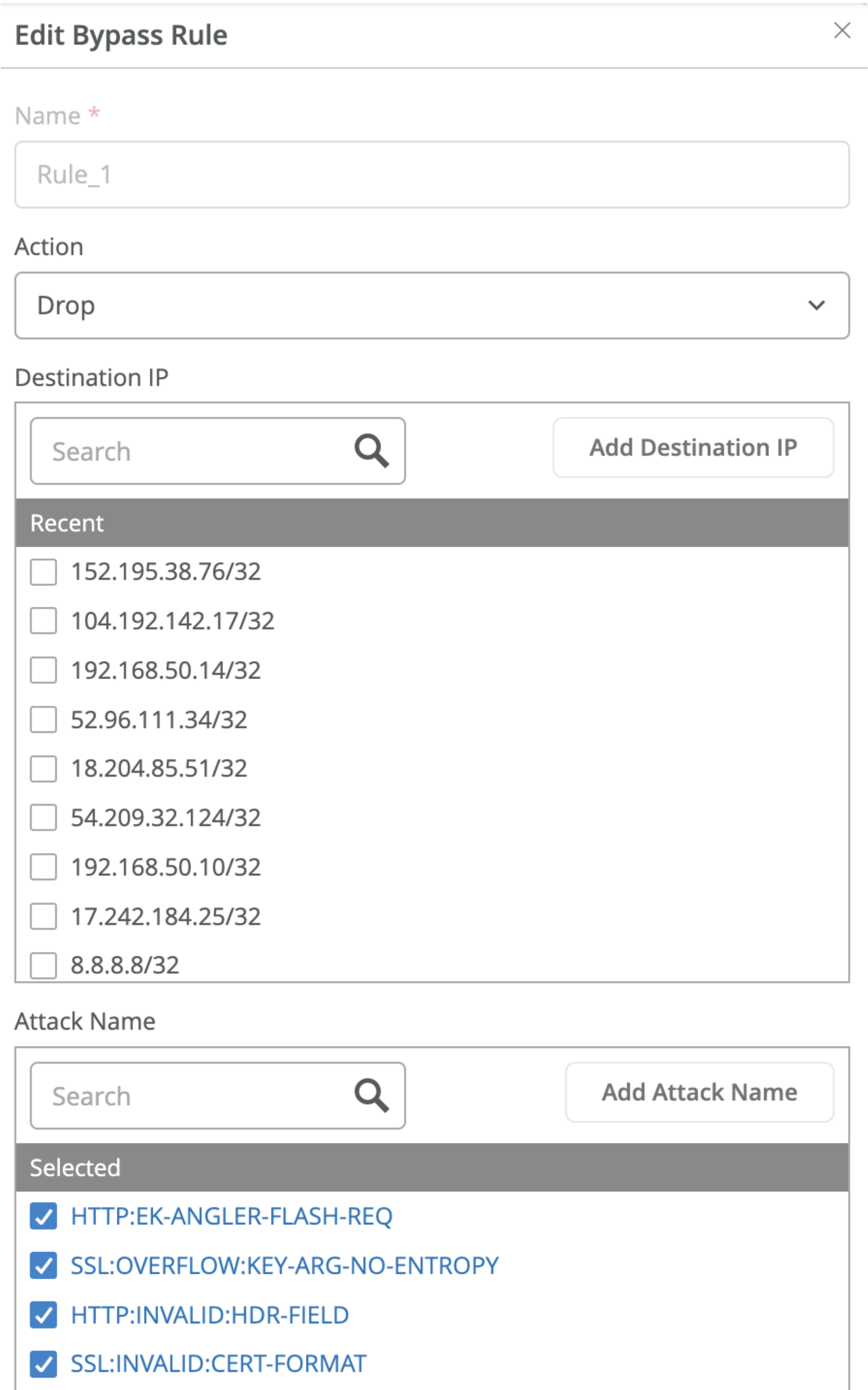
      - Strict

- Critical only– SRX

You need a base IDP profile to create an IDP bypass profile.

c. Click **Next**. The portal opens a rules page where you can define the rule for the IDP bypass profile.

Figure 157: IDP Bypass Profile Rule



Edit Bypass Rule

Name *

Rule_1

Action

Drop

Destination IP

Recent

□ 152.195.38.76/32

□ 104.192.142.17/32

□ 192.168.50.14/32

□ 52.96.111.34/32

□ 18.204.85.51/32

□ 54.209.32.124/32

□ 192.168.50.10/32

□ 17.242.184.25/32

□ 8.8.8.8/32

Attack Name

Selected

☑ HTTP:EK-ANGLER-FLASH-REQ

☑ SSL:OVERFLOW:KEY-ARG-NO-ENTROPY

☑ HTTP:INVALID:HDR-FIELD

☑ SSL:INVALID:CERT-FORMAT

- Action – Select the associated traffic action. Available options are — **Alter**, **Drop**, or **Close**.

- Destination IP – IP address of the destination for traffic you want to exempt. You can select one or more destination IP address from the populated list or you can enter the destination IP address by clicking **Add Destination IP**.

- Attack Name – Select the attacks you want IDP to exempt for the specified destination addresses from the displayed list. Alternatively you can enter the attack by clicking **Add Attack Name**. The attack you enter must be of type supported by Juniper Networks IPS Signature.

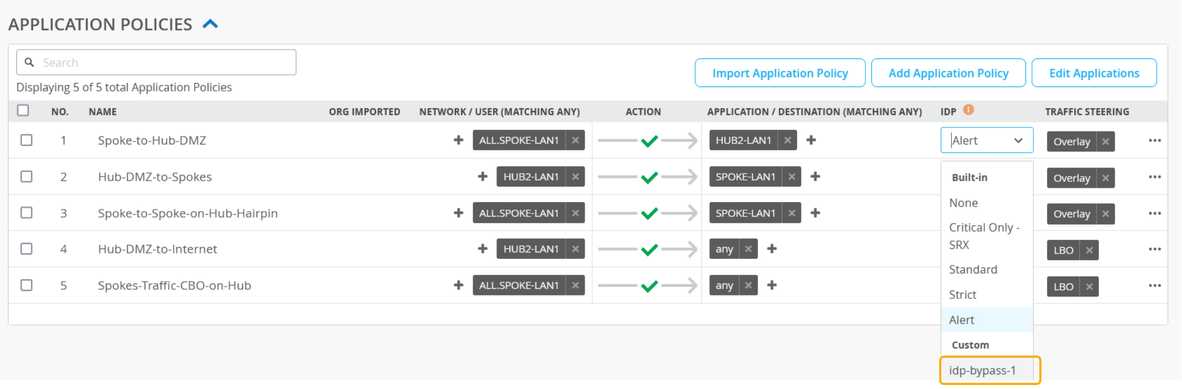
- Click **Save**.

The rule you created appears under IDP Bypass Profile pane. Next, you need to apply the IDP bypass profile in an application policy similar applying any IDP profile by using the following steps:

1. In the Juniper Mist cloud portal, click **Organization** > **WAN Edge Templates** and select a template for your spoke device.

2. Under the IDP column, select the IDP profile. For example, select the IDP bypass profile that you created in the previous step.

Figure 158: Apply IDP Bypass Profile in Application Policy



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	Alert	Overlay
□	2	Hub-DMZ-to-Spokes		HUB2-LAN1	✓	SPOKE-LAN1		Overlay
□	3	Spoke-to-Spoke-on-Hub-Hairpin		ALL.SPOKE-LAN1	✓	SPOKE-LAN1		Overlay
□	4	Hub-DMZ-to-Internet		HUB2-LAN1	✓	any		LBO
□	5	Spokes-Traffic-CBO-on-Hub		ALL.SPOKE-LAN1	✓	any		LBO

3. Click **Save** once you configure other options in application policy. See Configure Application Policies on SRX Series Firewalls.

You can view the generated events by navigating to **Site** > **Secure WAN Edge IDP/URL Events**.

RELATED DOCUMENTATION

Configure Application Policies on SRX Series Firewalls | 191

Juniper Mist WAN Assurance Configuration Hierarchy | 13

WAN Assurance Configuration Overview | 166

Enable Application Visibility on SRX Series Firewalls

IN THIS SECTION

The Juniper Networks Application Security (AppSecure) feature is a suite of application-aware security services for the Juniper Networks® SRX Series Firewalls. AppSecure enables you to see the applications on your network and learn how they work. It enables you to observe their behavioral characteristics and assess their relative risk, which allows the Juniper Mist™ cloud to track and report applications passing through the device.

Before You Begin

Consult this list to ensure that you have the licenses and application signatures necessary to enable application visibility.

- You need a valid AppSecure license on your SRX Series Firewall to use the feature. Use the `show system license` command to check if your device has the license. For details about license requirements and installation, see Juniper Licensing User Guide.

- We recommend using the latest version of application signatures. To install the latest version of application signatures, run the following commands on your device:

1. Download the application signature package version on your device. The command downloads the latest version of the package.

```
user@host> request services application-identifications download
Please use command "request services application-identification download status"
 to check status
```

```
user@host> request services application-identifications download status
Application package 3410 is downloaded successfully.
```

2. Install the application signature package version on your device.

```
user@host> request services application-identification install
Please use command "request services application-identification install status" to check
status
and use command "request services application-identification proto-bundle-status" to check
protocol bundle status
```

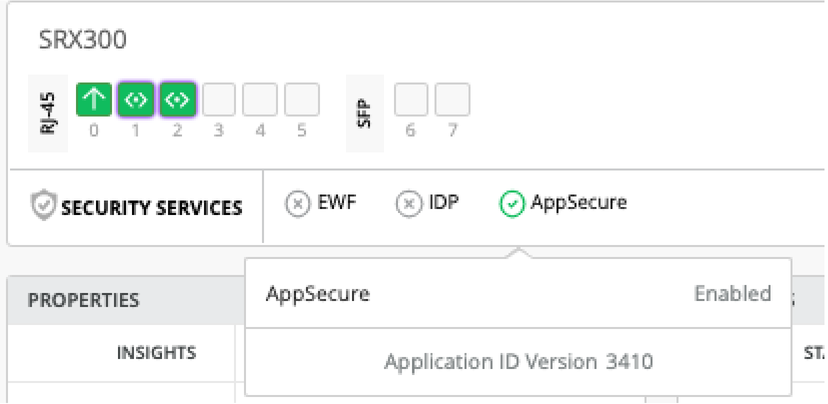
3. Verify the application signature package version installed on your device.

```
user@host> show services application-identification version
Application package version: 3410
```

For more details, see Predefined Application Signatures for Application Identification.

You can see the application signature version in the Juniper Mist cloud portal of your device under the **SECURITY SERVICES** panel.

Figure 159: Check Application Security (AppSecure) Version



AppSecure Enabled

Application ID Version 3410

Enable Application Visibility While Assigning a Device to the Site

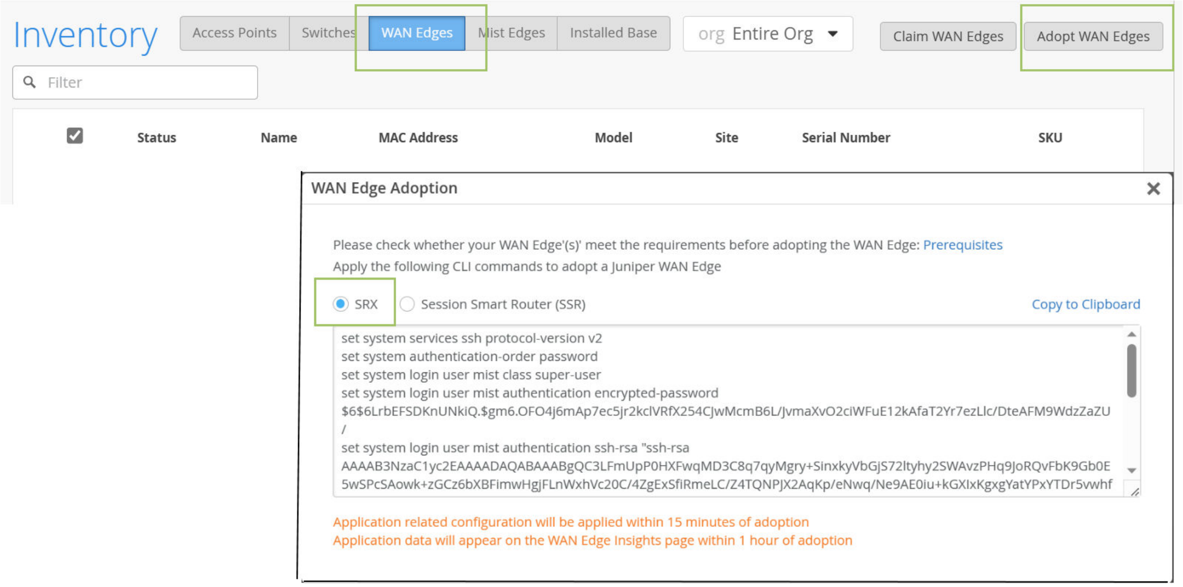
Application visibility provides insight into applications running on the network. You can analyze applications running on the network for performance and assurance.

You can enable or disable application visibility on your SRX Series Firewall in the Juniper Mist cloud portal by checking or unchecking the **My SRX devices have an App Track License** option.

To enable application visibility while assigning a device to a site:

1. In the Juniper Mist cloud portal, click **Organization** > **Inventory** and select WAN Edges from the main menu.
2. Click the **Adopt WAN Edges** button.

Figure 160: WAN Edge Adoption Commands



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$6LrbEFSDKnUNkiQ.$gm6.OFO4j6mAp7ec5jr2kclVRfX254CJwMcmB6L/JvmaXvO2ciWFuE12kAfaT2Yr7ezLlc/DteAFM9WdzZaZU
/
set system login user mist authentication ssh-rsa "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC3LFmUpP0HXFwqMD3C8q7qyMgry+SinxkyVbGjS72ltyhy2SWAvzPHq9JoRQvFbK9Gb0E
5wSPcSAowk+zGCz6bXBFimwHgjFLnWxhVc20C/4ZgExSfiRmeLC/Z4TQNPJX2AqKp/eNwq/Ne9AE0iu+kGXIxKgxgYatYPxYTDr5vwhf
```

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

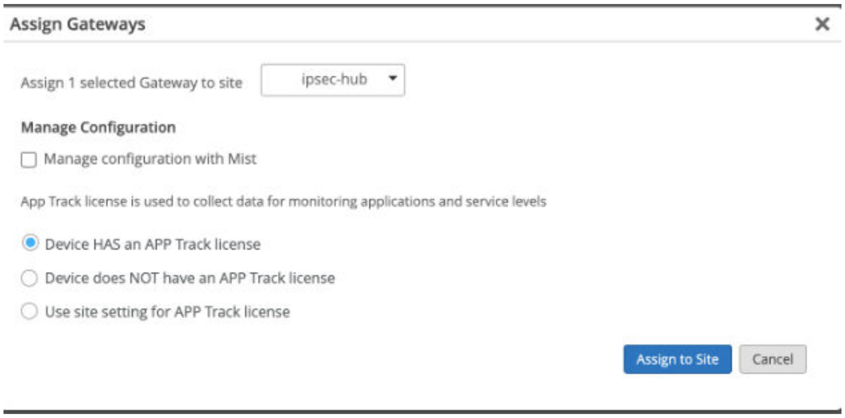
Juniper Mist generates a code snippet in the **WAN Edge Adoption** window.

3. Ensure that you've selected the SRX option, and click **Copy to Clipboard**.
4. Paste the copied commands to the SRX Series Firewall in configuration mode and commit the configuration. The code creates the following settings on your SRX Series Firewall:

   - Enable SSH.
   - Create a Juniper Mist cloud user.
   - Create a device ID and credentials.
   - Set up the outbound SSH client and associated timers.

   After you commit the configuration on your SRX Series Firewall, the device entry is populated in the inventory page of the Juniper Mist cloud portal.
5. Select the SRX Series Firewall and select **More** > **Assign to Site**.
6. Select the required site from the available list.
7. Select one of the options for the application tracking (AppTrack) license.

Figure 161: Check the AppTrack License Option



Assign Gateways

Assign 1 selected Gateway to site: ipsec-hub

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

- **Use site setting for App Track license**—Enable application visibility under site setting options.
- **Device has an App Track license**—Application visibility is already enabled on the device.
- **Device does NOT have an App Track license**—The device does not have application security license.

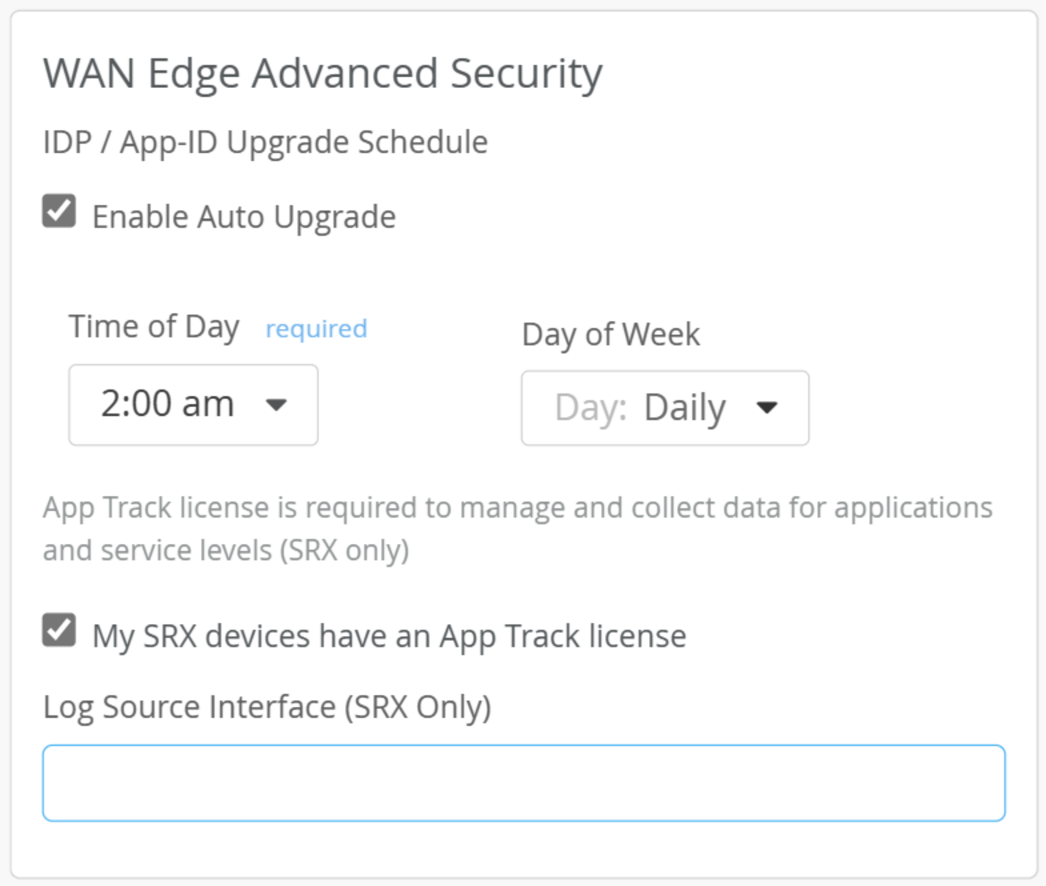
If you selected the **Use site setting for App Track license** option, continue with the following steps:

a. Navigate to **Organization** > **Site Configurations** and select your site.

b. Scroll down to the **WAN Edge Advanced Security** pane.

c. Check or uncheck the box next to **My SRX devices have an App Track license**

Figure 162: Check the AppTrack License Option



WAN Edge Advanced Security

IDP / App-ID Upgrade Schedule

☑ Enable Auto Upgrade

Time of Day required: 2:00 am

Day of Week: Day: Daily

App Track license is required to manage and collect data for applications and service levels (SRX only)

☑ My SRX devices have an App Track license

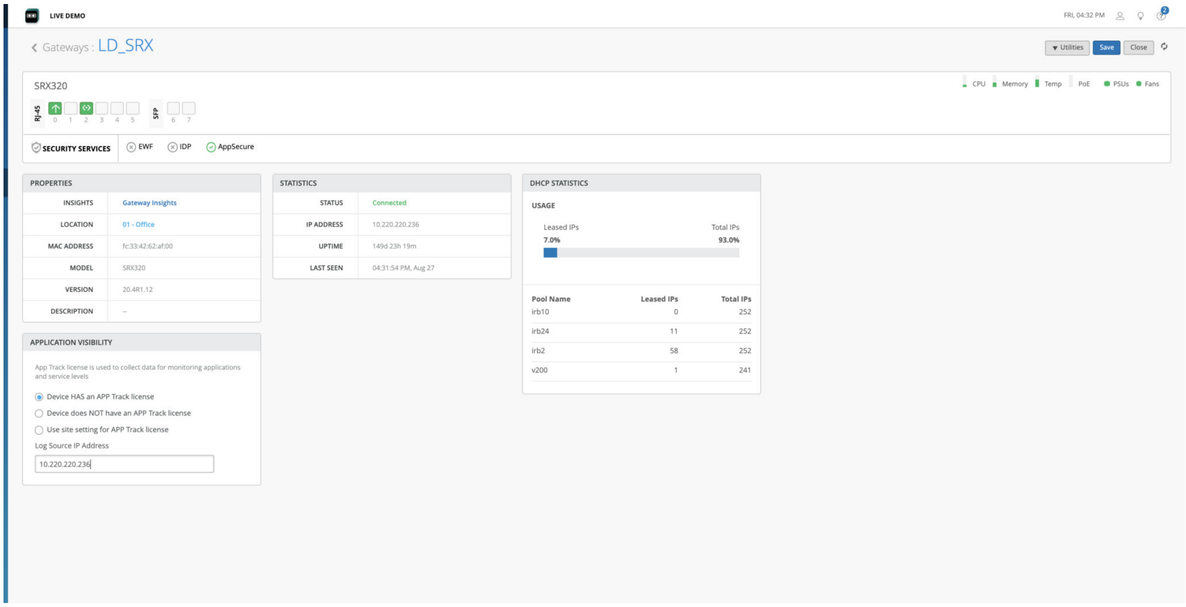
Log Source Interface (SRX Only)

- Check the box to enable application visibility.
- Uncheck the box to disable application visibility.

d. For the **Log Source Interface** option, provide the IP address of an interface of your SRX Series Firewall. Ensure that the interface has connectivity to the cloud or Internet. This interface acts as the source address for log messages for the application session records.

8. If you selected either **Device has an App Track license** or **Device does NOT have an App Track license**, ensure that the same option is reflected on the Gateways tab in the **Application Visibility** pane.

Figure 163: Set the AppTrack License Option



PROPERTIES

INSIGHTS	Gateway Insights
LOCATION	01 - Office
MAC ADDRESS	fc:33:42:62:af:00
MODEL	SRX320
VERSION	20.4R1.12
DESCRIPTION	--

STATISTICS

STATUS	Connected
IP ADDRESS	10.220.220.236
UPTIME	149d 23h 19m
LAST SEEN	04:31:54 PM, Aug 27

DHCP STATISTICS

USAGE

Leased IPs 7.0% Total IPs 93.0%

Pool Name	Leased IPs	Total IPs
irb10	0	252
irb24	11	252
irb2	58	252
v200	1	241

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: 10.220.220.236

You can verify API messages of **/sites/site-id/setting** to see the following options, depending on whether you selected or unselected **My SRX devices have an App Track License**:

- • The **“gateway_mgmt“: {“app_usage“: True}** message indicates that the check box is selected.
- The **“gateway_mgmt“: {“app_usage“: False}** message indicates that the check box is not selected.

Example:

```
GET /api/v1/sites/232527fe-4126-40bb-8c78-2c8d1dfed043/setting
HTTP 200 OK
Allow: OPTIONS, GET, PUT
Content-Type: application/json
Vary: Accept

{
   "switch_mgmt": {
      "root_password": "mist123"
   },
   <<< API OUTPUT TRIMMED >>>
   "zone": {
      "autozones_enabled": false,
      "autozones_rssi": -70
   },
   "gateway_mgmt": {
      "app_usage": true,
      "security_log_source_interface": "ge-0/0/0"
   },
   "id": "86f13595-9599-48a7-8c26-ad98a702b9e5",
   "for_site": true,
   "site_id": "232527fe-4126-40bb-8c78-2c8d1dfed043",
   "org_id": "001f3ef8-d69d-4780-b9c3-7a1f3cb123f0",
   "created_time": 1599493540,
   "modified_time": 1600069580
```

NOTE:

If you did not select the **site settings** option, the `gateway_mgmt` section will not be present in the device API.

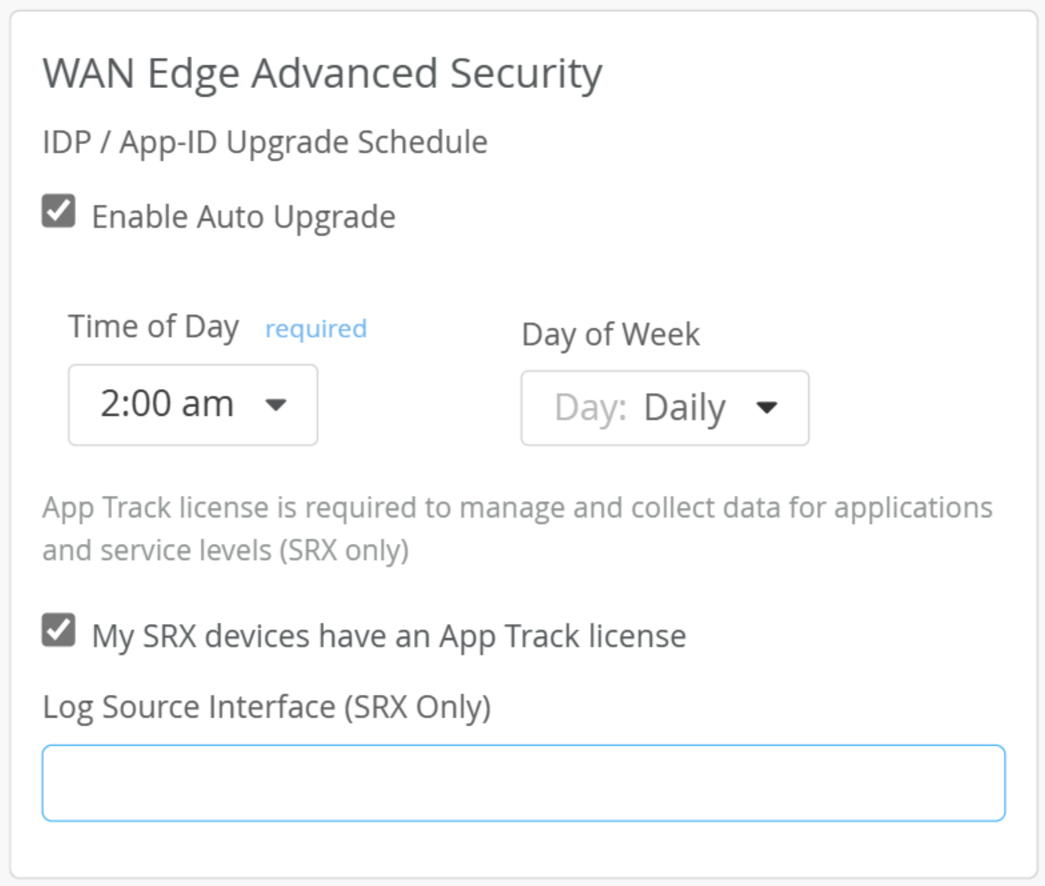
Enable Application Visibility on an SRX Series Firewall Already Assigned to a Site

If you did not enable application visibility while assigning the device to a site, you can enable it later.

To enable application visibility on an SRX Series Firewall that you already assigned to a site:

1. In the Juniper Mist™ cloud portal, select **Organization** > **Site Configurations**.
2. Select the site to which your device is assigned.
3. Scroll down to the **WAN Edge Advanced Security** pane.

Figure 164: Check the AppTrack License Option



WAN Edge Advanced Security

IDP / App-ID Upgrade Schedule

☑ Enable Auto Upgrade

Time of Day required: 2:00 am

Day of Week: Day: Daily

App Track license is required to manage and collect data for applications and service levels (SRX only)

☑ My SRX devices have an App Track license

Log Source Interface (SRX Only)

4. Check or uncheck the box next to **My SRX devices have an App Track license**.
   - Check the box to enable application visibility.
   - Uncheck the box to disable application visibility.
5. For the **Log Source Interface** option, provide the IP address of an interface on SRX Series Firewall that has connectivity to the cloud or Internet. This interface acts as the source address for log messages for the application session records.
6. Click **Save**.
7. To view the applications details, click **Monitor** > **Service Levels**. Select the **Insights** tab and scroll down to **Applications** section to get details about applications usage.

SEE ALSO

Configure Sites and Variables for SRX Series Firewalls | **168**

Monitor the Service Status of SRX Series Firewalls | **285**

Monitor the Service Status of SRX Series Firewalls

You can monitor the service status of the following features on your Juniper Networks® SRX Series Firewall in the Juniper Mist™ cloud portal:

- Enhanced Web Filtering (EWF)
- IDP
- Application Security

You need a valid license for your SRX Series Firewall to use the feature. For more details about license requirements and installation, see Juniper Licensing User Guide.

On the SRX Series Firewall, use the `show system license` command to display the license name with expiry date.

```
user@host> show system license
License usage:
                                    Licenses      Licenses      Licenses      Expiry
   Feature name                         used     installed        needed
   anti_spam_key_sbl                        0             1             0      2022-04-28
00:00:00 UTC
   idp-sig                                  0             1             0      2022-04-28
00:00:00 UTC
   dynamic-vpn                              0             2             0      permanent
   av_key_sophos_engine                     0             1             0      2022-04-28
00:00:00 UTC
   logical-system                           1             3             0      permanent
   wf_key_websense_ewf                      0             1             0      2022-04-28
00:00:00 UTC
   remote-access-ipsec-vpn-client           0             2             0      permanent

Licenses installed:
   License identifier: DemoLabJUNOS386107562
   License version: 4
   Valid for device: CV4720AF0436
   Customer ID: Juniper Internal
   Features:
      av_key_sophos_engine - Anti Virus with Sophos Engine
         date-based, 2021-04-27 00:00:00 UTC - 2022-04-28 00:00:00 UTC
      anti_spam_key_sbl - Anti-Spam
```

```
     date-based, 2021-04-27 00:00:00 UTC - 2022-04-28 00:00:00 UTC
  idp-sig - IDP Signature
     date-based, 2021-04-27 00:00:00 UTC - 2022-04-28 00:00:00 UTC
  wf_key_websense_ewf - Web Filtering EWF
     date-based, 2021-04-27 00:00:00 UTC - 2022-04-28 00:00:00 UTC
```

Check EWF Status

To check Enhanced Web Filtering (EWF) configuration status:

1. Confirm if EWF is enabled on your SRX Series Firewall in CLI operational mode:

```
user@host> show security utm web-filtering status
UTM web-filtering status:    Server status: no-config
root@00c52c4c3204>
```

   The **Server status: no-config** indicates that the EWF is not configured.

2. Configure EWF on your SRX Series Firewall using the CLI at the [edit] hierarchy level. Use configuration mode and commit the configuration.

   > **NOTE**: We've captured the following configuration from a lab environment and provided it for reference purposes only. Your own configuration may vary based on the specific requirements of your environment.

```
[edit]
set system syslog file utm-log any any
set system syslog file utm-log match RT_UTM
set security utm custom-objects url-pattern blacklist value https://*.poki.com
set security utm custom-objects custom-url-category restricted value blacklist
set security utm default-configuration anti-virus type sophos-engine
set security utm default-configuration anti-virus scan-options uri-check
set security utm default-configuration anti-virus scan-options timeout 30
set security utm default-configuration anti-virus sophos-engine sxl-timeout 5
set security utm default-configuration web-filtering url-blacklist restricted
set security utm default-configuration web-filtering type juniper-enhanced
set security utm default-configuration web-filtering juniper-enhanced server host
rp.cloud.threatseeker.com
set security utm default-configuration web-filtering juniper-enhanced server port 80
set security utm default-configuration web-filtering juniper-enhanced default permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
```

```
category Enhanced_Games action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Gambling action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Abused_Drugs action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Adult_Content action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Adult_Material action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Advanced_Malware_Command_and_Control action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Advanced_Malware_Payloads action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Bot_Networks action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Compromised_Websites action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Drugs action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Emerging_Exploits action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Files_Containing_Passwords action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Hacking action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Illegal_or_Questionable action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Keyloggers action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Malicious_Embedded_Link action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Malicious_Embedded_iFrame action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Malicious_Web_Sites action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Militancy_and_Extremist action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Mobile_Malware action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Network_Errors action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Newly_Registered_Websites action block
```

```
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Pay_to_Surf action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Phishing_and_Other_Frauds action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Potentially_Damaging_Content action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Potentially_Exploited_Documents action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Potentially_Unwanted_Software action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Racism_and_Hate action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Spyware action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Suspicious_Content action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Suspicious_Embedded_Link action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Unauthorized_Mobile_Marketplaces action block
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Alcohol_and_Tobacco action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Application_and_Software_Download action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Bandwidth action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Computer_Security action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Custom_Encrypted_Payloads action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Elevated_Exposure action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Entertainment action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Entertainment_Video action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_File_Download_Servers action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Freeware_and_Software_Download action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Instant_Messaging action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
```

```
category Enhanced_Internet_Auctions action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Internet_Radio_and_TV action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Intolerance action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Lingerie_and_Swimsuit action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Marijuana action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Media_File_Download action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Message_Boards_and_Forums action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Non_Traditional_Religions action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Non_Traditional_Religions_and_Occult_and_Folklore action log-and-
permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Nudity action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Parked_Domain action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Peer_to_Peer_File_Sharing action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Personals_and_Dating action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Prescribed_Medications action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Private_IP_Addresses action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Pro_Choice action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Pro_Life action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Proxy_Avoidance action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Sex action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Sex_Education action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Social_Networking_and_Personal_Sites action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
```

```
category Enhanced_Surveillance action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Tasteless action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Violence action log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile wf-home
category Enhanced_Web_and_Email_Spam action log-and-permit
set security utm utm-policy custom-utm-policy anti-virus http-profile junos-av-defaults
set security utm utm-policy custom-utm-policy web-filtering http-profile wf-home
```

3. Check the status in CLI operational mode.

   ```
   user@host> show security utm web-filtering status
   UTM web-filtering status:
   Server status: Juniper Enhanced using Websense server UP
   ```

   Now, the status changes to **Server status: Juniper Enhanced using Websense server UP**. This status indicates that the EWF service is enabled on your device.

4. You can check the status in the Juniper Mist cloud portal as shown in Figure 165 on page 293.

Check IDP Status

Before configuring Intrusion Detection and Prevention (IDP) you need to download and install the IDP security package using the following steps:

- Download the IDP package using the instructions in request security idp security-package download command.

- Install the package using the instructions in request security idp security-package install command.

This example uses the IDP templates which you download and install as follows: .

1. Download IDP template using the instructions in request security idp security-package download policy-templates command.

2. Install the templates using the instructions in request security idp security-package install policy-templates command.

3. Activate the template commit script

```
[edit]
user@host-1# set system scripts commit file templates.xsl
```

   The downloaded templates are saved to the Junos OS configuration database, and they are available in the CLI at the `[edit security idp idp-policy]` hierarchy level.

4. Activate the predefined policy as the active policy. In this example, you use `Recommended` policy as active policy.

```
[edit]

user@host-1# set security idp default-policy Recommended
user@host-1# set security idp active-policy Recommended
```

   For a list of predefined IDP policy templates, see Predefined IDP Policy Templates.

5. Enable the IDP policy in your configuration. Following snippet shows a configuration example.

```
set security idp idp-policy idpengine rulebase-ips rule 1 match from-zone any
set security idp idp-policy idpengine rulebase-ips rule 1 match source-address any
set security idp idp-policy idpengine rulebase-ips rule 1 match to-zone any
set security idp idp-policy idpengine rulebase-ips rule 1 match destination-address any
set security idp idp-policy idpengine rulebase-ips rule 1 match application junos-echo
set security idp idp-policy idpengine rulebase-ips rule 1 match attacks predefined-attack-groups Critical
```

   Example:

6. Use the following commands in operational mode to check for the IDP policy status:

   - Recommended IDP policy: `show security idp policies:`
   - Policy name: `show security idp policies`
   - IDP status: `show security idp status`
   - Check the IDP status in Juniper Mist Cloud portal as shown in Figure 165 on page 293 .

Configure Application Security

On your SRX Series Firewall, Application Security is enabled by default if you have a valid license. The OC-team ensures that all devices have the most up to date application signature version. If you want to change the version or install a custom version, see Predefined Application Signatures for Application Identification.

View Security Service Status in the Juniper Mist Cloud Portal

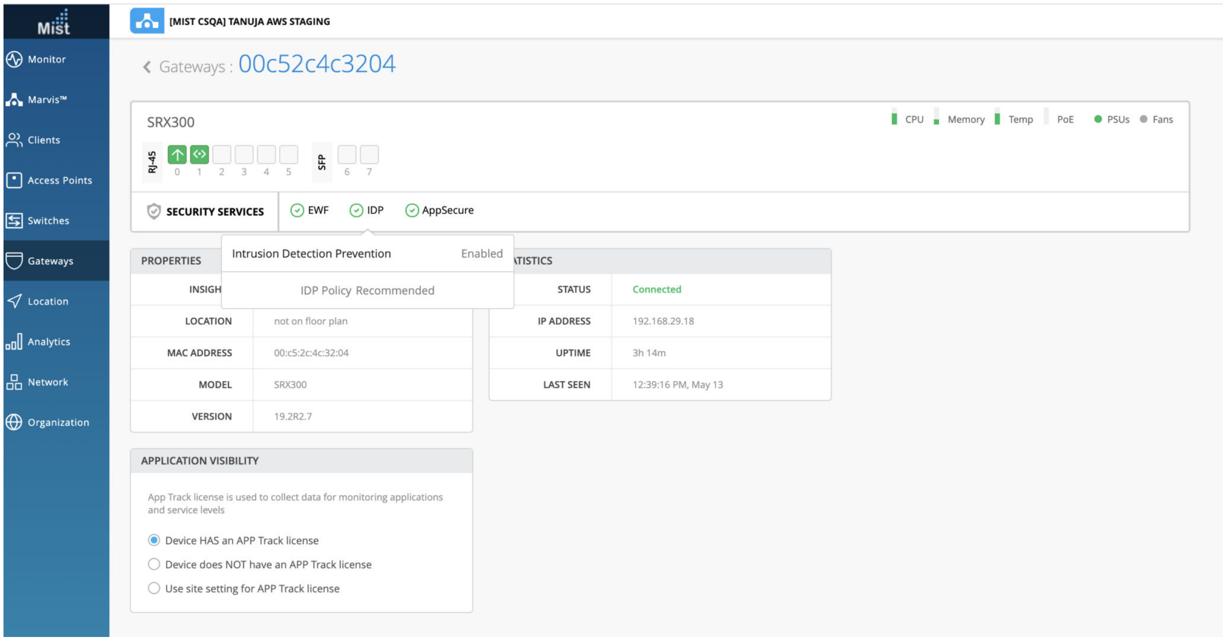
In the Juniper Mist cloud portal, you can view the status of security services under **SECURITY SERVICES** panel. Table 44 on page 292 provides the details of the status.

Table 44: Security Services Status Display

Security Services	Display Status	Meaning
EWF	Enabled	Connection to the Websense server is up.
	Disabled	EWF is not configured on your device.
	Down	Connection to the Websense server is down.
IDP	Enabled	IDP is configured and the IDP policy is applied.
	Disabled	IDP is not configured. In this case, the IDP policy name is displayed blank.
Application Security	Enabled	Application security is enabled. The application signature version is displayed.
	Disabled	Application security is not enabled. The application signature version is displayed as zero.

Figure 165 on page 293 shows security services status in Juniper Mist cloud portal.

Figure 165: Security Services Status



Intrusion Detection Prevention Enabled

IDP Policy Recommended

INSIGH	
LOCATION	not on floor plan
MAC ADDRESS	00:c5:2c:4c:32:04
MODEL	SRX300
VERSION	19.2R2.7

STATUS	Connected
IP ADDRESS	192.168.29.18
UPTIME	3h 14m
LAST SEEN	12:39:16 PM, May 13

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

NOTE: You can get details such as the presence or absence of a valid license and the status of the security services.

```
"service_status": {
      "idp_status": "disabled", // either "enabled" or "disabled"
      "idp_policy": "", // if the above is disabled this will be empty
      "appid_status": "disabled", // either "enabled" or "disabled"
      "ewf_status": "disabled", // either "enabled" (websense up), "disabled" (no
config) or "down" (websense down)
      "appid_version": 0 // this will be 0 if appid_status is disabled, as we then
don't check the version number
   },
```

RELATED DOCUMENTATION

IDP-Based Threat Detection for SRX Series Firewalls | 266

Enable Application Visibility on SRX Series Firewalls | 276

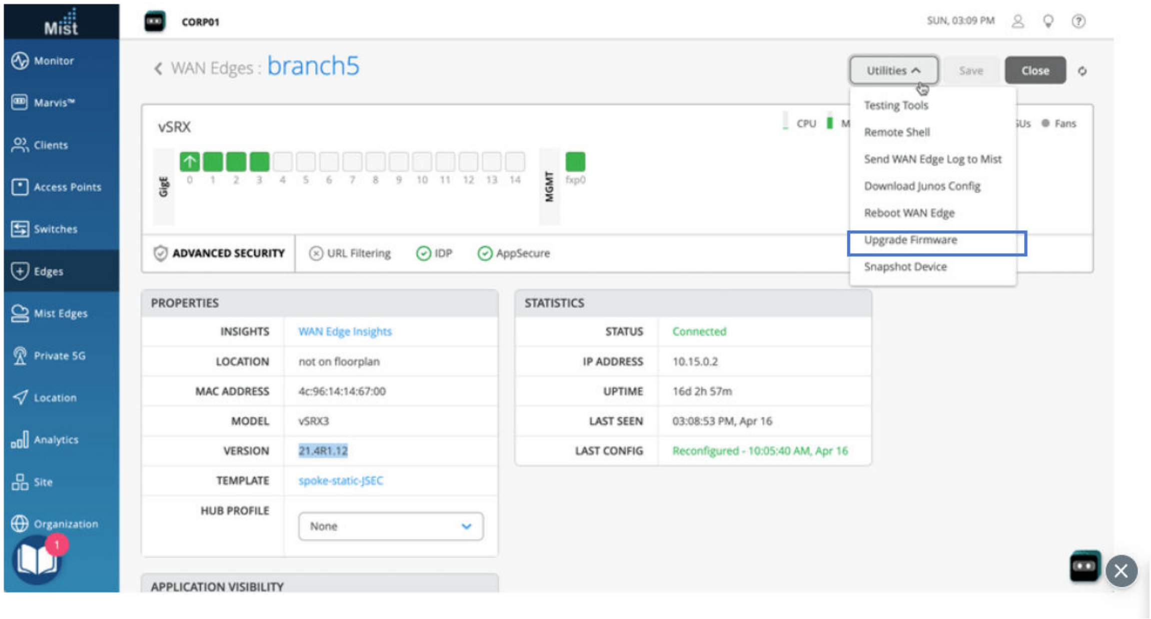
Upgrade a WAN Edge SRX Series Firewalls

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 can provide 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.

Figure 166: Upgrade Software



PROPERTIES

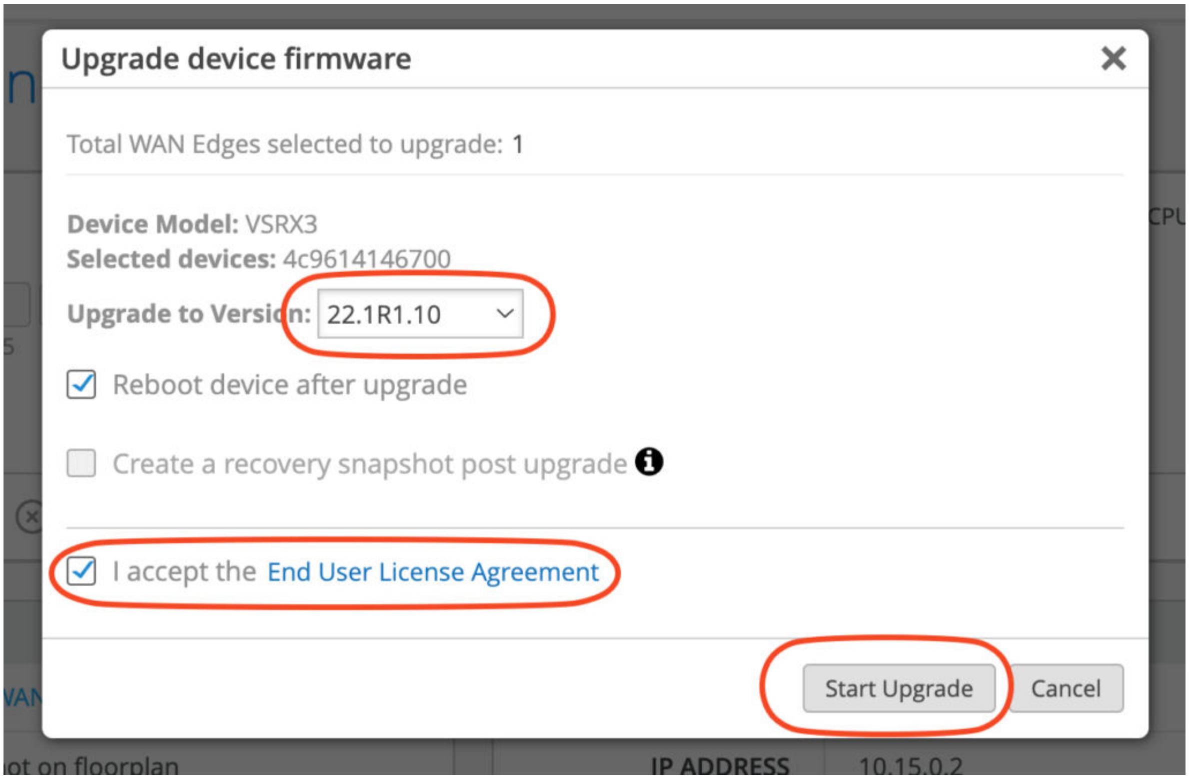
INSIGHTS	WAN Edge Insights
LOCATION	not on floorplan
MAC ADDRESS	4c:96:14:14:67:00
MODEL	vSRX3
VERSION	21.4R1.12
TEMPLATE	spoke-static-JSEC
HUB PROFILE	None

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.

Figure 167: 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 (HA) cluster, you can minimize the downtime by upgrading one node at a time.

RELATED DOCUMENTATION

Juniper Mist WAN Assurance Platform Considerations | 10

WAN Assurance Configuration Overview | 166

Juniper Mist WAN Assurance Configuration Hierarchy | 13

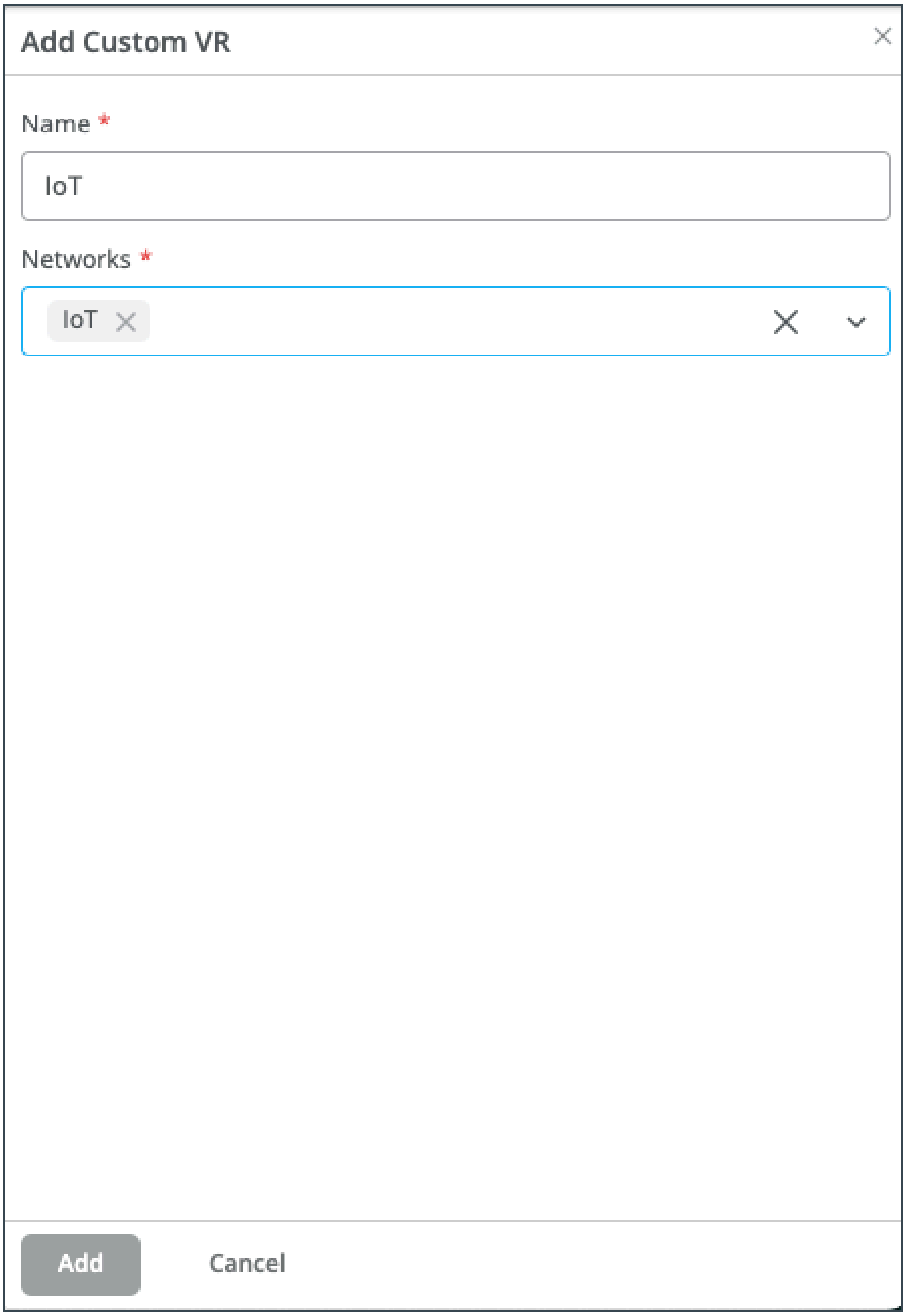
Configure a Custom VR for SRX Series Firewalls

A Custom Virtual Router (VR) is a virtual router that you can configure to be used in automatic route leaking. For SRX Series Firewalls, the Juniper Mist™ intent configuration model uses what is configured in the Application Policy to leak routes to the appropriate VR.

NOTE: The Juniper Mist intent configuration model evaluates the Network and Traffic Steering configuration in the Application Policy to determine whether automatic route leaking is needed. If automatic route leaking is needed, the Mist intent engine will automatically perform it.

To configure a Custom VR for an SRX Series Firewall deployed as a WAN Edge Device:

1. From the Mist Portal, navigate to the WAN Edge Device or the WAN Edge Template.
2. From the **CUSTOM VR** tile, click **Add Custom VR**, then give it a name and assign the appropriate Network(s).



Add Custom VR

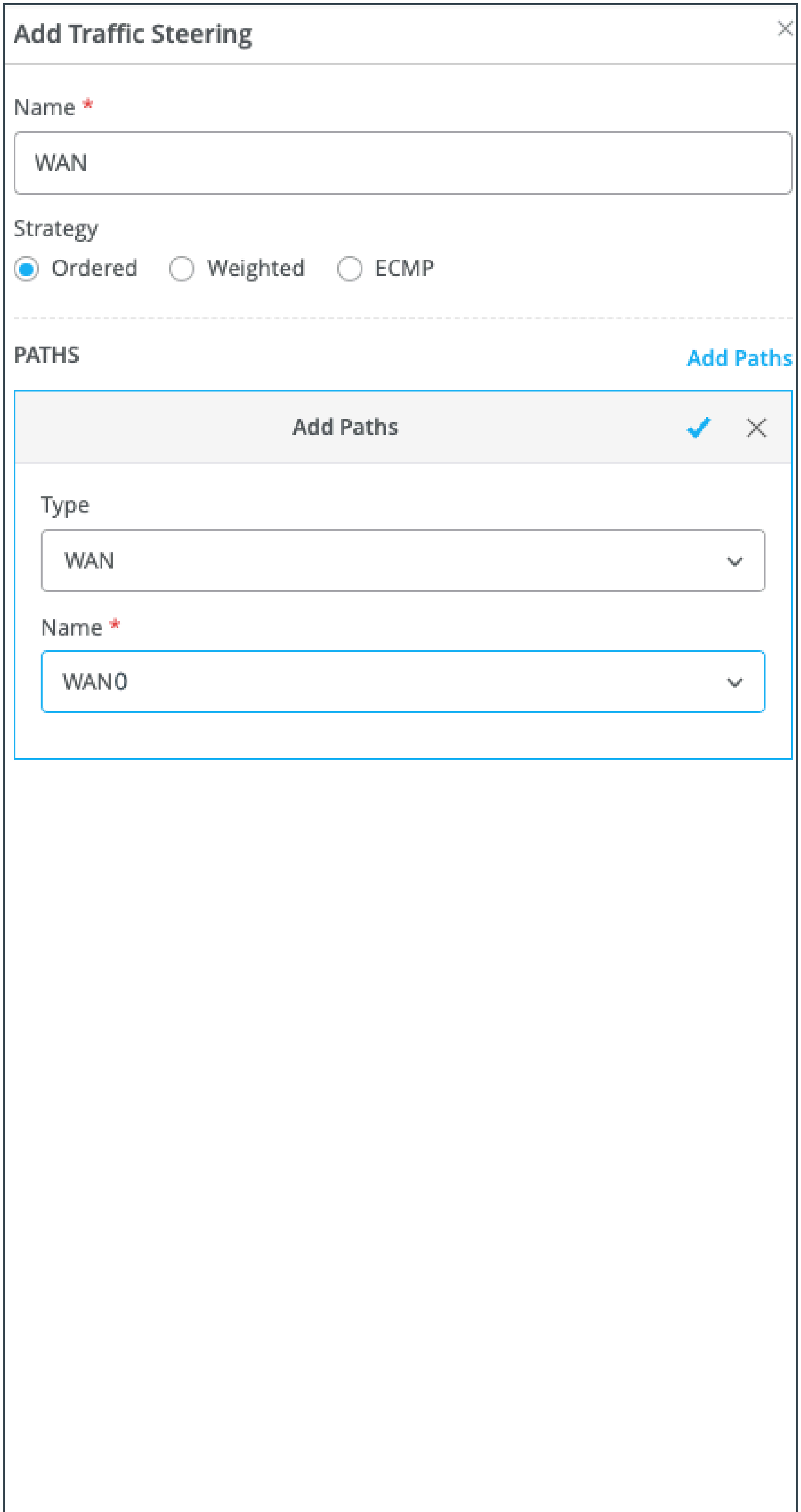
Name *

IoT

Networks *

IoT

3. Click **Add**.
4. Navigate to the **TRAFFIC STEERING** section and select **Add Traffic Steering** to create traffic steering policies for the necessary paths.



Add Traffic Steering

Name *

WAN

Strategy

● Ordered ○ Weighted ○ ECMP

PATHS

Add Paths ✓ ✕

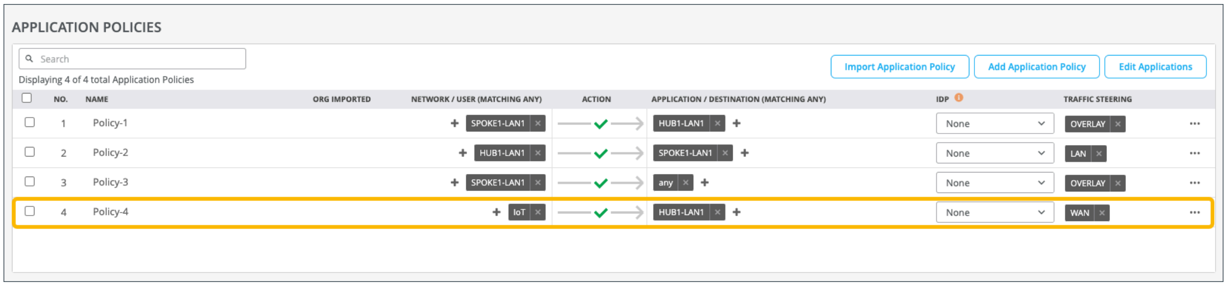
Type

WAN

Name *

WAN0

5. Select the **checkmark** in the **Add Paths** section when you are done, then select **Add** at the bottom of the window.
6. Navigate to the **APPLICATION POLICIES** tile and add or import application policies.
   a. Assign the Network that corresponds with the Custom VR you created in Step 2. Assign the Traffic Steering policy that you created in the Step 4.



APPLICATION POLICIES

Displaying 4 of 4 total Application Policies

□	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING	
□	1	Policy-1		SPOKE1-LAN1	✓	HUB1-LAN1	None	OVERLAY	···
□	2	Policy-2		HUB1-LAN1	✓	SPOKE1-LAN1	None	LAN	···
□	3	Policy-3		SPOKE1-LAN1	✓	any	None	OVERLAY	···
□	4	Policy-4		IoT	✓	HUB1-LAN1	None	WAN	···

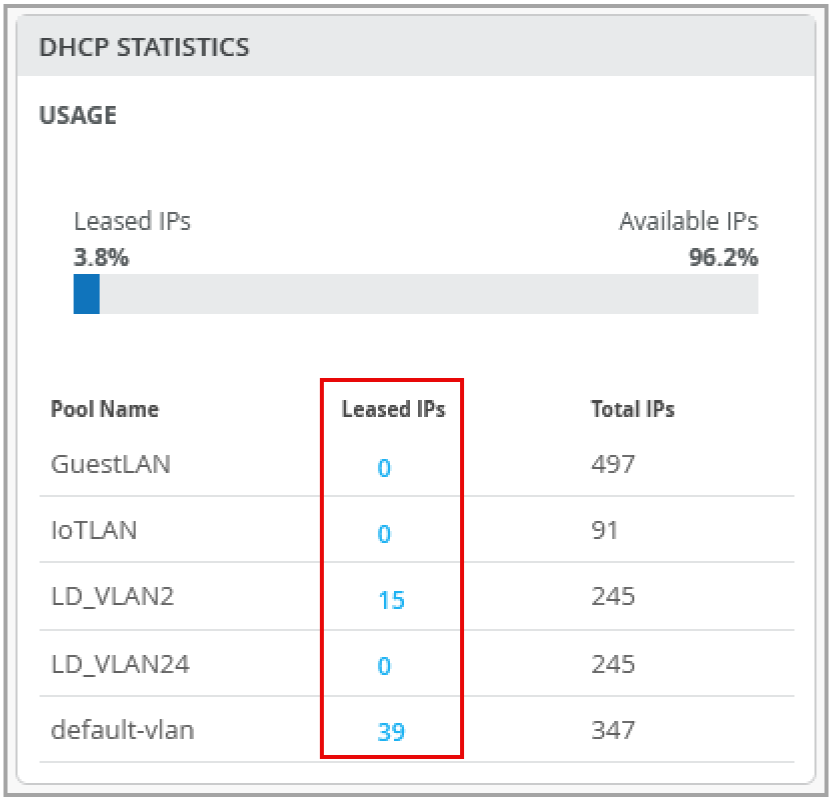
Revoke DHCP Lease on a WAN Edge Device

A DHCP server is assigned to a given network (for example, Guest_LAN). And then when a user device comes online in that specific network and requests a lease, the server in that network provides the device with a DHCP lease. And that lease is associated with the network.

You can view and revoke the DHCP lease on a WAN Edge device from the WAN Edge details page. The revoke option lets you release client devices from their current DHCP lease.

To view and revoke the DHCP lease information:

1. Click **WAN Edges** > *WAN Edges Name* to navigate to a WAN Edge details page.
2. In the DHCP Statistics section on the WAN Edge details page, click the hyperlinked value in the Leased IPs column to navigate to the Leased IPs window.



DHCP STATISTICS

USAGE

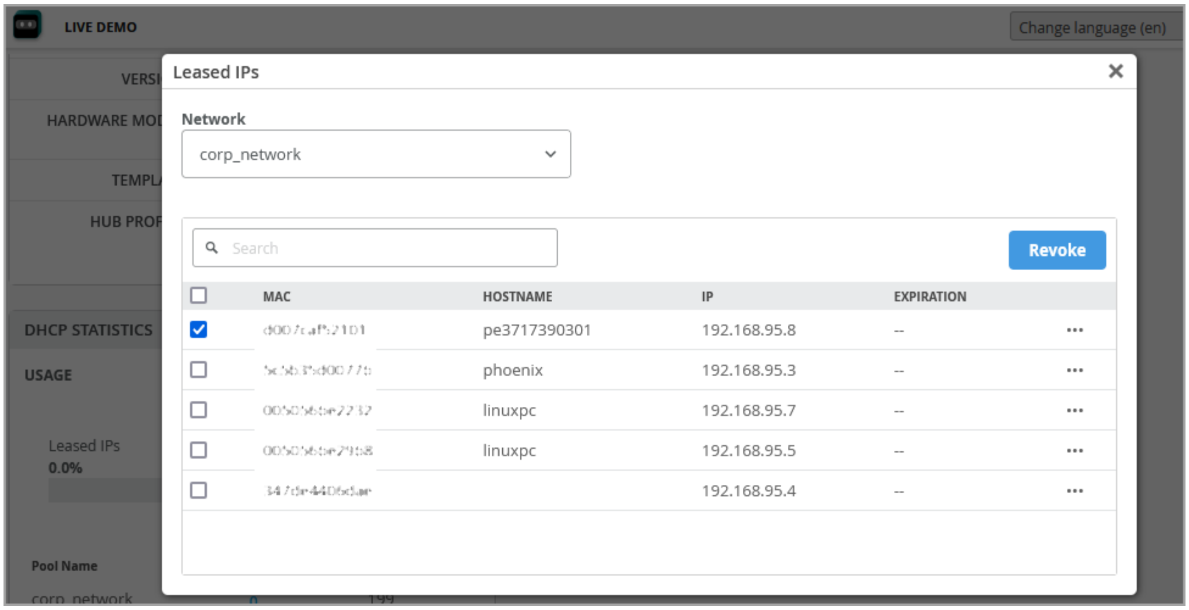
Leased IPs 3.8%

Available IPs 96.2%

Pool Name	Leased IPs	Total IPs
GuestLAN	0	497
IoTLAN	0	91
LD_VLAN2	15	245
LD_VLAN24	0	245
default-vlan	39	347

On the Leased IPs window, you can view the client devices (MAC Addresses or hostnames) along with the leased IP addresses and the lease expiry dates.

3. To revoke the DHCP lease, select a DHCP lease record from the Leased IP window and click **Revoke**.



Leased IPs ✕

Network: corp_network

Search

☐	MAC	HOSTNAME	IP	EXPIRATION	
☑	[redacted]	pe3717390301	192.168.95.8	--	•••
☐	[redacted]	phoenix	192.168.95.3	--	•••
☐	[redacted]	linuxpc	192.168.95.7	--	•••
☐	[redacted]	linuxpc	192.168.95.5	--	•••
☐	[redacted]		192.168.95.4	--	•••

Reserve DHCP IP Address

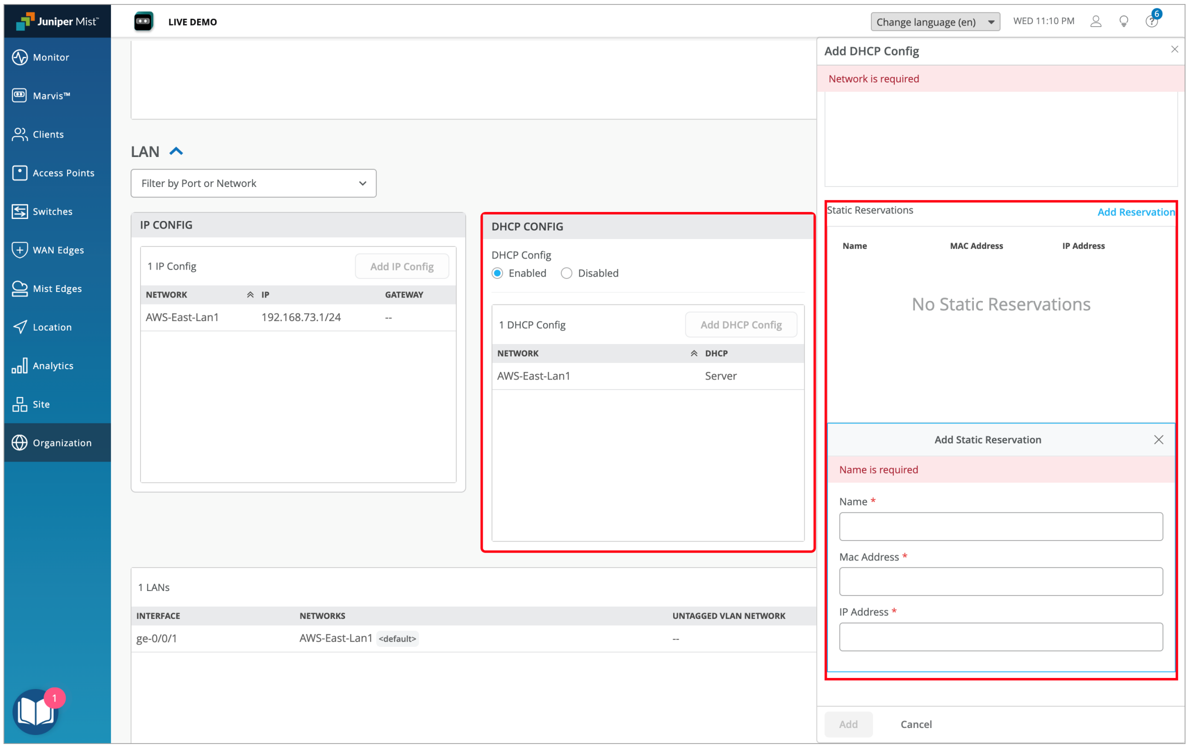
For a WAN Edge LAN interface, you can statically reserve a DHCP address provided that the interface has a DHCP server configured. Static DHCP IP address reservation involves binding a client MAC address to a static IP address from the DHCP address pool.

To reserve a DHCP IP address:

1. To create static DHCP address reservation at the device level, click **WAN Edges** > *WAN Edge Name*.

   If you want to create static DHCP address reservation at the template level, click **Organization** > **WAN Edge Templates** to open the WAN Edge template.
2. Navigate to the **LAN** configuration section.
3. In the DHCP Config box, click a configuration item to open the Edit DHCP Config page.

   Or, if you are creating a new DHCP configuration, click **Add DHCP Config** to open the Add DHCP Config page.



IP CONFIG

1 IP Config

NETWORK	IP	GATEWAY
AWS-East-Lan1	192.168.73.1/24	--

DHCP CONFIG

DHCP Config
● Enabled ○ Disabled

1 DHCP Config

NETWORK	DHCP
AWS-East-Lan1	Server

1 LANs

INTERFACE	NETWORKS	UNTAGGED VLAN NETWORK
ge-0/0/1	AWS-East-Lan1 <default>	--

Add DHCP Config

Network is required

Static Reservations

Name	MAC Address	IP Address

No Static Reservations

Add Static Reservation

Name is required

Name *

Mac Address *

IP Address *

4. Navigate to the Static Reservation section and then click **Add Reservation**.
5. Specify a configuration Name, MAC Address, and an IP Address.
6. Click **Add** and then save the configuration.

5

CHAPTER

WAN Assurance Design

WAN Assurance Design Overview

IN THIS SECTION

Design Guides

The Juniper® SD-WAN driven by Mist AI™ WAN Assurance solution design guides take administrators through advanced configurations for their hub and spoke Juniper SD-WAN deployment. The Juniper® SRX Series Firewall and Juniper® Networks Session Smart™ Routers have unique guides for high availability and full stack implementations. Juniper's SD-WAN solution is part of a full stack of AI-driven wired, wireless, and WAN solutions. The below design guides are platform-specific and require users to have completed the Mist WAN Assurance Configuration Guide.

Session Smart WAN Assurance High Availability and Full Stack Design Guide

Session Smart Routers deployed in Juniper SD-WAN driven by Mist AI WAN Assurance redundant/ highly available deployment requires a Juniper SD-WAN network configured in the Juniper Session Smart WAN Assurance Configuration Guide. The High Availability Design Guide walks users through creating redundant Session Smart WAN edge devices at both the hub and spoke for device and path failover. See "High Availability Design for Session Smart Routers" on page 304.

Session Smart Routers deployed in a Juniper SD-WAN driven by Mist AI WAN Assurance full stack will follow the Session Smart Full Stack Design Guide. This guide requires a Session Smart Juniper SD-WAN deployment admins who wish to add switches and APs for an end-to-end Juniper full stack of AI-driven wired, wireless, and WAN solutions. See "Full Stack Design for Session Smart Routers" on page 324.

SRX Series Firewall High Availability and Full Stack Design Guide

Juniper SD-WAN driven by Mist AI SRX Series Firewalls in highly available clusters must be deployed in Juniper SD-WAN driven by Mist AI WAN Assurance per the Juniper Mist WAN Configuration Guide. The SRX Series High Availability Design Guide walks users through creating a redundant SRX Series device at WAN edge for device and path failover.

SRX Series Firewalls in Mist WAN Assurance that wish to add the full stack of AI-driven solutions for wired, wireless, and WAN must first have a network deployed following the Mist WAN Configuration Guide. The full stack design guide is for administrators that want switches and APs included in their WAN for an end-to-end Juniper full stack Juniper Mist cloud solution.

RELATED DOCUMENTATION

Introduction to Juniper Mist WAN Assurance | 2

Juniper Mist WAN Assurance Platform Considerations | 10

Juniper Mist WAN Assurance Configuration Hierarchy | 13

Full Stack Design for Session Smart Routers

IN THIS SECTION

The Juniper® SD-WAN driven by Mist AI™ Full Stack design example is a follow-up to the Session Smart™ Router Mist WAN Assurance deployment documentation found in the Juniper Mist WAN Configuration Guide.

Overview

IN THIS SECTION

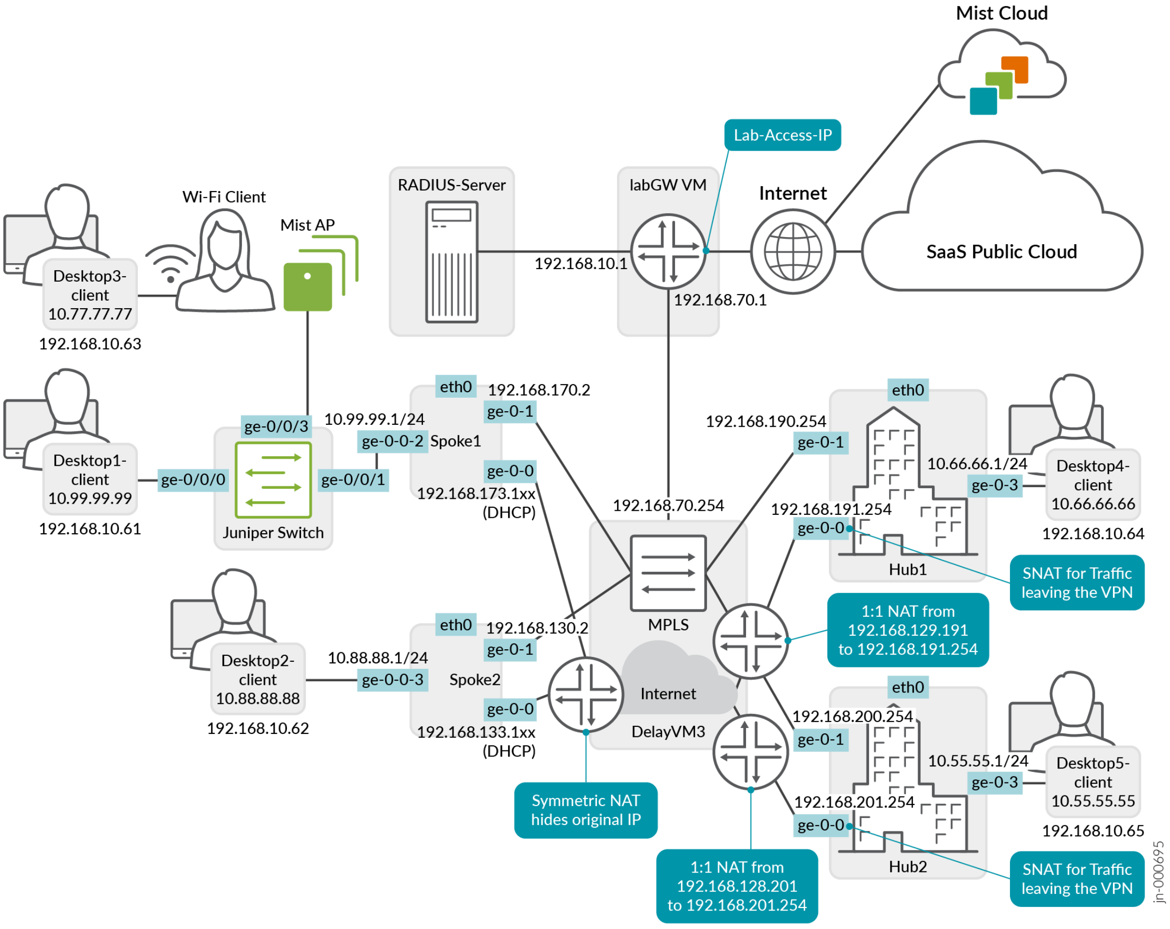
With this example you're expanding network capabilities by integrating Mist APs and Juniper EX Switches. This is more than just WAN Assurance, it's the Juniper AI Driven Enterprise. This full stack guide shows you how to set up your Juniper SD-WAN Session Smart WAN edge devices in concert with Mist wireless Access Points (APs) deployed in Wireless Assurance, and Juniper EX Series Switches deployed in Wired Assurance. This brings all your network devices into a cohesive onboarding, monitoring, and troubleshooting dashboard.

The Session Smart Full Stack Guide begins at the highest level of WAN Assurance, focusing on a key component known as the Session Smart Router. After completing the Juniper Validated Design (JVD) topology found in the Juniper Mist WAN Configuration Guide, you should already have this WAN Edge device deployed in a hub and spoke network. The Session Smart Router serves as the WAN edge device and foundation for building out your entire network. We'll evaluate and test the complete end-to-end solution to further optimize your network. This test encompasses the entire technology stack and is specifically designed for a branch that utilizes Juniper equipment.

For successful implementation of this guide, 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. Onboarding those into your LAN network for Mist management gives admins the Juniper AI Driven Enterprise to monitor and manage their WAN edge, switches, and APs all in the Mist dashboard.

Figure 168 on page 306 shows the Full Stack Juniper Mist WAN Assurance topology used in this example.

Figure 168: 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 found in the Juniper Mist WAN Configuration Guide topology. We'll show you how to do this using a Spokes configuration template found in the Mist WAN Configuration Guide. See "Configure WAN Edge Templates for Session Smart Routers " on page 92.

- **Desktop3 VM** (VLAN1077) is re-used and no longer attached to **Spoke3**. **Desktop3 VM** is now a viewer for the Raspberry Pi, the Wireless Client. Alternatively, you could use a local notebook.

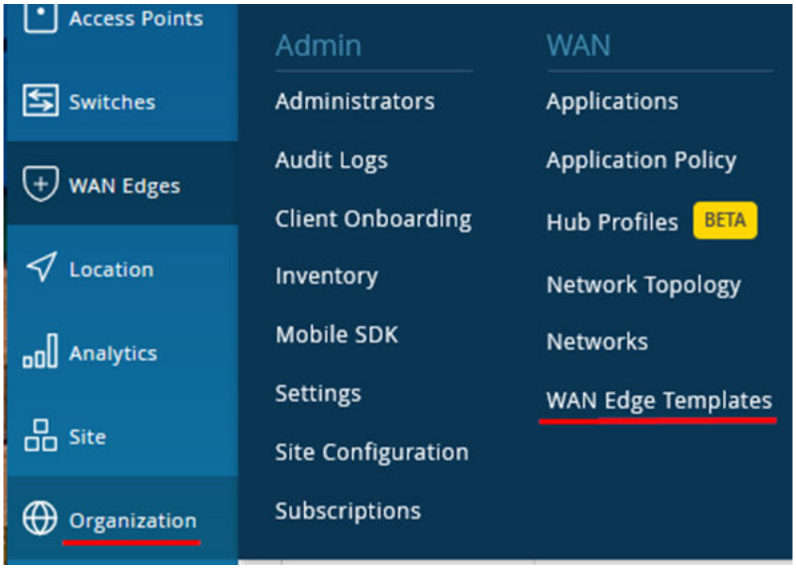
- **Desktop1 VM** (VLAN1099) is no longer directly attached to **Spoke1** and needs to be re-attached to the interface **ge-0/0/0** of the new branch switch.

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.

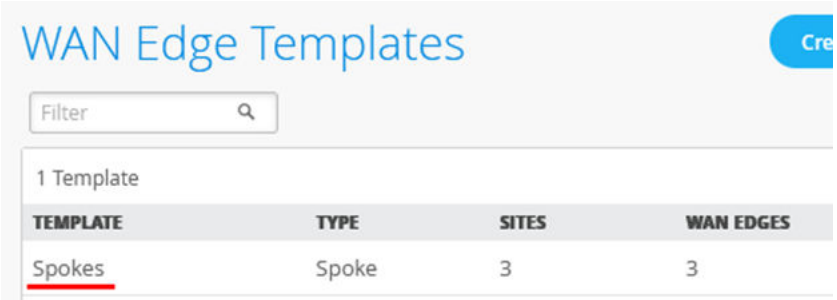
1. In the Juniper Mist™ portal, click **Organization** > **WAN** > **WAN Edge Templates**.

   Figure 169: Navigate to WAN Edge Template

   A list of existing templates, if any, appears.

   Figure 170: List of WAN Edge Templates

   WAN Edge Templates

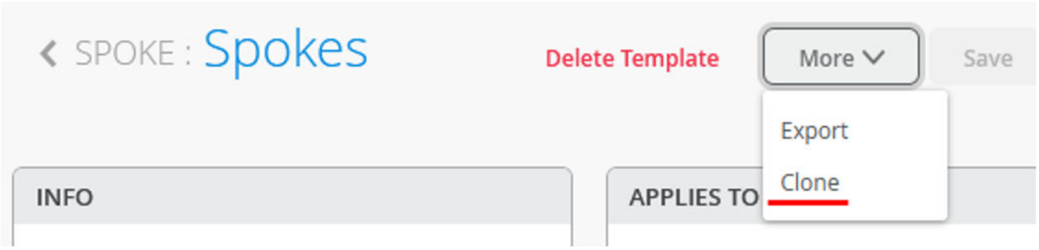
   1 Template

TEMPLATE	TYPE	SITES	WAN EDGES
Spokes	Spoke	3	3

   Create a spoke template by cloning an existing spoke template.

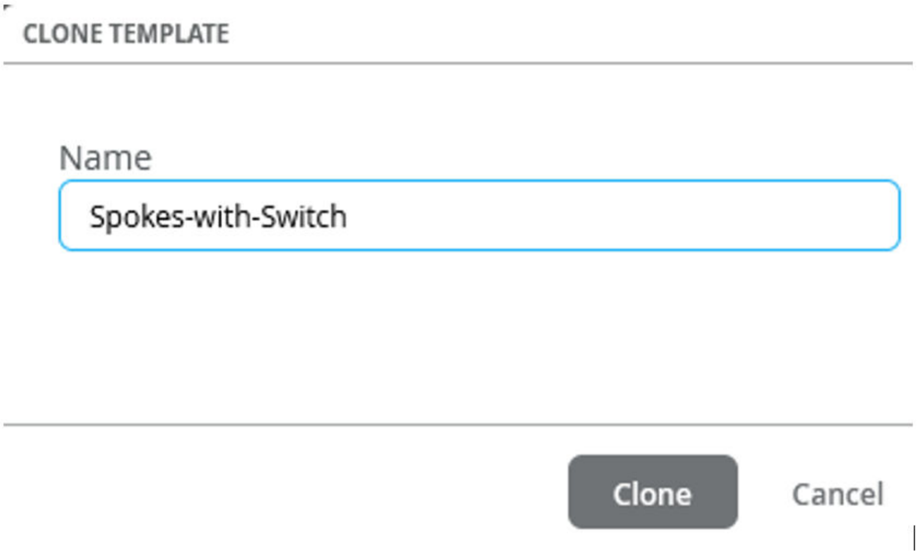
2. Click **More** and select **Clone**.

Figure 171: Selecting Clone Option for Template



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

Figure 172: Saving Cloned Template



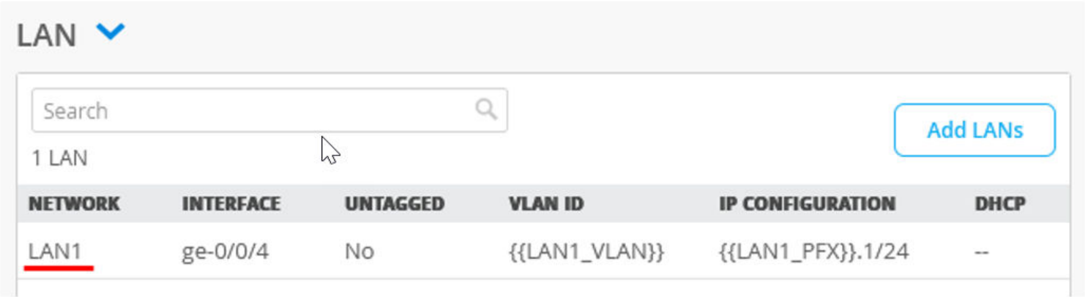
Name: Spokes-with-Switch

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

Edit the LAN Interface

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

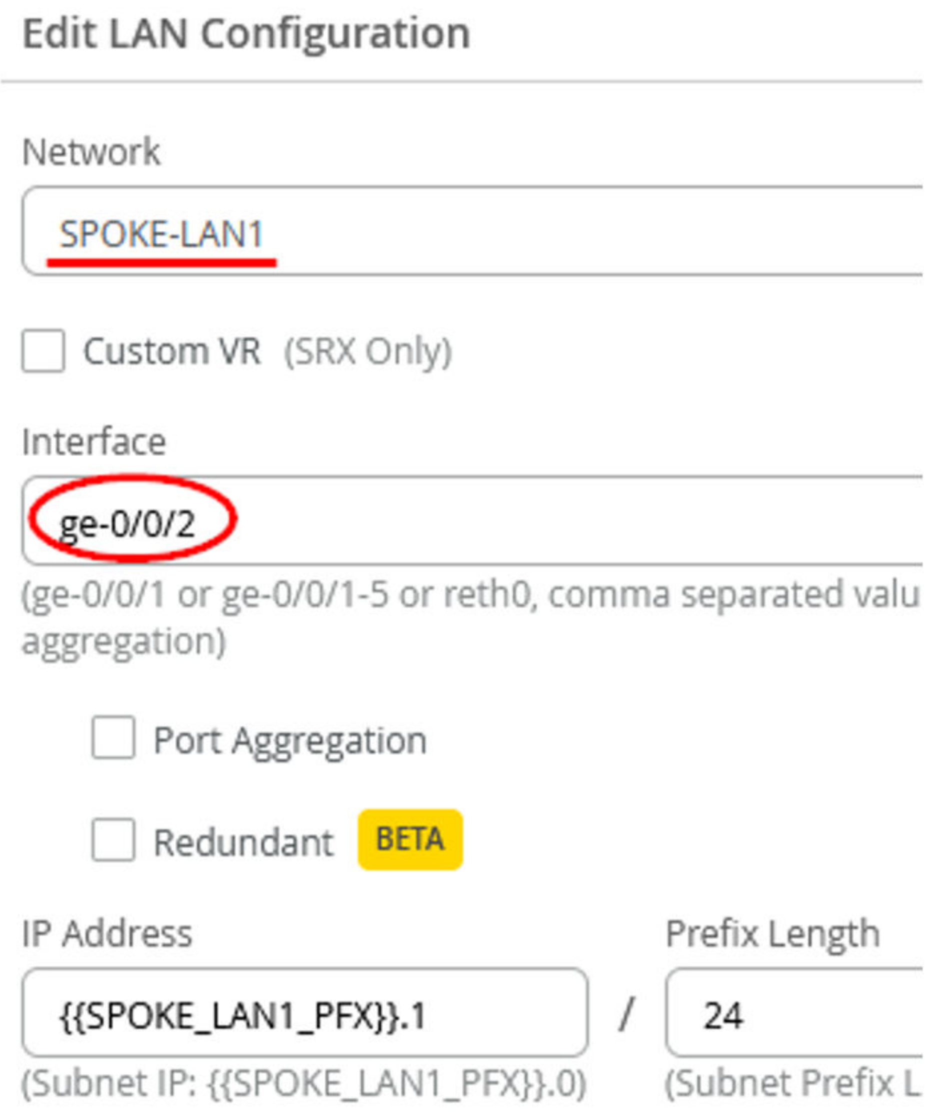
Figure 173: LAN Interface Configuration



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

Change the name of LAN interface as **SPOKE-LAN1** and set the **Interface** to ge-0/0/2.

Figure 174: Modify LAN Interface Configuration



Edit LAN Configuration

Network

SPOKE-LAN1

□ Custom VR (SRX Only)

Interface

ge-0/0/2

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

□ Port Aggregation

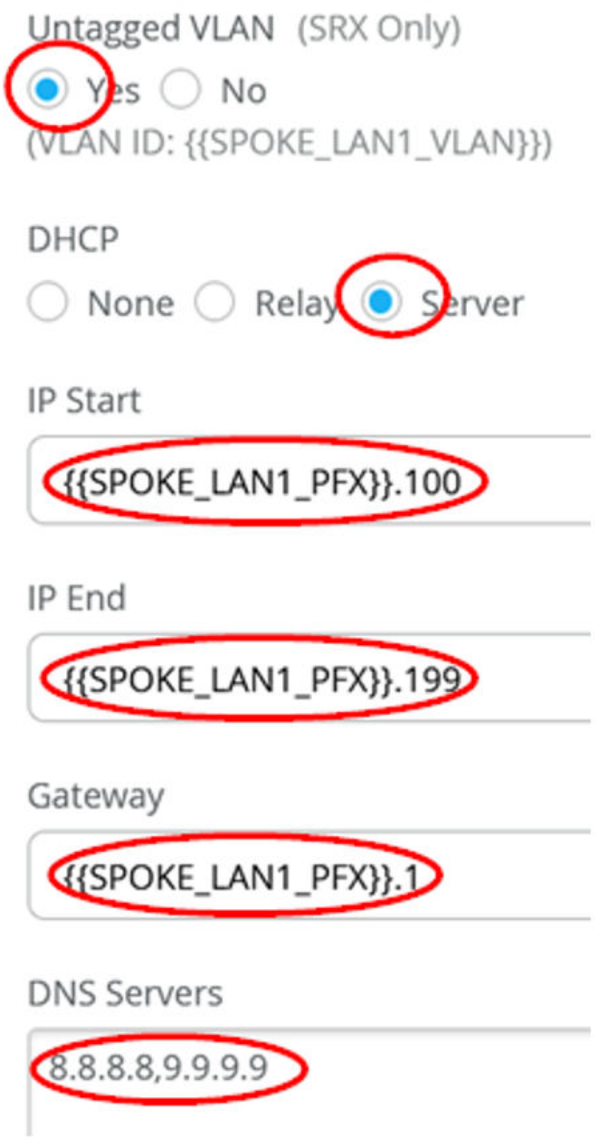
□ Redundant BETA

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

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

2. Continue to configure the SPOKE-LAN1 LAN interface:

Figure 175: 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

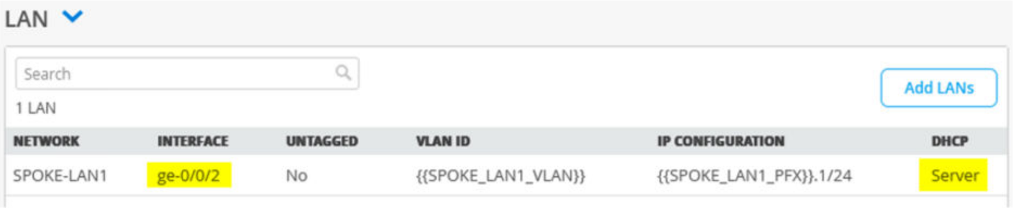
DNS Servers

8.8.8.8,9.9.9.9

- **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

3. Figure 176 on page 312shows the LAN interface you modified.

Figure 176: Summary of LAN Interface

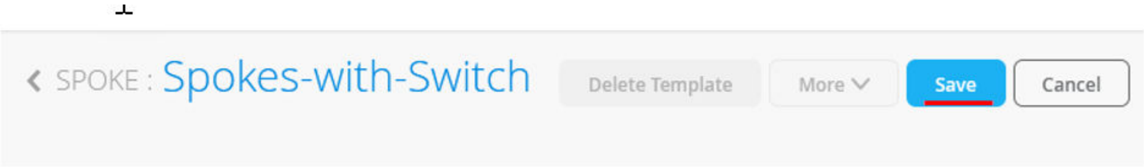


1 LAN

NETWORK	INTERFACE	UNTAGGED	VLAN ID	IP CONFIGURATION	DHCP
SPOKE-LAN1	ge-0/0/2	No	{{SPOKE_LAN1_VLAN}}	{{SPOKE_LAN1_PFX}}.1/24	Server

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

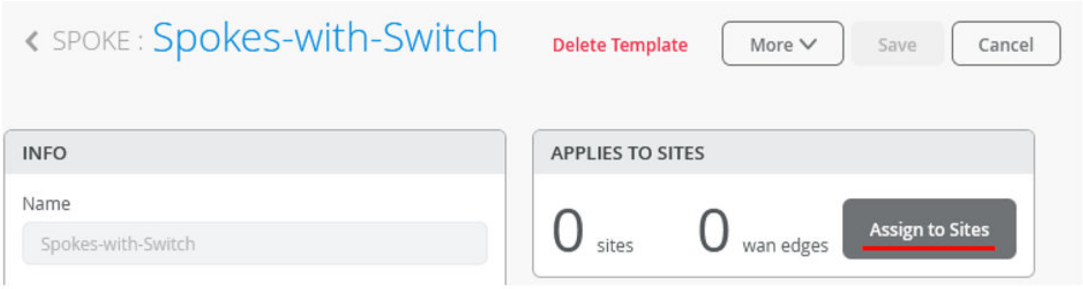
Figure 177: Saving WAN Edge Template



Assign the New Template to a Site

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

Figure 178: Assign Spoke Templates to Sites

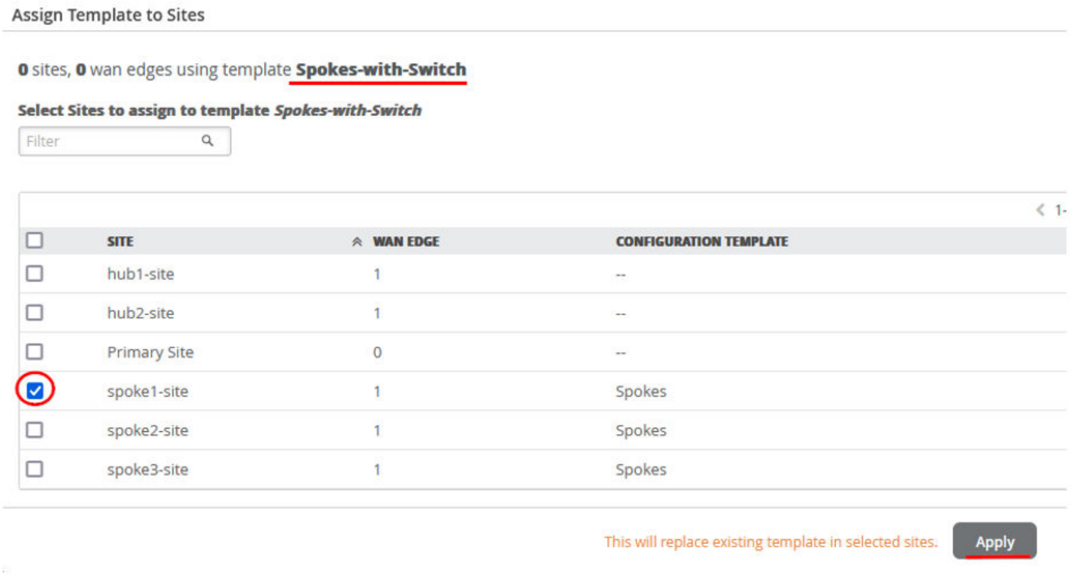


Name: Spokes-with-Switch

0 sites 0 wan edges

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

Figure 179: Select Sites to Assign Spoke Templates



Assign Template to Sites

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

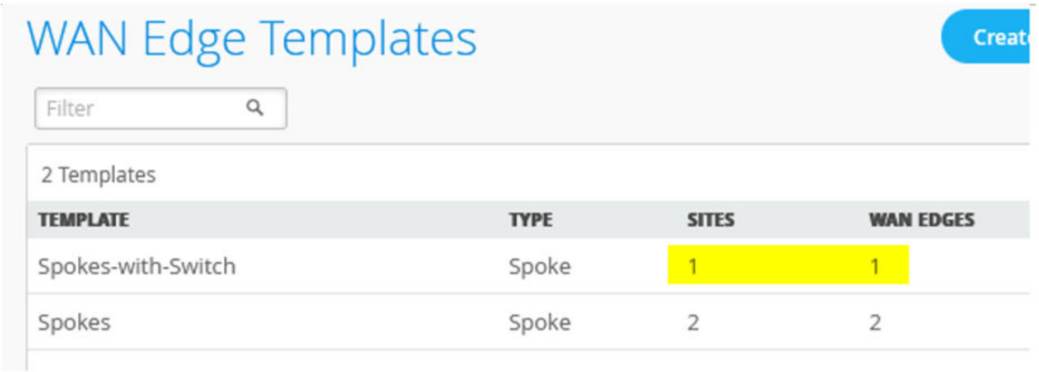
Select Sites to assign to template *Spokes-with-Switch*

☐	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.

3. Review the Template Settings as shown in Figure 180 on page 313.

Figure 180: Details of WAN Edge Template



WAN Edge Templates

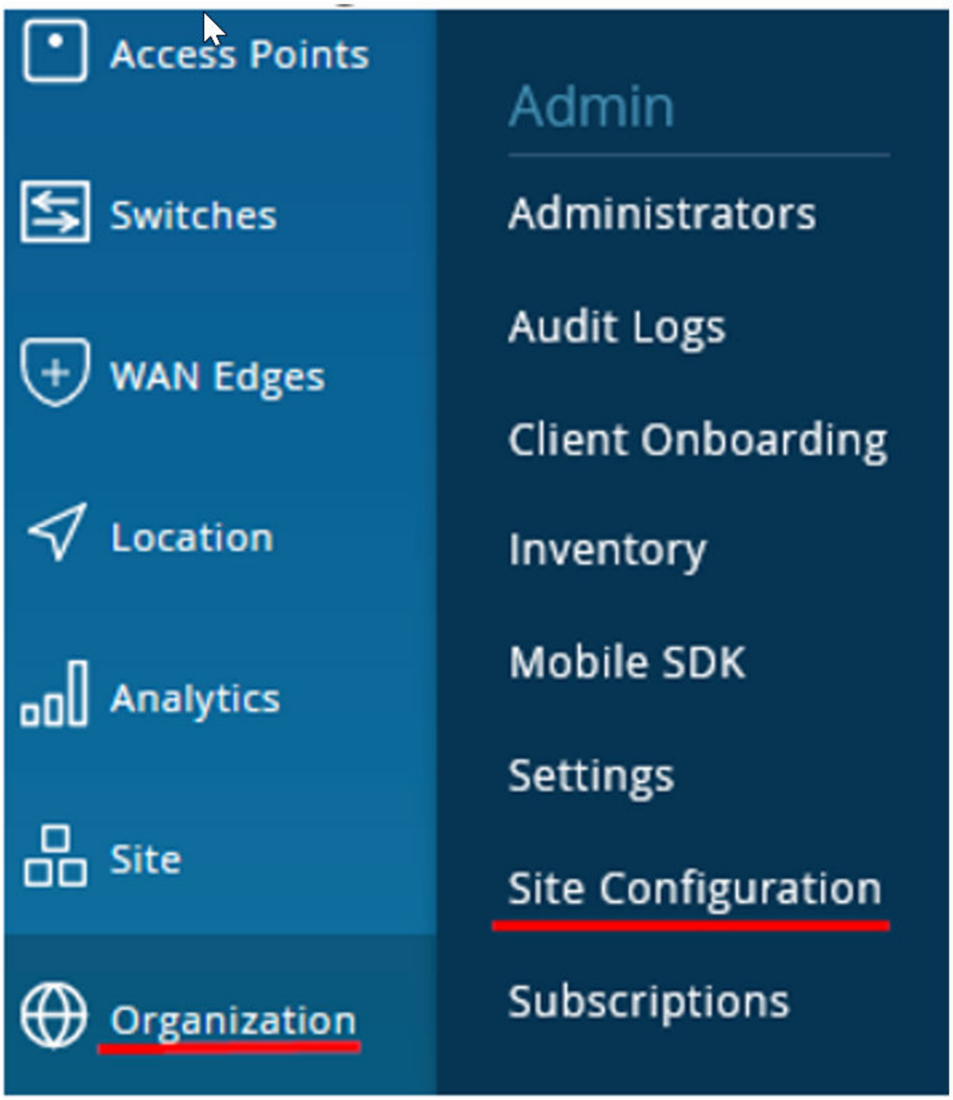
2 Templates

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

Change Spoke Variables in Preparation for Onboarding

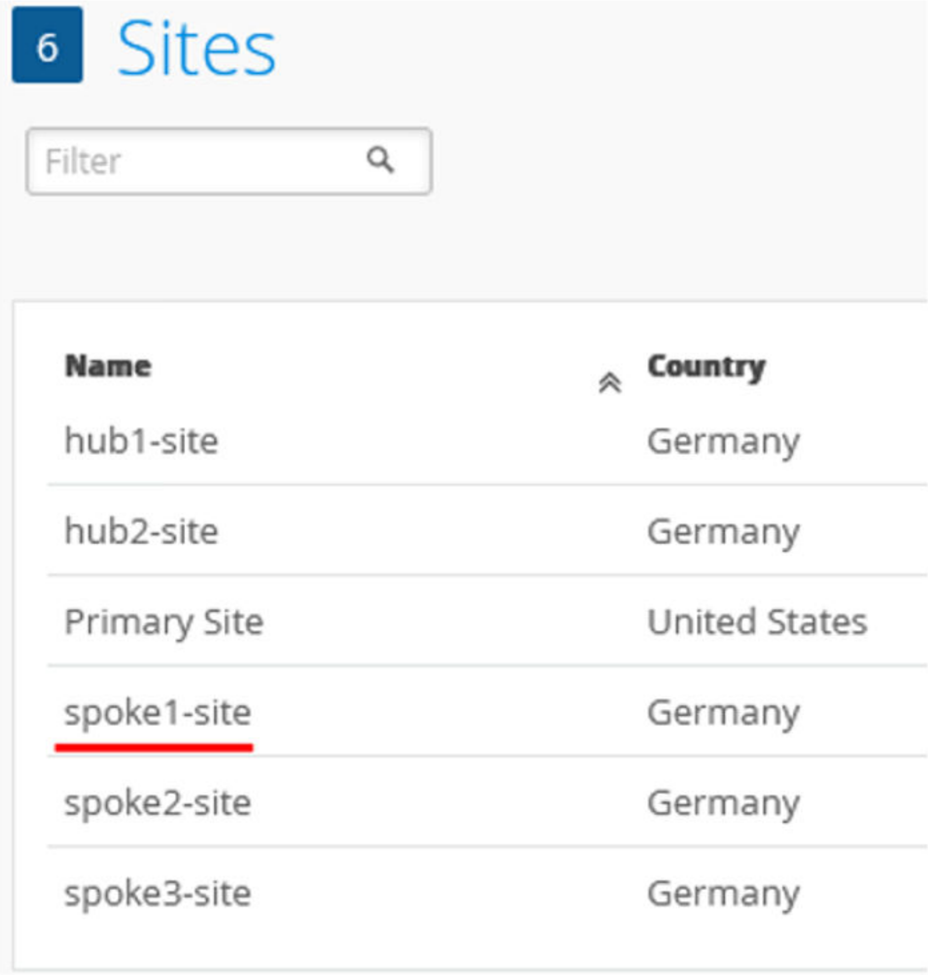
1. In the Juniper Mist cloud portal, click **Organization** >**Admin** > **Site Configuration**. A list of existing sites appears.

Figure 181: Navigate to Site Configuration



2. Click on the site **spoke1-site**. This is the same site, to which you have applied the template in previous procedure.

Figure 182: Selecting Sites for Modifying

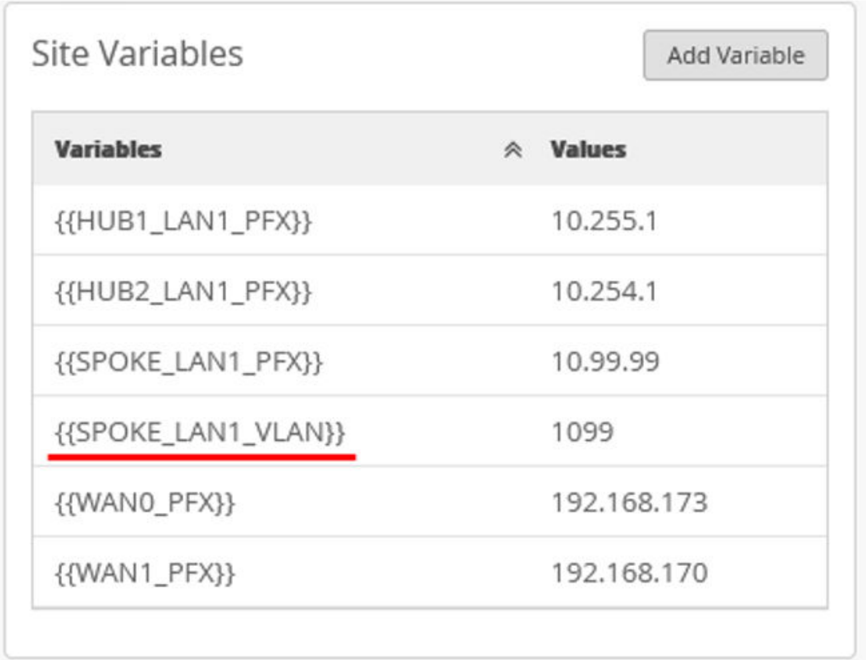


6 Sites

Name	Country
hub1-site	Germany
hub2-site	Germany
Primary Site	United States
spoke1-site	Germany
spoke2-site	Germany
spoke3-site	Germany

3. Scroll down the screen to the **Site Variables** settings pane and select the variable {{SPOKE_LAN1_VLAN}}.

Figure 183: Site Variables

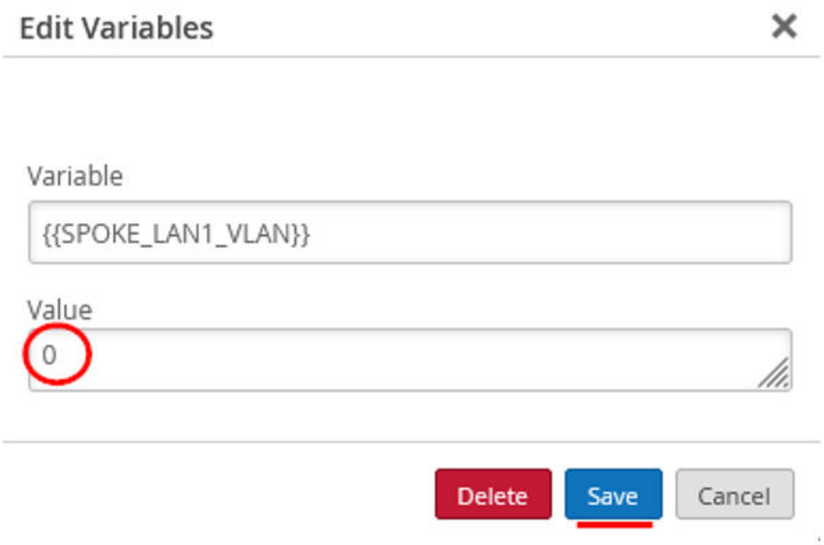


Site Variables

Variables	Values
{{HUB1_LAN1_PFX}}	10.255.1
{{HUB2_LAN1_PFX}}	10.254.1
{{SPOKE_LAN1_PFX}}	10.99.99
{{SPOKE_LAN1_VLAN}}	1099
{{WAN0_PFX}}	192.168.173
{{WAN1_PFX}}	192.168.170

4. Change the **Value** to 0 as you do not need a tagged VLAN, and then click **Save**.

Figure 184: Modify Site Variables



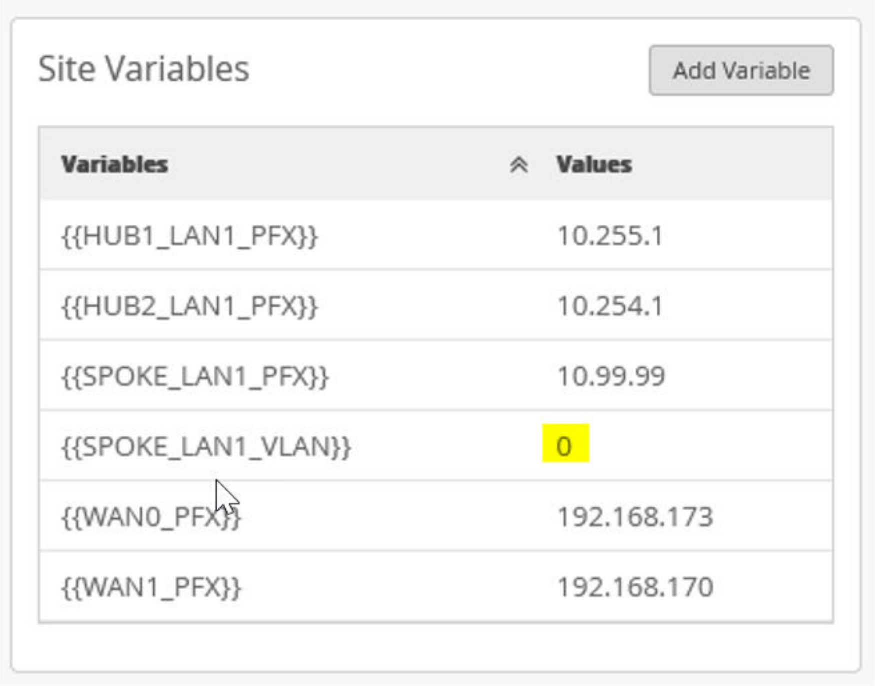
Edit Variables

Variable: {{SPOKE_LAN1_VLAN}}

Value: 0

5. Review your changes in the **Site Variable** pane.

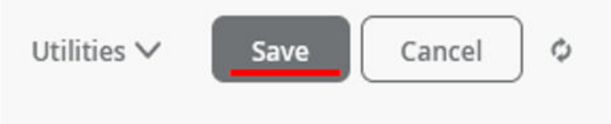
Figure 185: Site Variables



Variables	Values
{{HUB1_LAN1_PFX}}	10.255.1
{{HUB2_LAN1_PFX}}	10.254.1
{{SPOKE_LAN1_PFX}}	10.99.99
{{SPOKE_LAN1_VLAN}}	0
{{WAN0_PFX}}	192.168.173
{{WAN1_PFX}}	192.168.170

6. Save your changes.

Figure 186: Saving Changes



Add Your Switch to the Topology

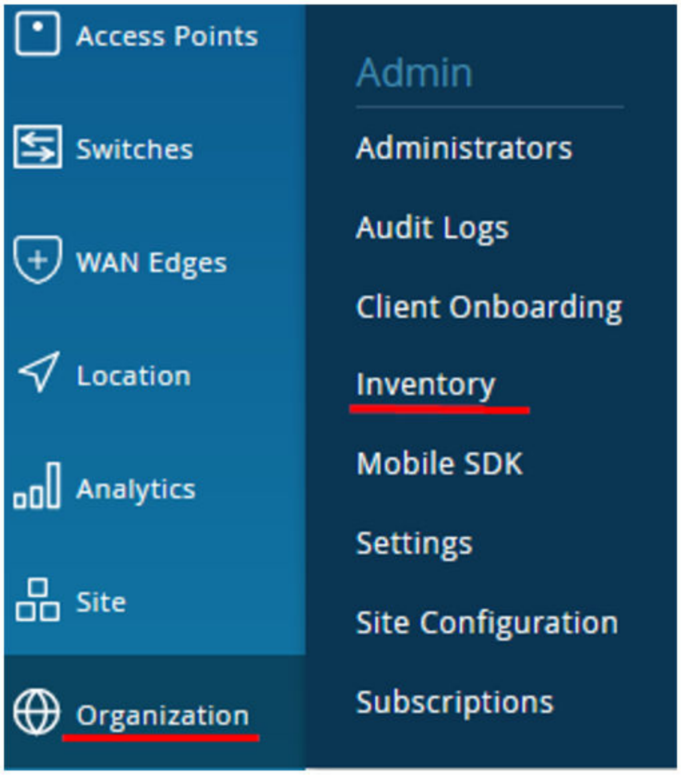
Now it is time to onboard your switch and add it to your infrastructure. For details on how to onboard your switch, refer to the product documentation for your switch in the Juniper TechLibrary.

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:

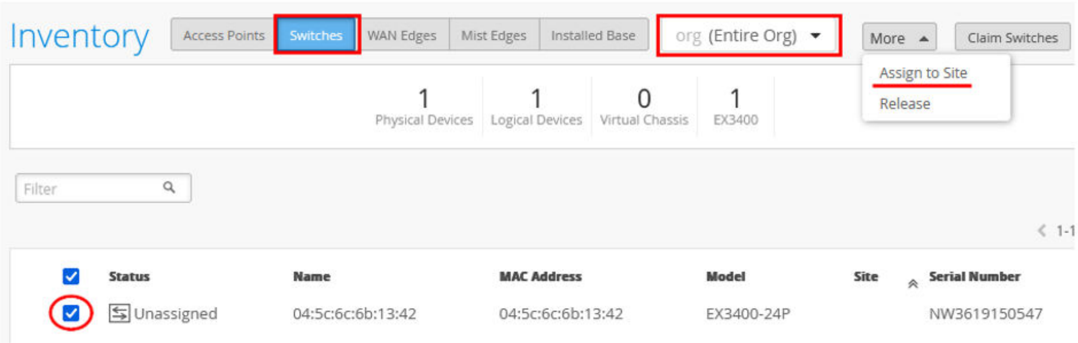
1. In the Juniper Mist portal, click **Organization** > **Admin** > **Inventory**.

Figure 187: Navigating to Inventory



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

Figure 188: EX Series Switch in Inventory

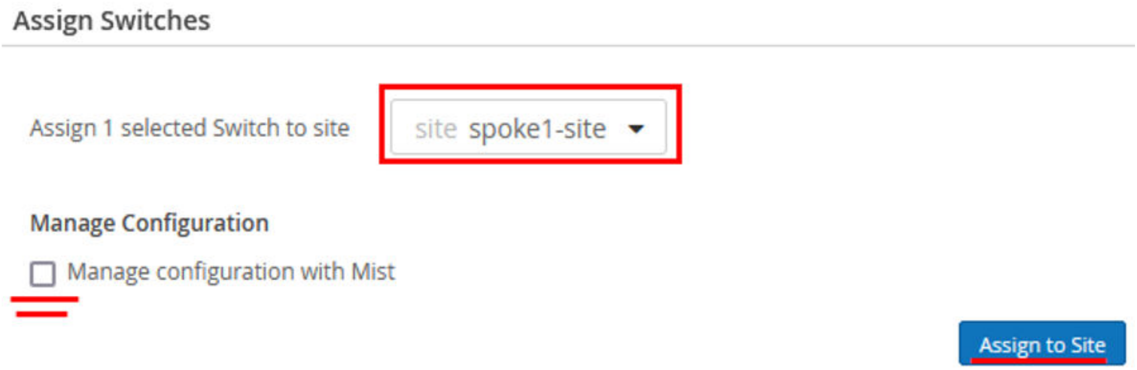


☑	Status	Name	MAC Address	Model	Site	Serial Number
☑	Unassigned	04:5c:6c:6b:13:42	04:5c:6c:6b:13:42	EX3400-24P		NW3619150547

3. Select your new switch and click **Assign to Site**.
4. In 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.

Figure 189: Selecting Site for Assigning Switch



Assign Switches

Assign 1 selected Switch to site: site spoke1-site

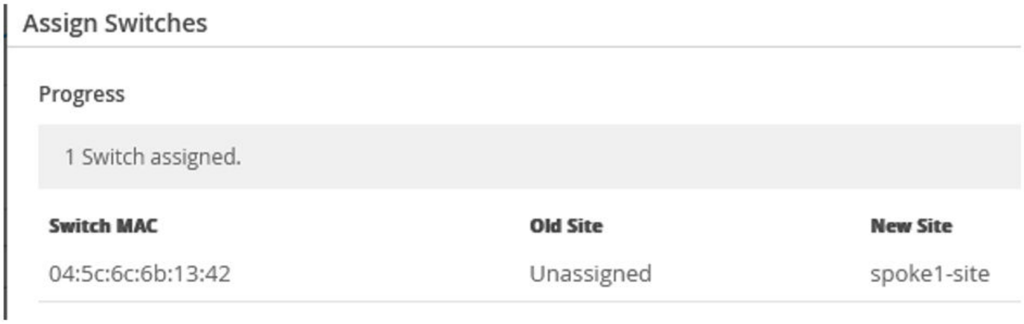
Manage Configuration

□ Manage configuration with Mist

5. Click **Assign to Site**.
6. Confirm the changes in the inventory once you assign the device to the site.

   You can see **spoke1-site** under **New Site**.

Figure 190: Assigned Switch to Site Details



Assign Switches

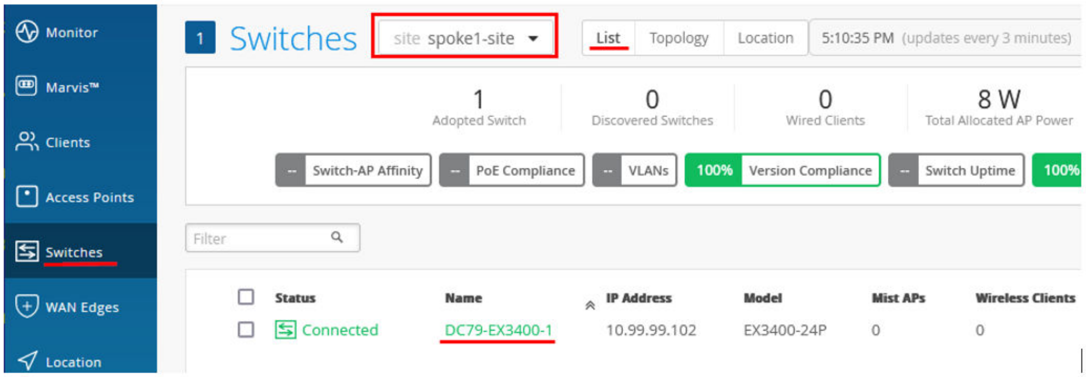
Progress

1 Switch assigned.

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

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

Figure 191: Selecting Assigned Switch for Modification



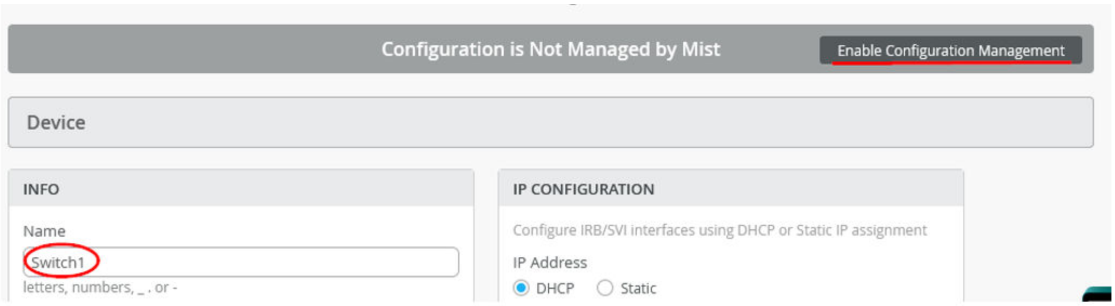
Status	Name	IP Address	Model	Mist APs	Wireless Clients
Connected	DC79-EX3400-1	10.99.99.102	EX3400-24P	0	0

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

8. Click the switch to open the switch configuration page.

9. Verify the device name, then scroll down to **Switch Configuration** section and check **Enable Configuration Management**.

Figure 192: Configuration of Assigned Switch

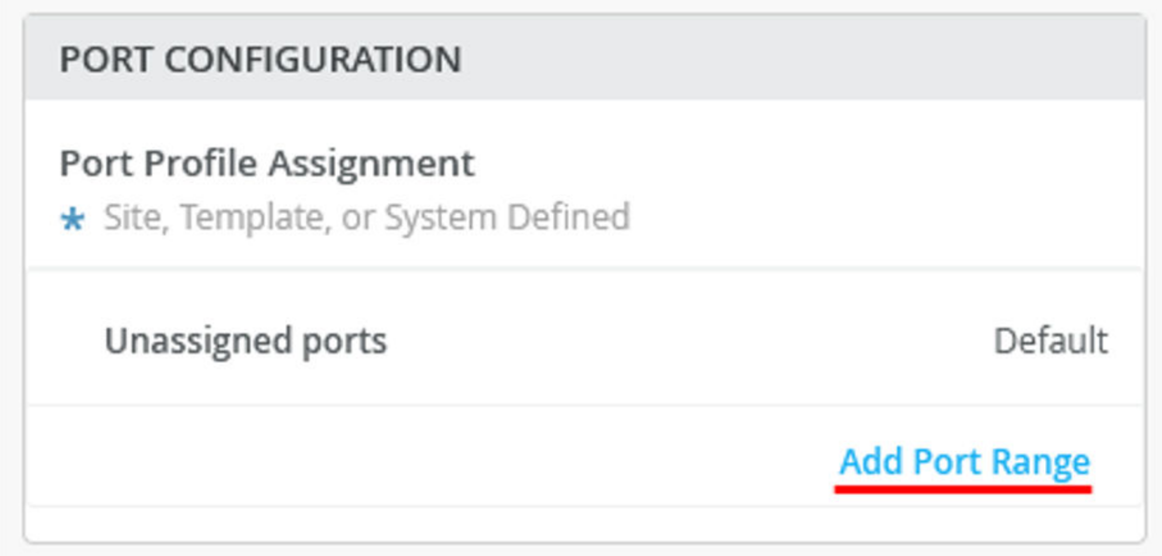

Configuration is Not Managed by Mist
Enable Configuration Management
Device
INFO
IP CONFIGURATION
Configure IRB/SVI interfaces using DHCP or Static IP assignment
letters, numbers, _ . or -

Name: Switch1

IP Address: ● DHCP ○ Static

10. Under **Port Configuration**, click **Add Port Range**.

Figure 193: Port Configuration of Assigned Switch



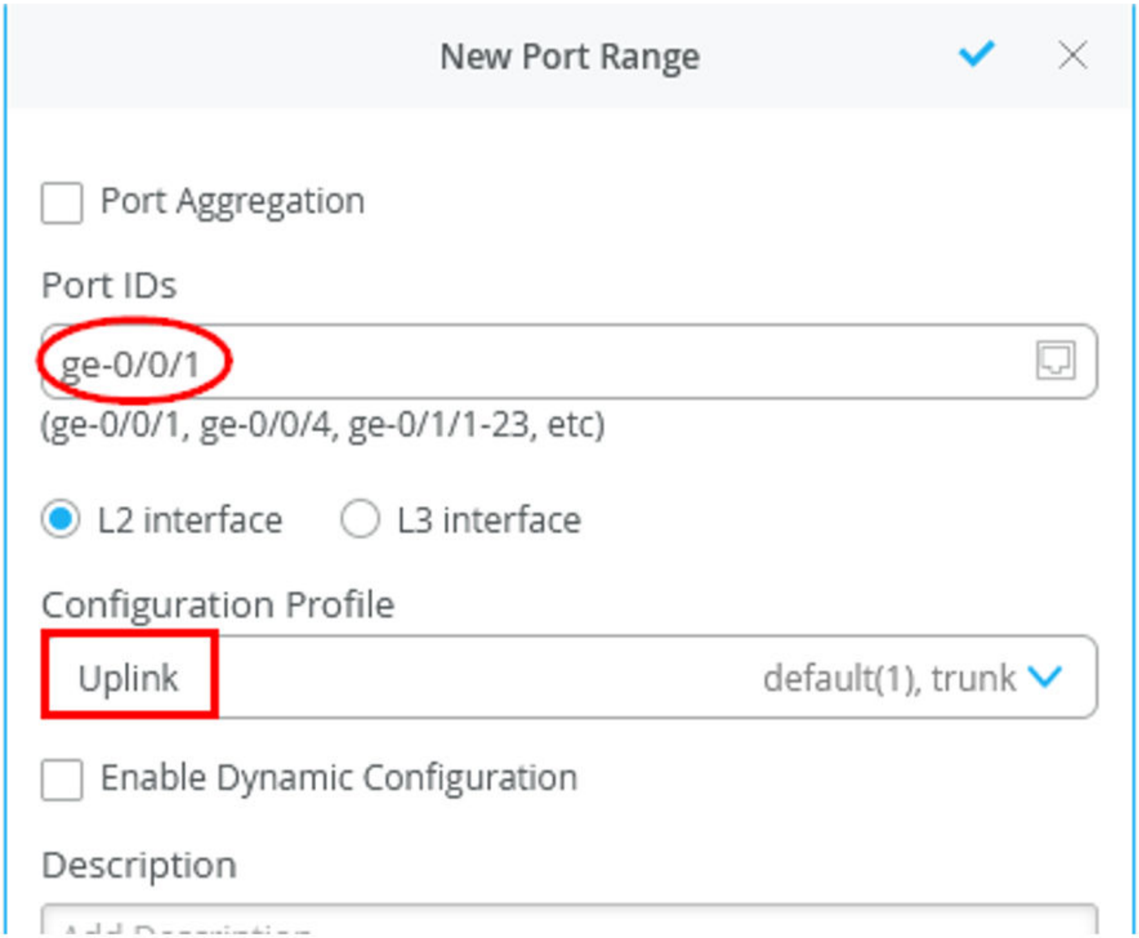
PORT CONFIGURATION

Port Profile Assignment

Unassigned ports: Default

11. In the New Port Range page, configure the following options:
    - Set the **Port IDs** as **ge-0/0/1**.
    - Select the existing **Configuration Profile** as **Uplink**.

Figure 194: 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

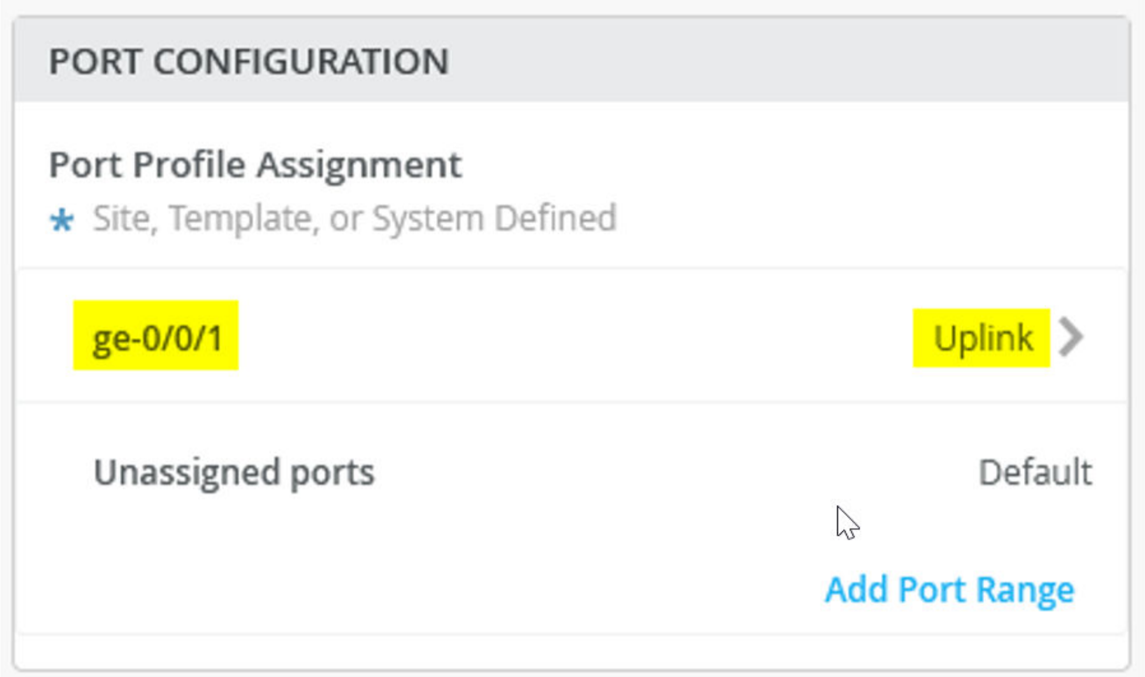
□ Enable Dynamic Configuration

Description

Add Description

12. Figure 193 on page 321 shows the summary of port configuration.

Figure 195: Port Configuration of Assigned Switch



PORT CONFIGURATION

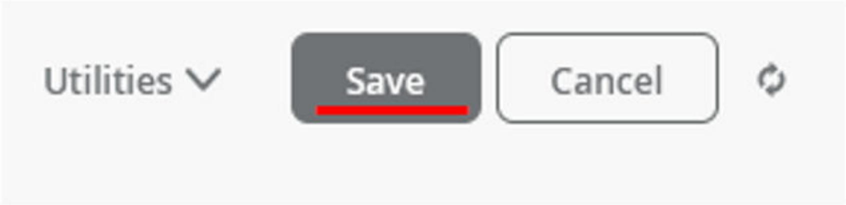
Port Profile Assignment

* Site, Template, or System Defined

ge-0/0/1	Uplink
Unassigned ports	Default

13. Save your changes.

Figure 196: Save Changes



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

SEE ALSO

- WAN Assurance Configuration Overview | 31
- Configure Sites and Variables for Session Smart Routers | 33
- Configure Networks for Session Smart Routers | 38
- Configure Applications for Session Smart Routers | 48
- Configure Application Policies on Session Smart Routers | 58

High Availability Design for Session Smart Routers

IN THIS SECTION

Juniper® Networks Session Smart™ High Availability (HA) Design Guide is for administrators who want to deploy HA Juniper Session Smart Routers at the Edge, but not for Whitebox setups.

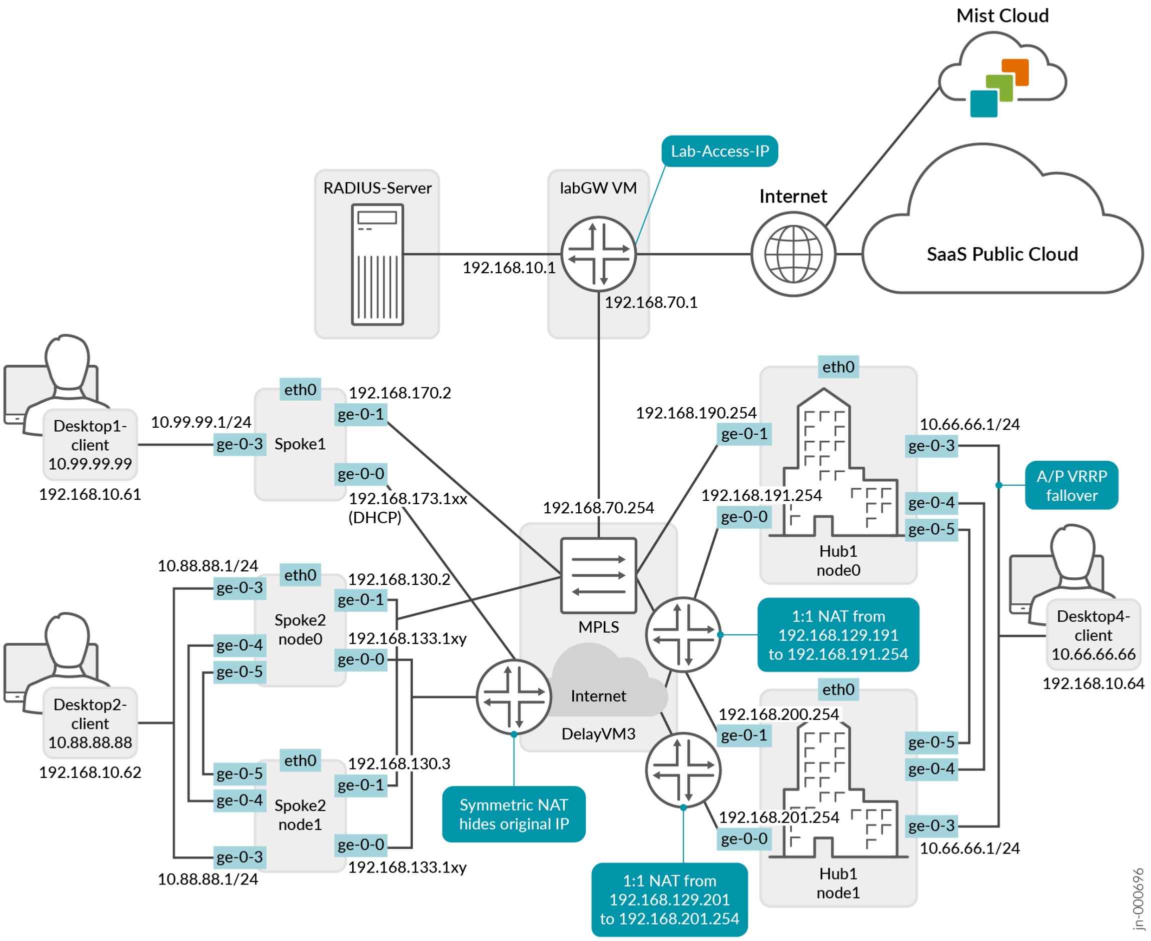
In this documentation you'll find step-by-step guidance for setting up a highly available hub and spoke deployment using Juniper® Mist WAN Assurance. Since this HA deployment builds upon the topology referenced in the Juniper Session Smart WAN Assurance Configuration Guide, you'll need to configure your network with that topology first. Building upon the reference topology in the Juniper Session Smart WAN Assurance Configuration Guide, you'll learn how to setup Session Smart Routers in an HA cluster configuration.

NOTE: Devices in an HA pair must be identical. An HA pair with two SSR120s will work. An HA pair with one SSR120 and one SSR102-AE will not work.

Overview

You will deploy a highly available Hub and Spoke as shown in Figure 197 on page 325. Here we see the Session Smart highly available Juniper Mist WAN Assurance topology for this HA Design Guide.

Figure 197: Juniper Validated Design Mist WAN Assurance with HA Session Smart WAN Edges



NOTE: Before you get started, be sure you've setup the topology described in the Juniper WAN Assurance Configuration Guide.

Interfaces

The Interfaces use the following pattern for each node:

Node0: ge-0/0/x

Node1: ge-1/0/x

WAN Interfaces for HA hubs require static IP addresses. Spokes reach out across the overlay to these WAN interface endpoints.

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. WAN interfaces on spoke devices 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.

LAN Interfaces

You'll need to define the LAN interfaces for both HA hubs and spokes are as redundant interfaces, and then specify the interfaces together as **ge-0/0/x, ge-1/0/x**. This will make them VRRP Interfaces.

Redundant VRRP Interfaces are only Active/Passive, meaning only the currently active Session Smart Router interface will broadcast VRRP.

The redundant VRRP interfaces must be in the same Layer 2 domain and need a single static IP address. The Active/Passive Interfaces will have a shared MAC address. Based on the device, the system decides who will be node0 and who will be node1.

- The lowest MAC address will be selected for node0.
- For Redundant VRRP interfaces, you can define which **node** is the primary, but we recommend leaving the default to node0 for consistency.

NOTE: It's important to be aware of the two specific Ethernet interfaces that handle HA synchronization and fabric data exchange on the supported devices. See the Session Smart documentation https://www.juniper.net/documentation/us/en/software/session-smart-router/docs/concepts_ha_theoryofoperation.

The HA synchronization link ensures that the two devices are chronologically synchronized and can swap appropriately in the event of an interface or device failure. The synchronization interface serves as the back-or-midplane of a chassis-based router.

The fabric interface is a forwarding interface between two nodes in a router and is used when the ingress interface and egress interface for a given session are active on different nodes. The synchronization and fabric interfaces are usually the two last ports of the system. You must wire them back-to-back with direct patch cables.

Configure High Availability

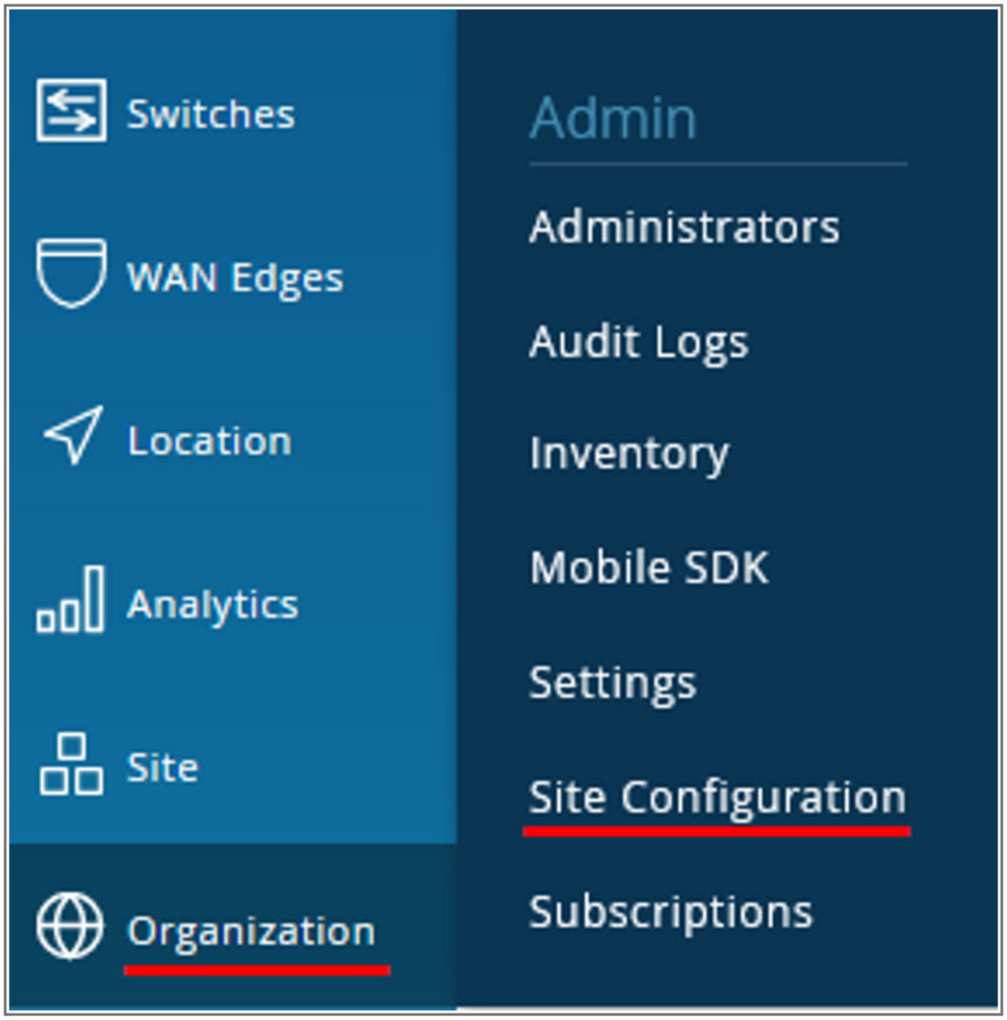
The following steps outline the process of adding the HA Hub Site.

To add a highly available hub we'll need to create the first HA Site for the redundant interfaces. Later, we'll clone this one for redundancy. Remember this HA Node will be the first device in a pair for path failover in the event of an issue or failure.

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. See "WAN Assurance Configuration Overview" on page 31.

1. In the Juniper Mist™ portal, click **Organization** > **Admin** > **Site Configuration**..

Figure 198: Site Configuration



A list of existing sites, if any, appears.

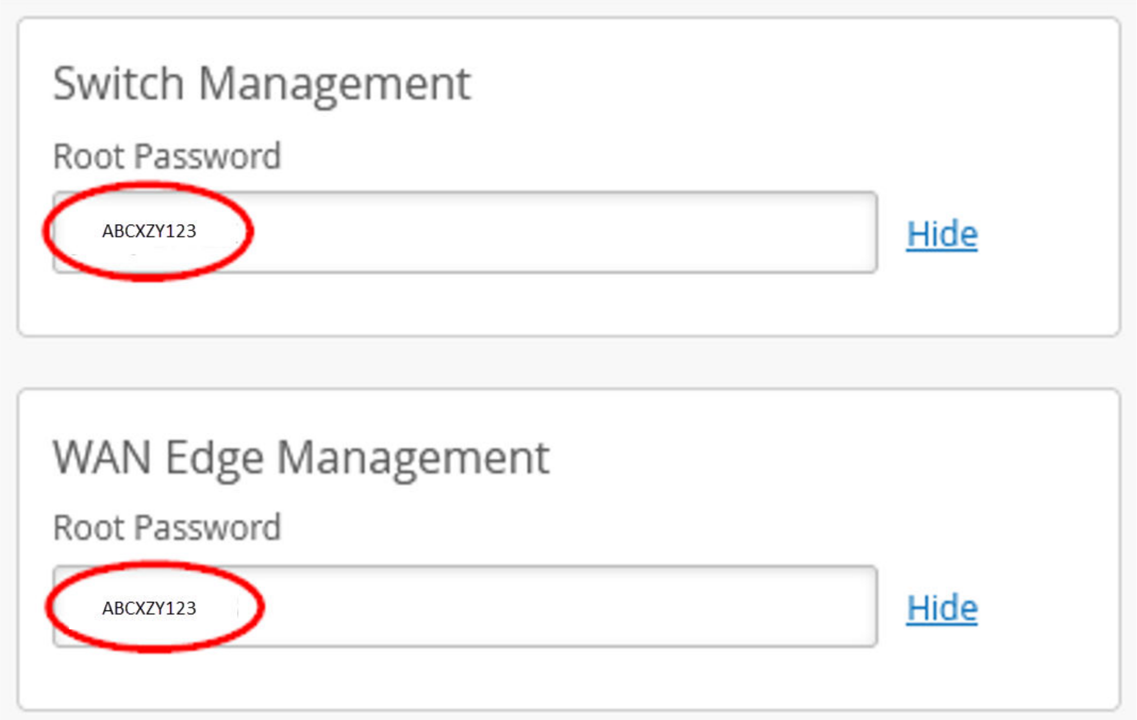
2. Click **Create Site** in the upper right corner. The New Site window appears.

    a. Give the site a name. In this example, name the site as **hahub-site**.

    b. Add a location for your site

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

Figure 199: Configure Root Password



Switch Management

Root Password

ABCXZY123

WAN Edge Management

Root Password

ABCXZY123

When you activate a device to be managed by Mist Cloud, it will set a random root password for security if you don’t define it.

3. Define a LAN interface with the following variables. When you define a LAN interface, the variables on the hahub-site merge with the existing hub1-site and hub2-site.

   Remember, the whole purpose of Site Variables is to provide simplicity and flexibility for deployment at a large scale. 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.

   Use Table 45 on page 329 to complete the list of variables you need to add.

Table 45: Variable Settings for Sites

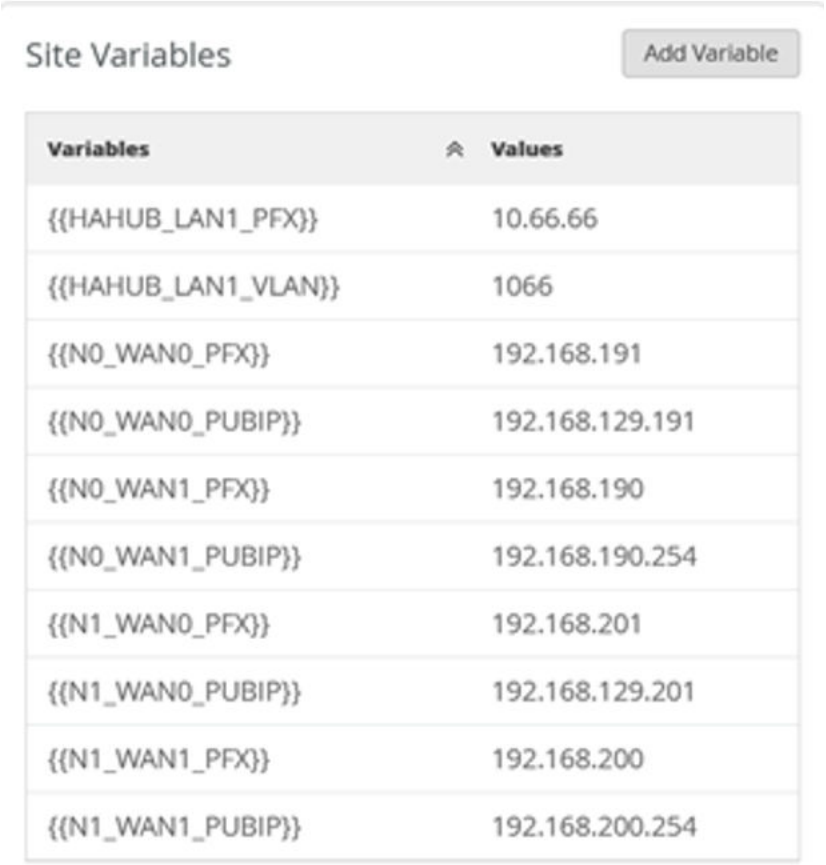
Site Name	Variable	Value
hahub-site	{{HAHUB_LAN1_PFX}}	10.66.66
hahub-site	{{HAHUB_LAN1_VLAN}}	1066
hahub-site	{{N0_WAN0_PFX}}	192.168.191

Table 45: Variable Settings for Sites *(Continued)*

Site Name	Variable	Value
hahub-site	{{N0_WAN1_PFX}}	192.168.190
hahub-site	{{N0_WAN0_PUBIP}}	192.168.129.191
hahub-site	{{N0_WAN1_PUBIP}}	192.168.190.254
hahub-site	{{N1_WAN0_PFX}}	192.168.201
hahub-site	{{N1_WAN1_PFX}}	192.168.200
hahub-site	{{N1_WAN0_PUBIP}}	192.168.129.201
<hahub-site	{{N1_WAN1_PUBIP}}	192.168.200.254

Figure 200 on page 331shows the list of newly created variables.

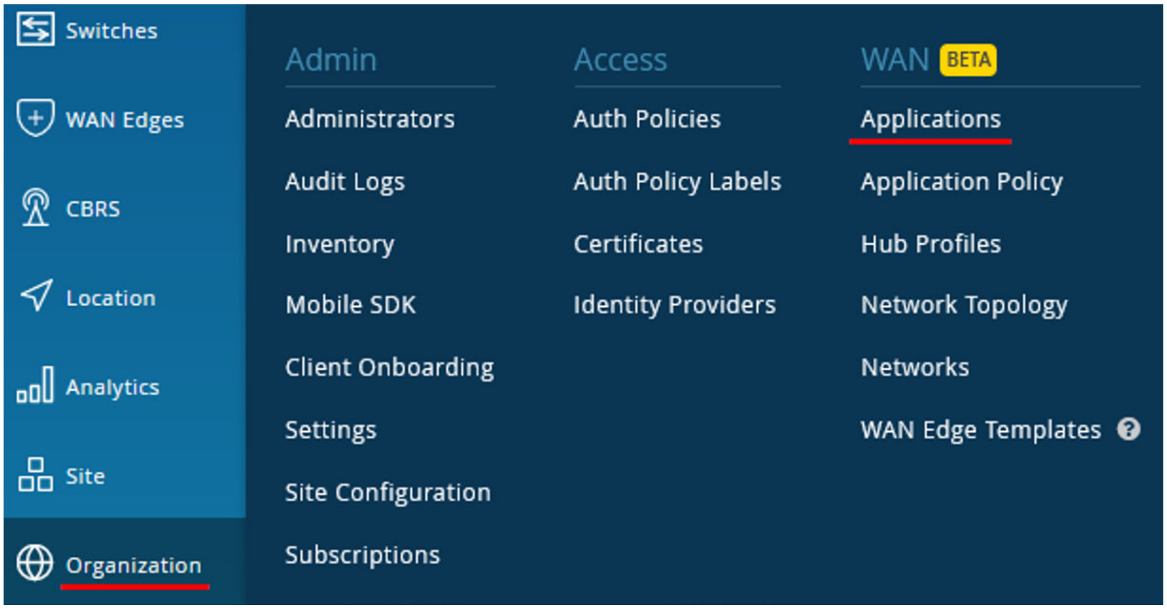
Figure 200: Site Variables



Variables	Values
{{HAHUB_LAN1_PFX}}	10.66.66
{{HAHUB_LAN1_VLAN}}	1066
{{N0_WAN0_PFX}}	192.168.191
{{N0_WAN0_PUBIP}}	192.168.129.191
{{N0_WAN1_PFX}}	192.168.190
{{N0_WAN1_PUBIP}}	192.168.190.254
{{N1_WAN0_PFX}}	192.168.201
{{N1_WAN0_PUBIP}}	192.168.129.201
{{N1_WAN1_PFX}}	192.168.200
{{N1_WAN1_PUBIP}}	192.168.200.254

4. Click **Save** to save your changes for the site.
5. In the Juniper Mist portal, click **Organization** > **WAN**> **Applications**.

Figure 201: Add Applications



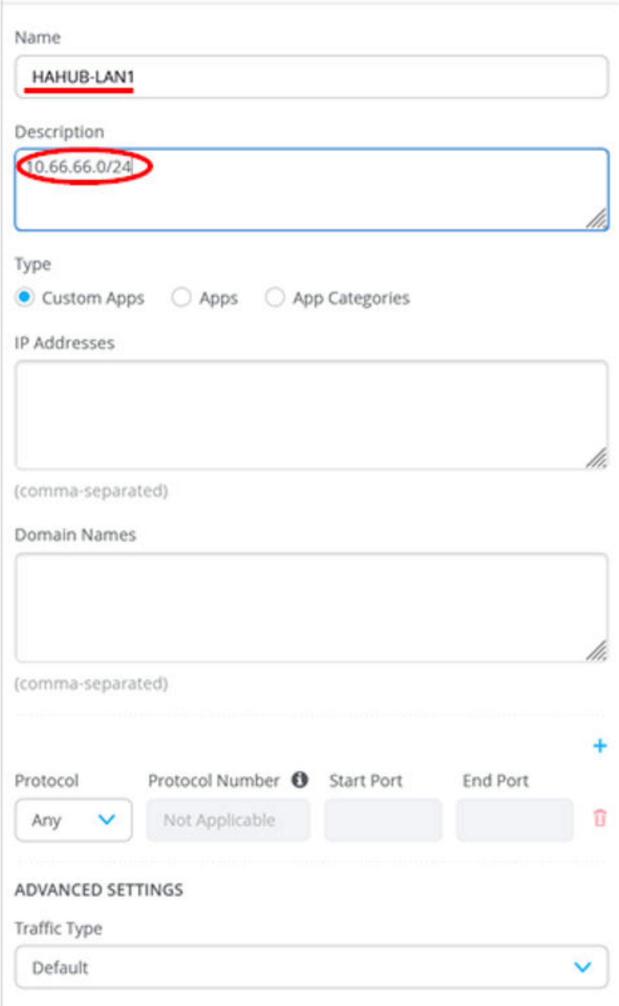
A list of existing applications, if any, appears.

6. Configure a match for all IP addresses attached at the LAN interface of the HA hub site.

   Configure the following items:

   - **Name**—HAHUB-LAN1
   - **IP addresses**—Configure the single IP prefix **10.66.66.0/24** for now.

Figure 202: Configure Applications



Name

HAHUB-LAN1

Description

10.66.66.0/24

Type

● Custom Apps ○ Apps ○ App Categories

IP Addresses

(comma-separated)

Domain Names

(comma-separated)

Protocol	Protocol Number	Start Port	End Port
Any	Not Applicable		

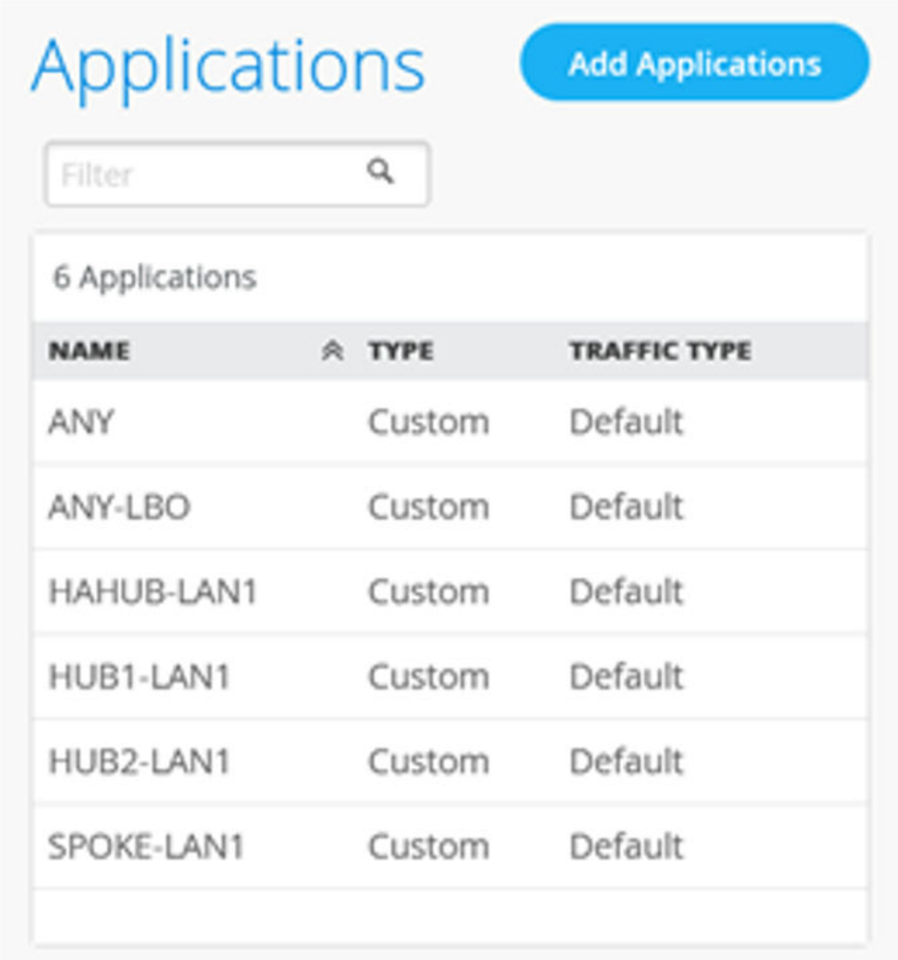
ADVANCED SETTINGS

Traffic Type

Default

Figure 203 on page 334 shows the application you created under applications list.

Figure 203: Applications List

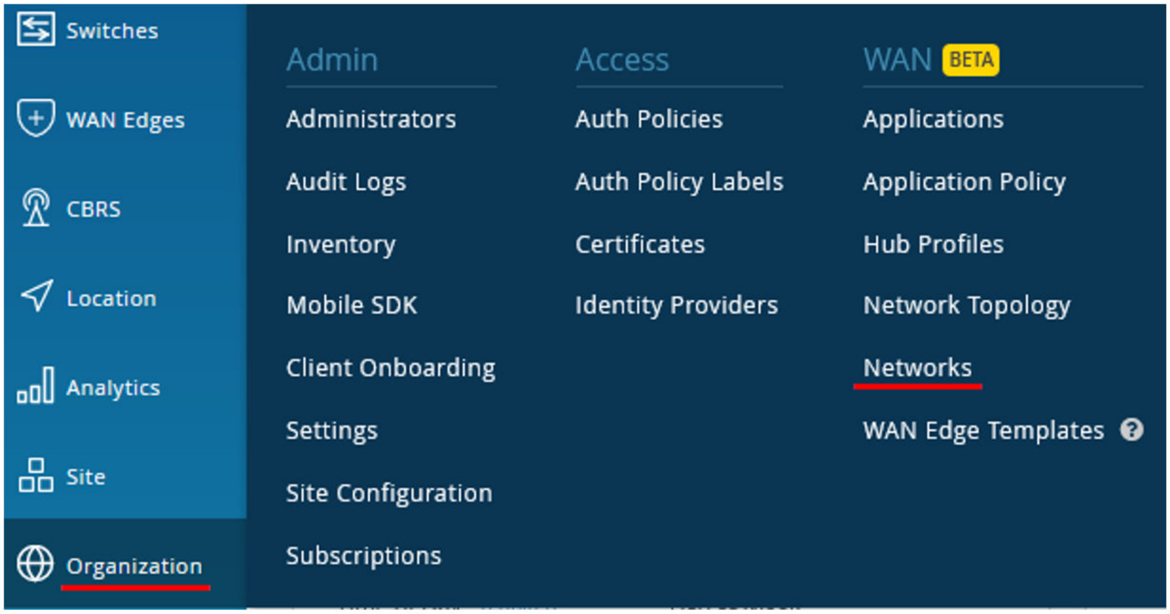


6 Applications

NAME	TYPE	TRAFFIC TYPE
ANY	Custom	Default
ANY-LBO	Custom	Default
HAHUB-LAN1	Custom	Default
HUB1-LAN1	Custom	Default
HUB2-LAN1	Custom	Default
SPOKE-LAN1	Custom	Default

7. In the Juniper Mist cloud portal, click **Organization** > **WAN** > **Networks**.

Figure 204: Configure Traffic Source



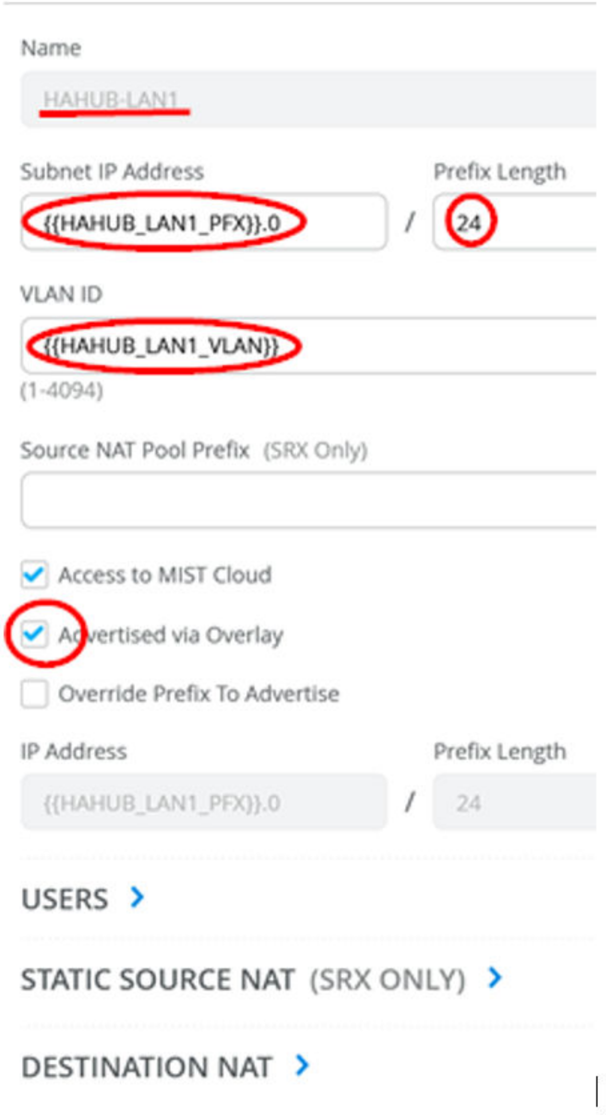
A list of existing networks, if any, appears.

8. Click Add Networks in the upper right corner.

   The Add Network window appears

9. Configure the options for the traffic source.

Figure 205: Configure Network (Traffic Source)



Name

HAHUB-LAN1

Subnet IP Address {{HAHUB_LAN1_PFX}}.0 / Prefix Length 24

VLAN ID {{HAHUB_LAN1_VLAN}}

(1-4094)

Source NAT Pool Prefix (SRX Only)

☑ Access to MIST Cloud

☑ Advertised via Overlay

☐ Override Prefix To Advertise

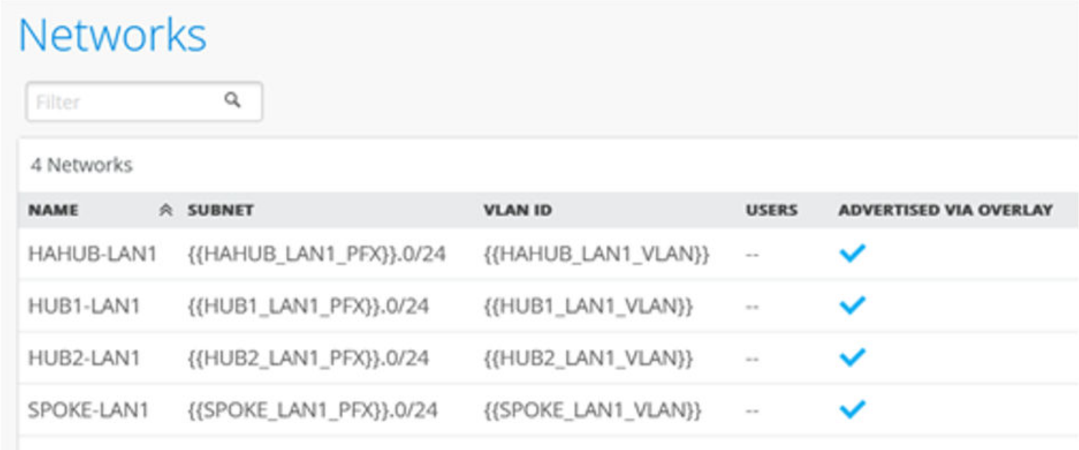
IP Address {{HAHUB_LAN1_PFX}}.0 / Prefix Length 24

- **Name:** HAHUB-LAN1
- **Subnet IP Address:** {{HAHUB_LAN1_PFX}}.0. This value substitutes via site variables that contain the first three octets.)
- **Prefix Length**: 24 (Hardcoded)
- **VLAN ID**: {{HAHUB_LAN1_VLAN}} (For automatic tagging via site variable.)
- Check **Access to Mist Cloud.** For possible future device management by the Mist Cloud with the correct policies.

- Check **Advertised via Overlay**. This option creates the endpoints for spoke communication across the WAN.

Figure 206 on page 337 shows the network you created under Networks list.

Figure 206: Networks List



Networks

Filter

4 Networks

NAME	SUBNET	VLAN ID	USERS	ADVERTISED VIA OVERLAY
HAHUB-LAN1	{{HAHUB_LAN1_PFX}}.0/24	{{HAHUB_LAN1_VLAN}}	--	✓
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}}	--	✓

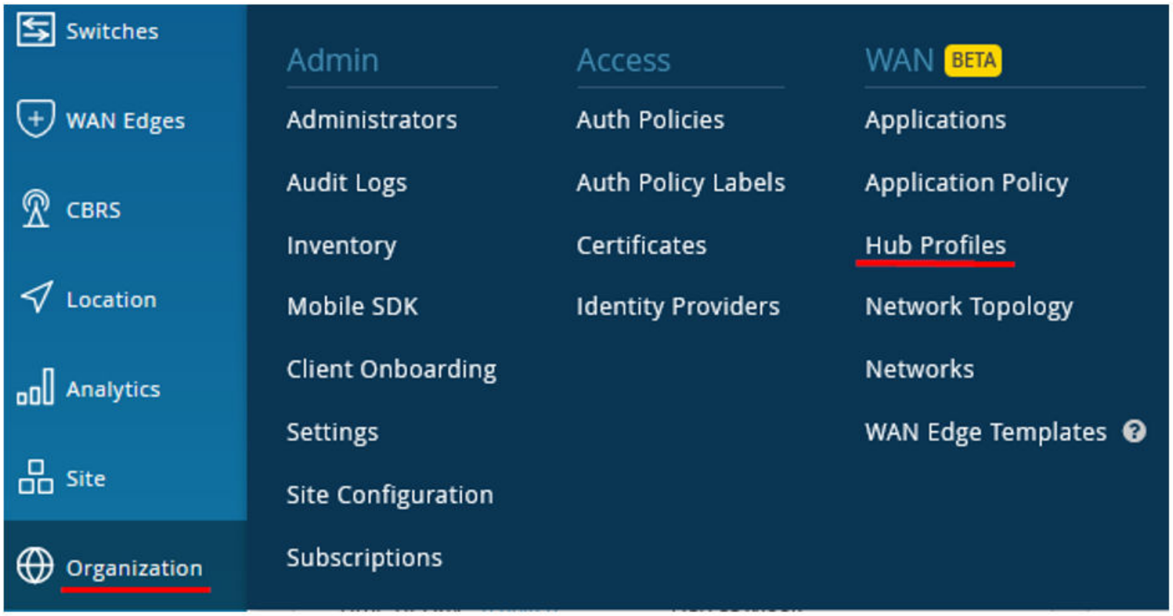
NOTE: Note: Networks are the sources of your traffic, the “who” in the Mist paradigm. Here we’re telling our Hub where the traffic requests will come from. This is the second part of the intent driven Mist expression bringing the “who” to the “what”.

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.

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

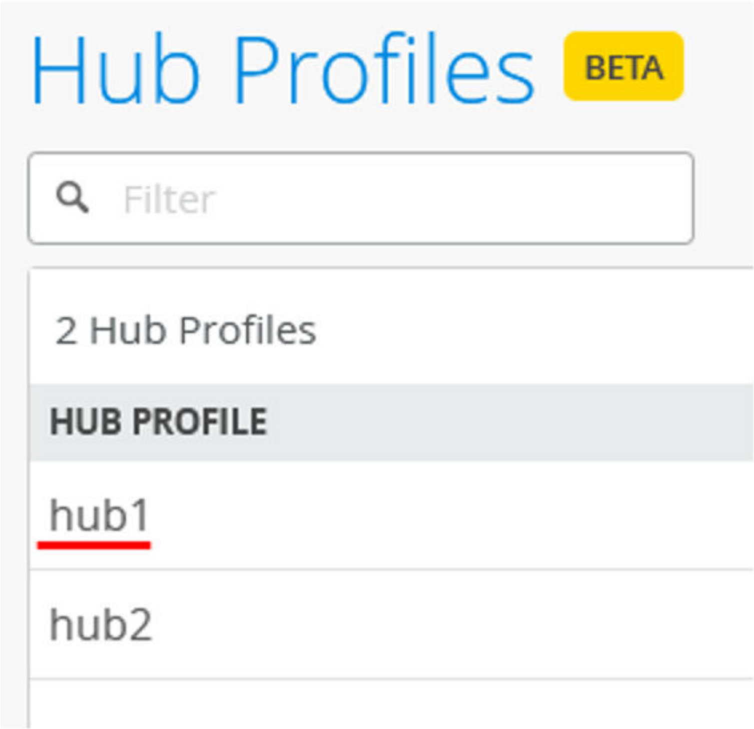
Figure 207: Configure Hub Profiles



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

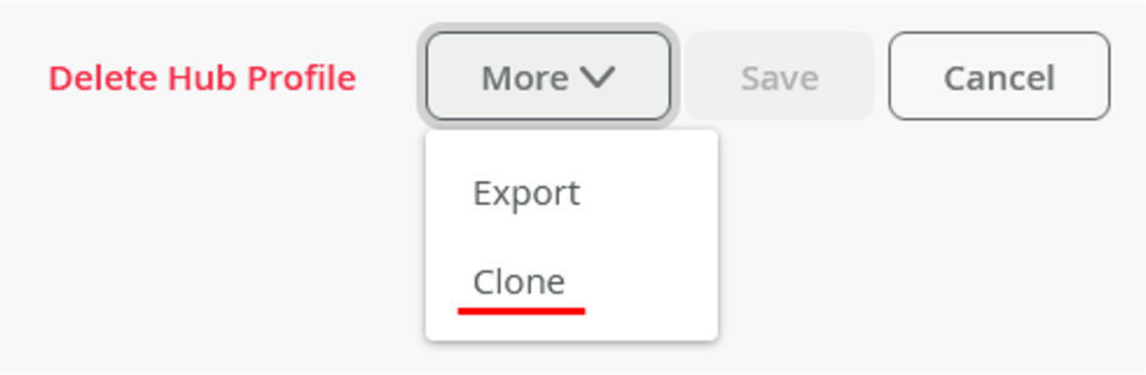
2. Click the hub profile (hub1) that you want to clone.

Figure 208: Select Hub Profile for Cloning



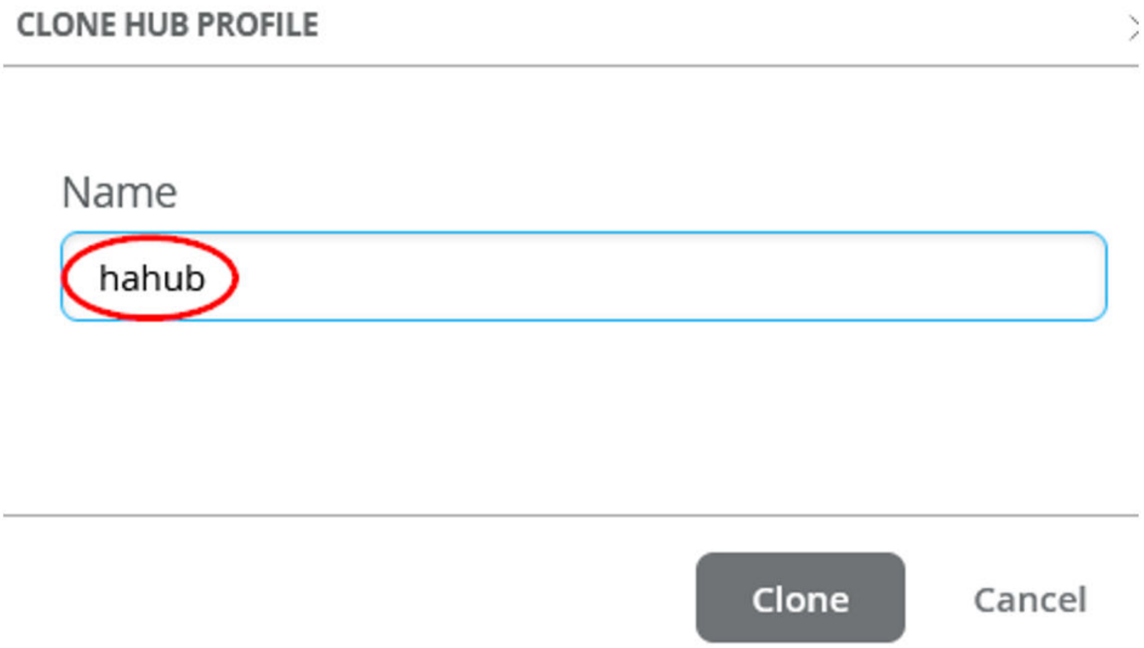
3. In the upper right corner of the screen, click **More** and select **Clone**.

Figure 209: Selecting Clone Option



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

Figure 210: Rename Cloned Hub Profile



Name

hahub

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

5. 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 Table 46 on page 340.

Table 46: WAN Interfaces Details in Hub Profile

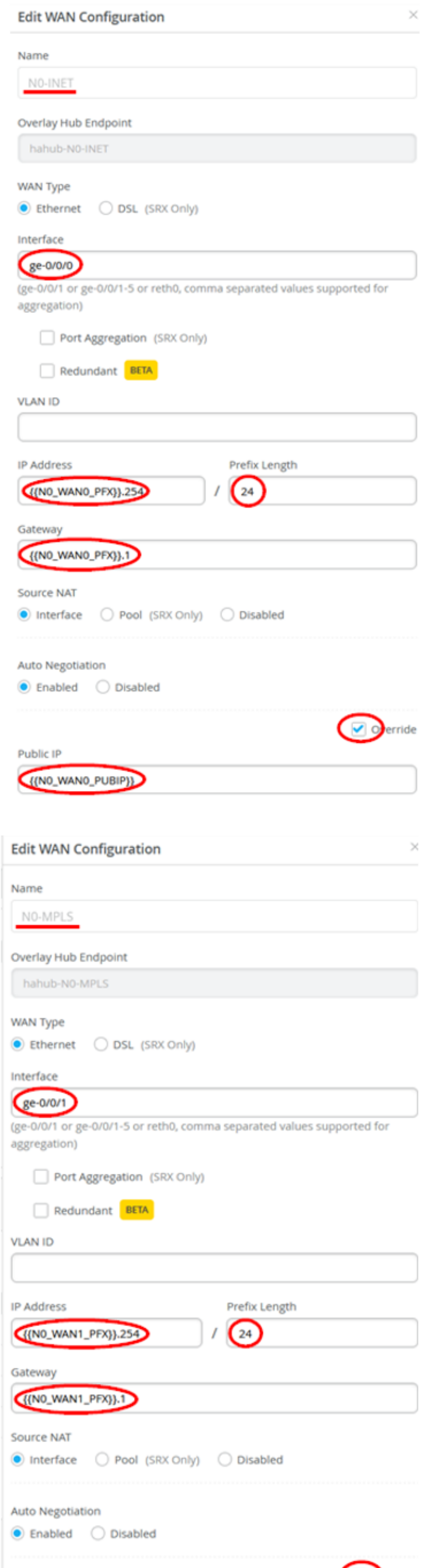
Option	First WAN	Second WAN	Third WAN	Fourth WAN
Name: (This indicates which topology it uses.)	N0-INET (Overlay endpoint: **hahub-N0-INET** (automatically generated))	N0-MPLS (Overlay endpoint: **hahub-N0-MPLS** (automatically generated)	N1-INET (Overlay endpoint: **hahub-N1-INET** (automatically generated)	N1-MPLS (Overlay endpoint: **hahub-N1-MPLS** (automatically generated)
Interface	ge-0/0/0	ge-0/0/1	ge-1/0/0	ge-1/0/1

Table 46: WAN Interfaces Details in Hub Profile *(Continued)*

Option	First WAN	Second WAN	Third WAN	Fourth WAN
IP Address:	{{N0_WAN0_PFX}}.254	{{N0_WAN1_PFX}}.254	{{N1_WAN0_PFX}}.254	{{N1_WAN1_PFX}}.254
Prefix Length:	24	24	24	24
Gateway:	{{N0_WAN0_PFX}}.1	{{N0_WAN1_PFX}}.1	{{N1_WAN0_PFX}}.1	{{N1_WAN1_PFX}}.1
Source NAT:	Enabled	Enabled	Enabled	Enabled
Check Override for Public IP	Yes	Yes	Yes	Yes
Public IP:	{{N0_WAN0_PUBIP}}	{{N0_WAN1_PUBIP}}	{{N1_WAN0_PUBIP}}	{{N1_WAN1_PUBIP}}

Figure 211 on page 342 shows WAN interface configuration.

Figure 211: WAN Interface Configuration (First)



Edit WAN Configuration

Name: N0-INET

Overlay Hub Endpoint: hahub-N0-INET

WAN Type: ● Ethernet ○ DSL (SRX Only)

Interface: ge-0/0/0

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

□ Port Aggregation (SRX Only)

□ Redundant BETA

VLAN ID:

IP Address: {{N0_WAN0_PFX}}.254 / Prefix Length: 24

Gateway: {{N0_WAN0_PFX}}.1

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

Auto Negotiation: ● Enabled ○ Disabled

☑ Override

Public IP: {{N0_WAN0_PUBIP}}

Edit WAN Configuration

Name: N0-MPLS

Overlay Hub Endpoint: hahub-N0-MPLS

WAN Type: ● Ethernet ○ DSL (SRX Only)

Interface: ge-0/0/1

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

□ Port Aggregation (SRX Only)

□ Redundant BETA

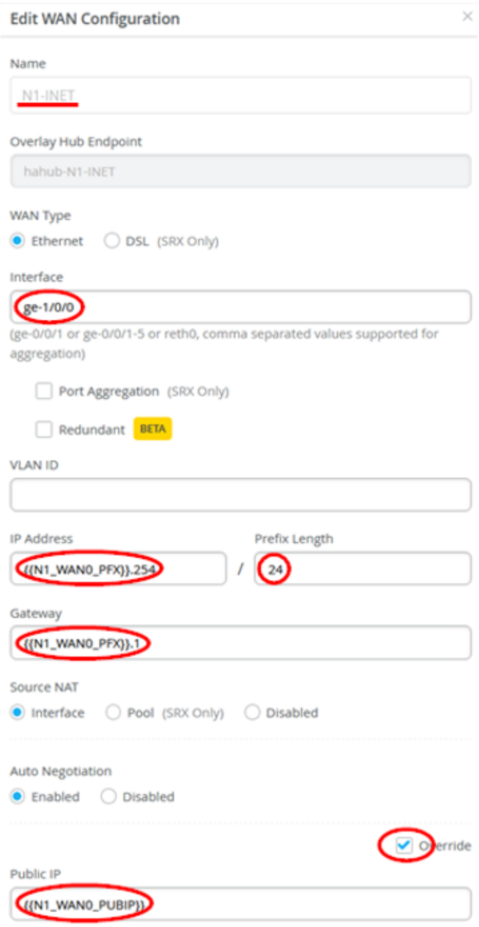
VLAN ID:

IP Address: {{N0_WAN1_PFX}}.254 / Prefix Length: 24

Gateway: {{N0_WAN1_PFX}}.1

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

Auto Negotiation: ● Enabled ○ Disabled



Edit WAN Configuration

Name

N1-INET

Overlay Hub Endpoint

hahub-N1-INET

WAN Type

● Ethernet ○ DSL (SRX Only)

Interface

ge-1/0/0

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

□ Port Aggregation (SRX Only)

□ Redundant BETA

VLAN ID

IP Address

{{N1_WAN0_PFX}}.254 / Prefix Length 24

Gateway

{{N1_WAN0_PFX}}.1

Source NAT

● Interface ○ Pool (SRX Only) ○ Disabled

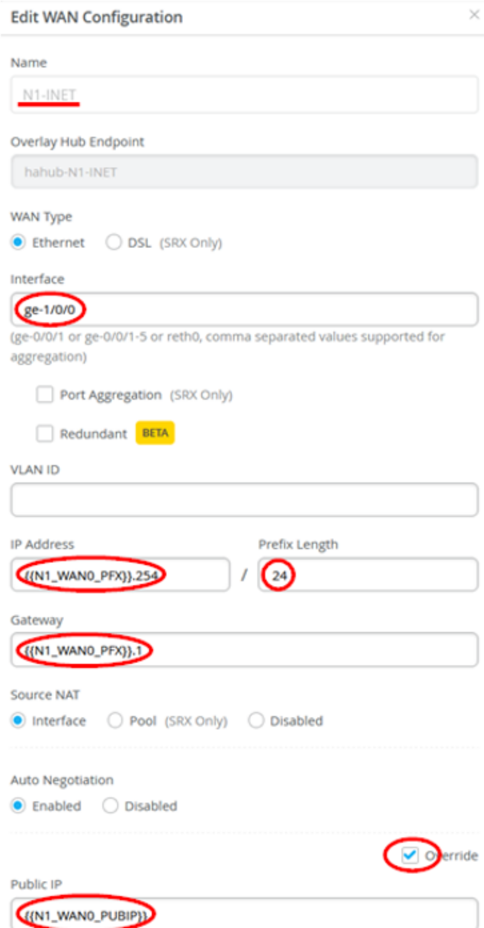
Auto Negotiation

● Enabled ○ Disabled

☑ Override

Public IP

{{N1_WAN0_PUBIP}}



Edit WAN Configuration

Name

N1-INET

Overlay Hub Endpoint

hahub-N1-INET

WAN Type

● Ethernet ○ DSL (SRX Only)

Interface

ge-1/0/0

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

□ Port Aggregation (SRX Only)

□ Redundant BETA

VLAN ID

IP Address

{{N1_WAN0_PFX}}.254 / Prefix Length 24

Gateway

{{N1_WAN0_PFX}}.1

Source NAT

● Interface ○ Pool (SRX Only) ○ Disabled

Auto Negotiation

● Enabled ○ Disabled

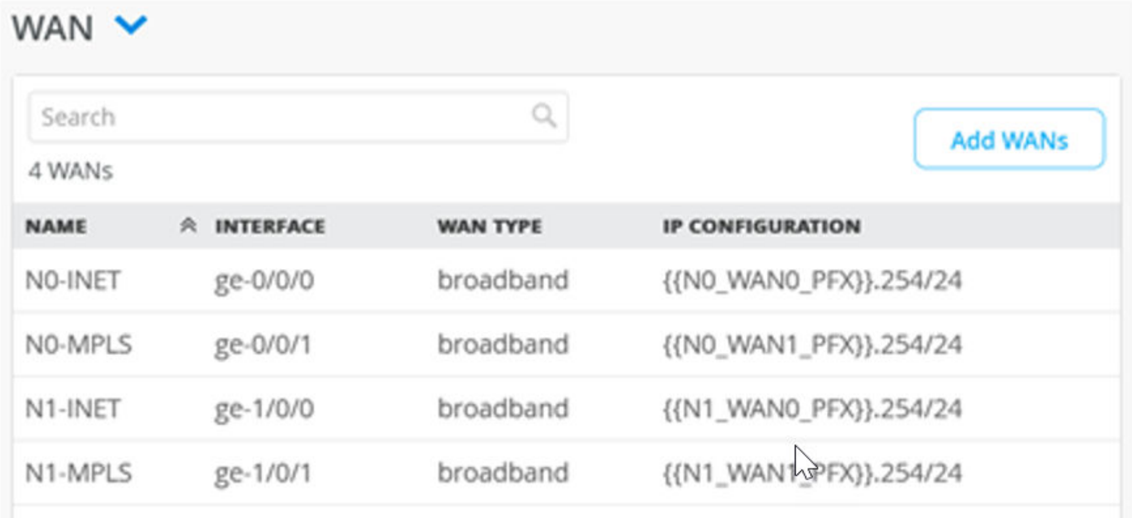
☑ Override

Public IP

{{N1_WAN0_PUBIP}}

The WAN interfaces for each node should look as shown in Figure 212 on page 344.

Figure 212: List of WAN Interfaces Configured in Hub Profile



WAN

4 WANs

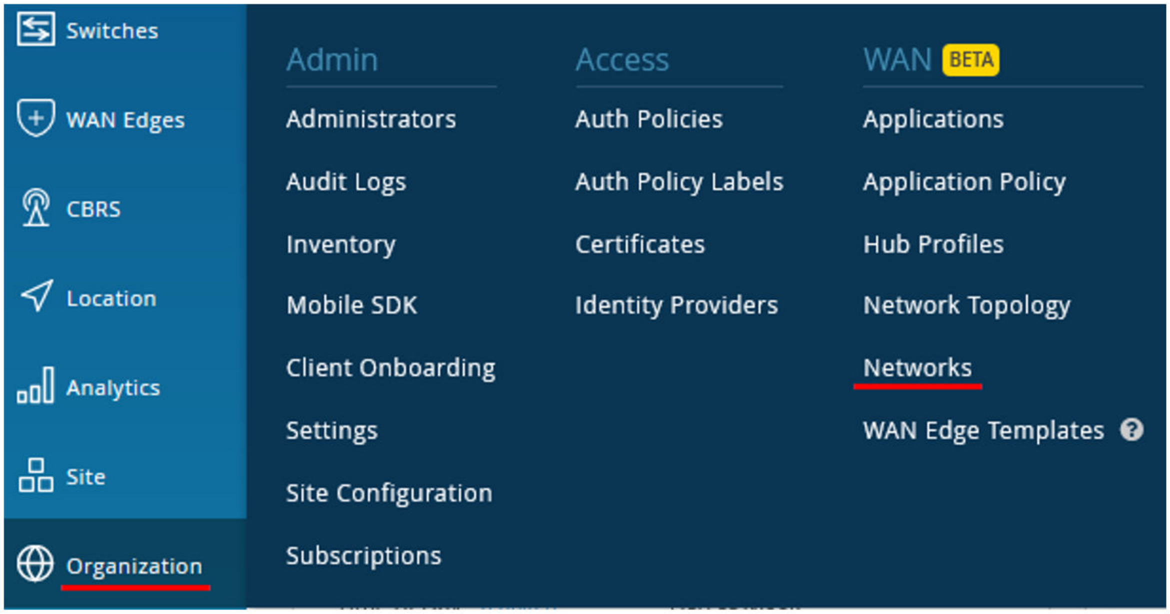
NAME	INTERFACE	WAN TYPE	IP CONFIGURATION
N0-INET	ge-0/0/0	broadband	{{N0_WAN0_PFX}}.254/24
N0-MPLS	ge-0/0/1	broadband	{{N0_WAN1_PFX}}.254/24
N1-INET	ge-1/0/0	broadband	{{N1_WAN0_PFX}}.254/24
N1-MPLS	ge-1/0/1	broadband	{{N1_WAN1_PFX}}.254/24

Define the VRRP Interfaces

Next, you'll define a **Network** for the redundant LAN interfaces for VRRP and cluster support.

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

Figure 213: Configure Traffic Source

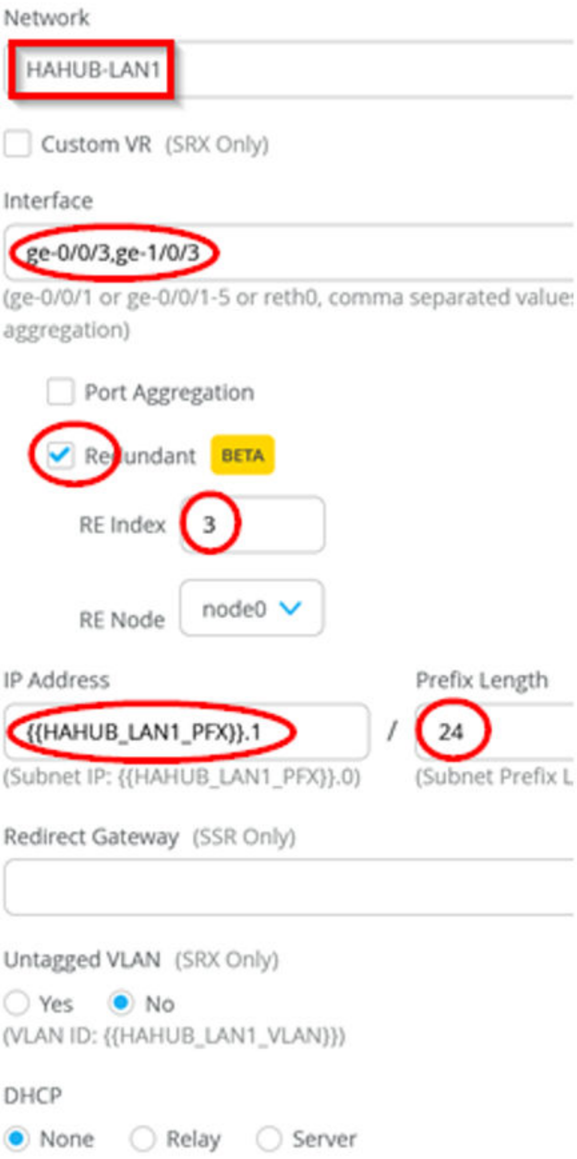


A list of existing networks, if any, appears.

2. Complete the configuration for the LAN interface with the following details:

   - **Network**: HAHUB-LAN1
   - **Interfaces**: ge-0/0/3,ge-1/0/3
   - **Redundant**: Enabled
   - **RE Index**: 3 (As a convention, we usually use the last octet as an index).
   - **IP Address**: {{HAHUB_LAN1_PFX}}.1
   - **Prefix**: 24 (Remains same)

Figure 214: Redundant LAN Interface Configuration



Network

HAHUB-LAN1

□ Custom VR (SRX Only)

Interface

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

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

□ Port Aggregation

☑ Redundant BETA

RE Index 3

RE Node node0

IP Address {{HAHUB_LAN1_PFX}}.1 / Prefix Length 24

(Subnet IP: {{HAHUB_LAN1_PFX}}.0) (Subnet Prefix L

Redirect Gateway (SSR Only)

Untagged VLAN (SRX Only)

○ Yes ● No

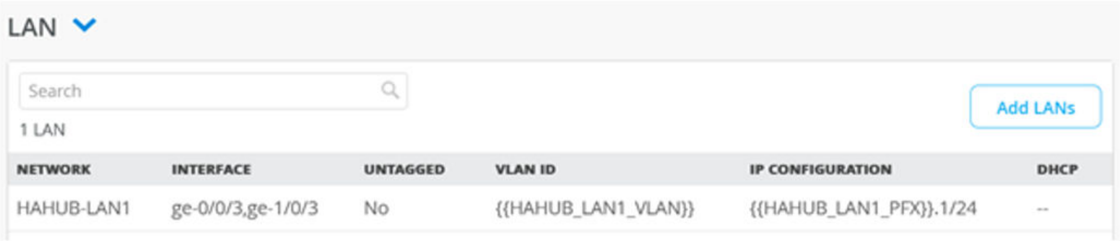
(VLAN ID: {{HAHUB_LAN1_VLAN}})

DHCP

● None ○ Relay ○ Server

Figure 215 on page 347 shows details of LAN interfaces configured for hub profile.

Figure 215: LAN Interface Configured for Hub Profile



1 LAN

NETWORK	INTERFACE	UNTAGGED	VLAN ID	IP CONFIGURATION	DHCP
HAHUB-LAN1	ge-0/0/3,ge-1/0/3	No	{{HAHUB_LAN1_VLAN}}	{{HAHUB_LAN1_PFX}}.1/24	--

Configure Traffic Steering Profile

Traffic steering rules direct the flow of data traffic from one location or device to another. These rules help control how data packets are routed within a network, ensuring efficient and optimized data delivery. **Traffic steering** rules can be set up for various purposes, such as load balancing, traffic optimization, security, and quality of service (QoS) management. This is the Mist expression of “how” we send our “who” **Networks** to our “what” **Applications**.

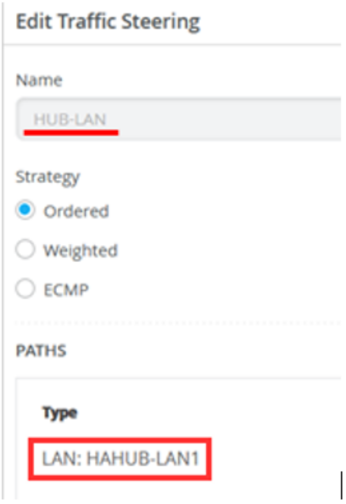
For example, in a load balancing scenario, **Traffic Steering** rules might determine how incoming data traffic is distributed across multiple servers to prevent overload on any single server and ensure even distribution of the workload. In a security context, **Traffic Steering** rules could be used to direct certain types of traffic through specific security checkpoints or firewalls for inspection before allowing them into the network.

For your **Traffic Steering** network, keep in mind Session Smart Secure Vector Routing™. Your Session Smart routers are constantly communicating with one another with synchronous and asynchronous Bidirectional Forwarding Detection for liveness and path health for path selection in real-time. **Traffic Steering** then is an order of what paths you’d like traffic to take.

Change the existing traffic steering rules for the cloned hub profile.

Scroll down to the TRAFFIC STEERING pane and edit the entry to change the rule for **HUB-LAN** to **Paths / Type: LAN: HAHUB-LAN1**

Figure 216: Edit Traffic Steering Policy



Edit Traffic Steering

Name

HUB-LAN

Strategy

● Ordered

○ Weighted

○ ECMP

PATHS

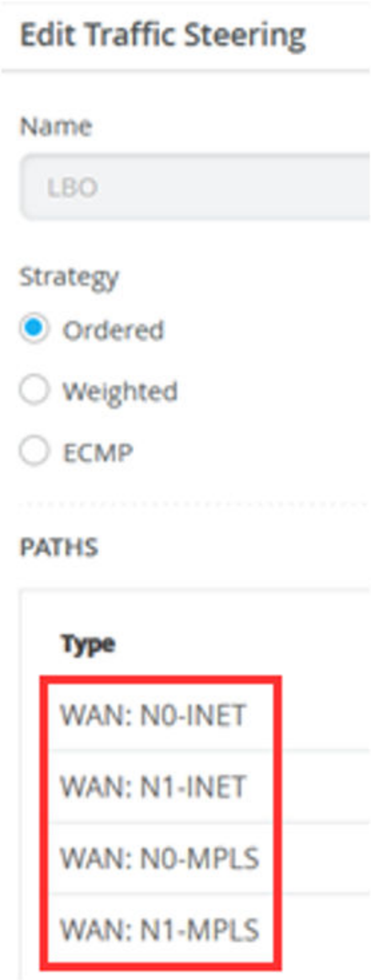
Type

LAN: HAHUB-LAN1

For LBO

- WAN: N0-INET
- WAN: N1-INET
- WAN: N0-MPLS
- WAN: N1-MPLS

Figure 217: Update Paths in a Traffic-Steering Policy (For LBO)



Edit Traffic Steering

Name

LBO

Strategy

● Ordered

○ Weighted

○ ECMP

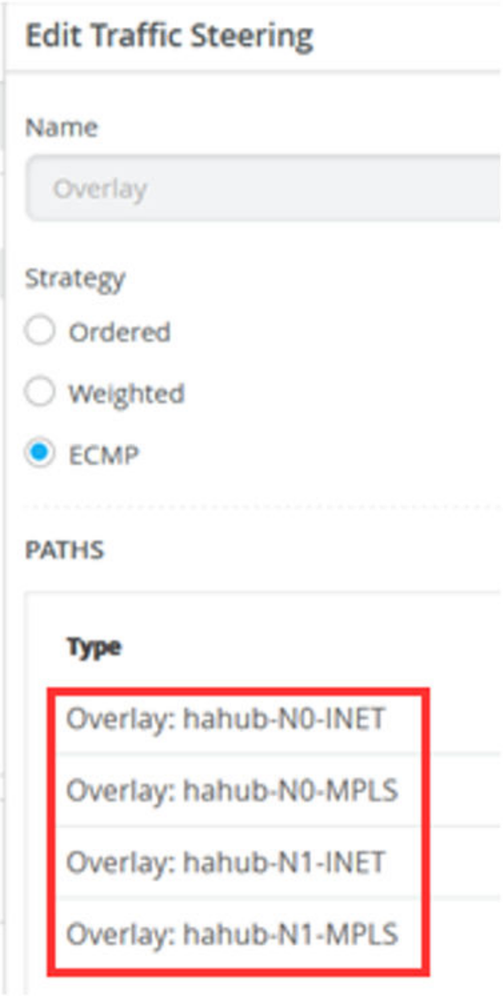
PATHS

Type
WAN: N0-INET
WAN: N1-INET
WAN: N0-MPLS
WAN: N1-MPLS

For Overlay

- Overlay: hahub-N0-INET
- Overlay: hahub-N0-MPLS
- Overlay: hahub-N1-INET
- Overlay: hahub-N1-MPLS

Figure 218: Update Paths in a Traffic-Steering Policy (For Overlay)



Edit Traffic Steering

Name

Overlay

Strategy

○ Ordered

○ Weighted

● ECMP

PATHS

Type

Overlay: hahub-N0-INET

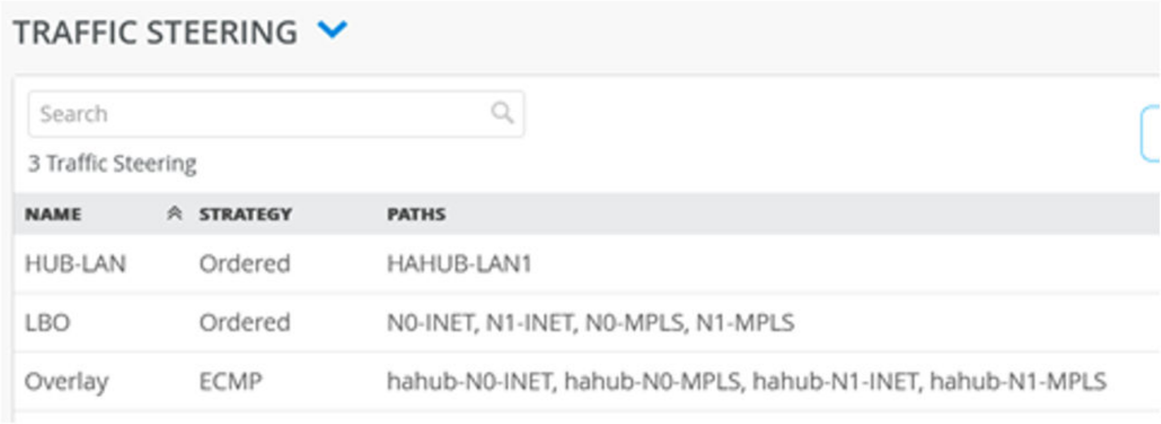
Overlay: hahub-N0-MPLS

Overlay: hahub-N1-INET

Overlay: hahub-N1-MPLS

The Traffic steering rules now combine the interfaces of the two nodes as shown in Figure 219 on page 351.

Figure 219: Updated Traffic Steering Rules



TRAFFIC STEERING

3 Traffic Steering

NAME	STRATEGY	PATHS
HUB-LAN	Ordered	HAHUB-LAN1
LBO	Ordered	N0-INET, N1-INET, N0-MPLS, N1-MPLS
Overlay	ECMP	hahub-N0-INET, hahub-N0-MPLS, hahub-N1-INET, hahub-N1-MPLS

Modify Application Policies

The **Application Policies** are like the ones for hub1 or hub2. But this time, you'll change what was **HUB1-LAN1** to **HAHUB-LAN1**. The changes are noted in **bold font.**

Update Application Rules according to the details provided in Table 47 on page 351.

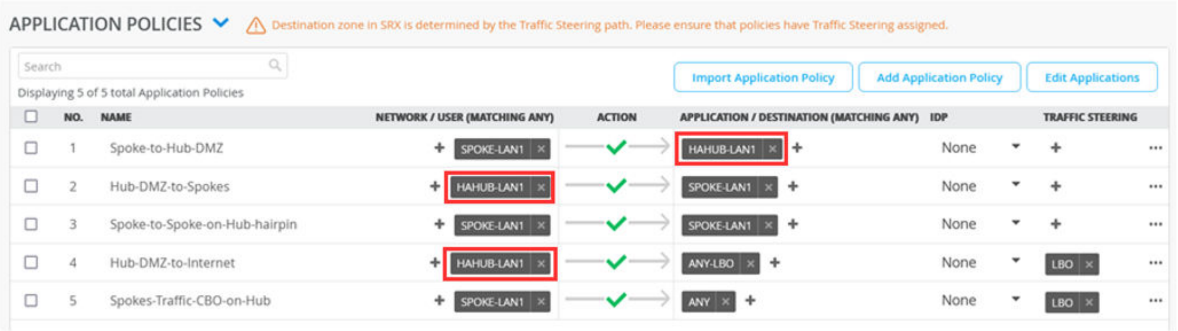
For example, wherever applicable, change HUB1-LAN to HAHUB-LAN1.

Table 47: Application Rules Configuration

No.	Rule Name	Network	Action	Destination	Steering
1	Spoke-to-Hub-DMZ	SPOKE-LAN1	Pass	**HAHUB-LAN1**	N/A
2	Hub-DMZ-to-Spokes	**HAHUB-LAN1**	Pass	SPOKE-LAN1	N/A
3	Spoke-to-Spoke-on-Hub-hairpin	SPOKE-LAN1	Pass	SPOKE-LAN1	N/A
4	Hub-DMZ-to-Internet	**HAHUB-LAN1**	Pass	ANY-LBO	LBO
5	Spokes-Traffic-CBO-on-Hub	SPOKE-LAN1	Pass	ANY	LBO

Figure 220 on page 352 shows the details of the updated application policies after you save your changes.

Figure 220: Updated Application Policy Summary



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

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	SPOKE-LAN1	✓	HAHUB-LAN1	None	
□	2	Hub-DMZ-to-Spokes	HAHUB-LAN1	✓	SPOKE-LAN1	None	
□	3	Spoke-to-Spoke-on-Hub-hairpin	SPOKE-LAN1	✓	SPOKE-LAN1	None	
□	4	Hub-DMZ-to-Internet	HAHUB-LAN1	✓	ANY-LBO	None	LBO
□	5	Spokes-Traffic-CBO-on-Hub	SPOKE-LAN1	✓	ANY	None	LBO

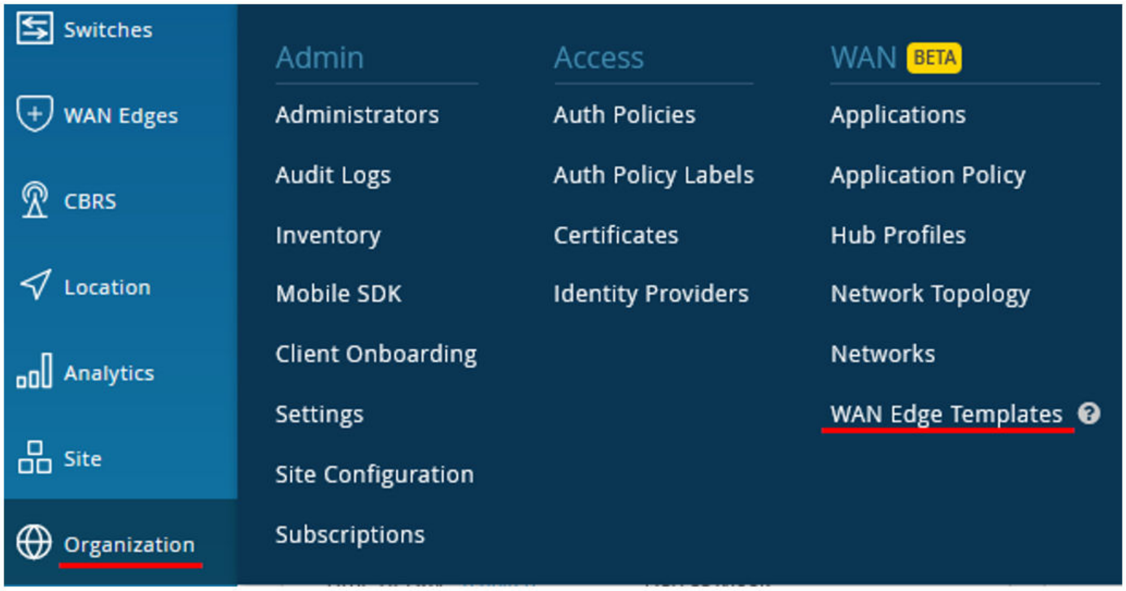
Create Spoke Templates

With our HA Hubs in place, it's time to create matching Spoke Templates, one spoke in standalone and the other in HA-Cluster for HA. To add a highly available spokes we'll need to create templates for the redundant interfaces. Later, we'll clone this for redundancy. Remember this HA Node will be the first WAN edge device in a pair for path failover in the event of an issue or failure.

1. 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.

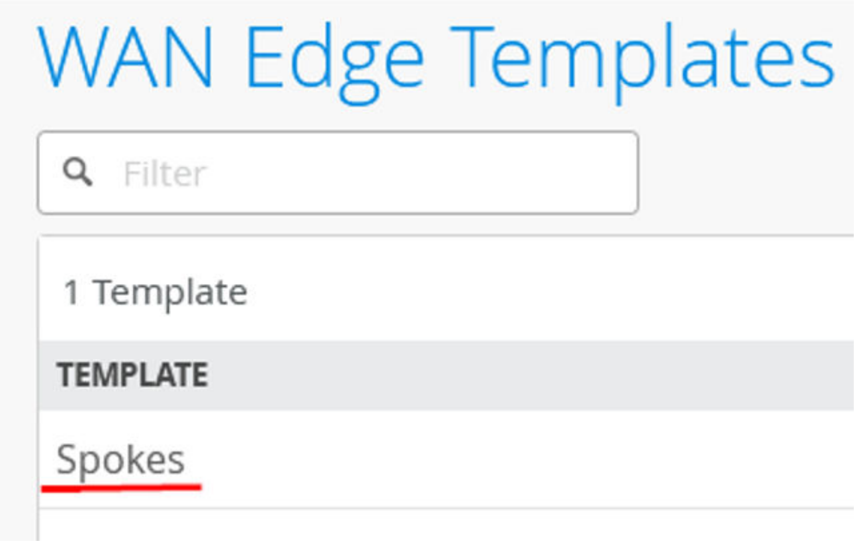
   In the Juniper Mist™ portal, click Organization > WAN > WAN Edge Templates. A list of existing templates, if any, appears.

Figure 221: Accessing WAN Edge Templates



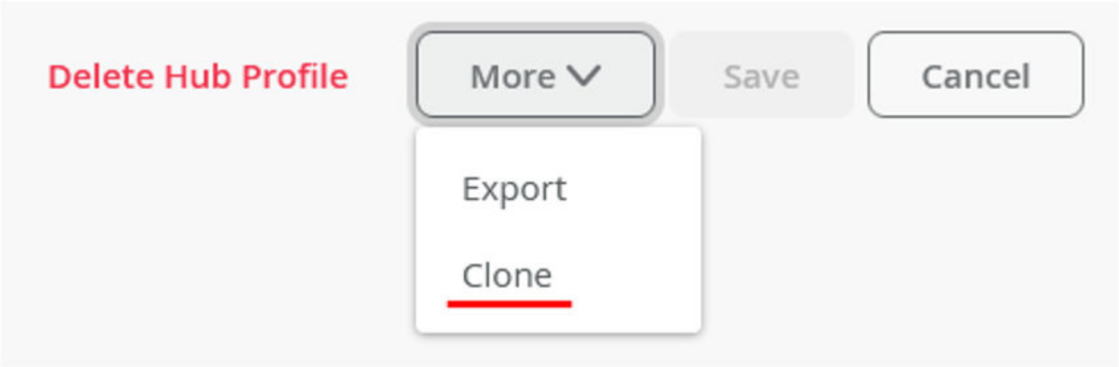
2. Create the new Spoke Template by cloning the existing template and modifying the clone. Simply select the existing profile Spokes and select **Clone**.

Figure 222: WAN Edge Templates



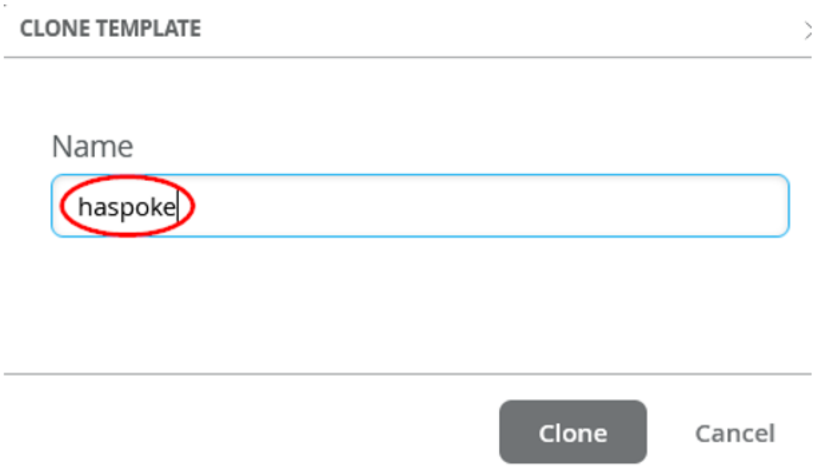
3. In the upper right corner of the screen, click More and select Clone.

Figure 223: Cloning Existing WAN Edge Template



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

Figure 224: Renaming Cloned Template


CLONE TEMPLATE

Name

haspoke

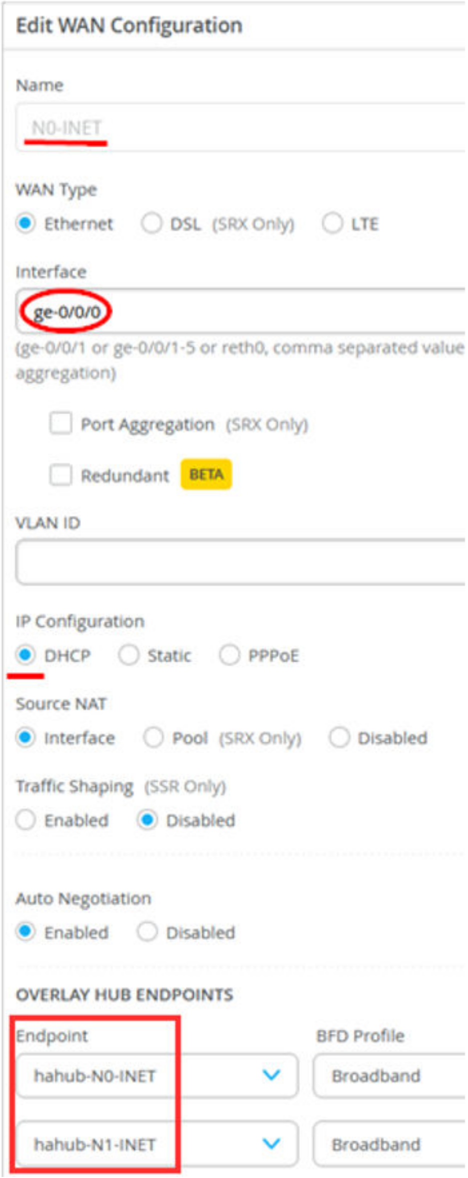
Best practice: Refresh your browser after cloning. This ensures that objects are refreshed.

5. Change your clone Template. Remove all older WAN interfaces and configure four WAN interfaces according to the details in Table 48 on page 355.

Table 48: WAN Interfaces Details for Spoke Template

Option	First WAN Interface	Second WAN Interface	Third WAN Interface	Fourth WAN Interface
Name (indicates which topology it uses)	N0-INET	N0-MPLS	N1-INET	N1-MPLS
WAN Type	Ethernet	Ethernet	Ethernet	Ethernet
Interface	ge-0/0/0	ge-0/0/1	ge-1/0/0	ge-1/0/1
IP Configuration:	DHCP	Static • IP Address: {{WAN1_PFX}}.2 • Gateway: {{WAN1_PFX}}.1 • Prefix: 24	DHCP	Static • IP Address: {{WAN1_PFX}}.3 • Gateway: {{WAN1_PFX}}.1 • Prefix: 24
Overlay Hub Endpoints	• Endpoint1: hahub-N0-INET • Endpoint2: hahub-N1-INET	• Endpoint1: hahub-N0-MPLS • Endpoint2: hahub-N1-MPLS	• Endpoint1:hahub-N0-INET • Endpoint2: hahub-N1-INET	• Endpoint1: hahub-N0-MPLS • Endpoint2: hahub-N1-MPLS

Figure 225: WAN Interface Configuration for Spoke Template



Edit WAN Configuration

Name

N0-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 value
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

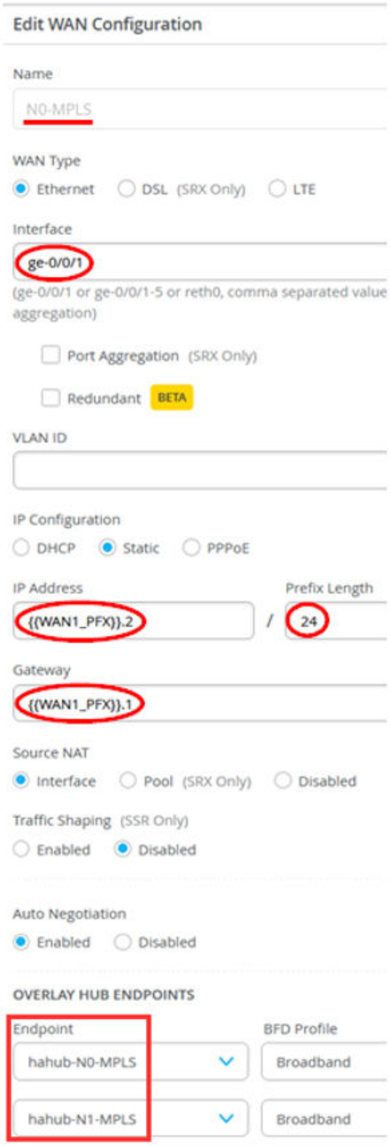
Auto Negotiation

● Enabled ○ Disabled

OVERLAY HUB ENDPOINTS

Endpoint	BFD Profile
hahub-N0-INET	Broadband
hahub-N1-INET	Broadband

Figure 226: WAN Interface (Second) Configuration for Spoke Template



Edit WAN Configuration

Name

N0-MPLS

WAN Type

● Ethernet ○ DSL (SRX Only) ○ LTE

Interface

ge-0/0/1

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

□ Port Aggregation (SRX Only)

□ Redundant BETA

VLAN ID

IP Configuration

○ DHCP ● Static ○ PPPoE

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

Gateway

{{WAN1_PFX}}.1

Source NAT

● Interface ○ Pool (SRX Only) ○ Disabled

Traffic Shaping (SSR Only)

○ Enabled ● Disabled

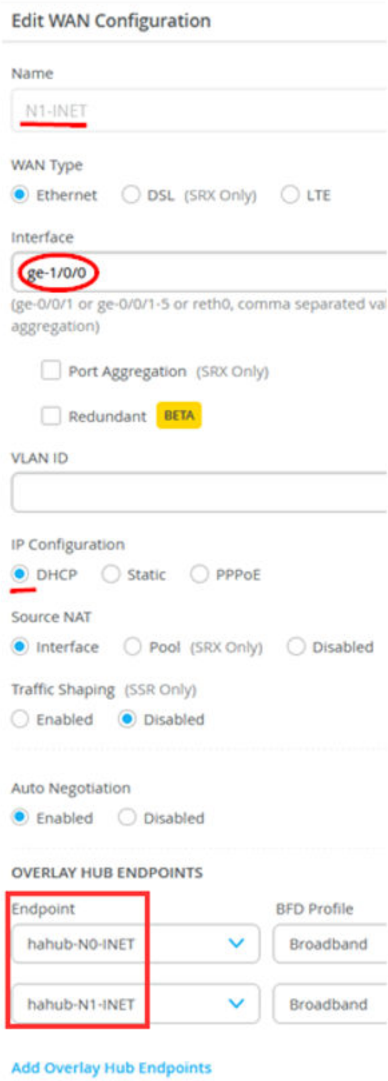
Auto Negotiation

● Enabled ○ Disabled

OVERLAY HUB ENDPOINTS

Endpoint	BFD Profile
hahub-N0-MPLS	Broadband
hahub-N1-MPLS	Broadband

Figure 227: WAN Interface (Third) Configuration for Spoke Template



Edit WAN Configuration

Name

N1-INET

WAN Type

● Ethernet ○ DSL (SRX Only) ○ LTE

Interface

ge-1/0/0

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

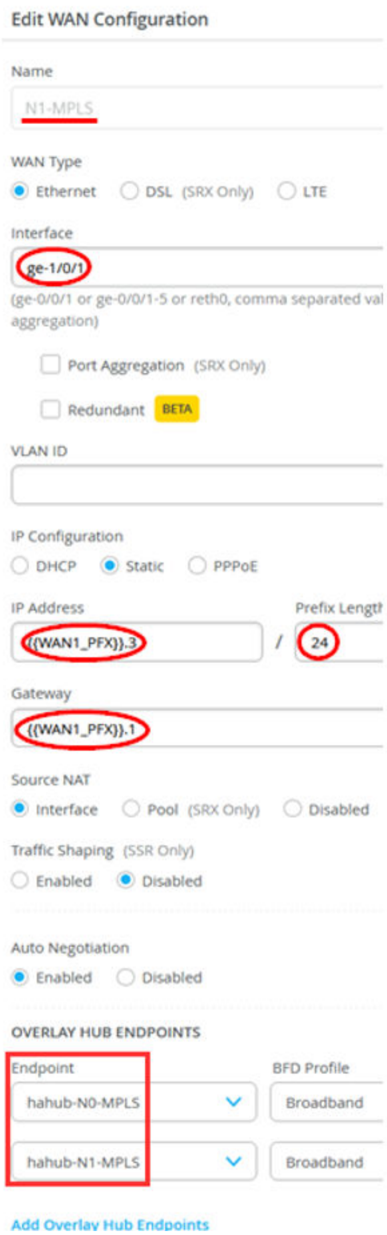
● Enabled ○ Disabled

OVERLAY HUB ENDPOINTS

Endpoint	BFD Profile
hahub-N0-INET	Broadband
hahub-N1-INET	Broadband

Add Overlay Hub Endpoints

Figure 228: WAN Interface (Fourth) Configuration for Spoke Template



Edit WAN Configuration

Name

N1-MPLS

WAN Type

● Ethernet ○ DSL (SRX Only) ○ LTE

Interface

ge-1/0/1

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

□ Port Aggregation (SRX Only)

□ Redundant BETA

VLAN ID

IP Configuration

○ DHCP ● Static ○ PPPoE

IP Address: {{WAN1_PFX}}.3 / Prefix Lengtt: 24

Gateway

{{WAN1_PFX}}.1

Source NAT

● Interface ○ Pool (SRX Only) ○ Disabled

Traffic Shaping (SSR Only)

○ Enabled ● Disabled

Auto Negotiation

● Enabled ○ Disabled

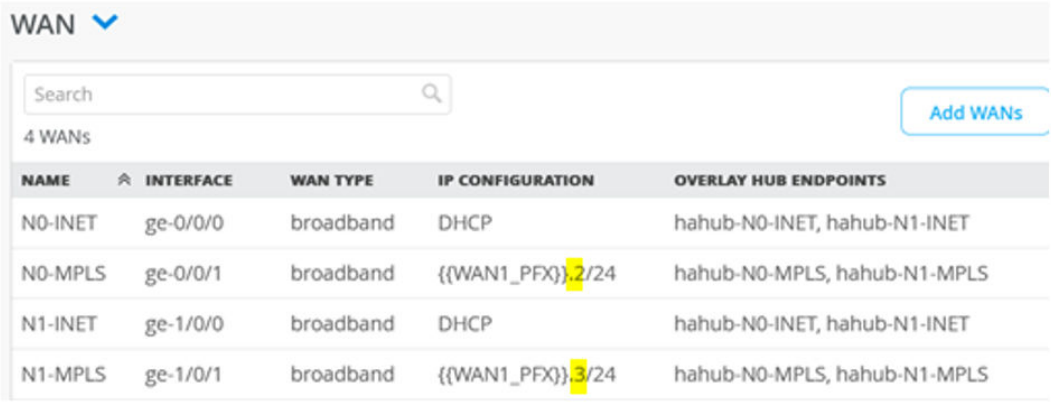
OVERLAY HUB ENDPOINTS

Endpoint	BFD Profile
hahub-N0-MPLS	Broadband
hahub-N1-MPLS	Broadband

Add Overlay Hub Endpoints

6. Mirror the configuration for each WAN and node1 interface as shown in Figure 229 on page 360. In this configuration, the Internet interfaces each get a DHCP-Lease and the MPLS interfaces have a different static IP address in the same subnet.

Figure 229: WAN Interfaces Configured in Spoke Template



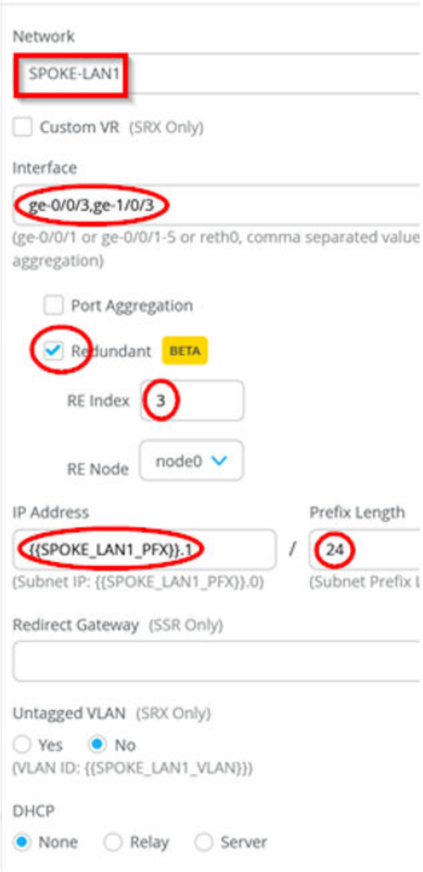
NAME	INTERFACE	WAN TYPE	IP CONFIGURATION	OVERLAY HUB ENDPOINTS
N0-INET	ge-0/0/0	broadband	DHCP	hahub-N0-INET, hahub-N1-INET
N0-MPLS	ge-0/0/1	broadband	{{WAN1_PFX}}.2/24	hahub-N0-MPLS, hahub-N1-MPLS
N1-INET	ge-1/0/0	broadband	DHCP	hahub-N0-INET, hahub-N1-INET
N1-MPLS	ge-1/0/1	broadband	{{WAN1_PFX}}.3/24	hahub-N0-MPLS, hahub-N1-MPLS

7. Edit the SPOKE-LAN1 interface to define it as a redundant interface for VRRP.

   Edit the LAN (SPOKE-LAN1) interface with the following details:

   - Network: SPOKE-LAN1
   - Add the interfaces: ge-0/0/3, ge-1/0/3
   - Redundant: Enabled
   - RE Index: 3 (As per convention, use the last octet as your index)
   - IP Address: {{SPOKE_LAN1_PFX}}.1
   - Prefix: 24 (did not change)

Figure 230: LAN Interface Configuration



Network

SPOKE-LAN1

□ Custom VR (SRX Only)

Interface

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

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

□ Port Aggregation

☑ Redundant BETA

RE Index 3

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

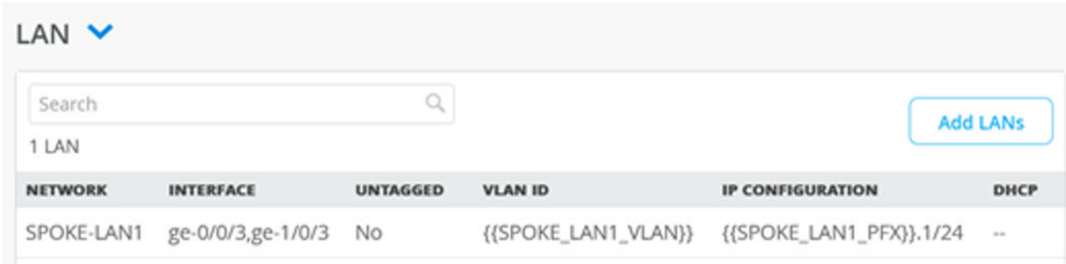
(VLAN ID: {{SPOKE_LAN1_VLAN}})

DHCP

● None ○ Relay ○ Server

Figure 231 on page 361 shows the overview the LAN interface you modified.

Figure 231: LAN Interface Configured in Spoke Template



1 LAN

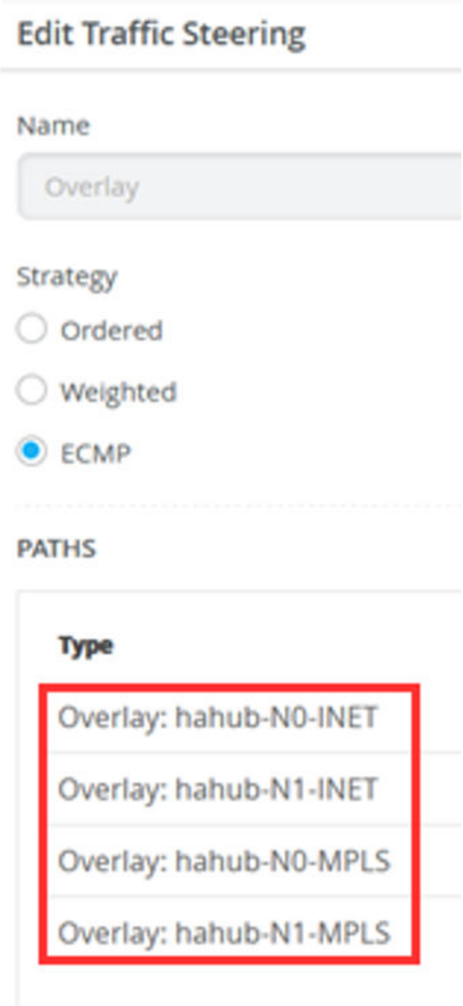
NETWORK	INTERFACE	UNTAGGED	VLAN ID	IP CONFIGURATION	DHCP
SPOKE-LAN1	ge-0/0/3,ge-1/0/3	No	{{SPOKE_LAN1_VLAN}}	{{SPOKE_LAN1_PFX}}.1/24	--

8. Change the traffic steering rules to combine the interfaces of the two HA nodes. Hence, change the existing rule for the **Overlay** as follows:

   Paths / Type

- Type=**Overlay: hahub-N0-INET**
- Type=**Overlay: hahub-N0-MPLS**
- Type=**Overlay: hahub-N1-INET**
- Type=**Overlay: hahub-N1-MPLS**

Figure 232: Modify Traffic Steering Rules in Spokes Template



Edit Traffic Steering

Name: Overlay

Strategy

○ Ordered

○ Weighted

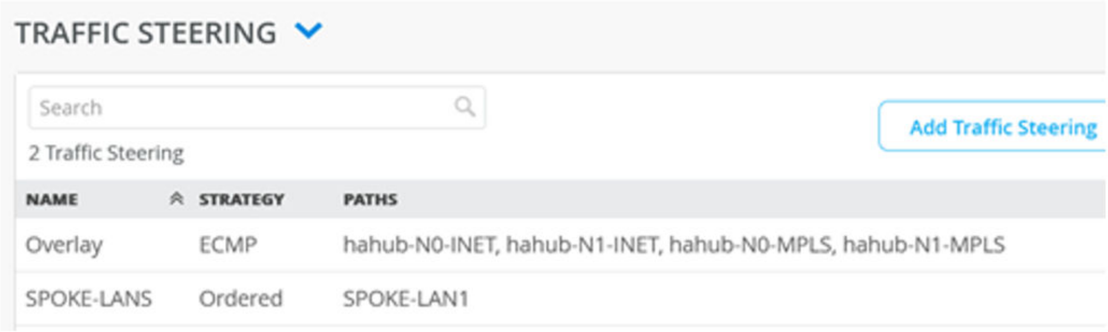
● ECMP

PATHS

Type
Overlay: hahub-N0-INET
Overlay: hahub-N1-INET
Overlay: hahub-N0-MPLS
Overlay: hahub-N1-MPLS

Figure 233 on page 363shows the modified traffic steering rules.

Figure 233: Modified Traffic Steering Rules in Spokes Template



TRAFFIC STEERING

Search

Add Traffic Steering

2 Traffic Steering

NAME	STRATEGY	PATHS
Overlay	ECMP	hahub-N0-INET, hahub-N1-INET, hahub-N0-MPLS, hahub-N1-MPLS
SPOKE-LANS	Ordered	SPOKE-LAN1

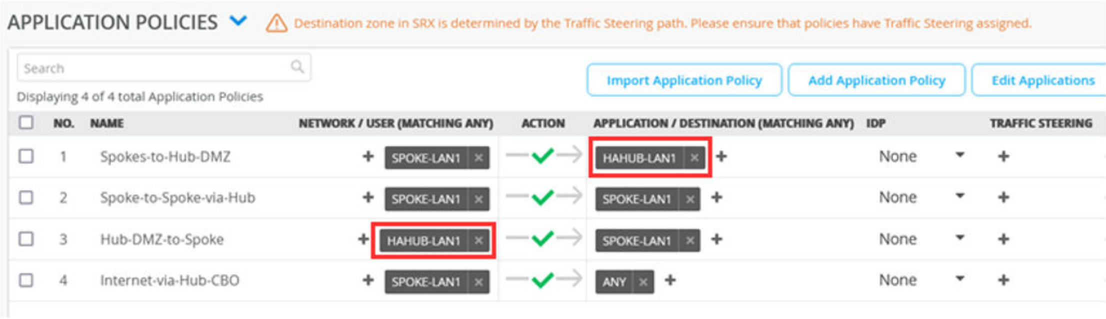
9. The Application Policies are VERY similar to the ones for spokes. We have indicated the changes you need to make below **Bold Font**. Modify the application policies according to the details provided in Table 49 on page 363.

Table 49: Application Policies in Spoke Template

No.	Rule Name	Network	Action	Destination	Steering
1	Spoke-to-Hub-DMZ	SPOKE-LAN1	Pass	**HAHUB-LAN1**	N/A
2	Spoke-to-Spoke-via-Hub	SPOKE-LAN1	Pass	SPOKE-LAN1	N/A
3	Hub-DMZ-to-Spoke	**HAHUB-LAN1**	Pass	SPOKE-LAN1	N/A
4	Internet-via-Hub-CBO	SPOKE-LAN1	Pass	ANY	N/A

Figure 234 on page 363 shows the details of application policy rules.

Figure 234: Modified Application Policies in Spoke Template



APPLICATION POLICIES

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

Search

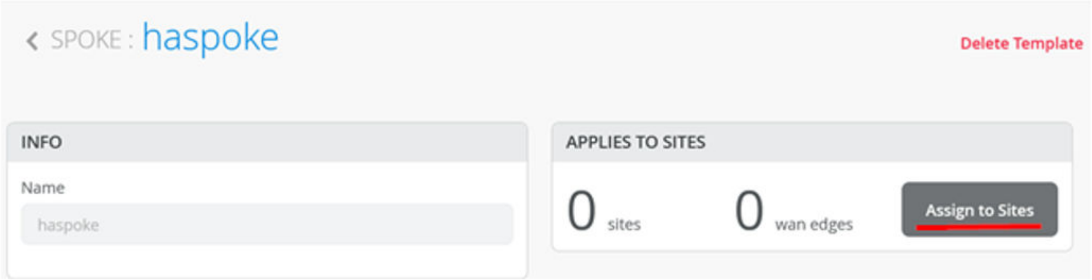
Import Application Policy | Add Application Policy | Edit Applications

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 ×	✓	HAHUB-LAN1 × +	None	+
☐	2	Spoke-to-Spoke-via-Hub	+ SPOKE-LAN1 ×	✓	SPOKE-LAN1 × +	None	+
☐	3	Hub-DMZ-to-Spoke	+ HAHUB-LAN1 ×	✓	SPOKE-LAN1 × +	None	+
☐	4	Internet-via-Hub-CBO	+ SPOKE-LAN1 ×	✓	ANY × +	None	+

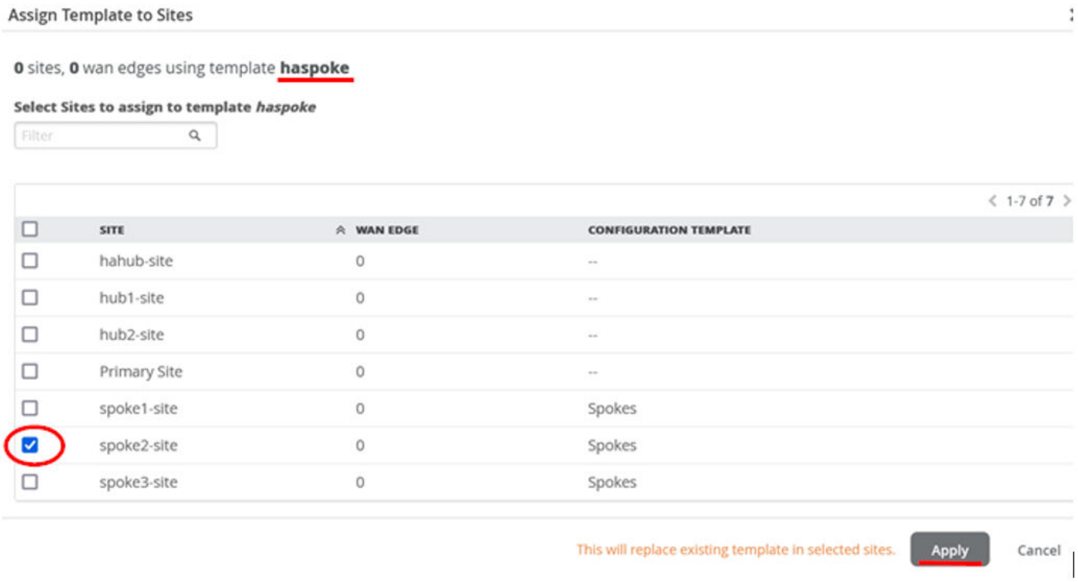
10. Assign the spoke template to site. Scroll to the top of the WAN Edge Templates page and click **Assign to Sites** under Spokes pane.

Figure 235: Assign Spoke Template to Sites



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

Figure 236: 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*

Filter

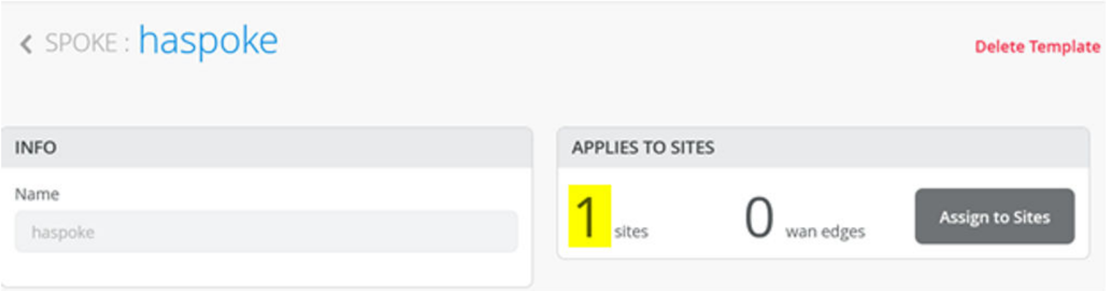
1-7 of 7

□	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.

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

Figure 237: Spoke Templates Applied to Sites

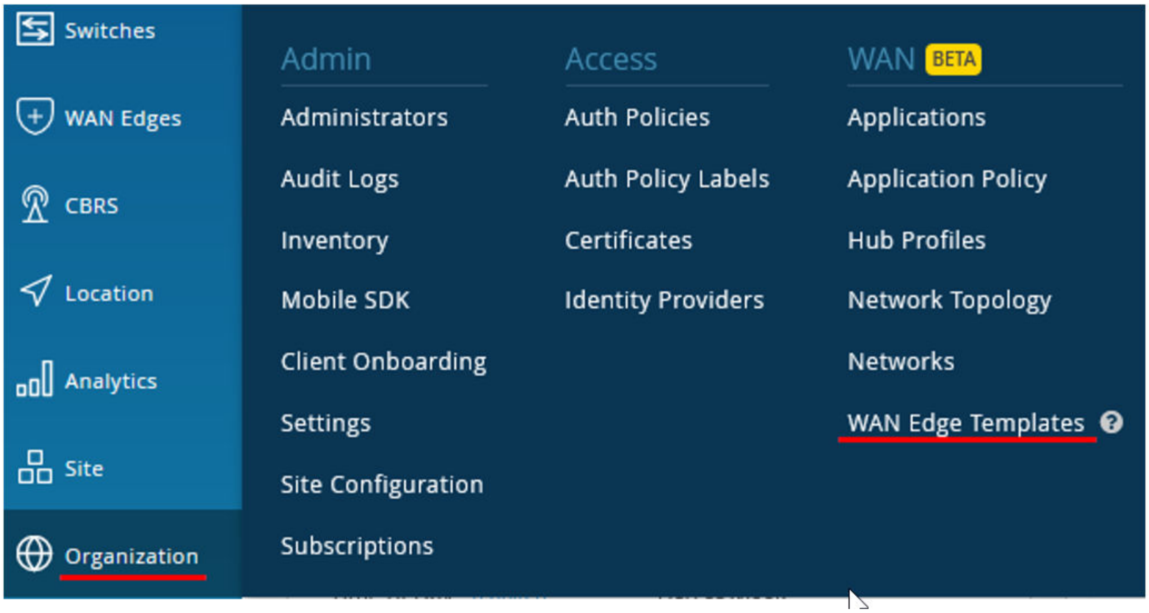


Create the Second Spoke Template

Now it’s time to clone our WAN Edge Template for our redundant spoke Node.

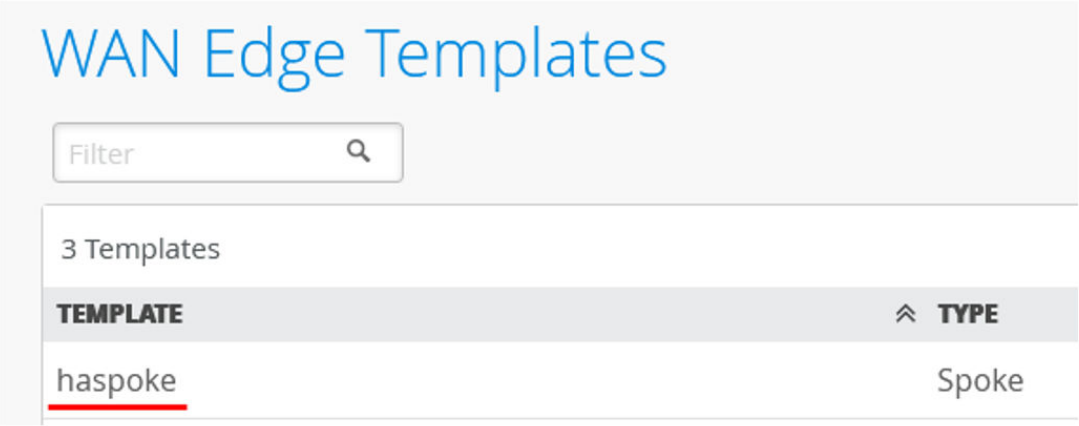
1. In the Juniper Mist cloud portal, click **Organization** > **WAN** > **WAN Edge Templates**. A list of existing templates, if any, appears.

Figure 238: WAN Edge Template



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

Figure 239: Select WAN Edge Template for Cloning

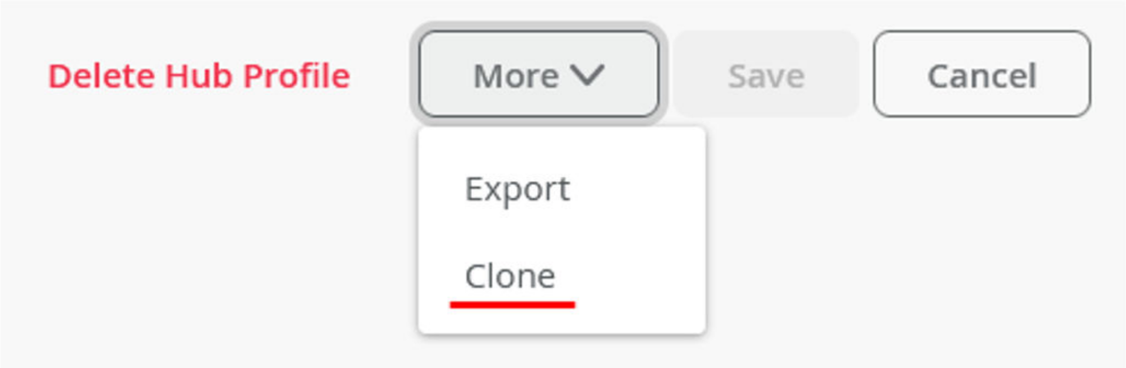


3 Templates

TEMPLATE	TYPE
haspoke	Spoke

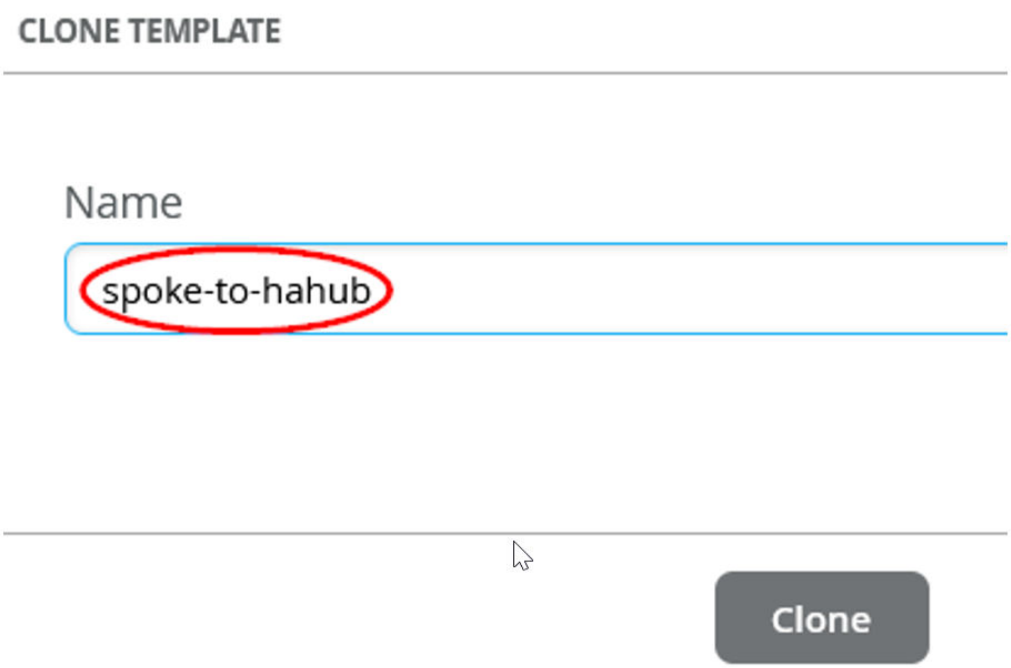
3. In the upper right corner of the screen, click **More** and select **Clone**.

Figure 240: Cloning WAN Edge Template



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

Figure 241: Renaming Cloned Template



CLONE TEMPLATE

Name: spoke-to-hahub

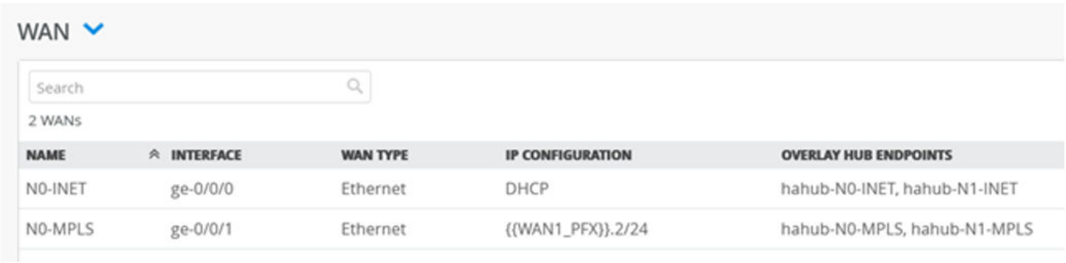
If you see any errors while naming the profile, refresh your browser.

Let’s edit the interfaces for the second node. There are few differences between this template and the former template. You have one single **node** with only two WAN interfaces. Configure the WAN interfaces:

- Delete the existing WAN interface Name: **N1-INET**
- Delete the existing WAN interface Name: **N1-MPLS**

Figure 242 on page 367 shows the result.

Figure 242: WAN Interface Details in New Cloned Template

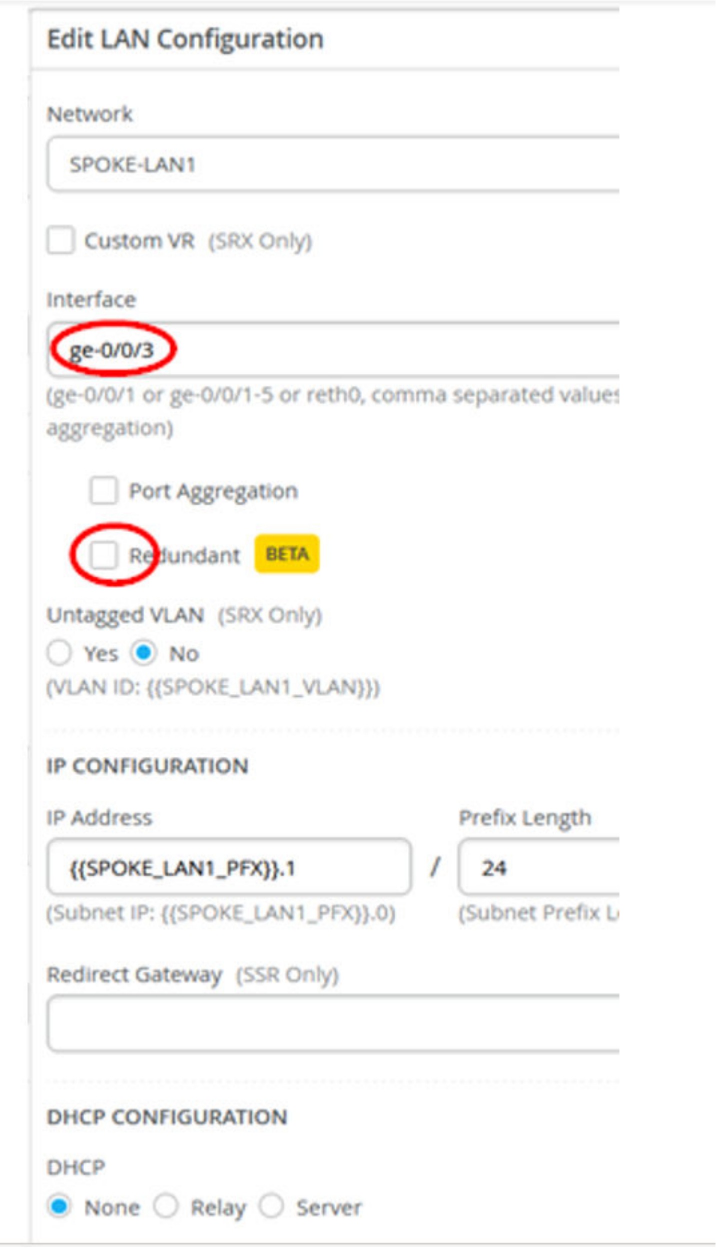


2 WANs

NAME	INTERFACE	WAN TYPE	IP CONFIGURATION	OVERLAY HUB ENDPOINTS
N0-INET	ge-0/0/0	Ethernet	DHCP	hahub-N0-INET, hahub-N1-INET
N0-MPLS	ge-0/0/1	Ethernet	{{WAN1_PFX}}.2/24	hahub-N0-MPLS, hahub-N1-MPLS

5. The LAN interfaces are no longer redundant. To archive this, configure the following Configure according to Figure 243 on page 368.

Figure 243: LAN Interface Configuration



Edit LAN Configuration

Network

SPOKE-LAN1

□ Custom VR (SRX Only)

Interface

ge-0/0/3

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

□ Port Aggregation

□ Redundant BETA

Untagged VLAN (SRX Only)

○ Yes ● No

(VLAN ID: {{SPOKE_LAN1_VLAN}})

IP CONFIGURATION

IP Address

{{SPOKE_LAN1_PFX}}.1 /

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

Prefix Length

24

(Subnet Prefix L

Redirect Gateway (SSR Only)

DHCP CONFIGURATION

DHCP

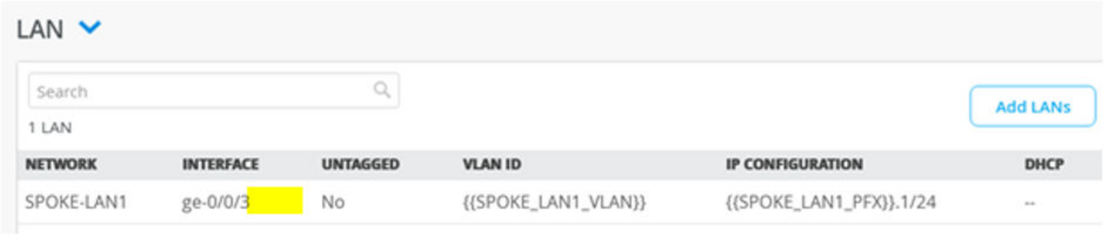
● None ○ Relay ○ Server

Configure the following options:

- Change the Interface: **ge-0/0/3**
- Change Redundant: **Disabled**

Figure 244 on page 369 shows the result.

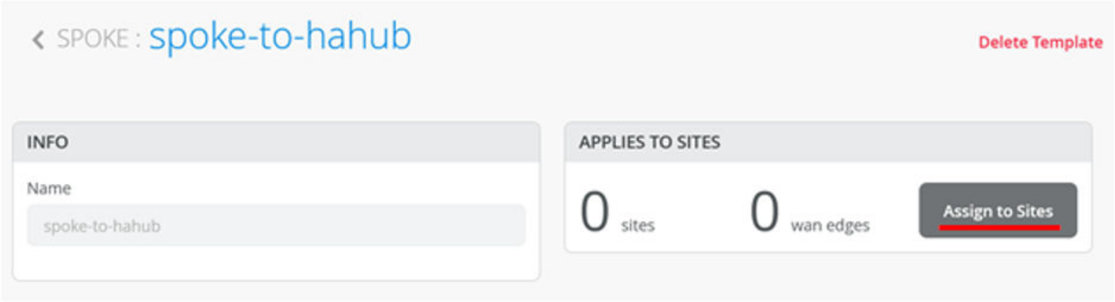
Figure 244: LAN Interface Details



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

6. The **Traffic Steering** rules and **Application Policies** are the same as in the last **Template** and do not need to be changed.
7. Assign the spoke template to site. Scroll to the top of the WAN Edge Templates page and click **Assign to Sites** under Spokes pane

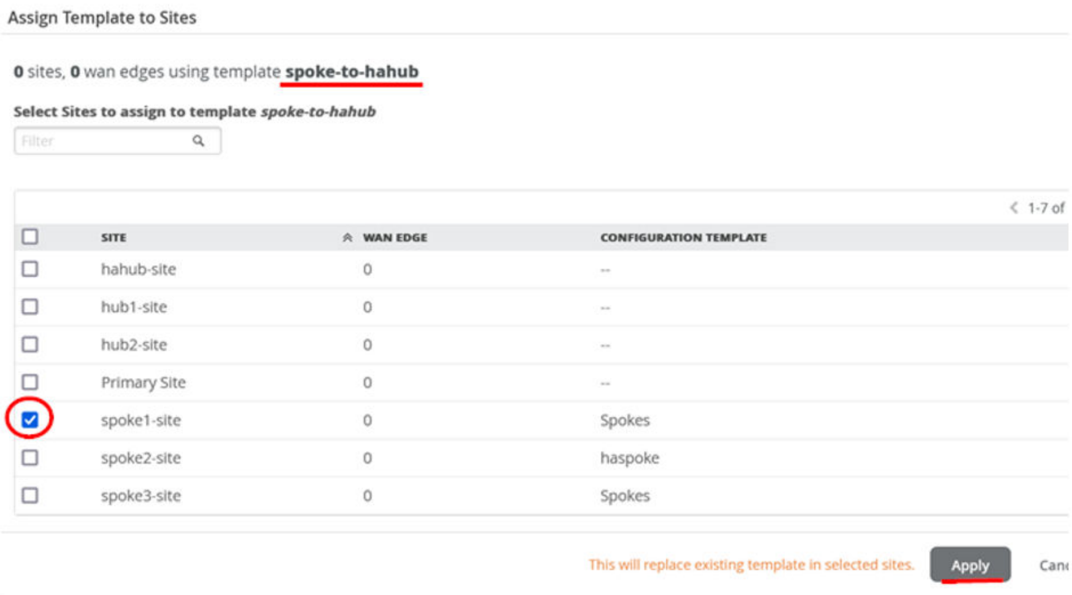
Figure 245: Assign Template to Site



Name: spoke-to-hahub

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

Figure 246: Selecting Site for Assigning Template



Assign Template to Sites

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

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

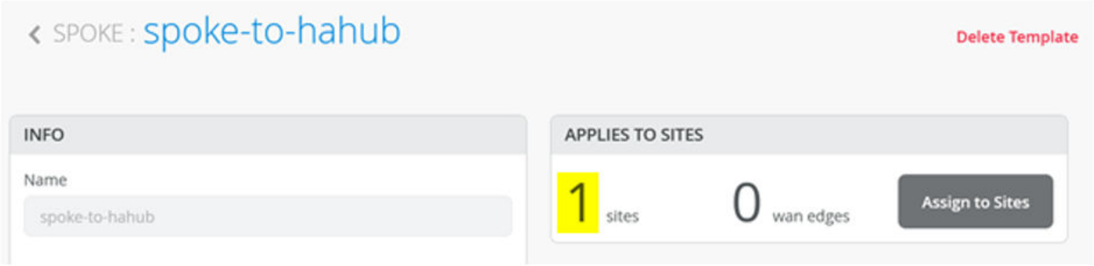
□	SITE	WAN EDGE	CONFIGURATION TEMPLATE
□	hahub-site	0	--
□	hub1-site	0	--
□	hub2-site	0	--
□	Primary Site	0	--
☑	spoke1-site	0	Spokes
□	spoke2-site	0	haspoke
□	spoke3-site	0	Spokes

This will replace existing template in selected sites.

9. Click **Apply**.

10. Ensure that your template is now assigned to a site. Check that your **Template** now has at least 1 **Site** assigned as shown in Figure 247 on page 370.

Figure 247: Spoke Templates Applied to Sites



SPOKE : spoke-to-hahub

INFO

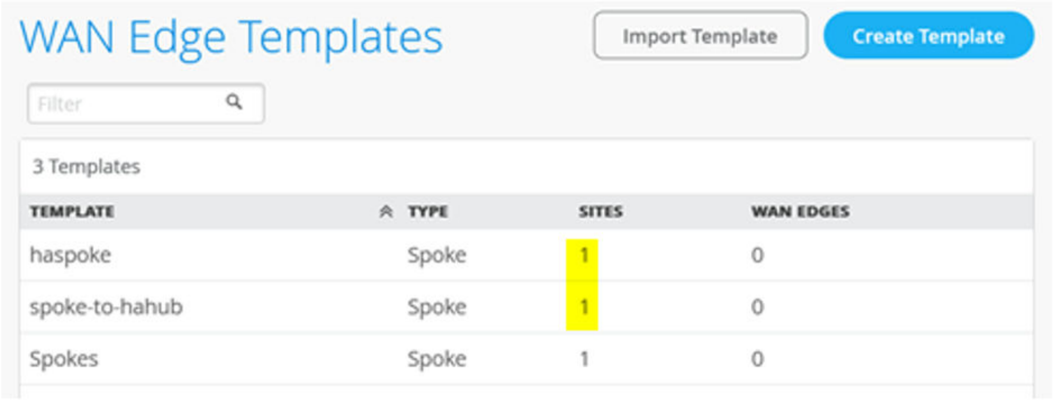
Name: spoke-to-hahub

APPLIES TO SITES

1 sites 0 wan edges

Figure 248 on page 371 shows the list of configured spoke templates.

Figure 248: List of WAN Edge Templates



3 Templates

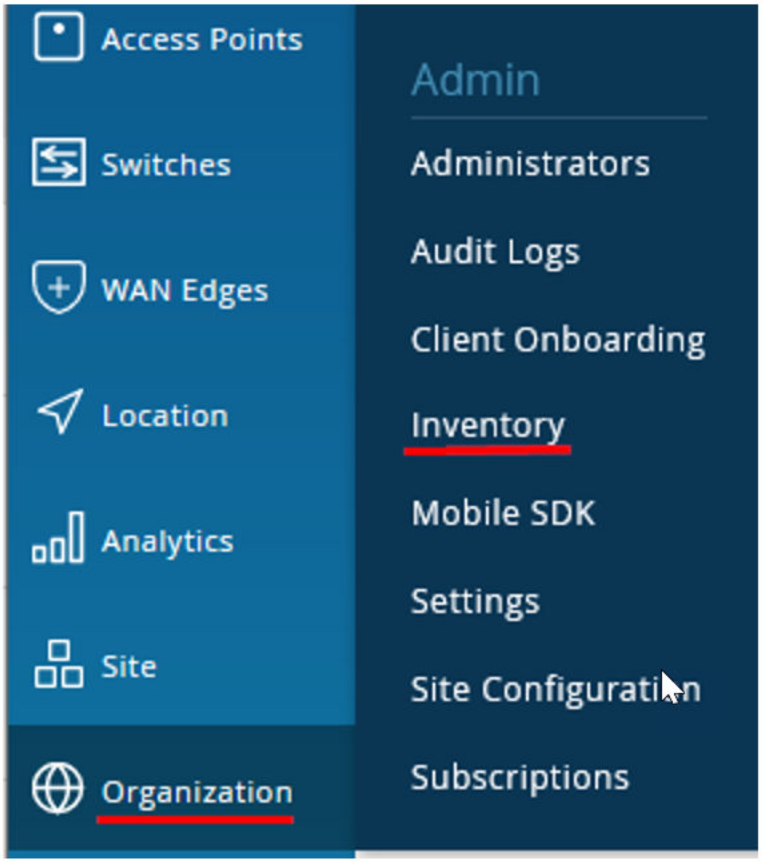
TEMPLATE	TYPE	SITES	WAN EDGES
haspoke	Spoke	1	0
spoke-to-hahub	Spoke	1	0
Spokes	Spoke	1	0

Onboard your Devices

You can **Claim** or **Adopt** to onboard devices into your organization inventory. For details on getting your Session Smart Router up and running in the Mist cloud, see SSR Series Devices.

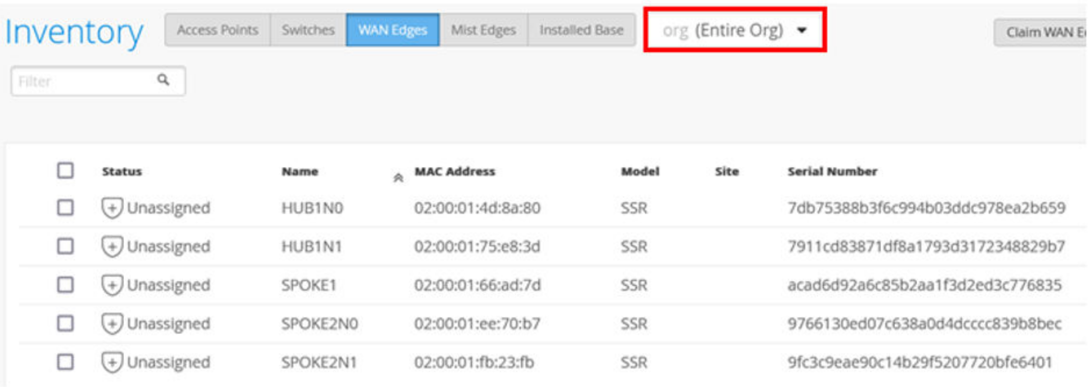
1. In the Juniper Mist portal. click **Organization** > **Admin** >**Inventory**.

Figure 249: Navigating to Inventory



2. 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 Figure 250 on page 372.

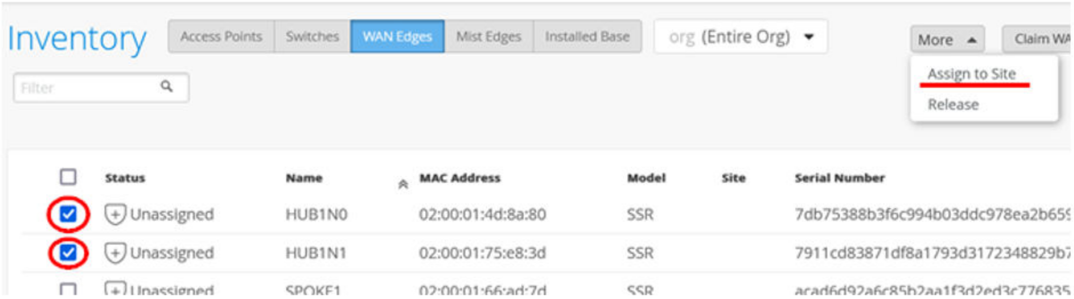
Figure 250: Session Smart Router in Inventory



□	Status	Name	MAC Address	Model	Site	Serial Number
□	Unassigned	HUB1N0	02:00:01:4d:8a:80	SSR		7db75388b3f6c994b03ddc978ea2b659
□	Unassigned	HUB1N1	02:00:01:75:e8:3d	SSR		7911cd83871df8a1793d3172348829b7
□	Unassigned	SPOKE1	02:00:01:66:ad:7d	SSR		acad6d92a6c85b2aa1f3d2ed3c776835
□	Unassigned	SPOKE2N0	02:00:01:ee:70:b7	SSR		9766130ed07c638a0d4dcccc839b8bec
□	Unassigned	SPOKE2N1	02:00:01:fb:23:fb	SSR		9fc3c9eae90c14b29f5207720bfe6401

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

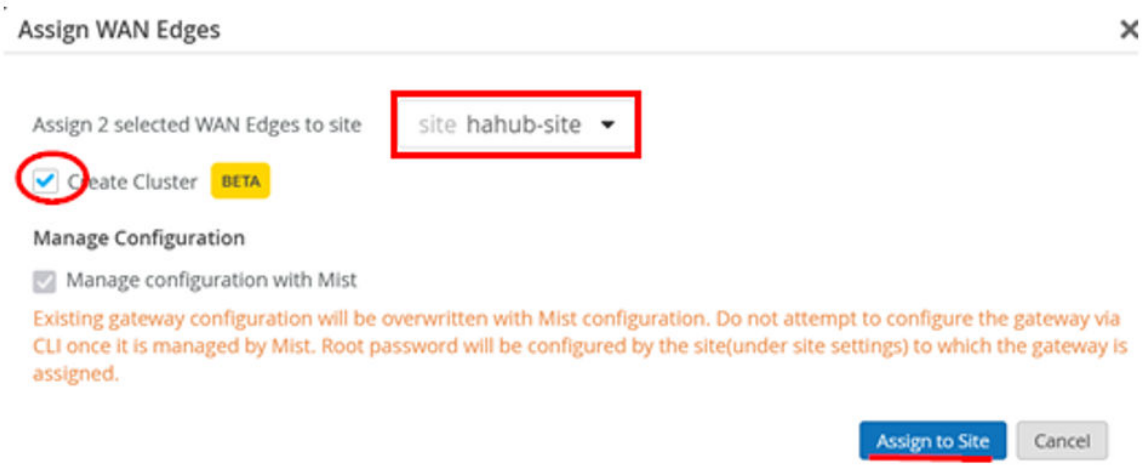
Figure 251: Assigning Session Smart Routers (HA Pair) to Site



☐	Status	Name	MAC Address	Model	Site	Serial Number
☑	Unassigned	HUB1N0	02:00:01:4d:8a:80	SSR		7db75388b3f6c994b03ddc978ea2b65
☑	Unassigned	HUB1N1	02:00:01:75:e8:3d	SSR		7911cd83871df8a1793d3172348829b7
☐	Unassigned	SPOKE1	02:00:01:66:ad:7d	SSR		acad6d92a6c85b2aa1f3d2ed3c776835

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

Figure 252: Assign Spoke Devices to Site and Initiate Cluster Formation



Assign 2 selected WAN Edges to site site hahub-site

☑ Create Cluster

Manage Configuration

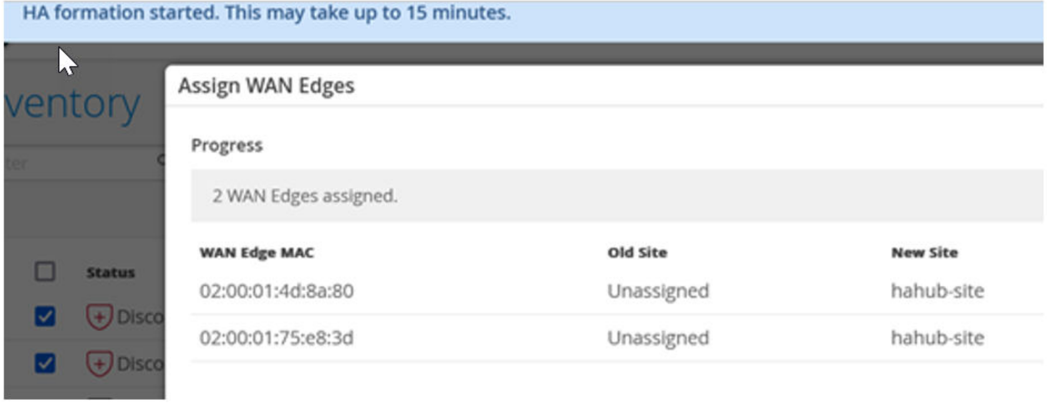
☑ Manage configuration with Mist

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 is assigned.

5. 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.

Figure 253: HA Cluster Formation for Assigned Devices



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

Assign WAN Edges

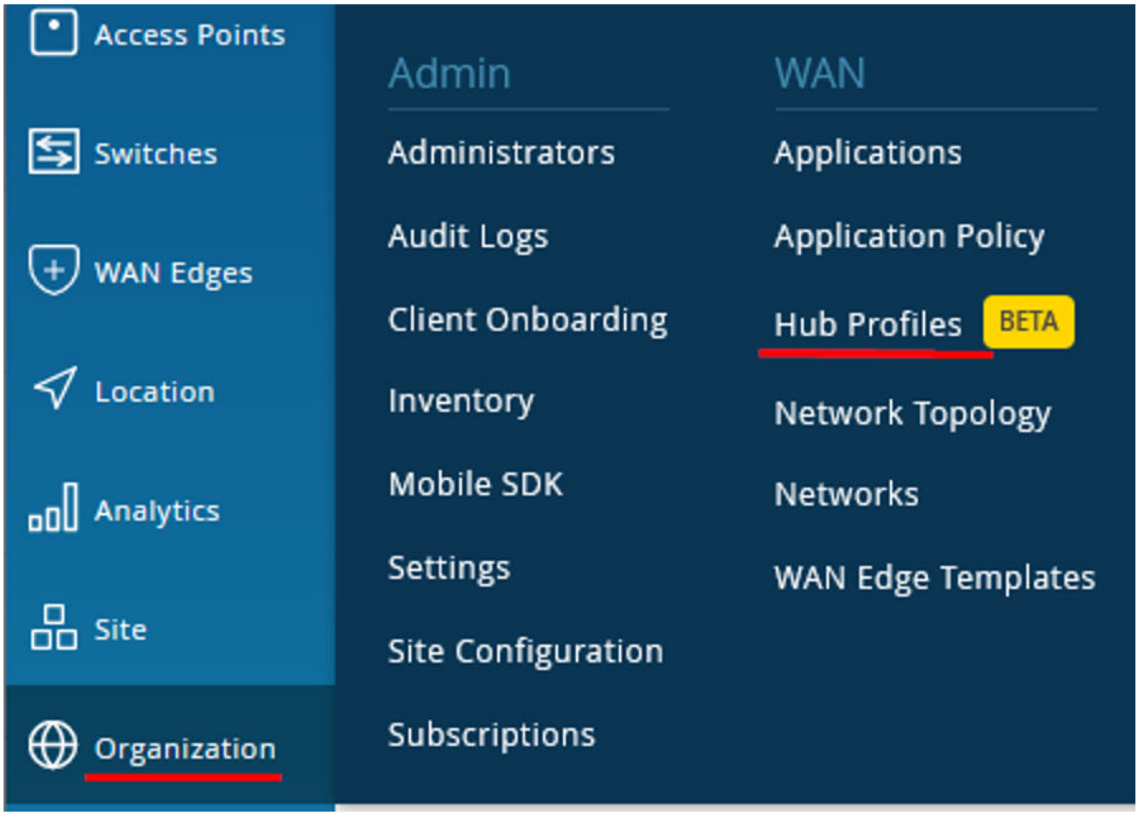
Progress

2 WAN Edges assigned.

WAN Edge MAC	Old Site	New Site
02:00:01:4d:8a:80	Unassigned	hahub-site
02:00:01:75:e8:3d	Unassigned	hahub-site

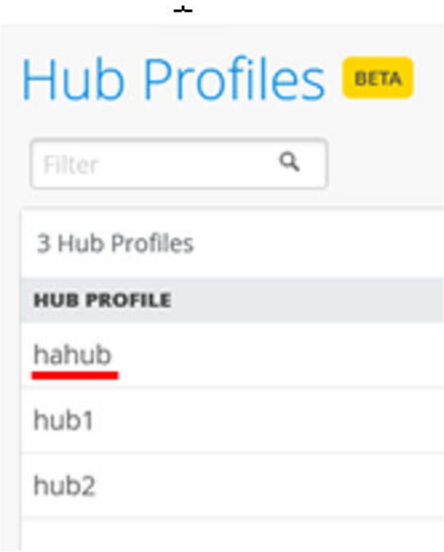
6. In the Juniper Mist portal, click **Organization** > **WAN** > **Hub Profiles**. The Hub Profile displays the list of existing profiles.

Figure 254: Navigating to Hub Profiles



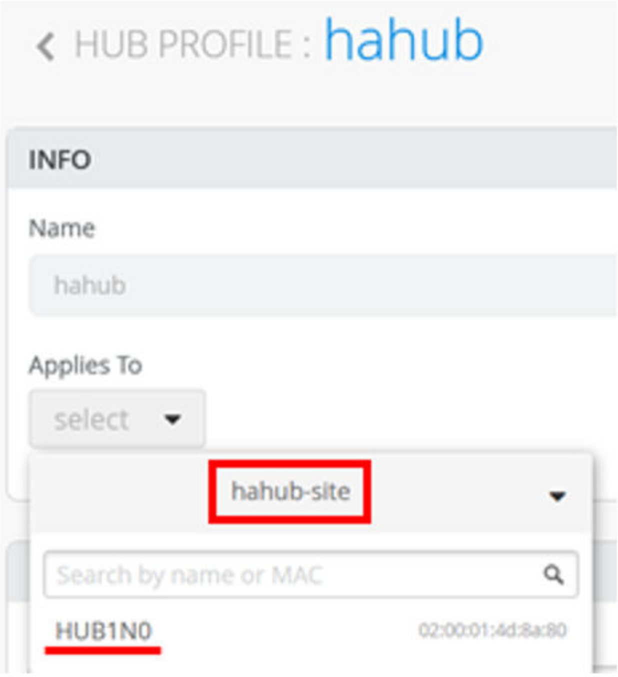
7. Click the hub profile (hahub) that you want to assign to a site.

Figure 255: Select Hub Profile



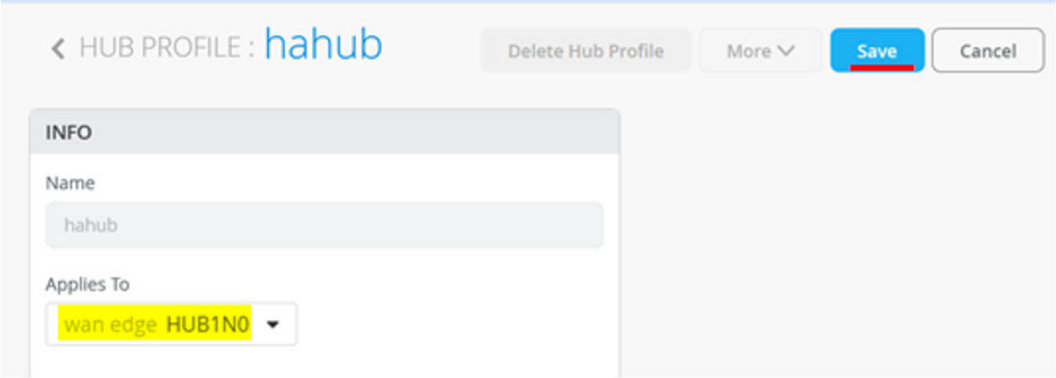
8. Under the **Applies To** option, select the site (hahub-site) from the list of available sites.

Figure 256: Select Sites for Applying Hub Profile



9. Check if have correct WAN Edge device selected, and click **Save**.

Figure 257: Select WAN Edge Device to Apply Template



< HUB PROFILE : hahub

Delete Hub Profile | More | Save | Cancel

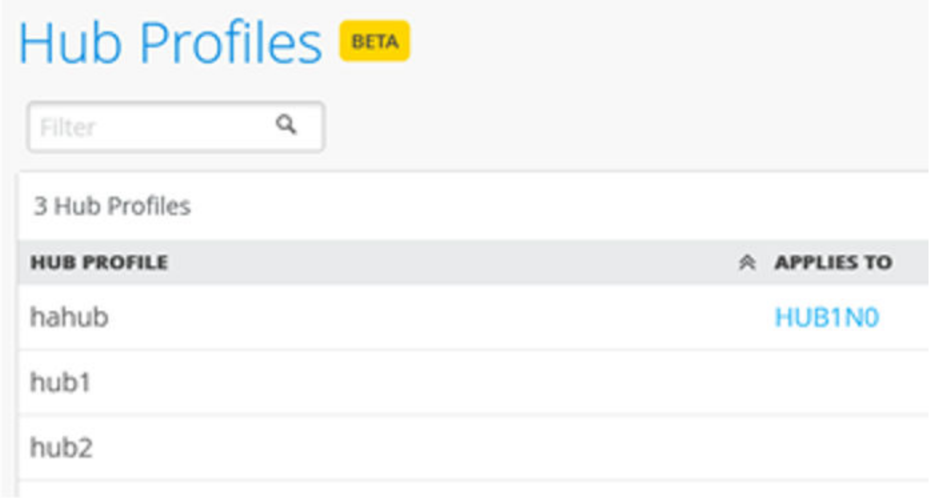
INFO

Name: hahub

Applies To: wan edge HUB1N0

10. You should now see the HA devices assigned to their **Hub Profile** in the as shown in Figure 258 on page 376.

Figure 258: Hub Profile Assignment Summary



Hub Profiles BETA

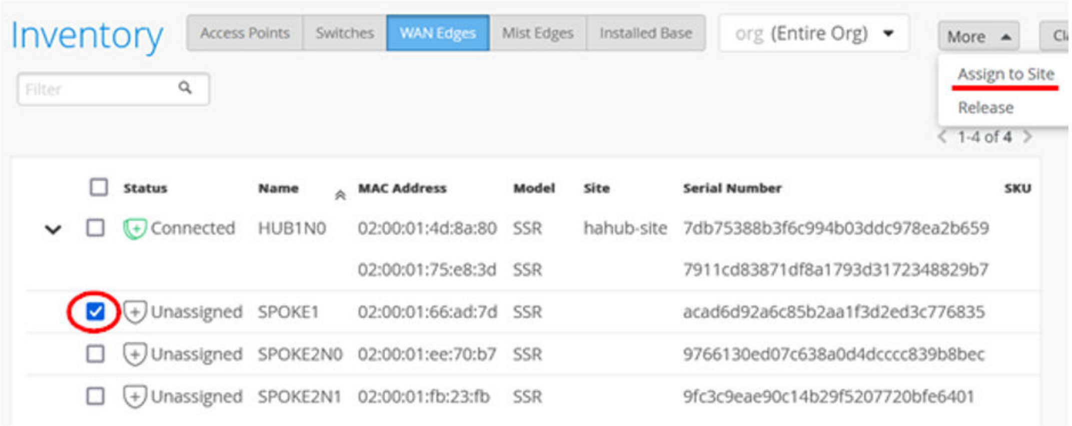
Filter

3 Hub Profiles

HUB PROFILE	APPLIES TO
hahub	HUB1N0
hub1	
hub2	

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

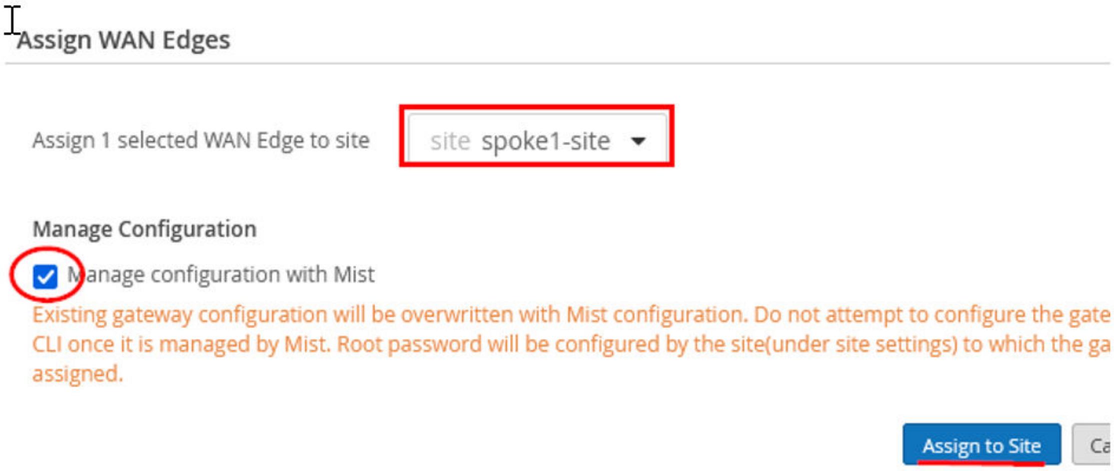
Figure 259: Assign Spoke Device To Site



	Status	Name	MAC Address	Model	Site	Serial Number	SKU
□	Connected	HUB1N0	02:00:01:4d:8a:80	SSR	hahub-site	7db75388b3f6c994b03ddc978ea2b659	
			02:00:01:75:e8:3d	SSR		7911cd83871df8a1793d3172348829b7	
☑	Unassigned	SPOKE1	02:00:01:66:ad:7d	SSR		acad6d92a6c85b2aa1f3d2ed3c776835	
□	Unassigned	SPOKE2N0	02:00:01:ee:70:b7	SSR		9766130ed07c638a0d4dcccc839b8bec	
□	Unassigned	SPOKE2N1	02:00:01:fb:23:fb	SSR		9fc3c9eae90c14b29f5207720bfe6401	

13. In Assign WAN Edges page, select **spoke1-site** and enable **Manage configuration with Mist**.

Figure 260: Assign WAN Edge Device to Site



Assign WAN Edges

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

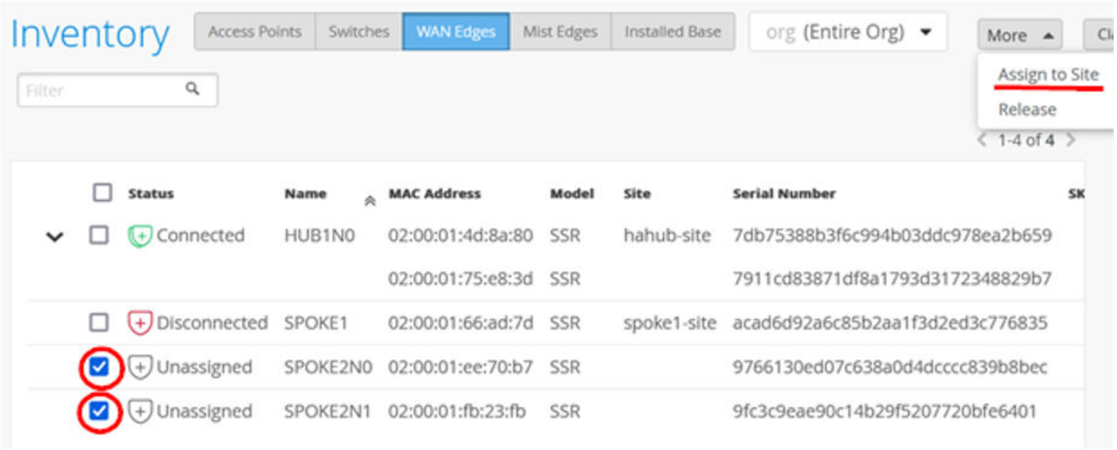
Manage Configuration

☑ Manage configuration with Mist

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

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

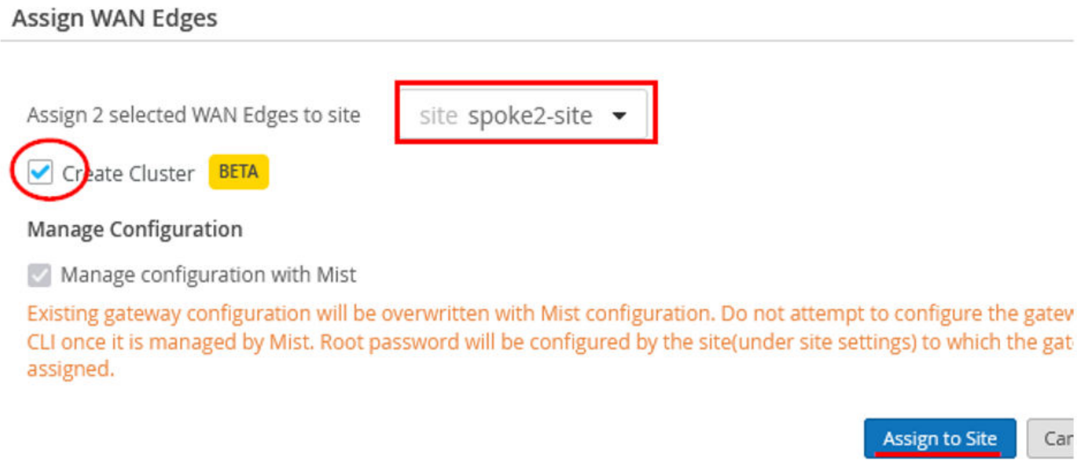
Figure 261: Assign Spoke Devices to Site



	Status	Name	MAC Address	Model	Site	Serial Number	SK
□	Connected	HUB1N0	02:00:01:4d:8a:80	SSR	hahub-site	7db75388b3f6c994b03ddc978ea2b659	
			02:00:01:75:e8:3d	SSR		7911cd83871df8a1793d3172348829b7	
□	Disconnected	SPOKE1	02:00:01:66:ad:7d	SSR	spoke1-site	acad6d92a6c85b2aa1f3d2ed3c776835	
☑	Unassigned	SPOKE2N0	02:00:01:ee:70:b7	SSR		9766130ed07c638a0d4dcccc839b8bec	
☑	Unassigned	SPOKE2N1	02:00:01:fb:23:fb	SSR		9fc3c9eae90c14b29f5207720bfe6401	

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

Figure 262: 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

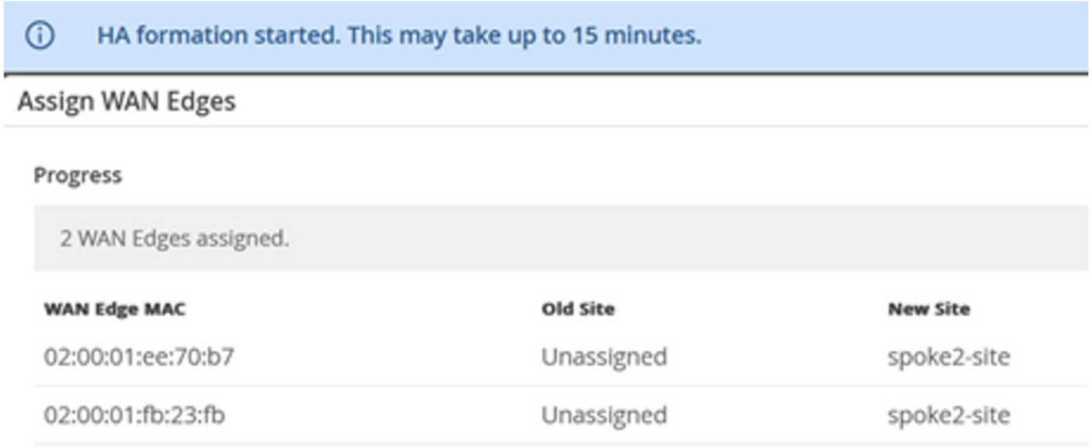
Manage Configuration

☑ 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.

The portal displays the details of WAN edge devices assigned to site and progress of cluster formation as shown in Figure 263 on page 379.

Figure 263: Cluster Formation Progress



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

Assign WAN Edges

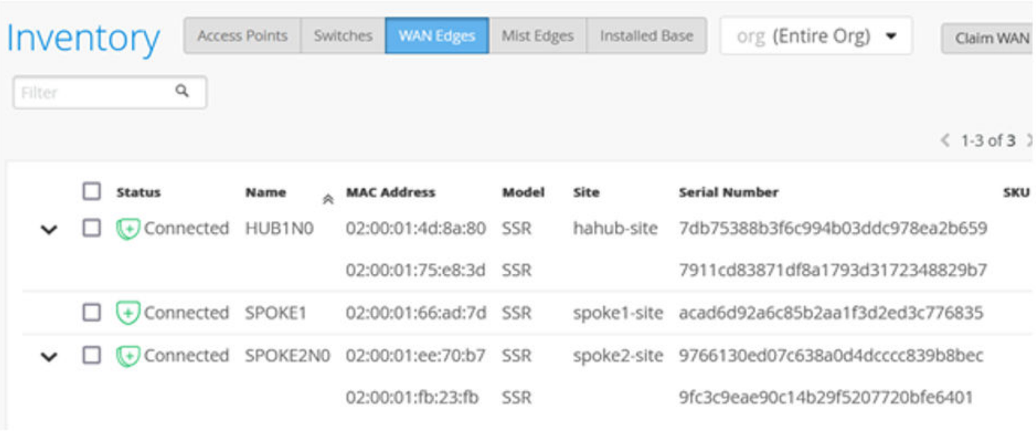
Progress

2 WAN Edges assigned.

WAN Edge MAC	Old Site	New Site
02:00:01:ee:70:b7	Unassigned	spoke2-site
02:00:01:fb:23:fb	Unassigned	spoke2-site

17. Go to Inventory Page. Figure 264 on page 379 shows the details of devices assigned to site and high availability pairs.

Figure 264: Inventory Display of HA Pair Details



	□	Status	Name	MAC Address	Model	Site	Serial Number	SKU
⌄	□	Connected	HUB1N0	02:00:01:4d:8a:80	SSR	hahub-site	7db75388b3f6c994b03ddc978ea2b659	
				02:00:01:75:e8:3d	SSR		7911cd83871df8a1793d3172348829b7	
	□	Connected	SPOKE1	02:00:01:66:ad:7d	SSR	spoke1-site	acad6d92a6c85b2aa1f3d2ed3c776835	
⌄	□	Connected	SPOKE2N0	02:00:01:ee:70:b7	SSR	spoke2-site	9766130ed07c638a0d4dcccc839b8bec	
				02:00:01:fb:23:fb	SSR		9fc3c9eae90c14b29f5207720bfe6401	

Refresh your browser and check under WAN Edges to find out if your Session Smart Routers are part of the inventory as HA Pairs.

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

Replace an Session Smart Router Node in a High Availability Cluster

You can replace an Session Smart Router device from a high availability cluster setup with few simple steps.

Before you replace a Session Smart Router node from the cluster, you must:

- Remove the cluster fabric cables from the node being replaced and connect it to the new replacement node.
- Make sure that the replacement Session Smart Router is both the same model as the device being replaced and has a firmware version higher than 6.0
- If you are replacing a node with a new out-of-the box Session Smart Router, ensure that you:
  - Claim the new Session Smart Router to the same site where the Session Smart Router cluster is present.
  - Upgrade the firmware of the Session Smart Router to a version above 6.0.

NOTE: Replacing a node in a high availability setup cause minimal impact on network services. Therefore, we recommend that you plan for a maintenance window to do this task.

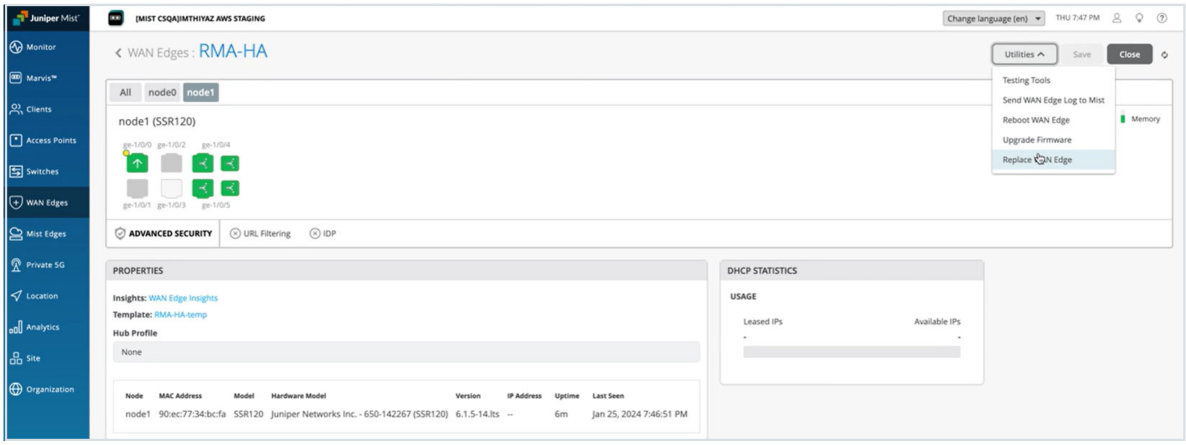
To replace a Session Smart Router:

1. In the Juniper Mist portal, on the left navigation bar, go to **Organization** > **Admin** >**Inventory** and select **WAN Edges** tab.

   Alternatively, you can also go to **WAN Edges** > **WAN Edges** page.

   The page displays a list of WAN edge devices. You can set the view as **org (Entire Org)** or **Site** in the inventory page.
2. Click the high availability pair that you want to replace a node to open the details in a new page.
3. Select **Replace WAN Edge** from Utilities drop-down.

Figure 265: Select Session Smart Routers (HA Pair) to Replace

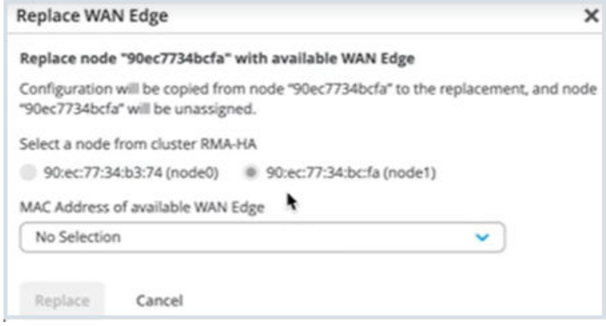


Insights: WAN Edge Insights
Template: RMA-HA-temp
Hub Profile
None

Node	MAC Address	Model	Hardware Model	Version	IP Address	Uptime	Last Seen
node1	90:ec:77:34:bc:fa	SSR120	Juniper Networks Inc. - 650-142267 (SSR120)	6.1.5-14.lts	--	6m	Jan 25, 2024 7:46:51 PM

4. On the Replace WAN Edge window, select the old Session Smart Router node that you want to replace and select the new replacement device's MAC address from the **MAC Address of available WAN Edge** drop-down list.

Figure 266: Replace Session Smart Router with Another Device



Replace node "90ec7734bcfa" with available WAN Edge

Configuration will be copied from node "90ec7734bcfa" to the replacement, and node "90ec7734bcfa" will be unassigned.

Select a node from cluster RMA-HA

○ 90:ec:77:34:b3:74 (node0) ● 90:ec:77:34:bc:fa (node1)

MAC Address of available WAN Edge

No Selection

After you click **Replace**, allow about 15 minutes to complete the replacement procedure.

Refresh your browser and check under WAN Edges to find out if your Session Smart Routers high availability setup is updated and available as a part of the inventory.

Replace a Standalone Session Smart Router

You can replace connected or disconnected Session Smart Router with another device of the same model.

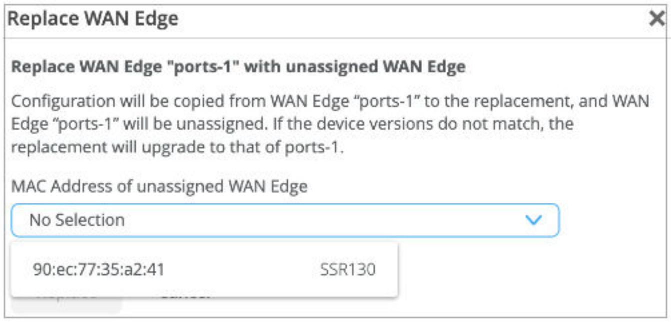
1. In the Juniper Mist portal, on the left navigation bar, go to **Organization** > **Admin** >**Inventory** and select **WAN Edges** tab.

Alternatively, you can also go to **WAN Edges** > **WAN Edges** page.

The page displays a list of WAN edge devices. You can set the view as **org (Entire Org)** or **Site** in the inventory page.

2. Click the Session Smart Router that you want to replace.
3. Select **Replace WAN Edge** from Utilities drop-down.
4. On the Replace WAN Edge window, select the new replacement device's MAC address from the **MAC Address of unassigned WAN Edge** drop-down list.

Figure 267: Replace a Standalone SRX Series Firewall



Replace WAN Edge

Replace WAN Edge "ports-1" with unassigned WAN Edge

Configuration will be copied from WAN Edge "ports-1" to the replacement, and WAN Edge "ports-1" will be unassigned. If the device versions do not match, the replacement will upgrade to that of ports-1.

MAC Address of unassigned WAN Edge

No Selection

90:ec:77:35:a2:41 SSR130

Juniper Mist portal displays a list of supported models available in the inventory page in unassigned state.

After you click **Replace**, allow about 15 minutes to complete the replacement procedure. System copies the configuration of the replaced Session Smart Router into the new device. The replaced Session Smart Router continues to be part of the site in unassigned state.

Refresh your browser and check under WAN Edges to find out if your Session Smart Router is available as a part of the inventory.

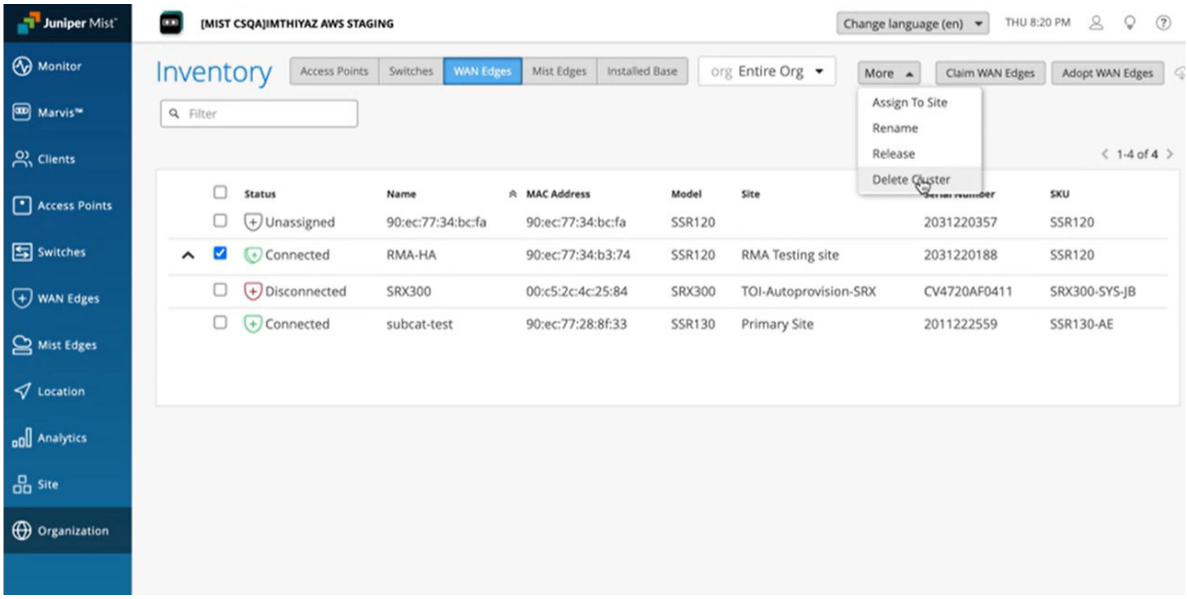
Delete a High Availability Cluster

1. In the Juniper Mist portal, on the left navigation bar, go to **Organization** > **Admin** >**Inventory** and select **WAN Edges** tab.

   Alternatively, you can also go to **WAN Edges** > **WAN Edges** page.

   The page displays a list of WAN edge devices. You can set the view as **org (Entire Org)** or **Site** in the inventory page.
2. Select the high availability pair and click **Delete Cluster** under **More**.

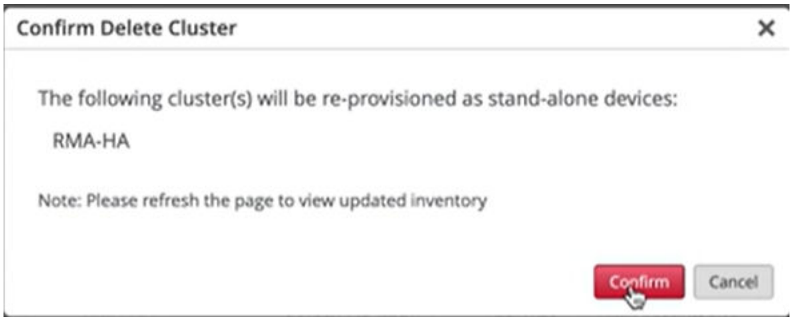
Figure 268: Select Session Smart Routers (HA Pair) to Delete



	Status	Name	MAC Address	Model	Site	Serial Number	SKU
□	Unassigned	90:ec:77:34:bc:fa	90:ec:77:34:bc:fa	SSR120		2031220357	SSR120
☑	Connected	RMA-HA	90:ec:77:34:b3:74	SSR120	RMA Testing site	2031220188	SSR120
□	Disconnected	SRX300	00:c5:2c:4c:25:84	SRX300	TOI-Autoprovision-SRX	CV4720AF0411	SRX300-SYS-JB
□	Connected	subcat-test	90:ec:77:28:8f:33	SSR130	Primary Site	2011222559	SSR130-AE

Click **Confirm** on the **Confirm Delete Cluster** message.

Figure 269: Delete Session Smart Router with Another Device


Confirm Delete Cluster

The following cluster(s) will be re-provisioned as stand-alone devices:

RMA-HA

Note: Please refresh the page to view updated inventory

Juniper Mist re-provisions the devices as standalone devices in the same site.

Refresh your browser and check under WAN Edges to find out if your Session Smart Routers are available as standalone devices in the inventory.

SEE ALSO

- WAN Assurance Configuration Overview | 31
- Configure Sites and Variables for Session Smart Routers | 33
- Configure Networks for Session Smart Routers | 38

Configure Applications for Session Smart Routers | 48

Configure Application Policies on Session Smart Routers | 58

Configure Hub Profile for Session Smart Routers | 66

Configure WAN Edge Templates for Session Smart Routers | 92

Onboard Session Smart Routers for WAN Configuration | 132

Onboard Session Smart Routers for WAN Configuration | 132

Full Stack Design for SRX Series Firewalls

IN THIS SECTION

The Juniper® SD-WAN driven by Mist AI™ Full Stack design example is a follow-up to the Mist WAN Assurance deployment for SRX Series Firewalls. For more details, see "WAN Assurance Configuration Overview" on page 166.

Overview

IN THIS SECTION

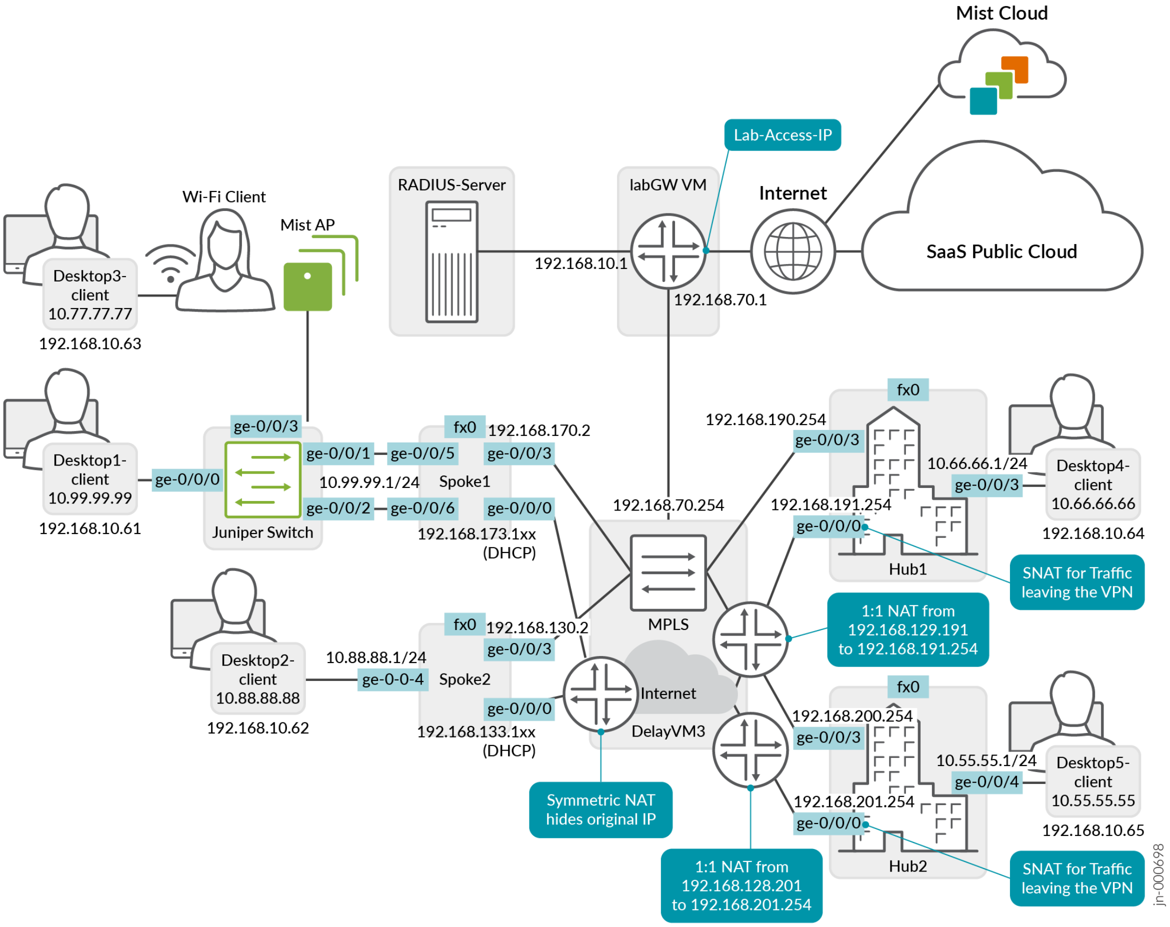
With this configuration example, you’re expanding network capabilities by integrating Mist APs and Juniper EX Switches. This full stack example shows you how to set up your Juniper SD-WAN SRX Series WAN edge devices in concert with Juniper EX Series Switches deployed in wired assurance. This brings all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

Figure 270 on page 386 shows the Full Stack Juniper Mist WAN Assurance topology used in this example.

Figure 270: 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. You can find the details on WAN edge templates here: "Configure WAN Edge Templates for SRX Series Firewalls" on page 217.

In addition, this example uses:

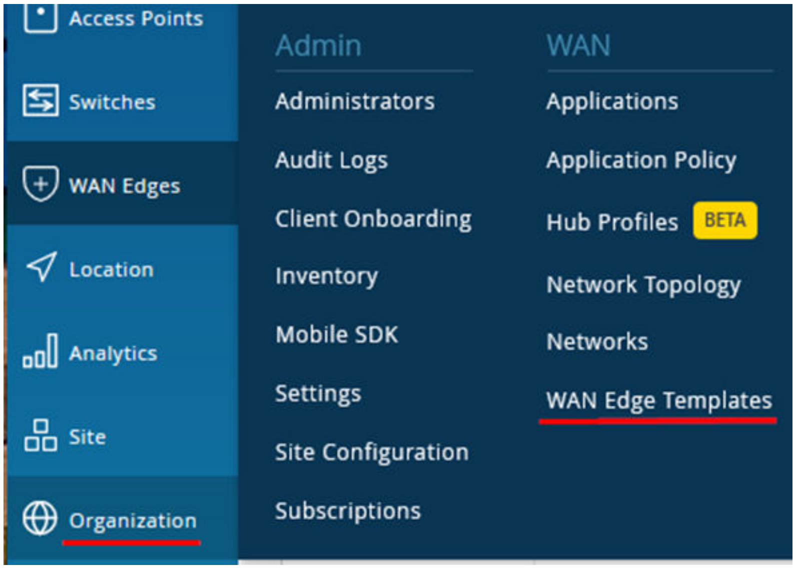
- **Desktop3 VM** (VLAN1077) - Operates as a viewer for the Raspberry Pi, the wireless client. Alternatively, you could use a local notebook.
- **Desktop1 VM** (VLAN1099) - Connected to the interface **ge-0/0/0** of the new branch switch.

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.

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

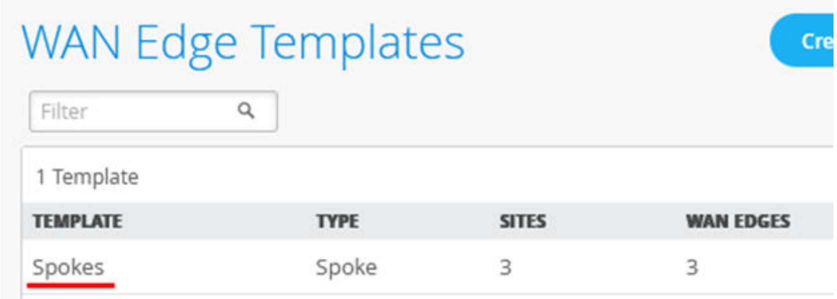
Figure 271: Navigate to WAN Edge Template



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

A list of existing templates, if any, appears.

Figure 272: List of WAN Edge Templates



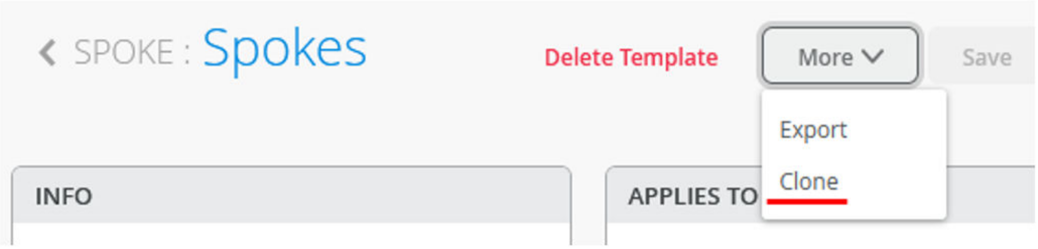
1 Template

TEMPLATE	TYPE	SITES	WAN EDGES
Spokes	Spoke	3	3

Create a spoke template by cloning an existing spoke template.

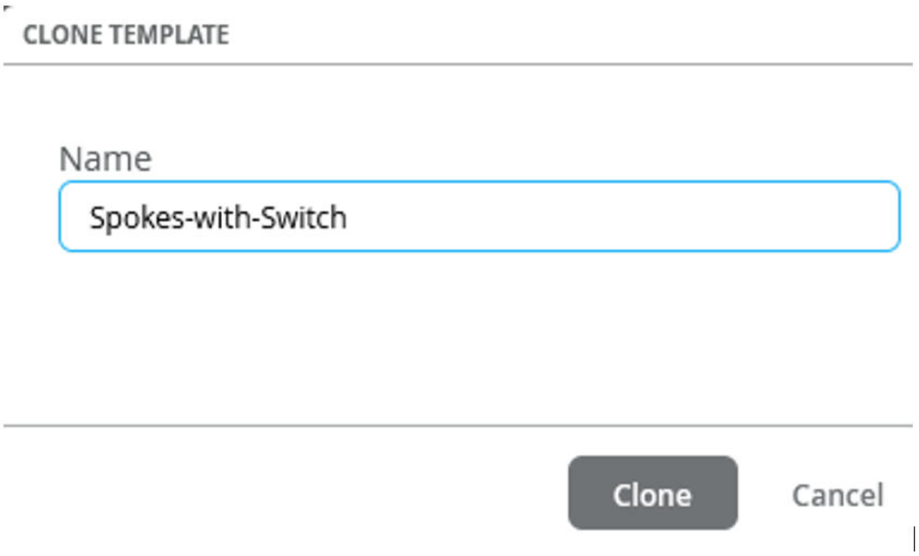
2. Click **More** and select **Clone**.

Figure 273: Selecting Clone Option for Template



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

Figure 274: Saving Cloned Template


CLONE TEMPLATE

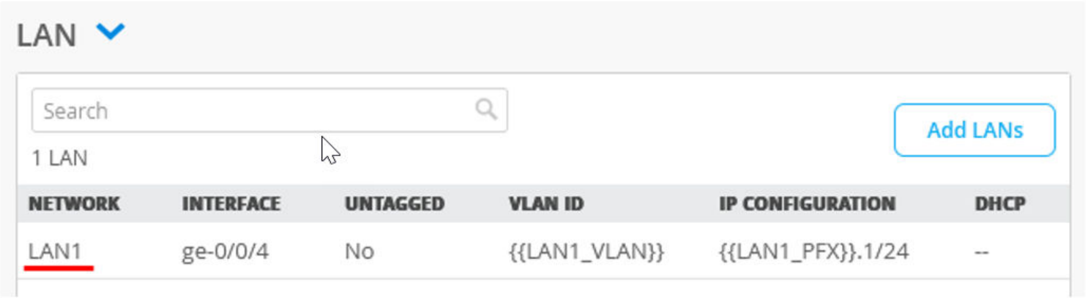
Name: Spokes-with-Switch

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

Edit the LAN Interface

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

Figure 275: LAN Interface Configuration on Template



LAN

Search

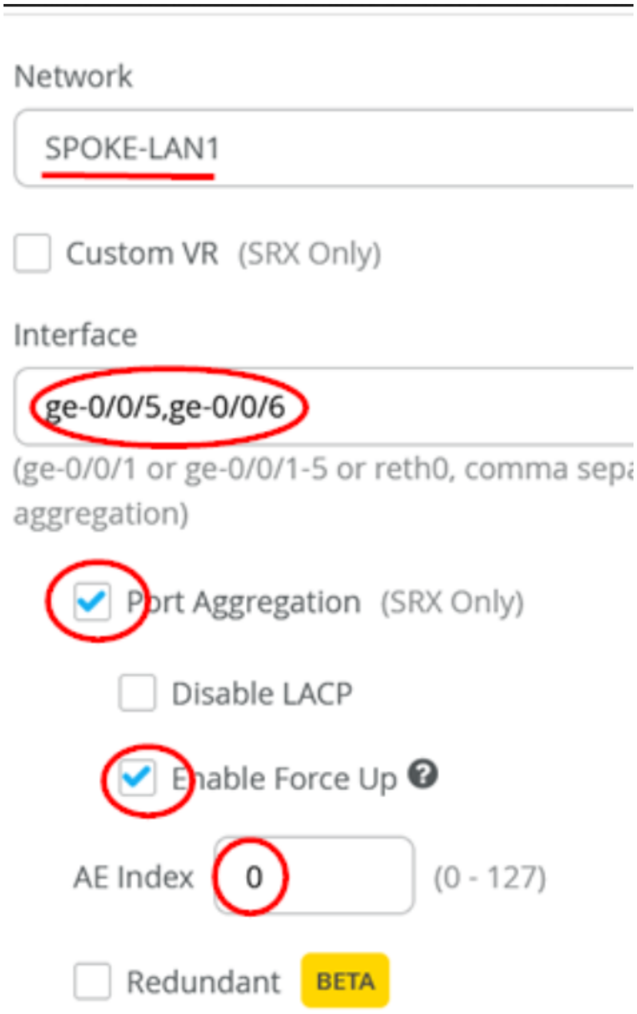
Add LANs

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:

Figure 276: 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 sep aggregation)

☑ Port Aggregation (SRX Only)

□ Disable LACP

☑ Enable Force Up

AE Index 0 (0 - 127)

□ Redundant BETA

- **Interface**—ge-0/0/5, ge-0/0/6.

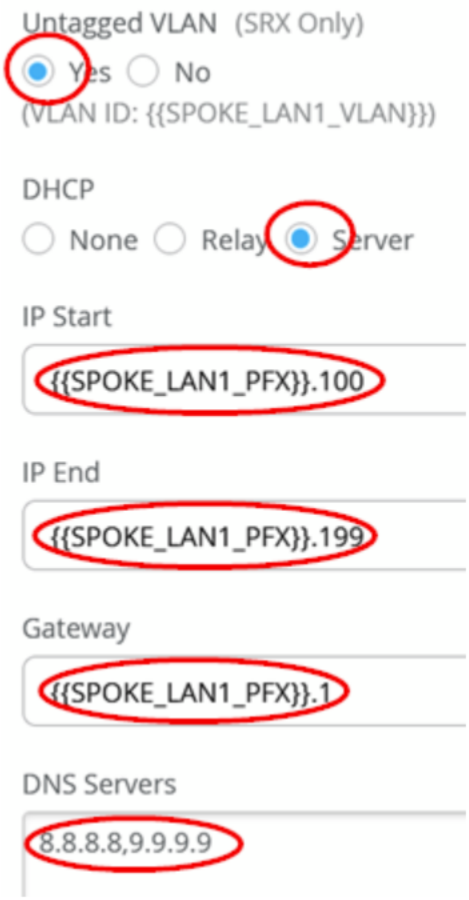
- **Port Aggregation**—Enable.

- **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).

2. Continue to configure the **SPOKE-LAN1** interface:

Figure 277: 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

- **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.

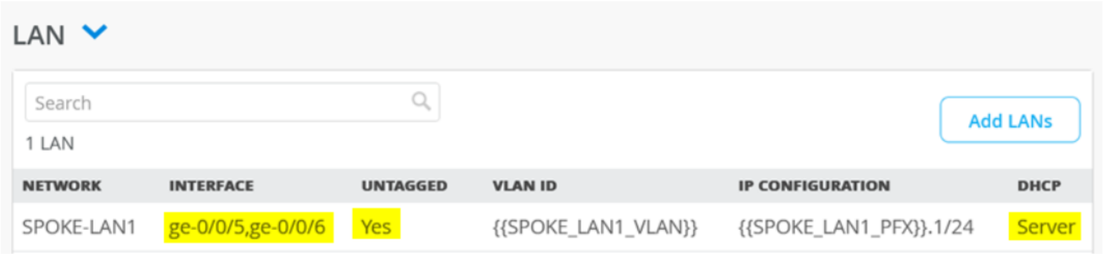
- **DHCP**—Server

- **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

3. Figure 278 on page 391shows the LAN interface you modified.

Figure 278: Summary of LAN Interface

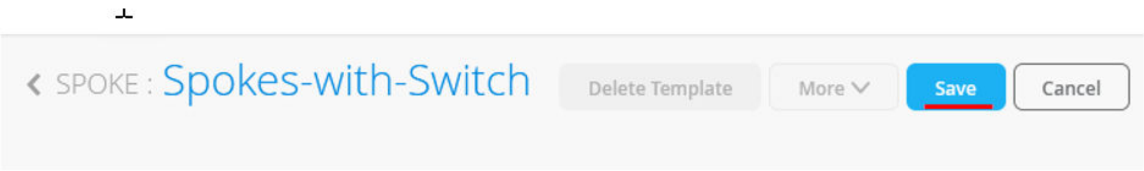


1 LAN

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

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

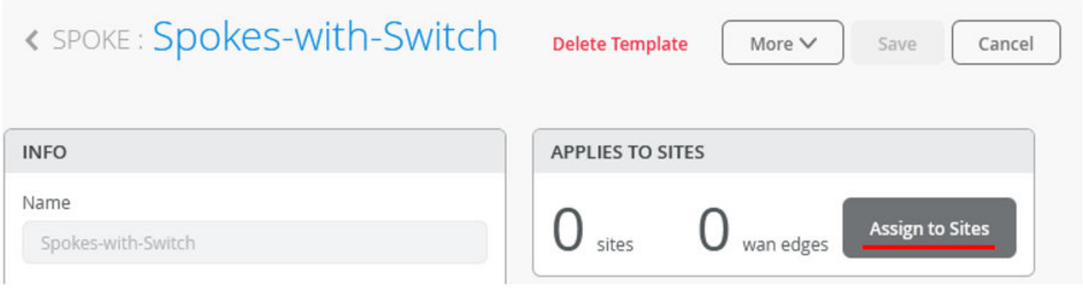
Figure 279: Saving WAN Edge Template



Assign the New Template to a Site

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

Figure 280: Assign Spoke Templates to Sites



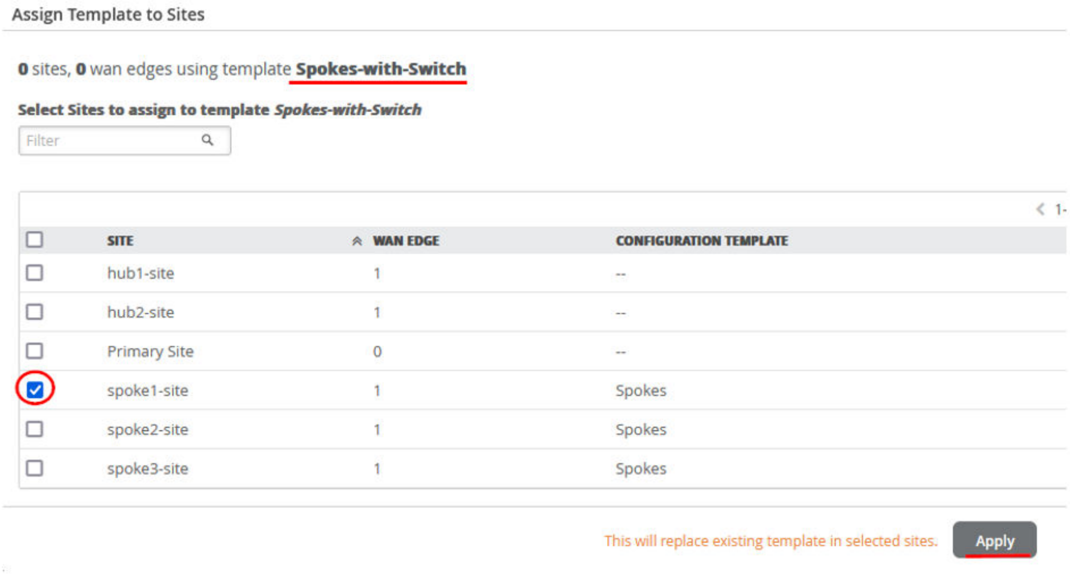
SPOKE : Spokes-with-Switch

Name: Spokes-with-Switch

0 sites 0 wan edges

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

Figure 281: Select Sites to Assign Spoke Templates



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

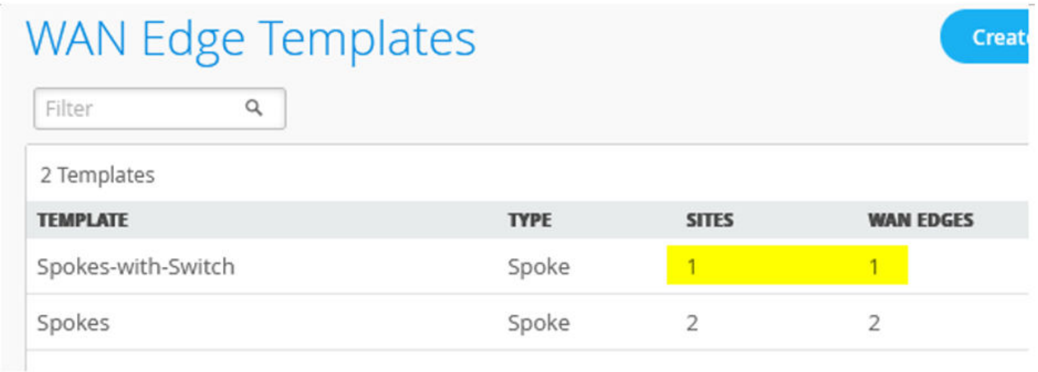
Select Sites to assign to template *Spokes-with-Switch*

□	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.

3. Review the template settings as shown in Figure 282 on page 393.

Figure 282: Details of WAN Edge Template



2 Templates

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

Add Your Switch to the Topology

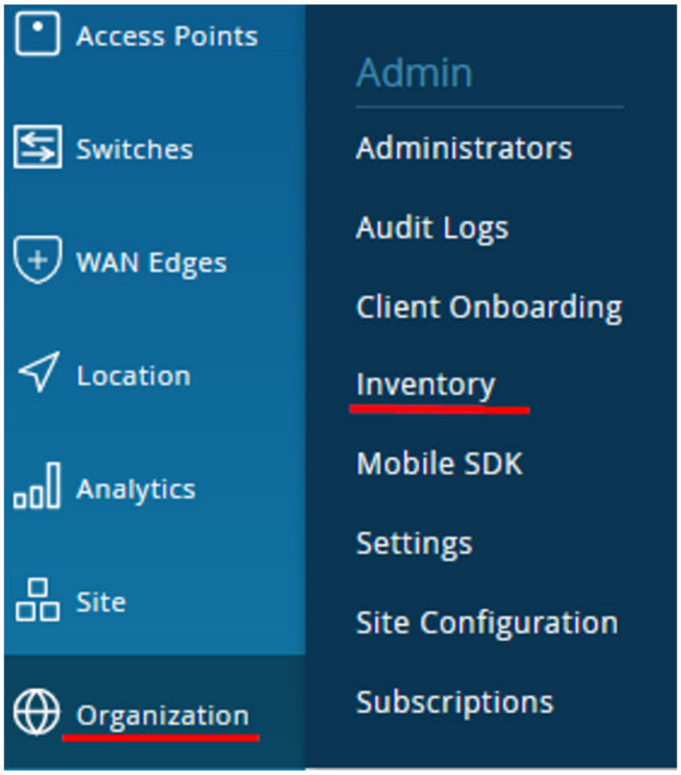
Now it is time to onboard your switch and add it to your infrastructure. For details on how to onboard your switch, refer to the product documentation for your switch in the Juniper TechLibrary.

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:

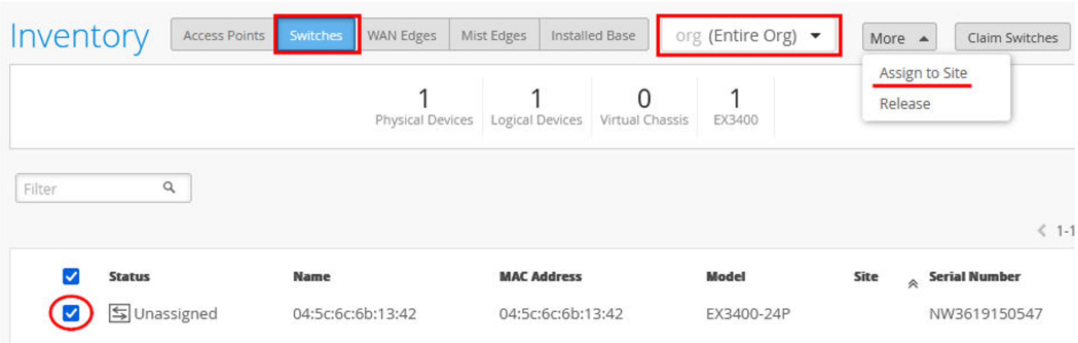
1. In the Juniper Mist portal, click **Organization** > **Admin** > **Inventory**.

Figure 283: Navigating to Inventory



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

Figure 284: EX Series Switch in Inventory



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

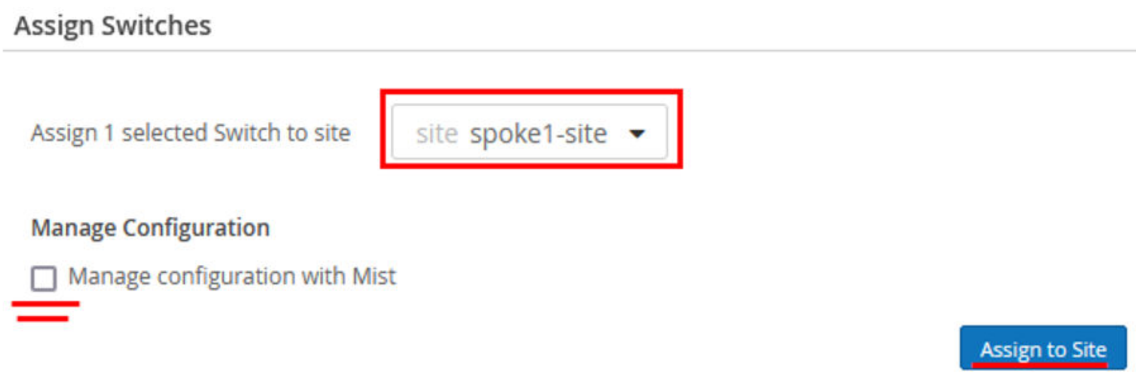
3. Select your new switch and click **Assign to Site**.

4. 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.

Figure 285: Selecting Site for Assigning Switch



Assign Switches

Assign 1 selected Switch to site: site spoke1-site

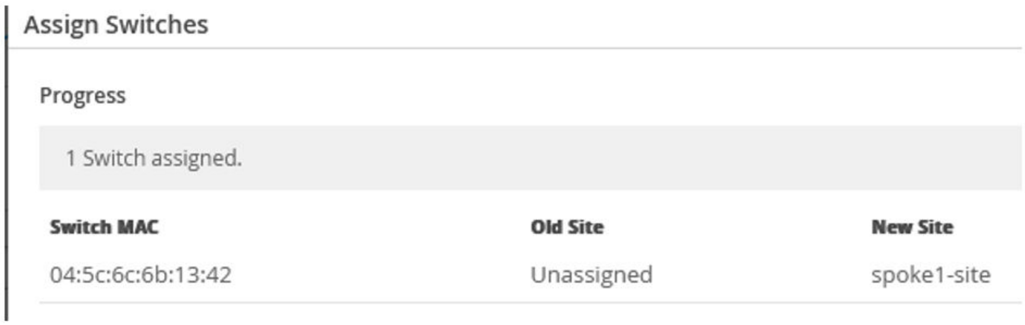
Manage Configuration

□ Manage configuration with Mist

5. Click **Assign to Site**.
6. Confirm the changes in the inventory once you assign the device to the site.

   You can see **spoke1-site** under **New Site**.

Figure 286: Assigned Switch to Site Details



Assign Switches

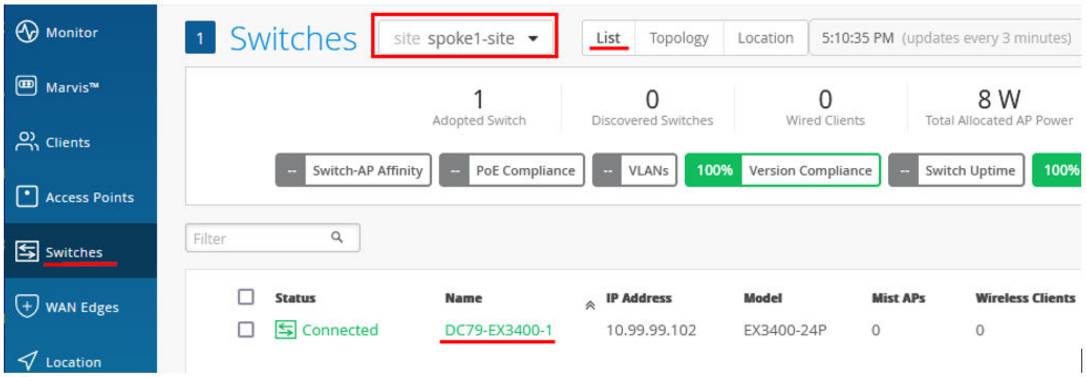
Progress

1 Switch assigned.

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

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

Figure 287: Selecting Assigned Switch for Modification



5:10:35 PM (updates every 3 minutes)

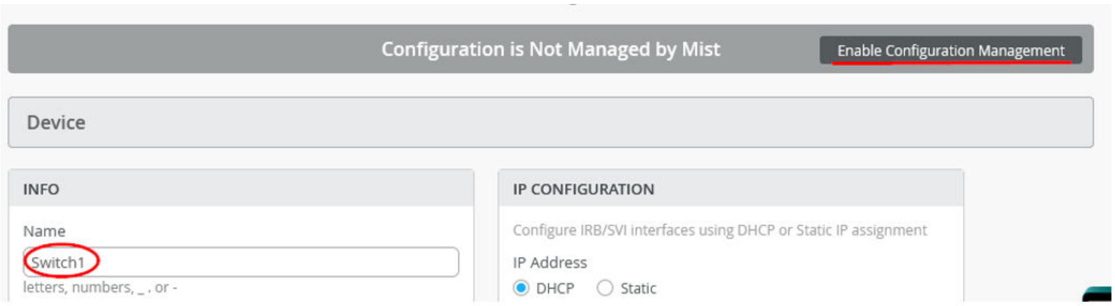
1 Adopted Switch | 0 Discovered Switches | 0 Wired Clients | 8 W Total Allocated AP Power

□	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.

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

Figure 288: Configuration of Assigned Switch



Configuration is Not Managed by Mist

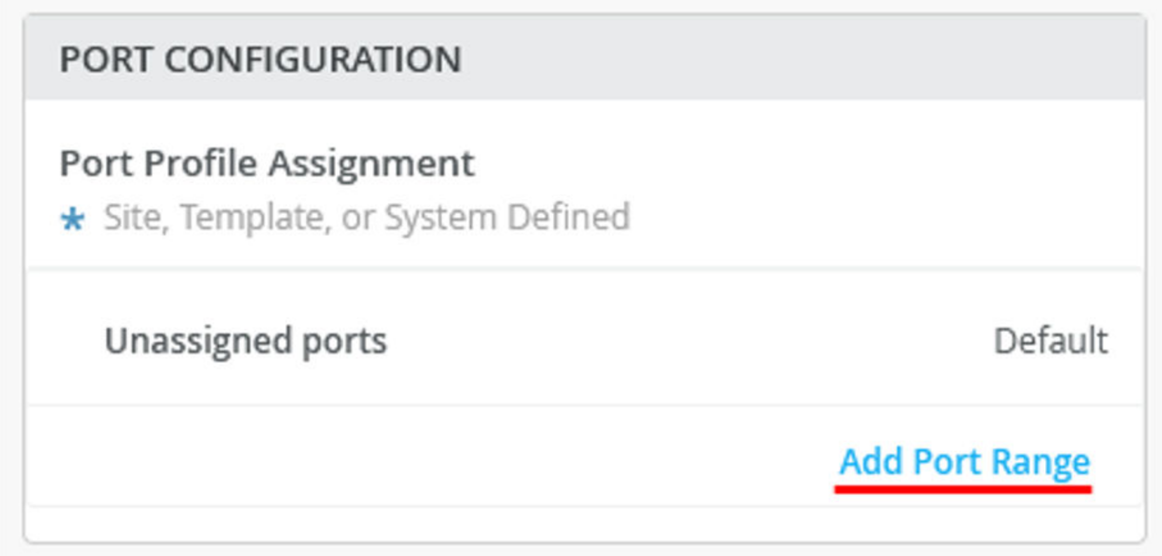
Name: Switch1
letters, numbers, _ . or -

Configure IRB/SVI interfaces using DHCP or Static IP assignment

IP Address: ● DHCP ○ Static

10. Under **Port Configuration**, click **Add Port Range**.

Figure 289: Port Configuration of Assigned Switch



PORT CONFIGURATION

Port Profile Assignment

* Site, Template, or System Defined

Unassigned ports Default

Add Port Range

11. In the **New Port Range** page, configure the following options:

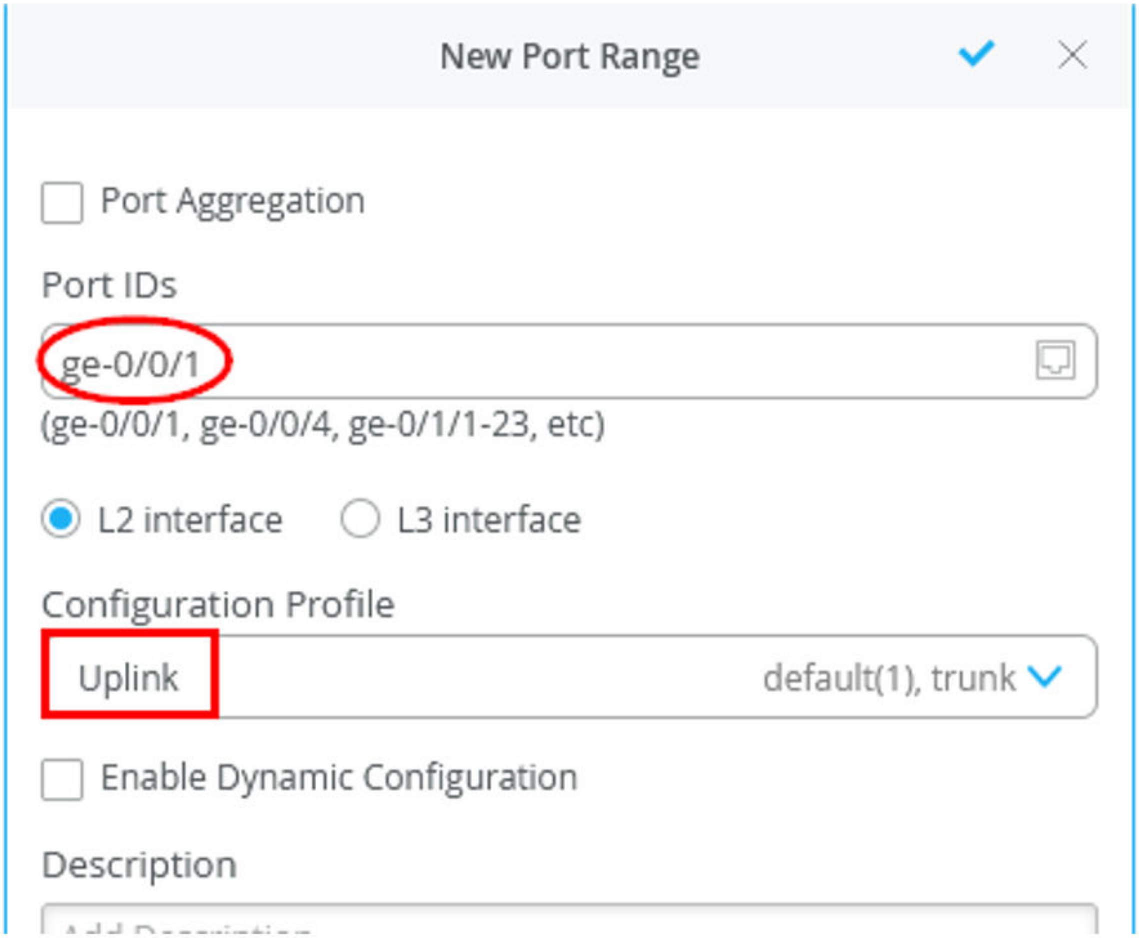
    - Enable **Port Aggregation**.

    - 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**.

Figure 290: 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

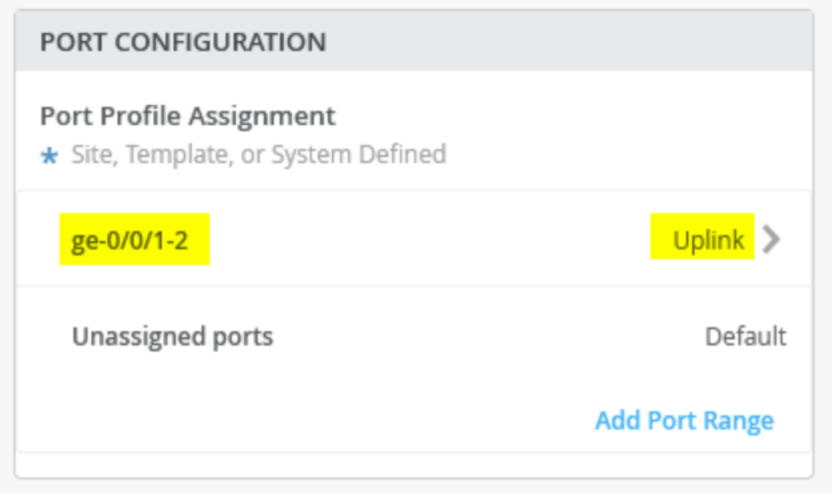
Uplink default(1), trunk

□ Enable Dynamic Configuration

Description

12. Figure 289 on page 397 shows the summary of port configuration.

Figure 291: Port Configuration of Assigned Switch



PORT CONFIGURATION

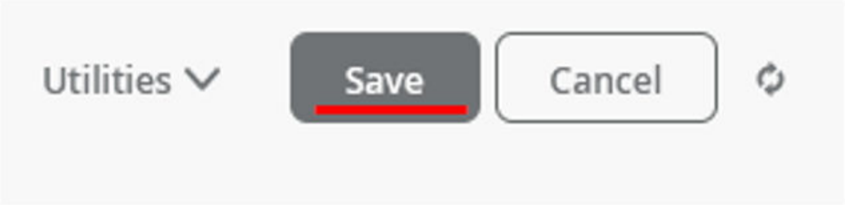
Port Profile Assignment

* Site, Template, or System Defined

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

13. Save your changes.

Figure 292: 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
```

SEE ALSO

High Availability Design for SRX Series Firewalls

IN THIS SECTION

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.

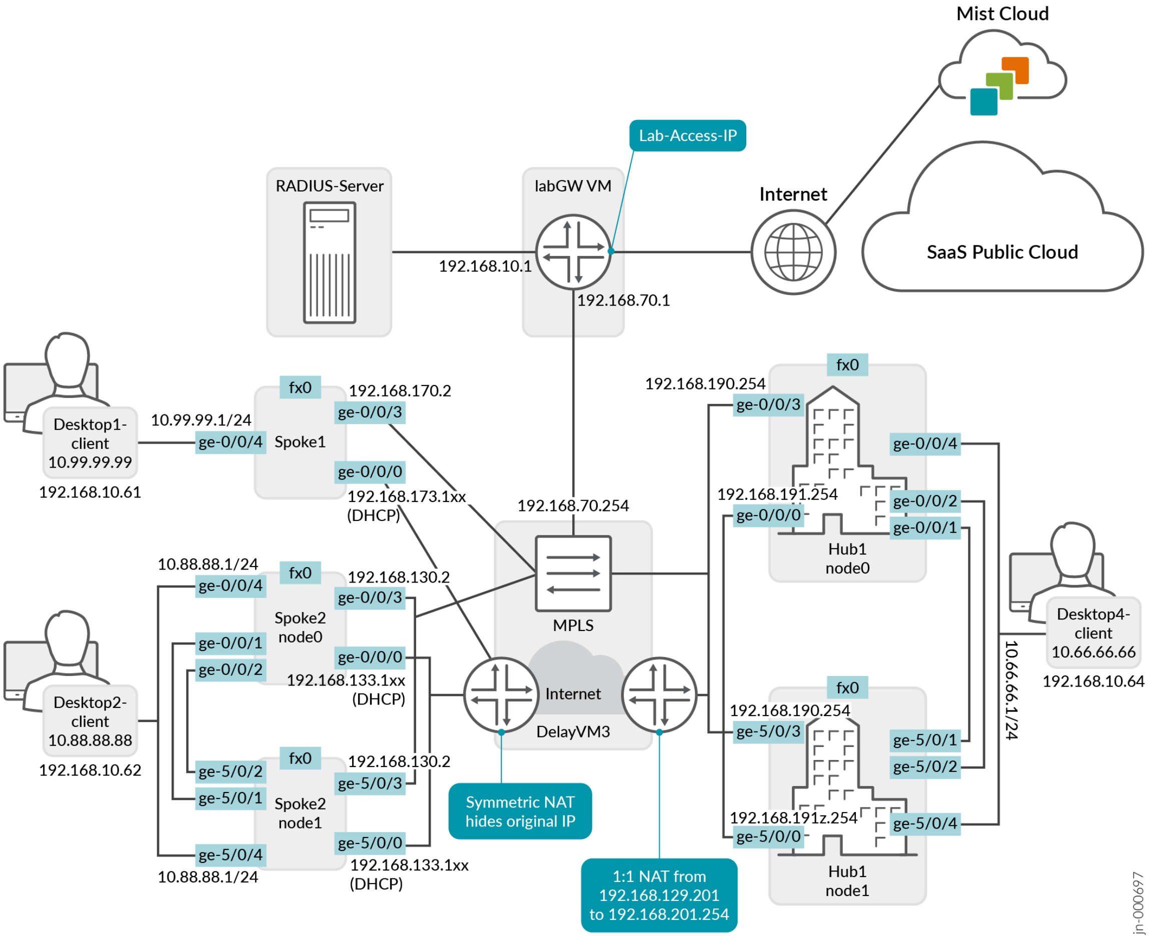
Juniper® SRX Series Firewall High Availability (HA) design example is for administrators who want to deploy HA Juniper SRX Series Firewall at the Edge, but not for Whitebox setups.

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 Figure 293 on page 401. Here we see the SRX Series highly available Juniper Mist WAN Assurance topology for this HA Design Guide.

Figure 293: Juniper Validated Design Mist WAN Assurance with HA SRX Series WAN Edges



NOTE: Before you get started, be sure you've setup the topology described in the Juniper WAN Assurance Configuration Guide.

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.

- 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 Chassis Cluster Fabric Interfaces.

- 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

Following samples show interfaces usage for the chassis cluster configuration.

NOTE: Only the WAN1, WAN0 and LAN1 are changeable in the List below if they do not conflict with others which are not changeable.

```
Primary Node0 Interface Table
Device MGMT
```

```
(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 chassis cluster and reboot both the nodes, the second node (node 1) renumbers its interfaces as shown in the following sample. You have to 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. See "WAN Assurance Configuration Overview" on page 31.

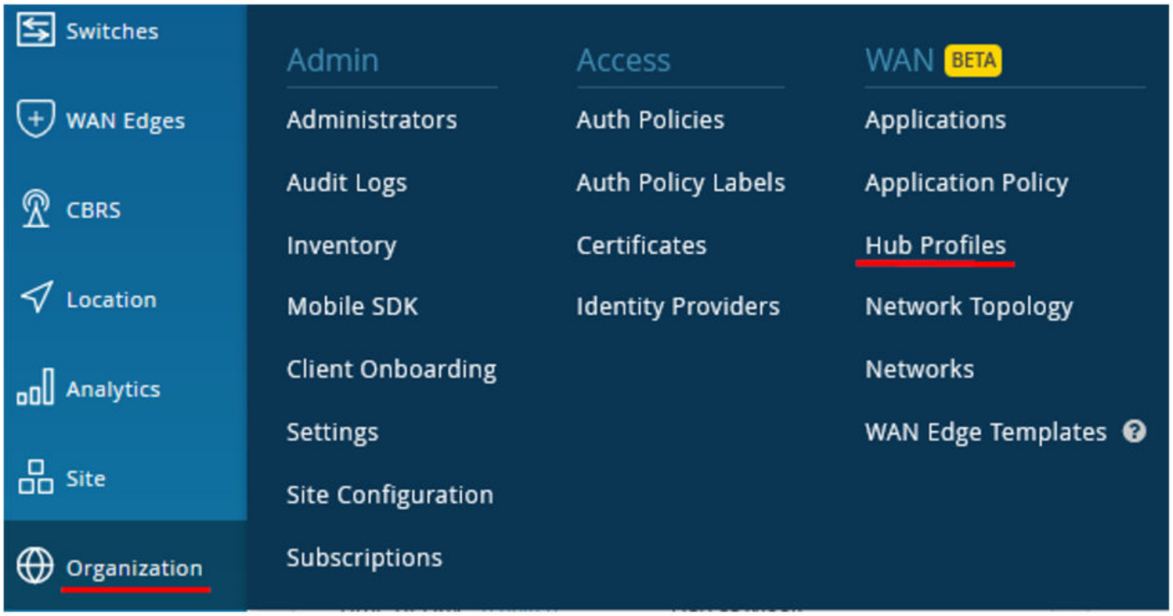
The following steps outline the process of creating high availability cluster.

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.

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

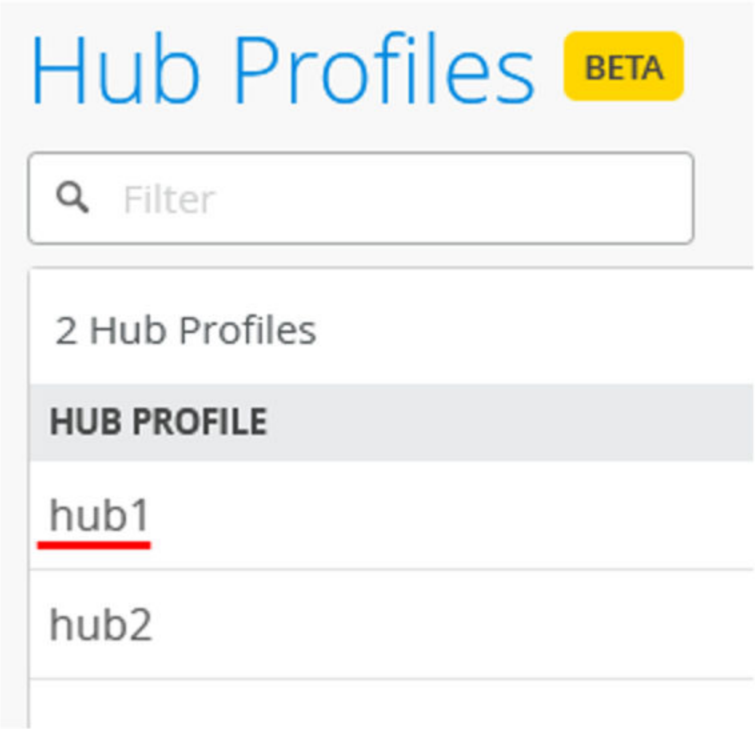
Figure 294: Configure Hub Profiles



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

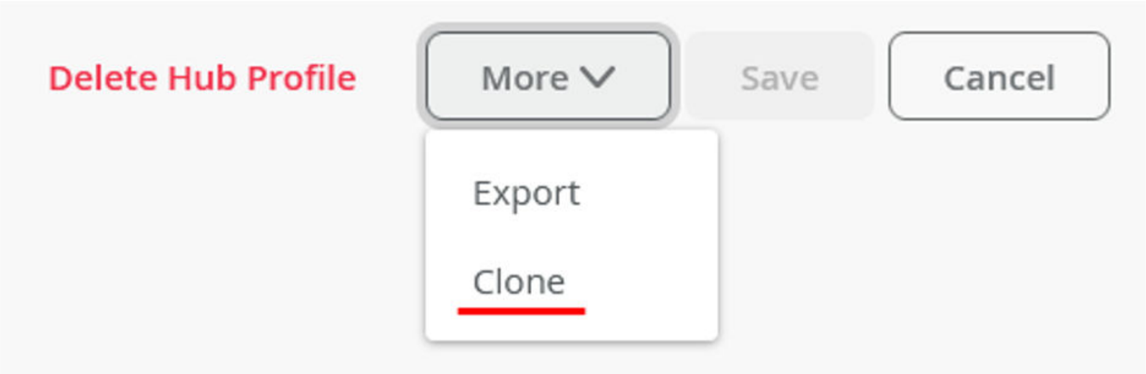
2. Click the hub profile (hub1) that you want to clone.

Figure 295: Select Hub Profile for Cloning



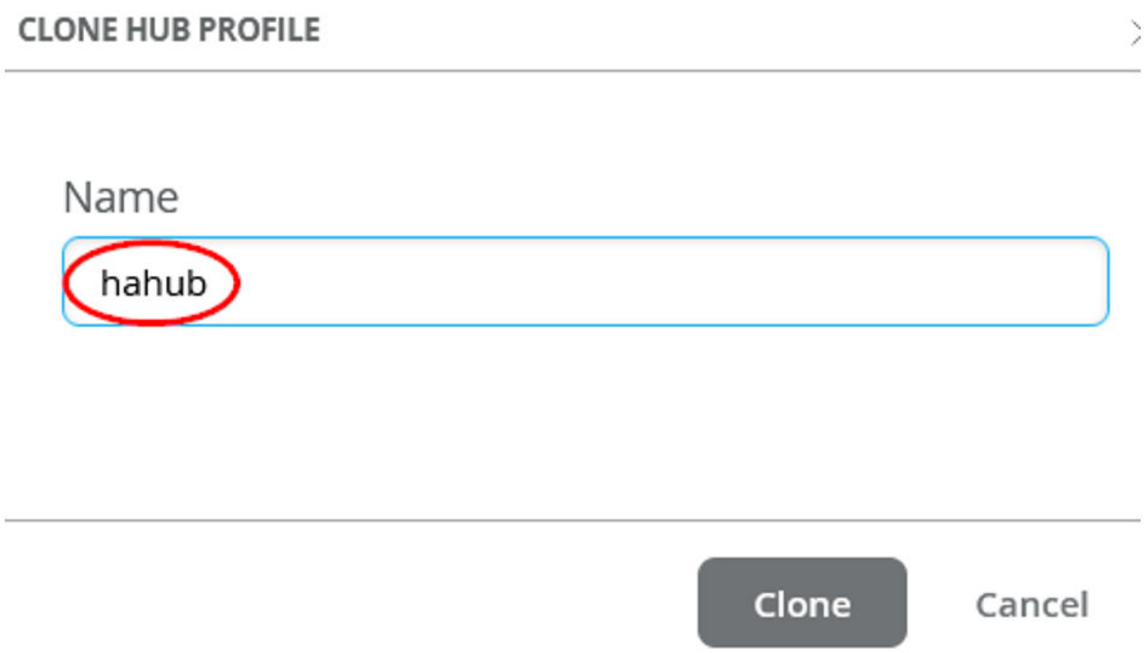
3. In the upper right corner of the screen, click **More** and select **Clone**.

Figure 296: Selecting Clone Option



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

Figure 297: Rename Cloned Hub Profile


CLONE HUB PROFILE

Name

hahub

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

5. 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 Table 50 on page 407.

Table 50: WAN Interfaces Details in Hub Profile

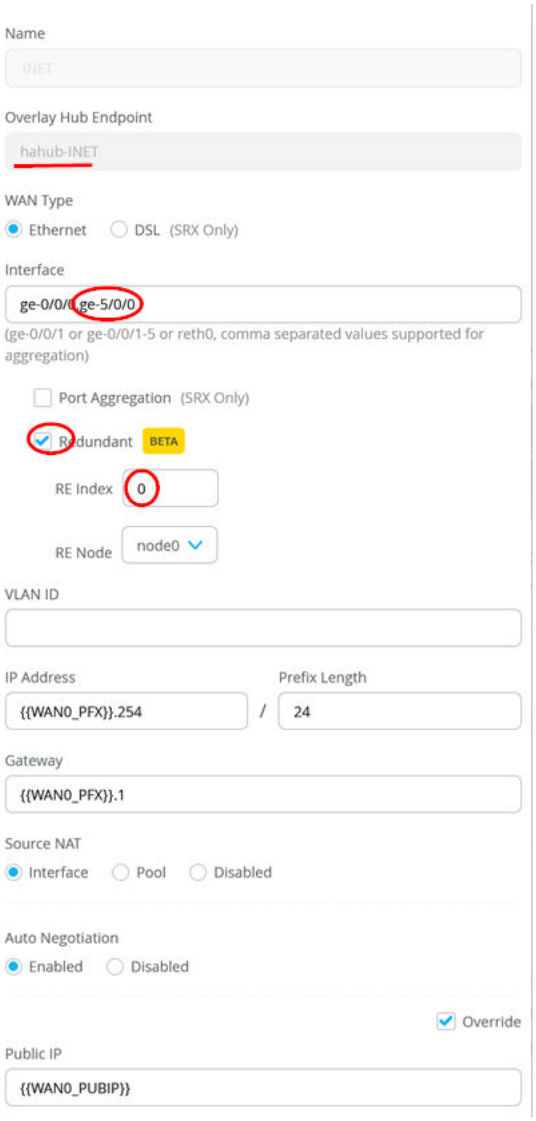
Option	First WAN	Second WAN
Name: (This indicates which topology it uses.)	INET	MPLS
Interface	ge-0/0/0, ge-5/0/0	ge-0/0/3,ge-5/0/3
Redundant	Enabled	Enabled
RE Index (as a convention, use the last octet as index)	0	0

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.

> **NOTE**: IP Address, prefix, gateway and public IP address remain same.
>
> The portal generates the overlay hub endpoints as **hahub-INET** and **hahub-MPLS** automatically.

Figure 298 on page 408 shows WAN interface configuration.

Figure 298: 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

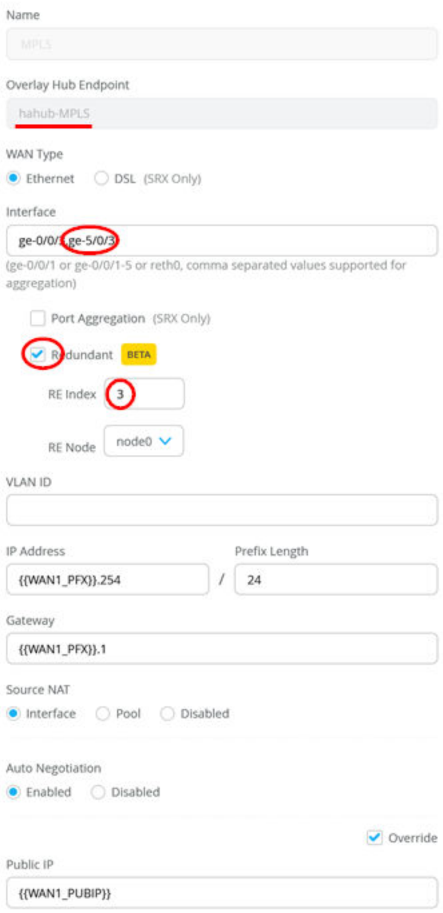
● Enabled ○ Disabled

☑ Override

Public IP

{{WAN0_PUBIP}}

Figure 299: 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 {{WAN1_PFX}}.254 / Prefix Length 24

Gateway

{{WAN1_PFX}}.1

Source NAT

● Interface ○ Pool ○ Disabled

Auto Negotiation

● Enabled ○ Disabled

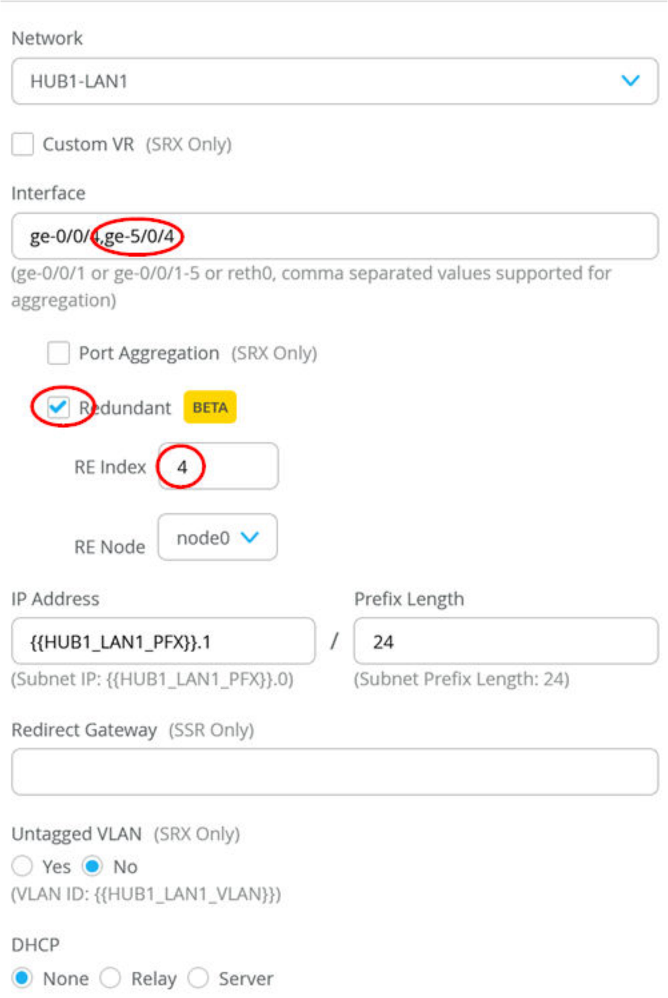
☑ Override

Public IP

{{WAN1_PUBIP}}

6. Complete the configuration for the LAN interface.

Figure 300: 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

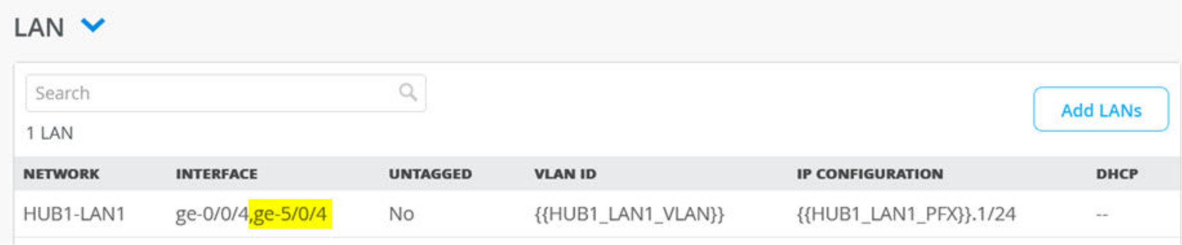
● None ○ Relay ○ Server

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.

Figure 301: LAN Interface Configuration

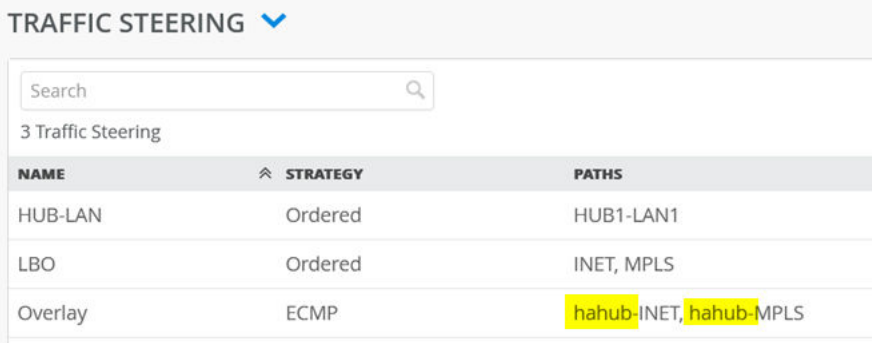


1 LAN

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	--

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

Figure 302: Traffic Steering Rules

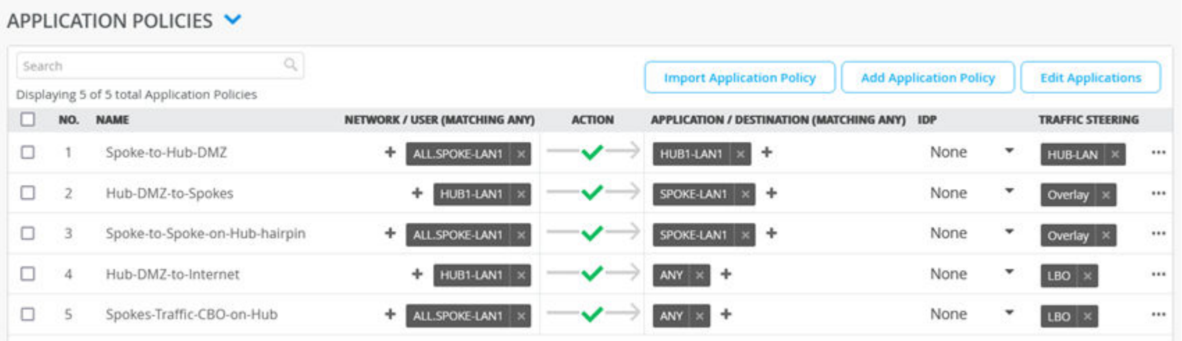


3 Traffic Steering

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

8. Retain the application policies rules.

Figure 303: Application Policies Rules



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

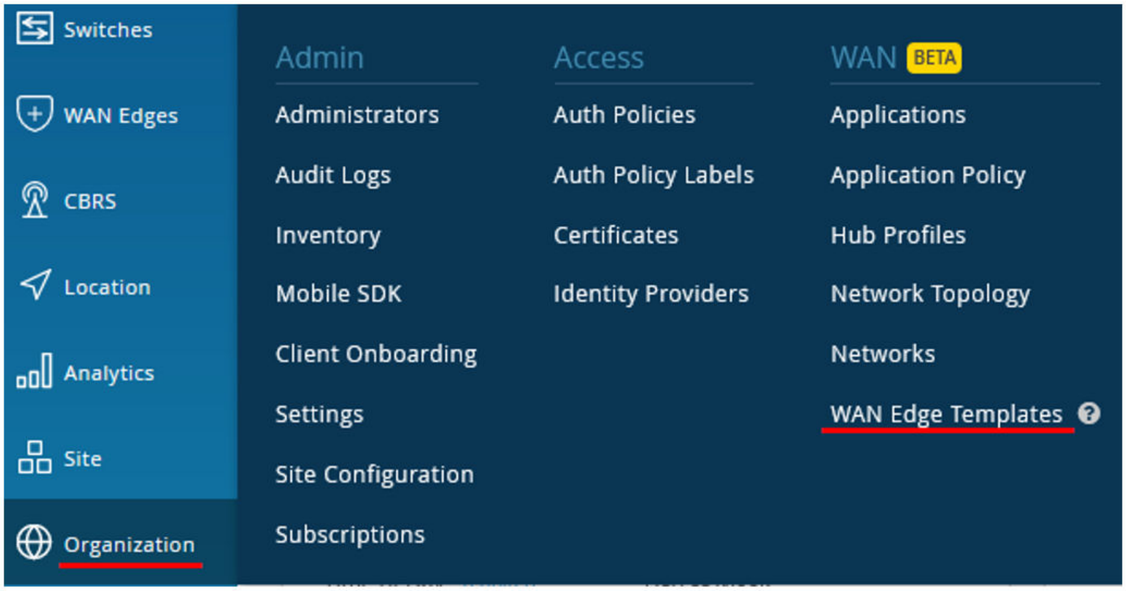
SUMMARY

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".

1. 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.

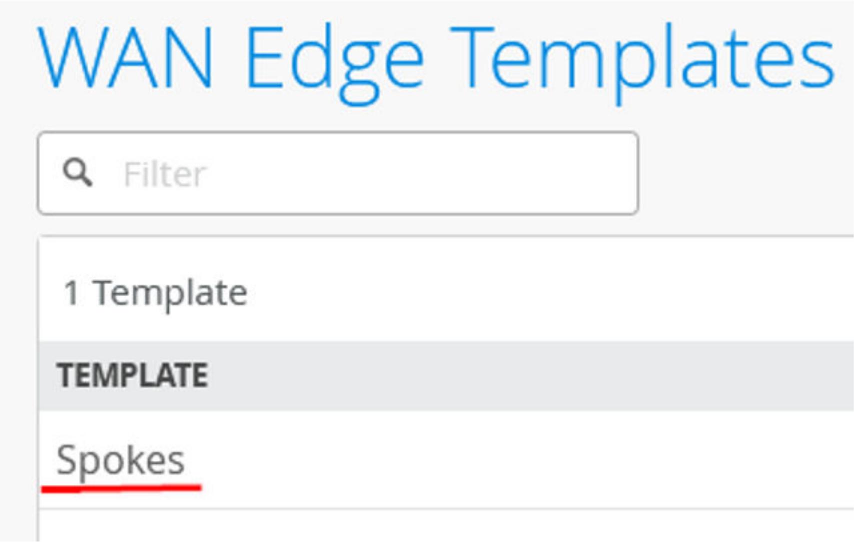
   In the Juniper Mist™ portal, click Organization > WAN > WAN Edge Templates. A list of existing templates, if any, appears.

   Figure 304: Accessing WAN Edge Templates

2. Create the new **SpokeTemplate** by cloning the existing template and modifying the clone. Simply select the existing profile Spokes and select **Clone**.

Figure 305: WAN Edge Templates



WAN Edge Templates

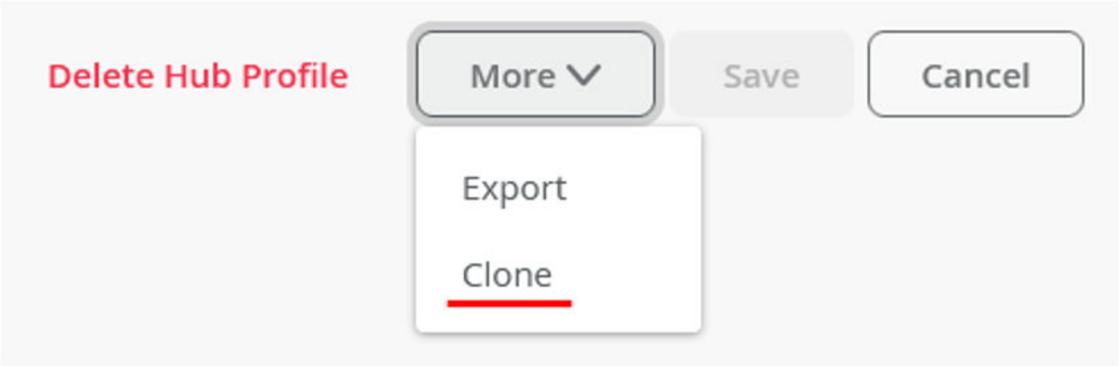
Filter

1 Template

TEMPLATE
Spokes

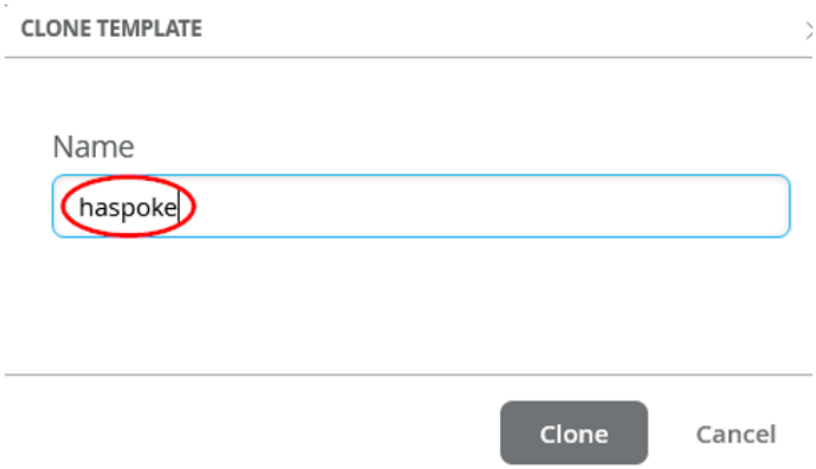
3. In the upper right corner of the screen, click More and select Clone.

Figure 306: Cloning Existing WAN Edge Template



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

Figure 307: Renaming Cloned Template



CLONE TEMPLATE

Name

haspoke

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

5. 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 Table 50 on page 407.

Table 51: WAN Interfaces Details in Hub Profile

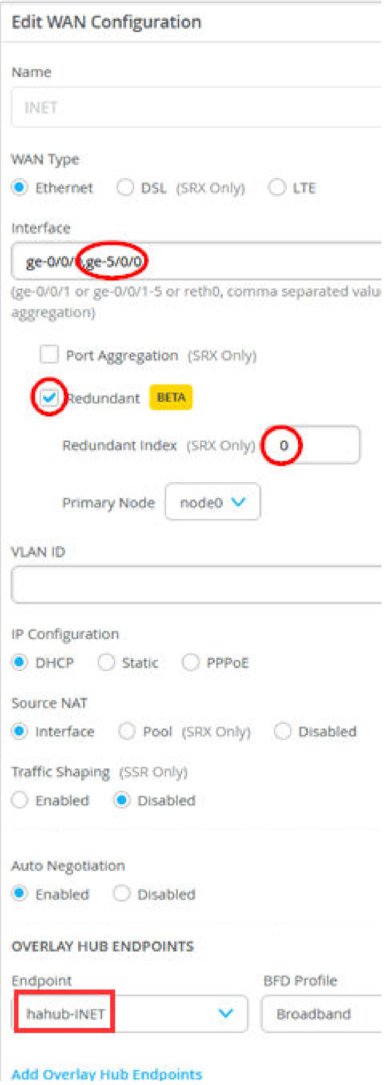
Option	First WAN	Second WAN
Name: (This indicates which topology it uses.)	INET	MPLS
Interface	ge-0/0/0, ge-5/0/0	ge-0/0/3,ge-5/0/3
Redundant	Enabled	Enabled
RE Index (as a convention, use the last octet as index)	0	0
Overlay Hub Endpoints	**hahub-INET**	**hahub-MPLS**

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.

Figure 298 on page 408 shows WAN interface configuration.

Figure 308: 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

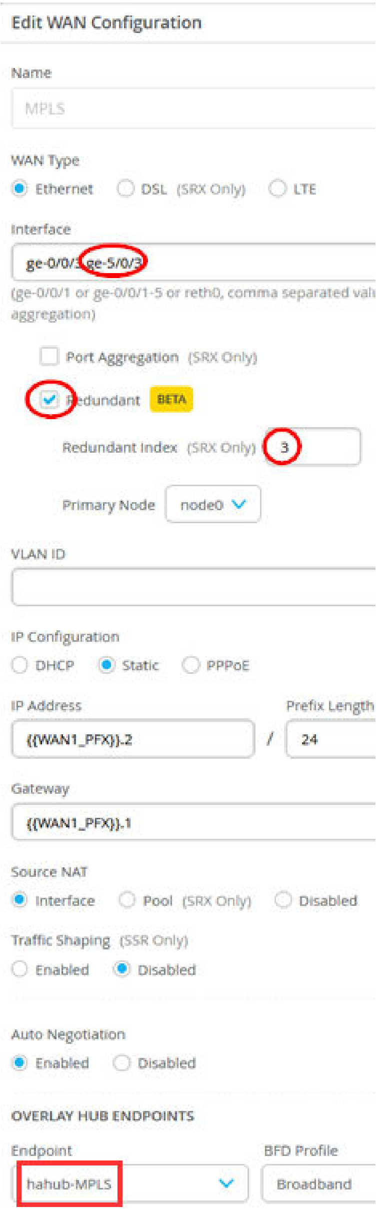
● Enabled ○ Disabled

OVERLAY HUB ENDPOINTS

Endpoint	BFD Profile
hahub-INET	Broadband

Add Overlay Hub Endpoints

Figure 309: 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		Prefix Length
{{WAN1_PFX}}.2	/	24

Gateway

{{WAN1_PFX}}.1

Source NAT

● Interface ○ Pool (SRX Only) ○ Disabled

Traffic Shaping (SSR Only)

○ Enabled ● Disabled

Auto Negotiation

● Enabled ○ Disabled

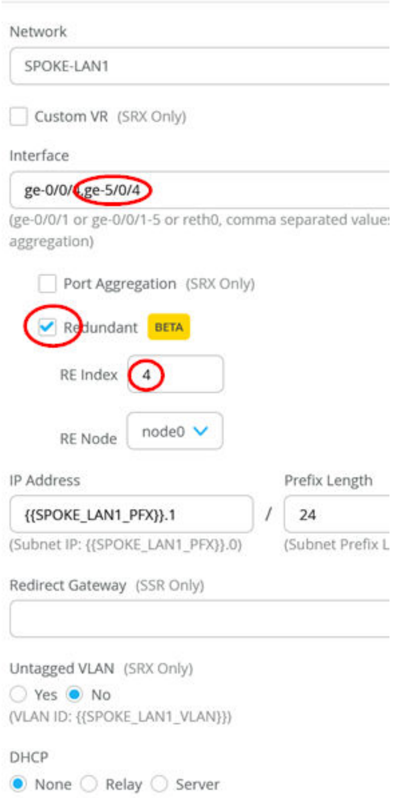
OVERLAY HUB ENDPOINTS

Endpoint	BFD Profile
hahub-MPLS	Broadband

6. 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.

Figure 310: 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 value
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

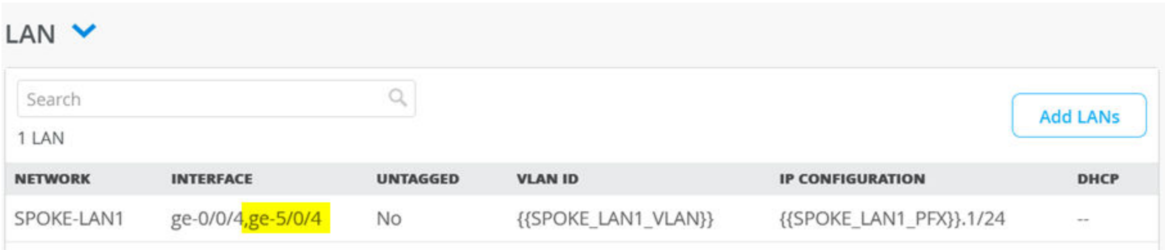
(VLAN ID: {{SPOKE_LAN1_VLAN}})

DHCP

● None ○ Relay ○ Server

shows LAN interface configuration.

Figure 311: LAN Interface Configuration

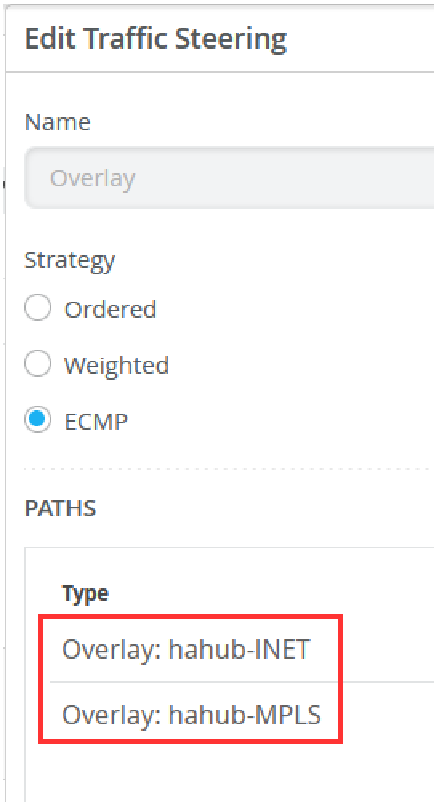


1 LAN

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	--

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

Figure 312: Traffic Steering Profile



Edit Traffic Steering

Name

Overlay

Strategy

○ Ordered

○ Weighted

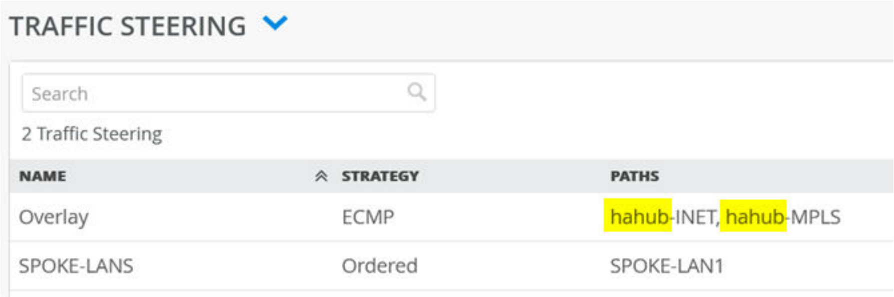
● ECMP

PATHS

Type
Overlay: hahub-INET
Overlay: hahub-MPLS

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

Figure 313: Modified Traffic Steering Rules

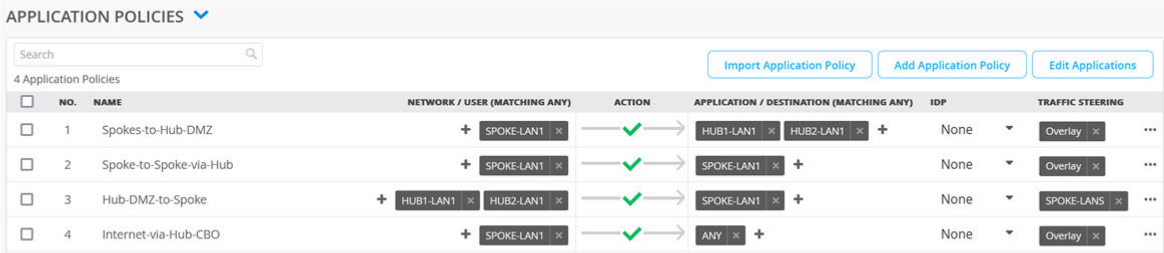


TRAFFIC STEERING

2 Traffic Steering

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

8. Retain the application policies without making any changes.



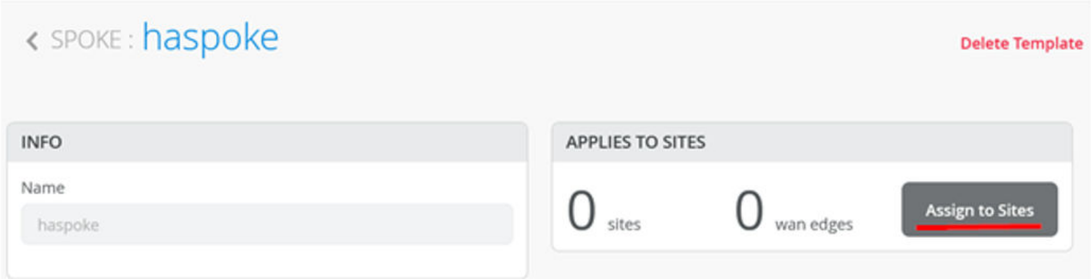
APPLICATION POLICIES

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 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

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

Figure 314: Assign Spoke Template to Sites



SPOKE : haspoke

INFO

Name: haspoke

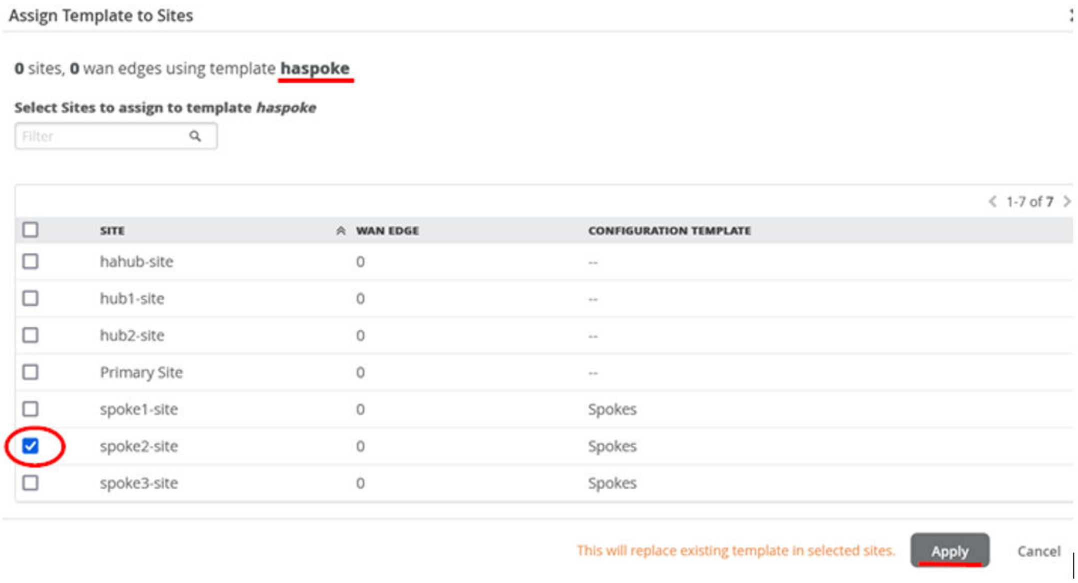
APPLIES TO SITES

0 sites

0 wan edges

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

Figure 315: Selecting Site for Assigning Spoke Template



Assign Template to Sites

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

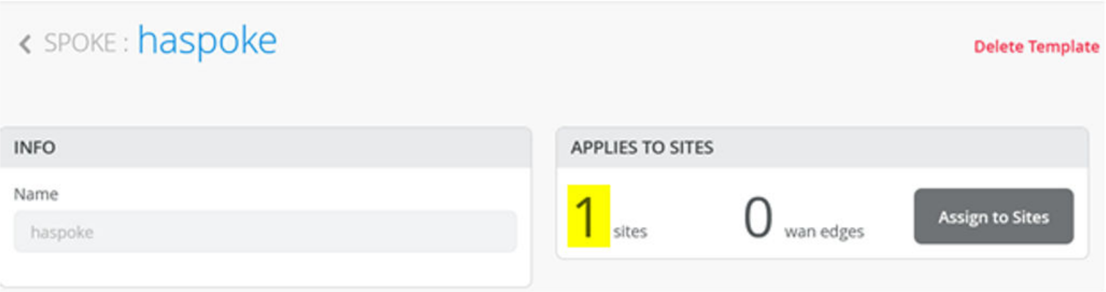
Select Sites to assign to template *haspoke*

☐	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.

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

Figure 316: Spoke Templates Applied to Sites



SPOKE : haspoke

INFO

Name: haspoke

APPLIES TO SITES

1 sites 0 wan edges

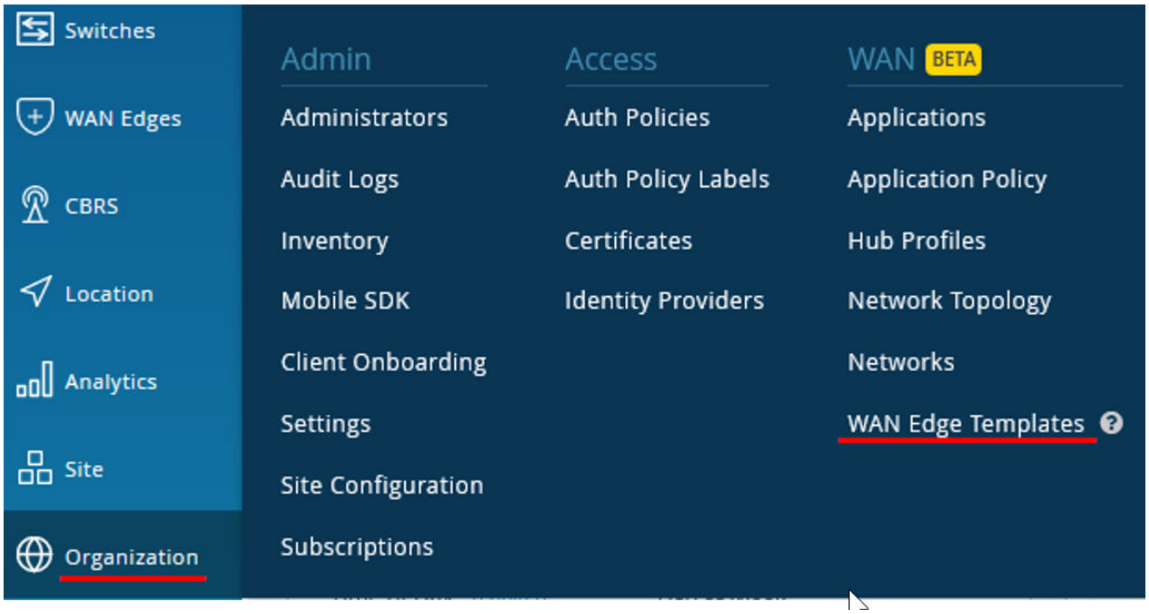
Create the Second Spoke Template

SUMMARY

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

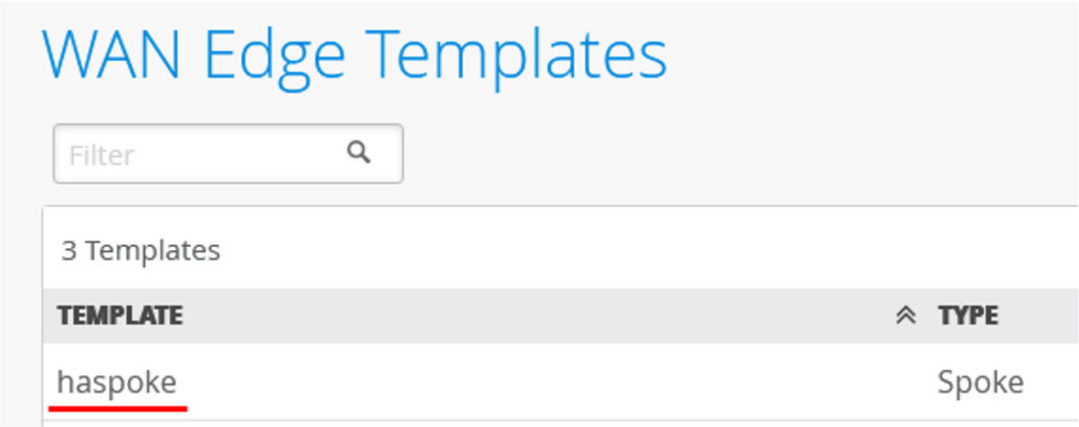
1. In the Juniper Mist cloud portal, click **Organization** > **WAN** > **WAN Edge Templates**. A list of existing templates, if any, appears.

Figure 317: WAN Edge Template



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

Figure 318: Select WAN Edge Template for Cloning

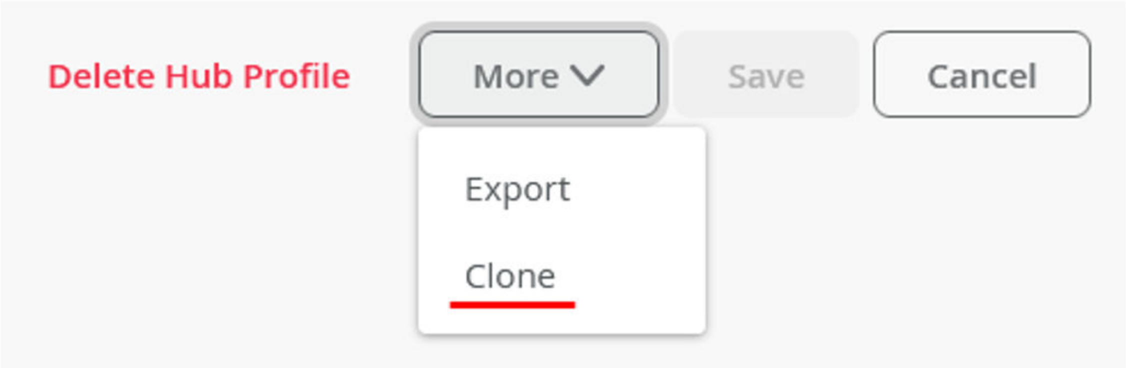


3 Templates

TEMPLATE	TYPE
haspoke	Spoke

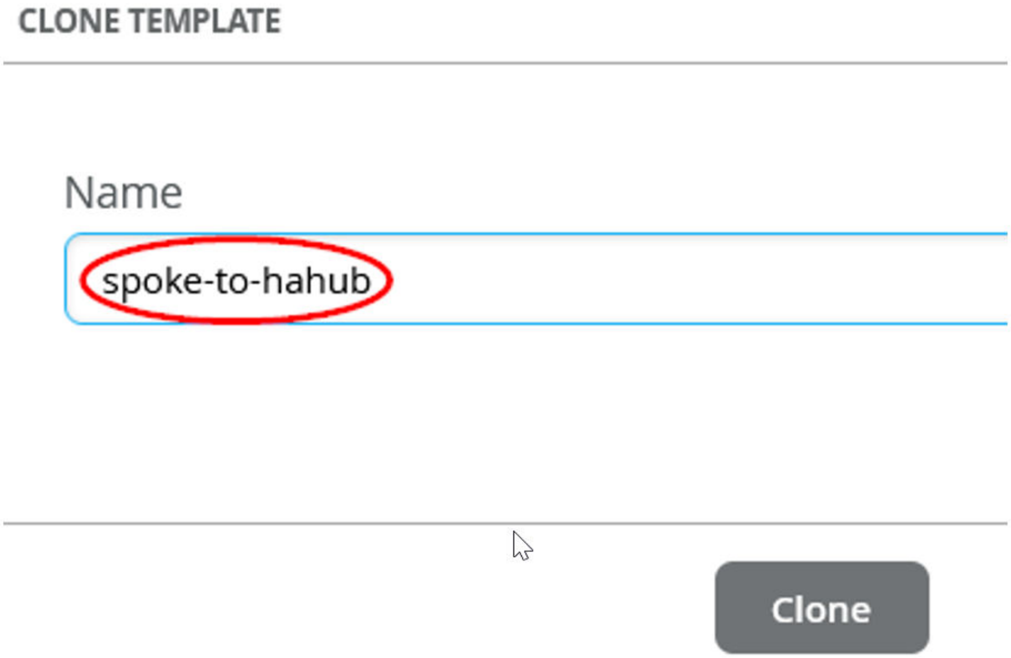
3. In the upper right corner of the screen, click **More** and select **Clone**.

Figure 319: Cloning WAN Edge Template



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

Figure 320: 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.

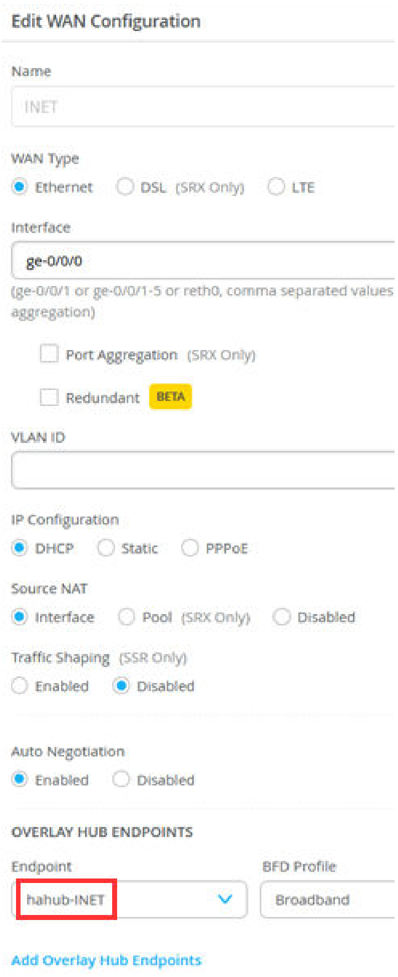
5. Modify the interfaces for the template.

   Change the **Overlay Hub EndPoints** as following:

   - For the interface INET—**hahub-INET**

- For the interface MPLS—**hahub-MPLS**

Figure 321: 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

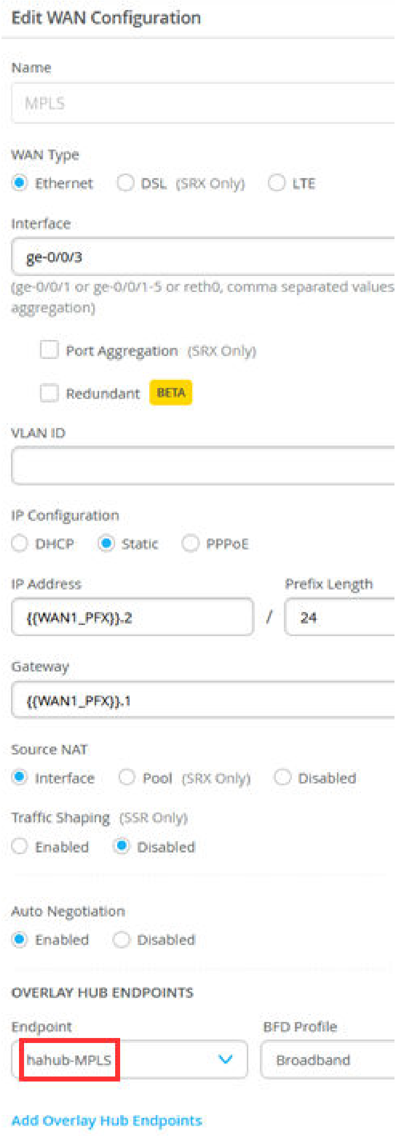
● Enabled ○ Disabled

OVERLAY HUB ENDPOINTS

Endpoint	BFD Profile
hahub-INET	Broadband

Add Overlay Hub Endpoints

Figure 322: 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

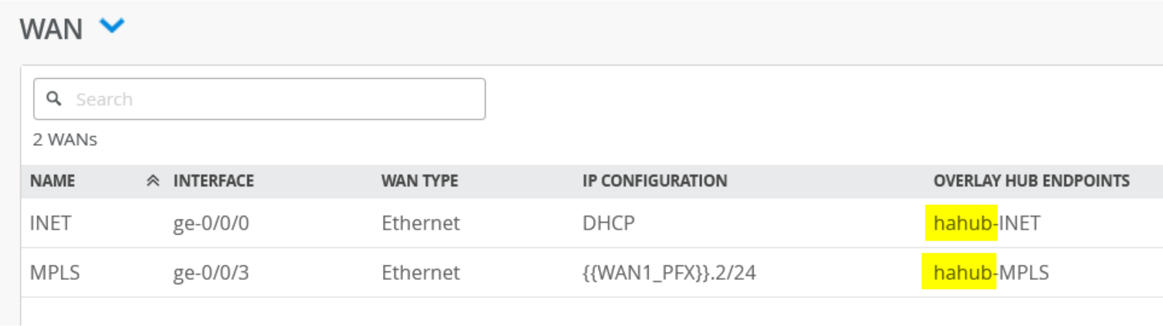
Endpoint: hahub-MPLS

BFD Profile: Broadband

Add Overlay Hub Endpoints

shows configured WAN interfaces.

Figure 323: WAN Interfaces Configuration

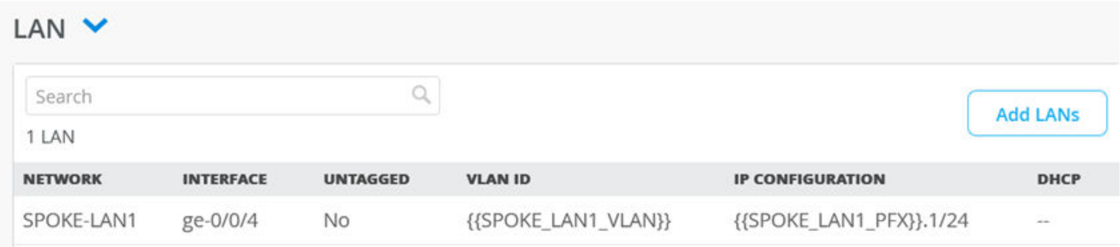


2 WANs

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

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

Figure 324: LAN Interfaces

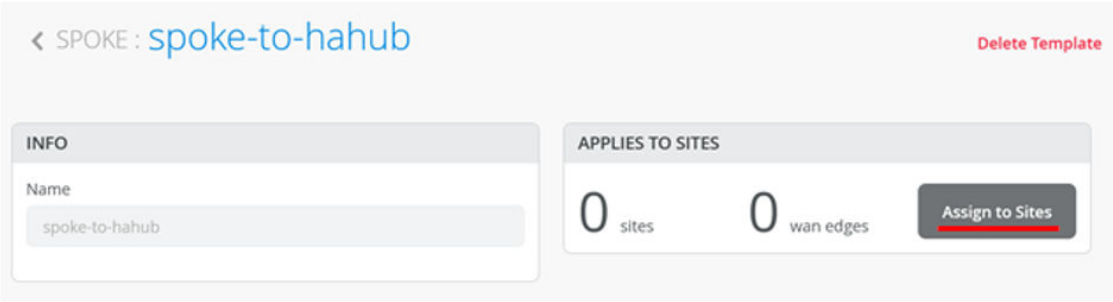


1 LAN

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

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

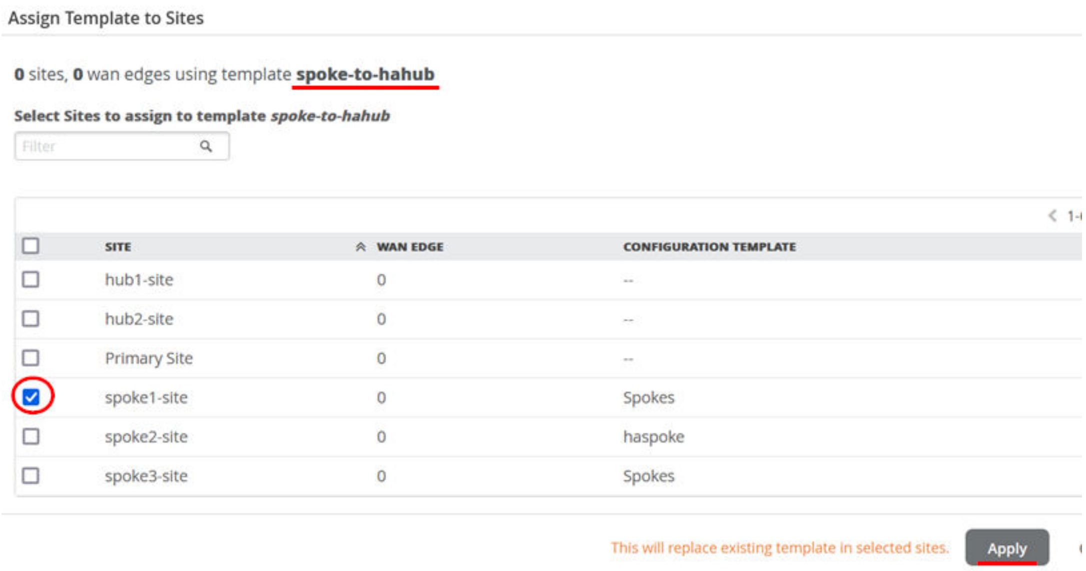
Figure 325: Assign Template to Site



Name: spoke-to-hahub

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

Figure 326: 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

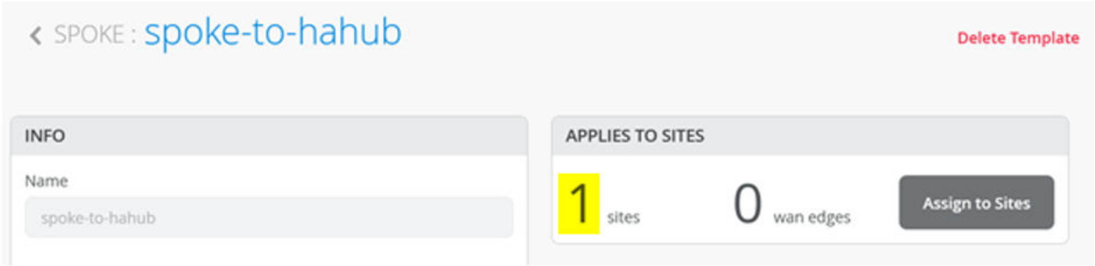
□	SITE	WAN EDGE	CONFIGURATION TEMPLATE
□	hub1-site	0	--
□	hub2-site	0	--
□	Primary Site	0	--
☑	spoke1-site	0	Spokes
□	spoke2-site	0	haspoke
□	spoke3-site	0	Spokes

This will replace existing template in selected sites.

11. Click **Apply**.

12. Ensure that your template is now assigned to a site. Check that your **Template** now has at least 1 **Site** assigned as shown in the following illustration:

Figure 327: Spoke Templates Applied to Sites



SPOKE : spoke-to-hahub

INFO

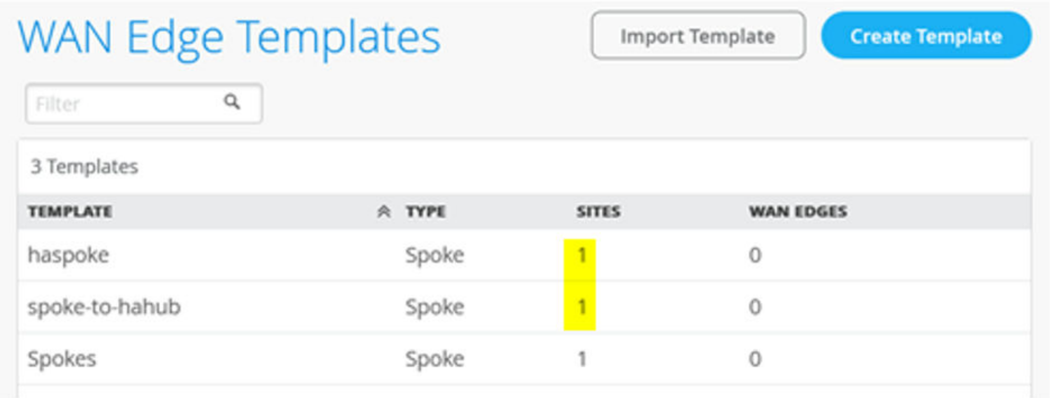
Name: spoke-to-hahub

APPLIES TO SITES

1 sites 0 wan edges

The following image shows the list of configured spoke templates:

Figure 328: List of WAN Edge Templates



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

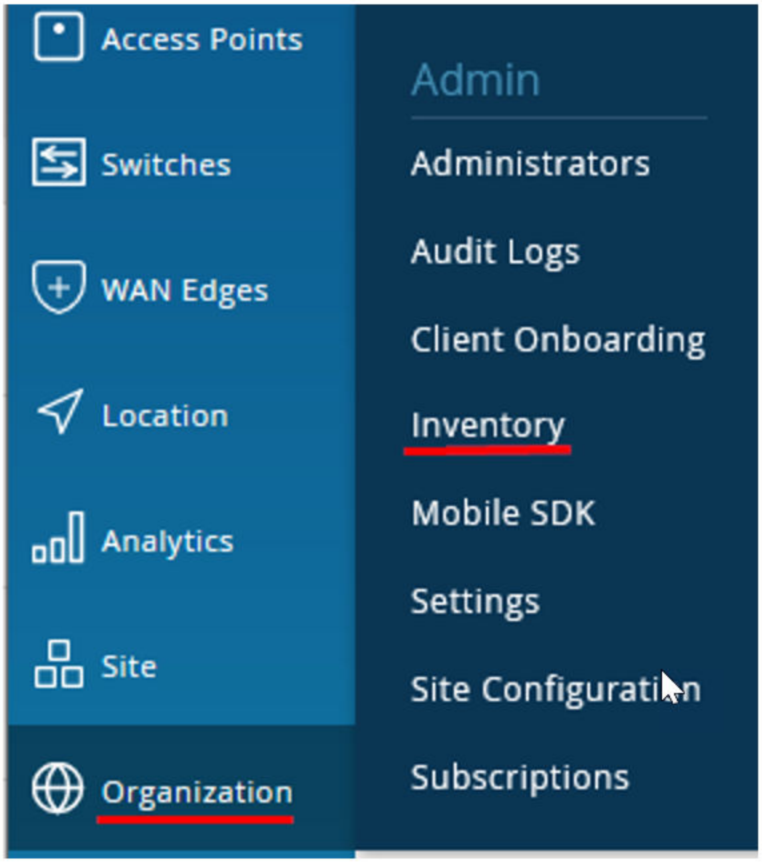
Onboard your Devices

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 Cloud-Ready SRX Firewalls.

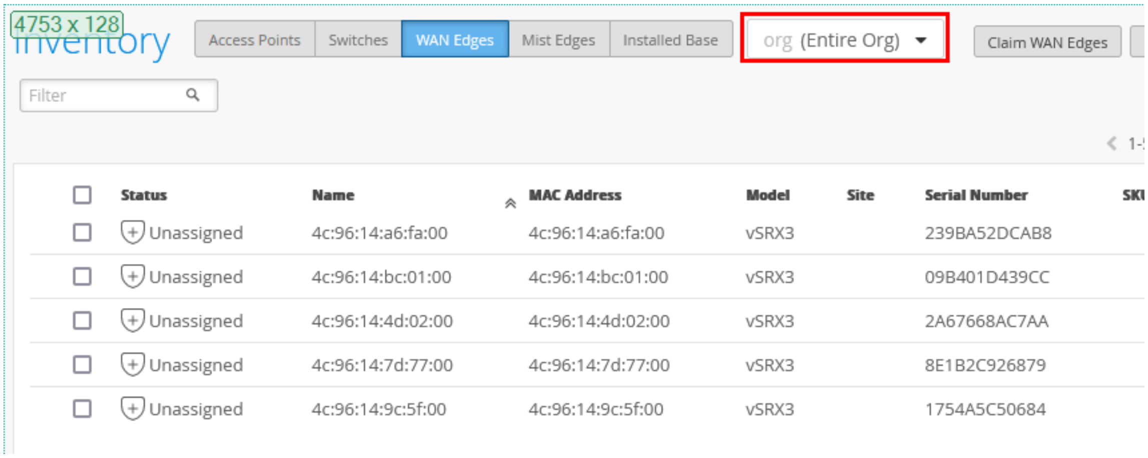
1. In the Juniper Mist portal. click **Organization** > **Admin** >**Inventory**.

Figure 329: Navigating to Inventory



2. Refresh your browser and check under WAN Edges to find out if your SRX Series Firewall is part of the inventory. Ensure you set the view as **org (Entire Org)** as shown in Figure 330 on page 428.

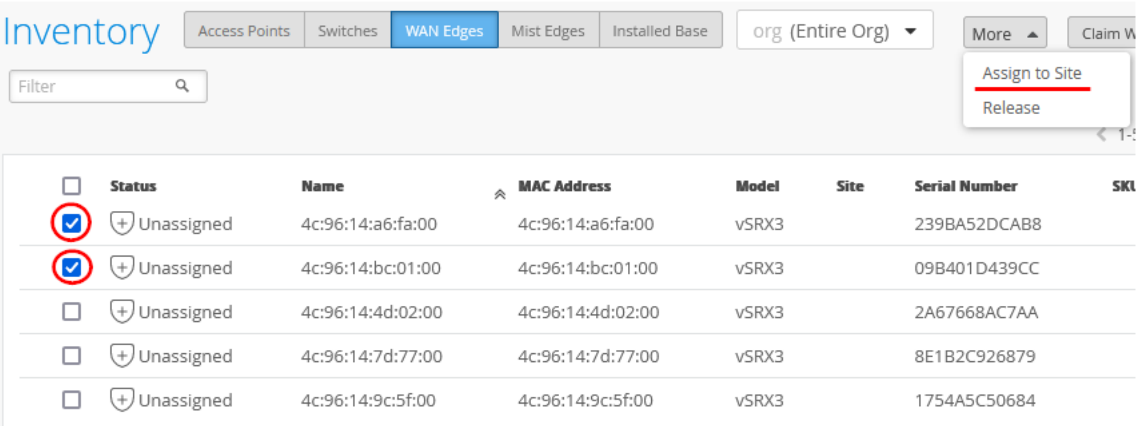
Figure 330: SRX Series in Inventory



□	Status	Name	MAC Address	Model	Site	Serial Number	SKI
□	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	

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

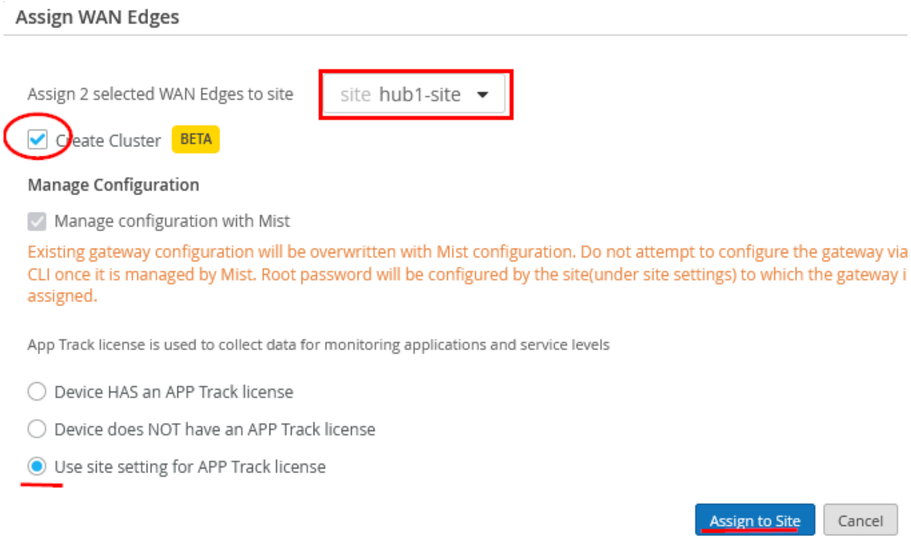
Figure 331: Assigning SRX Series Firewalls (HA Pair) to Site



☐	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	

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

Figure 332: Assign Spoke Devices to Site and Initiate Cluster Formation



Assign WAN Edges

Assign 2 selected WAN Edges to site: site hub1-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 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

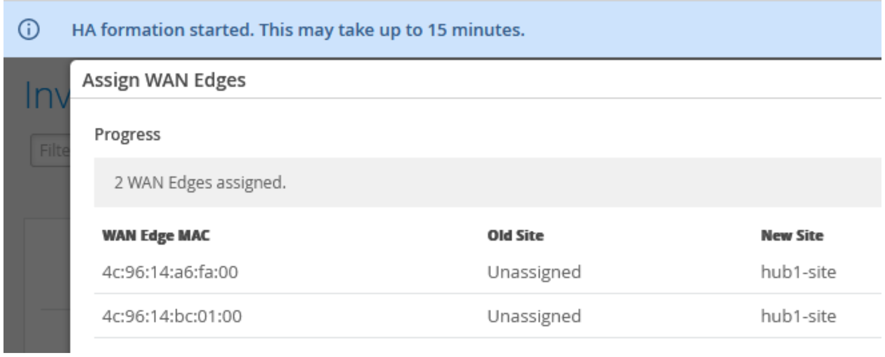
○ Device does NOT have an APP Track license

● Use site setting for APP Track license

5. 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.

Figure 333: HA Cluster Formation for Assigned Devices



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

Assign WAN Edges

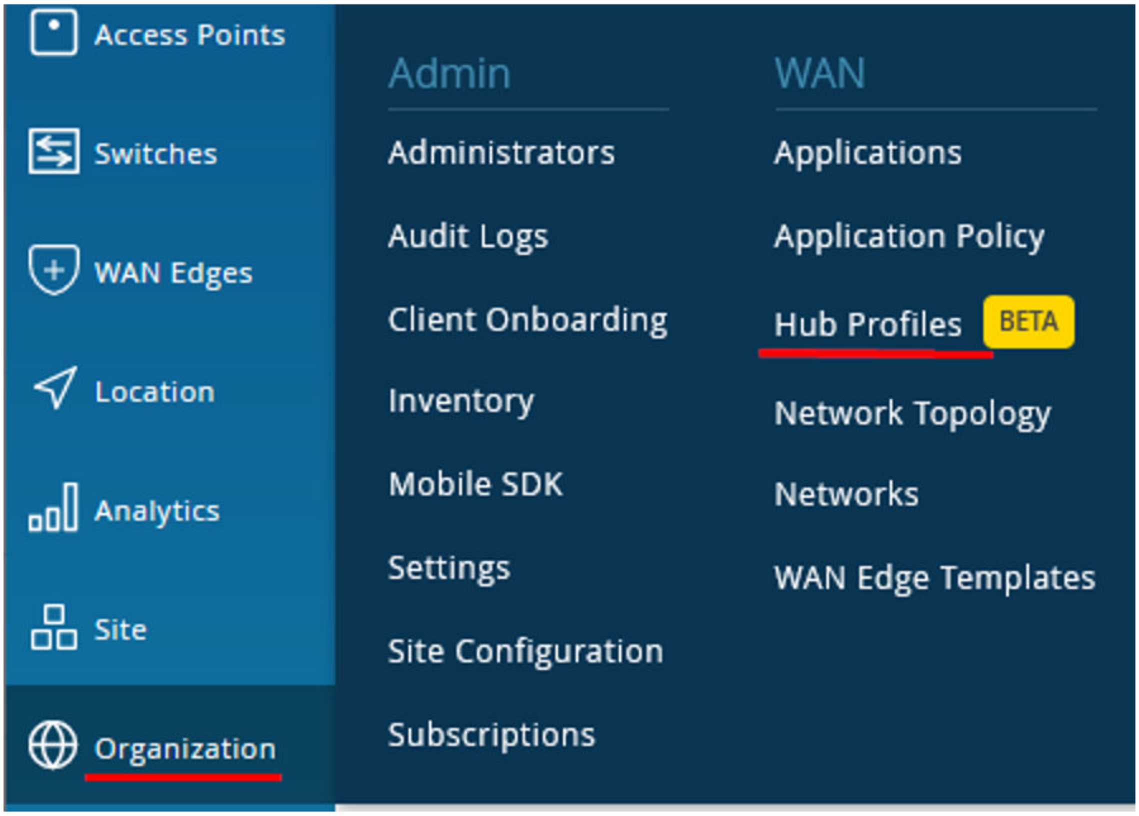
Progress

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

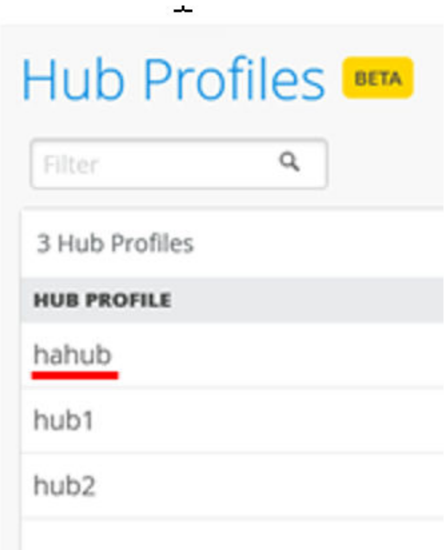
6. In the Juniper Mist portal, click **Organization** > **WAN** > **Hub Profiles**. The Hub Profile displays the list of existing profiles.

Figure 334: Navigating to Hub Profiles



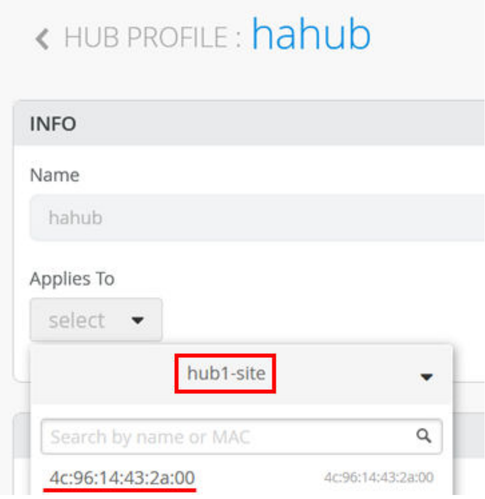
7. Click the hub profile (hahub) that you want to assign to a site.

Figure 335: Select Hub Profile



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

Figure 336: Select Sites for Applying Hub Profile

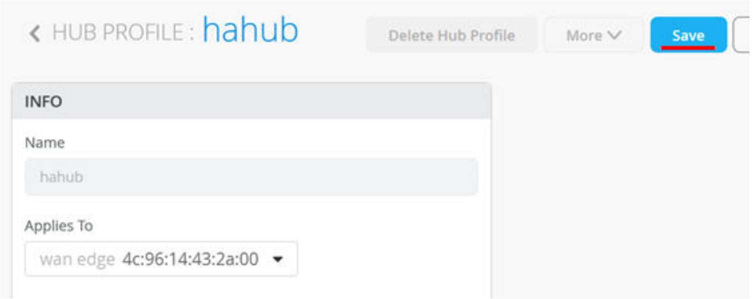


Name: hahub

Applies To

9. Check if have correct WAN Edge device selected, and click **Save**.

Figure 337: Select WAN Edge Device to Apply Template



HUB PROFILE : hahub

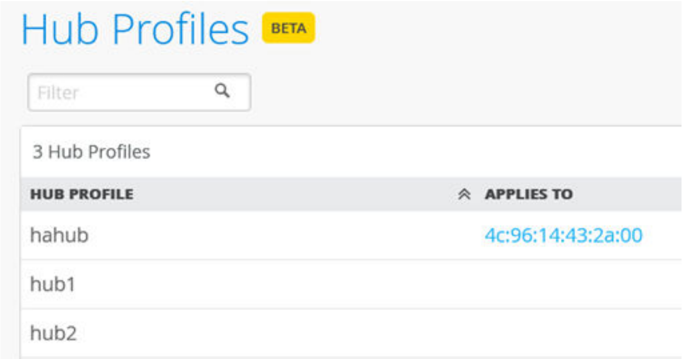
INFO

Name: hahub

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

10. You should now see the HA devices assigned to their **Hub Profile** in the as shown in Figure 338 on page 432.

Figure 338: Hub Profile Assignment Summary



3 Hub Profiles

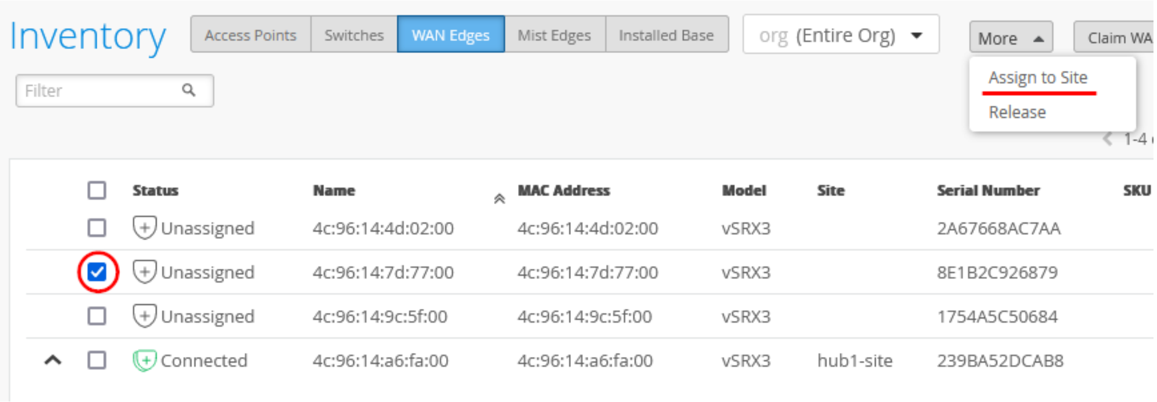
HUB PROFILE	APPLIES TO
hahub	4c:96:14:43:2a:00
hub1	
hub2	

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

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

12. Select the spoke device (SPOKE1) and click **Assign to Site**.

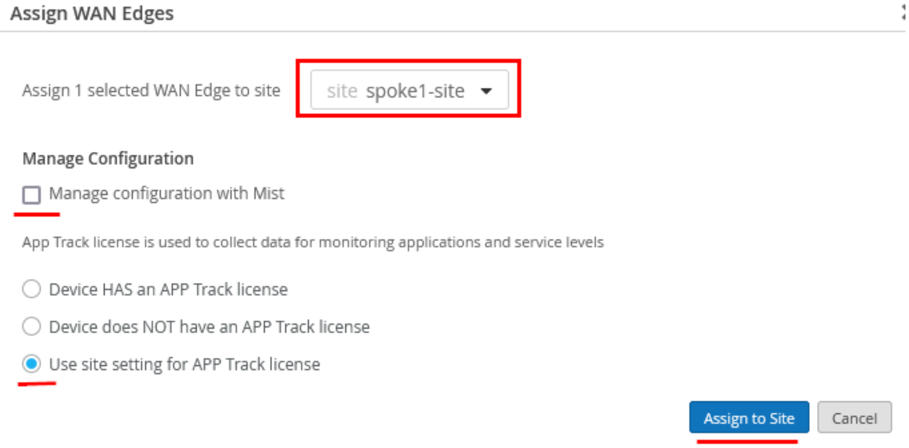
Figure 339: Assign Spoke Device To Site



	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	

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

Figure 340: 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

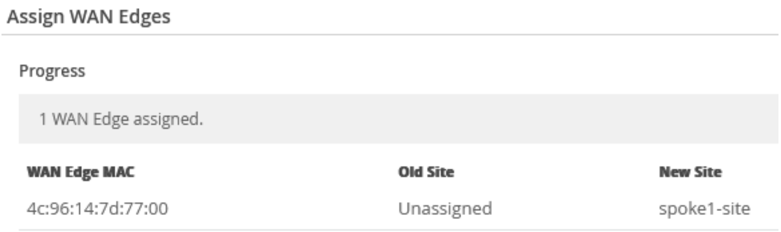
● Use site setting for APP Track license

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**.

14. Click **Assign to Site**.

The system confirms the assignment to the site as shown in

Figure 341: Assigned to Site



Assign WAN Edges

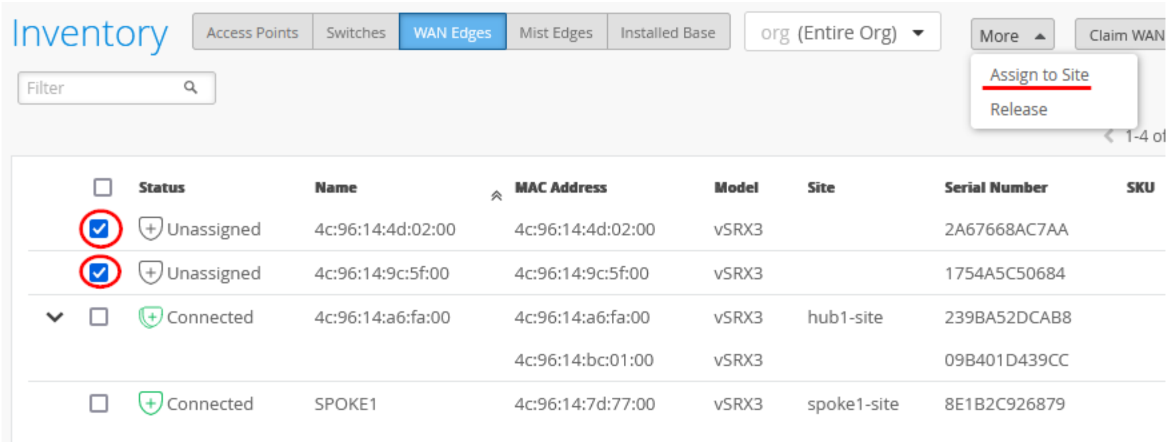
Progress

1 WAN Edge assigned.

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

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

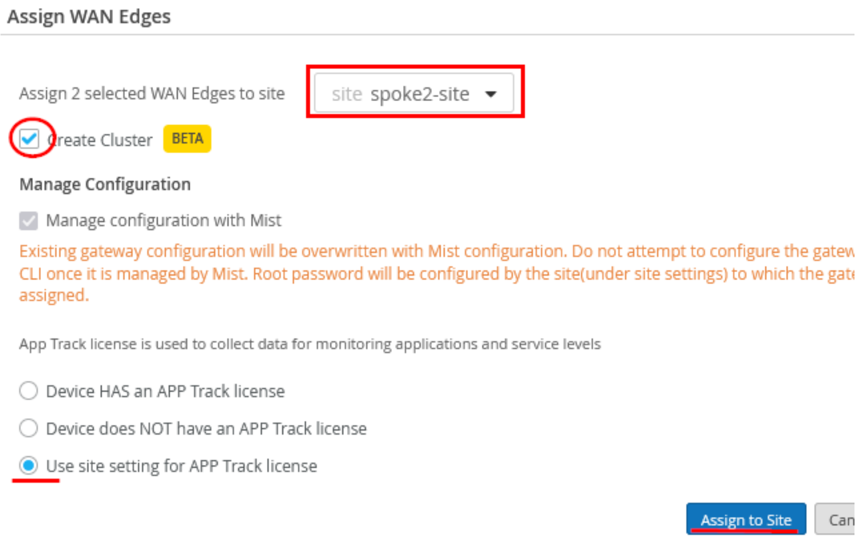
Figure 342: Assign Spoke Devices to Site



	☐	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	

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

Figure 343: 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

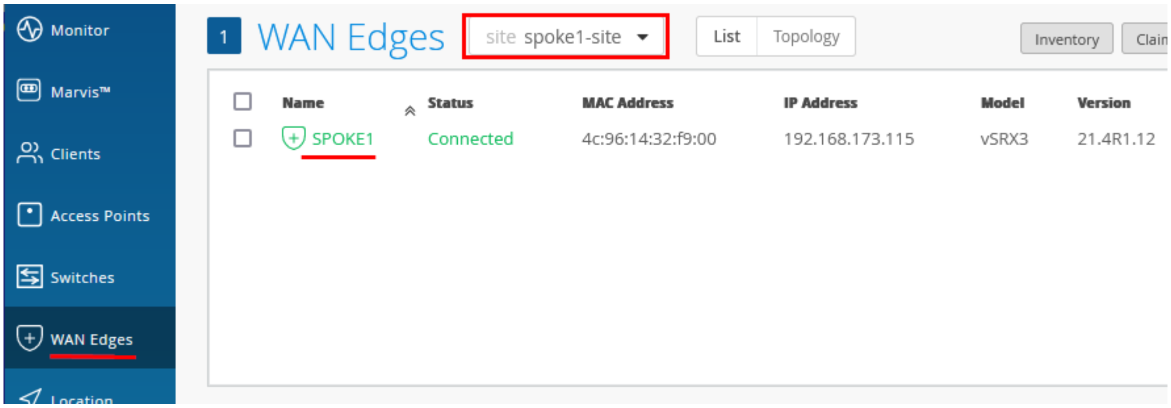
○ Device HAS an APP Track license

○ Device does NOT have an APP Track license

● Use site setting for APP Track license

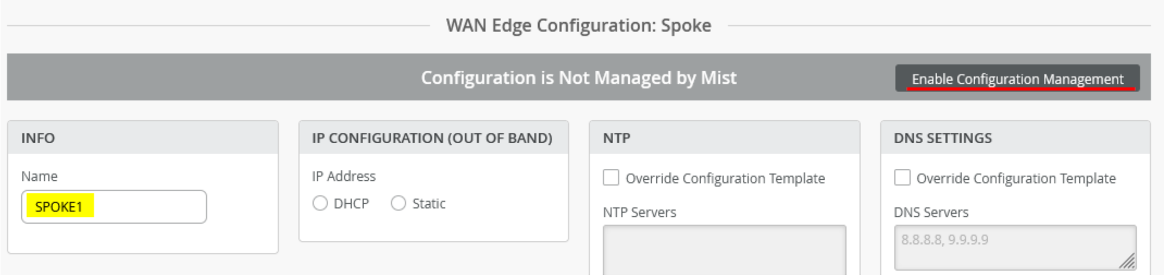
17. Go to Inventory Page. Figure 344 on page 435 shows the details of devices assigned to site and high availability pairs.

Figure 344: 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

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



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

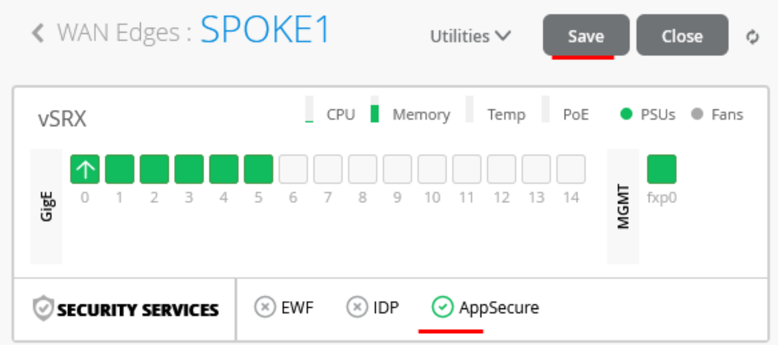
DNS SETTINGS

☐ Override Configuration Template

DNS Servers: 8.8.8.8, 9.9.9.9

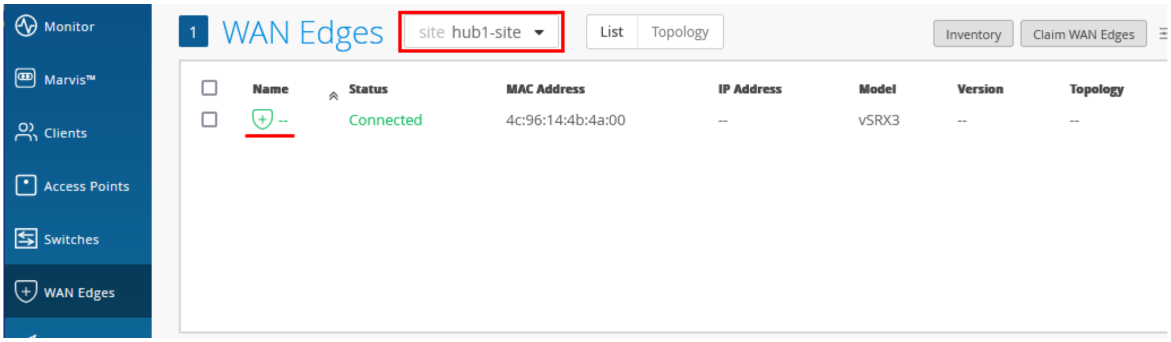
19. Save your changes.

Figure 345: Saving Spoke Device Configuration Changes



Now you have a topology with highly available hub and spoke of SRX Series using the WAN Assurance solution.

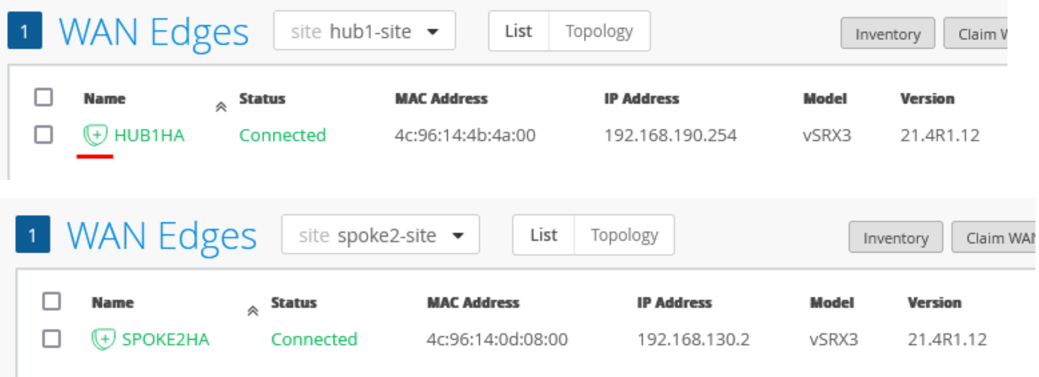
20. (Optional) In Juniper Mist portal, go to **WAN Edges** and select **hub1-site.**



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

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

Figure 346: Renaming Hub and Spoke HA Cluster Setup



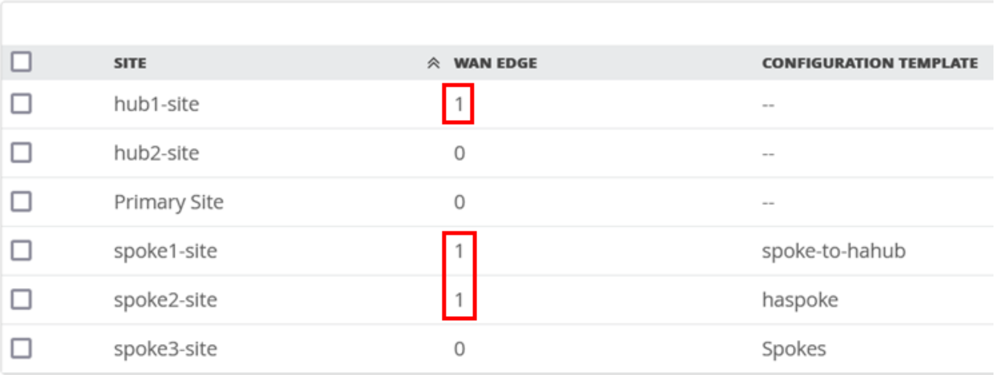
☐	Name	Status	MAC Address	IP Address	Model	Version
☐	HUB1HA	Connected	4c:96:14:4b:4a:00	192.168.190.254	vSRX3	21.4R1.12

☐	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.

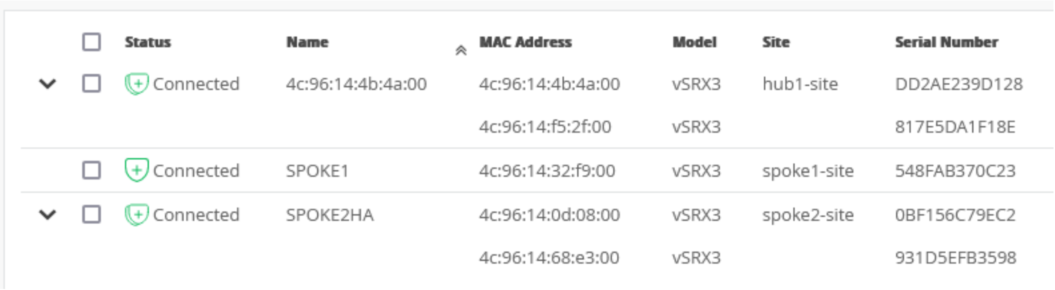
Figure 347: WAN Edge Template Assignments



□	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.

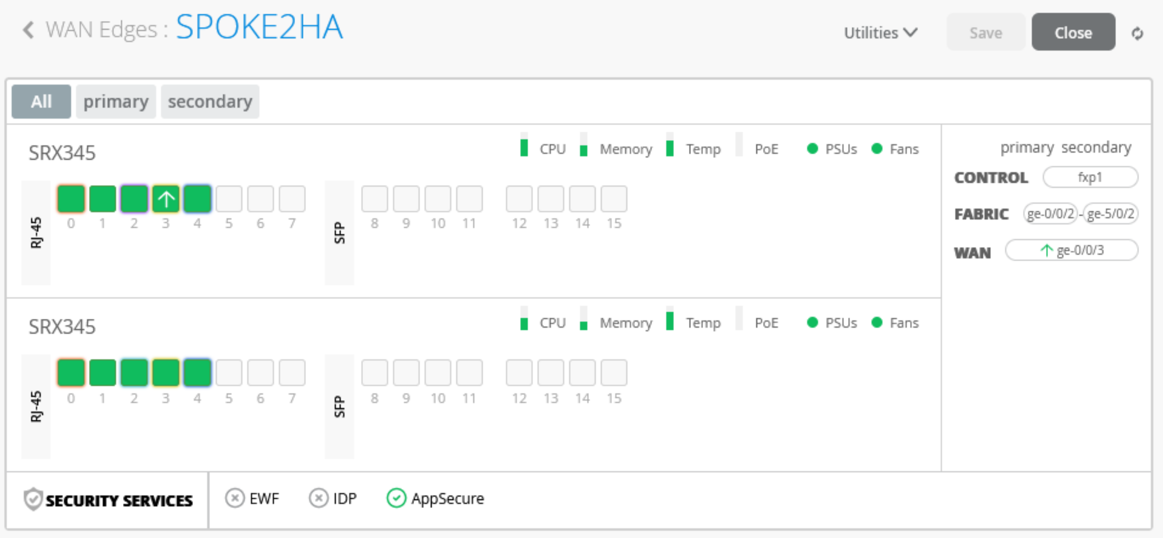
Figure 348: Device Inventory



	□	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

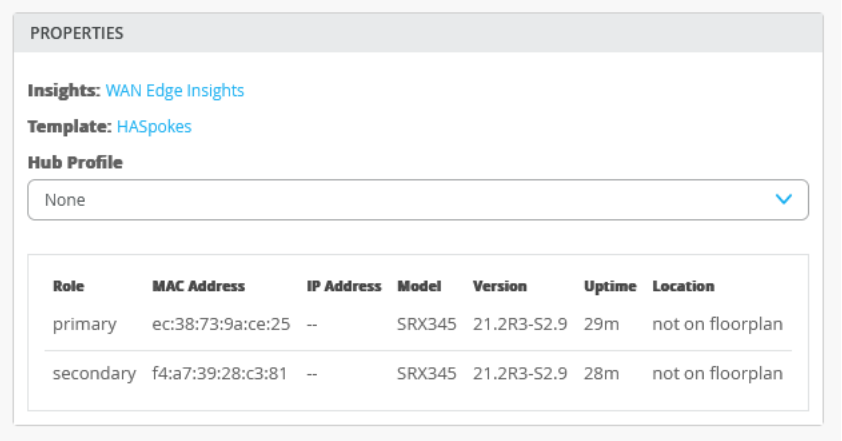
On the dashboard, for example, for the spoke devices that are part of high availability cluster, you can see the notion of primary and secondary device.

Figure 349: Example of SRX345 High Availability Cluster Display Details.



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

Figure 350: Properties Pane



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

Replace an SRX Series Firewall Node in a High Availability Cluster

You can replace an SRX Series Firewall device from a high availability cluster setup with few simple steps.

Before you replace a SRX Series Firewall node from the cluster, you must:

- Remove the cluster fabric cables from the node being replaced and connect it to the new replacement node.

- Make sure that the replacement SRX Series Firewall is both the same model as the device being replaced and has a same Junos OS version.

> **NOTE**: Replacing a node in a high availability setup cause minimal impact on network services. Therefore, we recommend that you plan for a maintenance window to do this task.

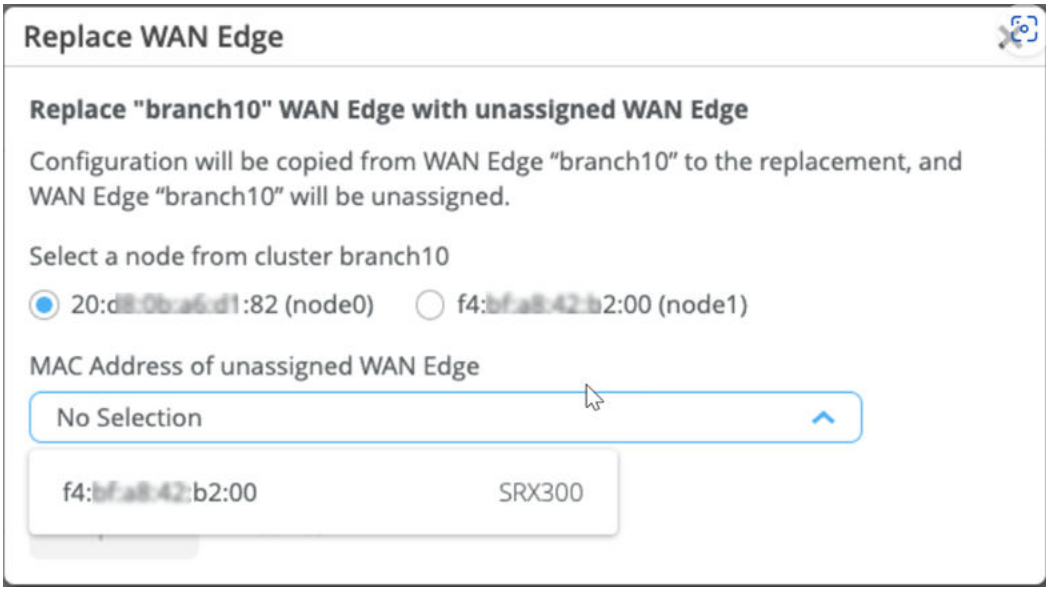
To replace an SRX Series Firewall node in a cluster:

1. In the Juniper Mist portal, on the left navigation bar, go to **Organization** > **Admin** >**Inventory** and select **WAN Edges** tab.

   Alternatively, select **WAN Edges** > **WAN Edges** page.

   The page displays a list of WAN edge devices. You can set the view as **org (Entire Org)** or **Site** in the inventory page.
2. Click the high availability pair that you want to replace.
3. Select **Utilities** > **Replace WAN Edge**.
4. On the Replace WAN Edge window, select the old SRX Series node that you want to replace and select the new replacement device's MAC address from the **MAC Address of unassigned WAN Edge** drop-down list.

Figure 351: Replace SRX Series Firewall in HA with Another Device



Replace WAN Edge

Replace "branch10" WAN Edge with unassigned WAN Edge

Configuration will be copied from WAN Edge "branch10" to the replacement, and WAN Edge "branch10" will be unassigned.

Select a node from cluster branch10

● 20:d[redacted]1:82 (node0) ○ f4:[redacted]2:00 (node1)

MAC Address of unassigned WAN Edge

No Selection

f4:[redacted]b2:00	SRX300

After you click **Replace**, allow about 15 minutes to complete the replacement procedure.

Refresh your browser and check under WAN Edges to find out if your SRX Series Firewall high availability setup is updated and available as a part of the inventory.

Replace a Standalone SRX Series Firewall

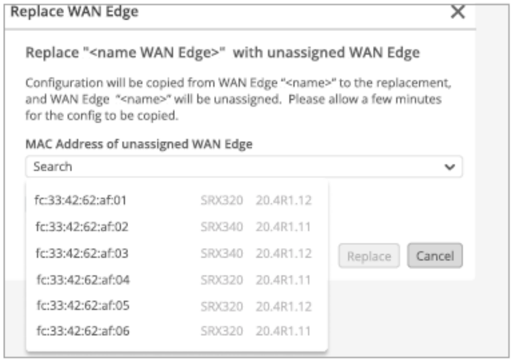
You can replace connected or disconnected SRX Series Firewall with another SRX Series Firewall of the same model.

1. In the Juniper Mist portal, on the left navigation bar, go to **Organization** > **Admin** >**Inventory** and select **WAN Edges** tab.

   Alternatively, you can also go to **WAN Edges** > **WAN Edges** page.

   The page displays a list of WAN edge devices. You can set the view as **org (Entire Org)** or **Site** in the inventory page.
2. Click the SRX Series Firewall that you want to replace.
3. Select **Utilities > Replace WAN Edge**.
4. On the Replace WAN Edge window, select the new replacement device's MAC address from the **MAC Address of unassigned WAN Edge** drop-down list.

Figure 352: Replace a Standalone SRX Series Firewall



Replace WAN Edge

Replace "<name WAN Edge>" with unassigned WAN Edge

Configuration will be copied from WAN Edge "<name>" to the replacement, and WAN Edge "<name>" will be unassigned. Please allow a few minutes for the config to be copied.

MAC Address of unassigned WAN Edge

Search

fc:33:42:62:af:01	SRX320	20.4R1.12
fc:33:42:62:af:02	SRX340	20.4R1.11
fc:33:42:62:af:03	SRX340	20.4R1.12
fc:33:42:62:af:04	SRX320	20.4R1.11
fc:33:42:62:af:05	SRX320	20.4R1.12
fc:33:42:62:af:06	SRX320	20.4R1.11

Juniper Mist portal displays a list of supported models available in the inventory page in unassigned state.

After you click **Replace**, allow about 15 minutes to complete the replacement procedure. System copies the configuration of the replaced SRX Series firewall into the new device. The replaced SRX Series continues to be part of the site in unassigned state.

Refresh your browser and check under WAN Edges to find out if your SRX Series Firewall is available as a part of the inventory.

Delete a High Availability Cluster

1. In the Juniper Mist portal, on the left navigation bar, go to **Organization** > **Admin** >**Inventory** and select **WAN Edges** tab.

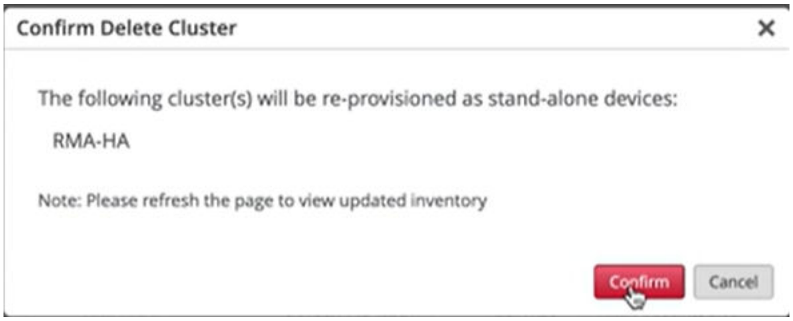
   Alternatively, select **WAN Edges** > **WAN Edges** page.

   The page displays a list of WAN edge devices. You can set the view as **org (Entire Org)** or **Site** in the inventory page.

2. Select the high availability pair and click **Delete Cluster** under **More**.

   Click **Confirm** on the **Confirm Delete Cluster** message.

Figure 353: Delete SRX Series Cluster



Confirm Delete Cluster

The following cluster(s) will be re-provisioned as stand-alone devices:

RMA-HA

Note: Please refresh the page to view updated inventory

Juniper Mist re-provisions the devices as standalone devices in the same site.

Refresh your browser and check under WAN Edges to find out if your SRX Series Firewalls are available as standalone devices in the inventory.

SEE ALSO

- Introduction to Juniper Mist WAN Assurance | 2
- Juniper Mist WAN Assurance Platform Considerations | 10
- Configure Sites and Variables for SRX Series Firewalls | 168
- Configure Networks for SRX Series Firewalls | 182
- Configure Applications for SRX Series Firewalls | 174
- Configure Application Policies on SRX Series Firewalls | 191
- Onboard SRX Series Firewalls for WAN Configuration | 259
- Configure Hub Profiles for SRX Series Firewalls | 197

6

CHAPTER

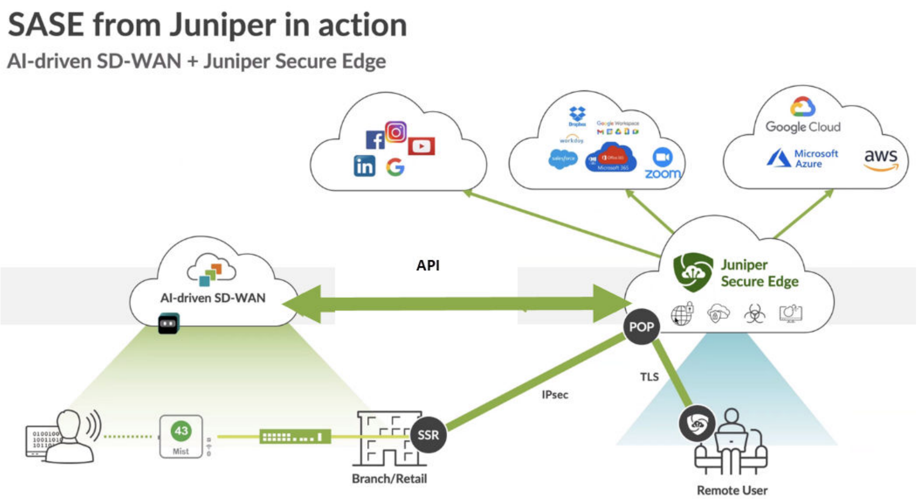
Secure Edge Connector

Juniper Mist Secure Edge Connector

IN THIS SECTION

Juniper Mist provides pre-built connectors specifically designed for the Juniper Networks® SRX Series Firewalls and Juniper® Session Smart™ Routers deployed as WAN edge devices. These connectors facilitate seamless integration with your Secure Service Edge (SSE) deployments. With minimal configuration, you can integrate the SSE into the Juniper Mist portal. As a result, your WAN Edge device establishes connections to the SSE using either IPsec or GRE protocols.

Figure 354: Traffic Inspection by Juniper Secure Edge



In this solution, an IPsec tunnel is configured between the WAN Edge device and SSE using the Secure Edge Connector within the WAN Edge template. Additionally, a BGP over IPsec connection is configured to dynamically learn routing destinations from the SSE device.

Following types of connectors are pre-built for you in Juniper Mist portal:

- Juniper Secure Edge (manual provisioning and auto provisioning)

- Zscaler (manual provisioning and auto provisioning)
- Custom

High-level workflow for setting up secure edge connectors with Juniper Secure Edge, custom, or Zscaler deployment to offload traffic from your WAN edge device (SSR Series Routers or SRX Series Firewalls):

1. Create and deploy a basic branch template for device connectivity.
2. Optionally configure a remote network in SSE. This step defines a remote source for inbound connectivity through the tunnel.
3. Configure a Secure Edge Connector and provider in the device template. This step creates a custom IPsec tunnel to the remote location and define encryption parameters.
4. Optionally configure a BGP peer to learn routes dynamically.
5. Configure an Application to allow traffic to be steered toward the IPsec tunnel. This application will be used in Application Policy to allow client networks to access the BGP learned routes.
6. Configure a Traffic Steering Policy to steer the Internet-bound traffic from the LAN side of a spoke or hub device to Secure Edge.

Application Policies for Secure Edge Connector

An Application Policy in the Juniper WAN Assurance design is a combination of Networks and Users as the source with Applications as the destination. These security rules define which networks/users can access these applications with Traffic Steering defining which path should be used.

To set up these policies, you need to create Networks, Applications, Traffic-steering profiles. For outbound traffic the Traffic Steering profile will include the Secure Edge Connector. For inbound use cases where traffic initiates from the Secure Edge Connector you include the remote network in the Secure Edge Connector and then use that network in an Application Policy to allow inbound access from the Secure Edge Connector. With this feature, you can securely connect to cloud-hosted services which need to initiate inbound traffic to a site.

Traffic Steering Profiles for Secure Edge Connector

Traffic Steering is required for SEC on both SRX Series Firewalls and Session Smart Routers before Juniper Mist creates the tunnels.

This requirement remains unless:

- A remote network is assigned to a Secure Edge Connector
- A BGP peer is assigned to a Secure Edge Connector

Dynamic Routing for Secure Edge Connectors

You can configure BGP peering over a Secure Edge Connector. This configuration leverages BGP for dynamic routing and uses BGP path selection to install routes in the route table. High-Level steps include:

- Verify that your Secure Edge Connector is established and is configured using the custom Secure Edge provider.
- Configure BGP import and export policies.
- Configure BGP neighbor options.
- Select the Secure Edge Connector for this BGP neighbor.
- Assign import and export policies.
- Verify that the BGP peers are exchanging routes over the tunnel interface.

RELATED DOCUMENTATION

Introduction to Juniper Mist WAN Assurance | 2
Juniper Mist WAN Assurance Platform Considerations | 10
Juniper Mist WAN Assurance Configuration Hierarchy | 13

Setup Secure Edge Connector with Juniper Secure Edge (Manual Provisioning)

IN THIS SECTION

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® Session Smart™ Routers, deployed as WAN edge device, to send a portion of traffic to Juniper Secure Edge for an inspection.

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).

For more information, see Juniper Secure Edge.

Configuration Overview

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 Juniper 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 (Session Smart Routers or SRX Series Firewalls), that connect to the LAN networks. These are the physical 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.

Topics in the following table present the overview information you need to use the cloud-based security of Secure Edge with the Juniper Mist™ cloud.

Table 52: Secure Edge Connector Configuration Workflow

Step	Task	Description
1	"Access Juniper Security Director Cloud and Check Active Subscriptions " on page 449	Access Juniper Security Director Cloud, go to your organization account, and check Secure Edge subscriptions. The subscription entitles you to configure Secure Edge services for your deployments.
2	"Configure a Service Location in Juniper Security Director Cloud " on page 450	Create service locations. This is where the vSRX-based VPN gateways creates secure connections between different networks.
3	"Generate Device Certificates in Juniper Security Director Cloud" on page 452	Generate digital certificates for Juniper Secure Edge to establish secure communications between Secure Edge and user endpoints.
4	"Create an IPsec Profile in Juniper Security Director Cloud " on page 455	Create IPsec profiles to establish IPsec tunnels for communication between the WAN edge devices on your Juniper Mist cloud network with Secure Edge instance.
5	"Create a Site in Juniper Security Director Cloud " on page 456	Create a site that hosts a WAN edge device (Session Smart Router or SRX Series Firewall). The traffic from the device is forwarded to the Secure Edge instance through a secure tunnel for an inspection.
6	"Deploy a Secure Edge Policy in Juniper Security Director Cloud " on page 464	Configure policies that define the security rules and actions for the traffic originating from or destined to the site.

7	"Get IPsec Tunnel Configuration Parameters to Apply in Juniper Security Director Cloud " on page 466	Note down the details such as service location IP or hostname, the IPsec profile name, and the pre-shared key. You need these details to set up IPsec tunnels from Juniper Mist side.
8	"Create Secure Edge Connectors in the Juniper Mist Cloud Portal " on page 469	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 device managed by Mist and the Secure Edge instance.
9	"Modify an Application Policy " on page 476	Create a new or change an existing application policy to direct the traffic from WAN edge device to the Internet through Juniper Security Director Cloud instead of going through a hub for centralized access.
10	"Verify the Configuration " on page 477	Confirm if your configuration is working by checking the established IPsec tunnels in: • WAN Insights in Mist portal • Security Director Cloud dashboard • Tunnel traffic flow on the WAN edge device CLI.

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.
- Create Your Secure Edge Tenant. See Create Your Secure Edge Tenant.
- We assume that you have adopted and configured the Session Smart Router or SRX Series Firewall deployed as WAN edge device in Juniper Mist Cloud.

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 VPN gateways hosted in a public cloud for your organization.

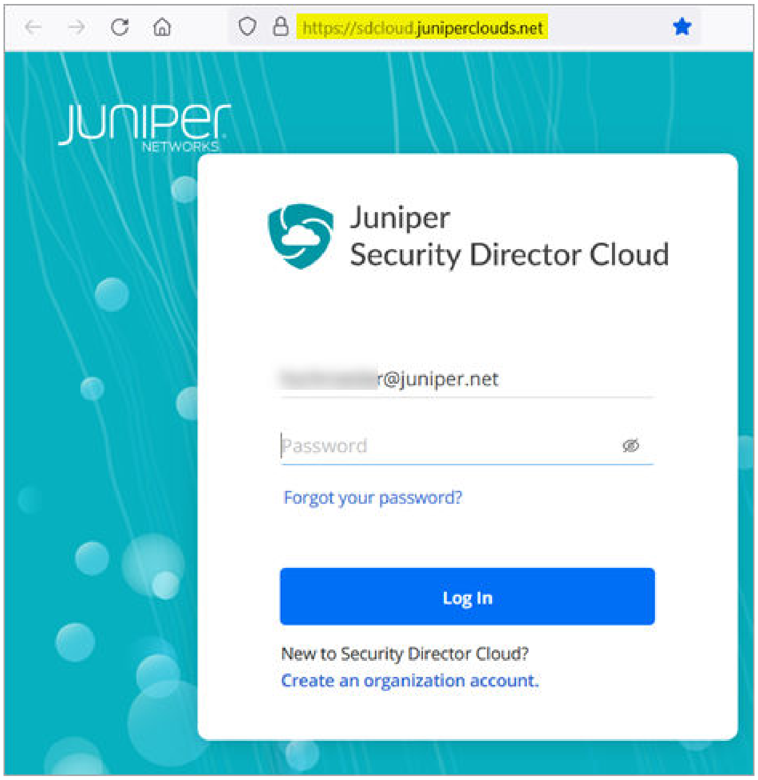
A tenant can have one or more service locations, which are the connection points for end users. To create a tenant, you need to have an account on Juniper Security Director Cloud. See Create Your Secure Edge Tenant for details.

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:

1. 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.

Figure 355: Access Juniper Security Director Cloud



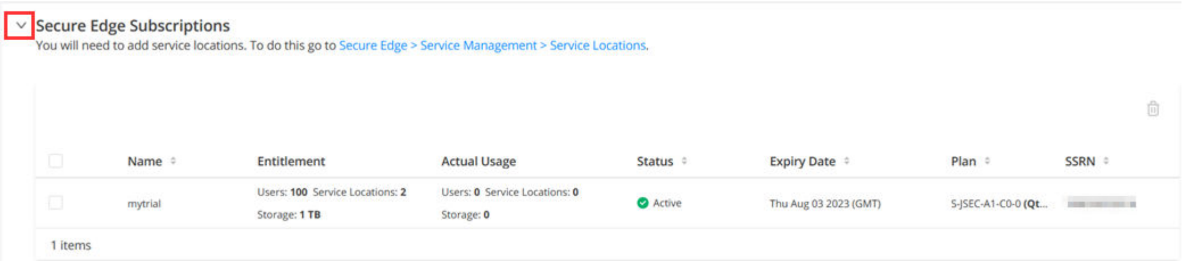
https://sdcloud.juniperclouds.net

[redacted]r@juniper.net

2. Select the required tenant in the upper right corner of the portal to continue.

3. Select **Administration** > **Subscriptions** to access the Juniper Security Director Cloud subscriptions page.

Figure 356: 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** Storage: **1 TB**	Users: **0** Service Locations: **0** Storage: **0**	✓ Active	Thu Aug 03 2023 (GMT)	S-JSEC-A1-C0-0 **(Qt...**	[redacted]

1 items

4. Scroll to the **Secure Edge Subscriptions** section to check whether you have an active subscription.

> **NOTE**:
> SRX Management Subscription

For details, see About the Subscriptions Page.

Assuming that you have active subscriptions, continue with next steps.

Configure Service Locations

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

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:

1. In Juniper Security Director Cloud menu, select **Secure Edge**>**Service Management**>**Service Locations**.

   The Service Locations page appears.

2. Click the Add (+) icon to create a new service location.

   Enter the details for the following fields:

   - **Region**—Choose the geographic region where you want to create a Secure Edge instance.
   - **PoP**—Select the location for the Secure Edge in the region.
   - **Number of Users**—Enter the total possible number of users this service location may need to serve.

   Table 53 on page 451 shows examples of service locations.

   Table 53: Service Location Fields

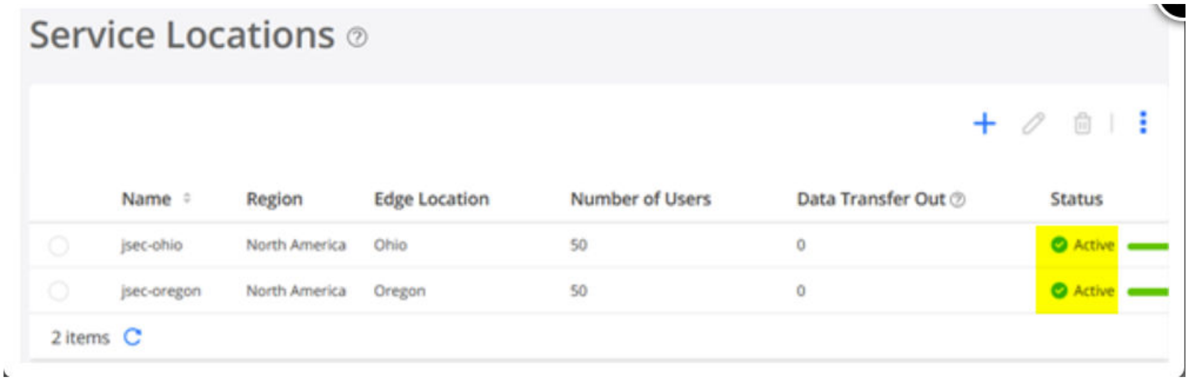
Field	Service Location	Service Location
Region	North America	North America
PoP	Ohio	Oregon
Number of Users	50 (we split the exiting equally)	50

3. Click **OK**.

   Security Director Cloud creates a service location and lists it on the Service Locations page.

   The status of the service location shows **In Progress** until the Secure Edge instance is fully deployed, as shown in Figure 357 on page 451.

Figure 357: Service Locations Status



Service Locations

Name	Region	Edge Location	Number of Users	Data Transfer Out	Status
jsec-ohio	North America	Ohio	50	0	Active
jsec-oregon	North America	Oregon	50	0	Active

2 items

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

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 certificate.

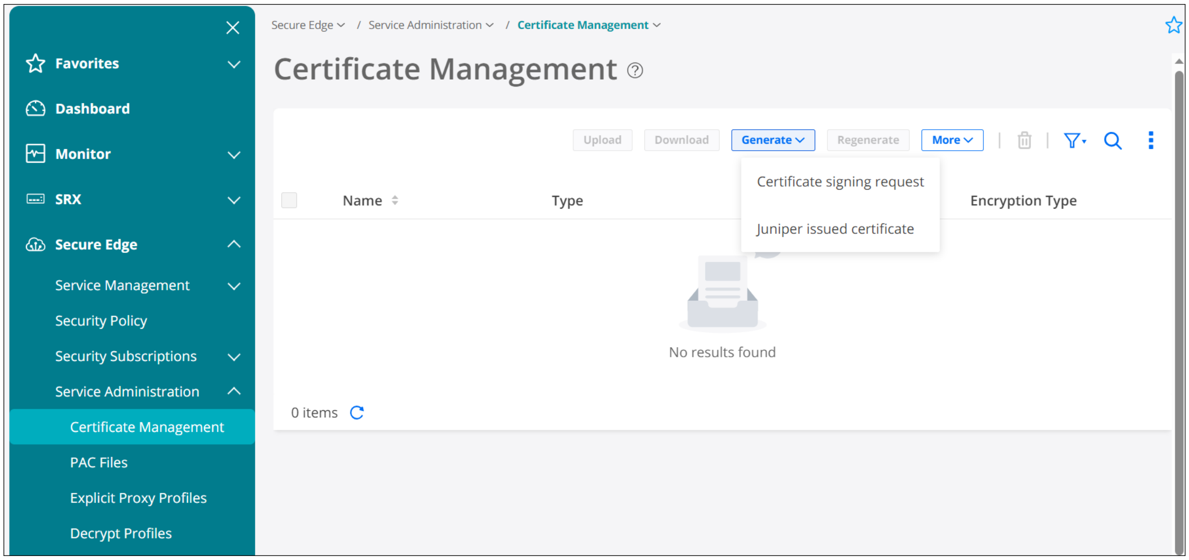
NOTE: This topic describes how to generate a TLS/SSL certificate. How you import and use the certificate depends on your company's client-management requirements and is beyond the scope of this topic.

To generate device certificates in Juniper Security Director Cloud:

1. Select **Secure Edge**>**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**.

Figure 358: Certificate Management



2. Select the relevant option:

   a. If your company has its own CA, and you want to generate a CSR, click **Certificate signing request**.

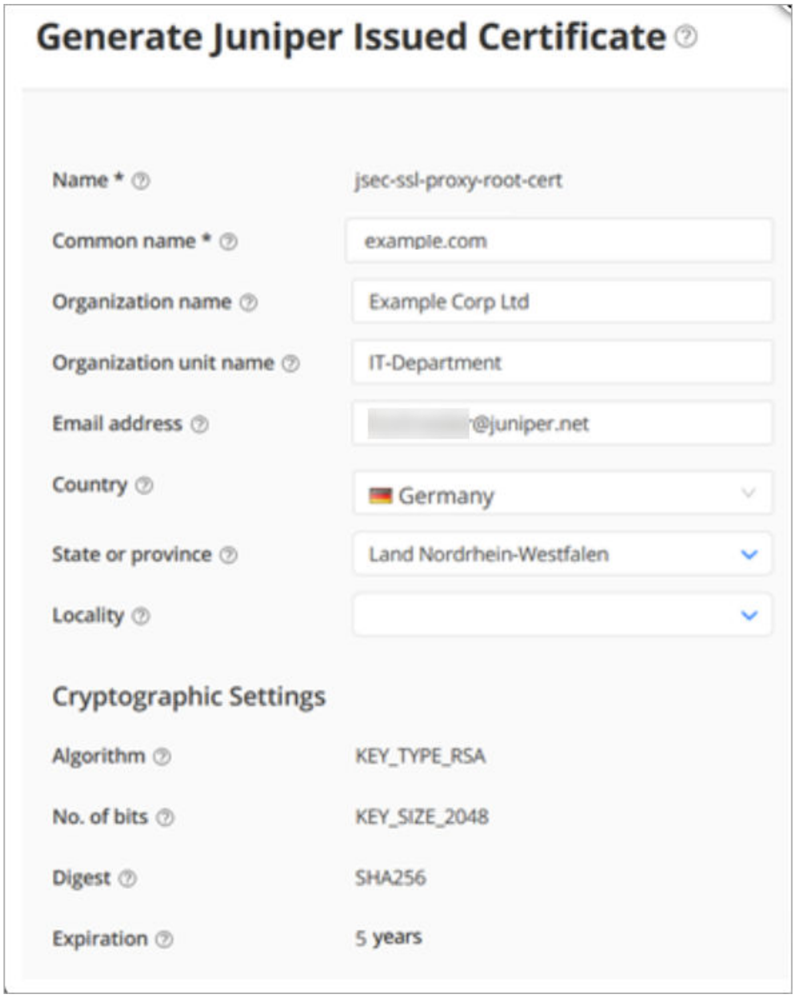
      After Juniper Secure Edge generates CSR, download the CSR and submit it to your CA to generate a new certificate. Once generated, click Upload to upload the certificate on the Certificate Management page.

   b. 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.

3. Enter the certificate details. In the **Common name** field, use the certificate's fully qualified domain name (FQDN).

Figure 359: 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	

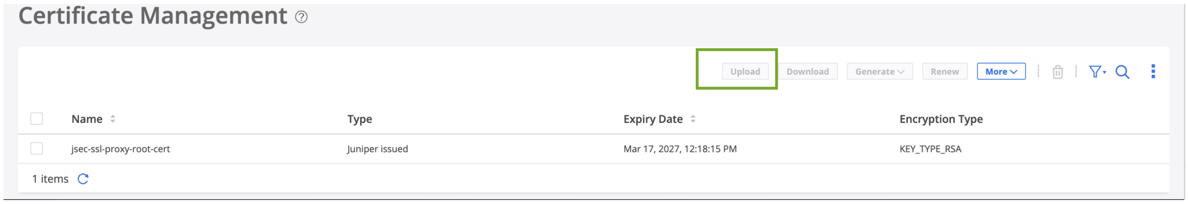
Cryptographic Settings

Algorithm	KEY_TYPE_RSA
No. of bits	KEY_SIZE_2048
Digest	SHA256
Expiration	5 years

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

4. Download the generated certificate.

Figure 360: Download the Certificate



Certificate Management

Name	Type	Expiry Date	Encryption Type
jsec-ssl-proxy-root-cert	Juniper issued	Mar 17, 2027, 12:18:15 PM	KEY_TYPE_RSA

1 items

The following sample shows the downloaded certificate:

```
-----BEGIN CERTIFICATE-----
$ABC123#1$ABC123#1 $ABC123#1$ABC123#1 $ABC123#1$ABC123#1 $ABC123#1$ABC123#1.
.
J$ABC123#1$XYZ123#1 $ABCBVFCC123#1$ABC123#1 $XYZ123#1$GTF123#1 $XZY123#1$BVFD123#1=
$ABC123#1$XYZ123#1 $ABCBVFCC123#1$ABC123#1 $XYZ123#1$GTF123#1 $XZY123#1$BVFD123#1=
-----END CERTIFICATE-----
```

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

Create an IPsec Profile in Juniper Security Director Cloud

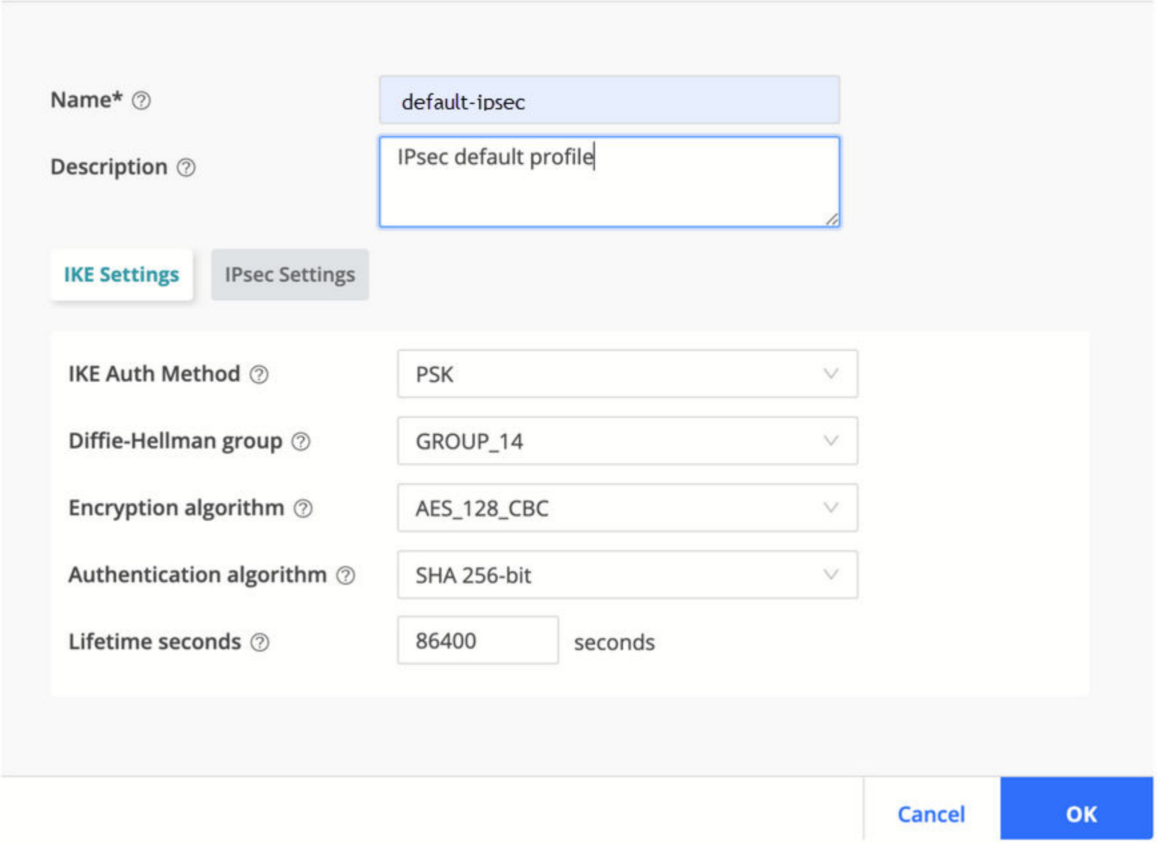
After you generate the certificates to establish secure communications between Secure Edge and WAN edge devices, you're ready to create IPsec profiles.

IPsec profiles define the parameters with which an IPsec tunnel is established when the WAN edge devices on your Juniper Mist™ cloud network start communicating with your Secure Edge instance.

To create an IPsec profile in Juniper Security Director Cloud:

1. In Juniper Security Director Cloud portal, select **Secure Edge** > **Service Management** > **IPsec Profiles** .
2. Click the Add (**+**) icon to create an IPsec profile.
   The Create IPsec Profile page appears.
3. For the profile name, use **default-ipsec**. Retain all default values for Internet Key Exchange (IKE) and IPsec; currently, they are not configurable on the Juniper Mist cloud portal.

Figure 361: Create an IPsec Profile



Name* ? default-ipsec

Description ? IPsec default profile

IKE Auth Method ?	PSK
Diffie-Hellman group ?	GROUP_14
Encryption algorithm ?	AES_128_CBC
Authentication algorithm ?	SHA 256-bit
Lifetime seconds ?	86400 seconds

You use this IPsec profile to create a site in the next task. On the Create Site page, if you select IPsec as the tunnel type on the Traffic Forwarding tab, you will attach the IPsec profile.

Create a Site in Juniper Secure Edge Cloud

You have now created IPsec profiles. These profiles define the parameters for the IPsec tunnel between WAN edge devices on your Juniper Mist™ cloud network and your Secure Edge instance.

At this point, you need to create a site in Juniper Security Director Cloud. A site represents a location that hosts a WAN edge device. The traffic from the WAN edge device is forwarded to the Secure Edge instance through a secure tunnel, and then inspected and enforced by the Secure Edge cloud services.

You can configure to forward some or all of the Internet-bound traffic from customer sites to the Juniper Secure Edge cloud through generic routing encapsulation (GRE) or IPsec tunnels from the WAN edge devices at the site.

NOTE: Overlapping branch addresses are not supported to the same POP within Secure Edge when using a stateful firewall at branch locations. Reverse path traffic to these overlapping IPs will be routed using equal-cost multipath (ECMP) across all connections. Traffic is routed using ECMP rather than per-session routing to the interface from which traffic originated. Consider reverse path traffic through ECMP when you configure the protected networks for a site.

To create a site in Juniper Security Director Cloud:

1. In Juniper Security Director Cloud portal, select **Secure Edge** >**Service Management** > **Sites**.

   The Sites page appears.
2. Click the Add (+) icon to create a site.
3. Complete the Site Details page as follows:

   a. Enter a unique site name and a description.

   b. Select the corresponding country from the list where the site is located.

   c. (Optional) Enter the zip code where the customer branch is located.

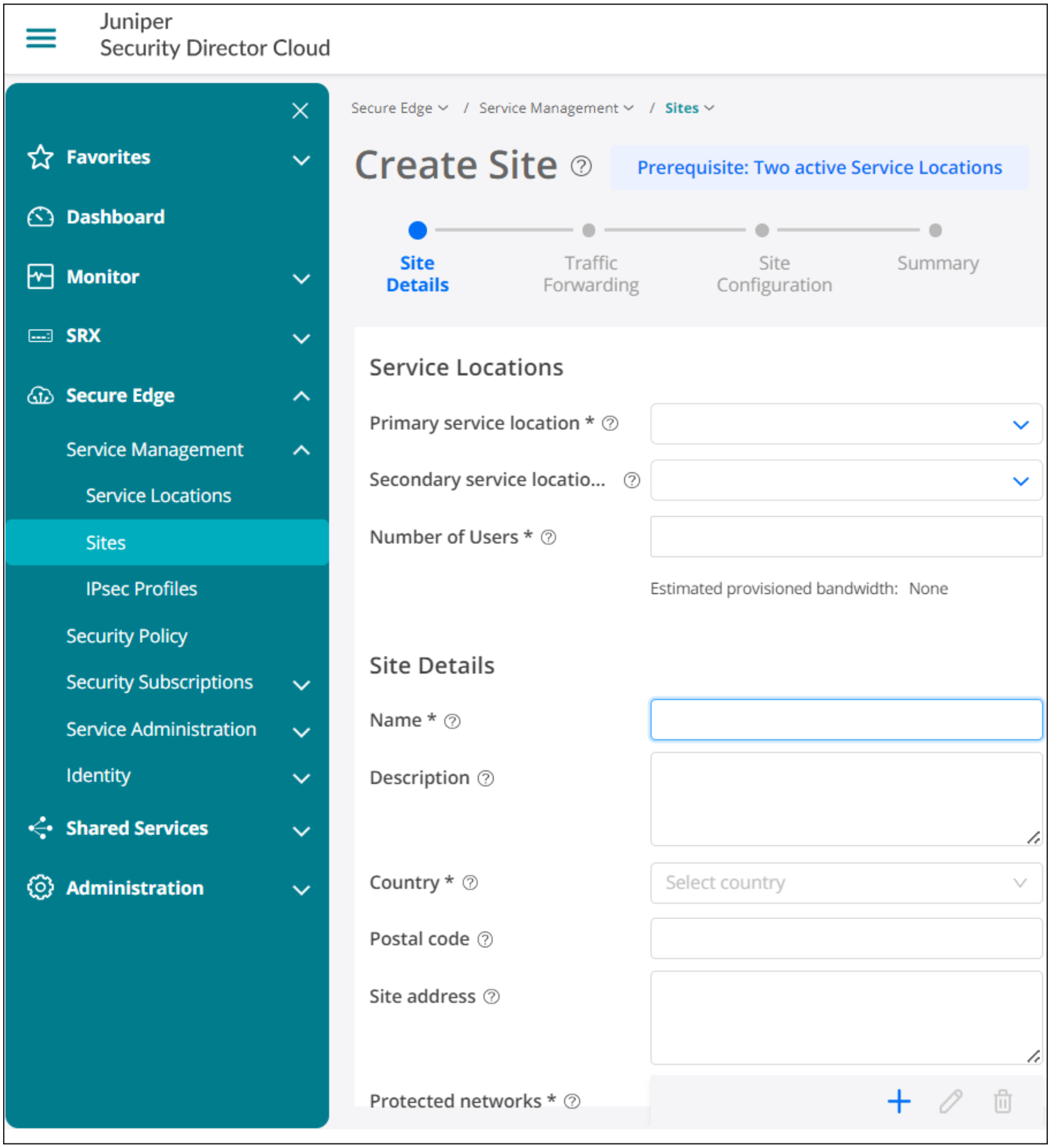
   d. (Optional) Enter the location (street address) of the site.

   e. Select the number of users who can use the network at the site.

   f. In the Protected networks field, click the Add (+) icon to add the private IP address range of the interface to be used for traffic flow through the tunnel.

   Figure 362 on page 458 and No Link Title show an example of a site.

Figure 362: Create Site in Juniper Secure Edge Cloud



Create Site ⓘ Prerequisite: Two active Service Locations

Service Locations

Primary service location * ⓘ

Secondary service locatio... ⓘ

Number of Users * ⓘ

Estimated provisioned bandwidth: None

Site Details

Name * ⓘ

Description ⓘ

Country * ⓘ Select country

Postal code ⓘ

Site address ⓘ

Protected networks * ⓘ

Table 54: Site-Creation Details

Fields	Values
Primary service location	jsec-oregon
Secondary service location	jsec-ohio

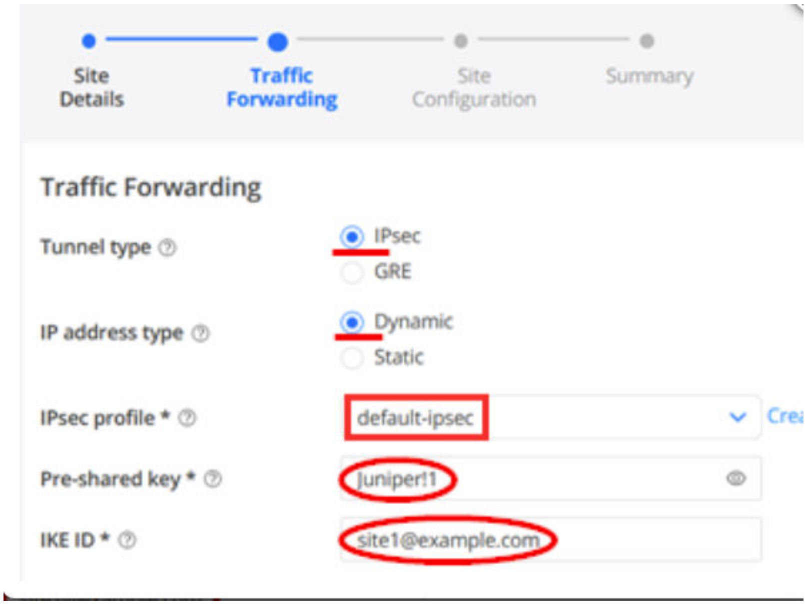
Table 54: Site-Creation Details *(Continued)*

Fields	Values
Number of Users	10
Name	spoke1-site
Country	Germany
Protected networks	10.99.99.0/24 (LAN network)

4. Click **Next**.

5. On the Traffic Forwarding page, enter the details according to the information provided in Figure 363 on page 459

Figure 363: Create Site: Traffic-Forwarding Details



Traffic Forwarding

Tunnel type ● IPsec ○ GRE

IP address type ● Dynamic ○ Static

IPsec profile * default-ipsec

Pre-shared key * juniper!1

IKE ID * site1@example.com

Table 55: Details for Traffic Forwarding Policy

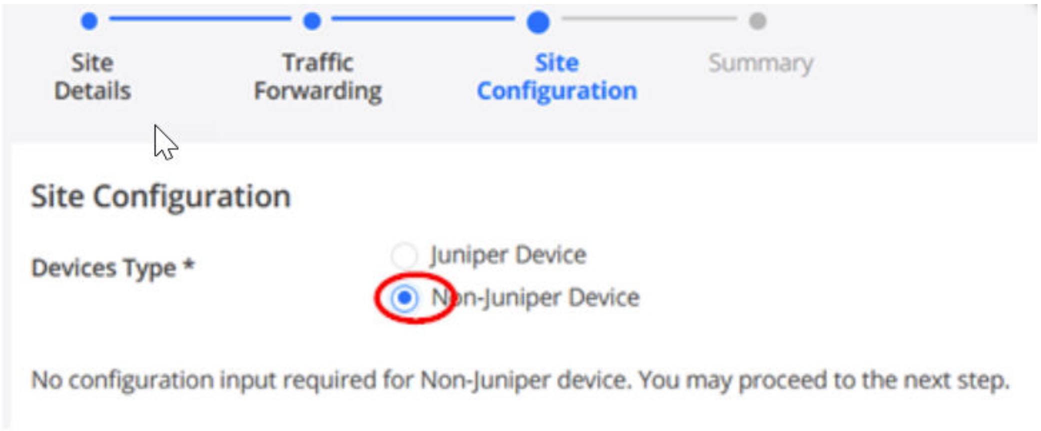
Field	Value
Tunnel type	IPsec

Table 55: Details for Traffic Forwarding Policy *(Continued)*

Field	Value
IP address type	Dynamic For the Static IP address type, you need to provide the device IP address in the Site IP address field.
IPsec profile	default-ipsec If you do not have a preconfigured IPsec profile, click Create IPsec Profile to create an IPsec profile.
Pre-shared key	Define a unique PSK for each site. Example: Juniper!1
IKE ID	site1@example.com (resembles an email address and must be a unique value for each site).

6. Click **Next**.
7. On the Site Configuration page, for the **Device Type** select **Non-Juniper Device**.

Figure 364: Create Site-Site Configuration



Site Configuration

Devices Type *

○ Juniper Device

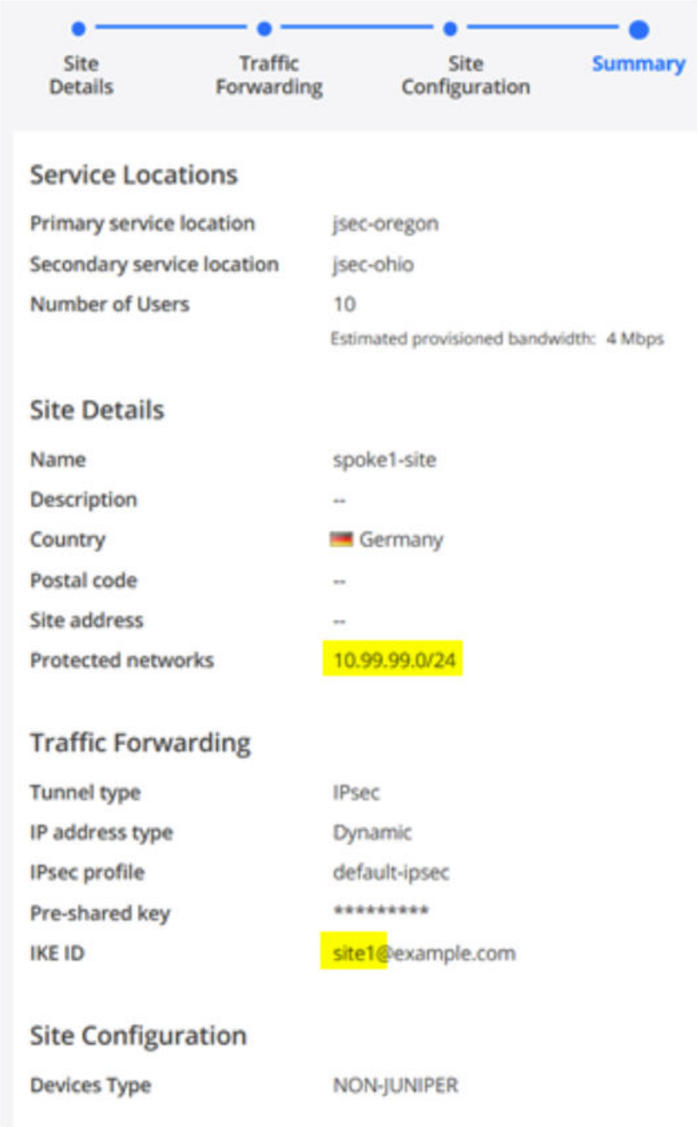
● Non-Juniper Device

No configuration input required for Non-Juniper device. You may proceed to the next step.

You must select this option because the devices that the Juniper Mist cloud portal manages do not have their configuration pushed through Juniper Security Director Cloud.

8. Click **Next**.
9. On the Summary page, review the configuration.

Figure 365: Create Site-Summary



Service Locations

Primary service location	jsec-oregon
Secondary service location	jsec-ohio
Number of Users	10 Estimated provisioned bandwidth: 4 Mbps

Site Details

Name	spoke1-site
Description	--
Country	Germany
Postal code	--
Site address	--
Protected networks	10.99.99.0/24

Traffic Forwarding

Tunnel type	IPsec
IP address type	Dynamic
IPsec profile	default-ipsec
Pre-shared key	*********
IKE ID	site1@example.com

Site Configuration

Devices Type	NON-JUNIPER

10. Click **Back** to edit any fields or **Finish** to create the new site.

11. Add two more sites using the same procedure. The following paragraphs describe the details to include in each site.

    a. Create a second site with the details provided in No Link Title and No Link Title.

    .

    Table 56: Site Creation for Second Site

Fields	Value
Primary service location	jsec-oregon

Table 56: Site Creation for Second Site *(Continued)*

Fields	Value
Secondary service location	jsec-oregon
Number of Users	10
Name	spoke2-site
Country	Germany
Protected networks	10.88.88.0/24 (LAN network)

Table 57: Traffic Forwarding for Second Site

Field	Value
Tunnel type	IPsec
IP address type	Dynamic
IPsec profile	default-ipsec
Pre-shared key	Define a unique PSK for each site. Example: Juniper!1
IKE ID	site2@example.com (resembles an email address and must be a unique value for each site).

b. Select **Devices Type=Non-Juniper Device** .

c. Create a third site with details as provided in No Link Title and No Link Title.

Table 58: Create a Third Site: Site Details

Fields	Value
Primary service location	jsec-oregon
Secondary service location	jsec-ohio

Table 58: Create a Third Site: Site Details *(Continued)*

Fields	Value
Number of Users	10
Name	spoke3-site
Country	Germany
Protected networks	10.77.77.0/24 (LAN network)

Table 59: Create a Third Site: Traffic-Forwarding Details

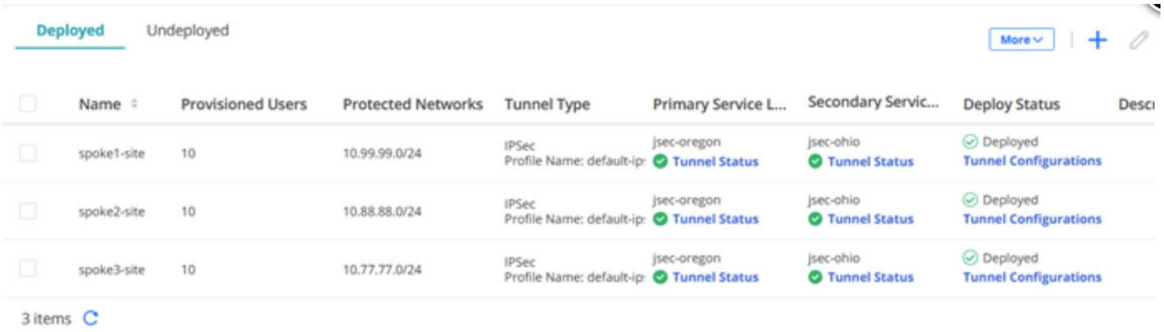
Field	Value
Tunnel type	IPsec
IP address type	Dynamic
IPsec profile	default-ipsec
Pre-shared key	Define a unique PSK for each site. Example: Juniper!1
IKE ID	site3@example.com (Resembles an email address and must be a unique value for each site).

d. Select **Devices Type**=**Non-Juniper Device** .

12. Review the **Summary** page. Modify any incorrect entries.

    Figure 366 on page 464 displays the list of sites you created.

Figure 366: Summary of Created Sites



□	Name	Provisioned Users	Protected Networks	Tunnel Type	Primary Service L...	Secondary Servic...	Deploy Status	Desc
□	spoke1-site	10	10.99.99.0/24	IPSec Profile Name: default-ip	jsec-oregon ✓ Tunnel Status	jsec-ohio ✓ Tunnel Status	✓ Deployed Tunnel Configurations	
□	spoke2-site	10	10.88.88.0/24	IPSec Profile Name: default-ip	jsec-oregon ✓ Tunnel Status	jsec-ohio ✓ Tunnel Status	✓ Deployed Tunnel Configurations	
□	spoke3-site	10	10.77.77.0/24	IPSec Profile Name: default-ip	jsec-oregon ✓ Tunnel Status	jsec-ohio ✓ Tunnel Status	✓ Deployed Tunnel Configurations	

3 items

Deploy a Secure Edge Policy in Juniper Security Director Cloud

Now that you have created sites in Juniper Security Director Cloud, its time to deploy one or more Juniper® Secure Edge policies.

Secure Edge policies specify how the network routes traffic. By default, when you create a new tenant, the Security Director Cloud creates a Secure Edge policy rule set with predefined rules.

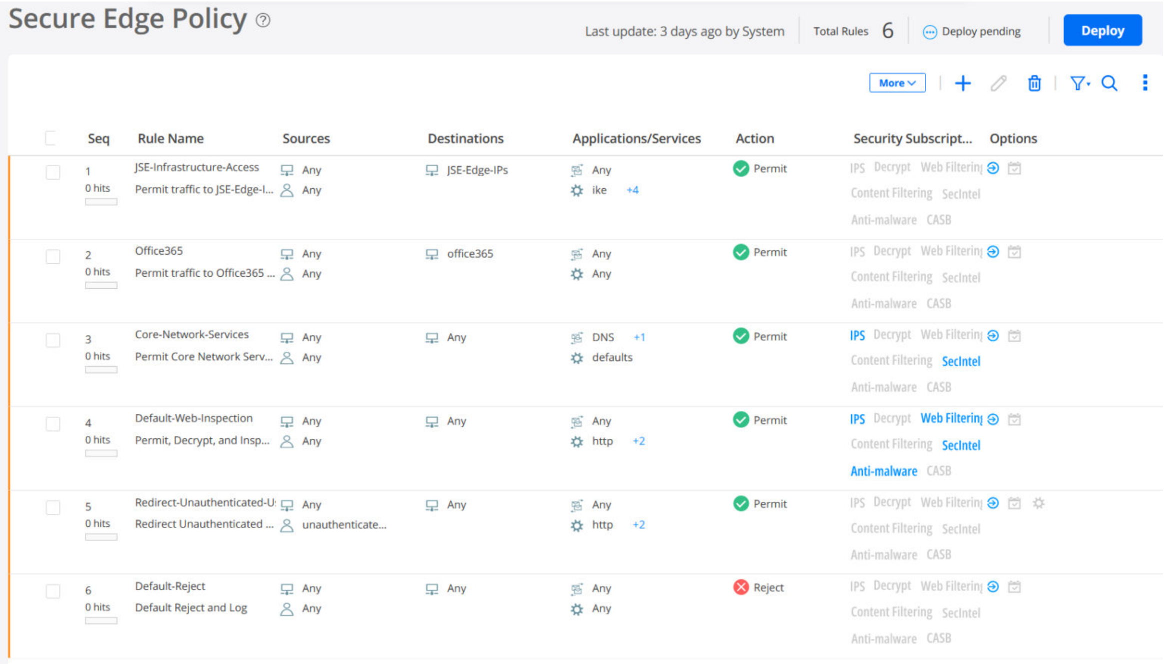
NOTE: Even if you do not change the default rule set, you must use the **Deploy** option to load the rules in your service locations.

To deploy a Secure Edge policy in Juniper Security Director Cloud:

1. In Juniper Security Director Cloud portal, click **Secure Edge** > **Security Policies**.

   A Secure Edge Policy page with default rules appears. You modify the default security policy set for better debugging. The default rule set does not allow ICMP pings to the outside (Internet), preventing you from pinging anything through the cloud.

Figure 367: Secure Edge Policy Details



Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscript...	Options
1 0 hits	JSE-Infrastructure-Access Permit traffic to JSE-Edge-I...	Any Any	JSE-Edge-IPs	Any ike +4	Permit	IPS Decrypt Web Filterin Content Filtering SecIntel Anti-malware CASB	
2 0 hits	Office365 Permit traffic to Office365 ...	Any Any	office365	Any Any	Permit	IPS Decrypt Web Filterin Content Filtering SecIntel Anti-malware CASB	
3 0 hits	Core-Network-Services Permit Core Network Serv...	Any Any	Any	DNS +1 defaults	Permit	IPS Decrypt Web Filterin Content Filtering SecIntel Anti-malware CASB	
4 0 hits	Default-Web-Inspection Permit, Decrypt, and Insp...	Any Any	Any	Any http +2	Permit	IPS Decrypt Web Filterin Content Filtering SecIntel Anti-malware CASB	
5 0 hits	Redirect-Unauthenticated-U: Redirect Unauthenticated ...	Any unauthenticate...	Any	Any http +2	Permit	IPS Decrypt Web Filterin Content Filtering SecIntel Anti-malware CASB	
6 0 hits	Default-Reject Default Reject and Log	Any Any	Any	Any Any	Reject	IPS Decrypt Web Filterin Content Filtering SecIntel Anti-malware CASB	

2. Click the Add (+) icon to create a rule, or select the existing rule and click the pencil icon to edit the rule.
3. Give the new rule the **Rule Name**=Allow-ICMP.
4. Click Add (+) to add sources.

   Under **Sources**, use the following default values:

   - **Addresses**=Any
   - **User Groups**=Any
5. Click Add (+) to add destinations.

   Under **Destinations**, for **Addresses**, use the default value =Any.
6. Under **Applications/Services**, configure the following values:

   - **Applications**=Any
   - **Services**=Specific (via search)
   - **Specific Service**=icmp-all

   Using the Right Arrow (>), move **specific service=icmp-all** to the right pane to activate it before you click **OK**.
7. Configure **Action**=Permit, and retain the default values for the remaining fields.

   The system places the new rule at the bottom of the rules list and treats this rule as the last rule in the rule set. If the rule is placed after a global rule (that denies all traffic), it will never get applied, because the global rule stops all further traffic. Therefore, for this example you change the position of the rule by selecting the rule. Then, use the **Move** > **Move** > **Move Top** options to move the selected rule to the top of the rule set. Moving the rule to the top of the rule set ensures that the system applies this rule first.

> **NOTE**: Whenever you modify a rule set, ensure that you use the **Deploy** button to complete the task. Otherwise, service locations continue to use the outdated rule sets.

8. Click **Deploy**.
9. On the **Deploy** page, check the **Run now** option and click **OK**.

   Service locations get the updated rule set after few minutes.
10. Select **Administration** > **Jobs** to view the status and progress of the deployed job.

Get IPsec Tunnel Configuration Parameters to Apply in Juniper Security Director Cloud

In the preceding tasks, you completed several actions to set up an IPsec tunnels in Juniper Secure Edge and have deployed the Secure Edge policy in Juniper Security Director Cloud. The final step in Security Director Cloud is to collect configuration data for each site. You'll need these details to complete the secure edge connector configuration ("Create Secure Edge Connectors in the Juniper Mist Cloud Portal" on page 469) in the Juniper Mist™ cloud to set up an IPsec tunnel. In this step, you'll note down the details of the sites you created.

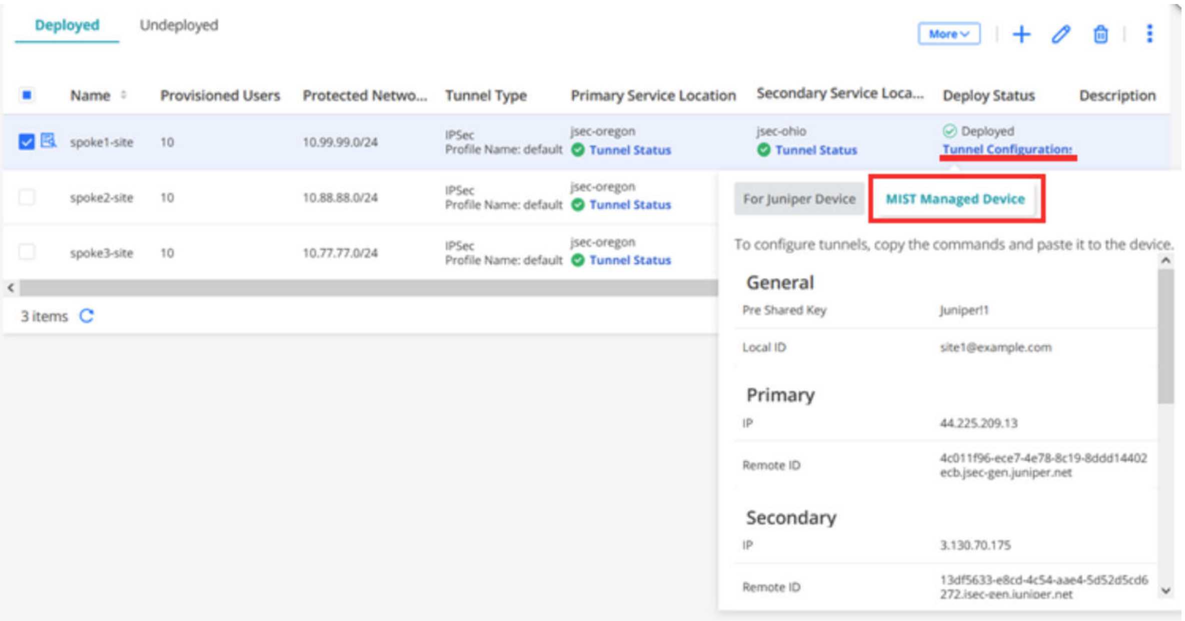
> **NOTE**: An automated configuration push to synchronize between Juniper Security Director Cloud and Juniper Mist cloud option not available.

To get IPsec tunnel configuration parameters to apply in Juniper Security Director Cloud:

1. In Juniper Security Director Cloud portal, select **Secure Edge** >**Service Management** > **Sites**.

   The Site page opens, displaying deployed site details.

Figure 368: Tunnel Configuration Details



■	Name	Provisioned Users	Protected Netwo...	Tunnel Type	Primary Service Location	Secondary Service Loca...	Deploy Status	Description
☑	spoke1-site	10	10.99.99.0/24	IPSec Profile Name: default	jsec-oregon ✓ Tunnel Status	jsec-ohio ✓ Tunnel Status	✓ Deployed Tunnel Configuration:	
□	spoke2-site	10	10.88.88.0/24	IPSec Profile Name: default	jsec-oregon ✓ Tunnel Status			
□	spoke3-site	10	10.77.77.0/24	IPSec Profile Name: default	jsec-oregon ✓ Tunnel Status			

For Juniper Device | MIST Managed Device

To configure tunnels, copy the commands and paste it to the device.

General

Pre Shared Key	Juniper!1
Local ID	site1@example.com

Primary

IP	44.225.209.13
Remote ID	4c011f96-ece7-4e78-8c19-8ddd14402 ecb.jsec-gen.juniper.net

Secondary

IP	3.130.70.175
Remote ID	13df5633-e8cd-4c54-aae4-5d52d5cd6 272.isec-een.iunioer.net

2. For each spoke site, click the **Tunnel Configuration** option under **Deployed Status**, and then check the **MIST Managed Device** tab for information.

   Note down the following details, which you will use in "Create Secure Edge Connectors in the Juniper Mist Cloud Portal" on page 469:

   - Pre-Shared Key
   - Local ID
   - IP address and remote ID of each service location tunnel

   he following samples show extracted information for all three sites you created in "Create a Site in Juniper Secure Edge Cloud" on page 456:

```
General spoke1-site

Pre Shared Key    abc!1
Local ID  site1@example.com

Primary
IP        44.225.209.13
Remote ID xxx123-exx7-xxyys-8c19-abcd123.123.juniper.net

Secondary
IP          3.130.70.175
```

```
Remote ID abc123-exx7-xxyys-8c19-abcd123.123.juniper.net


IKE Proposals
Authentication Method pre-shared-keys
DH group  group14
Encryption algorithm  aes-128-gcm
Lifetime  86400

IPsec Proposals
Protocol  esp
Encryption algorithm  aes-128-gcm
Lifetime  3600
PFS Group group14
```

The following sample is of the extracted information for site2:

```
General spoke2-site

Pre Shared Key abc!1
Local ID site2@example.com

Primary
IP 3.130.70.175
Remote ID xxx123-exx7-xxyys-8c19-abcd123.123.juniper.net


Secondary
IP 44.225.209.13
Remote ID abc123-exx7-xxyys-8c19-abcd123.123.juniper.net

IKE Proposals
Authentication Method pre-shared-keys
DH group group14
Encryption algorithm aes-128-gcm
Lifetime 86400

IPsec Proposals
Protocol esp
Encryption algorithm aes-128-gcm
```

```
Lifetime 3600
PFS Group group14
```

The following sample is of the extracted information for site3:

```
General spoke3-site

Pre Shared Key abc!1
Local ID site3@example.com

Primary
IP 44.225.209.13
Remote ID xxx123-exx7-xxyys-8c19-abcd123.123.juniper.net



Secondary
IP 3.130.70.175
Remote ID abc123-exx7-xxyys-8c19-abcd123.123.juniper.net



IKE Proposals
Authentication Method pre-shared-keys
DH group group14
Encryption algorithm aes-128-gcm
Lifetime 86400

IPsec Proposals
Protocol esp
Encryption algorithm aes-128-gcm
Lifetime 3600
PFS Group group14
```

You need these site details when you configure tunnels in the Mist cloud portal.

Create Secure Edge Connectors in the Juniper Mist Cloud Portal

You are about halfway to your ultimate goal of setting up a Secure Edge connector for the Session Smart Routers or SRX Series Firewalls in Juniper Mist™.

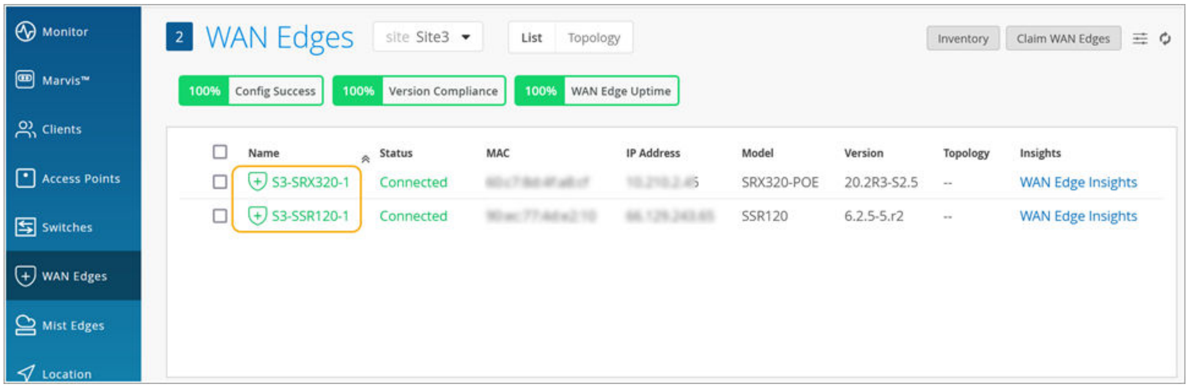
You create Secure Edge connectors in the Juniper Mist cloud portal. This task completes the configuration on the Mist cloud side of the tunnels to establish an IPsec tunnel between WAN edge devices managed by Mist and Security Director Cloud. Before you create the connectors, ensure that your site has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

To create Secure Edge connectors:

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

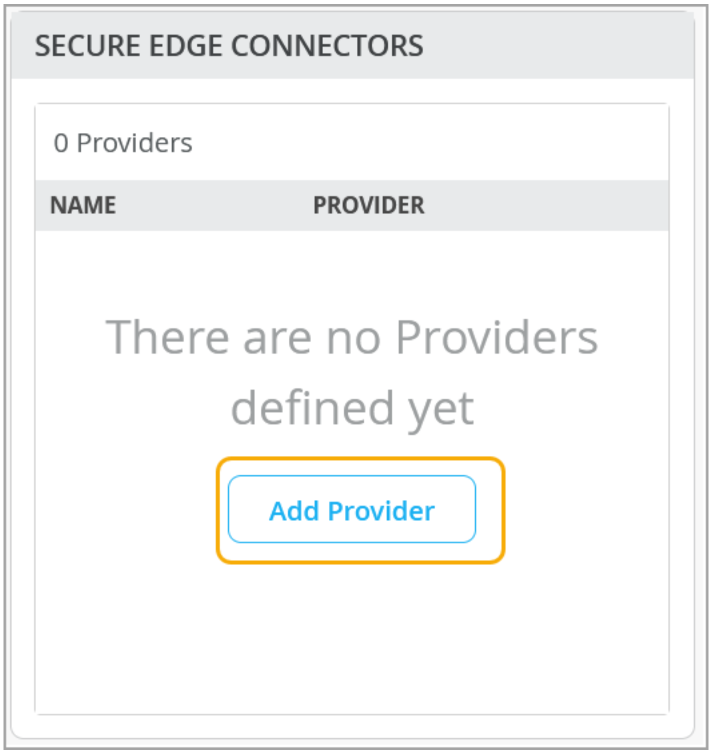
   The WAN Edges page displays site details.

Figure 369: Configure WAN Edge



□	Name	Status	MAC	IP Address	Model	Version	Topology	Insights
□	S3-SRX320-1	Connected	[redacted]	[redacted]	SRX320-POE	20.2R3-S2.5	--	WAN Edge Insights
□	S3-SSR120-1	Connected	[redacted]	[redacted]	SSR120	6.2.5-5.r2	--	WAN Edge Insights

2. Click the device and scroll down to Secure Edge Connectors.



SECURE EDGE CONNECTORS

0 Providers

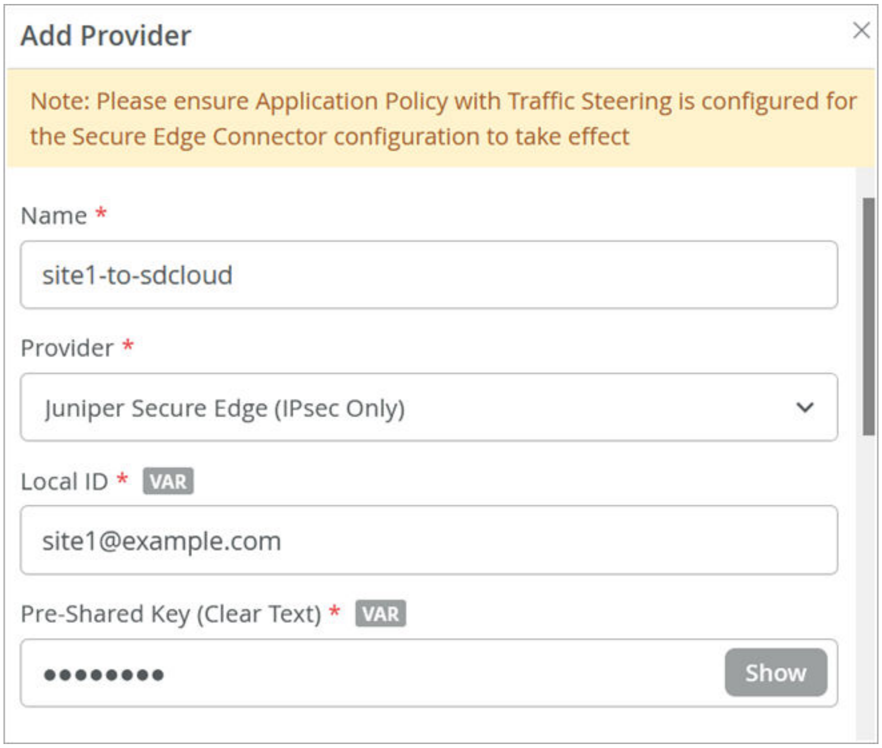
NAME	PROVIDER

There are no Providers defined yet

3. In the **Secure Edge Connectors** pane, click **Add Provider**.
4. Enter Secure Edge connector details.

> **NOTE**: Remember that these are same the details you gathered in "Get IPsec Tunnel Configuration Parameters to Apply in Juniper Security Director Cloud" on page 466.

Figure 370: Secure Edge Connector Configuration



Add Provider

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

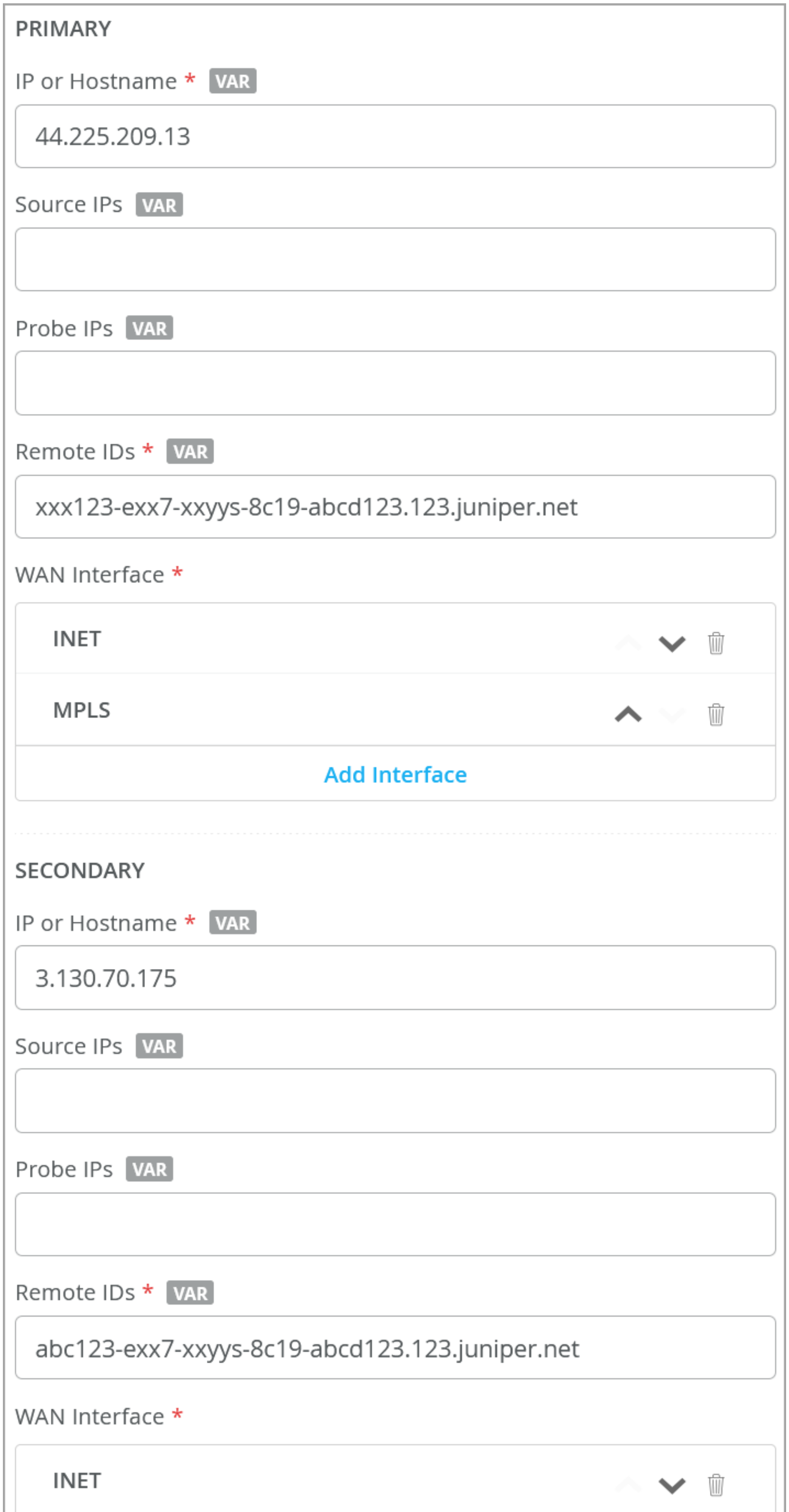
Name *
site1-to-sdcloud

Provider *
Juniper Secure Edge (IPsec Only)

Local ID * VAR
site1@example.com

Pre-Shared Key (Clear Text) * VAR
●●●●●●●● Show

Figure 371: Secure Edge Connector Configuration (Continued)



PRIMARY

IP or Hostname * VAR

44.225.209.13

Source IPs VAR

Probe IPs VAR

Remote IDs * VAR

xxx123-exx7-xxyys-8c19-abcd123.123.juniper.net

WAN Interface *

INET

MPLS

SECONDARY

IP or Hostname * VAR

3.130.70.175

Source IPs VAR

Probe IPs VAR

Remote IDs * VAR

abc123-exx7-xxyys-8c19-abcd123.123.juniper.net

WAN Interface *

INET

Table 60: Secure Edge Connector Details

Field	Value
Name	site1-to-sdcloud
Provider	Juniper Secure Edge
Local ID	site1@example.com
Pre-Shared Key	Juniper!1 (example)
Primary	
IP or Hostname	<IP address> (from Juniper Security Director Cloud tunnel configuration)
Probe IPs	-
Remote ID	<UUID>.jsec-gen.juniper.net (from Juniper Security Director Cloud tunnel configuration)
WAN Interface	• WAN0=INET • WAN1=MPLS
Secondary	
IP or Hostname	<IP address> from (From Juniper Security Director Cloud tunnel configuration)
Probe IPs	-
Remote ID	<UUID>.jsec-gen.juniper.net (from Juniper Security Director Cloud tunnel configuration)
WAN Interface	• WAN0=INET • WAN1=MPLS

Table 60: Secure Edge Connector Details *(Continued)*

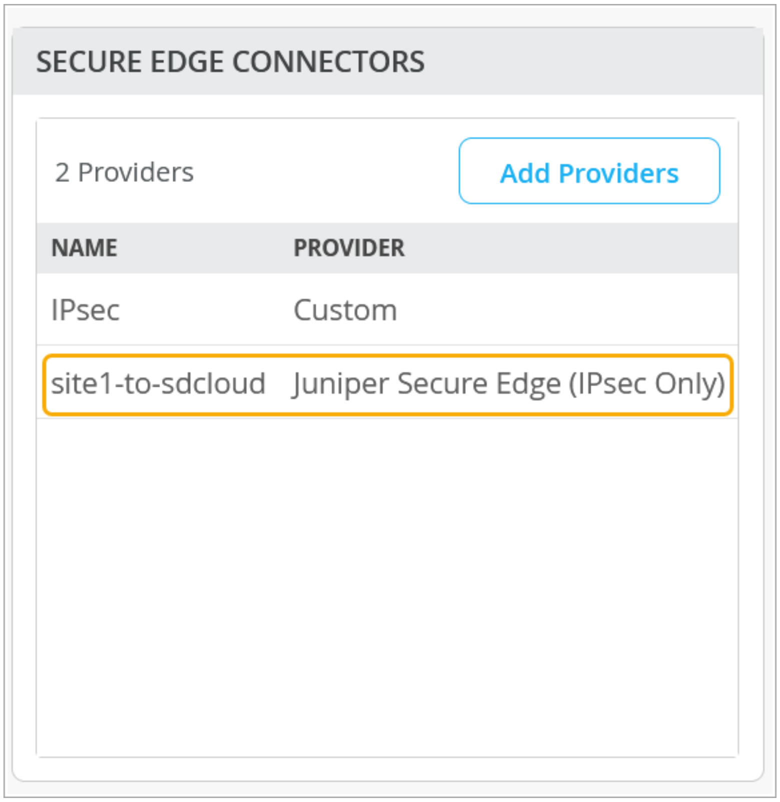
Field	Value
Mode	Active-standby

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

NOTE: Do not enable ICMP **Probe IPs** for Session Smart Router-based Secure Edge configuration. ICMP probes will be sourced from a nonroutable IP address toward the Secure Edge and dropped due to policy. In addition, if the source addresses are overlapping at all branches, routing to more than one branch with a probe IP address is not supported.

NOTE: The system generates text, application, and email descriptions automatically.

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



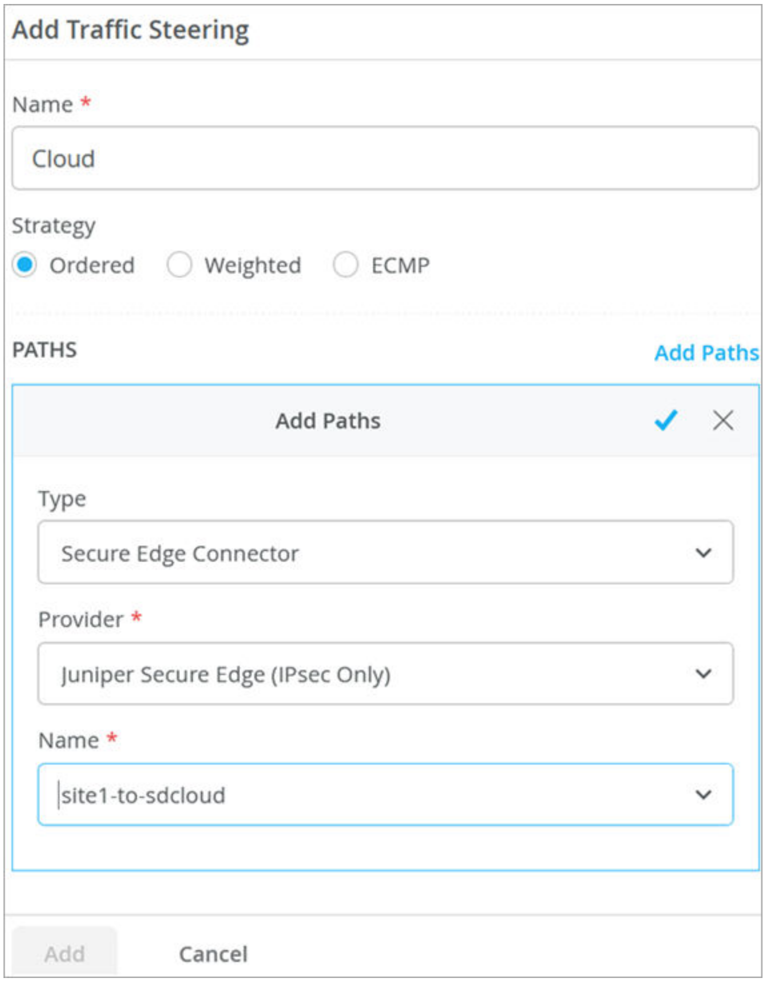
SECURE EDGE CONNECTORS

2 Providers

NAME	PROVIDER
IPsec	Custom
site1-to-sdcloud	Juniper Secure Edge (IPsec Only)

6. Add a new traffic-steering path on the WAN edge template or WAN edge device.

Figure 372: Add Traffic-Steering Options for Secure Edge



Add Traffic Steering

Name *

Cloud

Strategy

● Ordered ○ Weighted ○ ECMP

PATHS

Add Paths

Add Paths ✓ ✕

Type

Secure Edge Connector

Provider *

Juniper Secure Edge (IPsec Only)

Name *

site1-to-sdcloud

Add Cancel

Table 61: Traffic-Steering Path Configuration

Fields	Value
Name	Cloud
Strategy	Ordered
Paths	Select Type and Destination
Type	Secure Edge Connector

Table 61: Traffic-Steering Path Configuration *(Continued)*

Fields	Value
Provider	Juniper Secure Edge
Name	site1-to-sdcloud

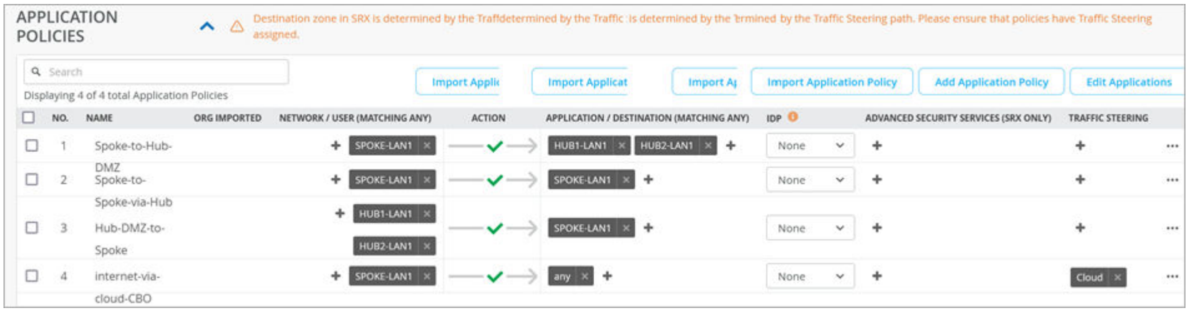
Modify an Application Policy

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.

Use the following steps to confirm if the configuration is working:

1. Add or edit an Application Policy on the WAN edge template or WAN edge device page.
2. Select the policy that you want to modify, and apply the changes.

Figure 373: Change Application Policies



Destination zone in SRX is determined by the Traffdetermined by the Traffic is determined by the ermined by the Traffic Steering path. Please ensure that policies have Traffic Steering assigned.

Displaying 4 of 4 total Application Policies

☐	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	ADVANCED SECURITY SERVICES (SRX ONLY)	TRAFFIC STEERING	
☐	1	Spoke-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 ×	···

If you are creating policies from the WAN edge device page, you ay want to select the **Override Template Settings** option as per requirement.

- In the application policy, you can include the traffic steering you have created in the previous step. In this example, change the **Traffic Steering** to **Cloud** in the last rule (Internet-via-Cloud-CBO).

3. Save the 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.

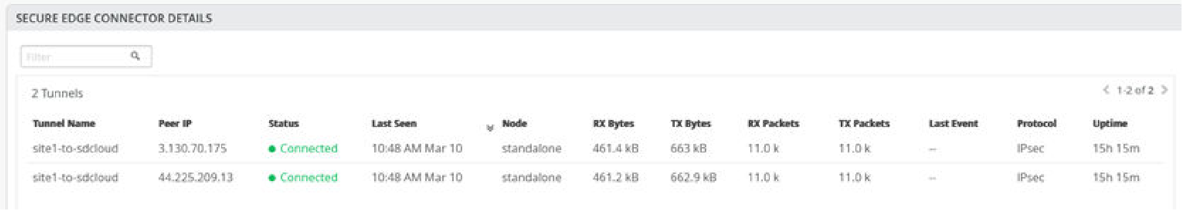
To verify the configuration:

1. (Optional) Depending on your environment, you can see the communication of the IPsec tunnel towards Juniper Security Director Cloud in CLI.

```
user@host:~# tcpdump -eni fabric6 port 4500
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on fabric6, link-type EN10MB (Ethernet), capture size 262144 bytes
18:43:46.835469 52:54:00:f4:02:77 > 52:54:00:14:07:6c, ethertype IPv4 (0x0800), length 317:
192.168.173.191.16534 > 44.225.209.13.4500: NONESP-encap: isakmp: child_sa ikev2_auth[I]
18:43:46.879282 52:54:00:f4:02:77 > 52:54:00:14:07:6c, ethertype IPv4 (0x0800), length 317:
192.168.173.191.16535 > 3.130.70.175.4500: NONESP-encap: isakmp: child_sa ikev2_auth[I]
18:43:46.884834 52:54:00:14:07:6c > 52:54:00:f4:02:77, ethertype IPv4 (0x0800), length 292:
44.225.209.13.4500 > 192.168.173.191.16534: NONESP-encap: isakmp: child_sa ikev2_auth[R]
18:43:46.974426 52:54:00:14:07:6c > 52:54:00:f4:02:77, ethertype IPv4 (0x0800), length 292:
3.130.70.175.4500 > 192.168.173.191.16535: NONESP-encap: isakmp: child_sa ikev2_auth[R]
18:43:58.001576 52:54:00:14:07:6c > 52:54:00:f4:02:77, ethertype IPv4 (0x0800), length 103:
44.225.209.13.4500 > 192.168.173.191.16534: NONESP-encap: isakmp: parent_sa inf2
18:43:58.002603 52:54:00:f4:02:77 > 52:54:00:14:07:6c, ethertype IPv4 (0x0800), length 103:
192.168.173.191.16534 > 44.225.209.13.4500: NONESP-encap: isakmp: parent_sa inf2[IR]
18:44:06.111512 52:54:00:14:07:6c > 52:54:00:f4:02:77, ethertype IPv4 (0x0800), length 103:
3.130.70.175.4500 > 192.168.173.191.16535: NONESP-encap: isakmp: parent_sa inf2
18:44:06.112368 52:54:00:f4:02:77 > 52:54:00:14:07:6c, ethertype IPv4 (0x0800), length 103:
192.168.173.191.16535 > 3.130.70.175.4500: NONESP-encap: isakmp: parent_sa inf2[IR]
18:44:06.896312 52:54:00:f4:02:77 > 52:54:00:14:07:6c, ethertype IPv4 (0x0800), length 103:
192.168.173.191.16534 > 44.225.209.13.4500: NONESP-encap: isakmp: child_sa inf2[I]
18:44:06.922069 52:54:00:14:07:6c > 52:54:00:f4:02:77, ethertype IPv4 (0x0800), length 103:
44.225.209.13.4500 > 192.168.173.191.16534: NONESP-encap: isakmp: child_sa inf2[R]
18:44:07.022463 52:54:00:f4:02:77 > 52:54:00:14:07:6c, ethertype IPv4 (0x0800), length 103:
192.168.173.191.16535 > 3.130.70.175.4500: NONESP-encap: isakmp: child_sa inf2[I]
18:44:07.022502 52:54:00:14:07:6c > 52:54:00:f4:02:77, ethertype IPv4 (0x0800), length 43:
44.225.209.13.4500 > 192.168.173.191.16534: isakmp-nat-keep-alive
18:44:07.097695 52:54:00:14:07:6c > 52:54:00:f4:02:77, ethertype IPv4 (0x0800), length 103:
3.130.70.175.4500 > 192.168.173.191.16535: NONESP-encap: isakmp: child_sa inf2[R]
18:44:07.113678 52:54:00:14:07:6c > 52:54:00:f4:02:77, ethertype IPv4 (0x0800), length 43:
3.130.70.175.4500 > 192.168.173.191.16535: isakmp-nat-keep-alive
```

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

Figure 374: Secure Edge Connector with Tunnel Details



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.

2. Check the new traffic flow using a VM desktop connected to the branch device. You can verify the traffic flow by using pings to the Internet.

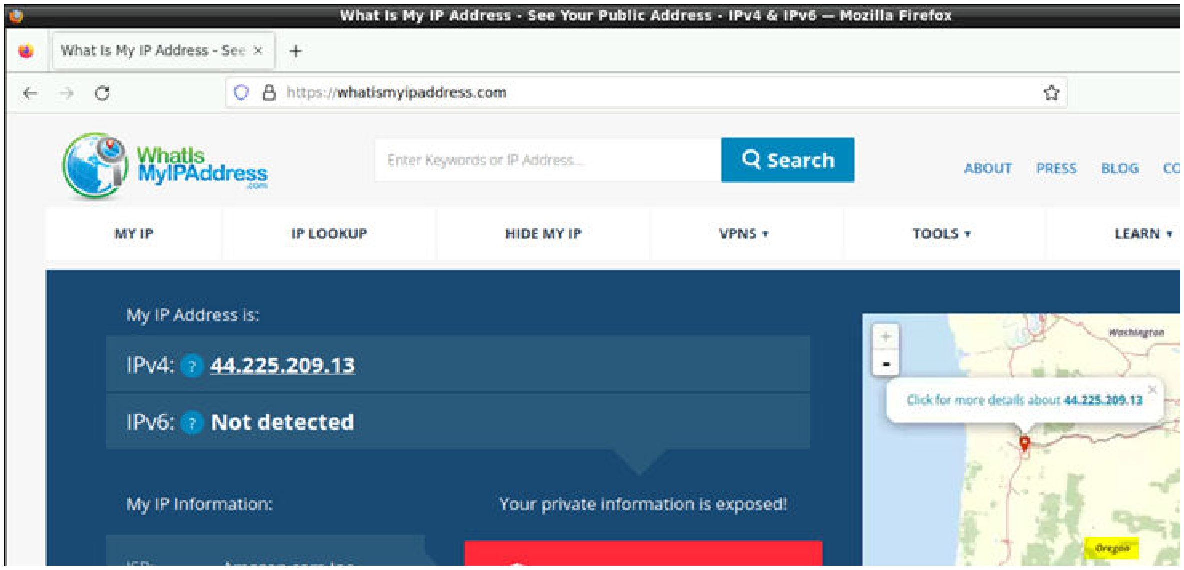
```
root@desktop1:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=100 time=40.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=100 time=39.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=100 time=38.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=100 time=37.9 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 37.942/38.914/40.507/1.059 ms

root@desktop1:~# ping 9.9.9.9
PING 9.9.9.9 (9.9.9.9) 56(84) bytes of data.
64 bytes from 9.9.9.9: icmp_seq=1 ttl=41 time=35.8 ms
64 bytes from 9.9.9.9: icmp_seq=2 ttl=41 time=34.3 ms
64 bytes from 9.9.9.9: icmp_seq=3 ttl=41 time=34.9 ms
64 bytes from 9.9.9.9: icmp_seq=4 ttl=41 time=33.7 ms
^C
--- 9.9.9.9 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 33.722/34.686/35.824/0.782 ms
```

NOTE: You may experience latency depending on the physical distance between your WAN edge device and Juniper Secure Edge service location.

3. Open a browser on a VM desktop 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.

   Figure 375 on page 479 and Figure 376 on page 480 show traffic from the primary and secondary service locations.

Figure 375: Traffic from Primary Service Location


What Is My IP Address - See Your Public Address - IPv4 & IPv6 — Mozilla Firefox
What Is My IP Address - See ×
https://whatismyipaddress.com
WhatIsMyIPAddress.com
Enter Keywords or IP Address...
Search
ABOUT
PRESS
BLOG
CO
MY IP
IP LOOKUP
HIDE MY IP
VPNS ▾
TOOLS ▾
LEARN ▾
Washington
Click for more details about 44.225.209.13
Oregon

My IP Address is:

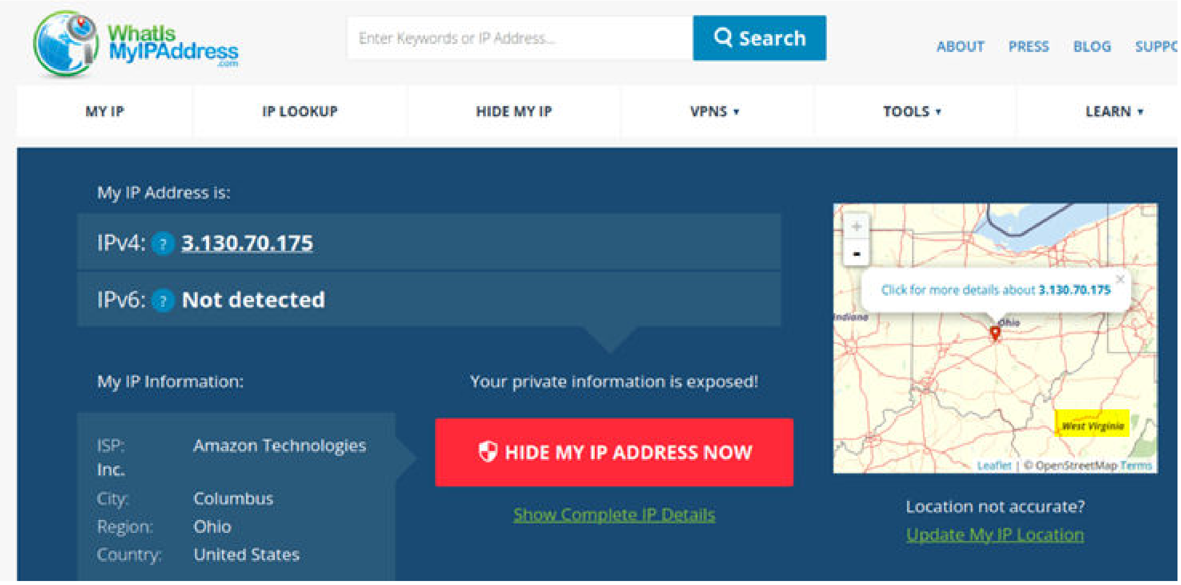
IPv4: 44.225.209.13

IPv6: Not detected

My IP Information:

Your private information is exposed!

Figure 376: 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

Location not accurate?

Update My IP Location

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

- Terminates the IPsec tunnel
- Routes traffic from branch devices to the Internet through Juniper Security Director Cloud

You can view this same public IP address in the packet captures showing established tunnel to the service location using Juniper Security Director Cloud. See "Verify the Configuration" on page 477.

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.

Setup Secure Edge Connector with Juniper Secure Edge (Auto-Provisioning)

IN THIS SECTION

Mist now offers automated Juniper Secure Edge connector tunnel provisioning. This feature allows you to effortlessly establish connections using predefined settings.

Configure Secure Edge Connector Auto-Provisioning

IN THIS SECTION

Prerequisites

- Activate Juniper Secure Edge account and check licenses, subscriptions, certificates. See "Access Juniper Security Director Cloud and Check Active Subscriptions" on page 449 and Figure 356 on page 450 .
- Launch the required number of service locations (with required capacity). See "Configure Service Locations" on page 450.

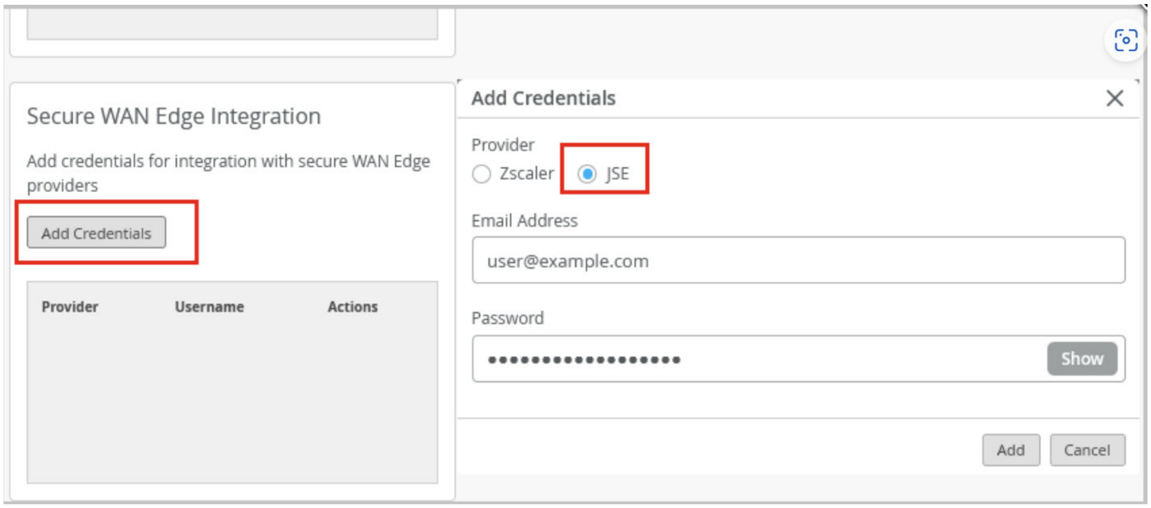
Watch the following video to understand how to setup Secure Edge Connector auto provisioning:

Video: Auto Provision JSE for Session Smart Routers

Add Juniper Secure Edge Connector Credentials in Juniper Mist Portal

1. Provide Juniper Secure Edge credential details in Juniper Mist portal.
   - On Juniper Mist portal, select **Organization** > **Settings**.
   - Scroll-down to **Secure WAN Edge Integration** pane and click **Add Credentials.**
   - In **Add Provider** window, enter the details.

Figure 377: Add Credentials for Juniper Secure Edge



Secure WAN Edge Integration

Add credentials for integration with secure WAN Edge providers

Provider	Username	Actions

Add Credentials

Provider: ○ Zscaler ● JSE

Email Address: user@example.com

Password: ••••••••••••••••••

- Provider—Select JSE.

- Email Address—Enter user name (email address) (Credentials of the user created on the Juniper Secure Edge portal)

- Password—Enter password for the user name.

- Click **Add** to continue.

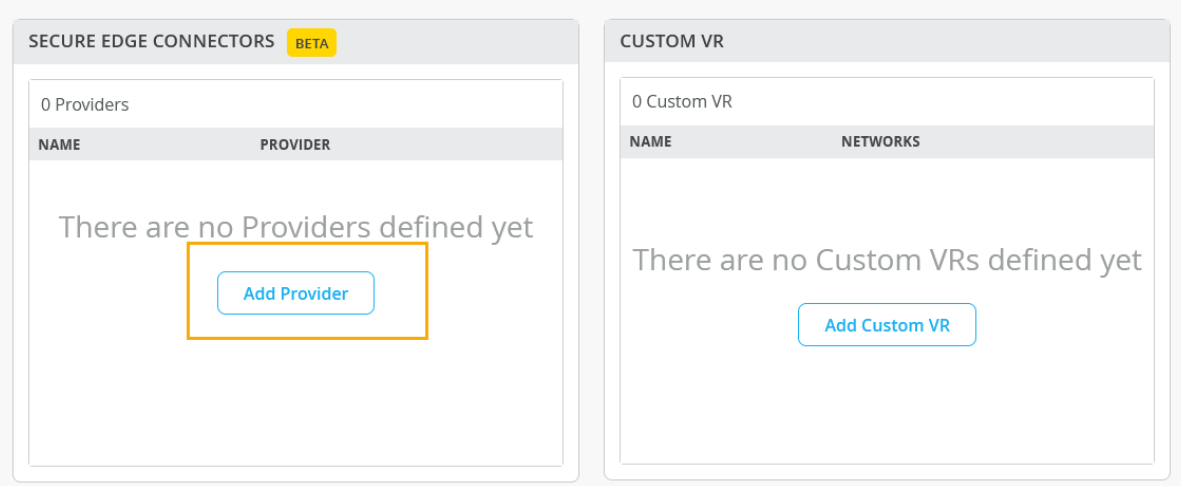
Configure Juniper Secure Edge Tunnel Auto-Provisioning

1. On Juniper Mist portal, go to Organization > WAN Edge Templates and click an existing template.

2. Scroll-down to **Secure Edge Connector**.

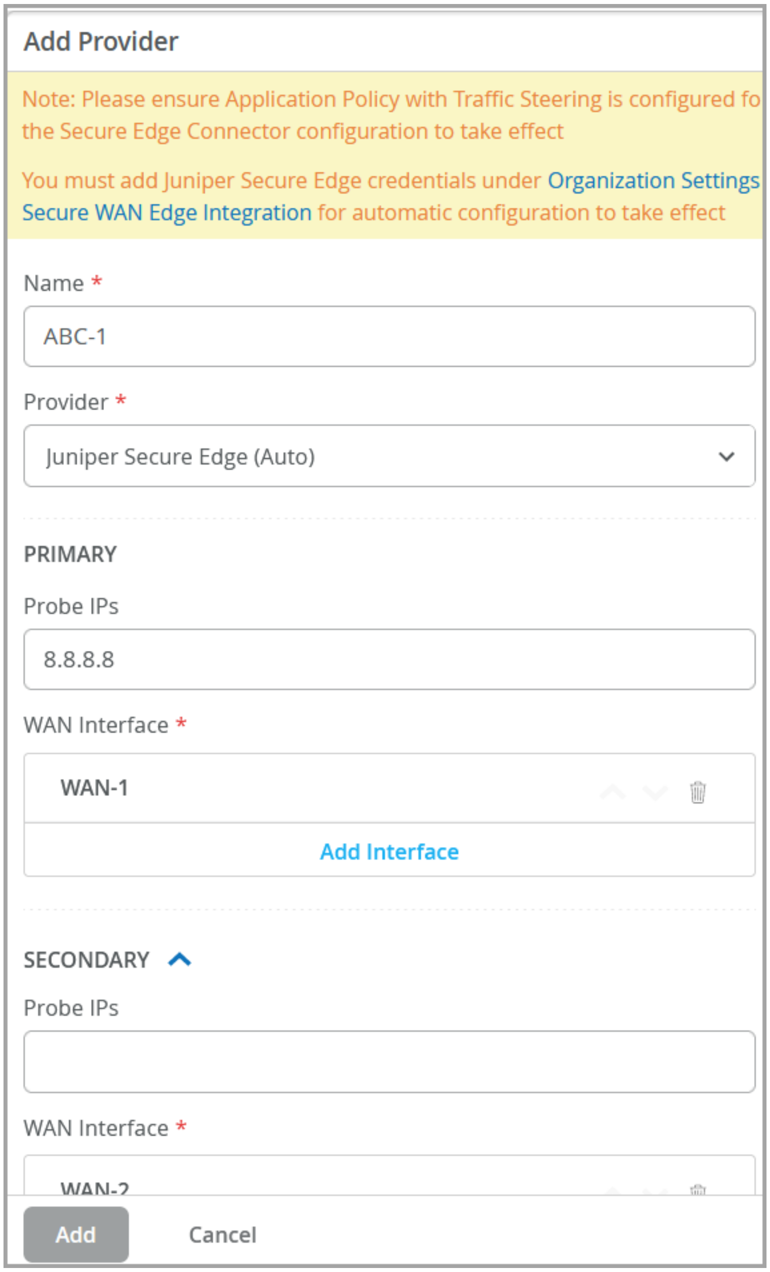
3. Click **Add Providers**

Figure 378: Add Provider



4. In **Add Provider** window, select **Juniper Secure Edge (Auto)** for automatic provisioning.

Figure 379: Select Juniper Secure Edge as Provider



Add Provider

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

You must add Juniper Secure Edge credentials under Organization Settings Secure WAN Edge Integration for automatic configuration to take effect

Name *

ABC-1

Provider *

Juniper Secure Edge (Auto)

PRIMARY

Probe IPs

8.8.8.8

WAN Interface *

WAN-1

SECONDARY

Probe IPs

WAN Interface *

WAN-2

Enter the following details:

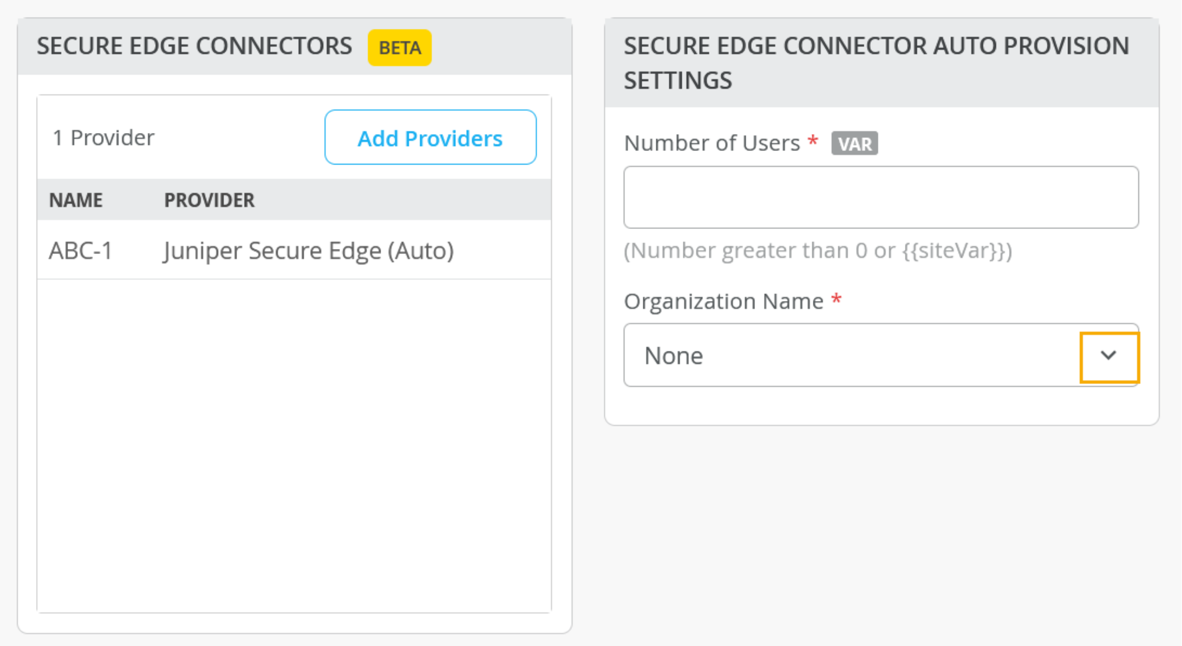
- Name—Enter a name for the JSE tunnel.
- Provider—Select Juniper Secure Edge (Auto).
- Probe IP—Enter probe IPs (primary and secondary). Enter probe IP 8.8.8.8 or any other well-known probe IP address.

- WAN Interface—Assign WAN interfaces under primary and secondary tunnel details for provisioning of primary and secondary tunnels.

5. Click **Add**.

6. In the **Secure Edge Connector Auto Provision Settings**enter the details. This option is available only if you have configured Juniper Secure Edge as provider in the previous step.

Figure 380: Secure Edge Connector Auto Provision Settings



NAME	PROVIDER
ABC-1	Juniper Secure Edge (Auto)

Number of Users * VAR

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

Organization Name *

None

- Number of Users—Enter the maximum number of users supported by the JSE tunnel

- Organization Name—Enter the organization name. The drop-down box displays all organizations associated with the user name in Juniper Secure Edge account. This is the same user name that you have entered in Juniper Secure Edge credential in **Organization** > **Settings**. See step 1 for details.

7. Click **Add** to continue.

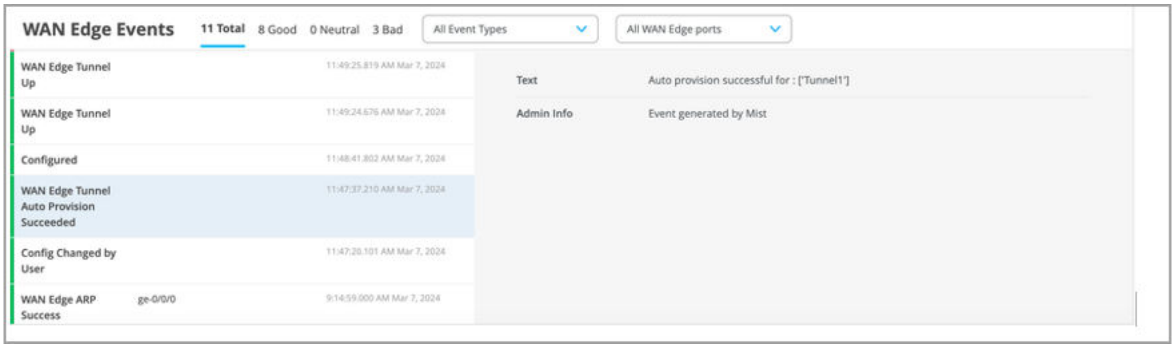
When you assign a template enabled with the Juniper Secure Edge (Auto) option to a site, an associated JSE site (location object) is automatically created and a tunnel from the device to the closest network point of presence (POP) is brought up.

For the Secure Edge Connector configuration to take effect, you must create an application policy with Mist Secure Edge Connector-to-Juniper Secure Edge traffic steering.

Verify Juniper Secure Edge Tunnels

On Juniper Mist portal, you can verify the established tunnels details in WAN Insights of the device once **WAN Edge Tunnel Auto Provision Succeeded** event appears under WAN Edge Events.

Figure 381: WAN Edge Events



WAN Edge Events

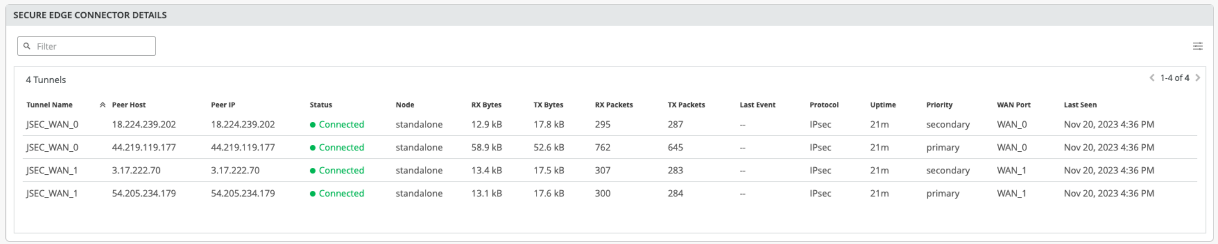
WAN Edge Tunnel Up		11:49:25.819 AM Mar 7, 2024
WAN Edge Tunnel Up		11:49:24.676 AM Mar 7, 2024
Configured		11:48:41.802 AM Mar 7, 2024
WAN Edge Tunnel Auto Provision Succeeded		11:47:37.210 AM Mar 7, 2024
Config Changed by User		11:47:20.101 AM Mar 7, 2024
WAN Edge ARP Success	ge-0/0/0	9:14:59.000 AM Mar 7, 2024

Text: Auto provision successful for : ['Tunnel1']

Admin Info: Event generated by Mist

Get the established tunnels status details in **WAN Edges > WAN Edge Insights** page Juniper Mist cloud portal.

Figure 382: Established Secure Edge Tunnels



SECURE EDGE CONNECTOR DETAILS

4 Tunnels

Tunnel Name	Peer Host	Peer IP	Status	Node	RX Bytes	TX Bytes	RX Packets	TX Packets	Last Event	Protocol	Uptime	Priority	WAN Port	Last Seen
JSEC_WAN_0	18.224.239.202	18.224.239.202	● Connected	standalone	12.9 kB	17.8 kB	295	287	--	IPsec	21m	secondary	WAN_0	Nov 20, 2023 4:36 PM
JSEC_WAN_0	44.219.119.177	44.219.119.177	● Connected	standalone	58.9 kB	52.6 kB	762	645	--	IPsec	21m	primary	WAN_0	Nov 20, 2023 4:36 PM
JSEC_WAN_1	3.17.222.70	3.17.222.70	● Connected	standalone	13.4 kB	17.5 kB	307	283	--	IPsec	21m	secondary	WAN_1	Nov 20, 2023 4:36 PM
JSEC_WAN_1	54.205.234.179	54.205.234.179	● Connected	standalone	13.1 kB	17.6 kB	300	284	--	IPsec	21m	primary	WAN_1	Nov 20, 2023 4:36 PM

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

SEE ALSO

Configure Application Policies on Session Smart Routers | 58

Juniper Mist WAN Assurance Platform Considerations | 10

Introduction to Juniper Mist WAN Assurance | 2

Setup Secure Edge Connector with Custom Provider

IN THIS SECTION

Juniper Mist offers custom option for tunnel provisioning. With minimal configuration, your WAN Edge device can establish connections to the SSE using either IPsec or GRE protocols.

Configure Secure Edge Connector with Custom Option

IN THIS SECTION

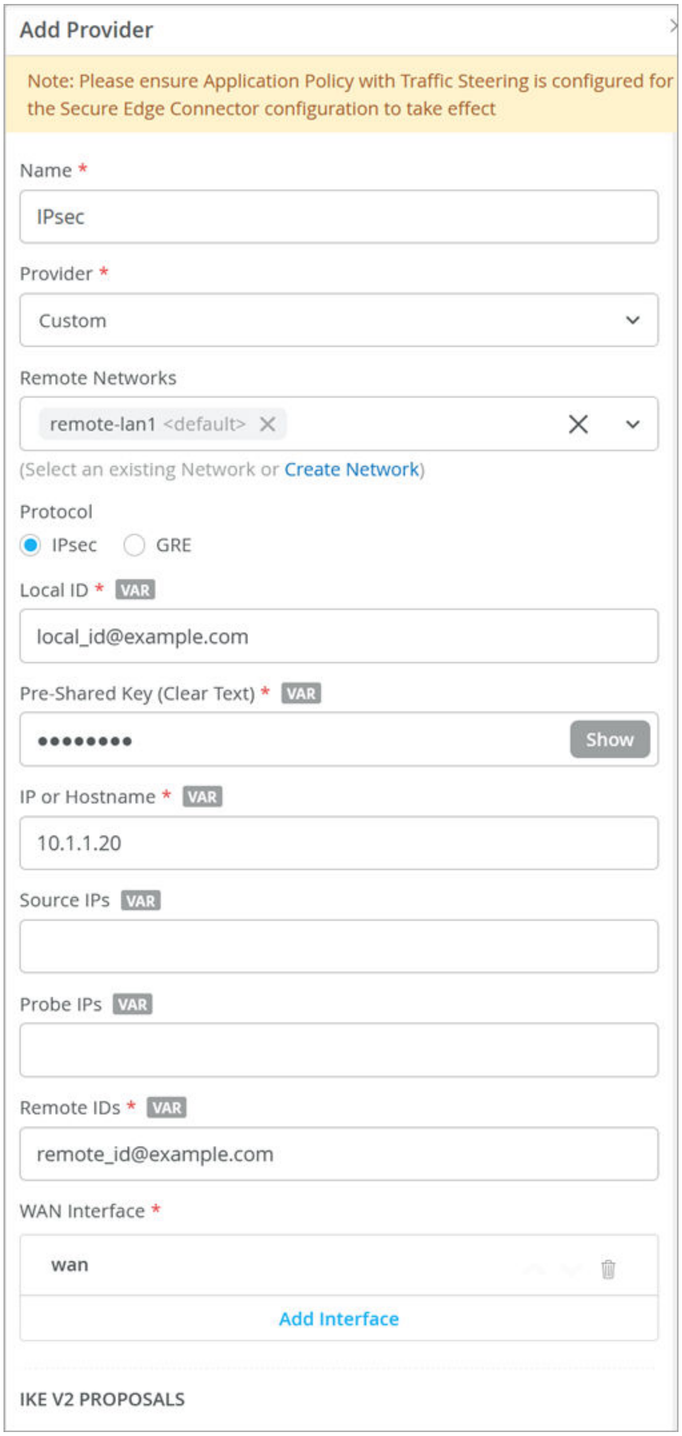
Prerequisites

- Kepp ready local and remote network account details.

Configure Tunnel Provisioning

1. On Juniper Mist portal, go to **Secure Edge Connector** at WAN Edge Templates-level, hub profile, or at Site-level.

Figure 383: Add Provider for Secure Edge Connector



Add Provider

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

Name * IPsec

Provider * Custom

Remote Networks remote-lan1 <default>

(Select an existing Network or Create Network)

Protocol ● IPsec ○ GRE

Local ID * VAR local_id@example.com

Pre-Shared Key (Clear Text) * VAR ●●●●●●●● Show

IP or Hostname * VAR 10.1.1.20

Source IPs VAR

Probe IPs VAR

Remote IDs * VAR remote_id@example.com

WAN Interface * wan

Add Interface

IKE V2 PROPOSALS

2. Click **Add Providers**.

3. In **Add Provider** window, select **Custom** option.

4. Enter the details for provisioning of tunnels.

a. i. **Name**—Enter the name of the service.

ii. **Provider**—Select **Custom**.

iii. **Remote Network**—Select an existing Network or create a network.

iv. **Provider**—Select **IPsec** or **GRE**.

v. For IPsec, enter the following options:

1. **Local ID**—Provide login ID of the local account.
2. **Preshared Key**—Provide preshared key (PSK). The length of the PSK must be between 6-255 characters.
3. **IP or Hostname**—IP address or hostname.
4. **Source IP**—Source IP address of the tunnel.
5. **Probe IPs**—Enter probe IP address. You can use any well-known IP (Example: 8.8.8.8).
6. **Remote ID**—Provide login ID of the remote account.
7. **WAN Interface**—Assign WAN interfaces for provisioning of primary and secondary tunnels. You can add multiple WAN interfaces and the first interface takes the priority. If first interface is down, then system uses the second interface to establish the tunnel.
8. IKEv2 proposal—Retain default values or select **Encryption Algorithm**, **Authentication Algorithm**, **DH Group** from drop-down and enter **Life Time** between 180 to 86400 seconds.
9. IPsec proposal—Retain default values or select **Encryption Algorithm**, **Authentication Algorithm**, **DH Group** from drop-down and enter **Life Time** between 180 to 86400 seconds.

vi. For GRE, enter the following options:

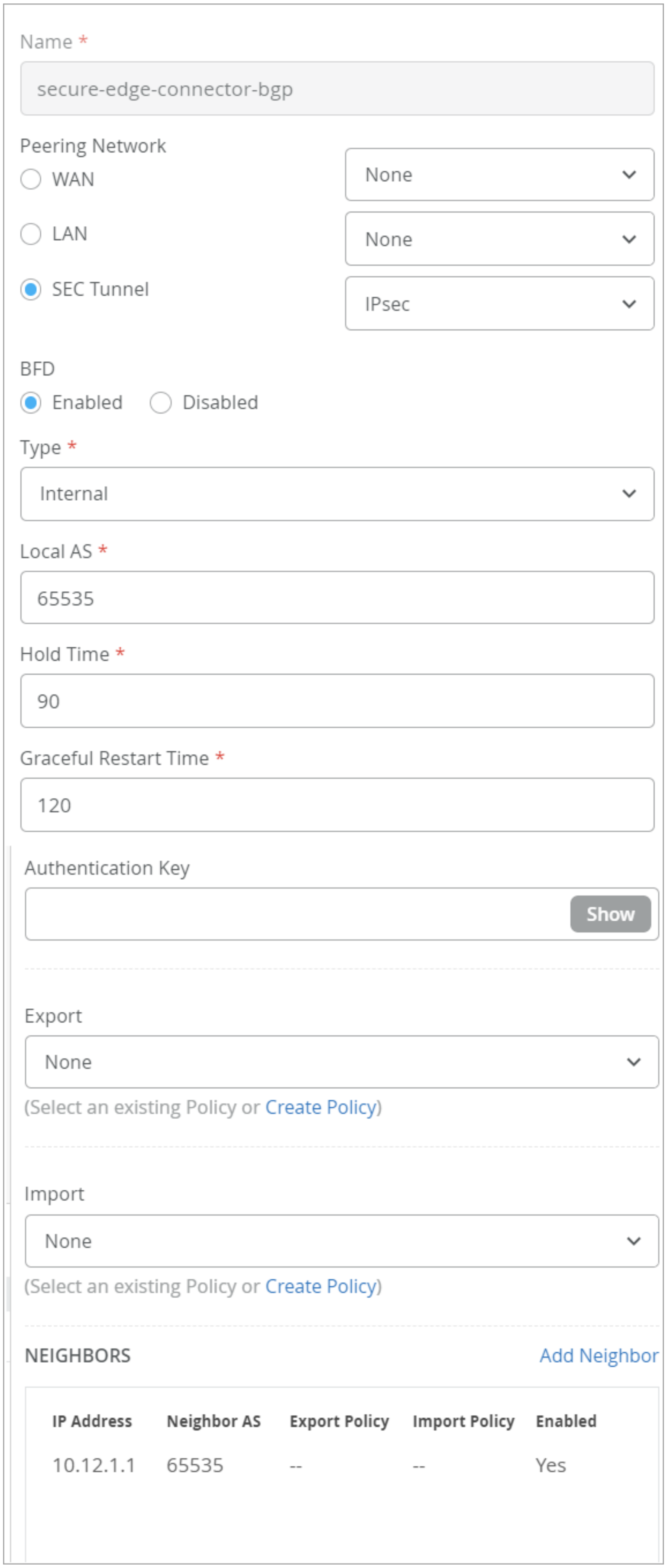
1. **IP or Hostname**—IP addresses or hostname.
2. **Source IP**—Source IP address of the tunnel.
3. **Probe IPs**—Enter probe IP address. You can use any well-known IP (Example: 8.8.8.8).
4. **Remote ID**—Provide login ID of the remote account.
5. **WAN Interface**—Assign WAN interfaces for provisioning of primary and secondary tunnels. You can add multiple WAN interfaces and the first interface takes the priority. If first interface is down, then system uses the second interface to establish the tunnel.

5. Click **Add** to continue.

6. Create new BGP Group.

   a. Scroll down to Routing pane and click **Add BGP Group**.

Figure 384: Add BGP Group



Name *

secure-edge-connector-bgp

Peering Network

○ WAN — None

○ LAN — None

● SEC Tunnel — IPsec

BFD

● Enabled ○ Disabled

Type *

Internal

Local AS *

65535

Hold Time *

90

Graceful Restart Time *

120

Authentication Key

Export

None

(Select an existing Policy or Create Policy)

Import

None

(Select an existing Policy or Create Policy)

NEIGHBORS

IP Address	Neighbor AS	Export Policy	Import Policy	Enabled
10.12.1.1	65535	--	--	Yes

b. In the **Add BGP Group** window, add details for the BGP group

c. For the Peering Network, select the same SEC provider (created in previous steps).

d. For Local AS, enter AS number or non-default AS for WAN Edge.

e. In Neighbors pane, click Add Neighbors.

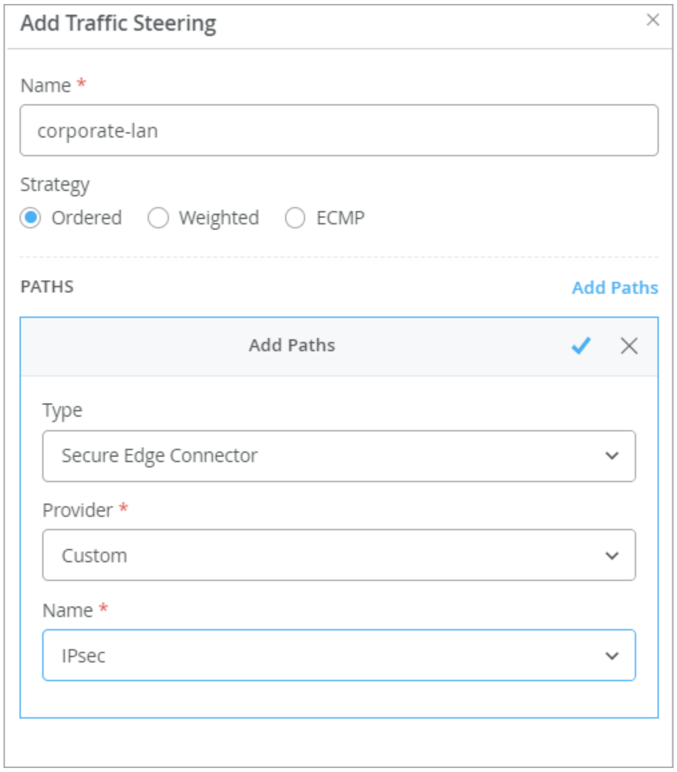
- Add BGP peer IP address of SSE and AS value.

- Optionally, you can add BGP policy for import or export of routes

For instructions to create BGP groups, see Configure BGP Groups.

7. Add a traffic steering profile on the WAN Edge Templates page or on WAN Edge Device page.

Figure 385: Add Traffic Steering for Secure Edge Connector



Name * corporate-lan

Strategy ● Ordered ○ Weighted ○ ECMP

Type Secure Edge Connector

Provider * Custom

Name * IPsec

- Enter the details for the traffic-steering path:

  - **Name**—Enter a name for the traffic-steering profile.

  - **Strategy**—Select a strategy. You can configure the traffic steering profile with any strategy (**Ordered** or **Weighted** or **ECMP**), based on your topology and configuration.

  - **Path**—Click **Add Paths** and enter the following details.

a. **Type**—Select **Secure Edge Connector**.

b. **Provider**—Select **Custom**.

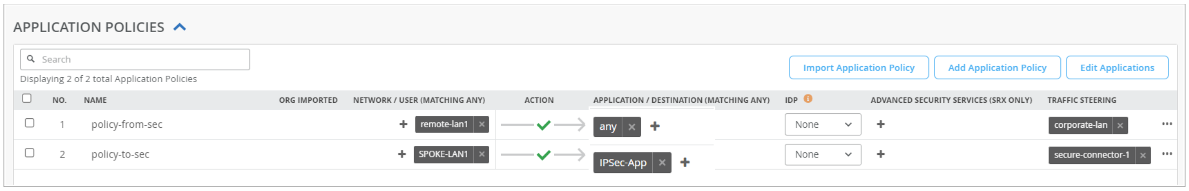
c. **Name**—Select the custom connector's name you have created in previous step.

- Click **Add**.

8. Add an application policy. Application policy allows the desired network to reach the more specific application using the route table. In the application policy, you can include the remote network you have created in the previous step. Use that network in an application policy to allow inbound access from the Secure Edge Connector. To create the application policy, in the Juniper Mist cloud portal, go to **Organization** > **WAN** > **Application Policy**.

   Following image shows an example of application policy with traffic steering configured in previous step.

Figure 386: Create Application Policies for Secure Edge Connectors



APPLICATION POLICIES

Search

Displaying 2 of 2 total Application Policies

☐	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	ADVANCED SECURITY SERVICES (SRX ONLY)	TRAFFIC STEERING
☐	1	policy-from-sec		remote-lan1	✓	any	None		corporate-lan
☐	2	policy-to-sec		SPOKE-LAN1	✓	IPSec-App	None		secure-connector-1

For instructions to create Application Policies, see Configure Application Policies .

Verification

On Juniper Mist portal, you can verify the established tunnels details in WAN Insights of the device once **WAN Edge Tunnel Auto Provision Succeeded** event appears under WAN Edge Events.

Once you update the template, the IPsec configuration will be pushed to the WAN Edge device. For first time IPSec deployment, the system takes time to download the software and configuration.

Once the IPSec configuration has been deployed, you can see the IPsec status by navigating to **WAN Edge** > ***WAN Edge Name*** > Secure Edge Connector Details.

You can view BGP neighbor status by navigating to **Monitor** > **Insights** > **WAN Edge**.

You can view learned routes by navigating to **WAN Edge** > **Utilities** > **Testing Tools** > **Routes** > **Show Routes**.

Related Topics

SEE ALSO

- Configure WAN Edge Templates for SRX Series Firewalls | 217
- Configure Hub Profiles for SRX Series Firewalls | 197
- WAN Assurance Configuration Overview | 166
- No Link Title
- No Link Title

Zscaler Integration

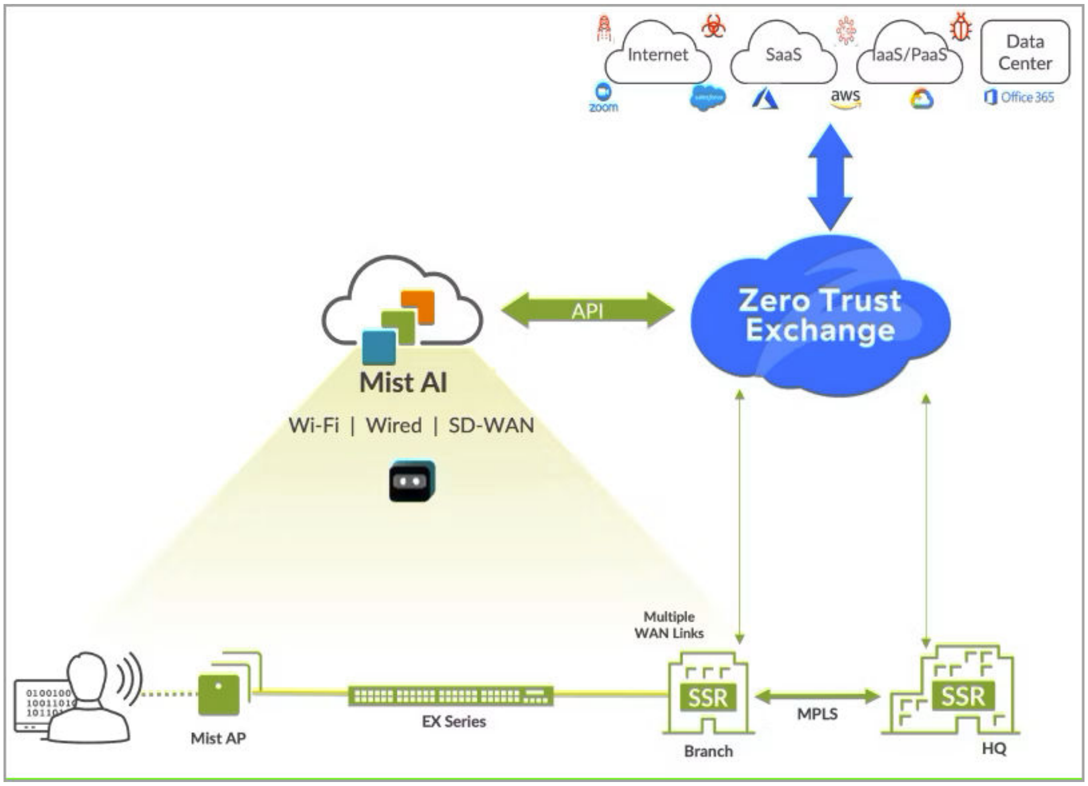
IN THIS SECTION

Juniper Mist™ provides pre-built connectors specifically designed for the Juniper Networks® SRX Series Firewalls and Juniper® Session Smart™ Routers deployed as WAN edge devices. These connectors facilitate seamless integration with your Secure Edge (SSE) deployments. With minimal configuration, you can integrate the SSE into the Juniper Mist portal. As a result, your WAN Edge device establishes connections to the SSE using either IPsec or GRE protocols.

Overview

Juniper SD-WAN with Mist AI enhances security, and integration with Zscaler offers a top-notch SASE solution for secure access across locations. Zscaler provides comprehensive cyber-security and zero trust connectivity, all integrated seamlessly with Juniper Mist Cloud.

Figure 387: Juniper Mist Integration with Zscaler



To improve cloud-to-cloud connectivity, Mist now offers automated Zscaler tunnel provisioning. WAN Assurance delivers an easy-to-use workflow for default Zscaler connections. This integration allows you to effortlessly establish connections from your devices using predefined settings. Juniper Mist Cloud portal allows simplified configuration and management of Zscaler Security Service Edge (SSE) connections—eliminating the need for additional platform logins.

Note the following about Zscaler tunnel provisioning:

- Automatic provisioning supports only IPsec tunnels.
- The tunnel auto provision process includes the creation of a new Zscaler location and VPN credential objects in the Zscaler cloud. These Zscaler resources will be deleted when the associated tunnel provider is removed from the Mist.
- Each auto orchestration requires the creation of one primary tunnel and one secondary tunnel.

Read the following topics to understand how to set up Zscaler tunnel configuration from the Juniper Mist Cloud.

Zscaler Manual Provisioning of Tunnels

IN THIS SECTION

Prerequisites

For IPsec Tunnels

- Zscaler cloud account
- Local ID and pre-shared key (PSK) configured from the Zscaler account. Ensure that you set the length of PSK between 6 to 255 characters.
- IP addresses or hostnames of the Zscaler public service edges tunnels (primary and secondary). See Locating the Hostnames and IP Addresses of Zscaler Enforcement Nodes (ZENs).
- Check Configuring an IPSec VPN Tunnel.

For GRE Tunnels

- Zscaler cloud account
- IP addresses or hostnames of the Zscaler public service edges tunnels (primary and secondary). See Locating the Hostnames and IP Addresses of Zscaler Enforcement Nodes (ZENs). See Configuring GRE Tunnels.
- Static IP address. See About Static IP

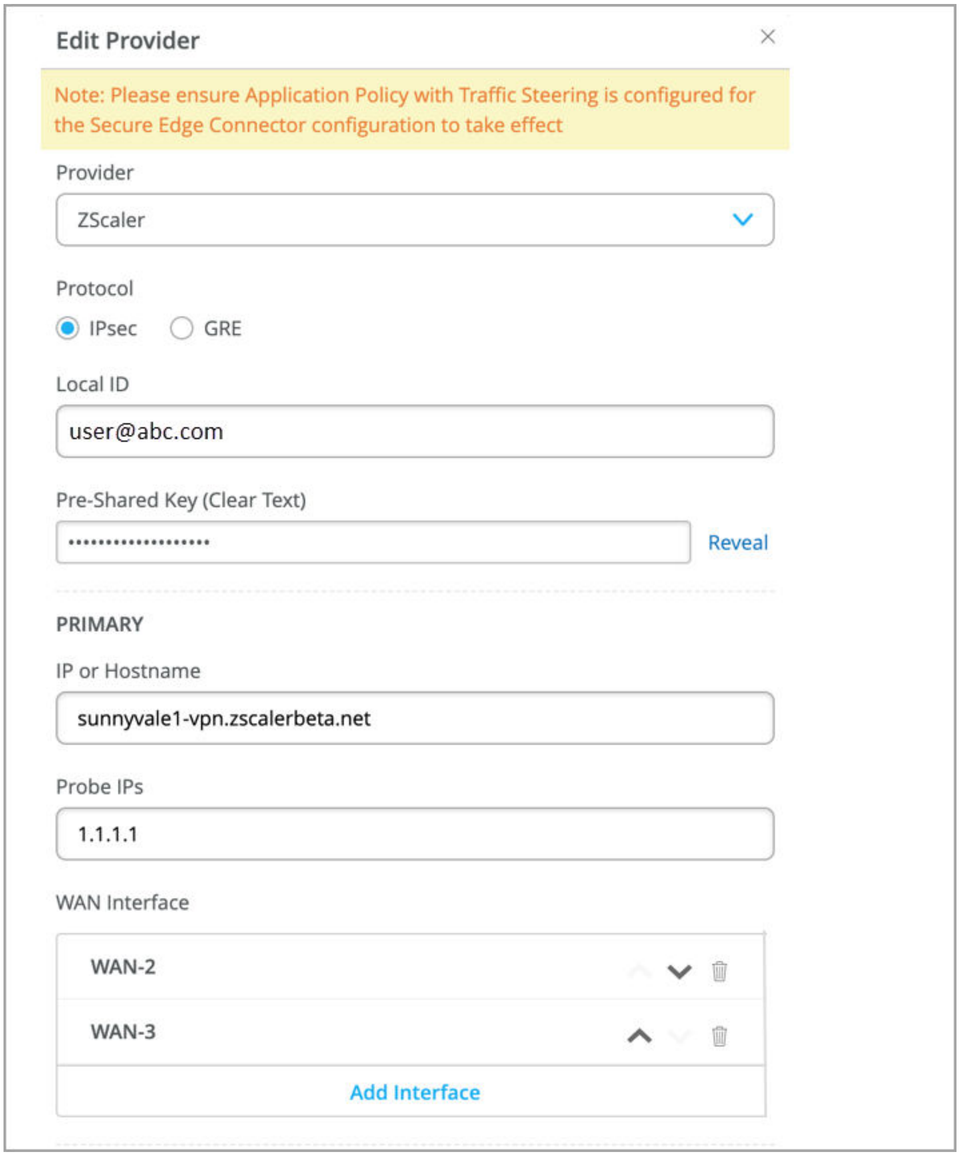
Configure Zscaler Tunnel Provisioning

1. On Juniper Mist portal, go to **Secure Edge Connector** at WAN Edge Templates-level, hub profile, or at Site-level.
2. Click **Add Providers**.
3. In **Add Provider** window, select **Zscaler** for manual provisioning.

4. Enter the details for Zscaler manual provisioning of tunnels.

   a. For IPsec Tunnels

Figure 388: Add Details for Zscaler IPsec Tunnels



Edit Provider

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

Provider: ZScaler

Protocol: ● IPsec ○ GRE

Local ID: user@abc.com

Pre-Shared Key (Clear Text): ••••••••••••••••••• Reveal

PRIMARY

IP or Hostname: sunnyvale1-vpn.zscalerbeta.net

Probe IPs: 1.1.1.1

WAN Interface:
WAN-2
WAN-3

i. **Name**—Enter the name of the service.

ii. **Provider**—Select Zscaler.

iii. **Protocol**—Select the protocol as IPsec.

iv. **Local ID**—Provide login ID of the Zscaler account.

v. **Preshared Key**—Provide preshared key (PSK) created with Zscaler account. The length of the PSK must be between 6-255 characters.

vi. **IP or Hostname**—IP addresses or hostname of the Zscaler DC. (See https://config.zscaler.com/zscalerbeta.net/cenr). We recommend to add IP address of the nearest DC to your device location.

vii. **Probe IPs**—Enter probe IP address. You can use any well-known IP (Example: 8.8.8.8). You need probe IP address to monitor the status of the Zscaler IPsec tunnel using probes.

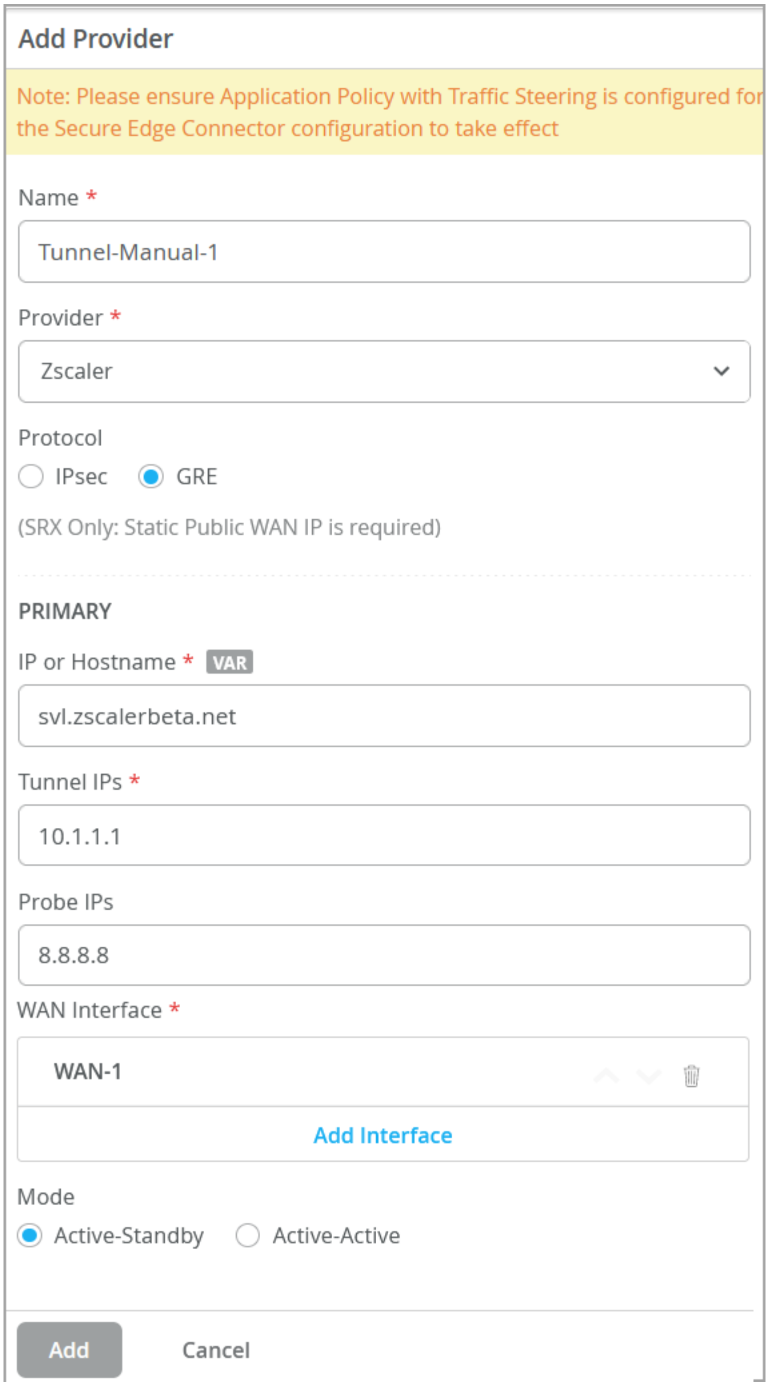
viii. **WAN Interface**—Assign WAN interfaces for provisioning of primary and secondary tunnels. You can add multiple WAN interfaces and the first interface takes the priority. If first interface is down, then system uses the second interface to establish the tunnel.

ix. **Mode**—Select active-standby option.

Configure secondary tunnel options (optional). Enter IP or Hostname, Probe IPs, WAN Interface, and Mode for the secondary tunnel.

b. **For GRE Tunnels:**

Figure 389: Add Details for Zscaler GRE Tunnels



Add Provider

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

Name *

Tunnel-Manual-1

Provider *

Zscaler

Protocol

○ IPsec ● GRE

(SRX Only: Static Public WAN IP is required)

PRIMARY

IP or Hostname * VAR

svl.zscalerbeta.net

Tunnel IPs *

10.1.1.1

Probe IPs

8.8.8.8

WAN Interface *

WAN-1

Mode

● Active-Standby ○ Active-Active

i. **Name**—Enter the name of the service.

ii. **Provider**—Select Zscaler.

iii. **Protocol**—Select the protocol as GRE.

iv. **IP or Hostname**—IP addresses or hostname of the Zscaler DC. (See https://config.zscaler.com/zscalerbeta.net/cenr). We recommend to add IP address of the nearest DC to your device location.

v. **Tunnel IP**—Static IP address created for GRE tunnel. See Configuring GRE Tunnels.

vi. **Probe IPs**—Enter probe IP address. You can use any well-known IP (Example: 8.8.8.8). You need probe IP address to monitor the status of the Zscaler IPsec tunnel using probes.

vii. **WAN Interface**—Assign WAN interfaces for provisioning of primary and secondary tunnels. You can add multiple WAN interfaces and the first interface takes the priority. If first interface is down, then system uses the second interface to establish the tunnel.

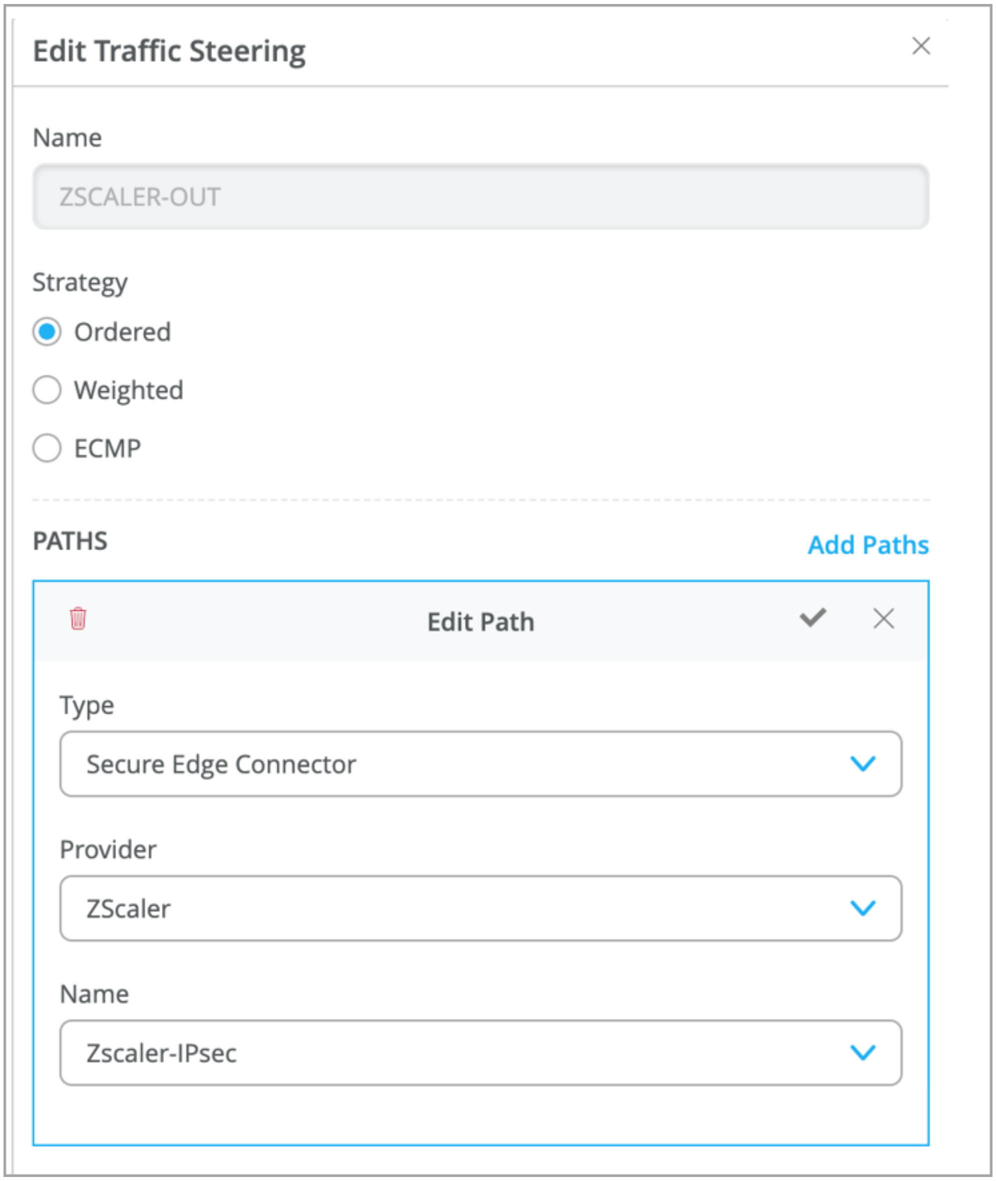
viii. **Mode**—Select active-standby option.

Enter IP or Hostname, Tunnel IP, Probe IPs, and WAN Interface for the secondary tunnel.

5. Click **Add** to continue.

6. Add a traffic steering profile on the WAN Edge Templates page or on WAN Edge Device page.

Figure 390: Traffic Steering Path



Edit Traffic Steering

Name: ZSCALER-OUT

Strategy
● Ordered
○ Weighted
○ ECMP

PATHS

Edit Path

Type: Secure Edge Connector

Provider: ZScaler

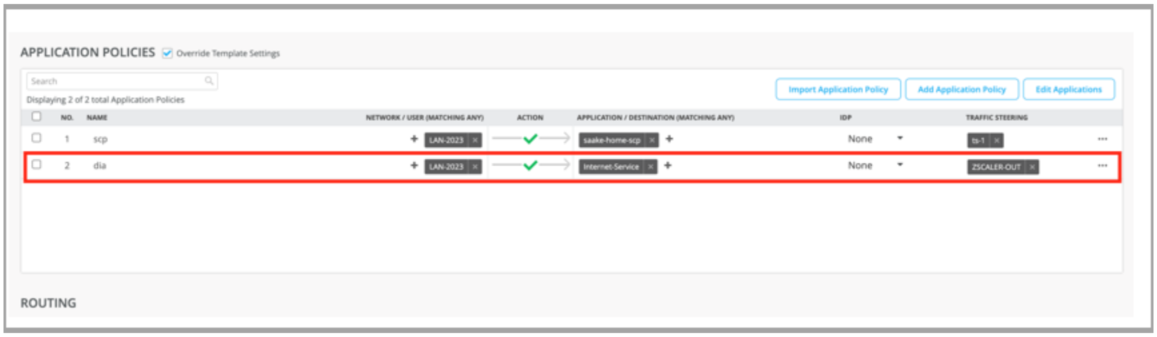
Name: Zscaler-IPsec

- Enter the details for the traffic-steering path:
  - **Name**—Enter a name for the traffic-steering profile.
  - **Strategy**—Select a strategy. You can configure the traffic steering profile with any strategy (Ordered/Weighted/ECMP), based on your topology and configuration.
  - **Type**—Select **Secure Edge Connector**.
  - **Provider**—Select **Zscaler**.

7. Add an application policy to refer the traffic steering profile you created. This step is required for provider tunnels to take effect. To create the application policy, in the Juniper Mist cloud portal, go to **Organization** > **WAN** > **Application Policy**

   Following image shows an example of application policy with traffic steering configured in previous step.

Figure 391: Application Policies



APPLICATION POLICIES ☑ Override Template Settings

Search

Displaying 2 of 2 total Application Policies

□	NO.	NAME	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING	
□	1	scp	+ LAN-2023 ×	✓	saake-home-scp × +	None	ts-1 ×	···
□	2	dia	+ LAN-2023 ×	✓	Internet-Service × +	None	ZSCALER-OUT ×	···

ROUTING

Zscaler Auto-Provisioning of Tunnels

IN THIS SECTION

Prerequisites

You need a partner key and the partner admin login credentials in Zscaler portal for auto-provisioning of Zscaler tunnels.

1. Add a partner API key.

   a. Use your Zscaler account to login admin portal.

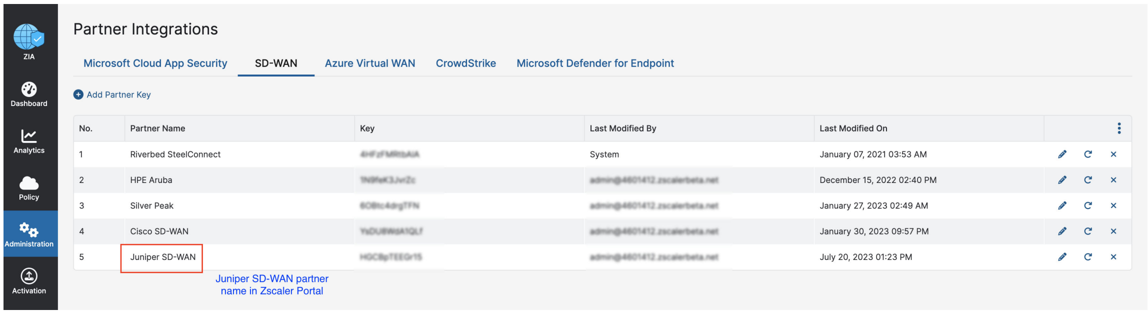
   b. Select **Administration** > **Partner Integrations.**

   c. Select the **SD-WAN** tab.

   d. Click **Add Partner Key**.

   e. In the **Add Partner Key** window, choose the partner name from a drop-down menu and click **Generate**.

Figure 392: Selecting SD-WAN Partner Integration



Partner Integrations

No.	Partner Name	Key	Last Modified By	Last Modified On	⋮
1	Riverbed SteelConnect	[redacted]	System	January 07, 2021 03:53 AM	✎ ↻ ✕
2	HPE Aruba	[redacted]	[redacted]	December 15, 2022 02:40 PM	✎ ↻ ✕
3	Silver Peak	[redacted]	[redacted]	January 27, 2023 02:49 AM	✎ ↻ ✕
4	Cisco SD-WAN	[redacted]	[redacted]	January 30, 2023 09:57 PM	✎ ↻ ✕
5	Juniper SD-WAN	[redacted]	[redacted]	July 20, 2023 01:23 PM	✎ ↻ ✕

Juniper SD-WAN partner name in Zscaler Portal

2. Provide credentials for the API access.

   a. Go to **Administration** > **Role Management** > **Add Partner Administrator Role.**

   b. Configure the following options:

      - **Name**—Name of the administrator role.

      - **Access Control**—Select the access control type as **Full**.

      - **Partner Access**—Select the type of access categories for the access control (SD- WAN API Partner access permission).

      Check Adding Partner Admin Roles for details.

3. Create a partner account for the SD-WAN Orchestrator. This admin user (username/password) is specifically used for SD-WAN partner authentication and it is different from Zscaler account admin user.

   a. Select **Administration** > **Administrator Management** > **Add Partner Administrator**.

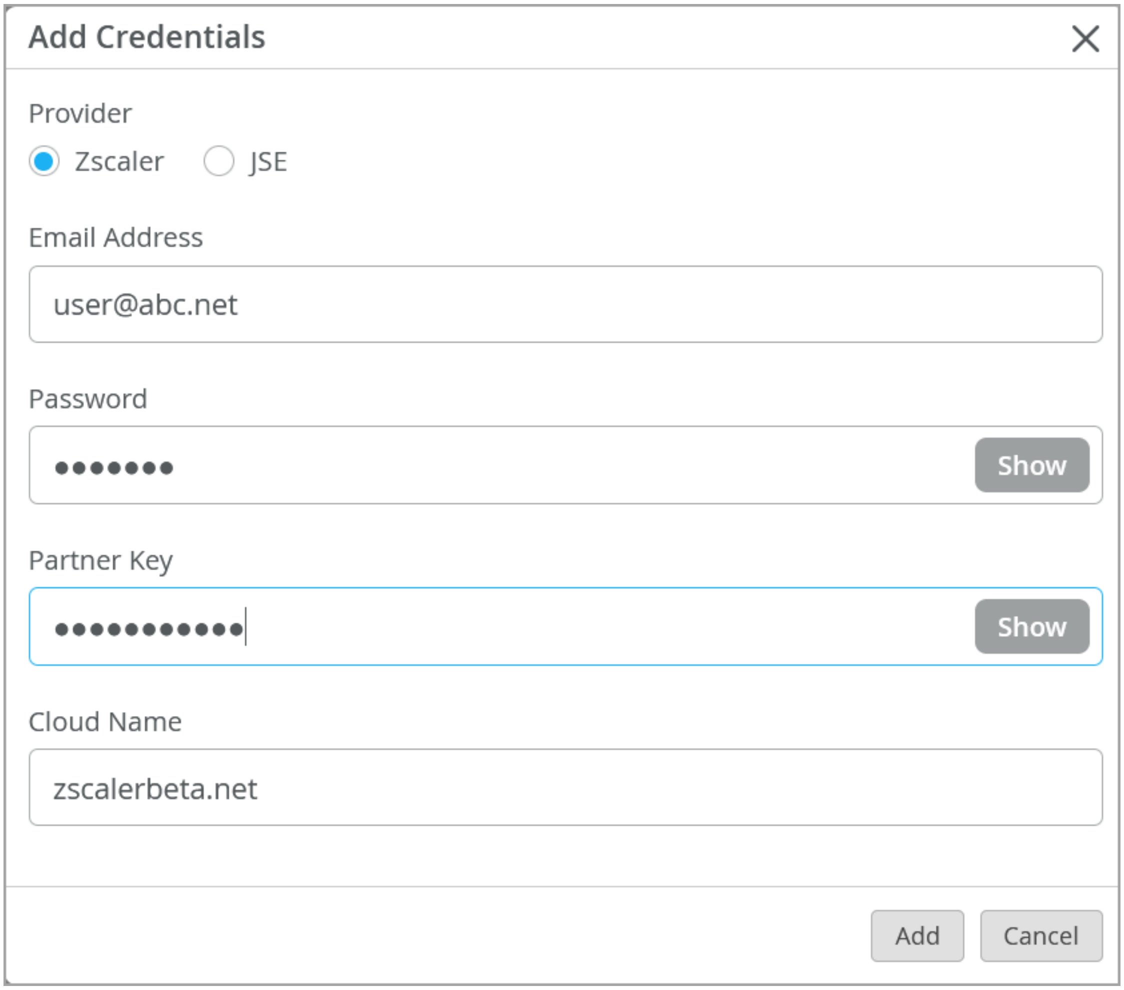
   b. Enter the details such as login ID, email address, name, partner role, and password. See Adding Partner Admins for details.

4. Find Zscaler Cloud name using What is My Cloud Name.

Add Zscaler Credentials in Juniper Mist Portal

1. Provide Zscaler credential details in Juniper Mist portal to integrate Juniper Mist cloud with Zscaler.
   - On Juniper Mist portal, select **Organization** > **Settings**.
   - Scroll-down to **Secure WAN Edge Integration** pane and click **Add Credentials**.
   - In **Add Provider** window, enter the details.

Figure 393: Add Credentials for Zscaler



Add Credentials

Provider

● Zscaler ○ JSE

Email Address

user@abc.net

Password

●●●●●●●

Partner Key

●●●●●●●●●●●

Cloud Name

zscalerbeta.net

- **Provider**—Select Zscaler.
- **Email Address**—Enter username (email address) (SD WAN partner user credentials)

    - **Password**—Enter password for the username.
    - **Partner Key**—Input partner key you created when configuring your Zscaler account.
    - **Cloud Name**—Zscaler cloud URL. For example, zscalerbeta.net.

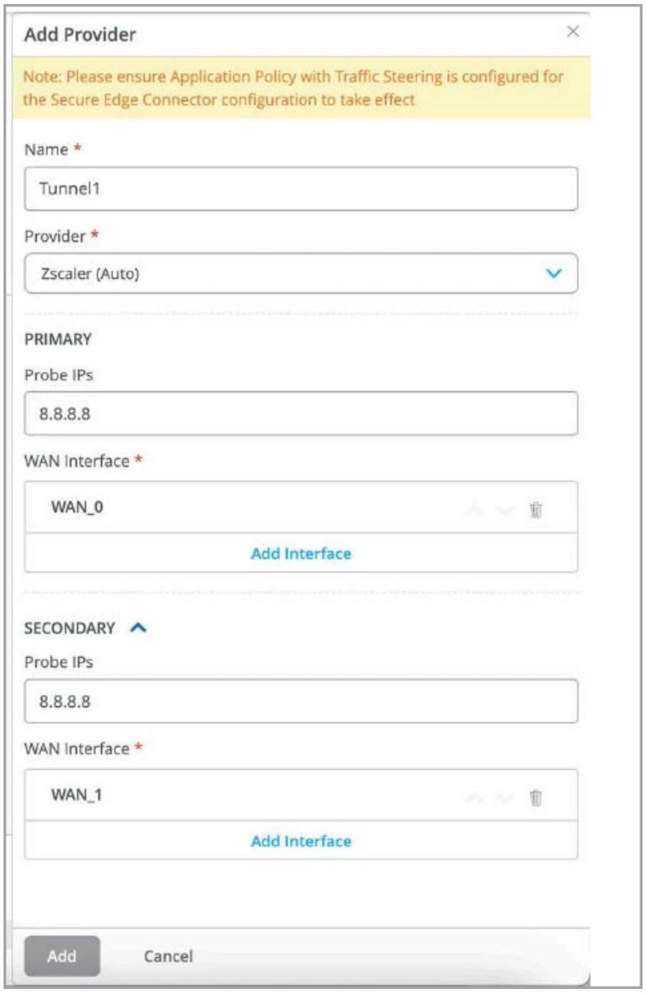
- Click **Add** to continue.

This procedure is one-time configurations at the organization level. To automatically provision the Zscaler tunnels across several sites, Mist Cloud uses the above-mentioned credentials for the given Organization.

Configure Zscaler Auto Tunnel Provisioning

1. On Juniper Mist portal, go to **Secure Edge Connector** at WAN Edge Templates-level or at Site-level.
2. Click **Add Providers**.
3. In **Add Provider** window, select **Zscaler (Auto)** for auto provisioning.

Figure 394: Add Details for Zscaler Tunnel Auto Provisioning



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

Name * Tunnel1

Provider * Zscaler (Auto)

PRIMARY

Probe IPs 8.8.8.8

WAN Interface * WAN_0

SECONDARY

Probe IPs 8.8.8.8

WAN Interface * WAN_1

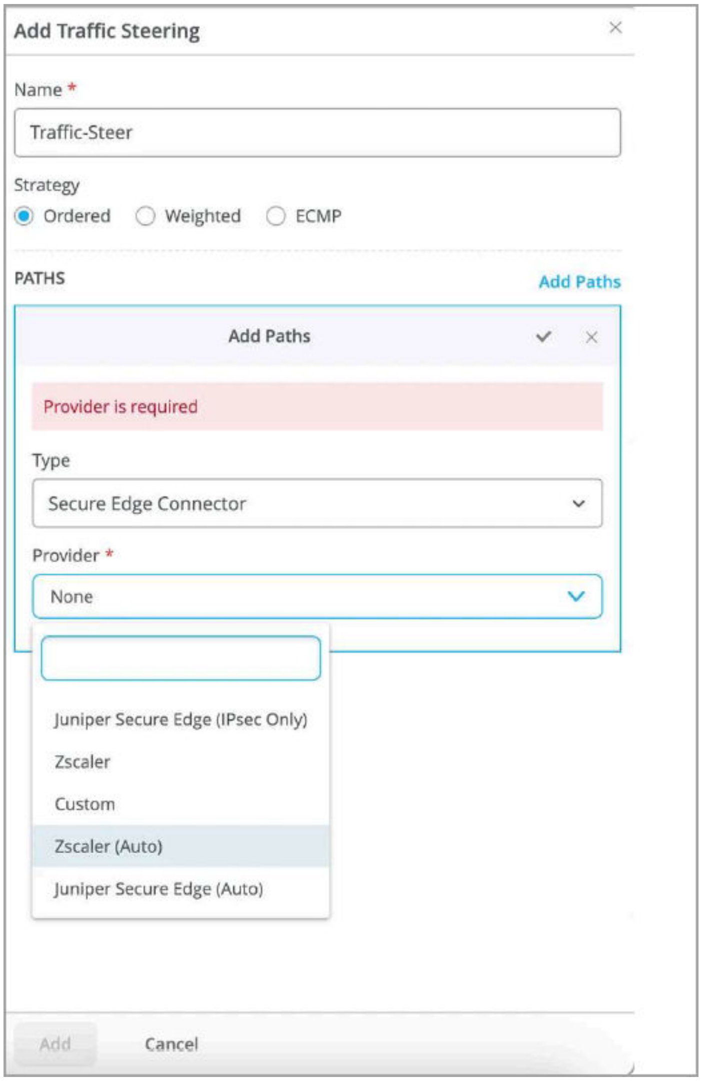
Enter the following details for Zscaler auto-provisioning:

- **Name**—Enter the username of the Zscaler account.
- **Provider**—Select Zscaler.
- **Probe IPs**—Enter probe IP address (primary and secondary). Enter any well-known IP address as probe IP. Example: 8.8.8.8.
- **WAN Interface**—Assign WAN interfaces under primary and secondary tunnel details for provisioning of primary and secondary tunnels.

4. Click **Add** to continue.

5. Add a traffic steering profile on the WAN Edge Templates page or on WAN Edge Device page.

Figure 395: Traffic Steering Path



Add Traffic Steering

Name *

Traffic-Steer

Strategy

● Ordered ○ Weighted ○ ECMP

PATHS

Add Paths

Add Paths

Provider is required

Type

Secure Edge Connector

Provider *

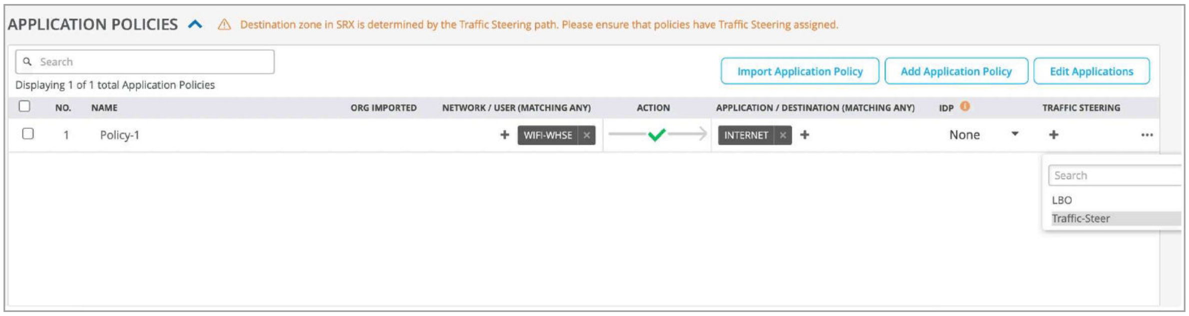
None

- You can add a new traffic-steering path by selecting:
  - **Name**—Enter a name for the traffic-steering profile.
  - **Strategy**—Select a strategy. You can configure the traffic steering profile with any strategy (Ordered/Weighted/ECMP), based on your topology and configuration.
  - **Type**—Select **Secure Edge Connector**.
  - **Provider**—Select **Zscaler**.

6. Add an application policy to refer the traffic steering profile you created. This is required for provisioning of provider tunnels to take effect. To create the application policy, in the Juniper Mist cloud portal, go to **Organization** > **WAN** > **Application Policy**

Following image shows an example of application policy with traffic steering configured in previous step.

Figure 396: Application Policies



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

Search

Displaying 1 of 1 total Application Policies

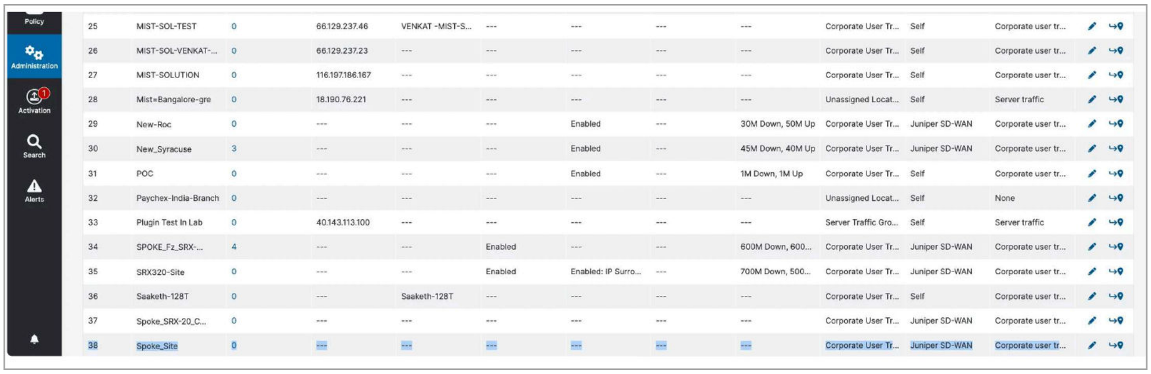
Import Application Policy | Add Application Policy | Edit Applications

□	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
□	1	Policy-1		+ WIFI-WHSE ×	✓	INTERNET × +	None	+ ···

When you assign a template that is enabled with the Zscaler (Auto) option to a site, the following operations take place:

- An associated Zscaler site (location object) is automatically created. You can view the location object in **Administration** > **Location Management** on Zscaler portal.

  Figure 397: Location Created in Zscaler Portal

25	MIST-SOL-TEST	0	66.129.237.46	VENKAT -MIST-S...	---	---	---	---	Corporate User Tr...	Self	Corporate user tr...
26	MIST-SOL-VENKAT-...	0	66.129.237.23	---	---	---	---	---	Corporate User Tr...	Self	Corporate user tr...
27	MIST-SOLUTION	0	116.197.186.167	---	---	---	---	---	Corporate User Tr...	Self	Corporate user tr...
28	Mist=Bangalore-gre	0	18.190.76.221	---	---	---	---	---	Unassigned Locat...	Self	Server traffic
29	New-Roc	0	---	---	---	Enabled	---	30M Down, 50M Up	Corporate User Tr...	Juniper SD-WAN	Corporate user tr...
30	New_Syracuse	3	---	---	---	Enabled	---	45M Down, 40M Up	Corporate User Tr...	Juniper SD-WAN	Corporate user tr...
31	POC	0	---	---	---	Enabled	---	1M Down, 1M Up	Corporate User Tr...	Self	Corporate user tr...
32	Paychex-India-Branch	0	---	---	---	---	---	---	Unassigned Locat...	Self	None
33	Plugin Test In Lab	0	40.143.113.100	---	---	---	---	---	Server Traffic Gro...	Self	Server traffic
34	SPOKE_Fz_SRX-...	4	---	---	Enabled	---	---	600M Down, 600...	Corporate User Tr...	Juniper SD-WAN	Corporate user tr...
35	SRX320-Site	0	---	---	Enabled	Enabled: IP Surro...	---	700M Down, 500...	Corporate User Tr...	Juniper SD-WAN	Corporate user tr...
36	Saaketh-128T	0	---	Saaketh-128T	---	---	---	---	Corporate User Tr...	Self	Corporate user tr...
37	Spoke_SRX-20_C...	0	---	---	---	---	---	---	Corporate User Tr...	Juniper SD-WAN	Corporate user tr...
38	Spoke_Site	0	---	---	---	---	---	---	Corporate User Tr...	Juniper SD-WAN	Corporate user tr...

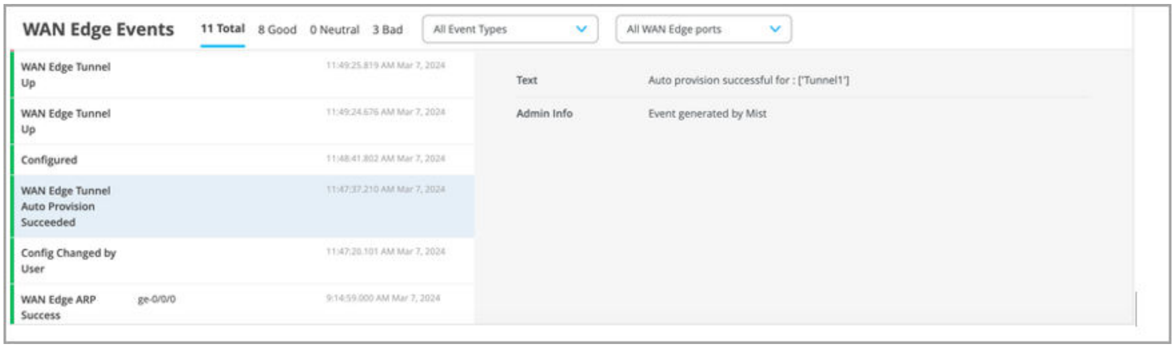
- The details required for tunnel creation are exchanged between Juniper Mist cloud and Zscaler.

- Tunnels are powered up from the device to the closest network point-of-presence (POP).

Verify Juniper Secure Edge Tunnels

On Juniper Mist portal, you can verify the established tunnels details in WAN Insights of the device once **WAN Edge Tunnel Auto Provision Succeeded** event appears under WAN Edge Events.

Figure 398: WAN Edge Events



WAN Edge Events

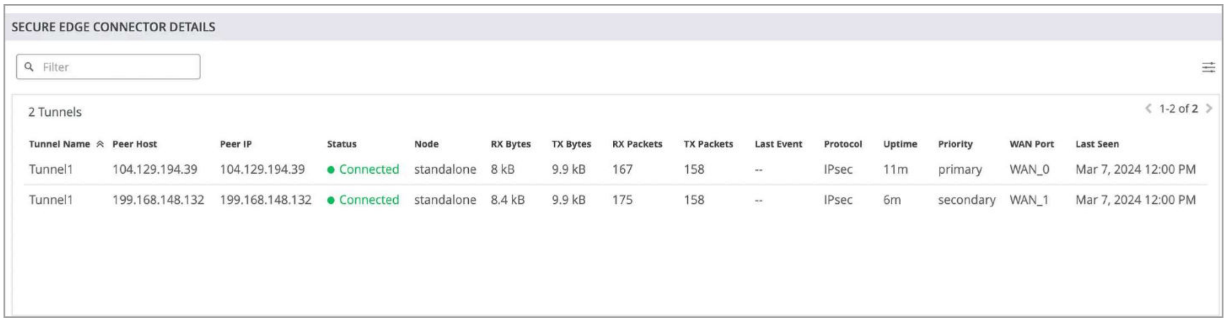
Event	Port	Time
WAN Edge Tunnel Up		11:49:25.819 AM Mar 7, 2024
WAN Edge Tunnel Up		11:49:24.676 AM Mar 7, 2024
Configured		11:48:41.802 AM Mar 7, 2024
WAN Edge Tunnel Auto Provision Succeeded		11:47:37.210 AM Mar 7, 2024
Config Changed by User		11:47:20.101 AM Mar 7, 2024
WAN Edge ARP Success	ge-0/0/0	9:14:59.000 AM Mar 7, 2024

Text: Auto provision successful for : ['Tunnel1']

Admin Info: Event generated by Mist

Get the established tunnels status details in **WAN Edges** > **WAN Edge Insights** page Juniper Mist cloud portal.

Figure 399: Status of Tunnels in WAN Edge Insights

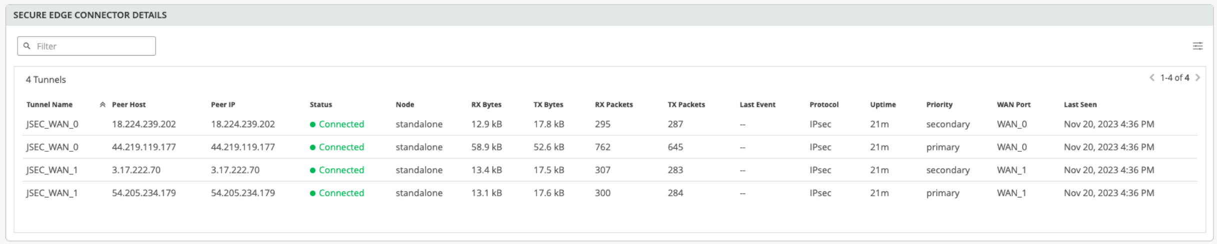


SECURE EDGE CONNECTOR DETAILS

2 Tunnels

Tunnel Name	Peer Host	Peer IP	Status	Node	RX Bytes	TX Bytes	RX Packets	TX Packets	Last Event	Protocol	Uptime	Priority	WAN Port	Last Seen
Tunnel1	104.129.194.39	104.129.194.39	● Connected	standalone	8 kB	9.9 kB	167	158	--	IPsec	11m	primary	WAN_0	Mar 7, 2024 12:00 PM
Tunnel1	199.168.148.132	199.168.148.132	● Connected	standalone	8.4 kB	9.9 kB	175	158	--	IPsec	6m	secondary	WAN_1	Mar 7, 2024 12:00 PM

Figure 400: Established Secure Edge Tunnels



SECURE EDGE CONNECTOR DETAILS

4 Tunnels

Tunnel Name	Peer Host	Peer IP	Status	Node	RX Bytes	TX Bytes	RX Packets	TX Packets	Last Event	Protocol	Uptime	Priority	WAN Port	Last Seen
JSEC_WAN_0	18.224.239.202	18.224.239.202	● Connected	standalone	12.9 kB	17.8 kB	295	287	--	IPsec	21m	secondary	WAN_0	Nov 20, 2023 4:36 PM
JSEC_WAN_0	44.219.119.177	44.219.119.177	● Connected	standalone	58.9 kB	52.6 kB	762	645	--	IPsec	21m	primary	WAN_0	Nov 20, 2023 4:36 PM
JSEC_WAN_1	3.17.222.70	3.17.222.70	● Connected	standalone	13.4 kB	17.5 kB	307	283	--	IPsec	21m	secondary	WAN_1	Nov 20, 2023 4:36 PM
JSEC_WAN_1	54.205.234.179	54.205.234.179	● Connected	standalone	13.1 kB	17.6 kB	300	284	--	IPsec	21m	primary	WAN_1	Nov 20, 2023 4:36 PM

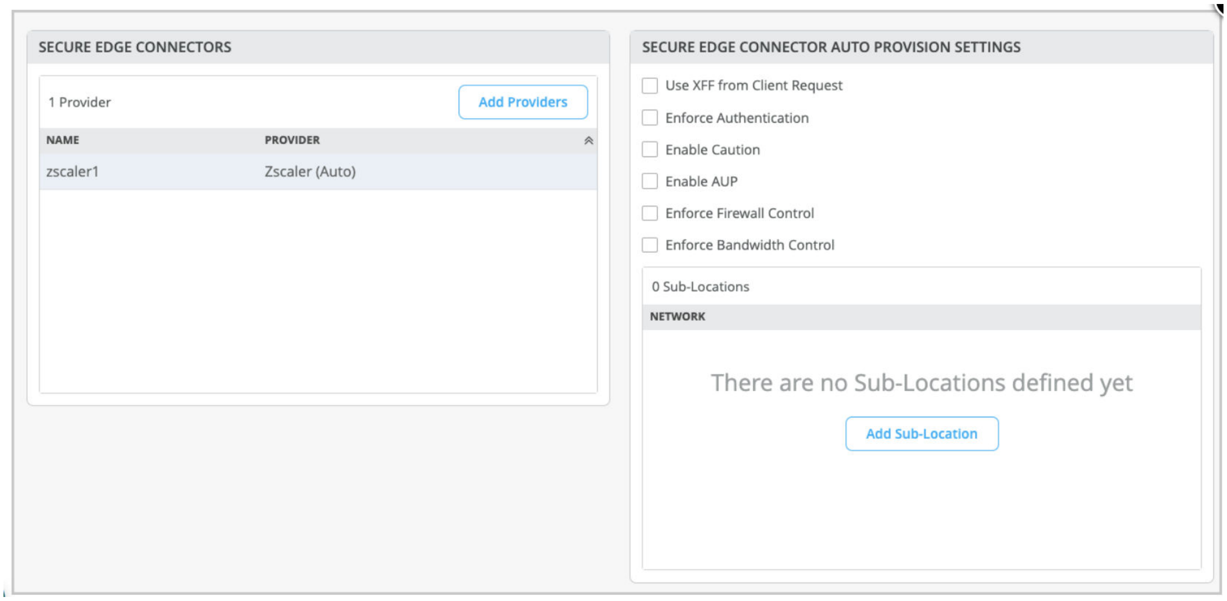
You can check the established tunnels in the Juniper Security Director Cloud dashboard and in the service location.

Secure Edge Connector Auto Provision Settings

You can configure gateway options per Zscaler location in **Secure Edge Connector Auto Provision Settings** on Juniper Mist portal. These settings offer additional control for configuring various traffic rules and policies, and they are optional parameters.

1. On Juniper Mist portal, select **Organization** > **WAN Edge Templates** or select **WAN Edges** > **WAN Edges** > *WAN Edge Name*.
2. Scroll-down to Secure Edge Connectors.
3. Select Zscaler (Auto) as the Secure Edge Connector. In the **Secure Edge Connector Auto Provision Settings** pane, you can define the gateway options.

Figure 401: Secure Edge Connector Auto Provision Settings



SECURE EDGE CONNECTORS

1 Provider

Add Providers

NAME	PROVIDER
zscaler1	Zscaler (Auto)

SECURE EDGE CONNECTOR AUTO PROVISION SETTINGS

- ☐ Use XFF from Client Request
- ☐ Enforce Authentication
- ☐ Enable Caution
- ☐ Enable AUP
- ☐ Enforce Firewall Control
- ☐ Enforce Bandwidth Control

0 Sub-Locations

NETWORK

There are no Sub-Locations defined yet

Add Sub-Location

- **Use XFF from Client Request**—Enable this option if this location uses proxy chaining to forward traffic to the Zscaler service.
- **Enforce Authentication**—Enable this option if you want to authenticate users from this location.
- **Enable Caution**— Set the caution interval for more than one minute to display a caution notification for unauthenticated users. Use this option if you have disabled **Enforce Authentication** option.
- **Enable AUP**—Enable to display Acceptable Use Policy (AUP) for unauthenticated traffic and mandate it for the users to accept it. Use this option if you have disabled **Enforce Authentication.**
- **Enforce Firewall Control**—Enable the firewall control options.

- **Bandwidth Control**—Enforce bandwidth control for the location. You can specify the maximum bandwidth limits for upload and downloads.

Zscaler Auto-Tunnel Provisioning with Sub-Locations

Juniper Mist supports configuration and provisioning of Zscaler sub-locations. A Zscaler sub-location is a child entity of the location object. Locations identify the various networks from which your organization sends its Internet traffic. Sub-locations can be used for specific uses cases. For example, an organization can define a Zscaler sub-location for its corporate network, and another sub-location for its guest network, even if their traffic goes through the same IPsec tunnel.

The organization uses the sub-locations to:

- Implement different policies based on IP addresses.

- Enforce authentication for the internal corporate network, while disabling it for the guest network.

- Enforce bandwidth control for sub-locations while ensuring that unused bandwidth remains available to the parent location.

Juniper Mist supports sub-location provisioning as part of the tunnel orchestration process, and you can define the sub-location options using the Mist portal.

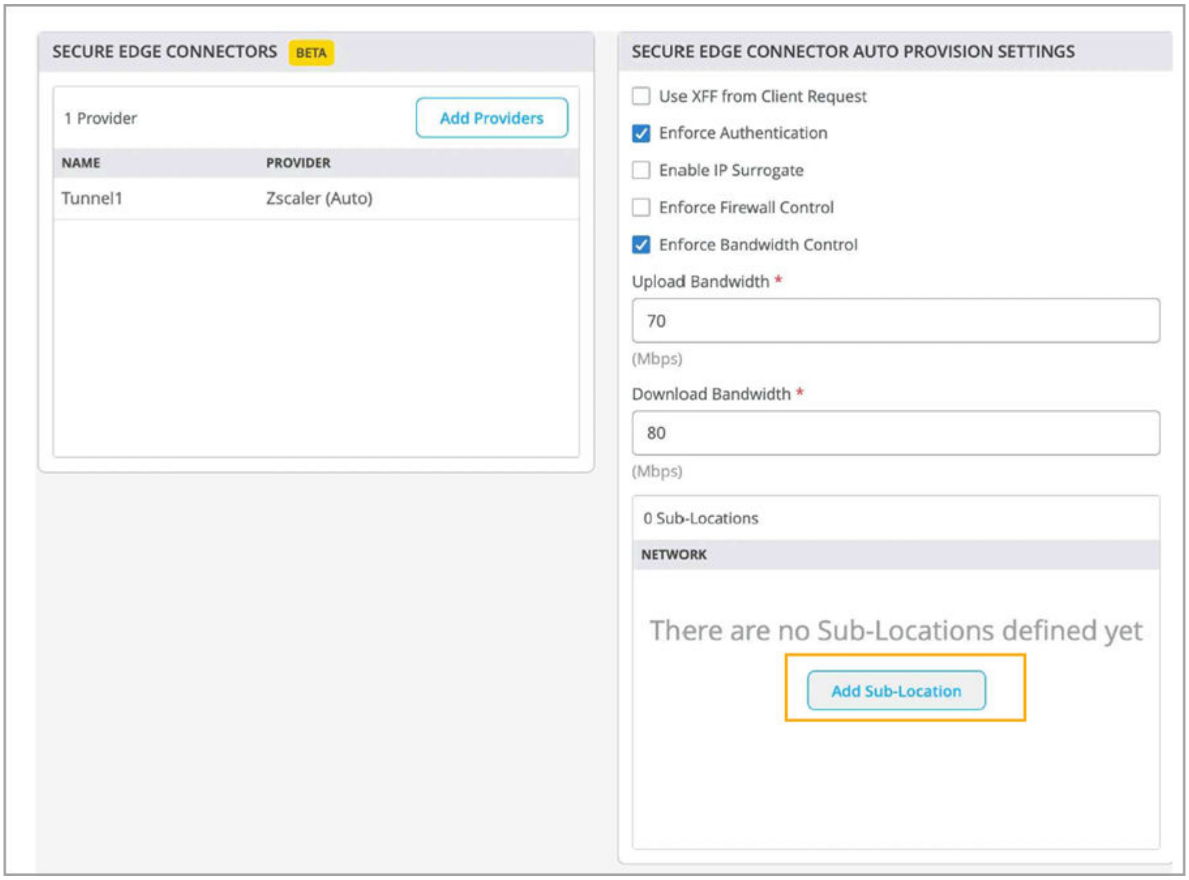
To configure Zscaler sub-locations:

1. On Juniper Mist portal, select **Organization** > **WAN Edge Templates** or select **WAN Edges** > **WAN Edges** > *WAN Edge Name*.

2. Scroll-down to **Secure Edge Connectors**.

3. Select Zscaler as the Secure Edge Connector. You'll see sub-location for the site below **Secure Edge Connector Auto Provision Settings** option.

Figure 402: Add Sub-Location



SECURE EDGE CONNECTORS BETA

1 Provider

NAME	PROVIDER
Tunnel1	Zscaler (Auto)

SECURE EDGE CONNECTOR AUTO PROVISION SETTINGS

□ Use XFF from Client Request

☑ Enforce Authentication

□ Enable IP Surrogate

□ Enforce Firewall Control

☑ Enforce Bandwidth Control

Upload Bandwidth *

70

(Mbps)

Download Bandwidth *

80

(Mbps)

0 Sub-Locations

NETWORK

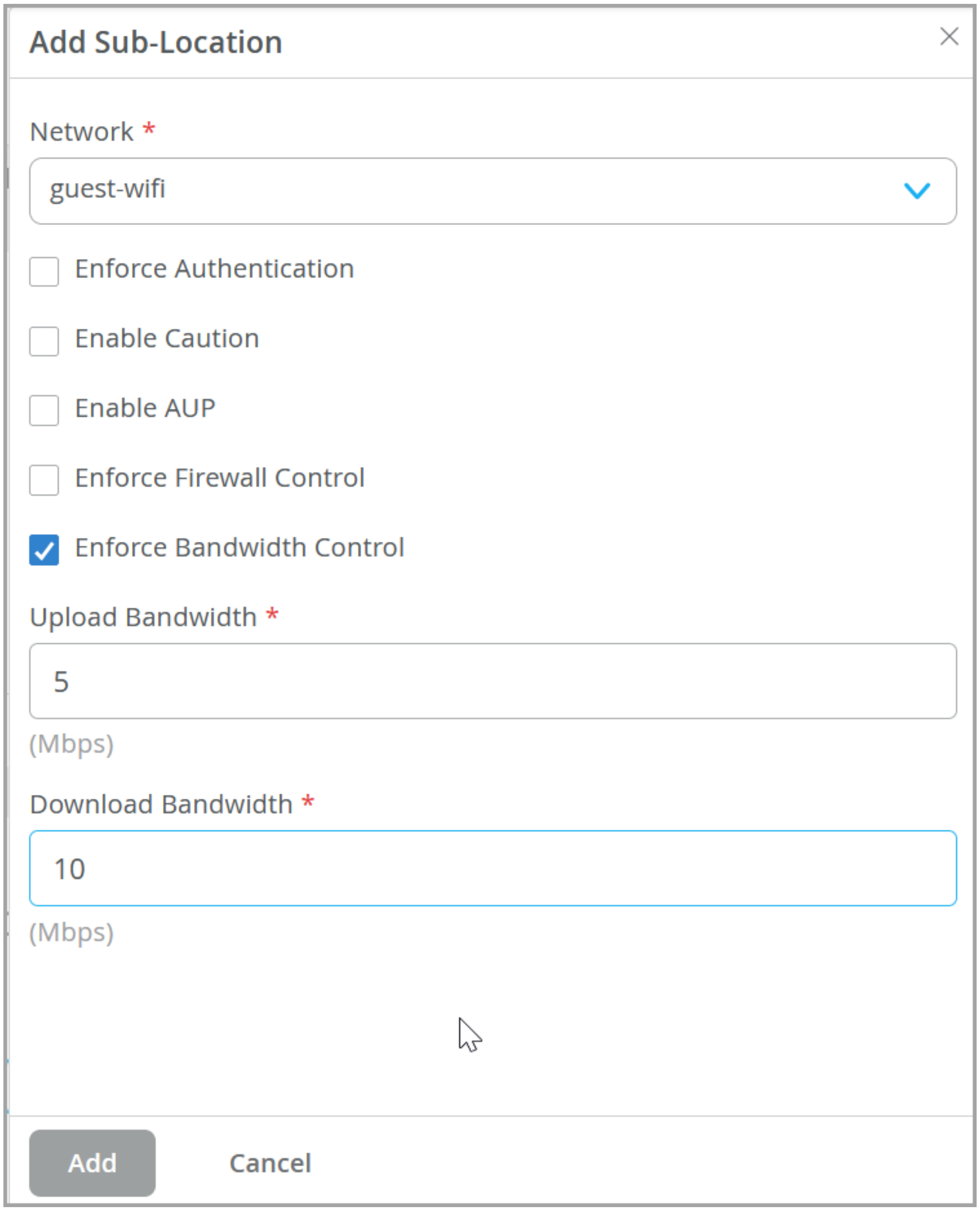
There are no Sub-Locations defined yet

4. Click **Add Sub-Location** to define the new sublocation.

   The **Add Sub-Location** option is available only when you select Zscaler as the Secure Edge Connector.

5. In the **Add Sub-Location** window, define settings for the sub-location.

Figure 403: Sub-Locations Settings



Add Sub-Location

Network *

guest-wifi

□ Enforce Authentication

□ Enable Caution

□ Enable AUP

□ Enforce Firewall Control

☑ Enforce Bandwidth Control

Upload Bandwidth *

5

(Mbps)

Download Bandwidth *

10

(Mbps)

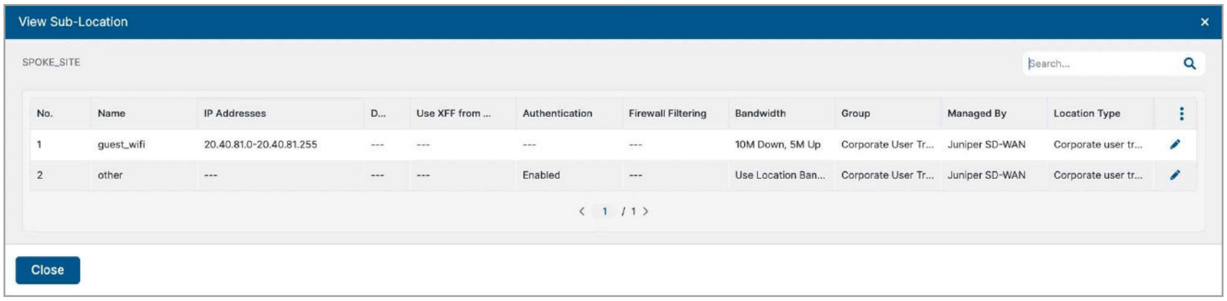
- **Network**—Select an existing network from the drop-down box.
- **Enforce Authentication**—To authenticate users from this location.
- **Enable Caution**— Display a caution notification for unauthenticated users. Use this option if you have disabled **Enforce Authentication** option.
- **Enable AUP**—Enable to display Acceptable Use Policy (AUP) for unauthenticated traffic and mandate it for the users to accept it. Use this option if you have disabled **Enforce Authentication**. The custom AUP Frequency must be a number between 1 and 180.

- **Enforce Firewall Control**—Enable the firewall control options.
- **Bandwidth Control**—Enforce bandwidth control for the location. You can specify the maximum bandwidth limits for upload and downloads. Upload and download bandwidth must be a number between 0.1 and 99999.

View Sub-Locations in Zscaler Portal

You can view the newly created sub-location in **Administration** > **Location Management** on Zscaler portal. On the Locations page, when you click the sublocation's number within the table, the sub-locations for the location appear.

Figure 404: View Configured Sub-Location in Zscaler Portal

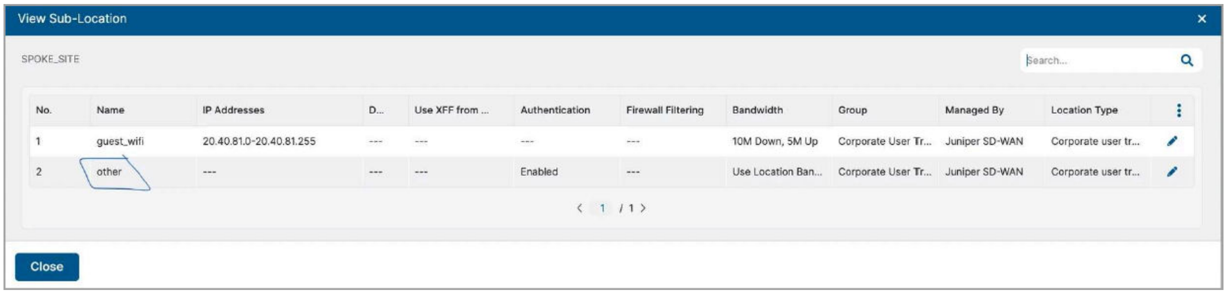


SPOKE_SITE

No.	Name	IP Addresses	D...	Use XFF from ...	Authentication	Firewall Filtering	Bandwidth	Group	Managed By	Location Type
1	guest_wifi	20.40.81.0-20.40.81.255	---	---	---	---	10M Down, 5M Up	Corporate User Tr...	Juniper SD-WAN	Corporate user tr...
2	other	---	---	---	Enabled	---	Use Location Ban...	Corporate User Tr...	Juniper SD-WAN	Corporate user tr...

< 1 / 1 >

Figure 405: View Other Sub-Location in Zscaler Portal



SPOKE_SITE

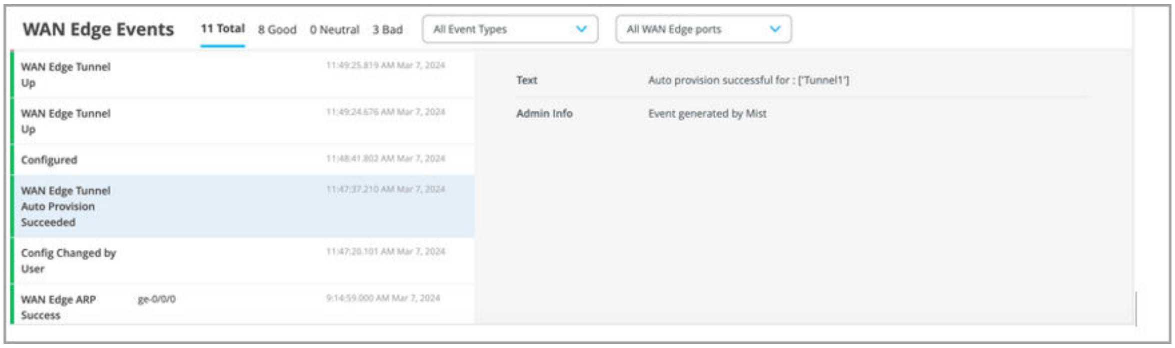
No.	Name	IP Addresses	D...	Use XFF from ...	Authentication	Firewall Filtering	Bandwidth	Group	Managed By	Location Type
1	guest_wifi	20.40.81.0-20.40.81.255	---	---	---	---	10M Down, 5M Up	Corporate User Tr...	Juniper SD-WAN	Corporate user tr...
2	other	---	---	---	Enabled	---	Use Location Ban...	Corporate User Tr...	Juniper SD-WAN	Corporate user tr...

< 1 / 1 >

Verification and Troubleshooting

On Juniper Mist portal, you can verify the established tunnels details in WAN Insights of the device once **WAN Edge Tunnel Auto Provision Succeeded** event appears under WAN Edge Events.

Figure 406: WAN Edge Events



WAN Edge Events

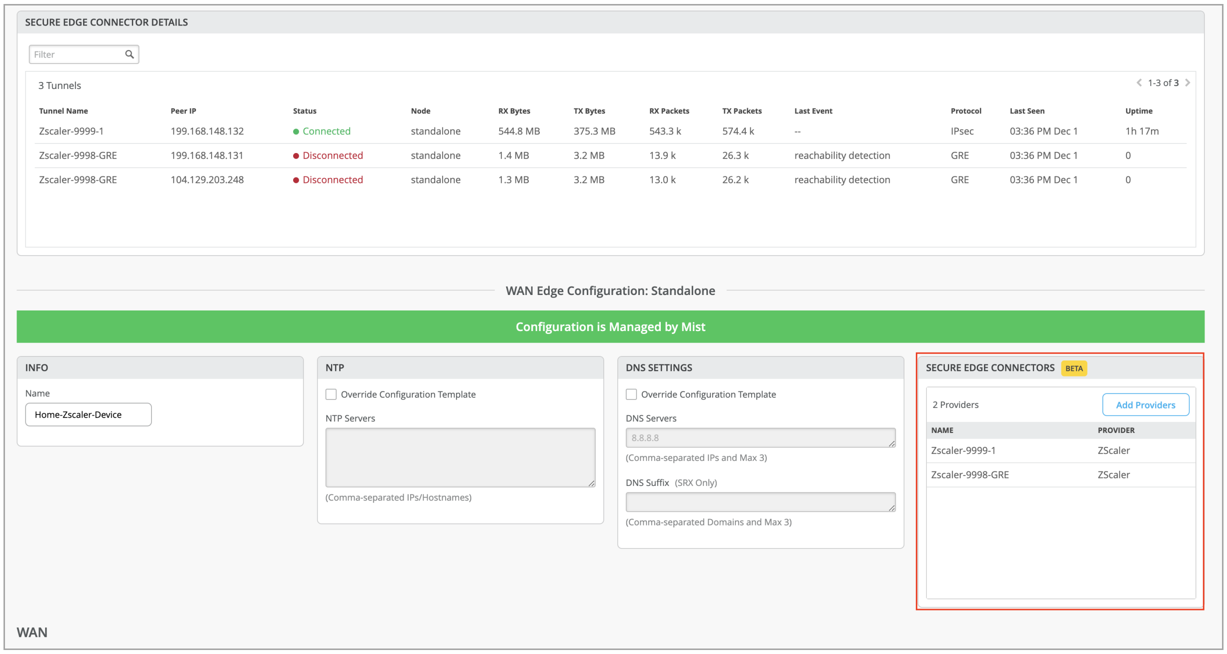
11 Total 8 Good 0 Neutral 3 Bad

Event	Port	Time
WAN Edge Tunnel Up		11:49:25.819 AM Mar 7, 2024
WAN Edge Tunnel Up		11:49:24.676 AM Mar 7, 2024
Configured		11:48:41.802 AM Mar 7, 2024
WAN Edge Tunnel Auto Provision Succeeded		11:47:37.210 AM Mar 7, 2024
Config Changed by User		11:47:20.101 AM Mar 7, 2024
WAN Edge ARP Success	ge-0/0/0	9:14:59.000 AM Mar 7, 2024

Text Auto provision successful for : ['Tunnel1']

Admin Info Event generated by Mist

Figure 407: View Established Tunnels



SECURE EDGE CONNECTOR DETAILS

3 Tunnels

1-3 of 3

Tunnel Name	Peer IP	Status	Node	RX Bytes	TX Bytes	RX Packets	TX Packets	Last Event	Protocol	Last Seen	Uptime
Zscaler-9999-1	199.168.148.132	● Connected	standalone	544.8 MB	375.3 MB	543.3 k	574.4 k	--	IPsec	03:36 PM Dec 1	1h 17m
Zscaler-9998-GRE	199.168.148.131	● Disconnected	standalone	1.4 MB	3.2 MB	13.9 k	26.3 k	reachability detection	GRE	03:36 PM Dec 1	0
Zscaler-9998-GRE	104.129.203.248	● Disconnected	standalone	1.3 MB	3.2 MB	13.0 k	26.2 k	reachability detection	GRE	03:36 PM Dec 1	0

WAN Edge Configuration: Standalone

Configuration is Managed by Mist

INFO

Name: Home-Zscaler-Device

NTP

□ Override Configuration Template

NTP Servers

(Comma-separated IPs/Hostnames)

DNS SETTINGS

□ Override Configuration Template

DNS Servers: 8.8.8.8

(Comma-separated IPs and Max 3)

DNS Suffix (SRX Only)

(Comma-separated Domains and Max 3)

SECURE EDGE CONNECTORS BETA

2 Providers

NAME	PROVIDER
Zscaler-9999-1	ZScaler
Zscaler-9998-GRE	ZScaler

WAN

If you are not able to establish the tunnel, the possible cause could be tunnel configuration issues or reachability issues from your device. You can use the following options to troubleshoot the issue:

- Check the Zscaler IP address or hostname configured on the Juniper Mist portal. Ensure that local ID and PSK configured on Zscaler account match with those configured on Juniper Mist portal.
- Ping the Zscaler public IP address from the WAN interface on your device and check if there are responses.
- Using the packet capture tool on the Mist portal. Run a PCAP on the WAN interface with Zscaler Public IP address as filter and check see if there is bidirectional packets. See "Troubleshoot SRX Series Firewalls Using Packet Captures" on page 638.

- If your security device is sending packets to Zscaler and there is no response from the Zscaler, do following:
  - Check if the Zscaler IP address is active
  - Check if any uplink router is blocking the traffic flow
  - Check NAT configuration if applicable

  Note that the packet capture results help you to detect the above issues.

Related Topics

SEE ALSO

Configure WAN Edge Templates for SRX Series Firewalls | 217

Configure Hub Profiles for SRX Series Firewalls | 197

WAN Assurance Configuration Overview | 166

No Link Title

No Link Title

7

CHAPTER

Cellular Edges

Cradlepoint Integration

IN THIS SECTION

Juniper Networks Mist Cloud supports Cradlepoint 5G cellular adapters, adding to Juniper's wired, wireless and SD-WAN portfolio of supported products.

Video: Now in 60: Cradlepoint integration with SD-WAN

Juniper Mist WAN Assurance supports the following Cradlepoint 5G adapters:

- W1850 Series 5G Wideband Adapter
- W1855 Series 5G Wideband Adapter
- W2000 Series 5G Wideband Adapter
- W2005 Series 5G Wideband Adapter
- W4005 Series 5G Wideband Adapter

Juniper Mist WAN Assurance supports the following Cradlepoint devices:

- E300 Series Enterprise Router
- E3000 Series Enterprise Router
- R1900 router
- AER2200 router

- CBA850 LTE adapter and its sub models

The Cradlepoint 5G adapters provide an LTE WAN backhaul mechanism across many verticals such as retail, warehousing, logistics. Juniper Mist integration with Cradlepoint enables you to use Cradlepoint 5G cellular adapters with Juniper's wired, wireless, and SD-WAN solutions driven by Mist AI.

You can now integrate your Cradlepoint NetCloud Manager account with the Juniper Mist cloud portal. The integration enables you to:

- Manage Cradlepoint devices from the Mist portal including onboarding, assigning devices to a site, and view device inventory details.
- Get visibility into the health, SLE, and Insights into Cradlepoint devices.
- Leverage Marvis, Juniper's virtual network assistant, to get proactive recommendations and self-driving network actions.

The integration enhances Juniper Mist's client-to-cloud user experience by additionally providing insights into the branch WAN adapters, helping the network admins reduce Mean Time to Identify (MTTI).

Prerequisite for Onboarding Cradlepoint Devices

To onboard Cradlepoint devices into Juniper Mist portal, you must:

1. Link Cradlepoint NetCloud account to the Juniper Mist portal.
2. Add account to your Mist organization as a Cellular Edge token.

On adding the Cellular Edge token to your organization in Juniper Mist, supported Cradlepoint devices that are managed by NetCloud are automatically onboarded to the Mist portal.

To integrate your NetCloud account with the Mist cloud, you need:

- Active Marvis subscription
- Deployed Mist device type on the site (minimum one)
- Cradlepoint devices managed from NetCloud

Integrate Cradlepoint NetCloud Account to the Juniper Mist Portal

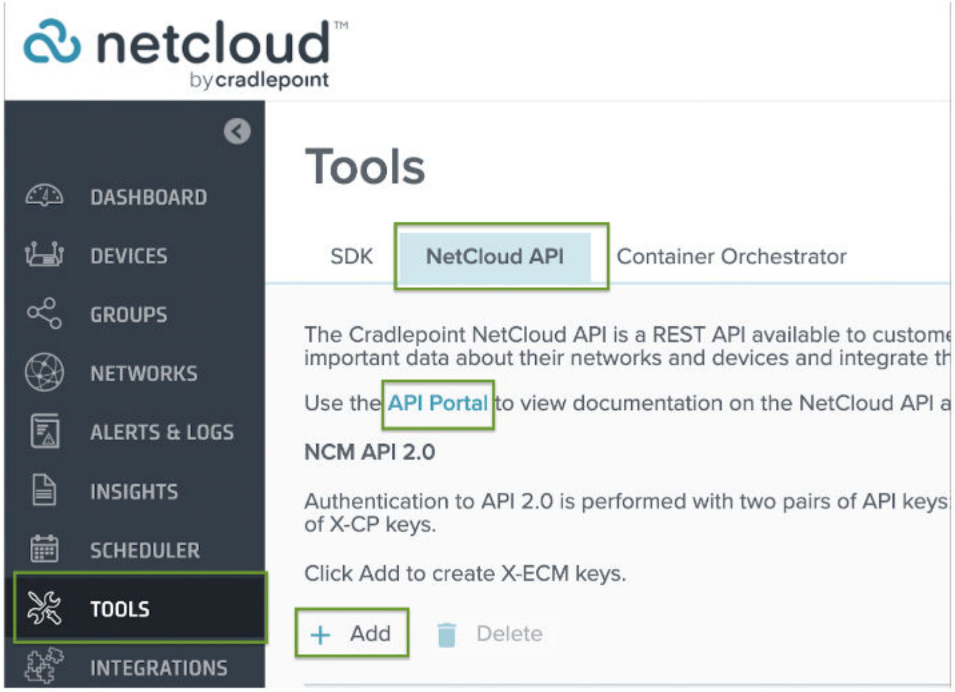
Use the following procedure to integrate your NetCloud account with the Mist cloud:

1. Generate the required API token (X-CP-API-ID, X-CP-API-KEY, X-ECM-API-ID, and X-ECM-API-KEY) from NetCloud dashboard with following steps:

   a. Log in to the NetCloud Manager.

   b. Click **Tools** in the left-side navigation panel, and then click the **NetCloud API** tab.

   Figure 408: Generating API Keys in NetCloud Dashboard

   The Cradlepoint NetCloud API is a REST API available to custome
   important data about their networks and devices and integrate th

   Use the API Portal to view documentation on the NetCloud API a

   NCM API 2.0

   Authentication to API 2.0 is performed with two pairs of API keys
   of X-CP keys.

   Click Add to create X-ECM keys.

   c. Click the **API Portal link** on the Tools page.
   On the API portal, you can view information about your API keys. Copy **X-CP-API-ID** and **X-CP-API-KEY** and save them for further reference.

   d. Navigate back to **Tools> NetCloud API > Create API Key**

   e. Click **Add** and select a role to associate with the keys and click **OK.** .

   The dialog opens and displays your **X-ECM-API-ID** and **X-ECM-API-KEY** key values. Copy these key values and save them for further reference.

   Keep ready all key values—**X-CP-API-ID**, **X-CP-API-KEY**, **X-ECM-API-ID**, and **X-ECM-API-KEY**

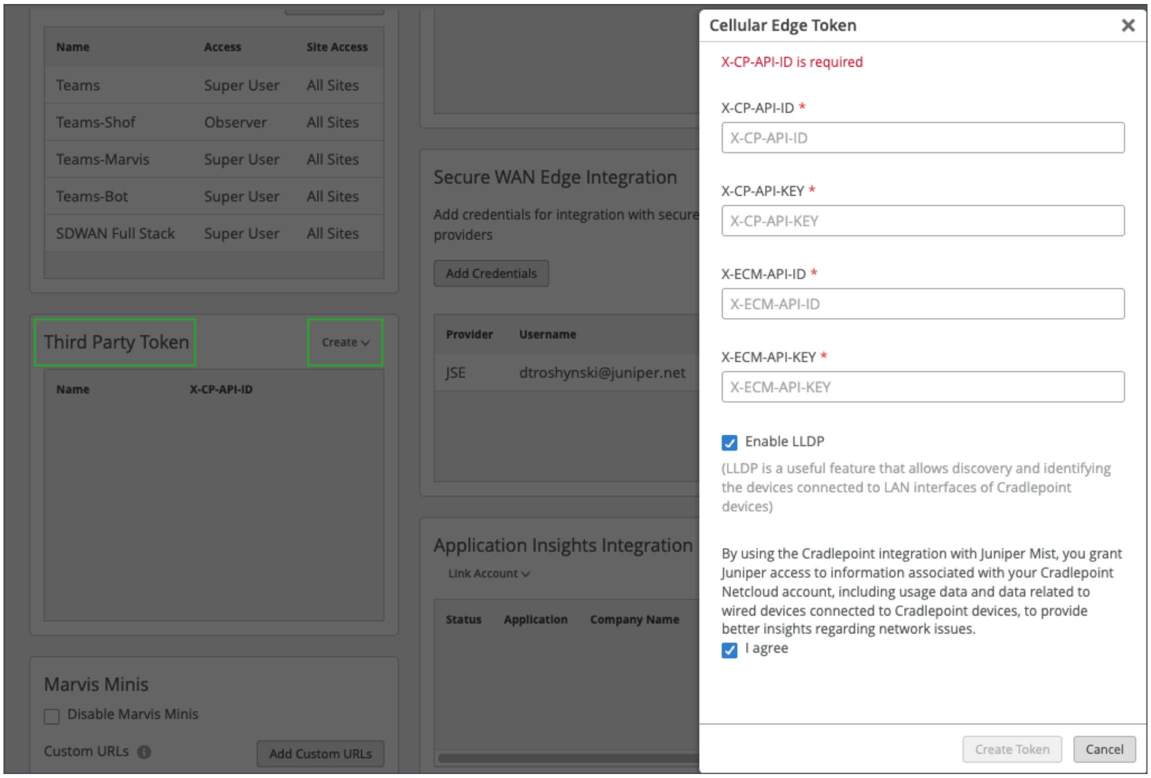
2. Log on to Juniper Mist portal and complete the following steps:

   a. On Juniper Mist portal, go to **Organization** > **Settings**.

   b. Scroll to **Third Party Token** pane and click **Create**.

c. Select **Cellular Edge** and enter the keys you saved in previous procedure.

Figure 409: Add Third Party Token for Cradlepoint



Name	Access	Site Access
Teams	Super User	All Sites
Teams-Shof	Observer	All Sites
Teams-Marvis	Super User	All Sites
Teams-Bot	Super User	All Sites
SDWAN Full Stack	Super User	All Sites

Third Party Token

Name	X-CP-API-ID

Secure WAN Edge Integration

Add credentials for integration with secure providers

Provider	Username
JSE	dtroshynski@juniper.net

Application Insights Integration

Status	Application	Company Name

Marvis Minis

☐ Disable Marvis Minis

Cellular Edge Token

X-CP-API-ID is required

X-CP-API-ID *

X-CP-API-KEY *

X-ECM-API-ID *

X-ECM-API-KEY *

☑ Enable LLDP

(LLDP is a useful feature that allows discovery and identifying the devices connected to LAN interfaces of Cradlepoint devices)

By using the Cradlepoint integration with Juniper Mist, you grant Juniper access to information associated with your Cradlepoint Netcloud account, including usage data and data related to wired devices connected to Cradlepoint devices, to provide better insights regarding network issues.

☑ I agree

By default, the LLDP option is enabled. LLDP allows discovery and identification of devices connected to the LAN ports on Cradlepoint devices.

> **NOTE**: The Cradlepoint R1900 router does not support LLDP today. Please contact your Cradlepoint account manager to request further information on future plans to add LLDP to this device.
>
> The latest release of NetCloud OS revealed that support for LLDP functionality is disabled for W1850 and W1855 Cradlepoint devices. This will be enabled in the next release, scheduled for August 2024.

d. Click **Create Token**.
You can see the entry for CradlePoint in the **Third Party Token** table after a successful integration.

View Cradlepoint Inventory

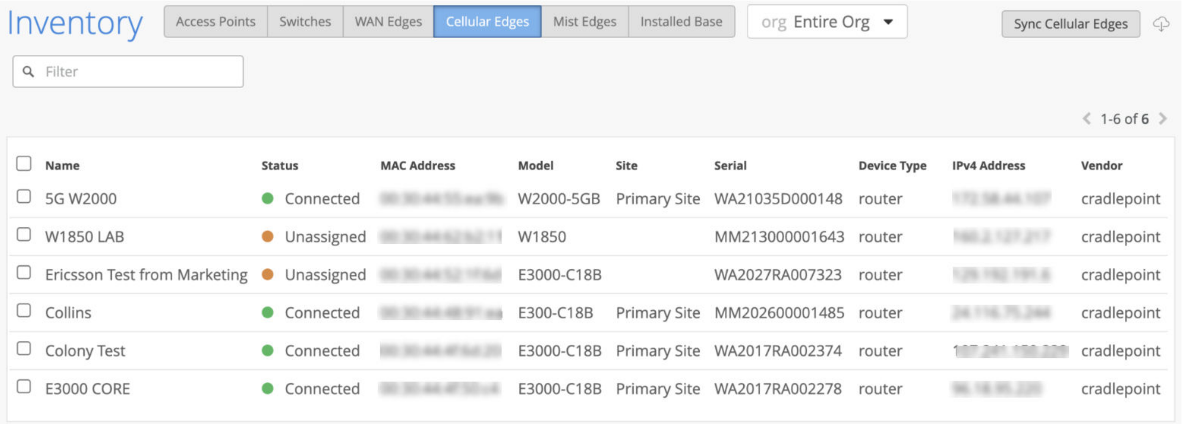
To view the inventory details of the Cradlepoint devices onboarded to the Mist portal:

1. On Juniper Mist portal, go to **Organization** > **Inventory** > **Cellular Edges**.

   The Mist Dashboard's Inventory displays the CradlePoint Inventory for the supported devices that are synced from NetCloud.

2. Click **Sync Cellular Edges** on the Inventory page if the Cellular Edge page does not display any data.

Figure 410: View CradlePoint Devices in Cellular Edge Inventory



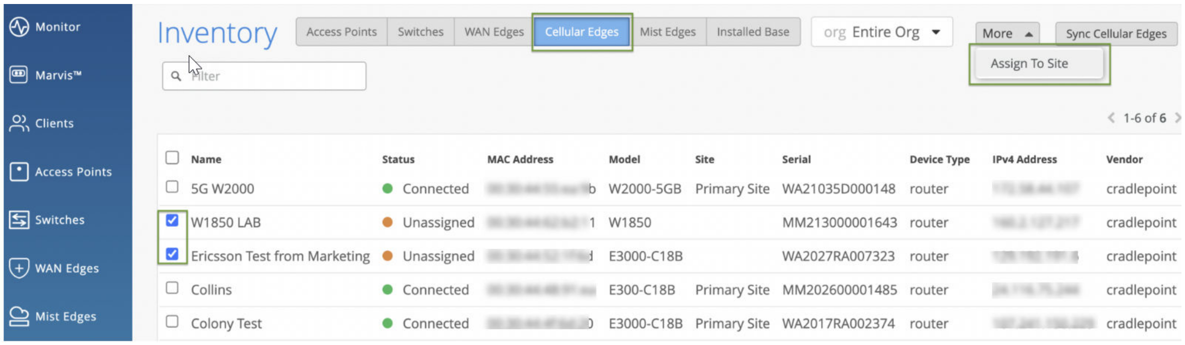
□	Name	Status	MAC Address	Model	Site	Serial	Device Type	IPv4 Address	Vendor
□	5G W2000	● Connected	[redacted]	W2000-5GB	Primary Site	WA21035D000148	router	[redacted]	cradlepoint
□	W1850 LAB	● Unassigned	[redacted]	W1850		MM213000001643	router	[redacted]	cradlepoint
□	Ericsson Test from Marketing	● Unassigned	[redacted]	E3000-C18B		WA2027RA007323	router	[redacted]	cradlepoint
□	Collins	● Connected	[redacted]	E300-C18B	Primary Site	MM202600001485	router	[redacted]	cradlepoint
□	Colony Test	● Connected	[redacted]	E3000-C18B	Primary Site	WA2017RA002374	router	[redacted]	cradlepoint
□	E3000 CORE	● Connected	[redacted]	E3000-C18B	Primary Site	WA2017RA002278	router	[redacted]	cradlepoint

Assign Cradlepoint Devices to a Site

To assign a Cradlepoint device to site:

1. On Juniper Mist portal, go to **Organization** > **Inventory** > **Cellular Edges.**
2. Select the device and click **More** > **Assign to Site** on the page

Figure 411: Assign Cradlepoint Devices to a Site



	Name	Status	MAC Address	Model	Site	Serial	Device Type	IPv4 Address	Vendor
□	5G W2000	● Connected	[redacted]	W2000-5GB	Primary Site	WA21035D000148	router	[redacted]	cradlepoint
☑	W1850 LAB	● Unassigned	[redacted]	W1850		MM213000001643	router	[redacted]	cradlepoint
☑	Ericsson Test from Marketing	● Unassigned	[redacted]	E3000-C18B		WA2027RA007323	router	[redacted]	cradlepoint
□	Collins	● Connected	[redacted]	E300-C18B	Primary Site	MM202600001485	router	[redacted]	cradlepoint
□	Colony Test	● Connected	[redacted]	E3000-C18B	Primary Site	WA2017RA002374	router	[redacted]	cradlepoint

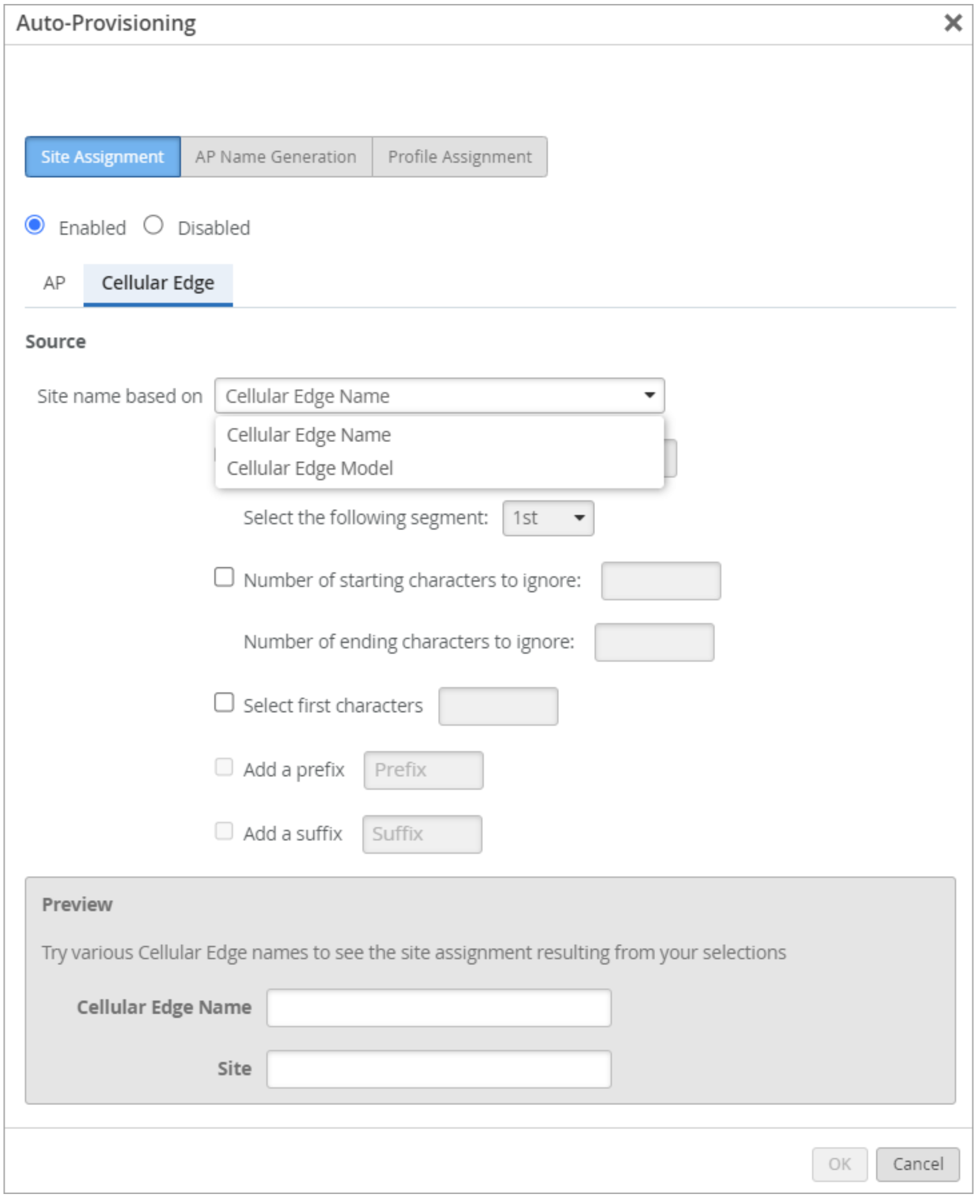
Auto-Provisioning

You can use auto-provisioning to automatically assign Cradlepoint devices to sites. Auto-provisioning allows you to define rules for assigning a device to a site. Mist automatically assigns the device to a site based on the auto-provisioning rules that you configure.

You can set up auto-provisioning from the **Organization** > **Settings** page in the Juniper Mist™ portal. See Automatically Assign Devices to a Site.

Juniper Mist™ can automatically assign a site based on:

- Device name—You can configure rules to derive the site name based on the device name (Cellular Edge Name).



Auto-Provisioning

Site Assignment | AP Name Generation | Profile Assignment

● Enabled ○ Disabled

AP | Cellular Edge

Source

Site name based on: Cellular Edge Name

- Cellular Edge Name
- Cellular Edge Model

Select the following segment: 1st

□ Number of starting characters to ignore:

Number of ending characters to ignore:

□ Select first characters

□ Add a prefix: Prefix

□ Add a suffix: Suffix

Preview

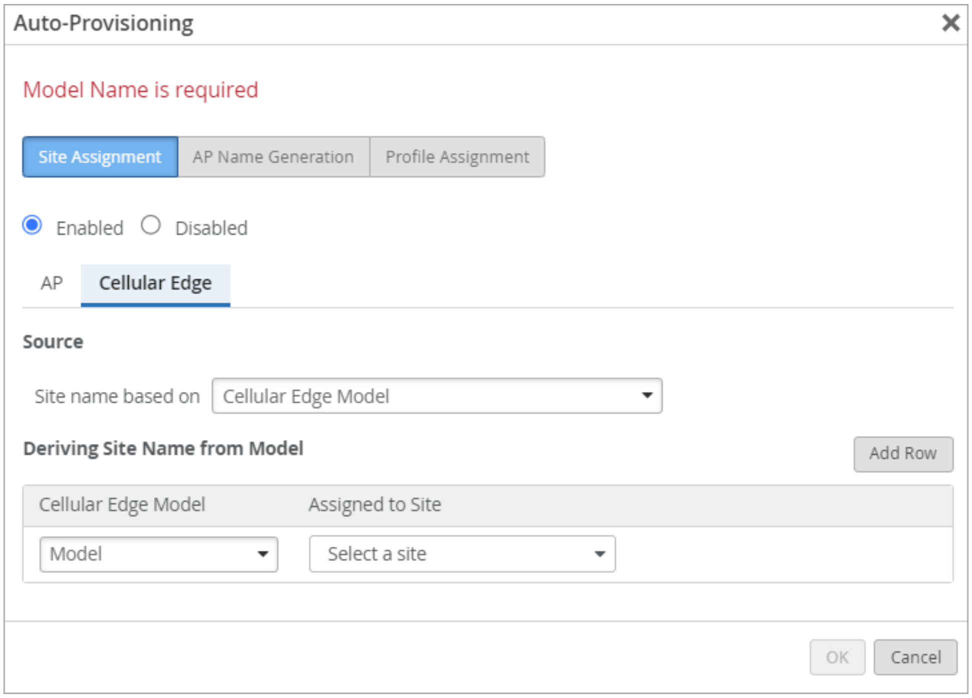
Try various Cellular Edge names to see the site assignment resulting from your selections

Cellular Edge Name

Site

OK | Cancel

- Device model—You can assign devices to sites based on the device model (Cellular Edge Model).



Auto-Provisioning

Model Name is required

● Enabled ○ Disabled

Source

Site name based on: Cellular Edge Model

Deriving Site Name from Model

Cellular Edge Model	Assigned to Site
Model	Select a site

If you do not configure auto-provisioning, Mist uses the LLDP information on the Cradlepoint device for site assignments. Mist first identifies a Juniper device that is connected to a port on the Cradlepoint device and is also in the same organization. Mist then assigns the Cradlepoint device to the same site that the Juniper device is assigned to.

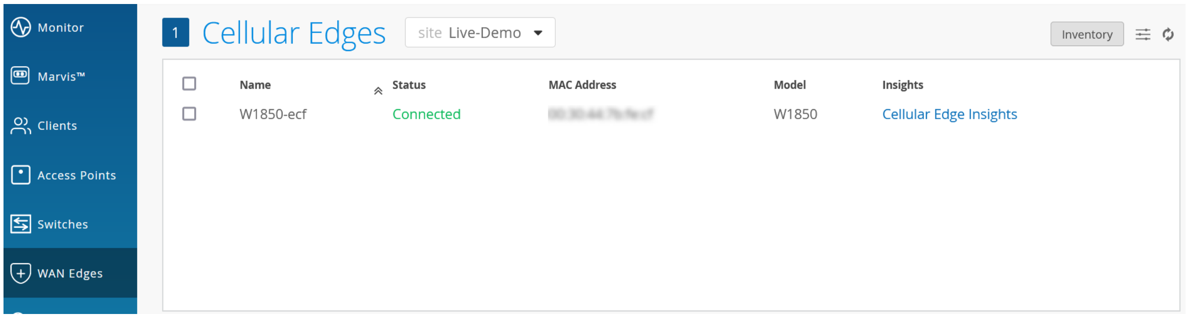
For the LLDP-based automatic site assignment to work, you must ensure that LLDP is enabled on both the Cradlepoint and Juniper devices. Automatic site assignment is applicable only for devices connecting to the Juniper Mist dashboard for the first time.

View Cradlepoint Device Details

To view Cradlepoint device details:

1. On Juniper Mist portal left-navigation bar, go to **WAN Edges > Cellular.**
2. Select the required site from drop-down menu to view Cradlepoint devices assigned to that site.

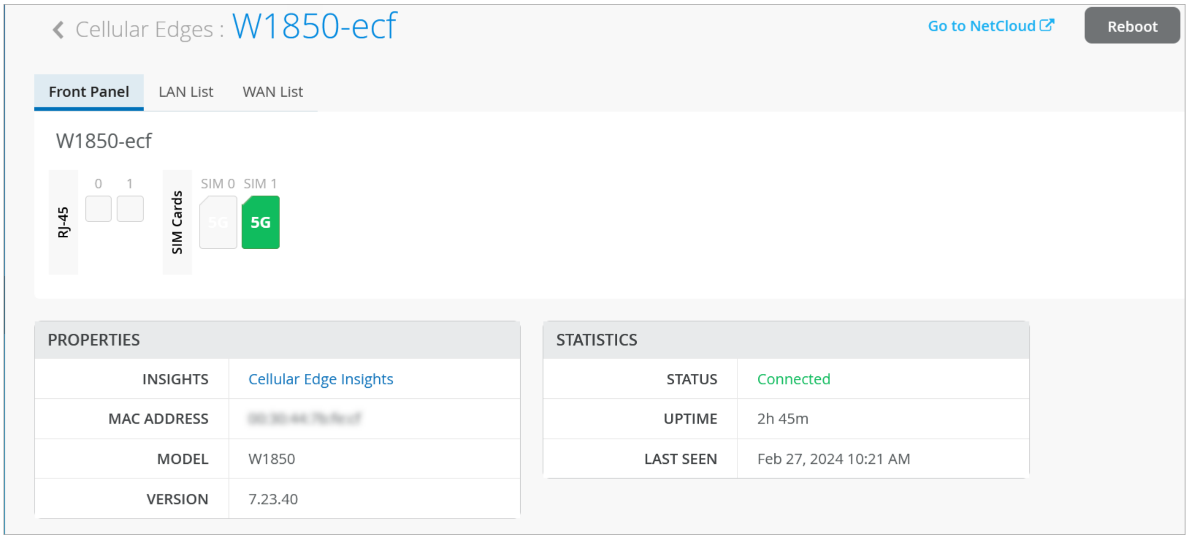
Figure 412: View Cradlepoint Device Details



☐	Name	Status	MAC Address	Model	Insights
☐	W1850-ecf	Connected	[redacted]	W1850	Cellular Edge Insights

Click the device name to open the device details page.

Figure 413: View Cradlepoint Device-Specific Details



PROPERTIES	
INSIGHTS	Cellular Edge Insights
MAC ADDRESS	[redacted]
MODEL	W1850
VERSION	7.23.40

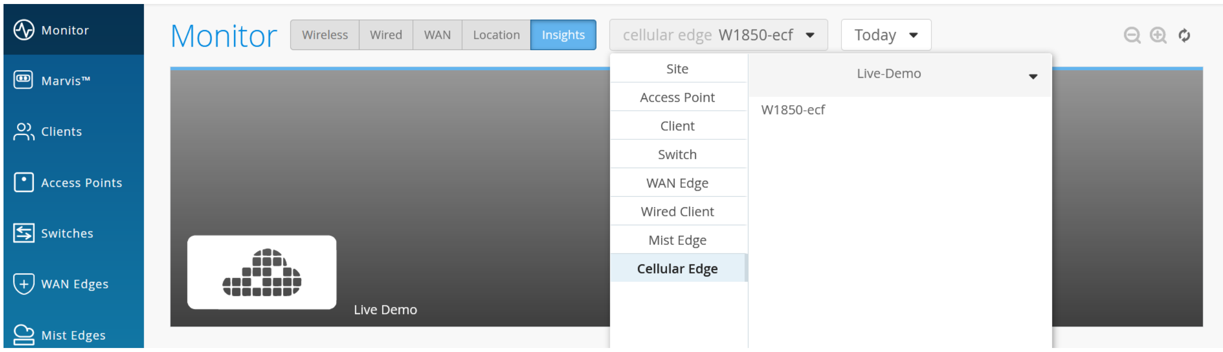
STATISTICS	
STATUS	Connected
UPTIME	2h 45m
LAST SEEN	Feb 27, 2024 10:21 AM

The page lists device-specific information such as properties, statistics, SIM list, and front panel details. You have an option to navigate to the NetCloud dashboard by clicking **Go to NetCloud**.

Get Cradlepoint Device Insights

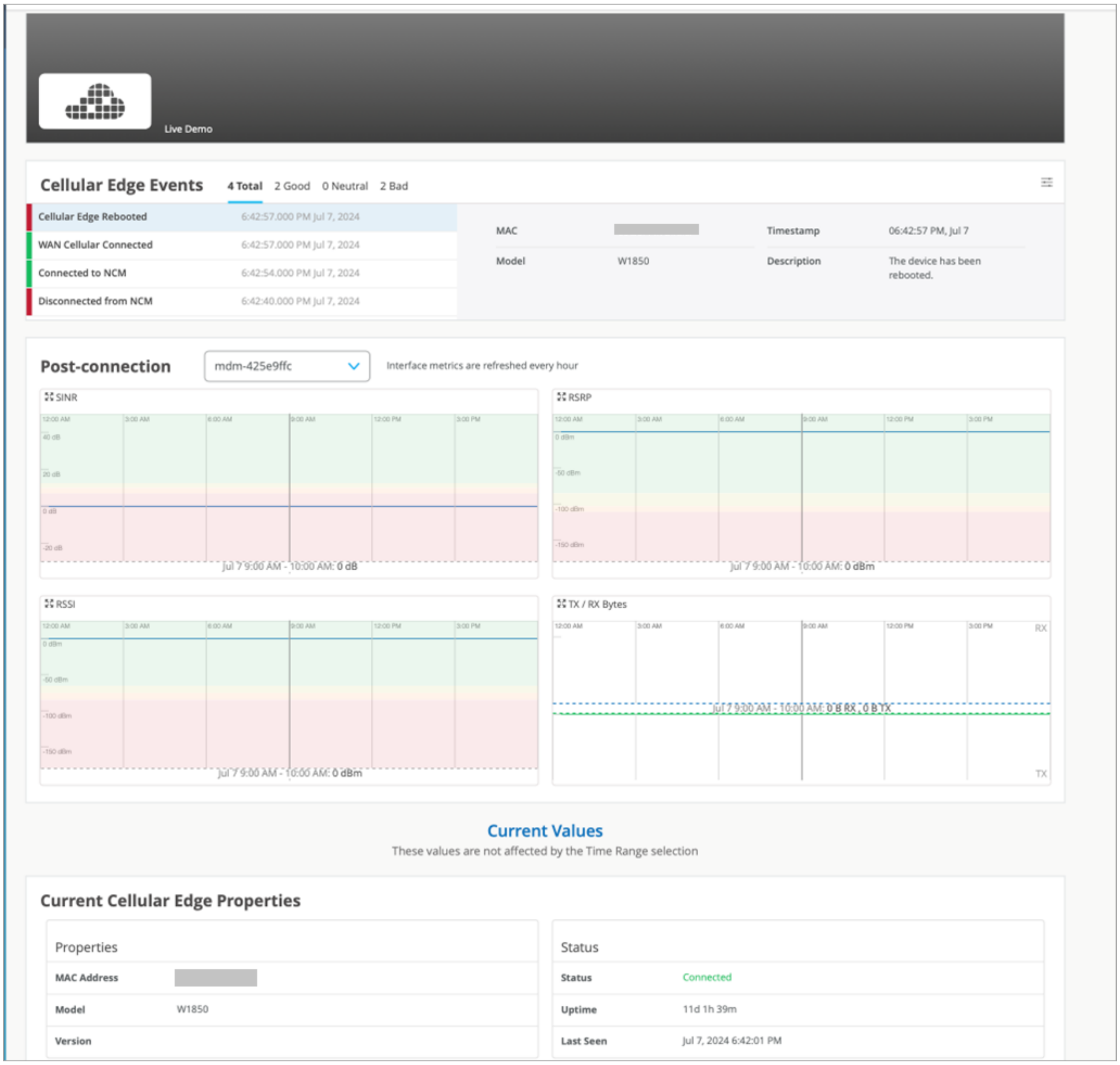
To get details of events related to cellular edge devices, select **Monitor** > **Service Levels** > **Insights**, and then select **Cellular Edge** as the context.

Figure 414: Select Cellular Edge to Display Insights



The page displays Cellular Edge device events, properties, and port details. For Cradlepoint devices, the events are ingested from NetCloud.

Figure 415: Cellular Edge Device Events



Live Demo

Cellular Edge Events 4 Total 2 Good 0 Neutral 2 Bad

Cellular Edge Rebooted	6:42:57.000 PM Jul 7, 2024
WAN Cellular Connected	6:42:57.000 PM Jul 7, 2024
Connected to NCM	6:42:54.000 PM Jul 7, 2024
Disconnected from NCM	6:42:40.000 PM Jul 7, 2024

MAC	[redacted]	Timestamp	06:42:57 PM, Jul 7
Model	W1850	Description	The device has been rebooted.

Post-connection mdm-425e9ffc Interface metrics are refreshed every hour

Current Values

These values are not affected by the Time Range selection

Current Cellular Edge Properties

Properties	
MAC Address	[redacted]
Model	W1850
Version	

Status	
Status	Connected
Uptime	11d 1h 39m
Last Seen	Jul 7, 2024 6:42:01 PM

The time series data charts include:

- SINR—Signal-to-Interference-plus-Noise Ratio (SINR) graph compares the level of the received signal to the level of background noise and interference.

- RSRP—Reference Signal Received Power (RSRP) represents a measure of the received power level in an LTE network. Supported range: -200 through 10 dBm.

- RSSI—Received signal strength indicator (RSSI) is a measurement of the AP radio signal and is typically measured by the client. The scale runs from -100 dBm (weakest) to 0 dBm (strongest).

- RSRQ—Reference Signal Received Quality (RSRQ) measures the quality of the reference signal received by the Cellular Edge device. RSRQ measures the strength of the signal received, by assessing the interference and noise level in the signal.

You can find the supported device events currently ingested at:

https://api.mist.com/api/v1/const/otherdevice_events

Configure Alerts for Cellular Edge Devices

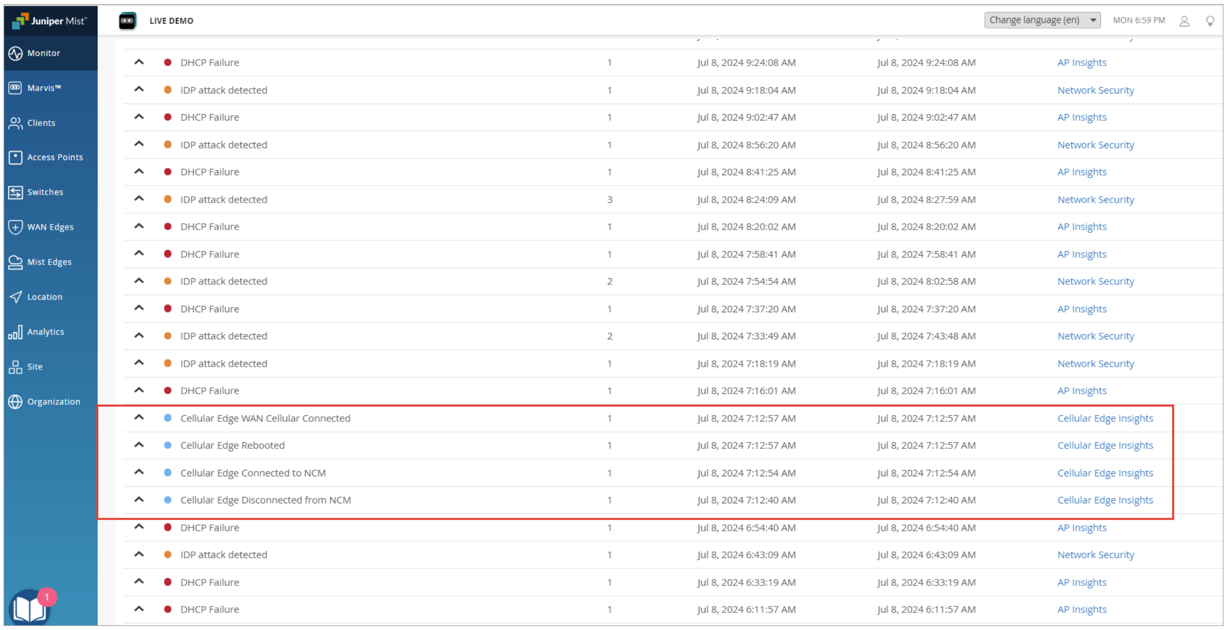
The Alerts Dashboard gives you visibility into issues with Cradlepoint devices. The dashboard provides information about all alerts that you enable on the Alerts Configuration page. You can also enable e-mail notifications for issues that you want to monitor closely. For information about configuring alerts, see Configure Alerts and Email Notifications.

You can configure alerts for issues such as

- Device disconnected from NCM
- Firmware upgrade
- Login failure
- Change of WAN Cellular service type
- Device reboot

For a list of alerts that you can enable for your Cradlepoint device, see Juniper Mist Alert Types.

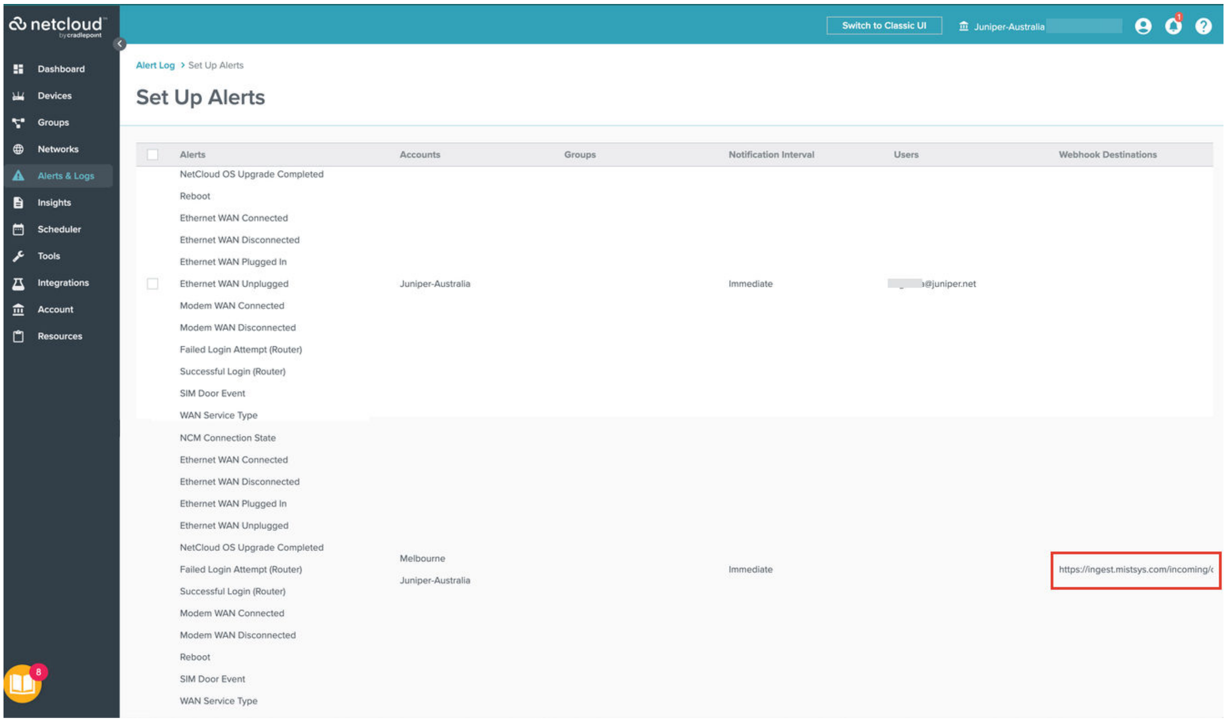
Here is a sample screenshot that shows the alerts for a Cradlepoint device:



DHCP Failure	1	Jul 8, 2024 9:24:08 AM	Jul 8, 2024 9:24:08 AM	AP Insights
IDP attack detected	1	Jul 8, 2024 9:18:04 AM	Jul 8, 2024 9:18:04 AM	Network Security
DHCP Failure	1	Jul 8, 2024 9:02:47 AM	Jul 8, 2024 9:02:47 AM	AP Insights
IDP attack detected	1	Jul 8, 2024 8:56:20 AM	Jul 8, 2024 8:56:20 AM	Network Security
DHCP Failure	1	Jul 8, 2024 8:41:25 AM	Jul 8, 2024 8:41:25 AM	AP Insights
IDP attack detected	3	Jul 8, 2024 8:24:09 AM	Jul 8, 2024 8:27:59 AM	Network Security
DHCP Failure	1	Jul 8, 2024 8:20:02 AM	Jul 8, 2024 8:20:02 AM	AP Insights
DHCP Failure	1	Jul 8, 2024 7:58:41 AM	Jul 8, 2024 7:58:41 AM	AP Insights
IDP attack detected	2	Jul 8, 2024 7:54:54 AM	Jul 8, 2024 8:02:58 AM	Network Security
DHCP Failure	1	Jul 8, 2024 7:37:20 AM	Jul 8, 2024 7:37:20 AM	AP Insights
IDP attack detected	2	Jul 8, 2024 7:33:49 AM	Jul 8, 2024 7:43:48 AM	Network Security
IDP attack detected	1	Jul 8, 2024 7:18:19 AM	Jul 8, 2024 7:18:19 AM	Network Security
DHCP Failure	1	Jul 8, 2024 7:16:01 AM	Jul 8, 2024 7:16:01 AM	AP Insights
Cellular Edge WAN Cellular Connected	1	Jul 8, 2024 7:12:57 AM	Jul 8, 2024 7:12:57 AM	Cellular Edge Insights
Cellular Edge Rebooted	1	Jul 8, 2024 7:12:57 AM	Jul 8, 2024 7:12:57 AM	Cellular Edge Insights
Cellular Edge Connected to NCM	1	Jul 8, 2024 7:12:54 AM	Jul 8, 2024 7:12:54 AM	Cellular Edge Insights
Cellular Edge Disconnected from NCM	1	Jul 8, 2024 7:12:40 AM	Jul 8, 2024 7:12:40 AM	Cellular Edge Insights
DHCP Failure	1	Jul 8, 2024 6:54:40 AM	Jul 8, 2024 6:54:40 AM	AP Insights
IDP attack detected	1	Jul 8, 2024 6:43:09 AM	Jul 8, 2024 6:43:09 AM	Network Security
DHCP Failure	1	Jul 8, 2024 6:33:19 AM	Jul 8, 2024 6:33:19 AM	AP Insights
DHCP Failure	1	Jul 8, 2024 6:11:57 AM	Jul 8, 2024 6:11:57 AM	AP Insights

The alerts are based on the events generated by NetCloud Manager (NCM). When you integrate the Cradlepoint NetCloud Account with Juniper Mist, Mist configures the list of events that will be sent as webhooks to the Mist cloud. The ingest service consumes these webhooks and generates events and alerts. These alerts can be forwarded as e-mails or webhooks from the Mist cloud to an external destination.

You can view the list of events in the **Alert & Logs**>**Set Up Alerts** page in NetCloud Manager as shown in the following example. You can also see the webhook listed on the right.

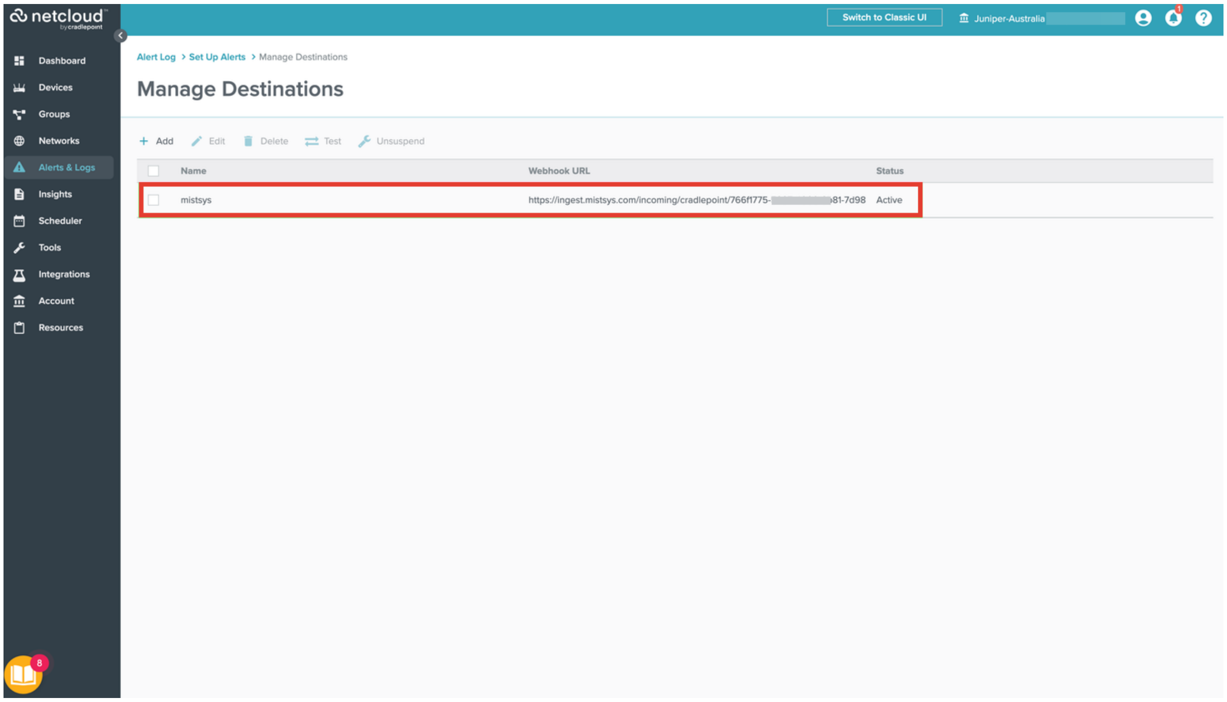


Alert Log > Set Up Alerts

Set Up Alerts

□	Alerts	Accounts	Groups	Notification Interval	Users	Webhook Destinations
□	NetCloud OS Upgrade Completed Reboot Ethernet WAN Connected Ethernet WAN Disconnected Ethernet WAN Plugged In Ethernet WAN Unplugged Modem WAN Connected Modem WAN Disconnected Failed Login Attempt (Router) Successful Login (Router) SIM Door Event WAN Service Type	Juniper-Australia		Immediate	[redacted]@juniper.net	
	NCM Connection State Ethernet WAN Connected Ethernet WAN Disconnected Ethernet WAN Plugged In Ethernet WAN Unplugged NetCloud OS Upgrade Completed Failed Login Attempt (Router) Successful Login (Router) Modem WAN Connected Modem WAN Disconnected Reboot SIM Door Event WAN Service Type	Melbourne Juniper-Australia		Immediate		https://ingest.mistsys.com/incoming/c

You can view the complete webhook URL in the **Alert & Logs**>**Set Up Alerts**>**Manage Destinations** page.



Manage Destinations

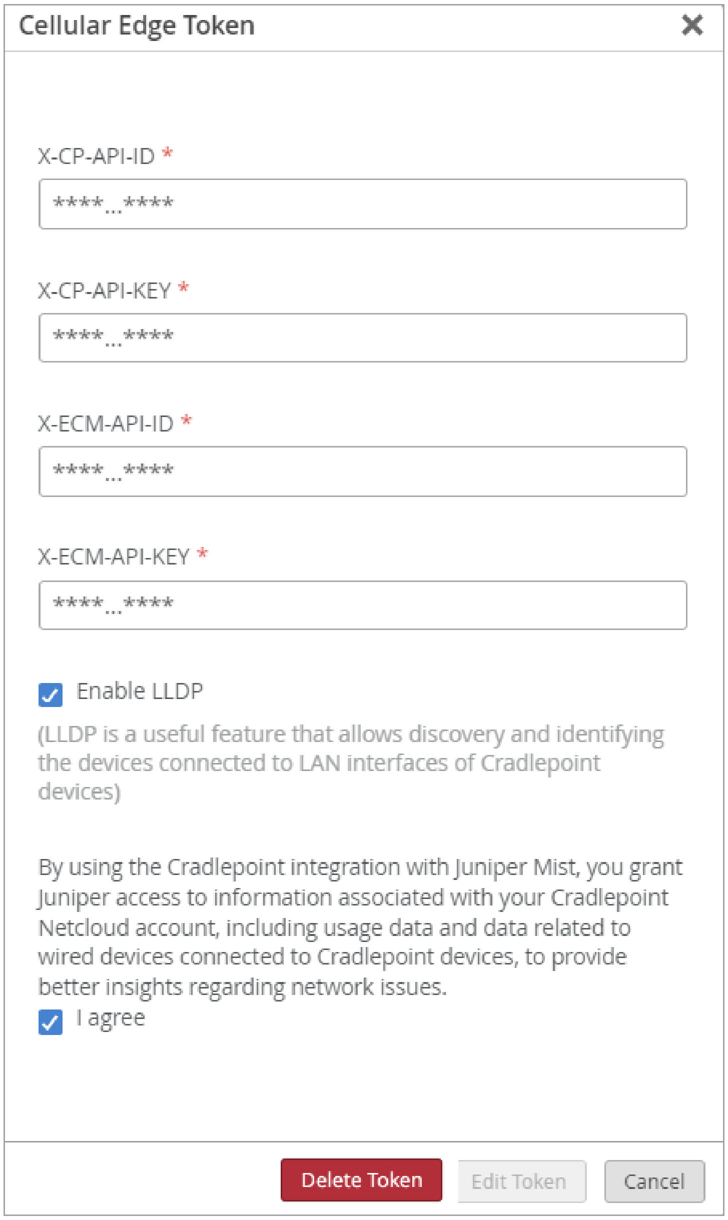
	Name	Webhook URL	Status
□	mistsys	https://ingest.mistsys.com/incoming/cradlepoint/766f1775-[redacted]81-7d98	Active

Unlink Cradlepoint Account From Juniper Mist Portal

1. On Juniper Mist portal, go to **Organization** > **Admin**> **Settings**.
2. Scroll-down to **Third Party Token** pane.
3. Click the Cradlepoint entry in the table.

   The The Cellular Edge Token window opens.

Figure 416: Delete Cradlepoint Tokens



Cellular Edge Token ✕

X-CP-API-ID *

****...****

X-CP-API-KEY *

****...****

X-ECM-API-ID *

****...****

X-ECM-API-KEY *

****...****

☑ Enable LLDP

(LLDP is a useful feature that allows discovery and identifying the devices connected to LAN interfaces of Cradlepoint devices)

By using the Cradlepoint integration with Juniper Mist, you grant Juniper access to information associated with your Cradlepoint Netcloud account, including usage data and data related to wired devices connected to Cradlepoint devices, to provide better insights regarding network issues.

☑ I agree

4. Click **Delete Token**.

   Table will not have any key entry post delete and Cellural Edge inventory also does not display any Cradlepoint devices.

SEE ALSO

Configure WAN Edge Templates for SRX Series Firewalls | 217

Configure Hub Profiles for SRX Series Firewalls | 197

WAN Assurance Configuration Overview | 166

Juniper Mist WAN Assurance Configuration Hierarchy | 13

8

CHAPTER

Monitor and Troubleshoot

WAN Assurance Monitoring, SLE, and Troubleshooting Overview

IN THIS SECTION

The Juniper® Mist™ WAN Assurance Monitoring, SLE, and Troubleshooting chapter is for system administrators and technical support who maintain enterprise SD-WAN networks. You should have completed the" WAN Configuration for SRX Series Firewalls" on page 166 or "WAN Configuration for Session Smart Routers" on page 31 before continuing with the WAN Edge Monitoring, SLE, and Troubleshooting.

Driven by Mist AI, the Juniper SD-WAN solution simplifies the monitoring and troubleshooting of the WAN edge. Juniper Mist WAN Assurance does this by consistently and proactively monitoring numerous variables that impact a user's network experience. Both the Juniper® Session Smart™ Router and Juniper® SRX Series Firewalls WAN Assurance platforms have unique solutions to the WAN edge and overlay that impact provisioning and deployment. Because of this, those monitoring and troubleshooting actions are platform-specific, and understanding your WAN Assurance platform is crucial.

You'll find separate topics for the Juniper® Session Smart™ Router and Juniper® SRX Series Firewalls WAN edge Monitoring, SLE, and Troubleshooting.

WAN Edge Monitoring

In the WAN edge monitoring guides, you'll explore the most efficient ways to monitor your WAN edge device in the Mist UI following your initial deployment phase. The Session Smart Secure Vector Routing WAN Assurance solution monitors liveness, jitter, latency, loss, and mean opinion score (MOS) to inform those user minutes. The SRX Series Firewall monitors the utilization of the IPsec tunnels that make up the overlay on the SRX Series WAN Assurance solution.

- "Troubleshoot Session Smart Router Deployed as WAN Edge " on page 613

- "Troubleshoot SRX Series Firewalls" on page 633

WAN Edge SLEs

The Juniper Mist WAN Assurance solution simplifies the entire network diagnosis process. WAN edge devices track metrics for WAN Edge Health, WAN Link Health, and Application Health to derive percentage ratings, which Juniper calls user minutes. User-minute metrics inform the basis for Mist monitoring, called service-level experiences (SLEs). Using critical metrics on application response times, WAN link status, gateway health, and other network conditions, both the SRX Series and Session Smart WAN edge devices gain insights into how these metrics impact end-user experiences and use them to identify the root causes of any service degradation. You can find an overview of all Mist SLEs here: https://www.juniper.net/documentation/us/en/software/mist/net-monitor/topics/concept/service-level-expectations.html. You'll find SLEs specific to your WAN edge device deployed in Juniper Mist™ WAN Assurance.

"WAN Assurance Monitoring, SLE, and Troubleshooting Overview" on page 535

Video: NOW in 60: Mist SLEs for WAN Assurance

WAN Edge Troubleshooting

Juniper Mist WAN Assurance troubleshooting tools give system admins proactive insights alongside traditional tools for diagnosing WAN edge issues and identifying things on a per-application level down to granular interface and port metrics for both Session Smart Routers and SRX Series Firewall WAN edge devices. Users will see the most difference in their guides depending on their platform when WAN edge troubleshooting. The Session Smart Secure Vector Routing creates the overlay, while a unique implementation of Bidirectional Forwarding Detection between Session Smart devices helps troubleshooting. You'll use Mist UI dashboard tools and leverage Juniper Mist Application Visibility, Application SLE, and Marvis to troubleshoot your Session Smart WAN edge.

For example, at times, within an overlay tunnel connecting a Hub to a spoke, not all the advertised routes may be visible on the overlay, which can lead to traffic being unable to traverse the tunnel. In such cases, we recommend following actions:

- Ensure the overlay advertisement is enabled for the networks that need to be advertised. Go to **Organization** > **WAN** > **Networks** and check if **Advertised via Overlay** is enabled for the specific network.

- Verify that the overlay tunnel is configured properly and that the correct routes are being advertised.

- Check the configuration on both the hub and spoke devices and ensure that the overlay tunnel is properly configured, including the correct IP addresses and route advertisements.
- Check the routing configuration on both the Hub and spoke devices. Verify that the routing tables on both devices include the necessary routes for the overlay tunnel, including routes to each other's network segments.
- Check the firewall configuration on both the hub and spoke devices. Ensure that the firewall rules are properly configured to allow traffic to pass across the overlay tunnel.
- Check the MTU (Maximum Transmission Unit) settings on both the hub and spoke devices. Verify that the MTU is set to the same value on both devices and that it is not set too high, which could cause fragmentation and slow down traffic.
- Check the connectivity between the hub and spoke devices. Verify that there are no network connectivity issues between the two devices, including issues with firewalls or NAT (Network Address Translation) devices in between.
- Check the logs on both the Hub and spoke devices for any error messages related to the overlay tunnel. Use the **show log** command to view the system logs and look for any errors related to the overlay tunnel.
- Check the firewall filters to make sure that traffic is allowed to pass through the tunnel.
- If you are still unable to resolve the issue, try restarting both the Hub and spoke devices

Troubleshooting gateways on your SRX Series Firewall uses the powerful and versatile Junos OS with the same Application Visibility, Application SLE, and Marvis to diagnose WAN edge connectivity.

- "Troubleshoot Session Smart Router Deployed as WAN Edge " on page 613
- "Troubleshoot SRX Series Firewalls" on page 633

RELATED DOCUMENTATION

Introduction to Juniper Mist WAN Assurance | 2
Juniper Mist WAN Assurance Platform Considerations | 10
Juniper Mist WAN Assurance Configuration Hierarchy | 13

Monitor SRX Series Firewall Deployed as WAN Edge

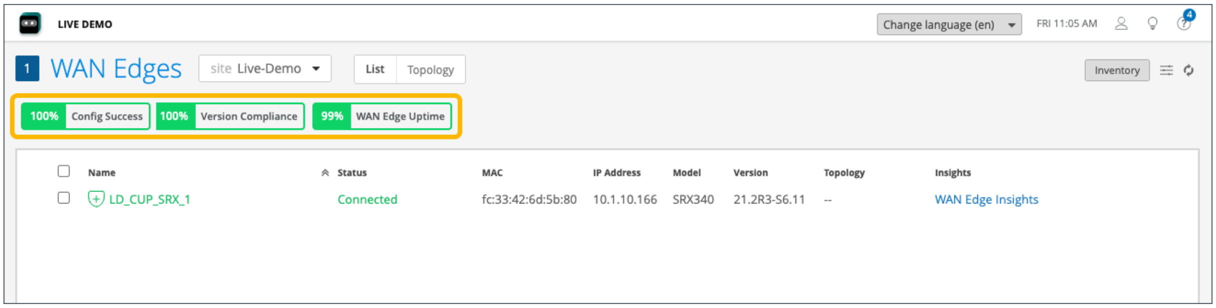
IN THIS SECTION

In monitoring a Juniper® SRX Series Firewall deployed as a WAN edge device, you'll explore the most efficient ways to monitor your WAN edge device in the Juniper Mist™ portal following your initial deployment phase.

WAN Edges

In the Juniper Mist Portal, select **WAN Edges > WAN Edges** to view basic device monitoring information. Notice the Organization name at the top of the GUI, LIVE DEMO. This is the largest container and represents your entire organization. Beneath the organization name, you can see your site devices in either a List format or a graphical Topology format. Here, you see **Live-Demo** is your site, and LD_CUP_SRX_1 is your WAN edge device.

Figure 417: Accessing WAN Edges Page



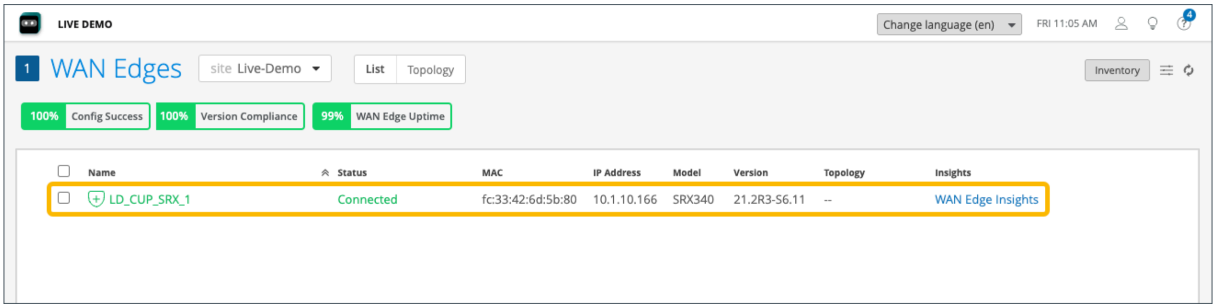
	Name	Status	MAC	IP Address	Model	Version	Topology	Insights
□	LD_CUP_SRX_1	Connected	fc:33:42:6d:5b:80	10.1.10.166	SRX340	21.2R3-S6.11	--	WAN Edge Insights

The List view outlines the following information:

- Config Success—Percentage of online WAN edges with successful configuration.

- Version Compliance—Percentage of WAN edges that have the same software version per model.
- WAN Edge Uptime—Percentage of time a WAN edge was up during the past seven days, averaged across all WAN edges.

Figure 418: WAN Edges List View



☐	Name	Status	MAC	IP Address	Model	Version	Topology	Insights
☐	LD_CUP_SRX_1	Connected	fc:33:42:6d:5b:80	10.1.10.166	SRX340	21.2R3-S6.11	--	WAN Edge Insights

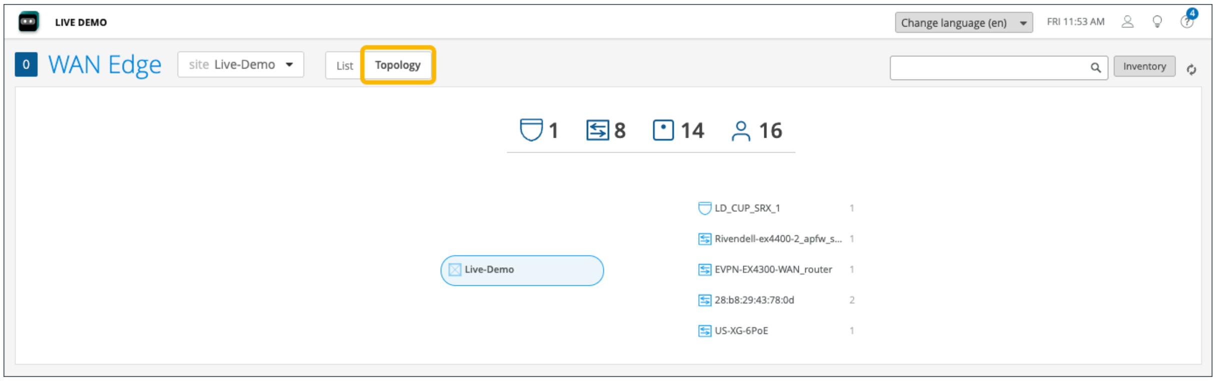
Beneath, you'll find WAN edge device details as shown in Table 63 on page 539.

Table 63: WAN Edge Device Details

Fields	Description
Name	Name
Status	Connected or disconnected
MAC	MAC address
IP Address	IP address
Model	Juniper Networks® SRX Series Firewalls or Juniper® Session Smart™ Routers.
Version	SRX Software Version
Topology	Hub or Spoke
Insights	Provides a direct link to the WAN Edge Insights page.

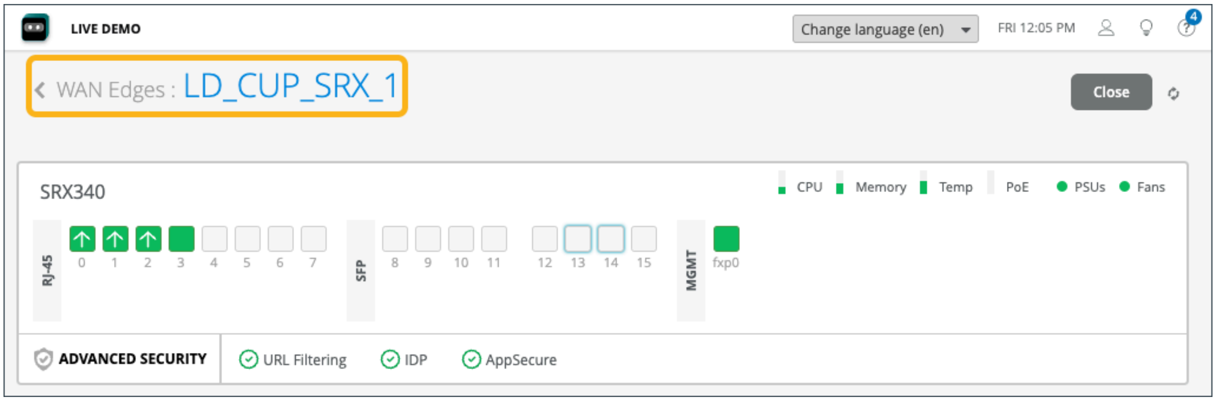
The **Topology** format presents the same information as the **List** view. For example, if you hover over the LD_CUP_SRX_1 device, you'll see the same information that displayed in the List view.

Figure 419: WAN Edges Topology View



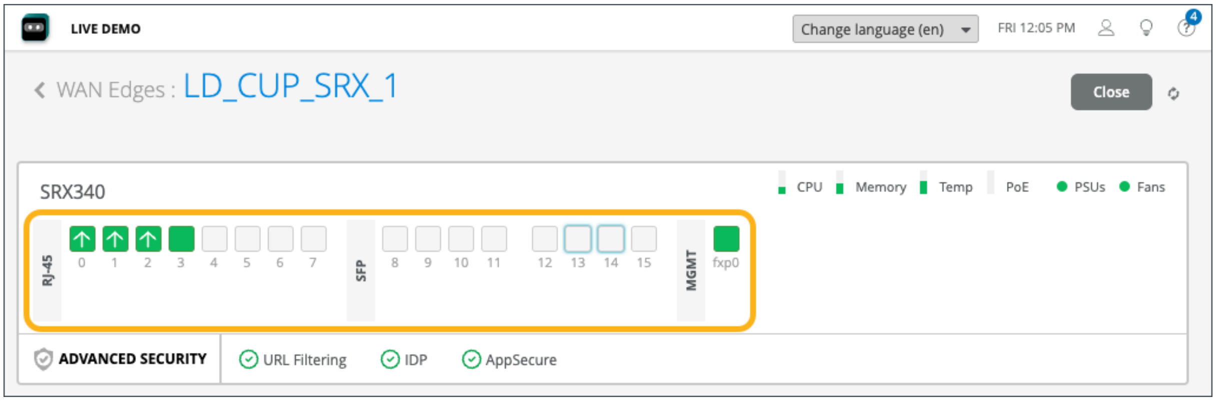
On both the List and Topology view, selecting your WAN edge device (LD_CUP_SRX_1 in this example) brings you to its Device Information page. The Device Information page provides different categories of monitoring information for your WAN edge device.

Figure 420: WAN Edges Device Information Page



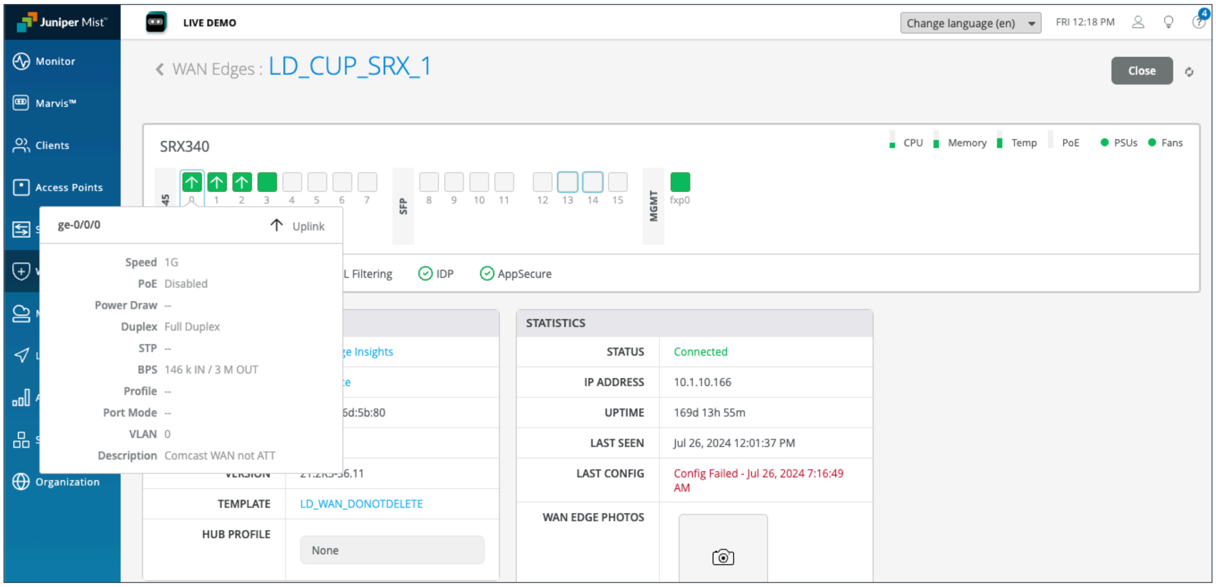
The first thing you'll notice on the Device Information Page are details about the WAN edge device you selected, (LD_CUP_SRX_1 in our figure). The information includes a graphical front view of the device ports and baseline status information such as CPU and memory utilization.

Figure 421: WAN Edges Device Information - Interfaces



For each Gigabit Ethernet interface, you'll find link information.

Figure 422: WAN Edge Device Information Page - Details



ge-0/0/0 ↑ Uplink

Speed	1G
PoE	Disabled
Power Draw	--
Duplex	Full Duplex
STP	--
BPS	146 k IN / 3 M OUT
Profile	--
Port Mode	--
VLAN	0
Description	Comcast WAN not ATT

TEMPLATE	LD_WAN_DONOTDELETE
HUB PROFILE	None

STATISTICS

STATUS	Connected
IP ADDRESS	10.1.10.166
UPTIME	169d 13h 55m
LAST SEEN	Jul 26, 2024 12:01:37 PM
LAST CONFIG	Config Failed - Jul 26, 2024 7:16:49 AM

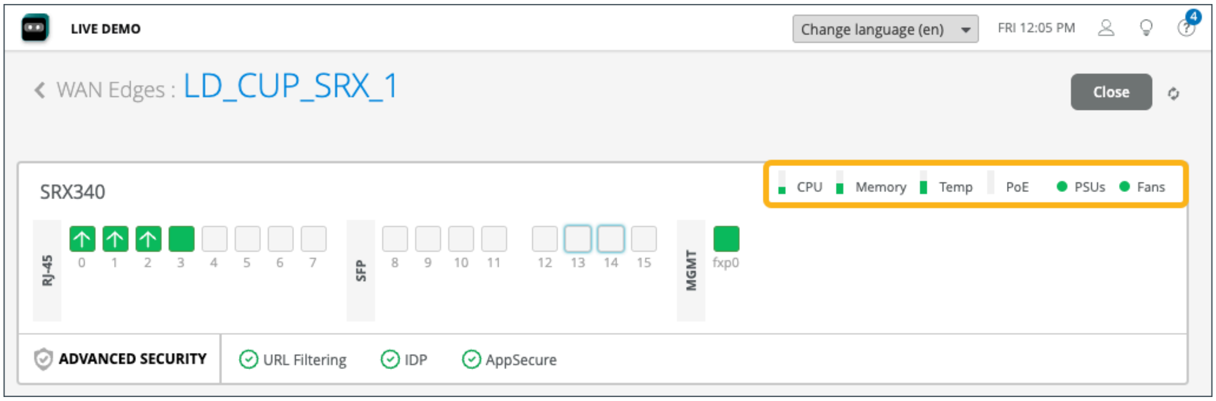
Table 64: Link Information for Gigabit Ethernet Interface

Fields	Description
Speed	Rated speed
PoE	Enabled or disabled
Power Draw	Measured PoE power draw

Duplex	Full or half
STP	True or false
BPS	Bits/second
Profile	The name of the Port profile assigned to the port
Port Mode	The mode of the port profile configuration (Trunk, Access, Port Network, or VoIP Network)
VLAN	VLAN tag
Description	Interface description

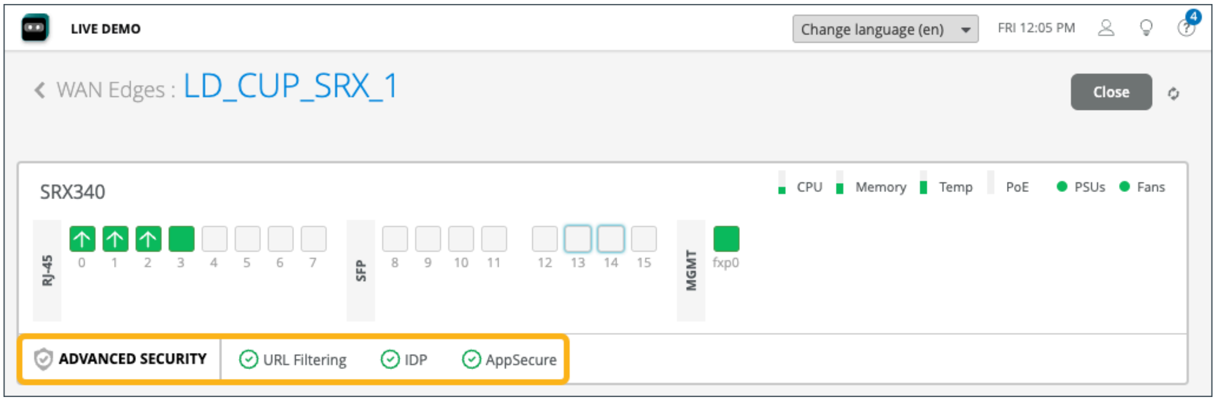
The CPU, Memory, and other status icons indicate how your device behaves. Hover over each status icon for deeper insights.

Figure 423: WAN Edges - CPU, Memory, and other status icons



Advanced Security information is listed below the device ports with a check mark or an X, indicating whether URL filtering, intrusion detection and prevention (IDP), or AppSecure (for application visibility) is active on this device. Here, URL filtering, IDP, and AppSecure are active with the green check mark.

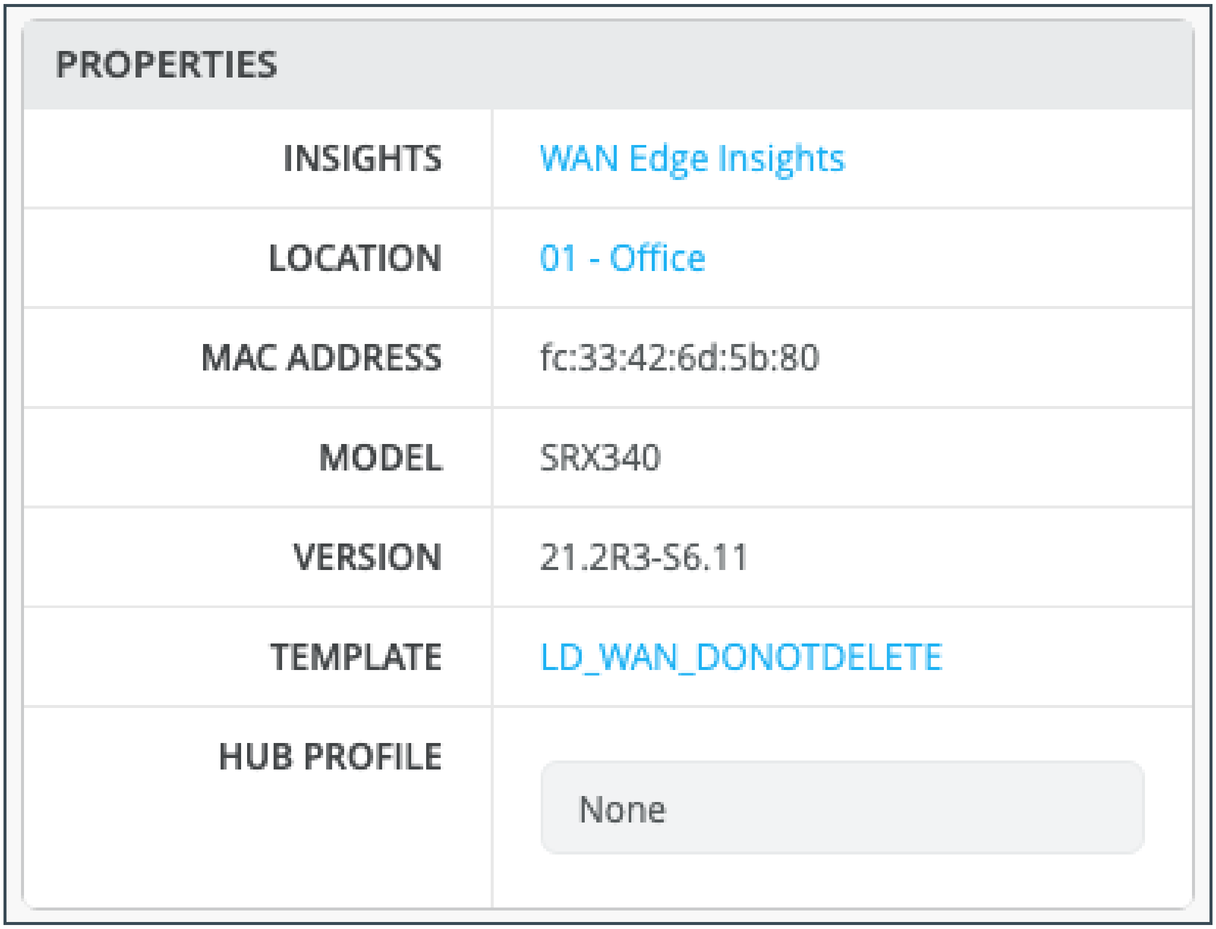
Figure 424: Advanced Security Details



ADVANCED SECURITY ✓ URL Filtering ✓ IDP ✓ AppSecure

Below the port information and security section, you'll find generalized data for your WAN edge device, including:

Figure 425: WAN Edge Device Properties



PROPERTIES

INSIGHTS	WAN Edge Insights
LOCATION	01 - Office
MAC ADDRESS	fc:33:42:6d:5b:80
MODEL	SRX340
VERSION	21.2R3-S6.11
TEMPLATE	LD_WAN_DONOTDELETE
HUB PROFILE	None

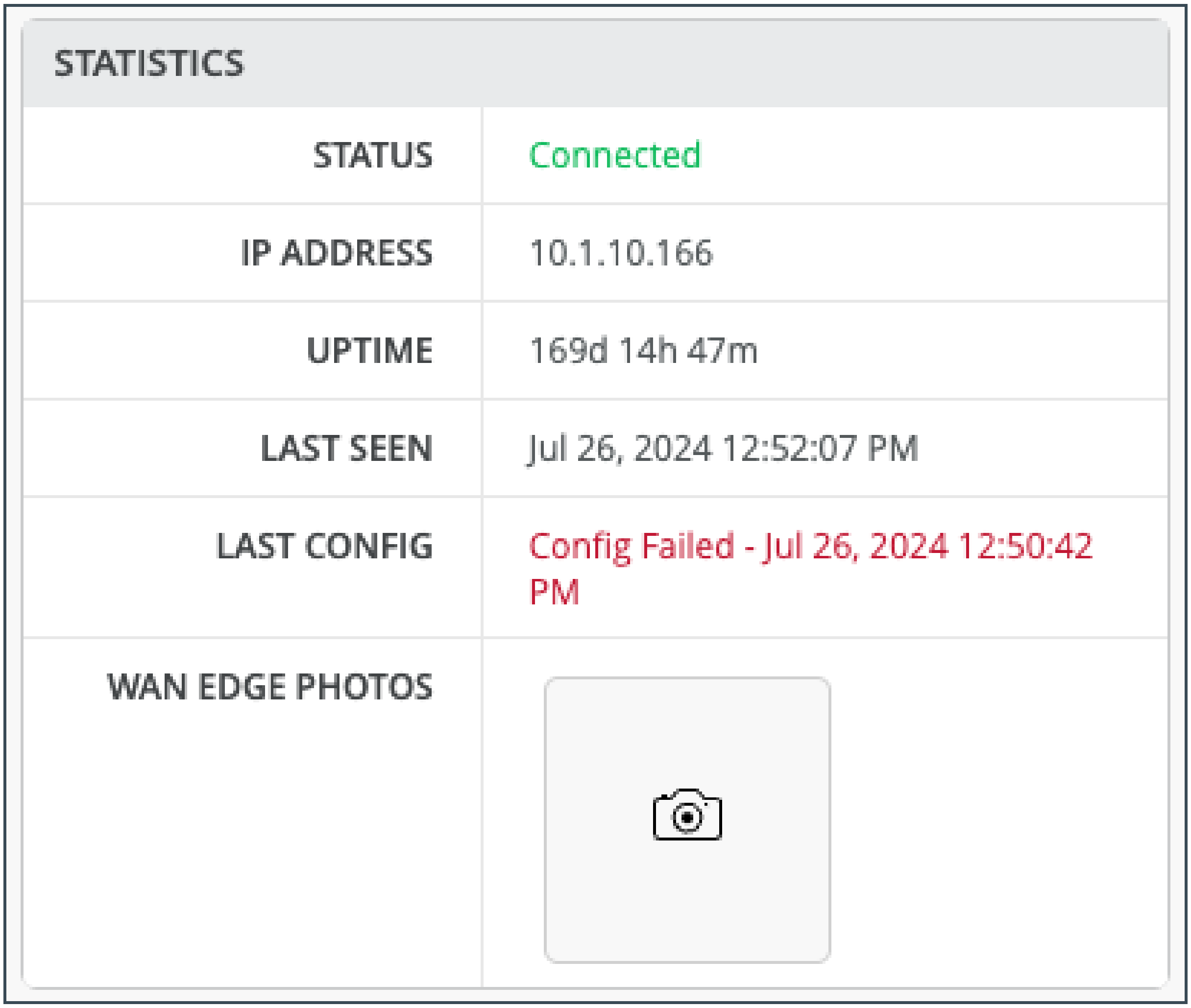
Properties contains generalized platform-related information.

Table 65: WAN Edge Platform-Related Details

Field	Description
Insights	Provides a direct link to WAN Edge Insights.
Location	Provides floorplan information.
MAC Address	MAC Address for the SRX device.
Model	Indicates if model type is SSR or SRX.
Version	Version of SRX Software.
Template	The WAN edge template applied to the device.
Hub Profile	The Hub Profile applied to the device.

Statistics displays action information about your platform.

Figure 426: WAN Edge Device Statistics



STATISTICS

STATUS	Connected
IP ADDRESS	10.1.10.166
UPTIME	169d 14h 47m
LAST SEEN	Jul 26, 2024 12:52:07 PM
LAST CONFIG	Config Failed - Jul 26, 2024 12:50:42 PM
WAN EDGE PHOTOS	

Table 66: WAN Edge Device Statistics

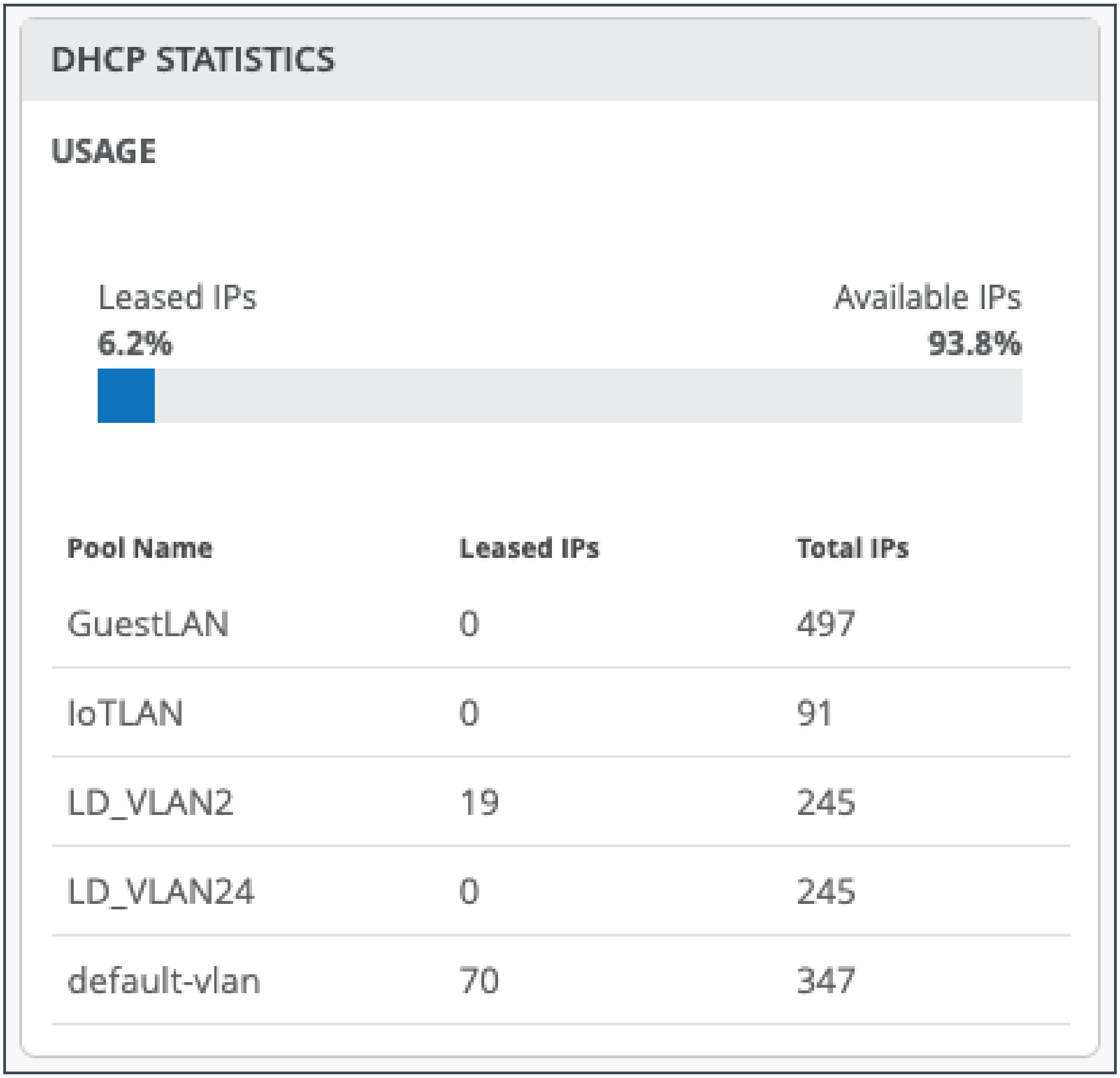
Field	Description
Status	Connected/Disconnected
IP Address	The IP address of the WAN edge device
Uptime	Day/Hour/Min uptime information
Last Seen	Last login
Last Config	Last Commit

WAN Edge Photos	Photos of the WAN edge device

If you configured DHCP servers on the WAN router itself, there will also be a DHCP Statistics pane with information about the leased IPs.

- **DHCP Statistics** presents IP information related to dynamic distributed IP addresses.

Figure 427: WAN Edge Device DHCP Statistics



DHCP STATISTICS

USAGE

Leased IPs 6.2%

Available IPs 93.8%

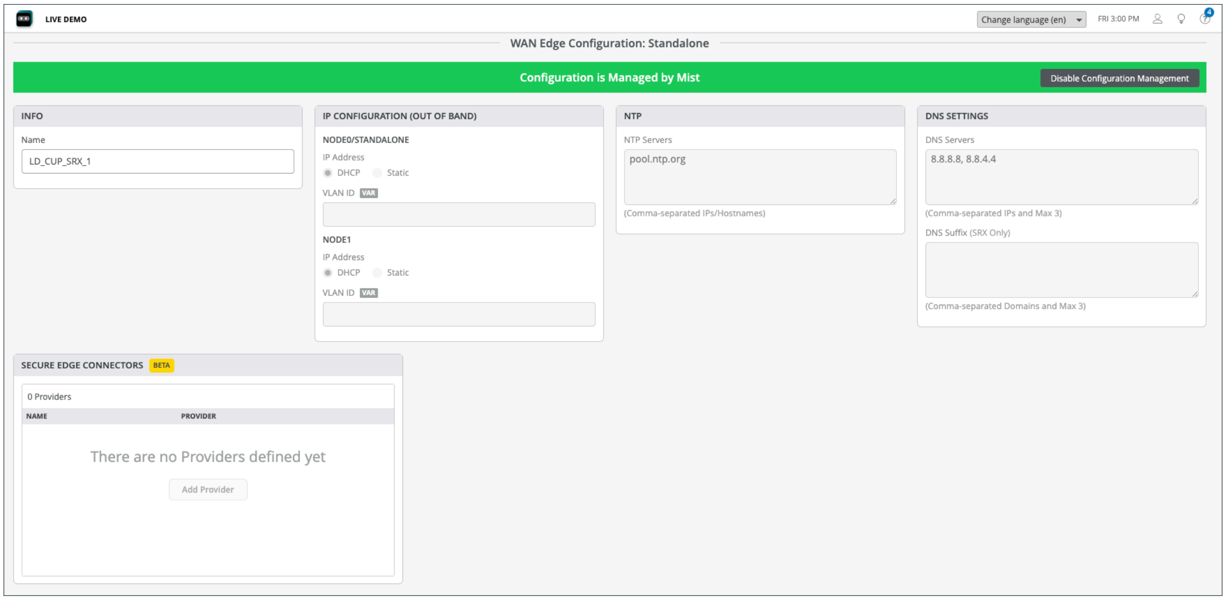
Pool Name	Leased IPs	Total IPs
GuestLAN	0	497
IoTLAN	0	91
LD_VLAN2	19	245
LD_VLAN24	0	245
default-vlan	70	347

Table 67: WAN Edge Device DHCP Statistics

Field	Description
Usage	The total figure presented as a percentage of Leased and Available IPs.
Pool Name	The name for given pool of addresses.
Leased IPs	Number of used IP addresses in each pool.
Total IPs	Total number of available IP addresses in each pool.

Scrolling down the Device Information page, you'll find configuration information for your WAN edge. Usually, WAN edges inherit templates or profiles. However, you can make individual changes to the configuration to be pushed to the device. In this example, a standalone WAN Edge Template was used.

Figure 428: WAN Edge Configuration: Standalone



WAN Edge Configuration: Standalone

Configuration is Managed by Mist

INFO

Name: LD_CUP_SRX_1

IP CONFIGURATION (OUT OF BAND)

NODE0/STANDALONE

IP Address: ● DHCP ○ Static

VLAN ID VAR

NODE1

IP Address: ● DHCP ○ Static

VLAN ID VAR

NTP

NTP Servers: pool.ntp.org

(Comma-separated IPs/Hostnames)

DNS SETTINGS

DNS Servers: 8.8.8.8, 8.8.4.4

(Comma-separated IPs and Max 3)

DNS Suffix (SRX Only)

(Comma-separated Domains and Max 3)

SECURE EDGE CONNECTORS BETA

0 Providers

NAME	PROVIDER

There are no Providers defined yet

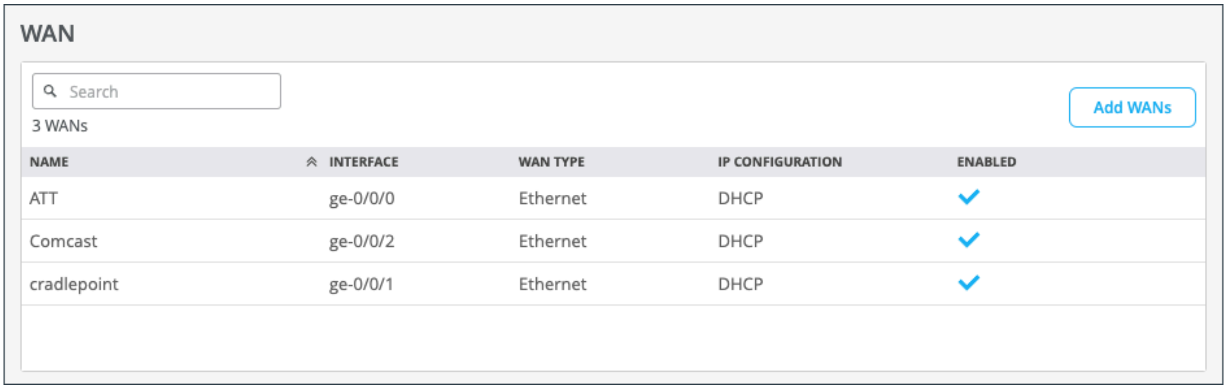
Table 68: WAN Edge Configuration: Standalone

Field	Description
Info	The name of the SRX device.
IP Configuration	Node0/standalone DHCP/Static, VLAN ID, node 1 DHCP/Static, VLAN ID.

NTP	Time Servers IP/Hostnames.
DNS Settings	DNS Servers, DNS Suffix (SRX only DNS suffix info).
Secure Edge Connectors (BETA)	Provider for the Secure Edge Connector.

Scrolling past the configuration, you'll find information for your connected WANs and LANs.

Figure 429: WAN Details



WAN

Search

3 WANs

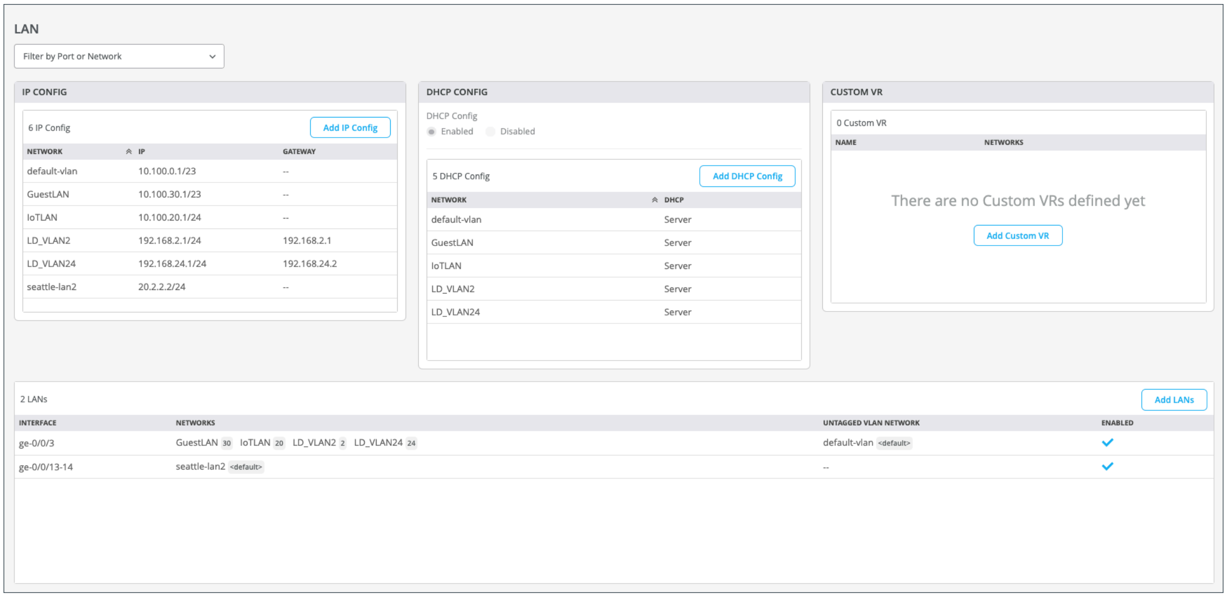
Add WANs

NAME	INTERFACE	WAN TYPE	IP CONFIGURATION	ENABLED
ATT	ge-0/0/0	Ethernet	DHCP	✓
Comcast	ge-0/0/2	Ethernet	DHCP	✓
cradlepoint	ge-0/0/1	Ethernet	DHCP	✓

Table 69: WAN Details

Field	Description
Name	Selected WAN Interface Name
Interface	Supports one of these interfaces for aggregation: ge-0/0/1, ge-0/0/1-5, or reth0.
WAN Type	Ethernet, DSL (SRX Only), or LTE
IP Configuration	DHCP, Static, or PPPoE
Enabled	Check mark indicates that the interface is enabled.

Figure 430: LAN Details



LAN

IP CONFIG

6 IP Config

NETWORK	IP	GATEWAY
default-vlan	10.100.0.1/23	--
GuestLAN	10.100.30.1/23	--
IoTLAN	10.100.20.1/24	--
LD_VLAN2	192.168.2.1/24	192.168.2.1
LD_VLAN24	192.168.24.1/24	192.168.24.2
seattle-lan2	20.2.2.2/24	--

DHCP CONFIG

DHCP Config

● Enabled ○ Disabled

5 DHCP Config

NETWORK	DHCP
default-vlan	Server
GuestLAN	Server
IoTLAN	Server
LD_VLAN2	Server
LD_VLAN24	Server

CUSTOM VR

0 Custom VR

NAME	NETWORKS

There are no Custom VRs defined yet

2 LANs

INTERFACE	NETWORKS	UNTAGGED VLAN NETWORK	ENABLED
ge-0/0/3	GuestLAN 30 IoTLAN 20 LD_VLAN2 2 LD_VLAN24 24	default-vlan <default>	✓
ge-0/0/13-14	seattle-lan2 <default>	--	✓

Table 70: LAN Details

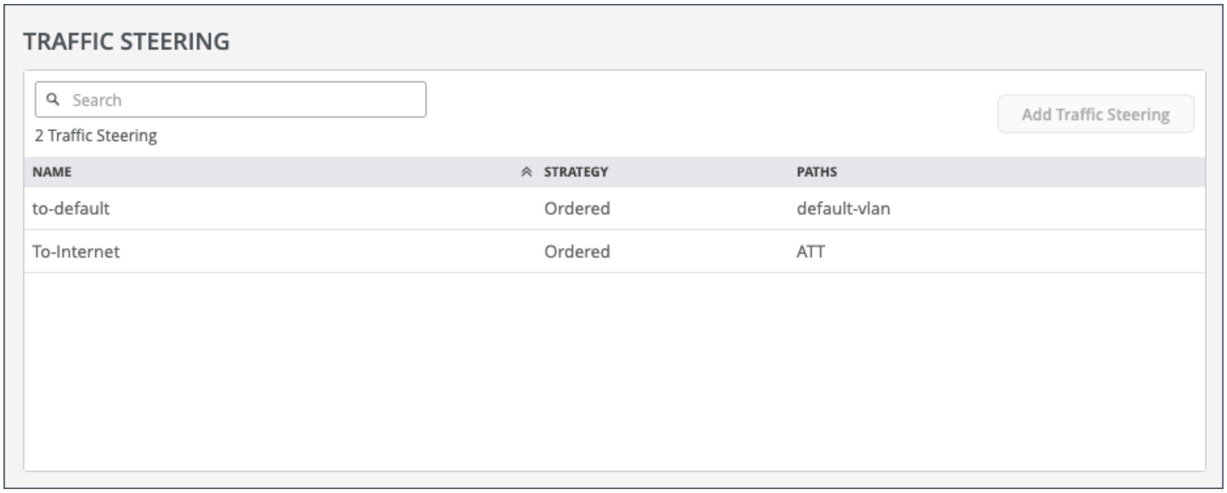
Field	Description
IP Config	Network, IP Address, Prefix Length.
DHCP Config	Server or Relay.
Custom VR	A virtual router that you can configure to be used in automatic route leaking.
LANs	• Interface—Supports one of these interfaces for aggregation: ge-0/0/1, ge-0/0/1-5, or reth0. • Networks—Networks that participate in the LAN. • Untagged VLAN Network—Untagged VLAN networks that participate in the LAN (SRX only). • Enabled—Check mark indicates that the interface is enabled.

Scrolling down, you have sections for Traffic Steering, Application Policies, and Routing (OSPF, BGP, Routing Policies, and Static Routes).

The Traffic Steering and Application Policies sections show how you use the SRX Series Firewall to create rules for path preference and routing behavior. Note that on the SRX Series Firewall deployed as a WAN edge, the Application Policy and Traffic Steering path determine destination zones and must be assigned.

Traffic Steering enables you to define different paths that traffic can take to reach its destination. Traffic Steering policies allow you to specify the paths for traffic to traverse, as well as the strategies for utilizing those paths.

Figure 431: Traffic Steering



2 Traffic Steering

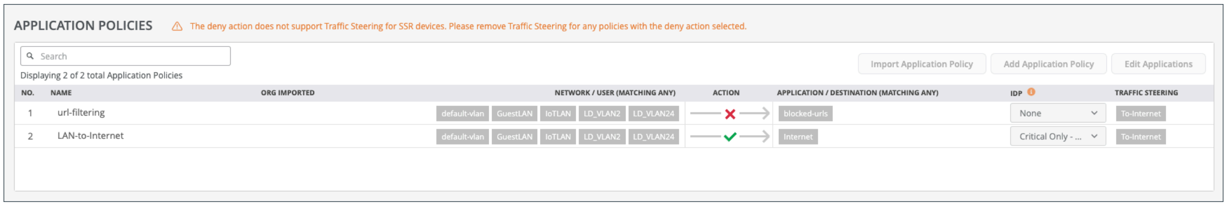
NAME	STRATEGY	PATHS
to-default	Ordered	default-vlan
To-Internet	Ordered	ATT

Table 71: Traffic Steering

Field	Description
Name	The name of the Traffic Steering policy.
Strategy	Ordered, weighted, ECMP.
Paths	LAN, WAN, Untagged VLAN (SRX only).

Application Policies are security policies in the Juniper WAN Assurance design, where you define which network and users can access which applications, and according to which traffic steering policy. You must create Networks, Applications, and establish Traffic Steering profiles to define an Application Policy. These elements become matching criteria to allow access to or block access from applications or destinations.

Figure 432: Application Policies



APPLICATION POLICIES ⚠ The deny action does not support Traffic Steering for SSR devices. Please remove Traffic Steering for any policies with the deny action selected.

Search

Displaying 2 of 2 total Application Policies

NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
1	url-filtering		default-vlan GuestLAN IoTLAN LD_VLAN2 LD_VLAN24	✗	blocked-urls	None	To-Internet
2	LAN-to-Internet		default-vlan GuestLAN IoTLAN LD_VLAN2 LD_VLAN24	✓	Internet	Critical Only - ...	To-Internet

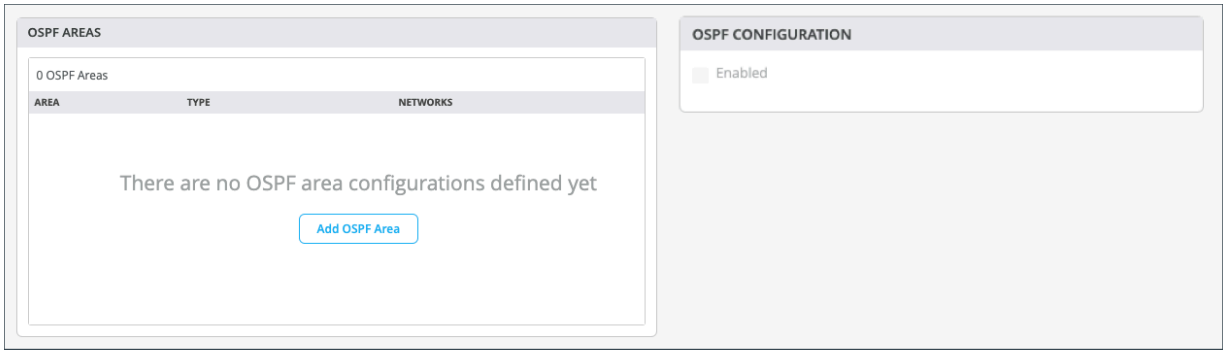
In the Juniper Mist™ cloud portal, the Networks or Users setting determines the source zone. The Applications and Traffic Steering settings determine the destination zone. Traffic Steering paths determine the destination zone in Juniper Networks® SRX Series Firewalls, so ensure that you assign Traffic Steering profiles to the Application Policies.

Table 72: Application Policies

Field	Description
Number	Ordered Policy Number
Name	Application policy name
Org Imported	Indicates if the policy was pushed down from the Organization level to the Site.
Network/User (Matching Any)	The “source” of your traffic
Action	Allow/Block
Application/Destination (Matching Any)	The “destination” for your traffic.
IDP	Indicates IDP/URL filtering (requires separate license)
Traffic Steering	Indicates path for traffic

Open Shortest Path First (OSPF) is used to determine the best path for forwarding IP packets. OSPF segments a network to improve scalability and control the flow of routing information. See "Configure OSPF" on page 251

Figure 433: Routing: OSPF Areas and OSPF Configuration



OSPF AREAS

0 OSPF Areas

AREA	TYPE	NETWORKS

There are no OSPF area configurations defined yet

OSPF CONFIGURATION

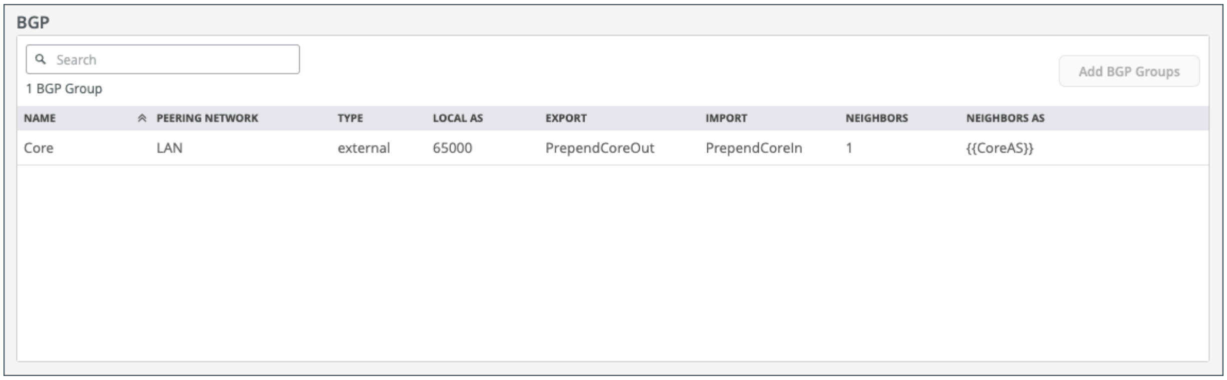
□ Enabled

Table 73: Routing: OSPF Areas and OSPF Configuration

Field	Description
Area	The identification area that your OSPF network or SRX Series Firewall belongs to.
Type	This is the OSPF Area type. Select Default (Area 0), Stub, or Not So Stubby Area (NSSA).
Networks	The name of your OSPF network.
Enabled	Selecting this check box causes the **Enable OSPF Areas** button to become selectable.

You can configure Border Gateway Protocol (BGP) for your SRX Series Firewall deployed as a WAN edge device. You can also manually add a BGP Group here.

Figure 434: Routing: BGP



1 BGP Group

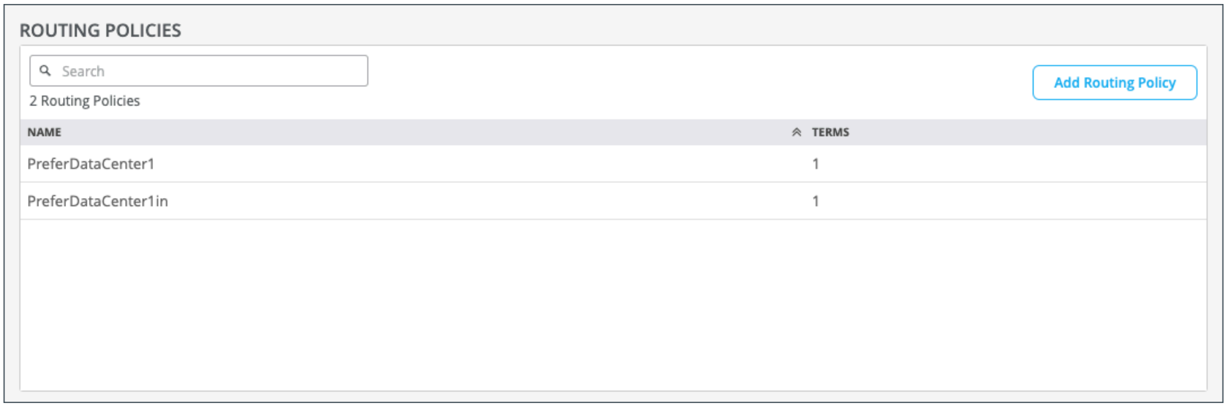
NAME	PEERING NETWORK	TYPE	LOCAL AS	EXPORT	IMPORT	NEIGHBORS	NEIGHBORS AS
Core	LAN	external	65000	PrependCoreOut	PrependCoreIn	1	{{CoreAS}}

Table 74: Routing: BGP

Field	Description
Name	BGP Name
Peering Network	The type of network being used for your BGP peering (WAN or LAN).
Type	Type of BGP Route (Internal or External)
Local AS	Autonomous System Number
Export	Export Route
Import	Import Route
Neighbors	Neighbor Route
Neighbor AS	Autonomous System Number for Neighbor Route

The Routing Policies section enables you to configure path preference and allows you to determine traffic behavior.

Figure 435: Routing: Routing Policies



ROUTING POLICIES

Search

2 Routing Policies

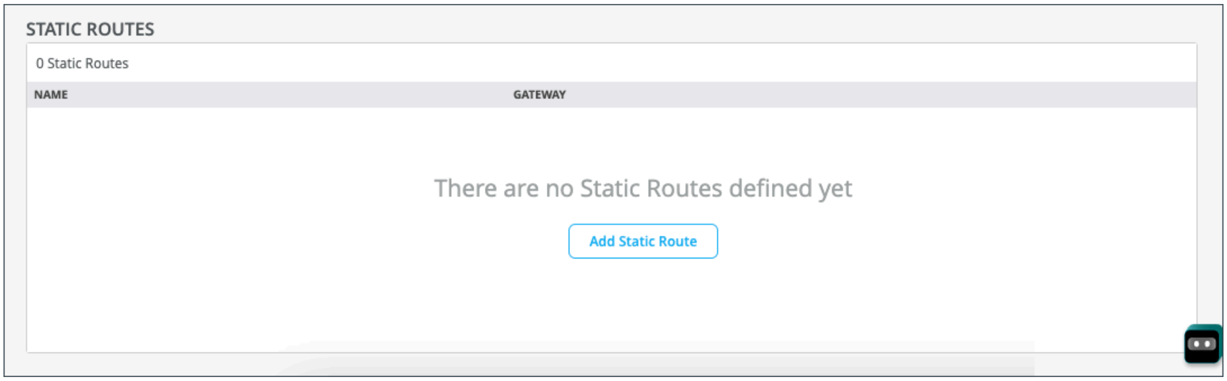
NAME	TERMS
PreferDataCenter1	1
PreferDataCenter1in	1

Table 75: Routing: Routing Policies

Field	Description
Name	The name of your routing policy.
Terms	These are the policy conditions such as prefix, routing protocol, and actions.

Static routes allow you to manually define the routes that your SRX Series Firewall deployed as a WAN edge device will use.

Figure 436: Routing: Static Routes



STATIC ROUTES

0 Static Routes

NAME	GATEWAY

There are no Static Routes defined yet

Table 76: Routing: Static Routes

Field	Description
Name	The name of your static route.
Gateway	The gateway that your static route will use when routing traffic.

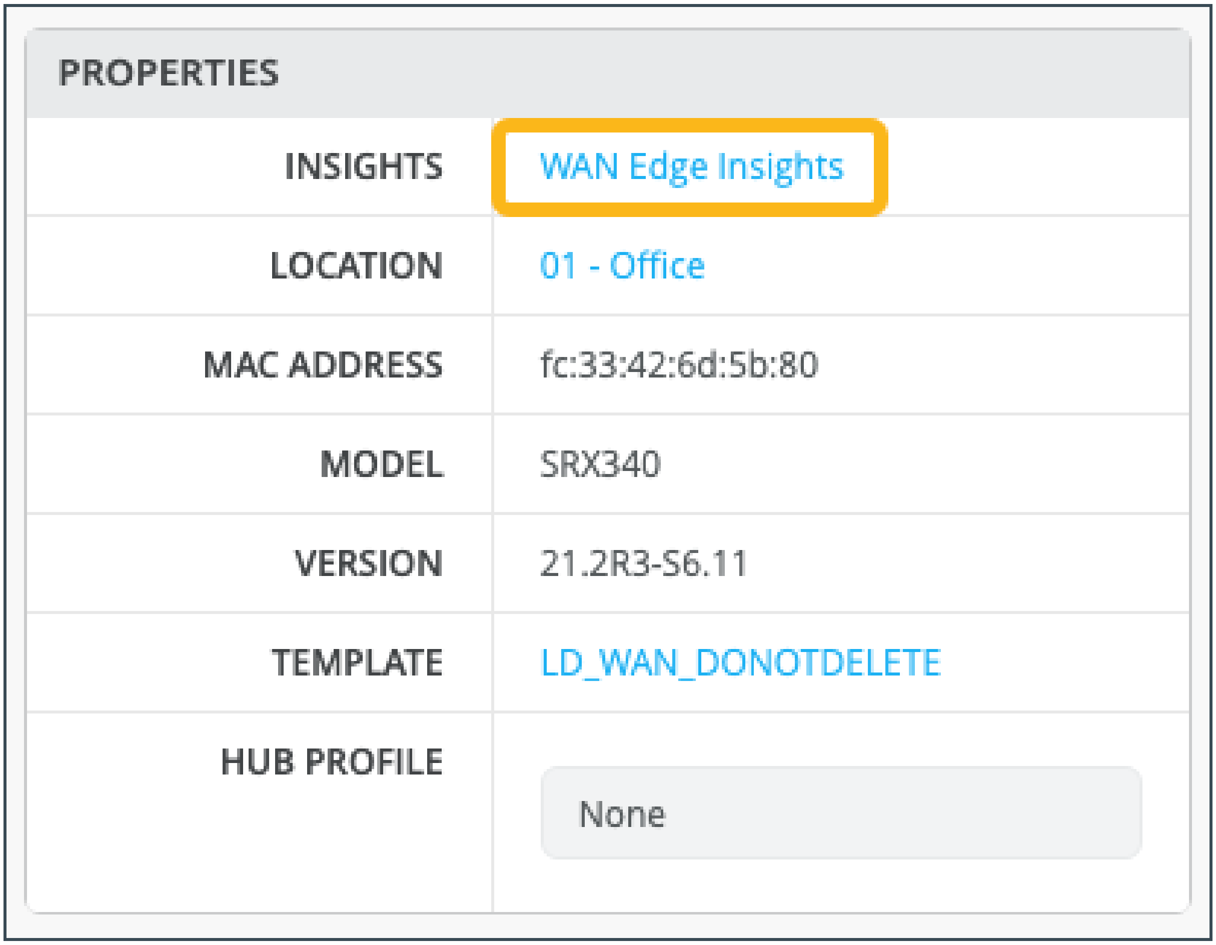
Monitoring: Device Information and WAN Edge Insights

IN THIS SECTION

WAN Edge Insights

The Properties pane for your selected WAN edge links to **WAN Edge Insights**. Click **WAN Edge Insights** for the next level of information about your WAN edge device.

Figure 437: WAN Edge Insights

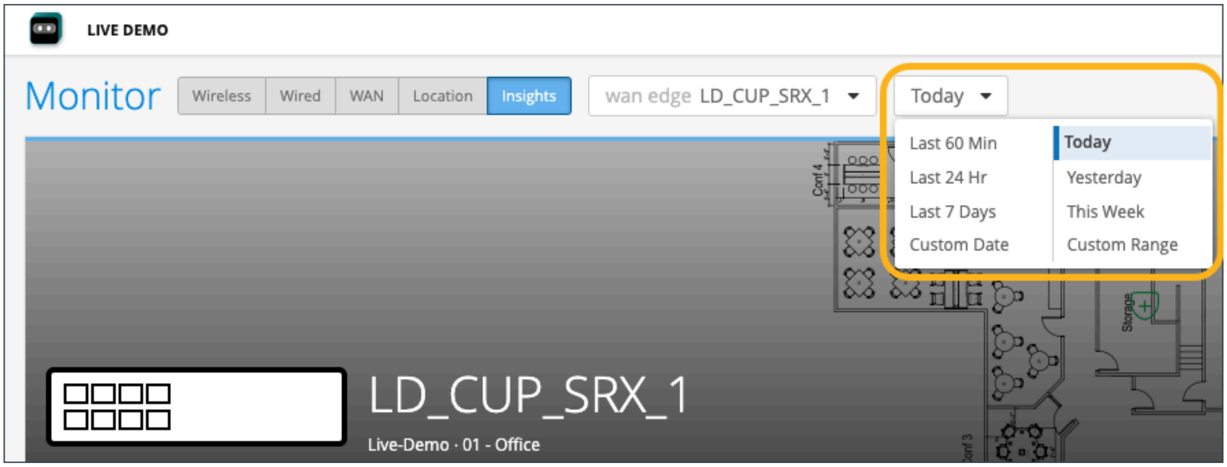


PROPERTIES

INSIGHTS	WAN Edge Insights
LOCATION	01 - Office
MAC ADDRESS	fc:33:42:6d:5b:80
MODEL	SRX340
VERSION	21.2R3-S6.11
TEMPLATE	LD_WAN_DONOTDELETE
HUB PROFILE	None

Next to the selected WAN edge (LD_CUP_SRX_1) on the Insights page, you can select a time frame for selected information. The default view is **Today,** but this can be set to a customized date or range of dates. Below this, you find (when the site location information is configured) where this WAN edge is configured via a street map.

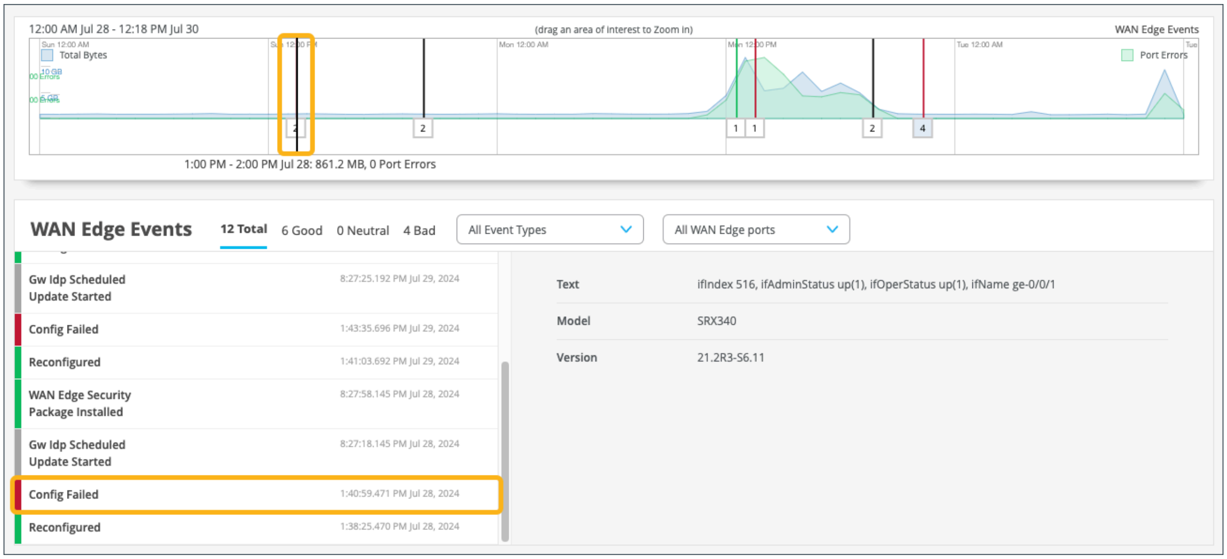
Figure 438: WAN Edge Insights-Select Time Duration



With your time frame selected, **WAN Edge Events** displays a time line of the traffic through the WAN edge during your specified time, and also displays a list of events.

Select a specific event in the listed WAN Edge Events for greater detail of the **Good**, **Neutral**, and **Bad** events.

Figure 439: WAN Edge Events Timeline



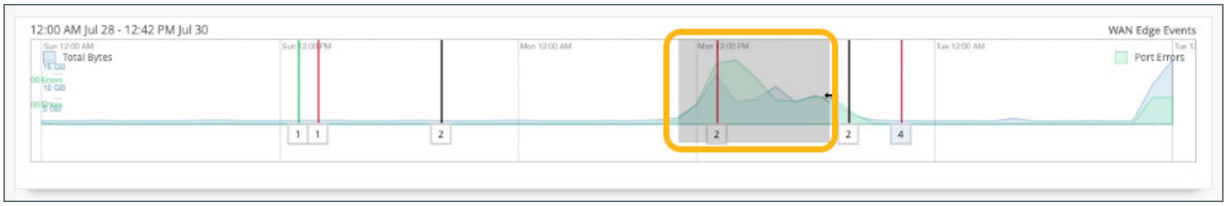
Gw Idp Scheduled Update Started	8:27:25.192 PM Jul 29, 2024
Config Failed	1:43:35.696 PM Jul 29, 2024
Reconfigured	1:41:03.692 PM Jul 29, 2024
WAN Edge Security Package Installed	8:27:58.145 PM Jul 28, 2024
Gw Idp Scheduled Update Started	8:27:18.145 PM Jul 28, 2024
Config Failed	1:40:59.471 PM Jul 28, 2024
Reconfigured	1:38:25.470 PM Jul 28, 2024

Text	ifIndex 516, ifAdminStatus up(1), ifOperStatus up(1), ifName ge-0/0/1
Model	SRX340
Version	21.2R3-S6.11

Your selection expands and displays detailed information about the selected time.

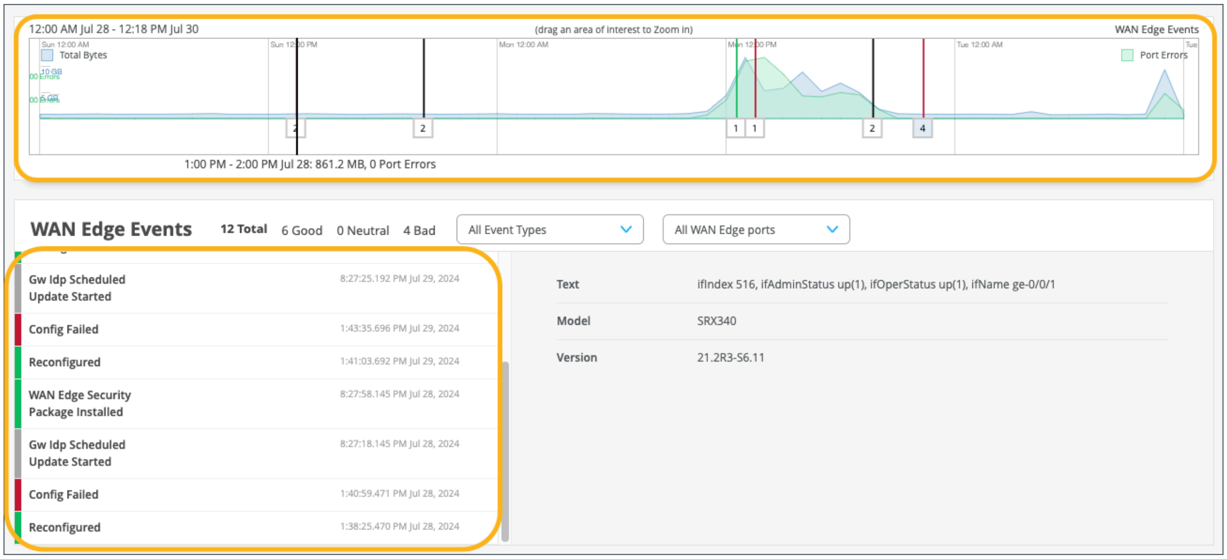
For a detailed portion of time, select a window of time with the mouse cursor. By doing this, you're able to adjust the window of events and isolate specific **Good**, **Neutral**, and **Bad** occurrences that happened on your network. With a smaller section, you'll get a more detailed view of that period.

Figure 440: WAN Edge Events Timeline Details View



Scroll down on the WAN Edge Events page for deeper insights within your selected period.

Figure 441: WAN Edge Events page


12:00 AM Jul 28 - 12:18 PM Jul 30
(drag an area of interest to Zoom in)
WAN Edge Events
Sun 12:00 AM
Total Bytes
Sun 12:00 PM
Mon 12:00 AM
Mon 12:00 PM
Tue 12:00 AM
Port Errors
1:00 PM - 2:00 PM Jul 28: 861.2 MB, 0 Port Errors

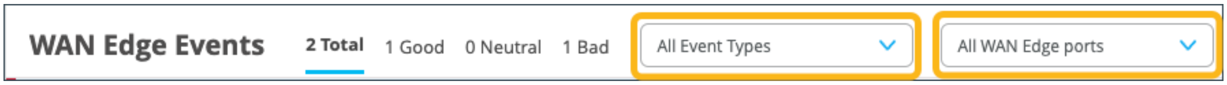
WAN Edge Events 12 Total 6 Good 0 Neutral 4 Bad All Event Types All WAN Edge ports

Gw Idp Scheduled Update Started	8:27:25.192 PM Jul 29, 2024
Config Failed	1:43:35.696 PM Jul 29, 2024
Reconfigured	1:41:03.692 PM Jul 29, 2024
WAN Edge Security Package Installed	8:27:58.145 PM Jul 28, 2024
Gw Idp Scheduled Update Started	8:27:18.145 PM Jul 28, 2024
Config Failed	1:40:59.471 PM Jul 28, 2024
Reconfigured	1:38:25.470 PM Jul 28, 2024

Text	ifIndex 516, ifAdminStatus up(1), ifOperStatus up(1), ifName ge-0/0/1
Model	SRX340
Version	21.2R3-S6.11

In the WAN Edge Events, you can narrow down the type of event by selecting a modifier in the Event Type drop-down menu. You can also filter your search by limiting the event types to a specific port.

Figure 442: WAN Edge Events Page

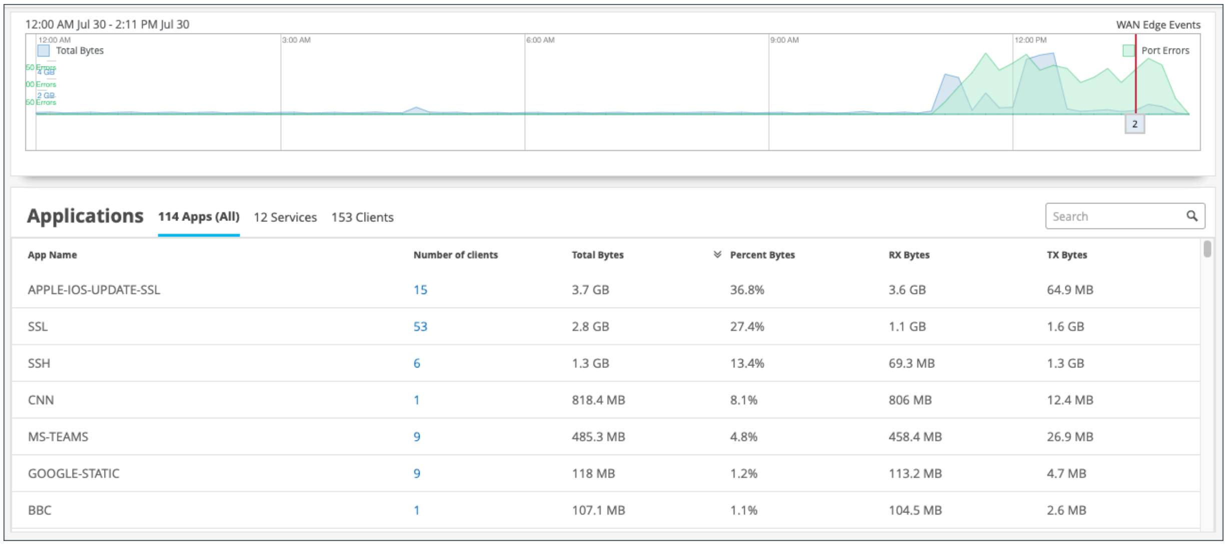


On the WAN Edge Events page, you can also view reports on applications on the Applications pane. On this pane:

- You can use the applications pane to monitor and troubleshoot specific application behavior.
- You can hover over the App Name to see more details about the services.
- You can view a client's use of a particular application by clicking the Clients tab.

NOTE: Ensure you've had a few hours for these metrics to be populated following initial deployment.

Figure 443: Applications

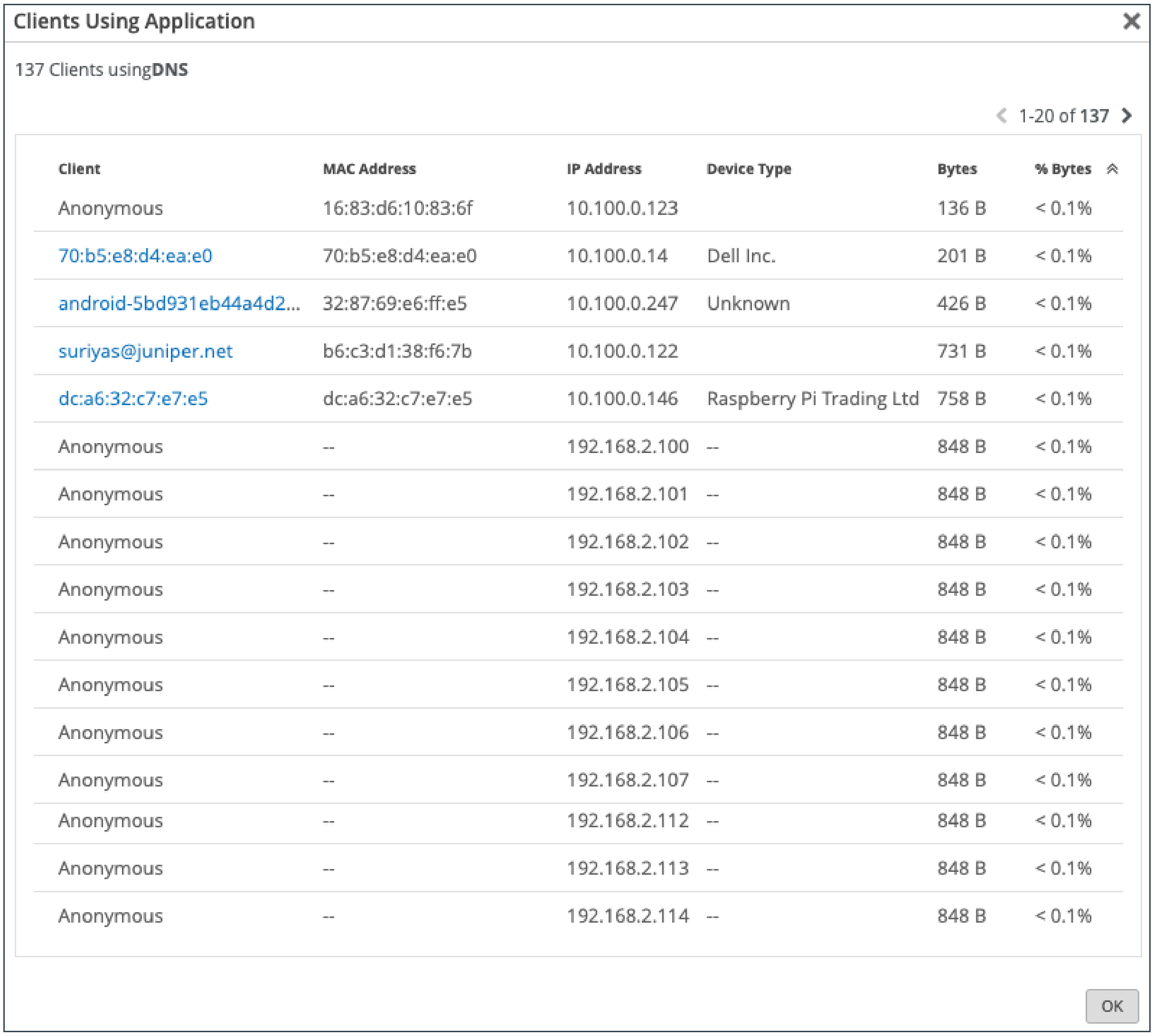


Applications 114 Apps (All) 12 Services 153 Clients

App Name	Number of clients	Total Bytes	Percent Bytes	RX Bytes	TX Bytes
APPLE-IOS-UPDATE-SSL	15	3.7 GB	36.8%	3.6 GB	64.9 MB
SSL	53	2.8 GB	27.4%	1.1 GB	1.6 GB
SSH	6	1.3 GB	13.4%	69.3 MB	1.3 GB
CNN	1	818.4 MB	8.1%	806 MB	12.4 MB
MS-TEAMS	9	485.3 MB	4.8%	458.4 MB	26.9 MB
GOOGLE-STATIC	9	118 MB	1.2%	113.2 MB	4.7 MB
BBC	1	107.1 MB	1.1%	104.5 MB	2.6 MB

In the **Number of Clients** column, you can click on the number to see more information about the clients using the application such as the Client name, MAC Address, IP Address, Device Type, and Bytes being used.

Figure 444: Clients Using Application



Clients Using Application

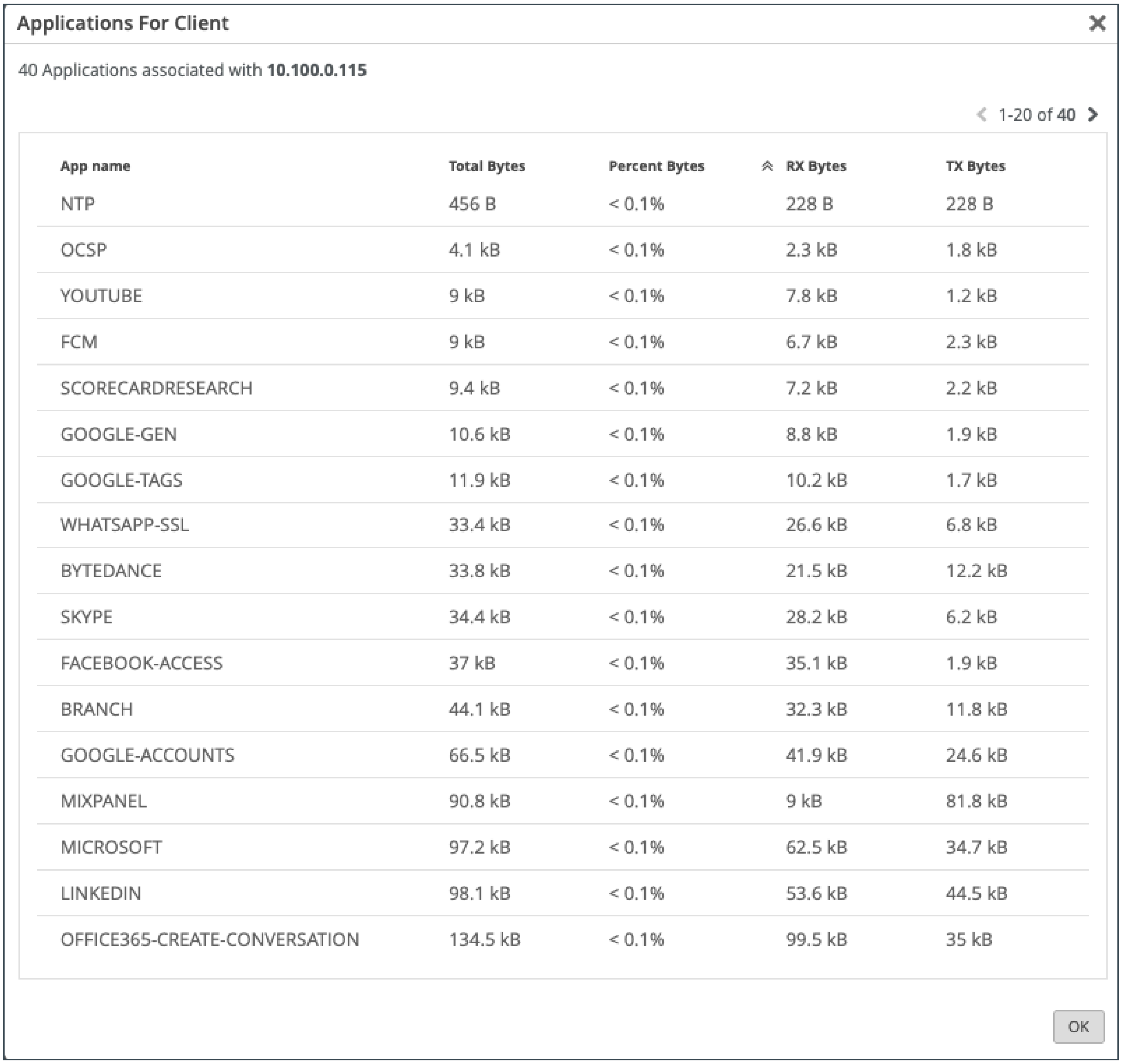
137 Clients using**DNS**

Client	MAC Address	IP Address	Device Type	Bytes	% Bytes
Anonymous	16:83:d6:10:83:6f	10.100.0.123		136 B	< 0.1%
70:b5:e8:d4:ea:e0	70:b5:e8:d4:ea:e0	10.100.0.14	Dell Inc.	201 B	< 0.1%
android-5bd931eb44a4d2...	32:87:69:e6:ff:e5	10.100.0.247	Unknown	426 B	< 0.1%
suriyas@juniper.net	b6:c3:d1:38:f6:7b	10.100.0.122		731 B	< 0.1%
dc:a6:32:c7:e7:e5	dc:a6:32:c7:e7:e5	10.100.0.146	Raspberry Pi Trading Ltd	758 B	< 0.1%
Anonymous	--	192.168.2.100	--	848 B	< 0.1%
Anonymous	--	192.168.2.101	--	848 B	< 0.1%
Anonymous	--	192.168.2.102	--	848 B	< 0.1%
Anonymous	--	192.168.2.103	--	848 B	< 0.1%
Anonymous	--	192.168.2.104	--	848 B	< 0.1%
Anonymous	--	192.168.2.105	--	848 B	< 0.1%
Anonymous	--	192.168.2.106	--	848 B	< 0.1%
Anonymous	--	192.168.2.107	--	848 B	< 0.1%
Anonymous	--	192.168.2.112	--	848 B	< 0.1%
Anonymous	--	192.168.2.113	--	848 B	< 0.1%
Anonymous	--	192.168.2.114	--	848 B	< 0.1%

NOTE: For SRX Series Firewalls deployed as a WAN edge running a DHCP server, clients using that application will display a HostName in the Client column if available. Otherwise, the MAC address will be displayed. Device Type and MAC Address columns will be populated as well.

Back on the Applications pane, you can click the **Clients** tab to see how much bandwidth a particular client is using. You can click the number in the **Number of applications** column to see more information.

Figure 445: Applications for Client



Applications For Client

40 Applications associated with **10.100.0.115**

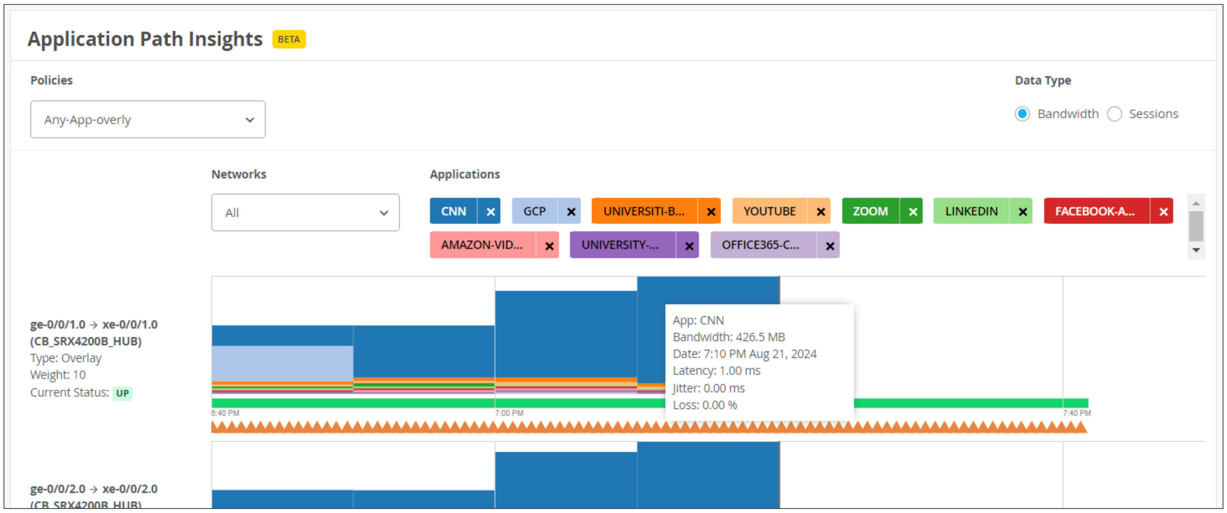
App name	Total Bytes	Percent Bytes	RX Bytes	TX Bytes
NTP	456 B	< 0.1%	228 B	228 B
OCSP	4.1 kB	< 0.1%	2.3 kB	1.8 kB
YOUTUBE	9 kB	< 0.1%	7.8 kB	1.2 kB
FCM	9 kB	< 0.1%	6.7 kB	2.3 kB
SCORECARDRESEARCH	9.4 kB	< 0.1%	7.2 kB	2.2 kB
GOOGLE-GEN	10.6 kB	< 0.1%	8.8 kB	1.9 kB
GOOGLE-TAGS	11.9 kB	< 0.1%	10.2 kB	1.7 kB
WHATSAPP-SSL	33.4 kB	< 0.1%	26.6 kB	6.8 kB
BYTEDANCE	33.8 kB	< 0.1%	21.5 kB	12.2 kB
SKYPE	34.4 kB	< 0.1%	28.2 kB	6.2 kB
FACEBOOK-ACCESS	37 kB	< 0.1%	35.1 kB	1.9 kB
BRANCH	44.1 kB	< 0.1%	32.3 kB	11.8 kB
GOOGLE-ACCOUNTS	66.5 kB	< 0.1%	41.9 kB	24.6 kB
MIXPANEL	90.8 kB	< 0.1%	9 kB	81.8 kB
MICROSOFT	97.2 kB	< 0.1%	62.5 kB	34.7 kB
LINKEDIN	98.1 kB	< 0.1%	53.6 kB	44.5 kB
OFFICE365-CREATE-CONVERSATION	134.5 kB	< 0.1%	99.5 kB	35 kB

The Application Path Insights (BETA) section shows you which applications are using the most bandwidth according to the selected Application Policy and Network. It displays the effective application flow over the path for the selected Application Policy. You can also change the Data Type to Sessions to see the number of sessions occurring per application. Hover over a section of the graph to view the bandwidth or sessions per application as well as jitter, loss, and latency.

NOTE: The Application Path Insights visualization data is available only if the configuration is managed by Juniper Mist.

Video: NOW in 60: WAN Assurance Application Insights Dashboard

Figure 446: Application Path Insights (BETA)



Application Path Insights BETA

Policies: Any-App-overly

Data Type: ● Bandwidth ○ Sessions

Networks: All

Applications: CNN ✕, GCP ✕, UNIVERSITI-B... ✕, YOUTUBE ✕, ZOOM ✕, LINKEDIN ✕, FACEBOOK-A... ✕, AMAZON-VID... ✕, UNIVERSITY-... ✕, OFFICE365-C... ✕

ge-0/0/1.0 → xe-0/0/1.0 (CB_SRX4200B_HUB)
Type: Overlay
Weight: 10
Current Status: UP

App: CNN
Bandwidth: 426.5 MB
Date: 7:10 PM Aug 21, 2024
Latency: 1.00 ms
Jitter: 0.00 ms
Loss: 0.00 %

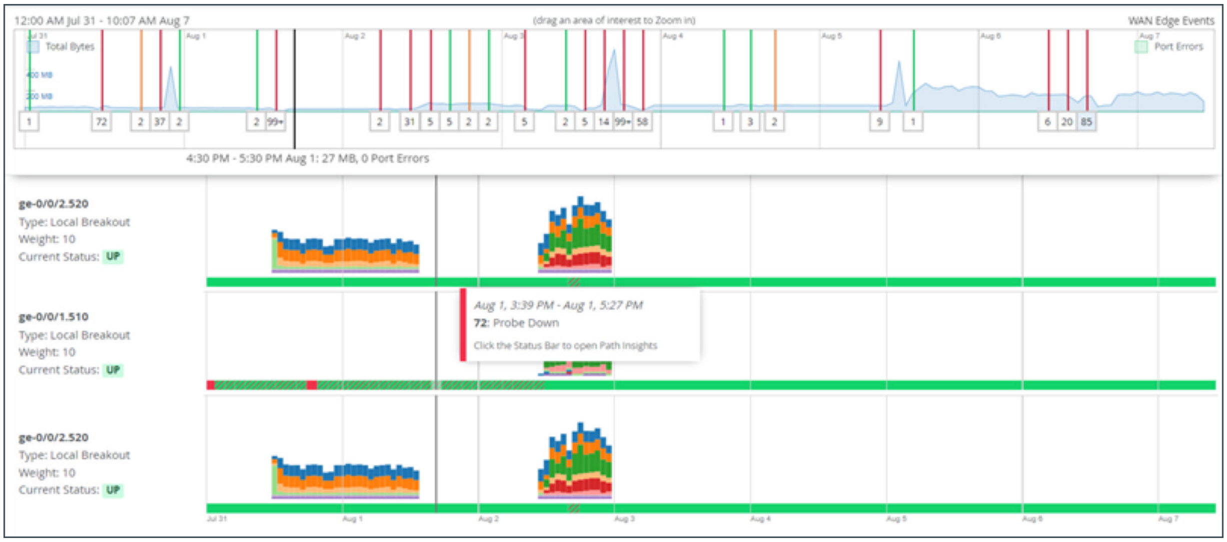
ge-0/0/2.0 → xe-0/0/2.0 (CB_SRX4200B_HUB)

The path state bar shows path state information over a timeline, and path state events are indicated by segments highlighted in different colors. For example, Path Up events are shown in green and Path Down events are shown in red.

You can hover over the highlighted portions of the path state bar to view a summary of path state events.

The Application Path Insights section also includes a summary view on the lefthand side that displays recent path state events.

Figure 447: Application Path Insights (BETA) continued



12:00 AM Jul 31 - 10:07 AM Aug 7

(drag an area of interest to Zoom in)

WAN Edge Events

4:30 PM - 5:30 PM Aug 1: 27 MB, 0 Port Errors

ge-0/0/2.520
Type: Local Breakout
Weight: 10
Current Status: UP

ge-0/0/1.510
Type: Local Breakout
Weight: 10
Current Status: UP

Aug 1, 3:39 PM - Aug 1, 5:27 PM
72: Probe Down
Click the Status Bar to open Path Insights

ge-0/0/2.520
Type: Local Breakout
Weight: 10
Current Status: UP

If you click on the bar, you will get a pop-up window where you can view more detailed information about the path state events. The list of events displays on the left and when you select an event, the reason for the event displays on the right.

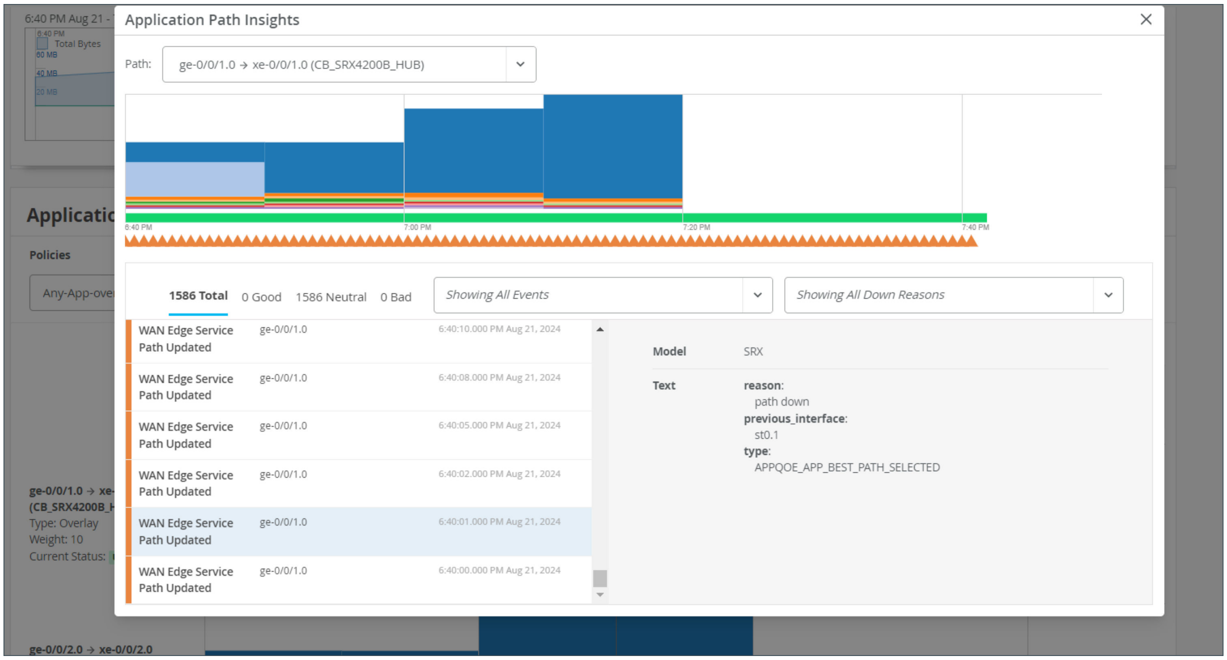
Path state events include:

- Path Update
- Port Up
- Port Down
- Path Up
- Path Down

Path state reasons include:

- Probe Down
- Peer Path Up
- Peer Path Down
- Config Change
- Best Path Selected
- SLA Metric Violation

Figure 448: Path State Events and Reasons



Path: ge-0/0/1.0 → xe-0/0/1.0 (CB_SRX4200B_HUB)

1586 Total 0 Good 1586 Neutral 0 Bad

Showing All Events

Showing All Down Reasons

WAN Edge Service Path Updated	ge-0/0/1.0	6:40:10.000 PM Aug 21, 2024
WAN Edge Service Path Updated	ge-0/0/1.0	6:40:08.000 PM Aug 21, 2024
WAN Edge Service Path Updated	ge-0/0/1.0	6:40:05.000 PM Aug 21, 2024
WAN Edge Service Path Updated	ge-0/0/1.0	6:40:02.000 PM Aug 21, 2024
WAN Edge Service Path Updated	ge-0/0/1.0	6:40:01.000 PM Aug 21, 2024
WAN Edge Service Path Updated	ge-0/0/1.0	6:40:00.000 PM Aug 21, 2024

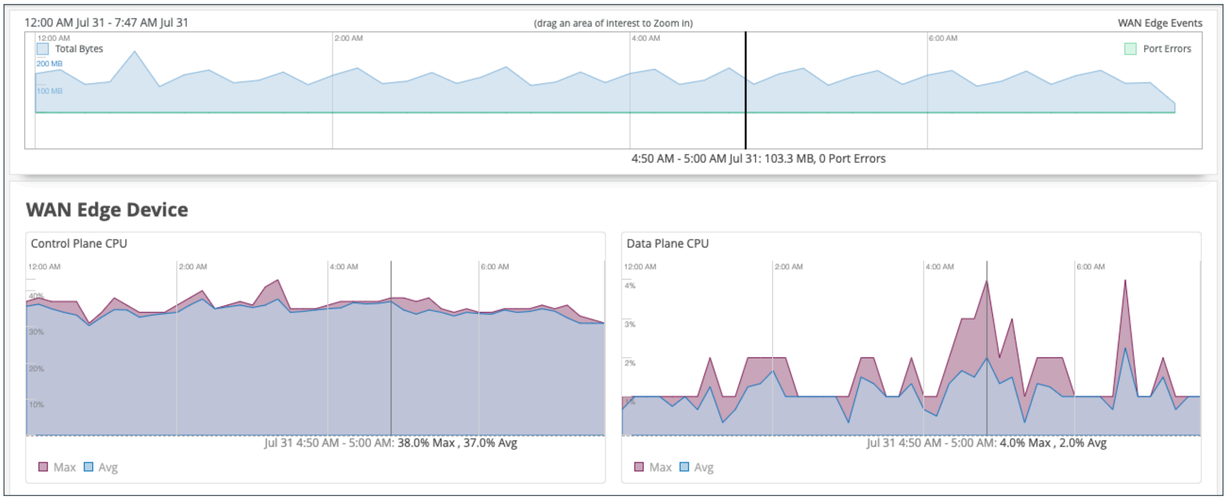
Model SRX

Text
reason:
path down
previous_interface:
st0.1
type:
APPQOE_APP_BEST_PATH_SELECTED

The **WAN Edge Device Charts** include Control Plane CPU, Data Plane CPU, Memory Utilization, and Power Draw.

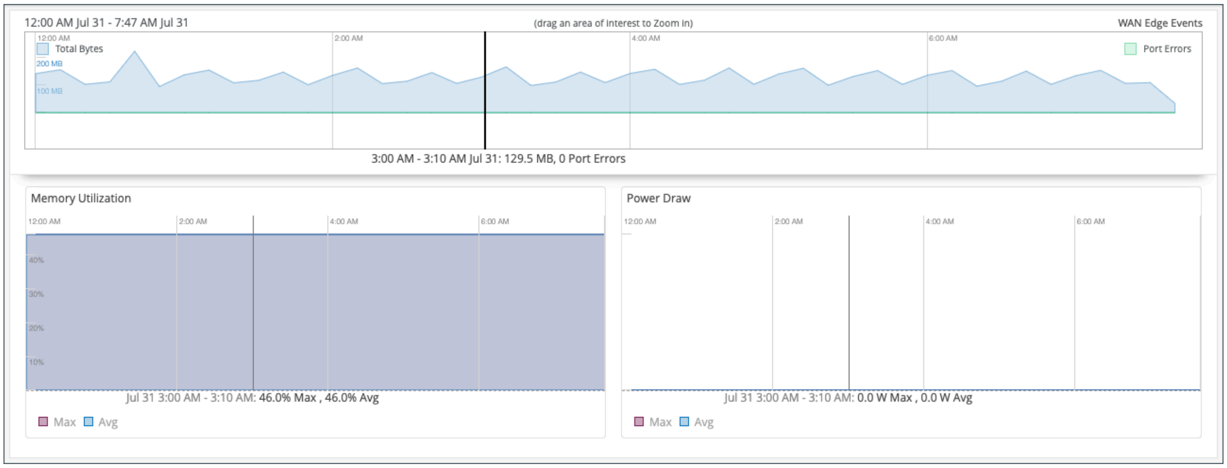
The **Control Plane CPU** and **Data Plane CPU** charts show you the percentage of CPU utilization for both max and average.

Figure 449: Control Plane CPU and Data Plane CPU



Memory Utilization and **Power Draw** shows you the percentage for both max and average.

Figure 450: Memory Utilization and Power Draw

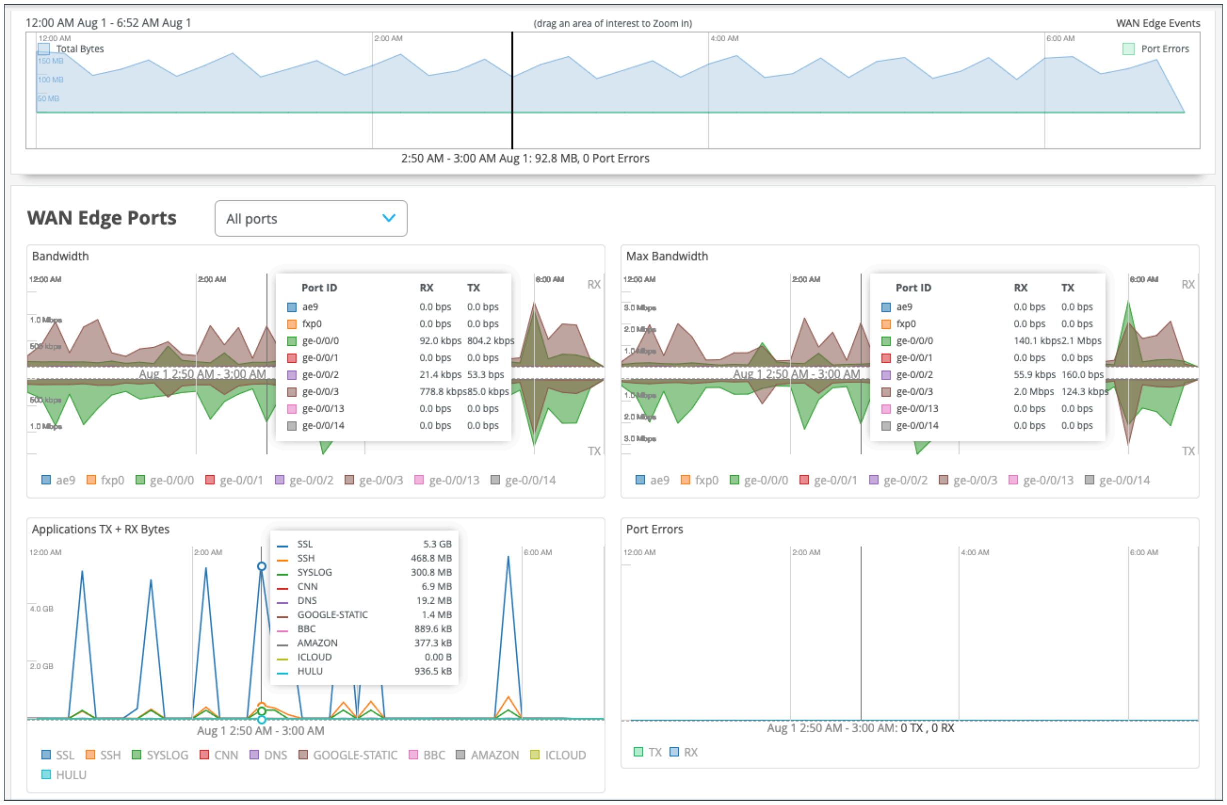

12:00 AM Jul 31 - 7:47 AM Jul 31
(drag an area of interest to Zoom in)
WAN Edge Events
12:00 AM
2:00 AM
4:00 AM
6:00 AM
Total Bytes
Port Errors
200 MB
100 MB
3:00 AM - 3:10 AM Jul 31: 129.5 MB, 0 Port Errors
Memory Utilization
12:00 AM
2:00 AM
4:00 AM
6:00 AM
40%
30%
20%
10%
Jul 31 3:00 AM - 3:10 AM: 46.0% Max , 46.0% Avg
Max
Avg
Power Draw
12:00 AM
2:00 AM
4:00 AM
6:00 AM
Jul 31 3:00 AM - 3:10 AM: 0.0 W Max , 0.0 W Avg
Max
Avg

The **WAN Edge Ports** charts include Bandwidth, Max Bandwidth, Applications TX + RX Bytes, Port Errors, and IPsec Traffic. From the drop down list at the top, you can select All ports to see utilization metrics in the charts for all interfaces, or you can select an interface to see the utilization metrics for that particular interface.

In the **Bandwidth** chart, you will see the bandwidth utilization metrics in megabits per second (Mbps) for that particular interface.

The **Max Bandwidth** chart displays insights into the highest point of link utilization recorded for received power signal (RX) and transmitted power signal (TX) packets on each port during the day. The data is shown in Mbps.

Figure 451: Bandwidth and Max Bandwidth



Bandwidth

Port ID	RX	TX
ae9	0.0 bps	0.0 bps
fxp0	0.0 bps	0.0 bps
ge-0/0/0	92.0 kbps	804.2 kbps
ge-0/0/1	0.0 bps	0.0 bps
ge-0/0/2	21.4 kbps	53.3 bps
ge-0/0/3	778.8 kbps	85.0 kbps
ge-0/0/13	0.0 bps	0.0 bps
ge-0/0/14	0.0 bps	0.0 bps

Max Bandwidth

Port ID	RX	TX
ae9	0.0 bps	0.0 bps
fxp0	0.0 bps	0.0 bps
ge-0/0/0	140.1 kbps	2.1 Mbps
ge-0/0/1	0.0 bps	0.0 bps
ge-0/0/2	55.9 kbps	160.0 bps
ge-0/0/3	2.0 Mbps	124.3 kbps
ge-0/0/13	0.0 bps	0.0 bps
ge-0/0/14	0.0 bps	0.0 bps

Applications TX + RX Bytes

SSL	5.3 GB
SSH	468.8 MB
SYSLOG	300.8 MB
CNN	6.9 MB
DNS	19.2 MB
GOOGLE-STATIC	1.4 MB
BBC	889.6 kB
AMAZON	377.3 kB
ICLOUD	0.00 B
HULU	936.5 kB

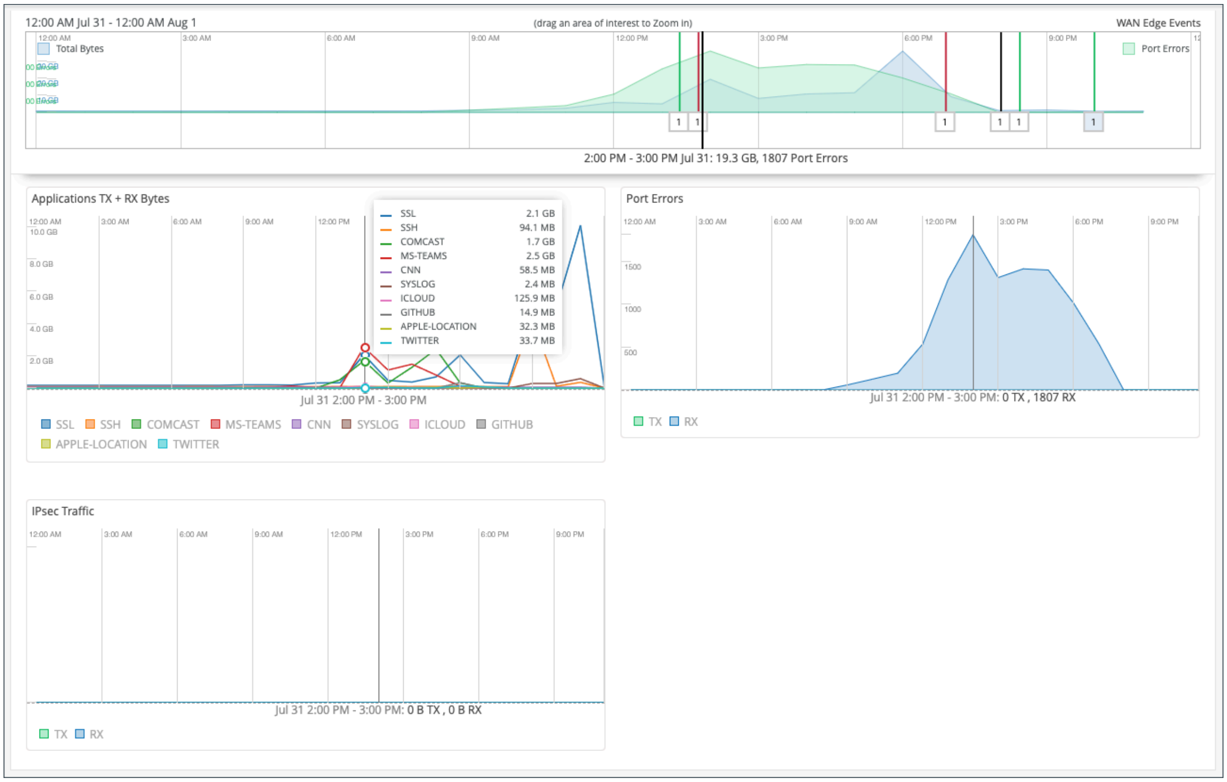
In the last three WAN Edge Ports charts, you'll find **Applications TX + RX Bytes**, **Port Errors**, and **IPsec Traffic**. Hover over the charts to find out more information.

The **Applications TX + RX Bytes** chart outlines transmit and receive data information, which can be isolated at an application level by clicking on the application name at the bottom of the chart to see Client, MAC address, IP address, device type, and bytes for bandwidth utilization.

The **Port Errors** chart will display port errors for receive and transmit packets throughout the day.

The **IPsec Traffic** chart will display the IPsec traffic for transmit and receive packets during the day in kilobytes or megabytes.

Figure 452: Applications TX + RX Bytes, Port Errors, and IPsec Traffic

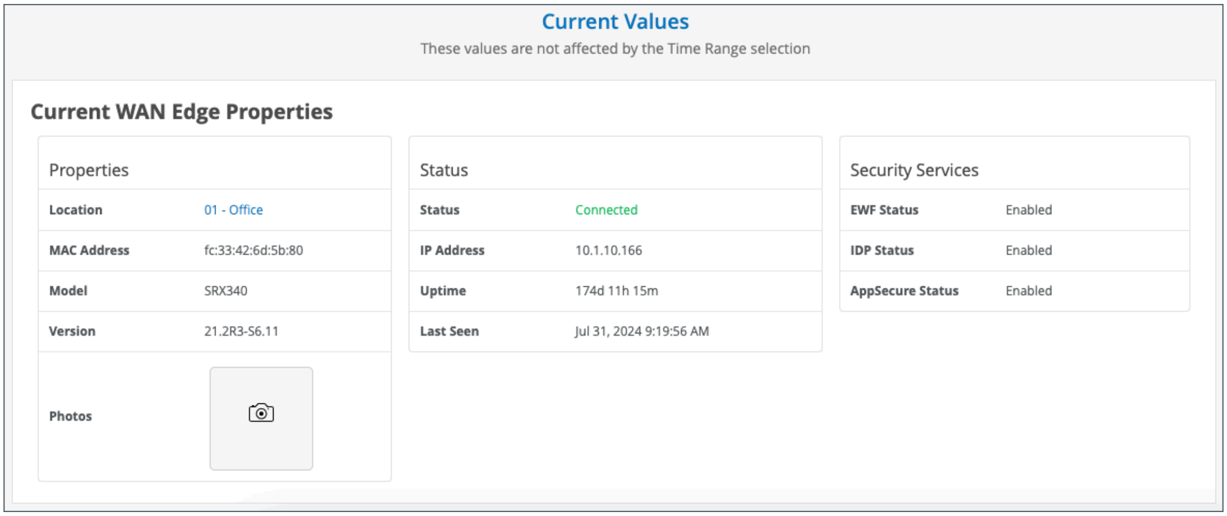


Peer Path Statistics

This applies only to Session Smart Routers deployed as WAN edge devices in Juniper Mist™ WAN Assurance. Therefore, no data will be populated in this section for SRX Series Firewalls deployed as a WAN edge device.

The final section of your WAN Edge Insights page is Current WAN Edge Properties. Time range selections do not impact information in the Current Values pane.

Figure 453: Current WAN Edge Properties



Current Values

These values are not affected by the Time Range selection

Current WAN Edge Properties

Properties

Location	01 - Office
MAC Address	fc:33:42:6d:5b:80
Model	SRX340
Version	21.2R3-S6.11
Photos	

Status

Status	Connected
IP Address	10.1.10.166
Uptime	174d 11h 15m
Last Seen	Jul 31, 2024 9:19:56 AM

Security Services

EWF Status	Enabled
IDP Status	Enabled
AppSecure Status	Enabled

Alerts for Interfaces Status

In Juniper Mist, alerts present network and device issues that are ongoing. You can view alerts on the Juniper Mist portal by selecting Monitor > Alerts.

You can set up alerts and email updates for when certain ports on a WAN Edge device go online or offline. To configure alerts for specific ports, you need to label these ports in the LAN or WAN settings of a WAN Edge device.

To configure the alerts and notifications for specific port, you must:

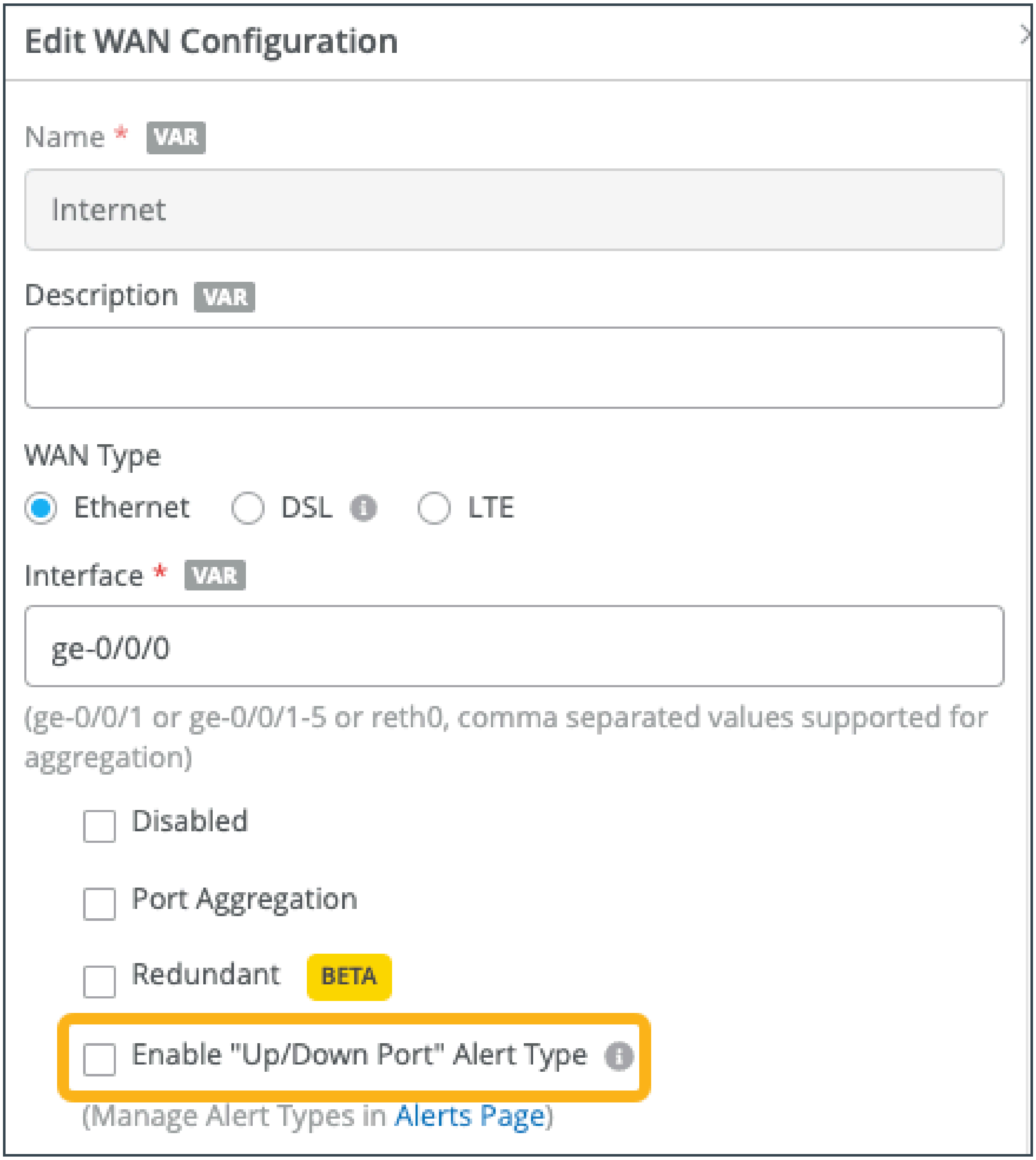
- Change the WAN or LAN settings to label the specified ports in the WAN Edge template or at device-level configuration page.

  1. In the Juniper Mist portal, select **Organization** > **WAN** > **WAN Edge Templates** and select the WAN or LAN configuration that you want to update (or add a new configuration).

     To configure this at the device-level, select **WAN Edges** on the left-navigation bar and select the WAN or LAN configuration of the selected device.

  2. Under Interface, enter the port or ports, and then select the **Enable "Up/Down Port" Alert Type** check-box.

Figure 454: Marking LAN Port or WAN Interface as Critical Interface



Edit WAN Configuration

Name * VAR

Internet

Description VAR

WAN Type

● Ethernet ○ DSL ○ LTE

Interface * VAR

ge-0/0/0

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

□ Disabled

□ Port Aggregation

□ Redundant BETA

□ Enable "Up/Down Port" Alert Type

(Manage Alert Types in Alerts Page)

Repeat these steps for all critical ports.

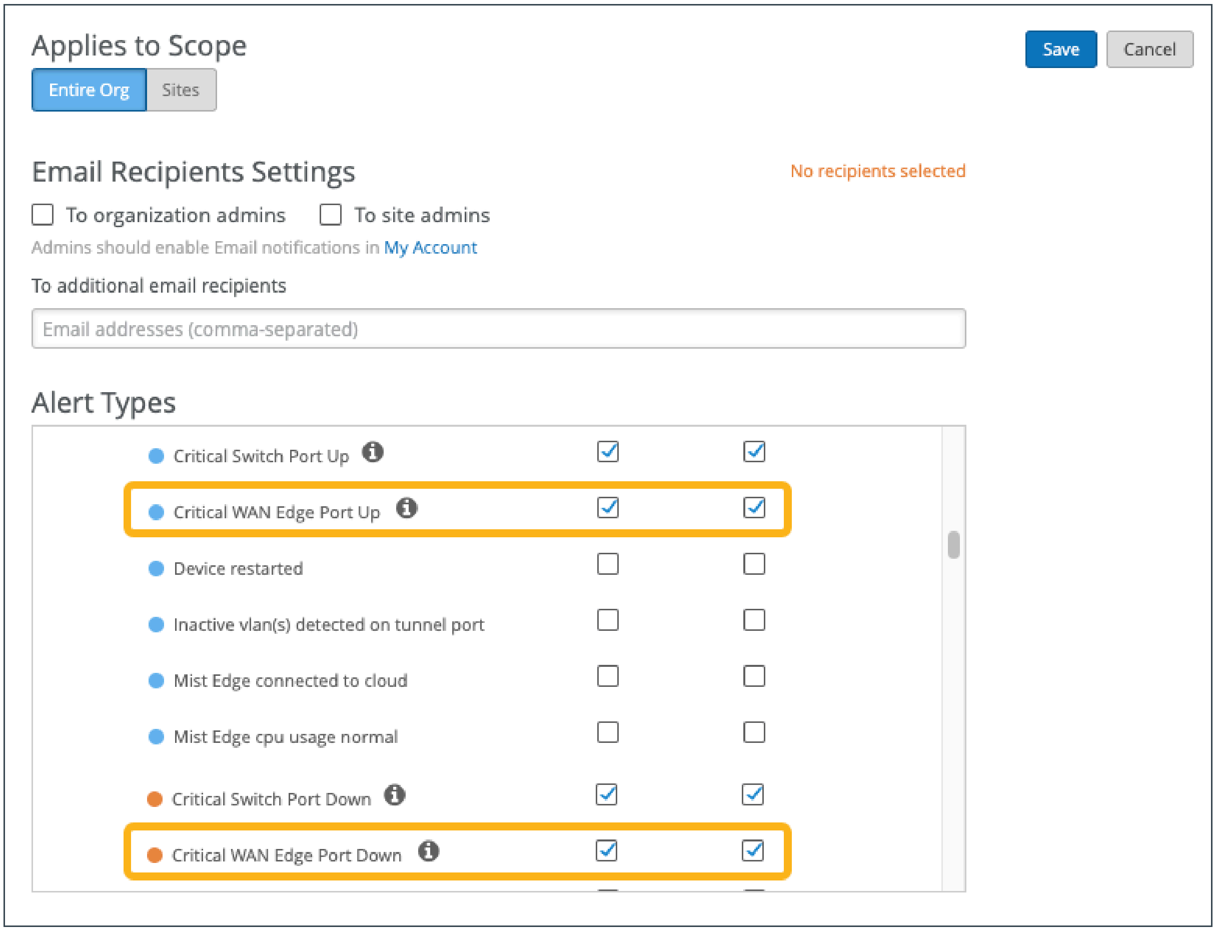
- Configure alerts and e-mail notifications for the specified ports on the Alerts page.

  1. Go to **Monitor > Alerts > Alerts Configuration** and use the following check-boxes to enable alerts for the selected port:

     - Critical WAN Edge Port Up

- Critical WAN Edge Port Down

Figure 455: Alerts Configuration for Critical Ports



Applies to Scope

Email Recipients Settings

No recipients selected

☐ To organization admins ☐ To site admins

Admins should enable Email notifications in My Account

To additional email recipients

Email addresses (comma-separated)

Alert Types

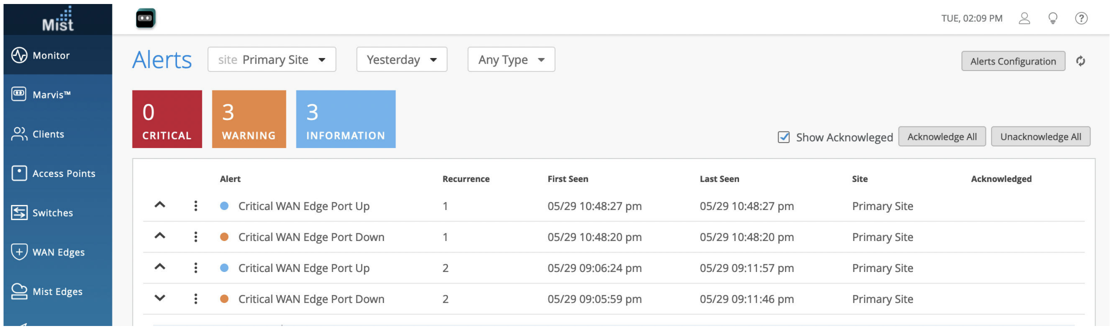
● Critical Switch Port Up	☑	☑
● Critical WAN Edge Port Up	☑	☑
● Device restarted	☐	☐
● Inactive vlan(s) detected on tunnel port	☐	☐
● Mist Edge connected to cloud	☐	☐
● Mist Edge cpu usage normal	☐	☐
● Critical Switch Port Down	☑	☑
● Critical WAN Edge Port Down	☑	☑

See Alert Configuration for details.

When you enable alerts and notifications:

- You'll receive an e-mail notification whenever a port transitions from one state to another.
- You can view the status in Monitor > Alerts page. Figure 456 on page 571 shows an example of the critical port status on the Juniper Mist Alerts dashboard.

Figure 456: Critical WAN Edge Port Status



Alert	Recurrence	First Seen	Last Seen	Site	Acknowledged
● Critical WAN Edge Port Up	1	05/29 10:48:27 pm	05/29 10:48:27 pm	Primary Site	
● Critical WAN Edge Port Down	1	05/29 10:48:20 pm	05/29 10:48:20 pm	Primary Site	
● Critical WAN Edge Port Up	2	05/29 09:06:24 pm	05/29 09:11:57 pm	Primary Site	
● Critical WAN Edge Port Down	2	05/29 09:05:59 pm	05/29 09:11:46 pm	Primary Site	

Monitor Session Smart Router Deployed as WAN Edge

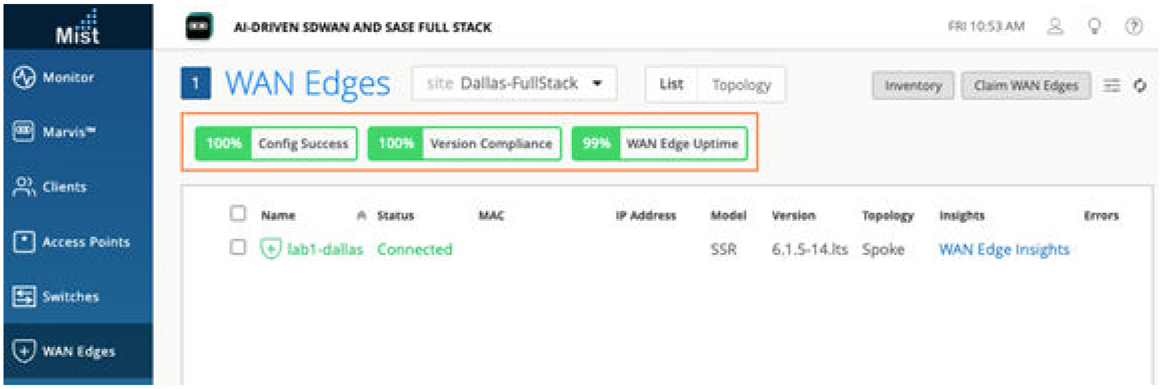
IN THIS SECTION

In monitoring Juniper® Session Smart™ Routers deployed as WAN edge device, you'll explore the most efficient ways to monitor your WAN edge device in the Juniper Mist™ portal following your initial deployment phase.

WAN Edges

In the Juniper Mist Portal, select **WAN Edges > WAN Edges** to view basic device monitoring. Notice the Organization name at the top of the GUI, AI-DRIVEN SDWAN AND SASE FULL STACK. This is the largest container and represents your entire organization. Beneath the organization name, you can see your site devices in either a List format or a graphical Topology format. Here, you see **Dallas-FullStack** is your site, and **lab1-dallas** is your WAN edge device.

Figure 457: Accessing WAN Edges Page

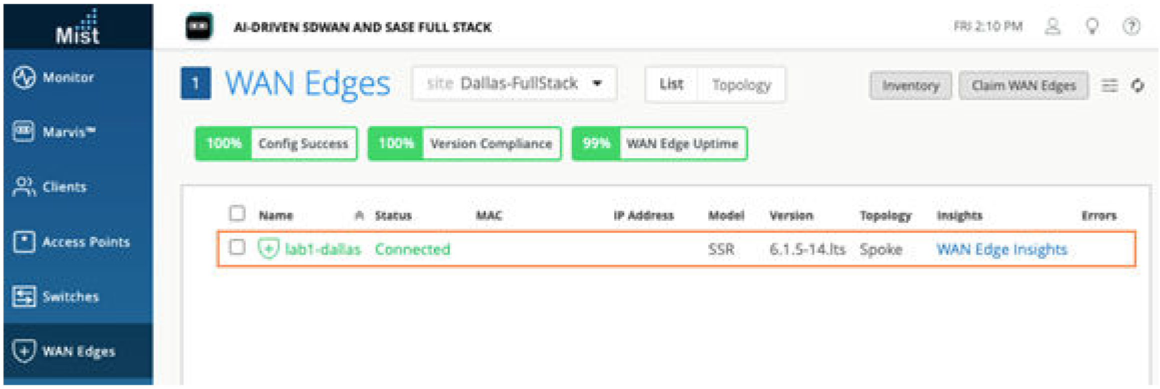


Name	Status	MAC	IP Address	Model	Version	Topology	Insights	Errors
lab1-dallas	Connected			SSR	6.1.5-14.lts	Spoke	WAN Edge Insights	

The List view outlines the following information:

- Config Success—Percentage of online WAN edges with successful configuration
- Version Compliance—Percentage of WAN edges that have the same software version per model.
- WAN Edge Uptime—Percentage of time a WAN edge was up during the past seven days, averaged across all EAN edges.

Figure 458: WAN Edges List View



Name	Status	MAC	IP Address	Model	Version	Topology	Insights	Errors
lab1-dallas	Connected			SSR	6.1.5-14.lts	Spoke	WAN Edge Insights	

Beneath, you'll find WAN edge device details as shown in Table 77 on page 572.

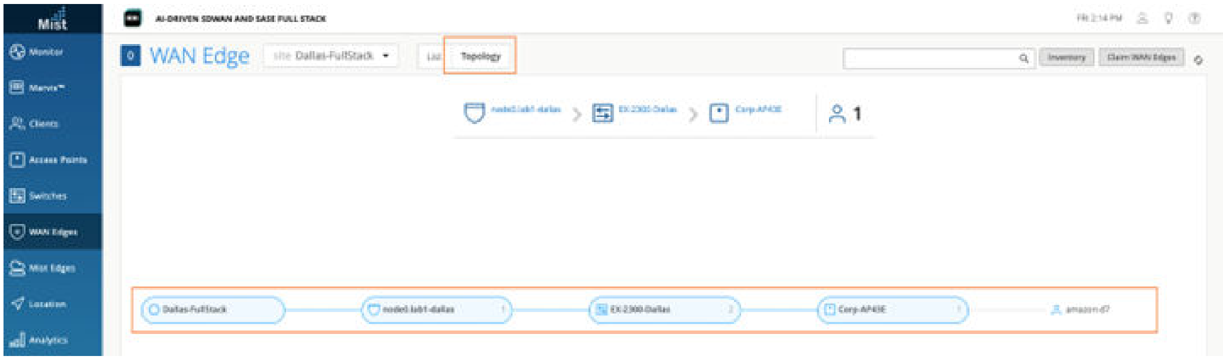
Table 77: WAN Edge Device Details

Fields	Description
Name	Name

Status	Connected or disconnected
MAC	MAC address
IP Address	IP address
Model	Juniper® Session Smart™ Routers or Juniper Networks® SRX Series Firewalls
Version	SSR Software Version
Topology	Hub or Spoke
Errors	Error state

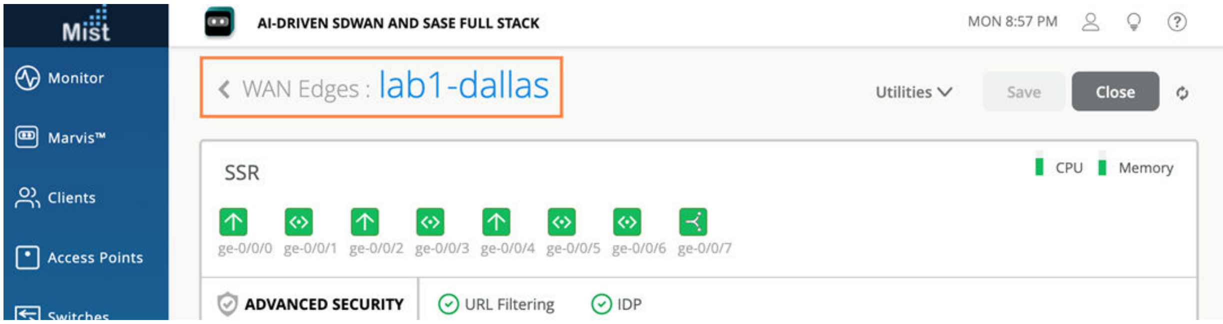
The **Topology** format presents the same information as the **List** view. For example, if you hover over the node0.lab1-dallas device, you'll see the same information as that displayed in the List view as you'll see in the figure below.

Figure 459: WAN Edges Topology View



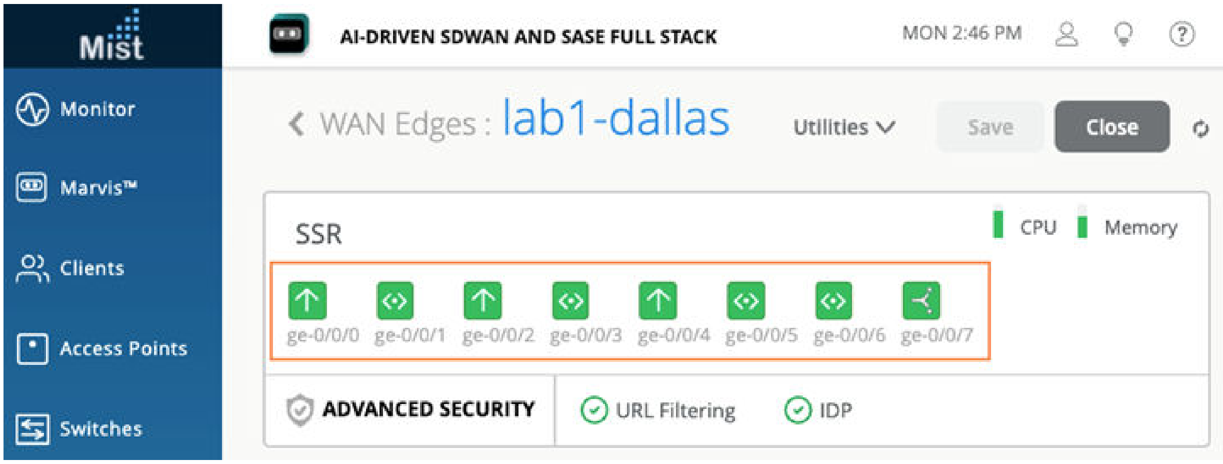
On both the List and Topology view, selecting your WAN edge device (lab1-dallas in this example) brings you to its Device Information page. The Device Information page provides different categories of monitoring information for your WAN edge device.

Figure 460: WAN Edges Device Information Page



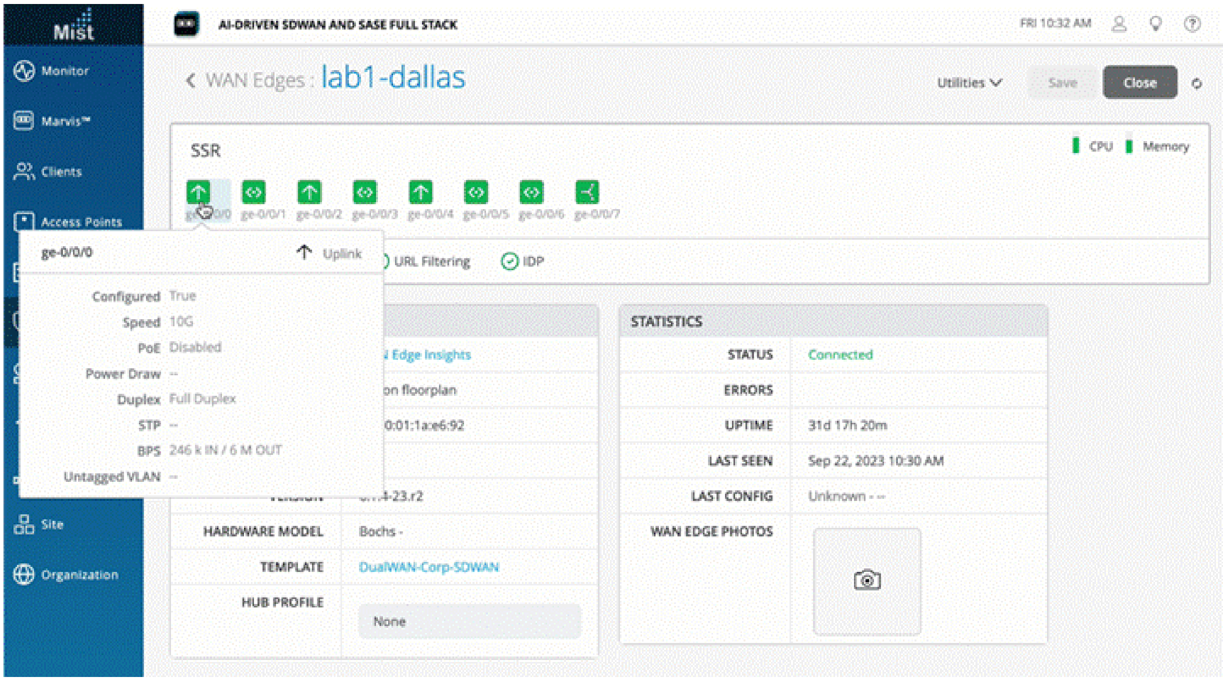
The first thing you'll notice on the Device Information Page is details about the WAN edge device you selected, (lab1-dallas in our figure). The information includes a graphical front view of the device ports and baseline status information such as CPU and memory utilization.

Figure 461: WAN Edges Device Information - Interfaces



For each Gigabit Ethernet interface you'll find link information.

Figure 462: WAN Edge Device Information Page- Details



ge-0/0/0 Uplink

Configured	True
Speed	10G
PoE	Disabled
Power Draw	--
Duplex	Full Duplex
STP	--
BPS	246 k IN / 6 M OUT
Untagged VLAN	--

	0:01:1a:e6:92
VERSION	...4-23.r2
HARDWARE MODEL	Bochs -
TEMPLATE	DualWAN-Corp-SDWAN
HUB PROFILE	None

STATISTICS

STATUS	Connected
ERRORS	
UPTIME	31d 17h 20m
LAST SEEN	Sep 22, 2023 10:30 AM
LAST CONFIG	Unknown - --
WAN EDGE PHOTOS	

Table 78: Link Information for Gigabit Ethernet Interface

Fields	Description
Configured	True or false
Speed	Rated speed
PoE	Enabled or disbaled
Power Draw	Measured PoE power draw
Duplex	Full or half
STP	True or false
BPS	Bits/second
Untagged VLAN	-

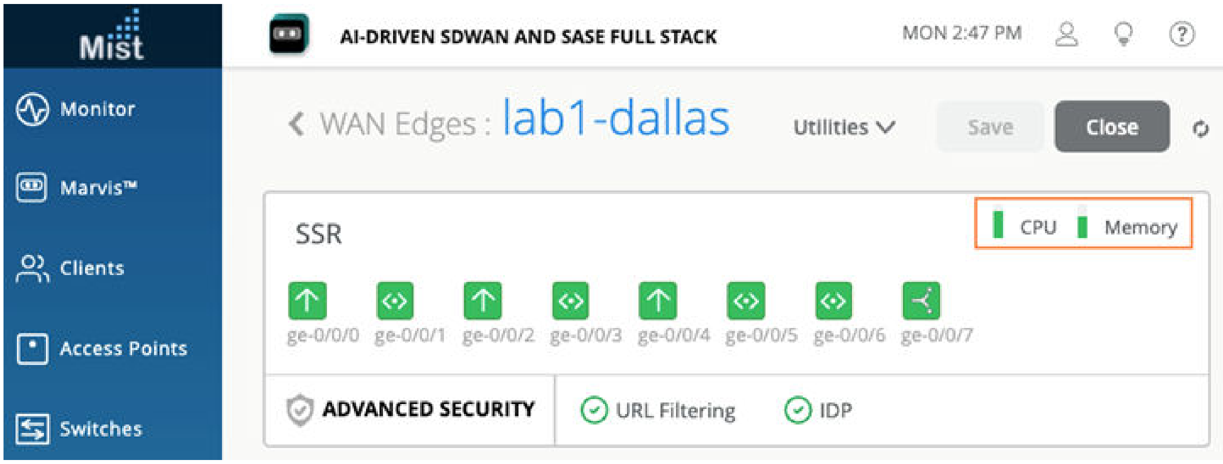
When hovering over Wired Clients, you'll get similar information with additional information.

Table 79: Wired Clients Details

Fields	Description
Hostname	Name of the device
Username	User name
MAC	MAC address of the device
IP Address	IP address of the device
Manufacturer	Type of device- SSR / SRX

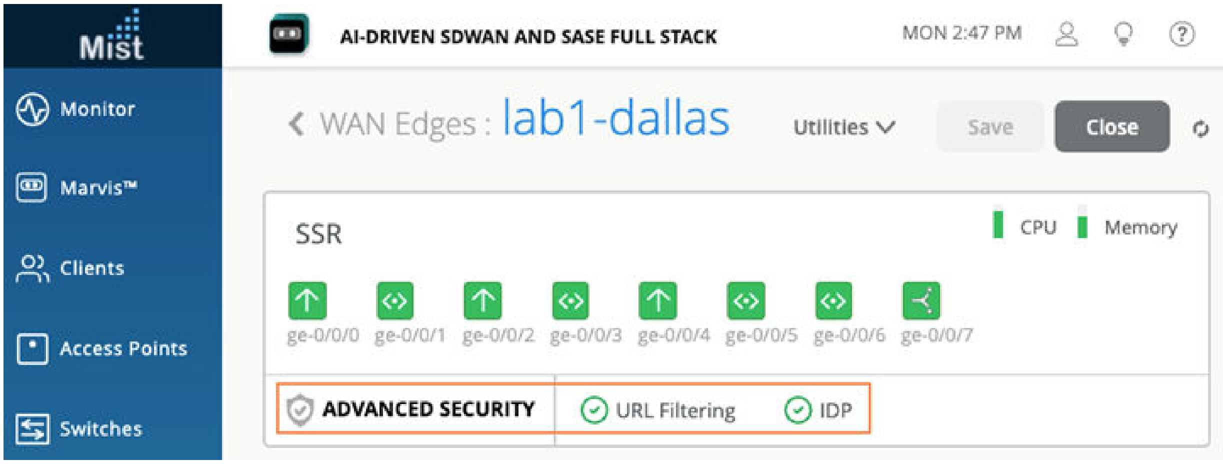
The CPU and Memory status icon indicates how your device behaves. Hover over each interface icon for deeper insights.

Figure 463: WAN Edges - CPU and Memory Status



Advanced Security information is listed below the device ports with a checkmark or an X, indicating whether URL filtering or intrusion detection and prevention (**IDP**) is active on this device. Here, both URL filtering and IDP are active with the green checkmark.

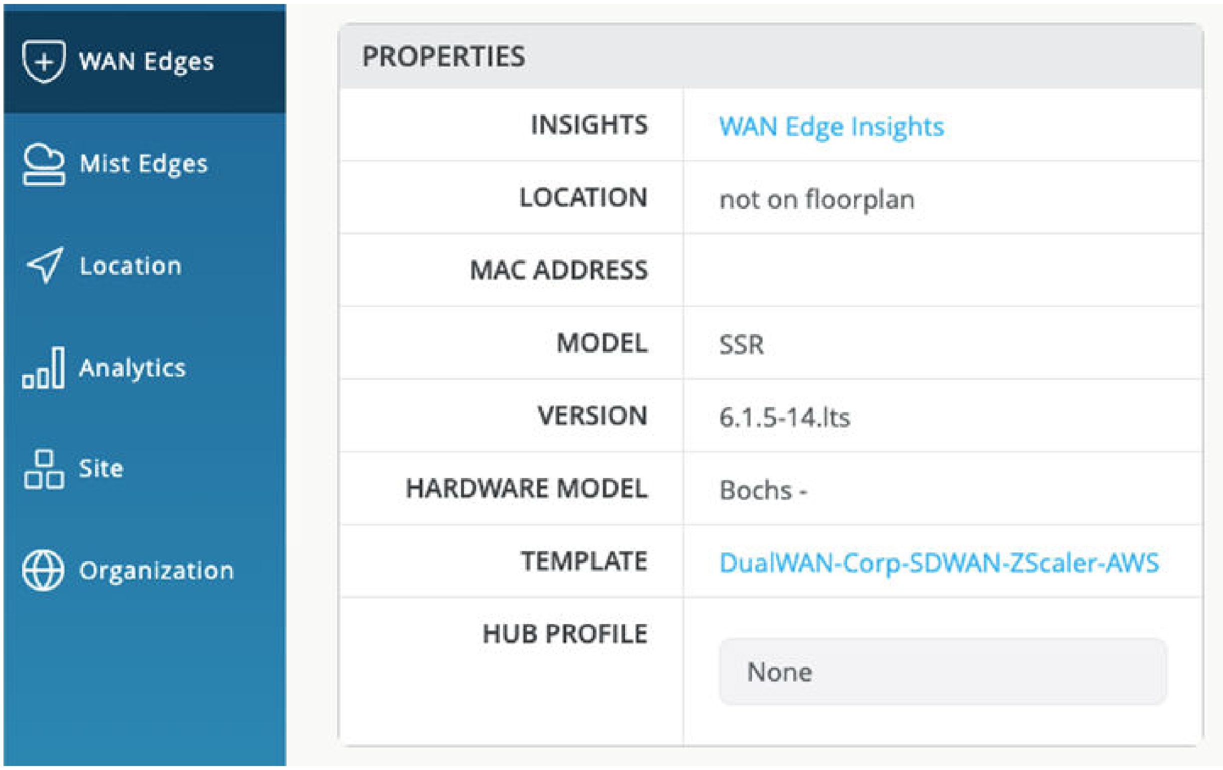
Figure 464: Advanced Security Details



ADVANCED SECURITY	✓ URL Filtering	✓ IDP

Below our port information and security section, you'll find generalized data for your WAN edge device, including:

Figure 465: WAN Edge Device Properties



PROPERTIES

INSIGHTS	WAN Edge Insights
LOCATION	not on floorplan
MAC ADDRESS	
MODEL	SSR
VERSION	6.1.5-14.lts
HARDWARE MODEL	Bochs -
TEMPLATE	DualWAN-Corp-SDWAN-ZScaler-AWS
HUB PROFILE	None

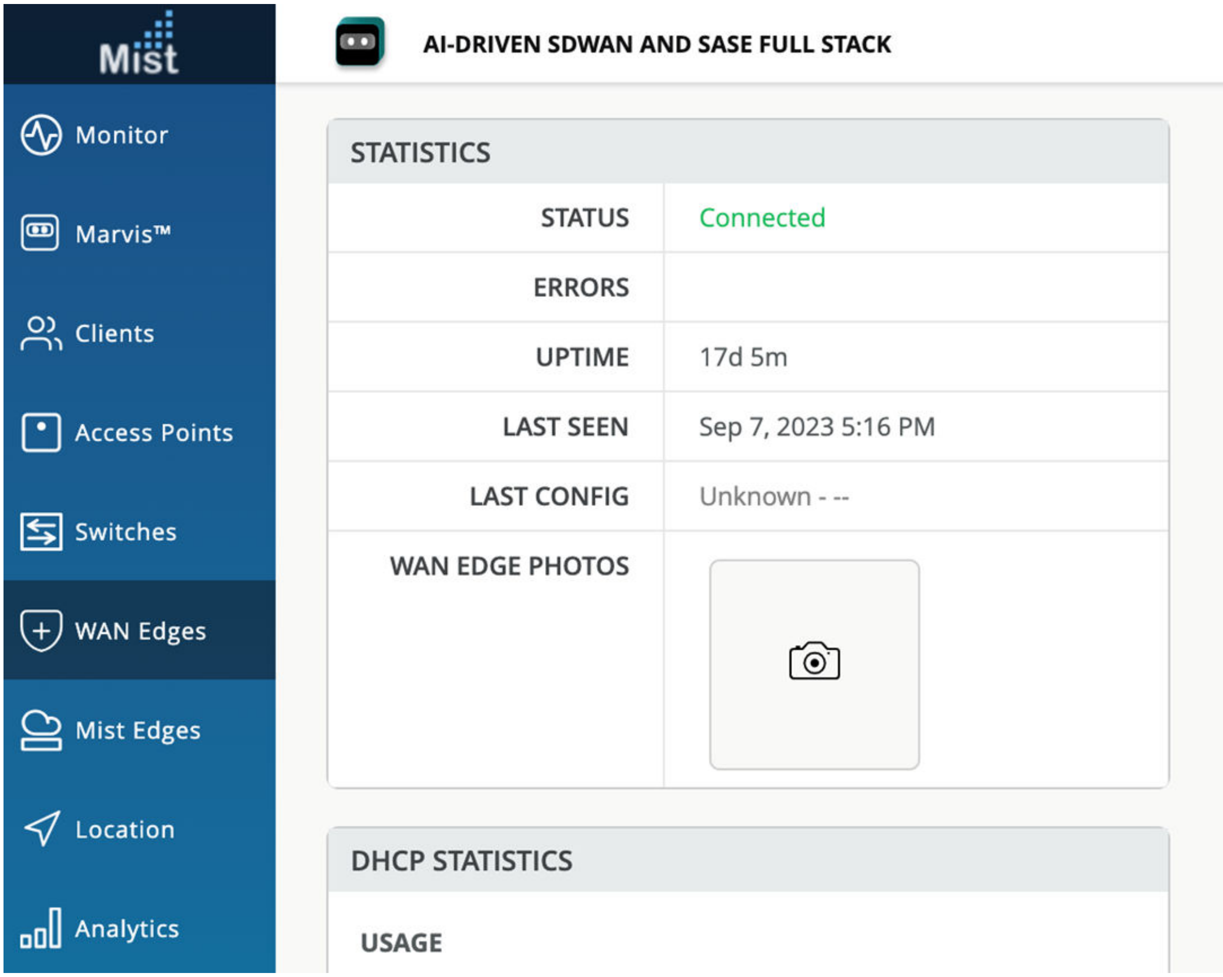
Properties contains generalized platform-related information.

Table 80: WAN Edge Platform-Related Details

Field	Description
Insights	Provides a direct link to WAN Edge Insights.
Location	Provides floorplan information
MAC Address	MAC Address for the SSR device
Model	Indicates if model type is SSR or SRX
Version	Version of the Session Smart Software
Hardware Model	Lists the Whitebox or Juniper Networks device model name and number.
Template	The applied WAN edge template to the device.
Hub Profile	The applied Hub Profile to the device.

Statistics displays action information about your platform.

Figure 466: WAN Edge Device Statistics



AI-DRIVEN SDWAN AND SASE FULL STACK

STATISTICS

STATUS	Connected
ERRORS	
UPTIME	17d 5m
LAST SEEN	Sep 7, 2023 5:16 PM
LAST CONFIG	Unknown - --
WAN EDGE PHOTOS	

DHCP STATISTICS

USAGE

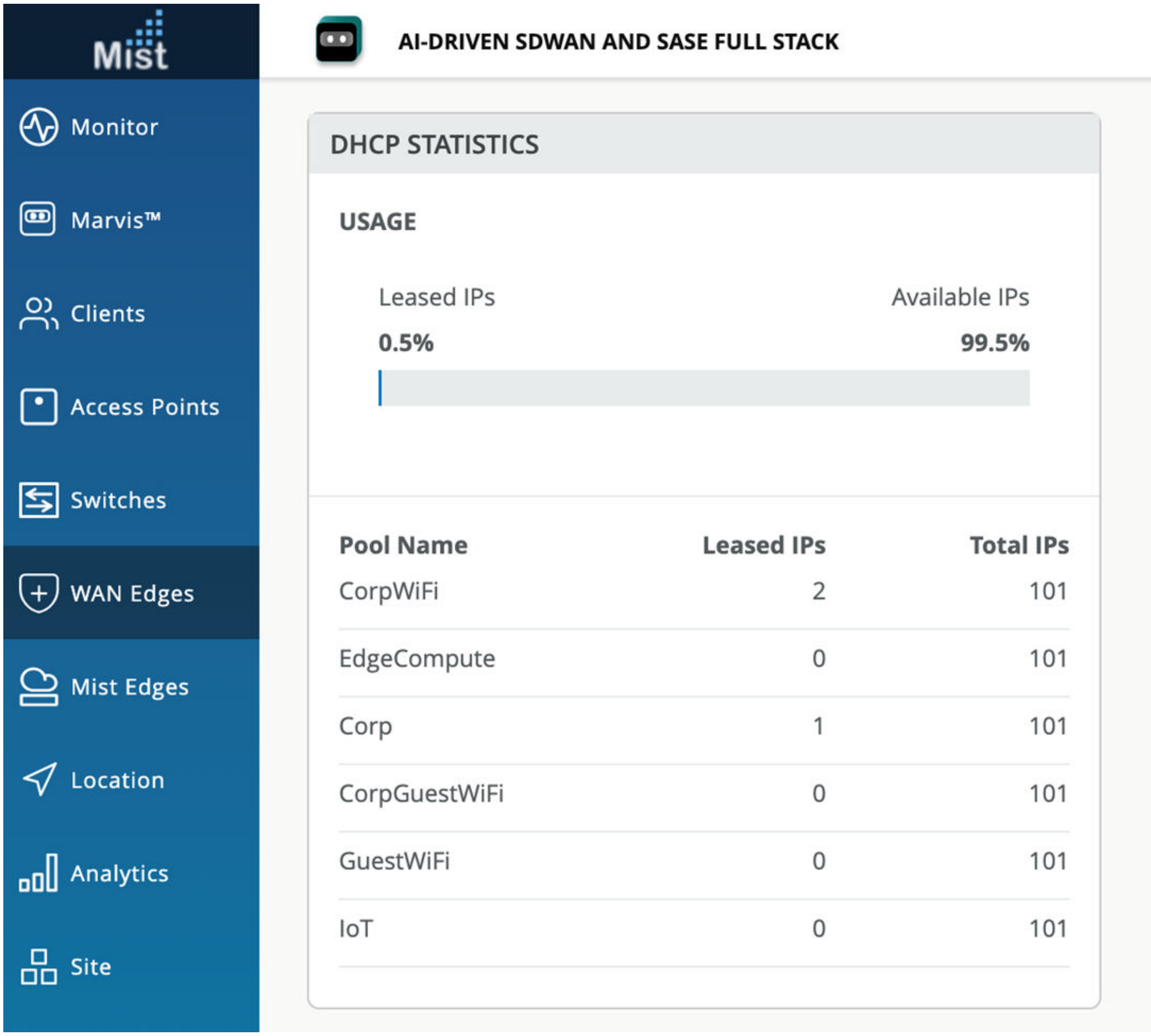
Table 81: WAN Edge Device Statistics

Field	Description
Status	Connected /Disconnected
Errors	Any commit errors
Uptime	Day/Hour/Min uptime information
Last Seen	Last login
Last Config	Last Commit
WAN Edge Photos	Photos of the WAN edge device

If you configured DHCP servers on the WAN router itself, there will also be a DHCP Statistics pane with information about the leased IPs.

- **DHCP Statistics** presents IP information related to dynamic distributed IP addresses.

Figure 467: WAN Edge Device DHCP Statistics



DHCP STATISTICS

USAGE

Leased IPs 0.5%

Available IPs 99.5%

Pool Name	Leased IPs	Total IPs
CorpWiFi	2	101
EdgeCompute	0	101
Corp	1	101
CorpGuestWiFi	0	101
GuestWiFi	0	101
IoT	0	101

Table 82: WAN Edge Device DHCP Statistics

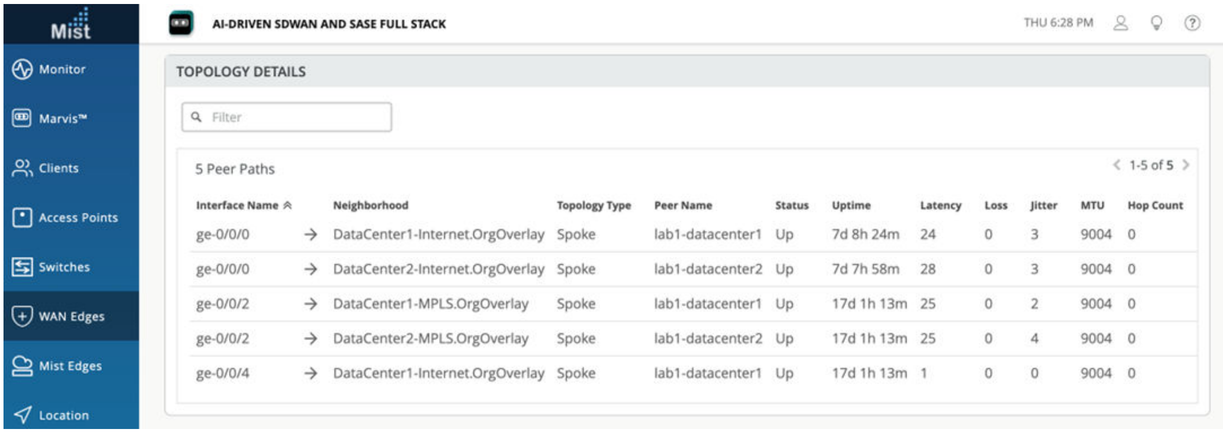
Field	Description
Usage	The total figure presented as a percentage of Leased and Available IPs

Pool Name	The name for given pool of addresses
Leased IPs	Number of used IP addresses in each pool.
Total IPs	Total number available of IP addresses in each pool.

As you scroll down the device information page, you'll find Secure Vector Routing (SVR)-based Paths between devices that provide information about connectivity through WAN interfaces to the hubs. Here, you can review your WAN edge device configuration. Usually, WAN edges inherit templates or profiles. However, you can make individual changes to the configuration to be pushed to the device.

Topology Details displays Peer Path information. Remember that a Session Smart SD-WAN network overlay is generated through Secure Vector Routing Peer connections between Session Smart devices.

Figure 468: Topology Details



TOPOLOGY DETAILS

5 Peer Paths

Interface Name		Neighborhood	Topology Type	Peer Name	Status	Uptime	Latency	Loss	Jitter	MTU	Hop Count
ge-0/0/0	→	DataCenter1-Internet.OrgOverlay	Spoke	lab1-datacenter1	Up	7d 8h 24m	24	0	3	9004	0
ge-0/0/0	→	DataCenter2-Internet.OrgOverlay	Spoke	lab1-datacenter2	Up	7d 7h 58m	28	0	3	9004	0
ge-0/0/2	→	DataCenter1-MPLS.OrgOverlay	Spoke	lab1-datacenter1	Up	17d 1h 13m	25	0	2	9004	0
ge-0/0/2	→	DataCenter2-MPLS.OrgOverlay	Spoke	lab1-datacenter2	Up	17d 1h 13m	25	0	4	9004	0
ge-0/0/4	→	DataCenter1-Internet.OrgOverlay	Spoke	lab1-datacenter1	Up	17d 1h 13m	1	0	0	9004	0

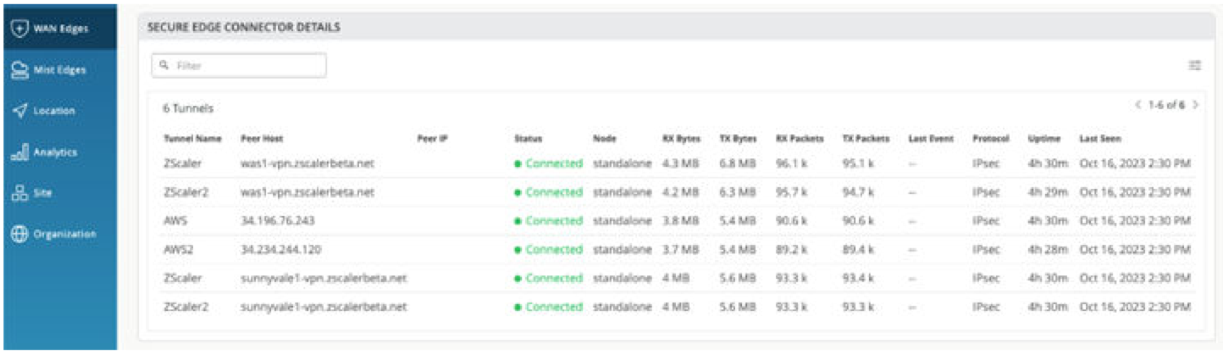
Table 83: Topology Details

Field	Description
Interface Name	Lists the name of the interface
Neighborhood	The shared layer 3 connection between Peers
Topology Type	Indicates Hub/Spoke
Status	Indicates up/down
Peer Name	Peer SVR device

Uptime	Time up and live
Latency	Measured in Milliseconds
Loss	Packet loss
Jitter	Measured in Milliseconds
MTU	Max Transmission Unit
Hop Count	Number of Hops

Secure Edge Connector Details include tunnel information from your WAN edge connection to the Secure Edge cloud.

Figure 469: Secure Edge Connector Details



Tunnel Name	Peer Host	Peer IP	Status	Node	RX Bytes	TX Bytes	RX Packets	TX Packets	Last Event	Protocol	Uptime	Last Seen
ZScaler	was1-vpn.zscalerbeta.net		● Connected	standalone	4.3 MB	6.8 MB	96.1 k	95.1 k	–	IPsec	4h 30m	Oct 16, 2023 2:30 PM
ZScaler2	was1-vpn.zscalerbeta.net		● Connected	standalone	4.2 MB	6.3 MB	95.7 k	94.7 k	–	IPsec	4h 29m	Oct 16, 2023 2:30 PM
AWS	34.196.76.243		● Connected	standalone	3.8 MB	5.4 MB	90.6 k	90.6 k	–	IPsec	4h 30m	Oct 16, 2023 2:30 PM
AWS2	34.234.244.120		● Connected	standalone	3.7 MB	5.4 MB	89.2 k	89.4 k	–	IPsec	4h 28m	Oct 16, 2023 2:30 PM
ZScaler	sunnyvale1-vpn.zscalerbeta.net		● Connected	standalone	4 MB	5.6 MB	93.3 k	93.4 k	–	IPsec	4h 30m	Oct 16, 2023 2:30 PM
ZScaler2	sunnyvale1-vpn.zscalerbeta.net		● Connected	standalone	4 MB	5.6 MB	93.3 k	93.3 k	–	IPsec	4h 30m	Oct 16, 2023 2:30 PM

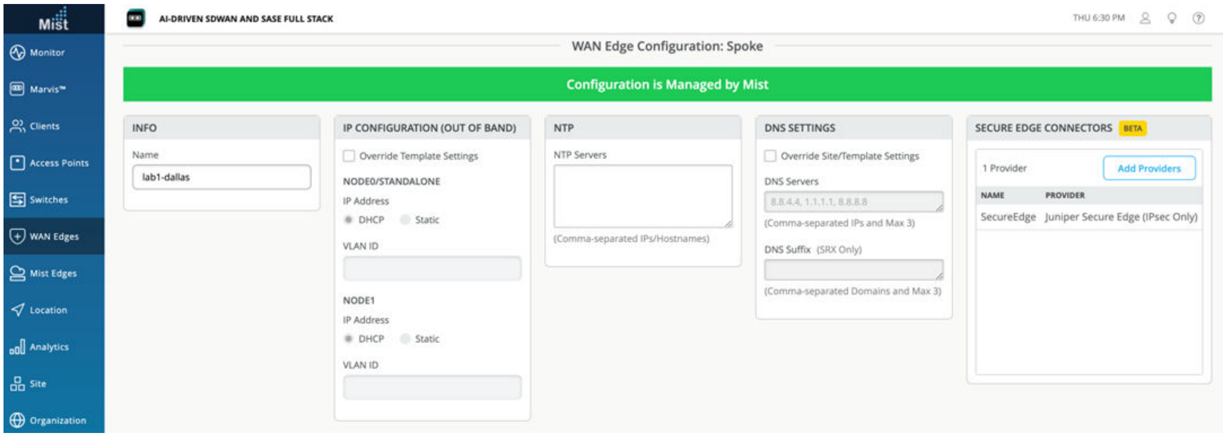
Table 84: Secure Edge Connector Details

Fields	Description
Tunnel Name	Name
Peer Host	Peer Host IP Address
Peer IP	Peer IP
Status	Connected/Disconnected
Node	Standalone/HA

RX Bytes	Volume of data, in bytes, received by the interface.
TX Bytes	Volume of data, in bytes, transmitted by the interface.
RX Packets	Packets received by the interface.
TX Packets	Packets transmitted by the interface.
Last Event	System events
Protocol	Protocol
Uptime	time live
Last Seen	Last login

Scrolling down the device information page, you'll find configuration information for your WAN edge. First, it'll indicate hub or spoke with relevant information about your **WAN Edge Configuration**.

Figure 470: WAN Edge Configuration: Spoke



WAN Edge Configuration: Spoke

Configuration is Managed by Mist

INFO

Name: lab1-dallas

IP CONFIGURATION (OUT OF BAND)

□ Override Template Settings

NODE0/STANDALONE

IP Address: ● DHCP ○ Static

VLAN ID

NODE1

IP Address: ● DHCP ○ Static

VLAN ID

NTP

NTP Servers

(Comma-separated IPs/Hostnames)

DNS SETTINGS

□ Override Site/Template Settings

DNS Servers: 8.8.4.4, 1.1.1.1, 8.8.8.8

(Comma-separated IPs and Max 3)

DNS Suffix (SRX Only)

(Comma-separated Domains and Max 3)

SECURE EDGE CONNECTORS

1 Provider

NAME	PROVIDER
SecureEdge	Juniper Secure Edge (IPsec Only)

Table 85: WAN Edge Configuration: Spoke

Field	Description
Info	Name
IP Configuration	Override Template Settings, node1 DHCP/Static, VLAN ID, node 2 DHCP/Static, VLAN ID

NTP	Time Servers IP/Hostnames
DNS	Override Template Settings, DNS Servers, (SRX only DNS suffix info)
Secure Edge Connector	Provider for the Secure Edge Connector.

Scrolling past the configuration, you'll find information for your connected WANs and LANs.

Figure 471: WAN Details

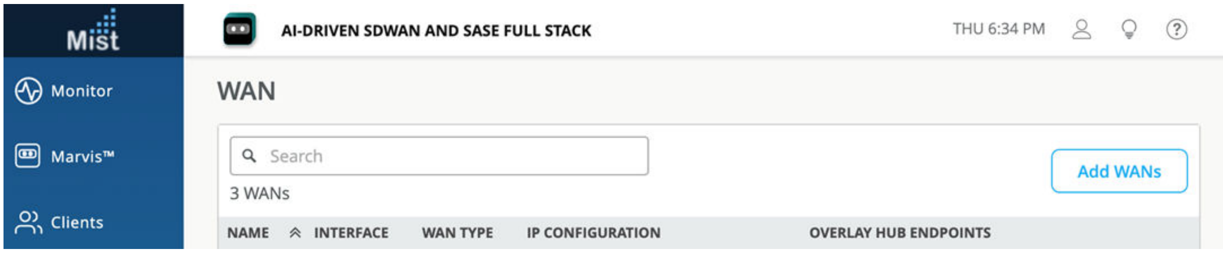


Table 86: WAN Details

Field	Description
Name	Selected WAN Interface Name
Interface	Supports one of these interfaces for aggregation: ge-0/0/1, ge-0/0/1-5, or reth0.
WAN Type	Ethernet, DSL (SRX Only) LTE
IP Configuration	DHCP, Static, or PPPoE
Overlay Hub Endpoints	SVR Peer connections to the Hub

Figure 472: LAN Details

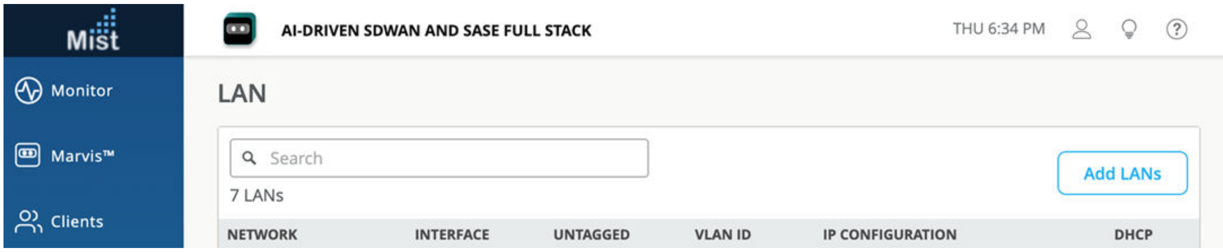


Table 87: LAN Details

Field	Description
Network	Selected LAN name.
Interface	Supports one of these interfaces for aggregation: ge-0/0/1, ge-0/0/1-5, or reth0.
Untagged	Untagged VLAN (SRX only)
VLAN ID	DHCP, Static, or PPPoE
IP Configuration	SVR Peer connections to the Hub
DHCP	Relay, Server, none.

The Traffic Steering and Application Policy sections show how you use the Session Smart Secure Vector Routing process to create rules for path choice and routing behavior. Note that on the SRX Series deployed as a WAN edge, the Application Policy and Traffic Steering path determine destination zones and must be assigned. The Session Smart router is first and foremost, a router and will use the closest match for the address.

Figure 473: Traffic Steering

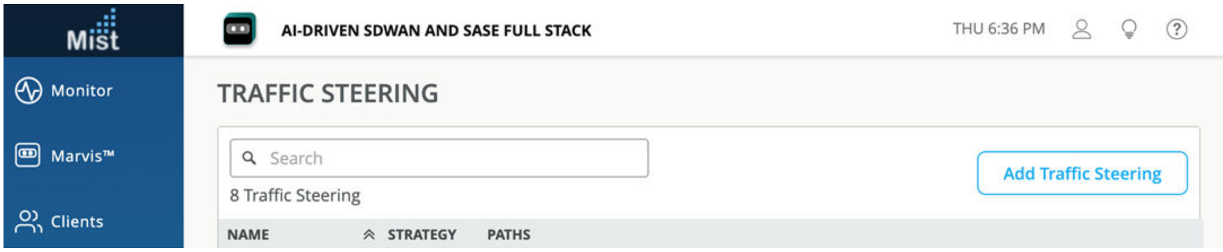
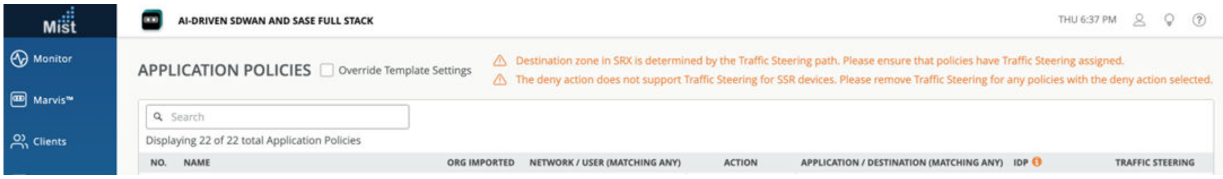


Table 88: Traffic Steering

Field	Description
Name	Selected Traffic Steering name.
Strategy	Ordered, weighted, ECMP
Paths	Untagged VLAN (SRX only)

Application Policies are the heart of Juniper's AI-Driven SD-WAN. Remember that 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. You must create Networks, Applications, and establish Traffic Steering profiles to define an Application Policy. These elements become matching criteria to allow access to or block access from applications or destinations.

Figure 474: Application Policies


Mist
Monitor
Marvis™
Clients
AI-DRIVEN SDWAN AND SASE FULL STACK
THU 6:37 PM
APPLICATION POLICIES
□ Override Template Settings
Search

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

⚠ The deny action does not support Traffic Steering for SSR devices. Please remove Traffic Steering for any policies with the deny action selected.

Displaying 22 of 22 total Application Policies

NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING

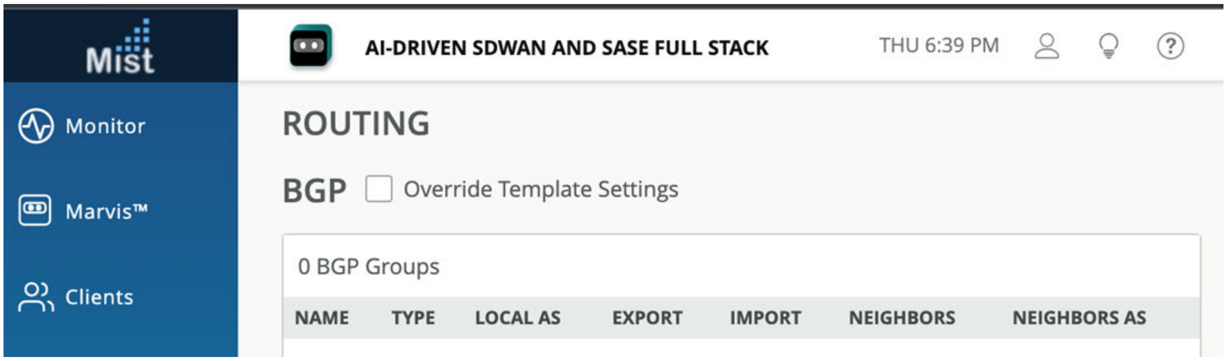
In the Juniper Mist™ cloud portal, the Networks or Users setting determines the source zone. The Applications and Traffic Steering settings determine the destination zone. Traffic Steering paths determine the destination zone in Juniper Networks® SRX Series Firewalls, so ensure that you assign Traffic Steering profiles to the Application Policies.

Table 89: Application Policies Details

Field	Description
Number	Ordered Policy Number
Name	Selected name
Org Imported	Indicates if the policy was pushed down from the Organization level to the Site.
Network/User (Matching Any)	The "source" of your traffic
Action	Allow/Block
Application/Destination (Matching Any)	The "destination" for your traffic.
IDP	Indicates IDP/URL filtering (requires separate license)
Traffic Steering	Indicate path for traffic

The bottom of the Device Information page has tables for routing properties such as BGP and static routes connected to your WAN edge device. You can also manually add a BGP Group here.

Figure 475: Routing Details



ROUTING

BGP □ Override Template Settings

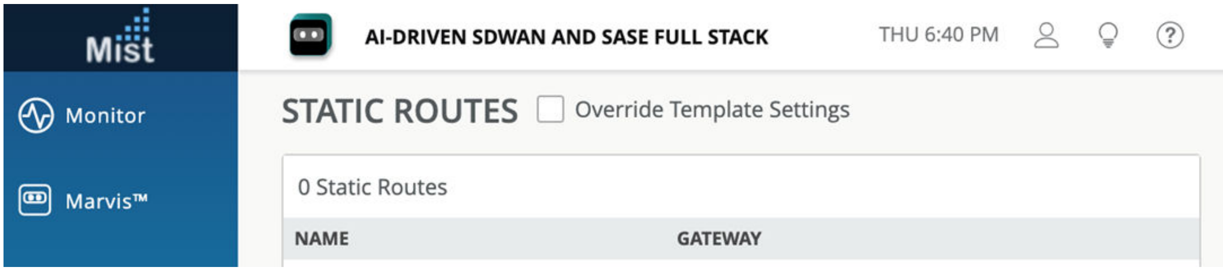
0 BGP Groups

NAME	TYPE	LOCAL AS	EXPORT	IMPORT	NEIGHBORS	NEIGHBORS AS

Table 90: Routing Details

Field	Description
Name	BGP Name
Type	Type of BGP Route
Local AS	Autonomous System Number
Export	Exported Route
Import	Imported Route
Neighbors	Neighbor Route
Neighbor AS	Autonomous System Number for Neighbor Route

Figure 476: Static Routes



STATIC ROUTES □ Override Template Settings

0 Static Routes

NAME	GATEWAY

Static Routes display name and gateway information.

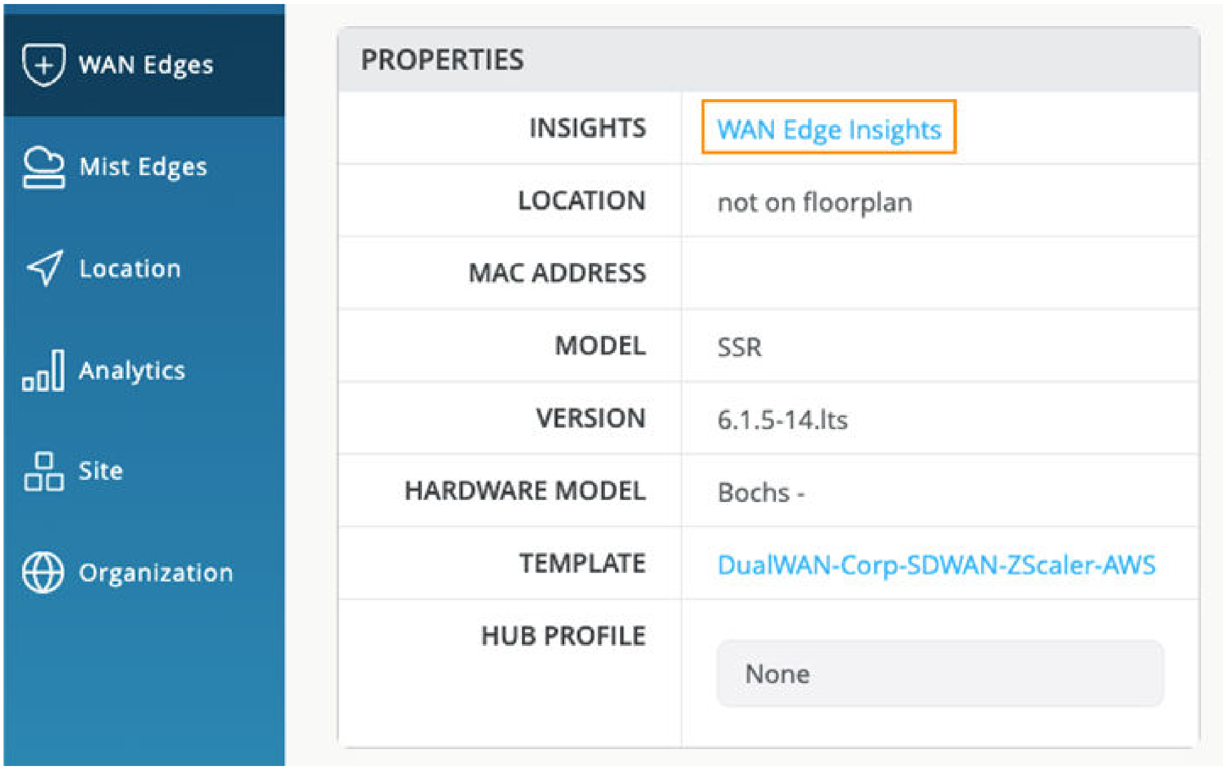
Monitoring: Device Information, WAN Edge Insights, Peer Path Statistics

IN THIS SECTION

WAN Edge Insights

The Properties pane for your selected WAN edge links to **WAN Edge Insights**. Click **WAN Edge Insights** for the next level of information about your WAN edge device.

Figure 477: WAN Edge Insights

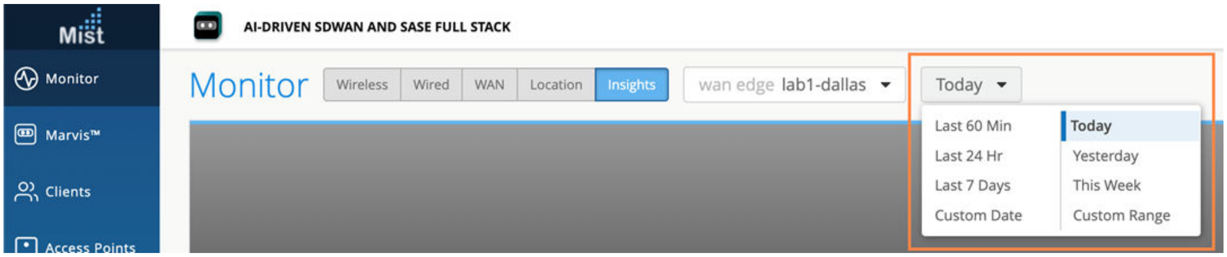


PROPERTIES

INSIGHTS	WAN Edge Insights
LOCATION	not on floorplan
MAC ADDRESS	
MODEL	SSR
VERSION	6.1.5-14.lts
HARDWARE MODEL	Bochs -
TEMPLATE	DualWAN-Corp-SDWAN-ZScaler-AWS
HUB PROFILE	None

Next to the selected WAN edge (lab1-dallas) on the Insights page, you can select a timeframe for selected information. The default view is **Today,** but this can be set to a customized date or range of dates. Below this, you find (when the site location information is configured) where this WAN edge is configured via a street map.

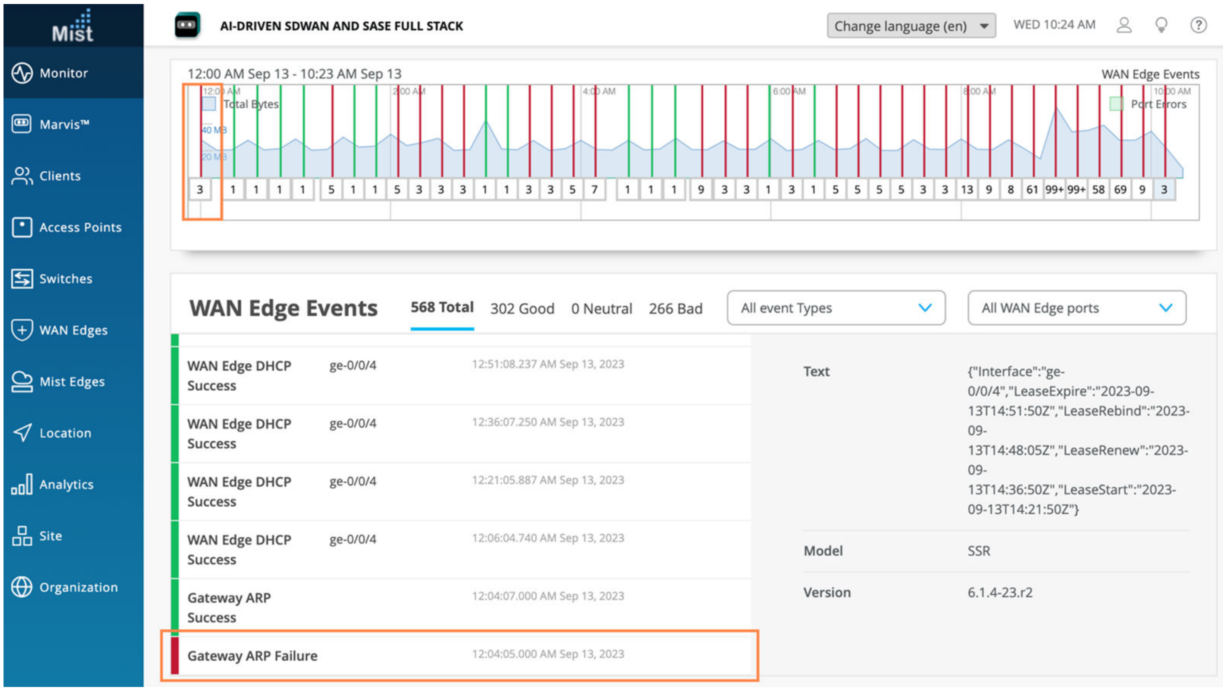
Figure 478: WAN Edge Insights-Select Time Duration



With your timeframe selected, **WAN Edge Events** displays a timeline of the traffic through the WAN edge during your specified time, and a list of events in the same window.

Select a specific event in the listed WAN Edge Events for greater detail of the **Good**, **Neutral**, and **Bad** events.

Figure 479: WAN Edge Events Timeline



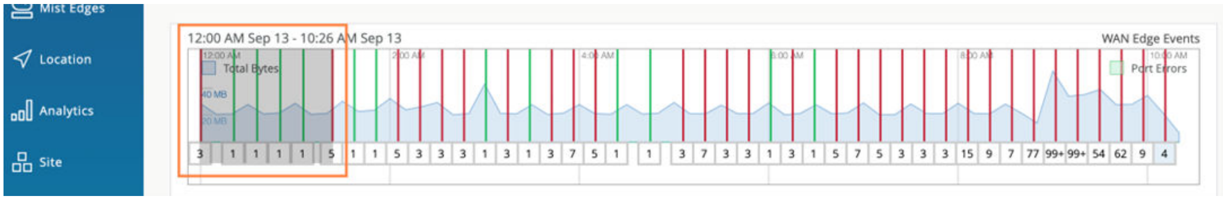
WAN Edge DHCP Success	ge-0/0/4	12:51:08.237 AM Sep 13, 2023
WAN Edge DHCP Success	ge-0/0/4	12:36:07.250 AM Sep 13, 2023
WAN Edge DHCP Success	ge-0/0/4	12:21:05.887 AM Sep 13, 2023
WAN Edge DHCP Success	ge-0/0/4	12:06:04.740 AM Sep 13, 2023
Gateway ARP Success		12:04:07.000 AM Sep 13, 2023
Gateway ARP Failure		12:04:05.000 AM Sep 13, 2023

Text	{"Interface":"ge-0/0/4","LeaseExpire":"2023-09-13T14:51:50Z","LeaseRebind":"2023-09-13T14:48:05Z","LeaseRenew":"2023-09-13T14:36:50Z","LeaseStart":"2023-09-13T14:21:50Z"}
Model	SSR
Version	6.1.4-23.r2

Your selection expands and displays detailed information about the selected time.

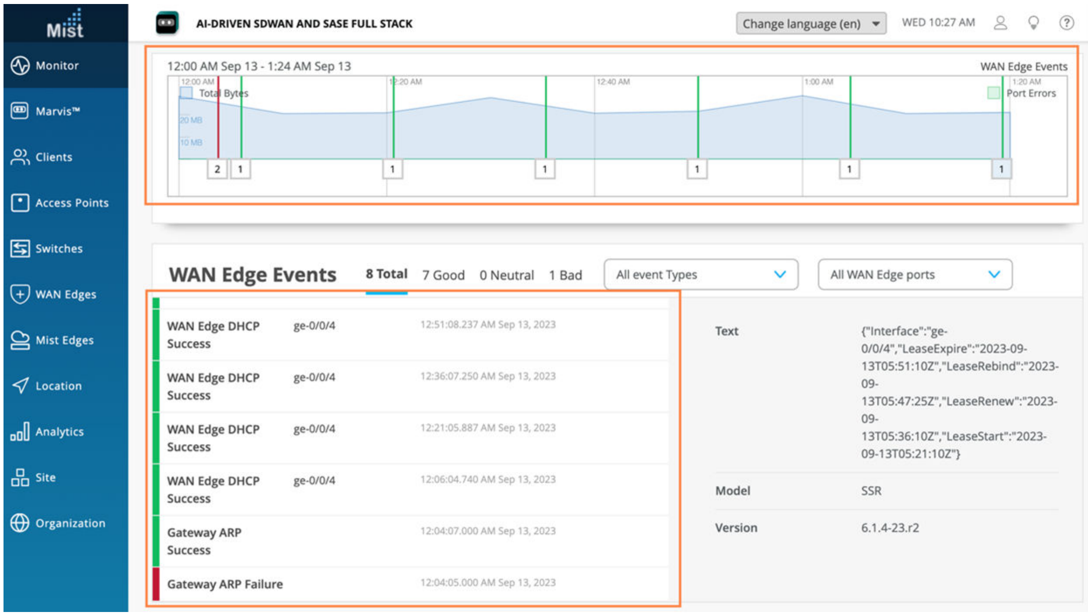
For a detailed portion of time, select a window of time with the mouse cursor. By doing this, you're able to adjust the window of events and isolate specific **Good**, **Neutral**, and **Bad** things that happened on your network. With a smaller section you'll get a more detailed view of that period.

Figure 480: WAN Edge Events Timeline Details View



Drill down the WAN Edge Events page for deeper insights within your selected period.

Figure 481: WAN Edge Events page

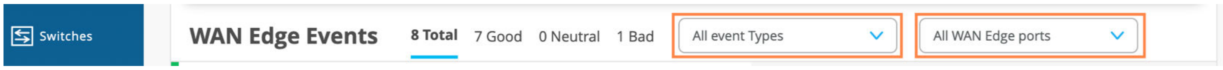


WAN Edge DHCP Success	ge-0/0/4	12:51:08.237 AM Sep 13, 2023
WAN Edge DHCP Success	ge-0/0/4	12:36:07.250 AM Sep 13, 2023
WAN Edge DHCP Success	ge-0/0/4	12:21:05.887 AM Sep 13, 2023
WAN Edge DHCP Success	ge-0/0/4	12:06:04.740 AM Sep 13, 2023
Gateway ARP Success		12:04:07.000 AM Sep 13, 2023
Gateway ARP Failure		12:04:05.000 AM Sep 13, 2023

Text	{"Interface":"ge-0/0/4","LeaseExpire":"2023-09-13T05:51:10Z","LeaseRebind":"2023-09-13T05:47:25Z","LeaseRenew":"2023-09-13T05:36:10Z","LeaseStart":"2023-09-13T05:21:10Z"}
Model	SSR
Version	6.1.4-23.r2

We can continue that way: You can narrow down on the type of event by selecting a modifier in the Event Type drop-down menu. You can also filter your search by limiting the event types to a specific port

Figure 482: WAN Edge Events Page

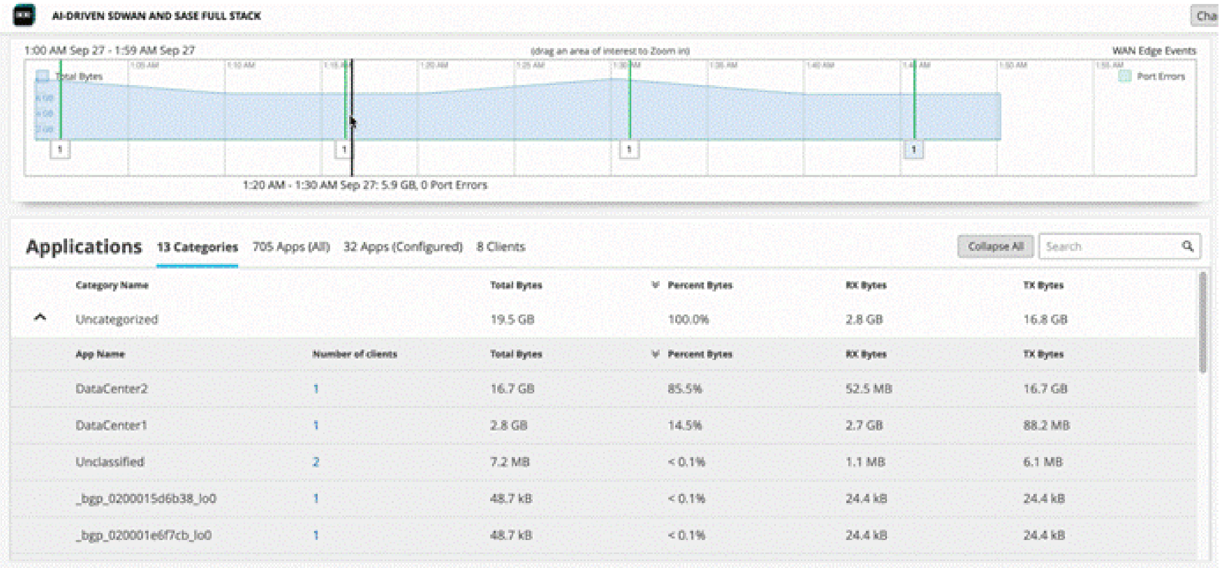


On the WAN Edge Events page, you can also view reports on applications on the Applications pane. On this pane:

- You can use categorized applications to monitor and troubleshoot specific application behavior.
- You can expand the categories to see more details.
- You can view a client's use of a particular application by clicking the Clients tab.

NOTE: Ensure you've had a few hours for these metrics to be populated following initial deployment.

Figure 483: Applications


AI-DRIVEN SDWAN AND SASE FULL STACK
Cha
1:00 AM Sep 27 - 1:59 AM Sep 27
(drag an area of interest to Zoom in)
WAN Edge Events
Total Bytes
Port Errors
1:05 AM
1:10 AM
1:20 AM
1:25 AM
1:30 AM
1:35 AM
1:40 AM
1:50 AM
1:55 AM
1
1
1
1
1:20 AM - 1:30 AM Sep 27: 5.9 GB, 0 Port Errors
Collapse All
Search

Applications 13 Categories 705 Apps (All) 32 Apps (Configured) 8 Clients

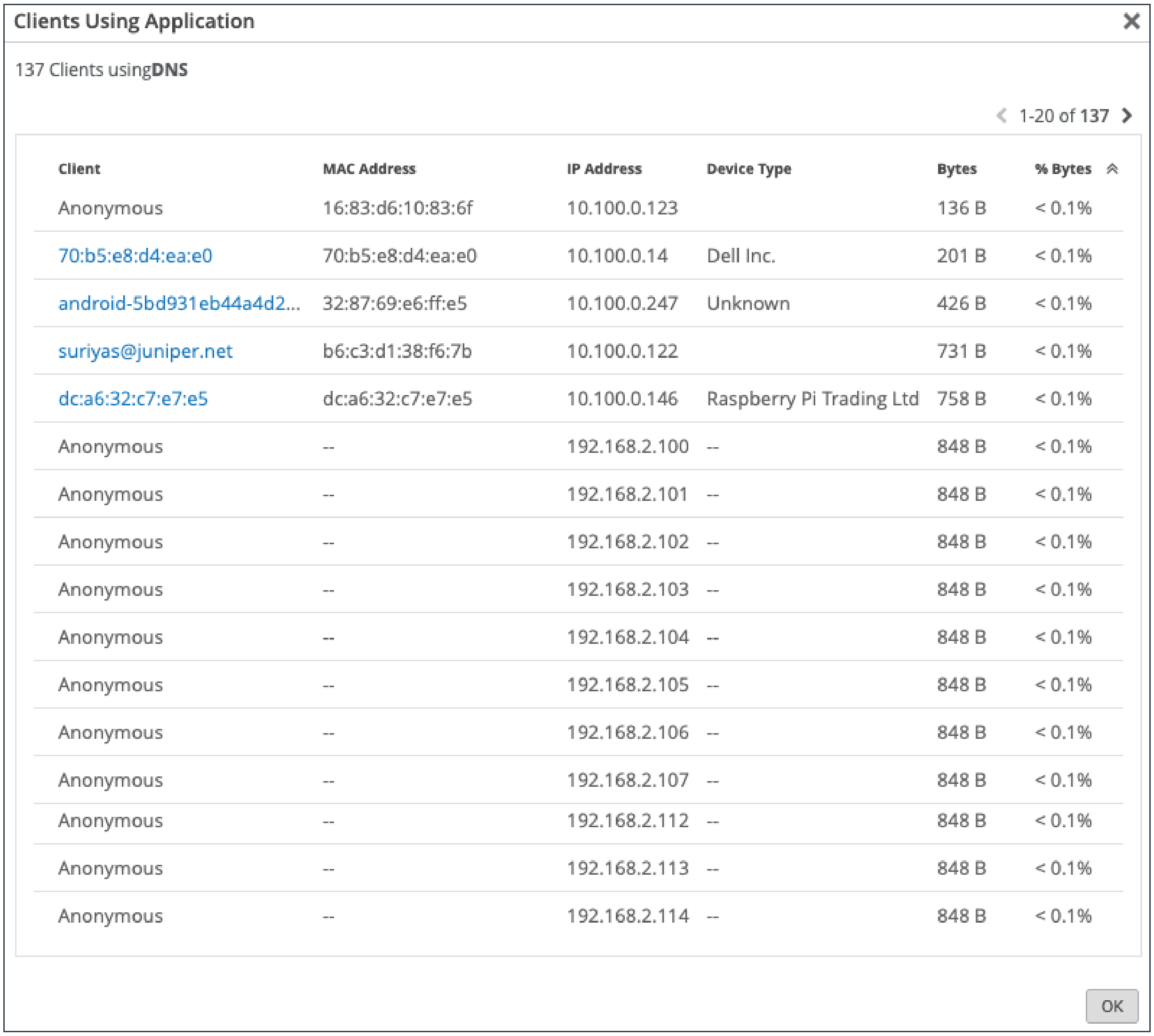
	Category Name		Total Bytes	Percent Bytes	RX Bytes	TX Bytes
^	Uncategorized		19.5 GB	100.0%	2.8 GB	16.8 GB
	App Name	**Number of clients**	**Total Bytes**	**Percent Bytes**	**RX Bytes**	**TX Bytes**
	DataCenter2	1	16.7 GB	85.5%	52.5 MB	16.7 GB
	DataCenter1	1	2.8 GB	14.5%	2.7 GB	88.2 MB
	Unclassified	2	7.2 MB	< 0.1%	1.1 MB	6.1 MB
	_bgp_0200015d6b38_lo0	1	48.7 kB	< 0.1%	24.4 kB	24.4 kB
	_bgp_020001e6f7cb_lo0	1	48.7 kB	< 0.1%	24.4 kB	24.4 kB

Click the **Clients** tab to see which client is using how much bandwidth.

Click the **Apps** tab, then in the **Number of Clients** column, you can click on the number of clients to see more information such as the Client name, MAC Address, IP Address, Device Type, and Bytes being used.

NOTE: For Session Smart Router devices running a DHCP server, clients using that application will display a HostName in the Client column if available. Otherwise, the MAC address will be displayed. Device Type and MAC Address columns will be populated as well.

Figure 484: Clients Using Application



Clients Using Application

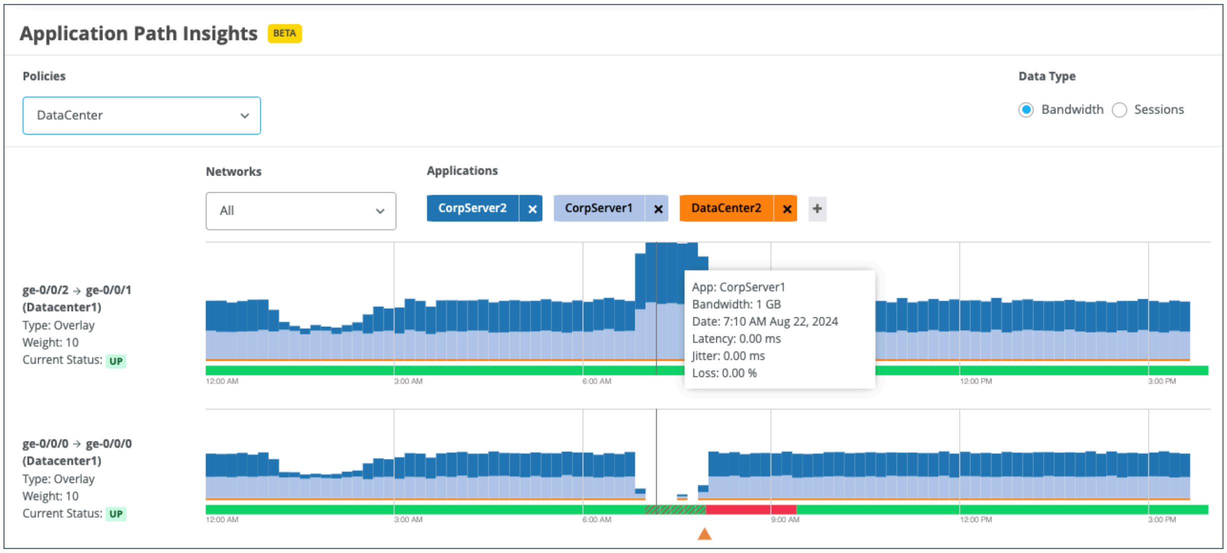
137 Clients using**DNS**

Client	MAC Address	IP Address	Device Type	Bytes	% Bytes
Anonymous	16:83:d6:10:83:6f	10.100.0.123		136 B	< 0.1%
70:b5:e8:d4:ea:e0	70:b5:e8:d4:ea:e0	10.100.0.14	Dell Inc.	201 B	< 0.1%
android-5bd931eb44a4d2...	32:87:69:e6:ff:e5	10.100.0.247	Unknown	426 B	< 0.1%
suriyas@juniper.net	b6:c3:d1:38:f6:7b	10.100.0.122		731 B	< 0.1%
dc:a6:32:c7:e7:e5	dc:a6:32:c7:e7:e5	10.100.0.146	Raspberry Pi Trading Ltd	758 B	< 0.1%
Anonymous	--	192.168.2.100	--	848 B	< 0.1%
Anonymous	--	192.168.2.101	--	848 B	< 0.1%
Anonymous	--	192.168.2.102	--	848 B	< 0.1%
Anonymous	--	192.168.2.103	--	848 B	< 0.1%
Anonymous	--	192.168.2.104	--	848 B	< 0.1%
Anonymous	--	192.168.2.105	--	848 B	< 0.1%
Anonymous	--	192.168.2.106	--	848 B	< 0.1%
Anonymous	--	192.168.2.107	--	848 B	< 0.1%
Anonymous	--	192.168.2.112	--	848 B	< 0.1%
Anonymous	--	192.168.2.113	--	848 B	< 0.1%
Anonymous	--	192.168.2.114	--	848 B	< 0.1%

The Application Path Insights (BETA) section shows you which applications are using the most bandwidth according to the selected Application Policy and Network. You can also change the Data Type to Sessions to see the number of sessions occurring per application. Hover over a section of the graph to view the bandwidth or sessions per application as well as jitter, loss, and latency.

Video: NOW in 60: WAN Assurance Application Insights Dashboard

Figure 485: Application Path Insights (BETA)



Application Path Insights BETA

Policies

DataCenter

Data Type

● Bandwidth ○ Sessions

Networks

All

Applications

CorpServer2 × CorpServer1 × DataCenter2 × +

ge-0/0/2 → ge-0/0/1
(Datacenter1)
Type: Overlay
Weight: 10
Current Status: UP

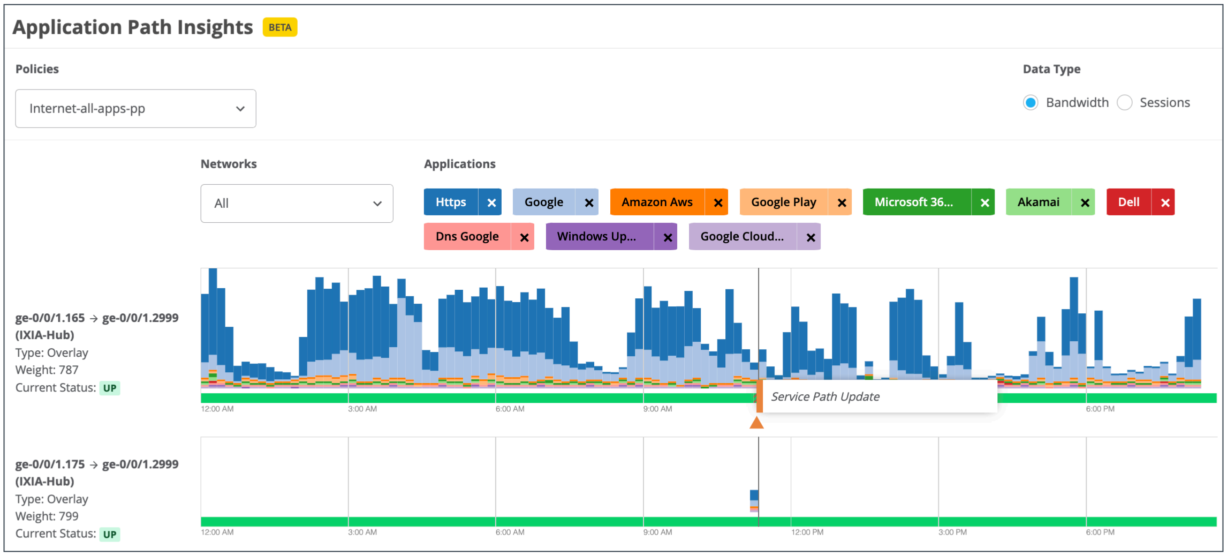
App: CorpServer1
Bandwidth: 1 GB
Date: 7:10 AM Aug 22, 2024
Latency: 0.00 ms
Jitter: 0.00 ms
Loss: 0.00 %

ge-0/0/0 → ge-0/0/0
(Datacenter1)
Type: Overlay
Weight: 10
Current Status: UP

The path state bar shows path state information over a timeline, and path state events are indicated by segments highlighted in different colors. For example, Path Up events are shown in green and Path Down events are shown in red.

If you see an orange triangle below the path state bar, this indicates that a Service Path Update event occurred. You can hover over the triangle to see the details.

Figure 486: Service Path Update



Application Path Insights BETA

Policies

Internet-all-apps-pp

Data Type

● Bandwidth ○ Sessions

Networks

All

Applications

Https × Google × Amazon Aws × Google Play × Microsoft 36... × Akamai × Dell × Dns Google × Windows Up... × Google Cloud... ×

ge-0/0/1.165 → ge-0/0/1.2999
(IXIA-Hub)
Type: Overlay
Weight: 787
Current Status: UP

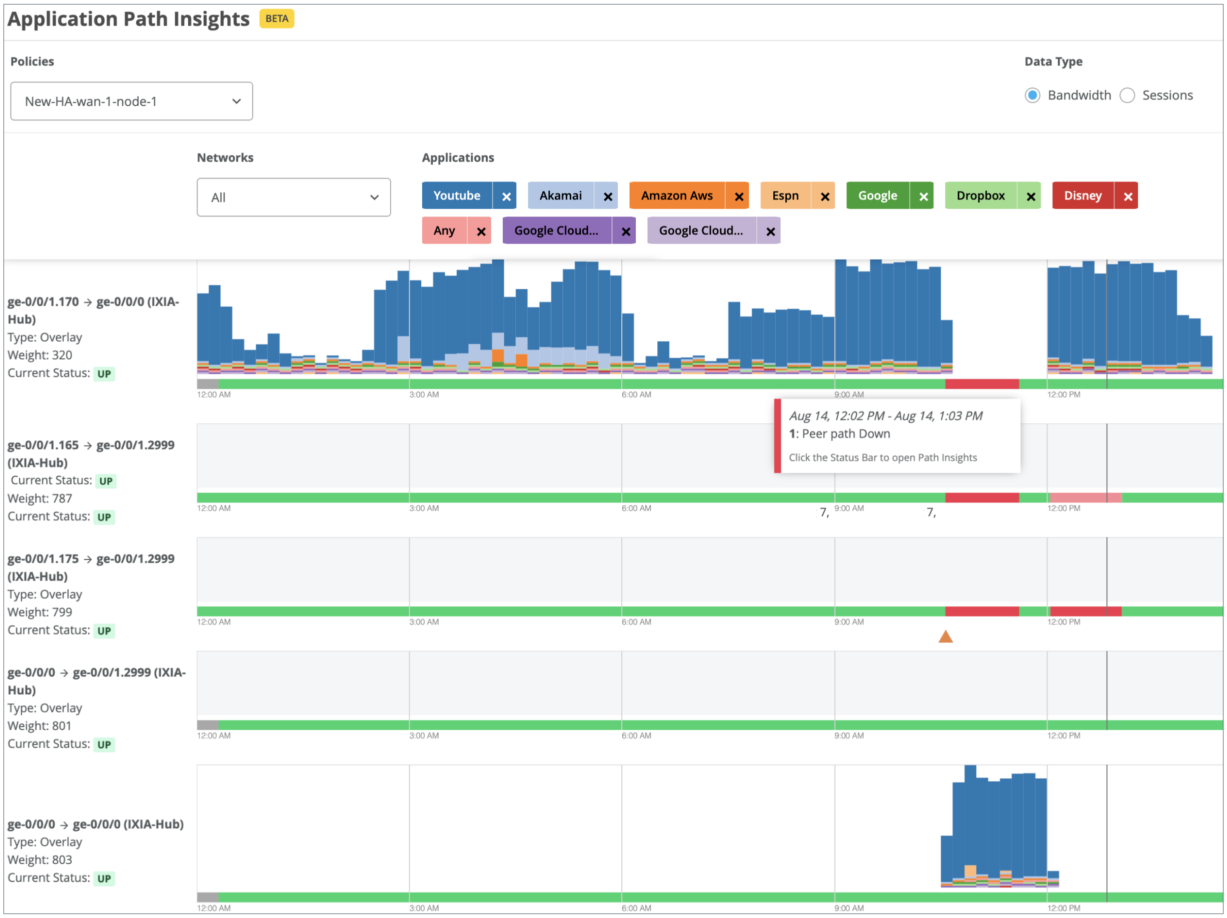
Service Path Update

ge-0/0/1.175 → ge-0/0/1.2999
(IXIA-Hub)
Type: Overlay
Weight: 799
Current Status: UP

The Application Path Insights section also includes a summary view on the lefthand side that displays recent path state events.

You can also hover over the highlighted portions of the path state bar to view a summary of the path state event.

Figure 487: Application Path Insights (BETA) continued



Application Path Insights BETA

Policies: New-HA-wan-1-node-1

Data Type: ● Bandwidth ○ Sessions

Networks: All

Applications: Youtube ✕ Akamai ✕ Amazon Aws ✕ Espn ✕ Google ✕ Dropbox ✕ Disney ✕ Any ✕ Google Cloud... ✕ Google Cloud... ✕

ge-0/0/1.170 → ge-0/0/0 (IXIA-Hub)
Type: Overlay
Weight: 320
Current Status: UP

Aug 14, 12:02 PM - Aug 14, 1:03 PM
1: Peer path Down
Click the Status Bar to open Path Insights

ge-0/0/1.165 → ge-0/0/1.2999 (IXIA-Hub)
Current Status: UP
Weight: 787
Current Status: UP

ge-0/0/1.175 → ge-0/0/1.2999 (IXIA-Hub)
Type: Overlay
Weight: 799
Current Status: UP

ge-0/0/0 → ge-0/0/1.2999 (IXIA-Hub)
Type: Overlay
Weight: 801
Current Status: UP

ge-0/0/0 → ge-0/0/0 (IXIA-Hub)
Type: Overlay
Weight: 803
Current Status: UP

If you click on the bar, you will get a pop-up window where you can view more detailed information about the path state events. The list of events displays on the left, and when you select an event, the reason for the event displays on the right.

Path state events include:

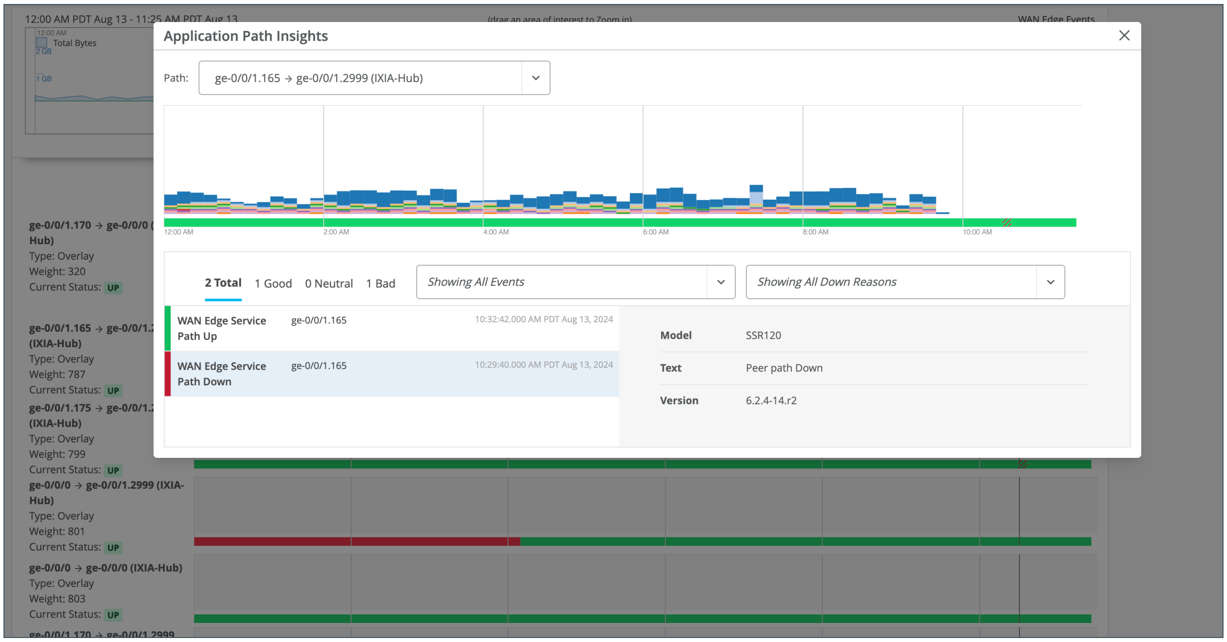
- Path Add
- Path Remove
- Path Update
- Port Down
- Path Up

- Path Down

  Path Down Reasons include:

  - Probe Down
  - Peer Path Down
  - ARP Unresolved
  - DHCP Failure

Figure 488: Path State Events and Reasons - Example 1



Application Path Insights

Path: ge-0/0/1.165 → ge-0/0/1.2999 (IXIA-Hub)

2 Total 1 Good 0 Neutral 1 Bad

Showing All Events

Showing All Down Reasons

Event	Interface	Time
WAN Edge Service Path Up	ge-0/0/1.165	10:32:42.000 AM PDT Aug 13, 2024
WAN Edge Service Path Down	ge-0/0/1.165	10:29:40.000 AM PDT Aug 13, 2024

Model	SSR120
Text	Peer path Down
Version	6.2.4-14.r2

ge-0/0/1.170 → ge-0/0/0 (
Hub)
Type: Overlay
Weight: 320
Current Status: UP

ge-0/0/1.165 → ge-0/0/1.2
(IXIA-Hub)
Type: Overlay
Weight: 787
Current Status: UP

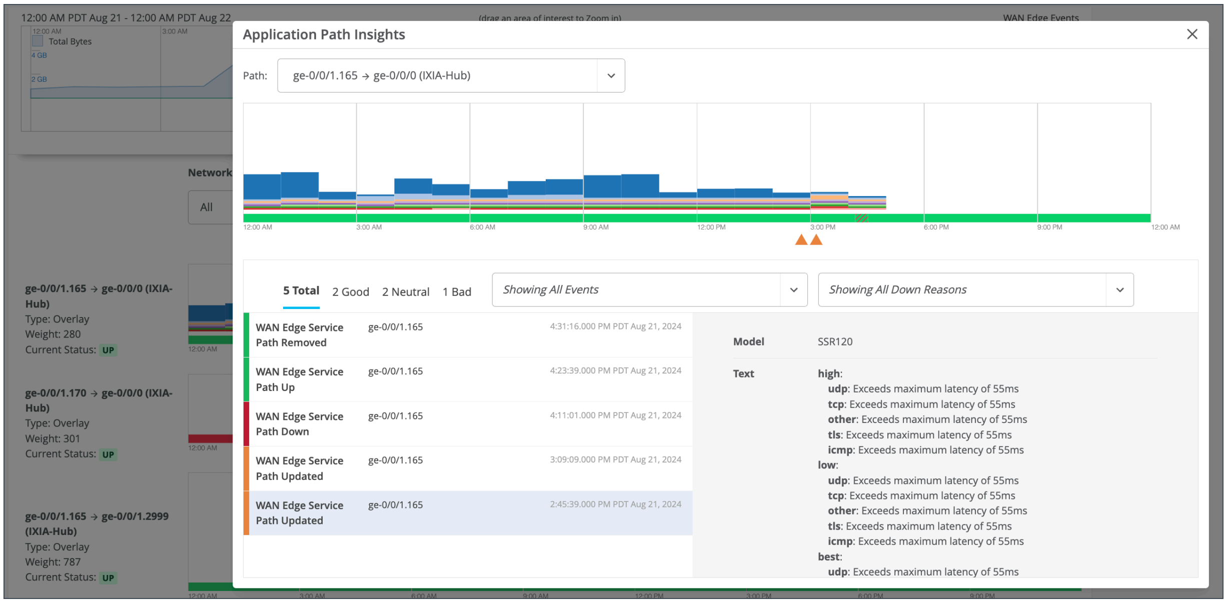
ge-0/0/1.175 → ge-0/0/1.2
(IXIA-Hub)
Type: Overlay
Weight: 799
Current Status: UP

ge-0/0/0 → ge-0/0/1.2999 (IXIA-Hub)
Type: Overlay
Weight: 801
Current Status: UP

ge-0/0/0 → ge-0/0/0 (IXIA-Hub)
Type: Overlay
Weight: 803
Current Status: UP

ge-0/0/1.170 → ge-0/0/1.2999

Figure 489: Path State Events and Reasons - Example 2



Application Path Insights

Path: ge-0/0/1.165 → ge-0/0/0 (IXIA-Hub)

5 Total 2 Good 2 Neutral 1 Bad

Showing All Events

Showing All Down Reasons

Event	Interface	Time
WAN Edge Service Path Removed	ge-0/0/1.165	4:31:16.000 PM PDT Aug 21, 2024
WAN Edge Service Path Up	ge-0/0/1.165	4:23:39.000 PM PDT Aug 21, 2024
WAN Edge Service Path Down	ge-0/0/1.165	4:11:01.000 PM PDT Aug 21, 2024
WAN Edge Service Path Updated	ge-0/0/1.165	3:09:09.000 PM PDT Aug 21, 2024
WAN Edge Service Path Updated	ge-0/0/1.165	2:45:39.000 PM PDT Aug 21, 2024

Model SSR120

Text
high:
- **udp**: Exceeds maximum latency of 55ms
- **tcp**: Exceeds maximum latency of 55ms
- **other**: Exceeds maximum latency of 55ms
- **tls**: Exceeds maximum latency of 55ms
- **icmp**: Exceeds maximum latency of 55ms

low:
- **udp**: Exceeds maximum latency of 55ms
- **tcp**: Exceeds maximum latency of 55ms
- **other**: Exceeds maximum latency of 55ms
- **tls**: Exceeds maximum latency of 55ms
- **icmp**: Exceeds maximum latency of 55ms

best:
- **udp**: Exceeds maximum latency of 55ms

ge-0/0/1.165 → ge-0/0/0 (IXIA-Hub)
Type: Overlay
Weight: 280
Current Status: UP

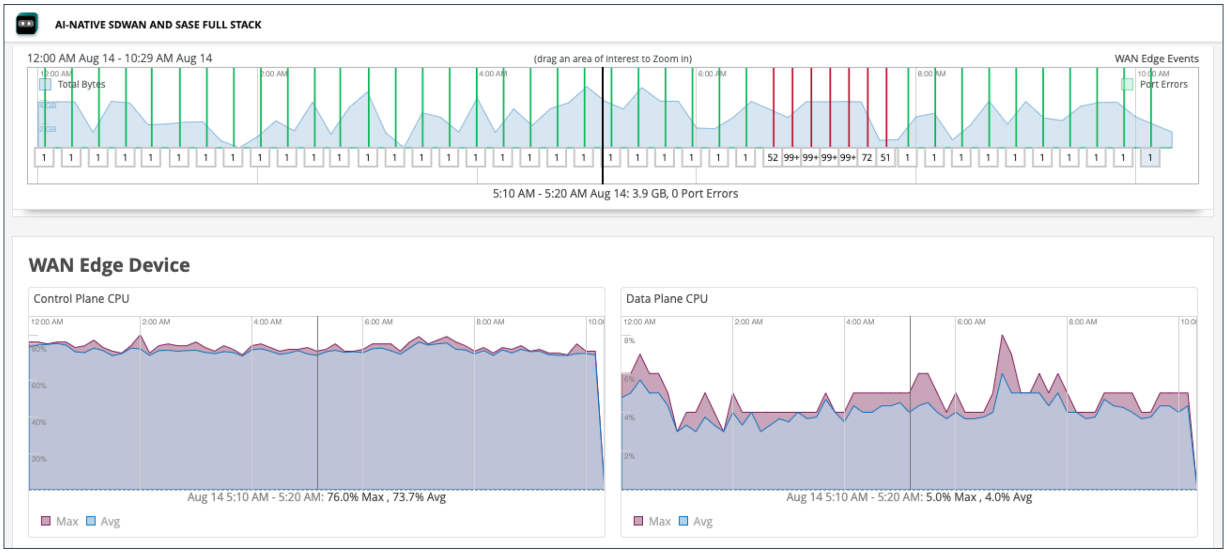
ge-0/0/1.170 → ge-0/0/0 (IXIA-Hub)
Type: Overlay
Weight: 301
Current Status: UP

ge-0/0/1.165 → ge-0/0/1.2999 (IXIA-Hub)
Type: Overlay
Weight: 787
Current Status: UP

WAN Edge Device charts include Control Plane CPU, Data Plane CPU, and Memory Utilization.

Control Plane CPU shows CPU utilization for both max and average. The Data Plane CPU chart displays the CPU utilization for both max and average.

Figure 490: Control Plane CPU and Data Plane CPU



AI-NATIVE SDWAN AND SASE FULL STACK

12:00 AM Aug 14 - 10:29 AM Aug 14

5:10 AM - 5:20 AM Aug 14: 3.9 GB, 0 Port Errors

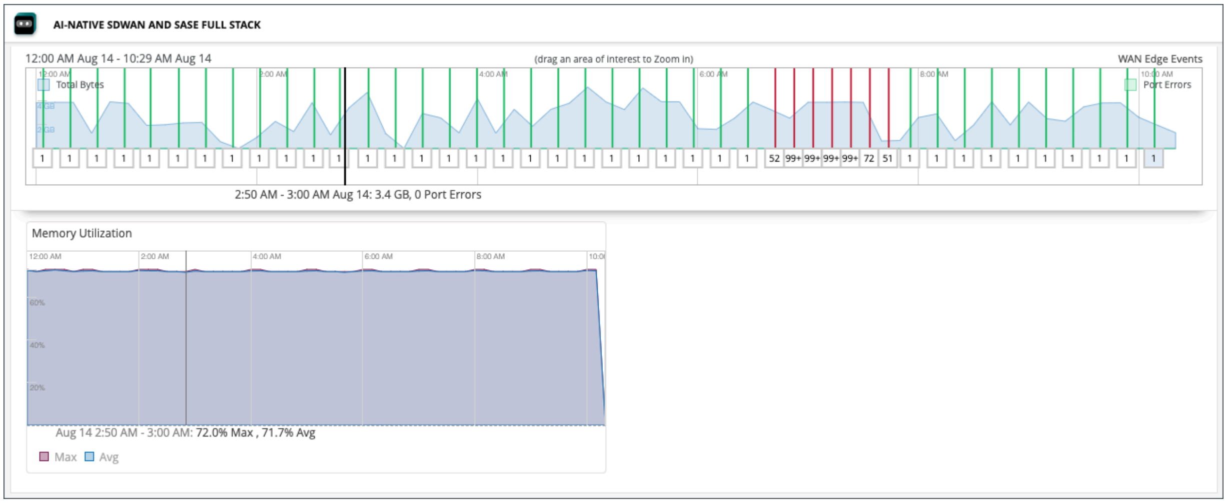
WAN Edge Device

Aug 14 5:10 AM - 5:20 AM: 76.0% Max , 73.7% Avg

Aug 14 5:10 AM - 5:20 AM: 5.0% Max , 4.0% Avg

Memory Utilization displays the max and average memory utilization.

Figure 491: Memory Utilization


AI-NATIVE SDWAN AND SASE FULL STACK
12:00 AM Aug 14 - 10:29 AM Aug 14
(drag an area of interest to Zoom in)
WAN Edge Events
12:00 AM
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
Total Bytes
Port Errors
52
99+
99+
99+
99+
72
51
2:50 AM - 3:00 AM Aug 14: 3.4 GB, 0 Port Errors
Memory Utilization
60%
40%
20%
Aug 14 2:50 AM - 3:00 AM: 72.0% Max , 71.7% Avg
Max
Avg

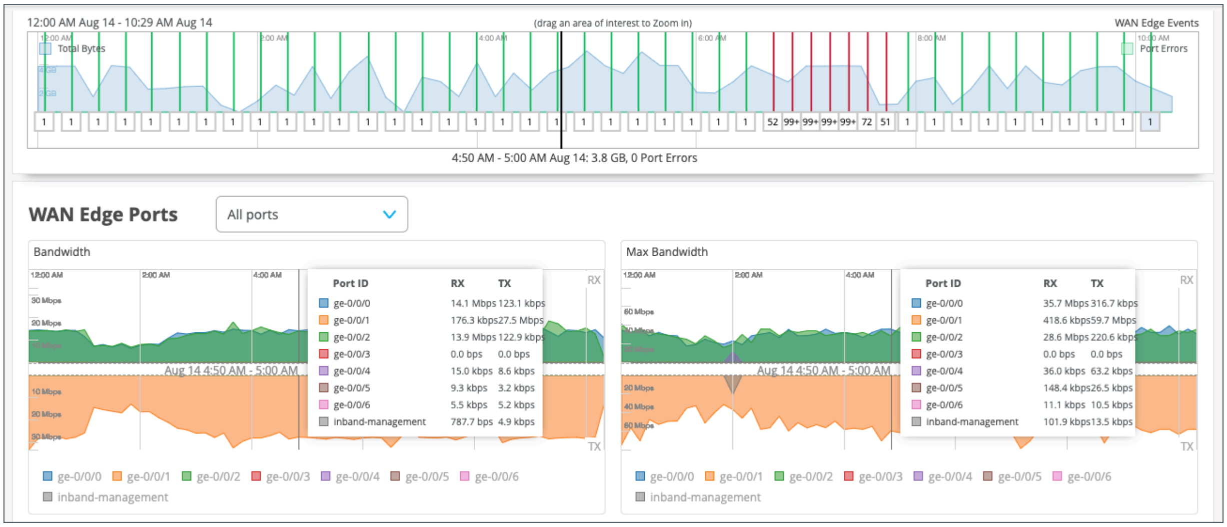
WAN Edge Ports charts

The **WAN Edge Ports** charts include Bandwidth, Max Bandwidth, Applications TX + RX Bytes, and Port Errors. From the drop down list at the top, you can select All ports to see utilization metrics in the charts for all interfaces, or you can select an interface to see the utilization metrics for that particular interface.

In the **Bandwidth** chart, you will see the bandwidth utilization metrics in megabits per second (Mbps) for that particular interface.

The **Max Bandwidth** chart displays insights into the highest point of link utilization recorded for received power signal (RX) and transmitted power signal (TX) packets on each port during the day. The data is shown in Mbps.

Figure 492: Bandwidth and Max Bandwidth



Port ID	RX	TX
ge-0/0/0	14.1 Mbps	123.1 kbps
ge-0/0/1	176.3 kbps	27.5 Mbps
ge-0/0/2	13.9 Mbps	122.9 kbps
ge-0/0/3	0.0 bps	0.0 bps
ge-0/0/4	15.0 kbps	8.6 kbps
ge-0/0/5	9.3 kbps	3.2 kbps
ge-0/0/6	5.5 kbps	5.2 kbps
inband-management	787.7 bps	4.9 kbps

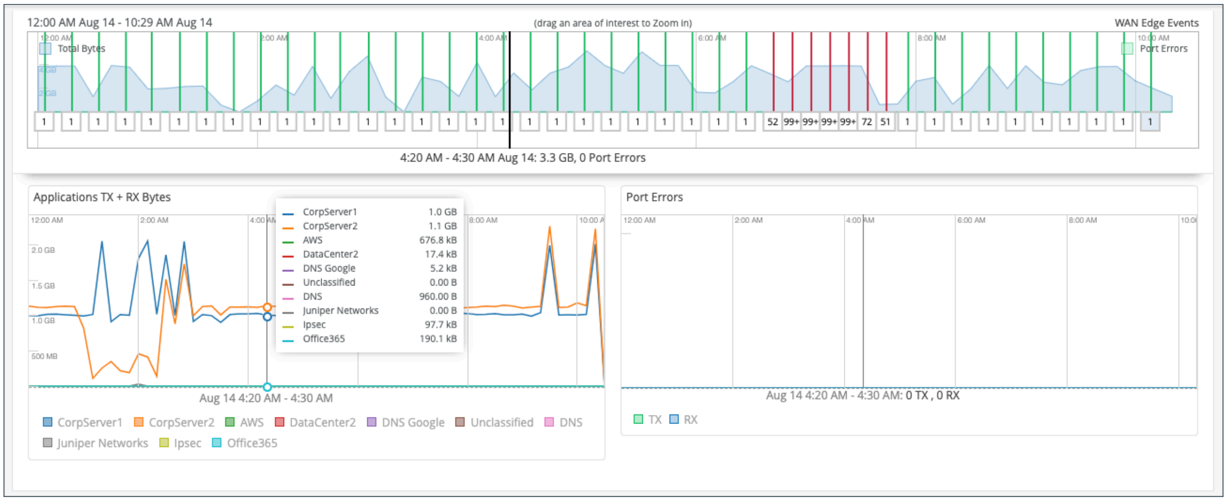
Port ID	RX	TX
ge-0/0/0	35.7 Mbps	316.7 kbps
ge-0/0/1	418.6 kbps	59.7 Mbps
ge-0/0/2	28.6 Mbps	220.6 kbps
ge-0/0/3	0.0 bps	0.0 bps
ge-0/0/4	36.0 kbps	63.2 kbps
ge-0/0/5	148.4 kbps	26.5 kbps
ge-0/0/6	11.1 kbps	10.5 kbps
inband-management	101.9 kbps	13.5 kbps

In the last two WAN Edge Ports charts, you'll find **Applications TX + RX Bytes** and **Port Errors**. Hover over the charts to find out more information.

The **Applications TX + RX Bytes** chart outlines transmit and receive data information, which can be isolated at an application level by clicking on the application name at the bottom of the chart to see Client, MAC address, IP address, device type, and bytes for bandwidth utilization.

The **Port Errors** chart displays port errors for receive and transmit packets throughout the day.

Figure 493: Applications TX + RX Bytes and Port Errors



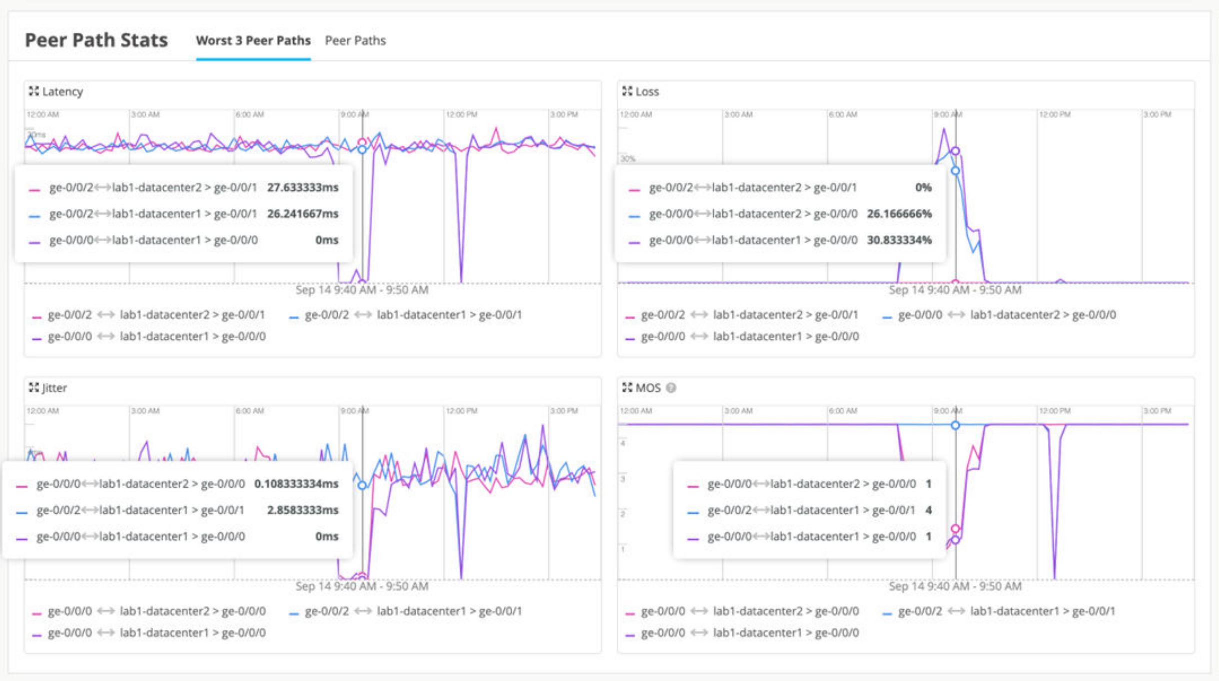
CorpServer1	1.0 GB
CorpServer2	1.1 GB
AWS	676.8 kB
DataCenter2	17.4 kB
DNS Google	5.2 kB
Unclassified	0.00 B
DNS	960.00 B
Juniper Networks	0.00 B
Ipsec	97.7 kB
Office365	190.1 kB

Peer Path Statistics

The Session Smart WAN edge devices deployed in Juniper Mist™ WAN Assurance provide insights for liveness and path quality through Session Smart, Secure Vector Routing. The Session Smart use of the Bidirectional Forwarding Detection (BFD) signal on port 1280 checks with the downstream Session Smart Routers for liveness and monitors jitter, latency, loss, and mean opinion score (MOS). This insight works only with our Session Smart devices.

We return to WAN Edge Insights to find the Session Smart Peering metrics on your Mist dashboard. These graphs are at the bottom of the page, with a default view showing the worst three peer connections: jitter, latency, loss, and MOS. Drill down into the data here, using the same time ranges for the WAN Edge Charts. This also means that the graphs are interrelated and cross referenced.

Figure 494: Peer Path Statistics


Peer Path Stats
Worst 3 Peer Paths
Peer Paths
Latency
12:00 AM
3:00 AM
6:00 AM
9:00 AM
12:00 PM
3:00 PM
30ms
Sep 14 9:40 AM - 9:50 AM
ge-0/0/2 ↔ lab1-datacenter2 > ge-0/0/1
ge-0/0/2 ↔ lab1-datacenter1 > ge-0/0/1
ge-0/0/0 ↔ lab1-datacenter1 > ge-0/0/0
Loss
30%
ge-0/0/2 ↔ lab1-datacenter2 > ge-0/0/1
ge-0/0/0 ↔ lab1-datacenter2 > ge-0/0/0
ge-0/0/0 ↔ lab1-datacenter1 > ge-0/0/0
Jitter
ge-0/0/0 ↔ lab1-datacenter2 > ge-0/0/0
ge-0/0/2 ↔ lab1-datacenter1 > ge-0/0/1
ge-0/0/0 ↔ lab1-datacenter1 > ge-0/0/0
MOS
4
3
2
1
ge-0/0/0 ↔ lab1-datacenter2 > ge-0/0/0
ge-0/0/2 ↔ lab1-datacenter1 > ge-0/0/1
ge-0/0/0 ↔ lab1-datacenter1 > ge-0/0/0

Latency

- ge-0/0/2↔lab1-datacenter2 > ge-0/0/1 **27.633333ms**
- ge-0/0/2↔lab1-datacenter1 > ge-0/0/1 **26.241667ms**
- ge-0/0/0↔lab1-datacenter1 > ge-0/0/0 **0ms**

Loss

- ge-0/0/2↔lab1-datacenter2 > ge-0/0/1 **0%**
- ge-0/0/0↔lab1-datacenter2 > ge-0/0/0 **26.166666%**
- ge-0/0/0↔lab1-datacenter1 > ge-0/0/0 **30.833334%**

Jitter

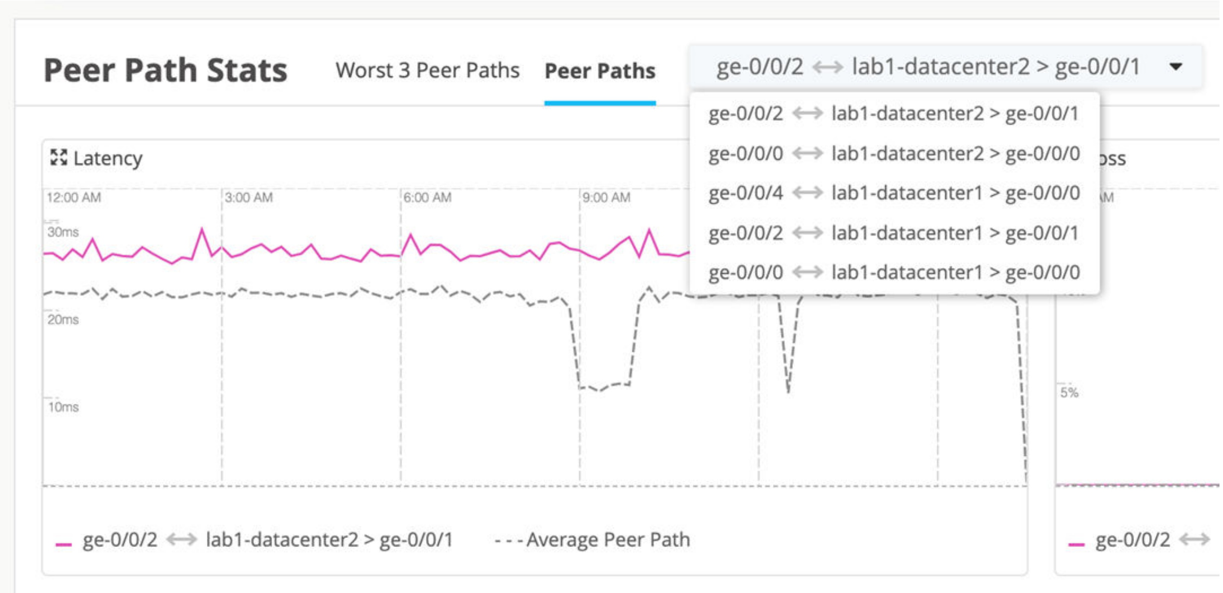
- ge-0/0/0↔lab1-datacenter2 > ge-0/0/0 **0.108333334ms**
- ge-0/0/2↔lab1-datacenter1 > ge-0/0/1 **2.8583333ms**
- ge-0/0/0↔lab1-datacenter1 > ge-0/0/0 **0ms**

MOS

- ge-0/0/0↔lab1-datacenter2 > ge-0/0/0 **1**
- ge-0/0/2↔lab1-datacenter1 > ge-0/0/1 **4**
- ge-0/0/0↔lab1-datacenter1 > ge-0/0/0 **1**

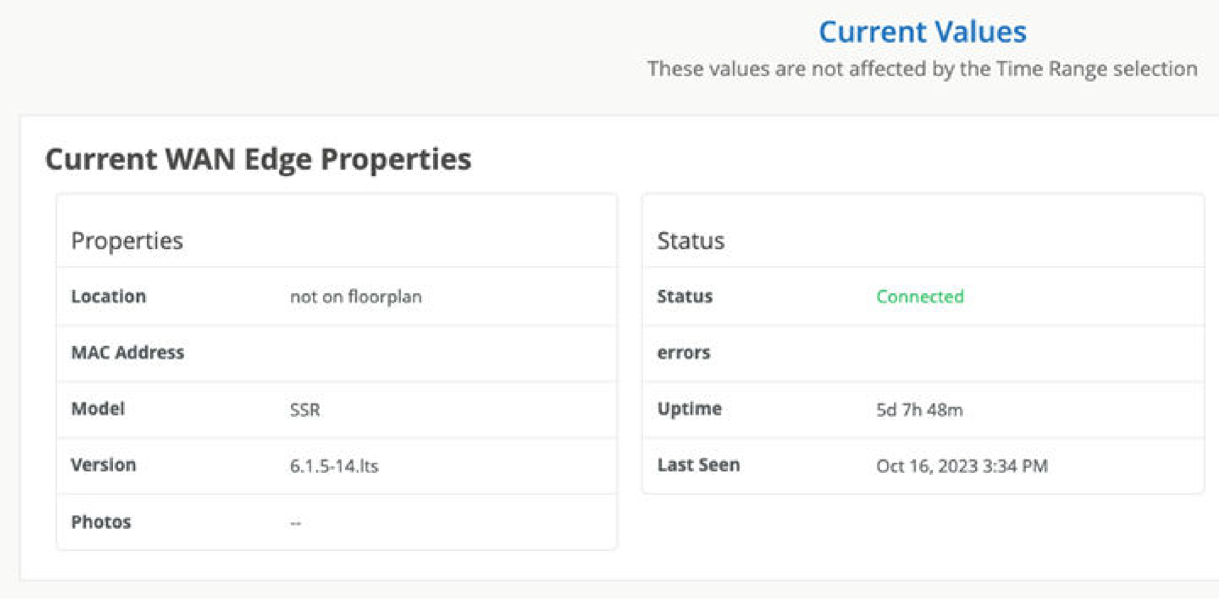
You can also drill down and select a specific peer path to view statistics.

Figure 495: Peer Path Statistics for Specific Peer


Peer Path Stats
Worst 3 Peer Paths
Peer Paths
ge-0/0/2 ⟷ lab1-datacenter2 > ge-0/0/1
ge-0/0/2 ⟷ lab1-datacenter2 > ge-0/0/1
ge-0/0/0 ⟷ lab1-datacenter2 > ge-0/0/0
ge-0/0/4 ⟷ lab1-datacenter1 > ge-0/0/0
ge-0/0/2 ⟷ lab1-datacenter1 > ge-0/0/1
ge-0/0/0 ⟷ lab1-datacenter1 > ge-0/0/0
Latency
12:00 AM
3:00 AM
6:00 AM
9:00 AM
30ms
20ms
10ms
oss
5%
ge-0/0/2 ⟷ lab1-datacenter2 > ge-0/0/1
- - - Average Peer Path
ge-0/0/2 ⟷

The final information on your WAN Edge Insights page is Current WAN Edge Properties. Time range selections do not impact information in the Current Values pane.

Figure 496: Current WAN Edge Properties



Current Values

These values are not affected by the Time Range selection

Current WAN Edge Properties

Properties	
Location	not on floorplan
MAC Address	
Model	SSR
Version	6.1.5-14.lts
Photos	--

Status	
Status	Connected
errors	
Uptime	5d 7h 48m
Last Seen	Oct 16, 2023 3:34 PM

Alerts for Interfaces Status

In Juniper Mist, alerts present network and device issues that are ongoing. You can view alerts on Juniper Mist portal by selecting Monitor > Alerts.

You can set up alerts and email updates for when certain ports on a WAN Edge device go online or offline. To configure alerts for specific ports, you need to label these ports in LAN or WAN settings of WAN Edge device.

To configure the alerts and notifications for specific port, you must:

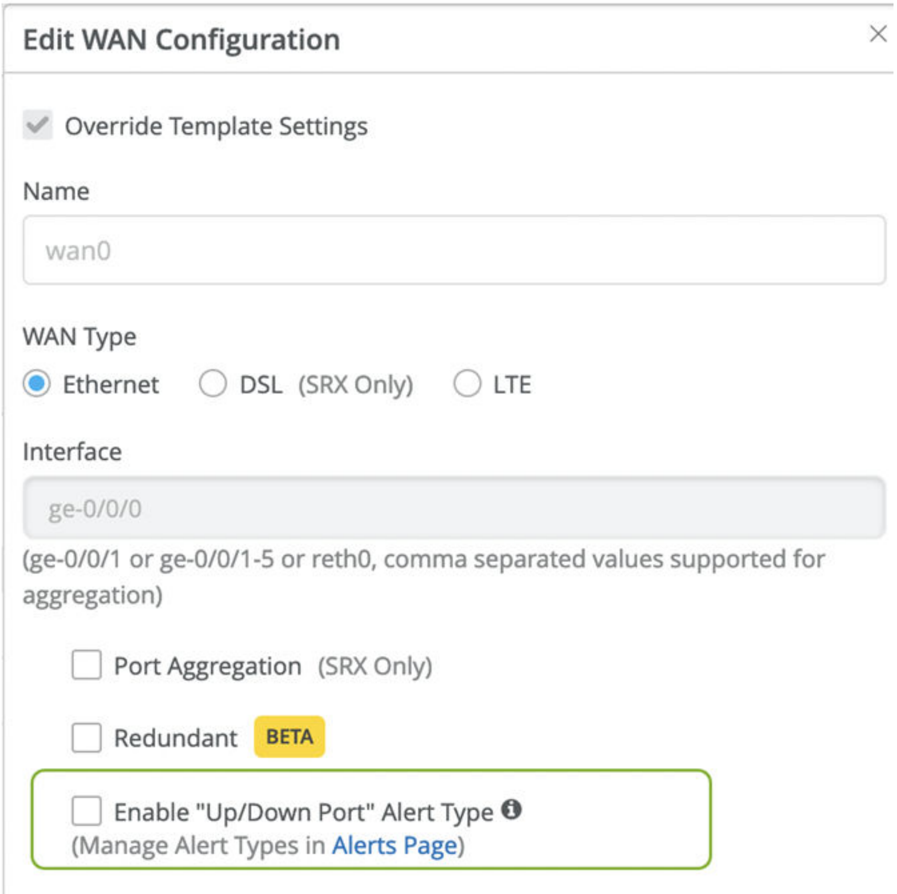
- Change the WAN or LAN settings to label the specified ports in WAN Edge template or at device-level configuration page.

  1. In the Juniper Mist cloud portal, select **Organization > WAN > WAN Edge Templates** and select the WAN or LAN configuration that you want to update. (Or add a new configuration.)

     To configure at the device-level, select **WAN Edges** on the left-navigation bar and select WAN or LAN configuration of the selected device.

  2. Under Interface, enter the port or ports, and then select **Enable “Up/Down Port” Alert Type** check-box.

Figure 497: Marking LAN Port or WAN Interface as Critical Interface



Edit WAN Configuration

☑ Override Template Settings

Name

wan0

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 supported for aggregation)

□ Port Aggregation (SRX Only)

□ Redundant BETA

□ Enable "Up/Down Port" Alert Type ℹ
(Manage Alert Types in Alerts Page)

Repeat these steps for all critical ports.

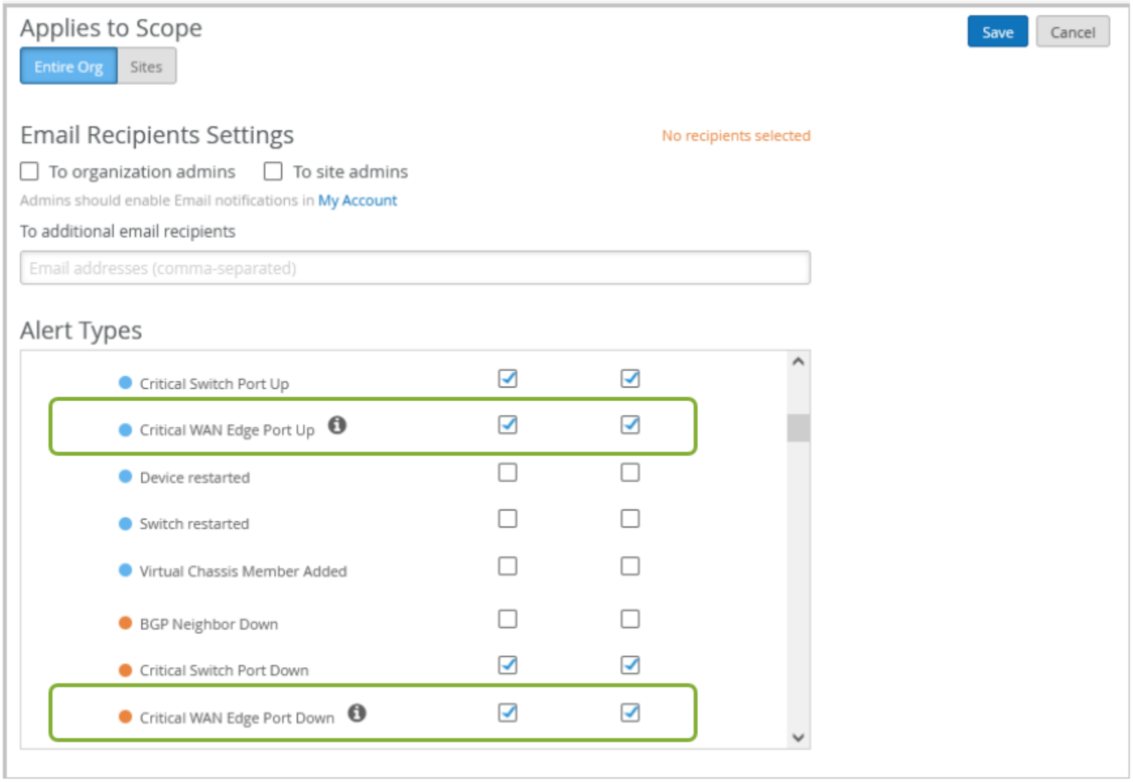
- Configure alerts and e-mail notifications for the specified ports in Alerts page.

  1. Go to **Monitor** > **Alerts** > **Alerts Configuration** and use the following check-boxes to enable alerts for the selected port:

     - Critical WAN Edge Port Up

     - Critical WAN Edge Port Down

Figure 498: Alerts Configuration for Critical Ports



Applies to Scope

Entire Org | Sites

Save | Cancel

Email Recipients Settings

No recipients selected

□ To organization admins □ To site admins

Admins should enable Email notifications in My Account

To additional email recipients

Email addresses (comma-separated)

Alert Types

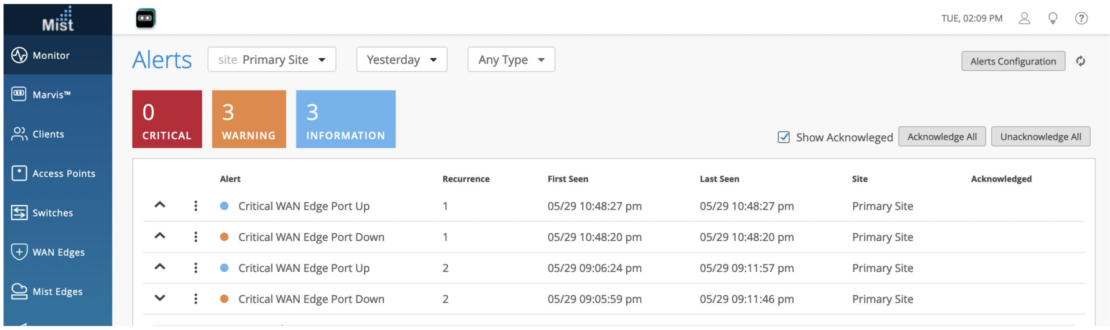
Alert		
● Critical Switch Port Up	☑	☑
● Critical WAN Edge Port Up	☑	☑
● Device restarted	□	□
● Switch restarted	□	□
● Virtual Chassis Member Added	□	□
● BGP Neighbor Down	□	□
● Critical Switch Port Down	☑	☑
● Critical WAN Edge Port Down	☑	☑

See Alert Configuration for details.

When you enable alerts and notifications:

- You'll receive an e-mail notification whenever a port transitions from one state to another.
- You can view the status in Monitor > Alerts page. Figure 499 on page 603 shows an example of the critical port status on Juniper Mist Alerts dashboard.

Figure 499: Critical WAN Edge Port Status



Alerts

site Primary Site | Yesterday | Any Type | Alerts Configuration

0 CRITICAL | 3 WARNING | 3 INFORMATION

☑ Show Acknowleged | Acknowledge All | Unacknowledge All

Alert	Recurrence	First Seen	Last Seen	Site	Acknowledged
● Critical WAN Edge Port Up	1	05/29 10:48:27 pm	05/29 10:48:27 pm	Primary Site	
● Critical WAN Edge Port Down	1	05/29 10:48:20 pm	05/29 10:48:20 pm	Primary Site	
● Critical WAN Edge Port Up	2	05/29 09:06:24 pm	05/29 09:11:57 pm	Primary Site	
● Critical WAN Edge Port Down	2	05/29 09:05:59 pm	05/29 09:11:46 pm	Primary Site	

Service-Level Experiences for Session Smart Router Deployed as WAN Edge

IN THIS SECTION

Get familiar with Service Level Expectations (SLEs) for Juniper® Session Smart™ Routers deployed as WAN edge device and learn more efficient ways to monitor your WAN edge device in the Juniper Mist™ portal using SLE insights.

WAN Edge SLEs

The Juniper SD-WAN driven by Mist AI WAN Assurance solution simplifies the way you monitor your WAN edge. Session Smart™ and SRX Series WAN edge devices have unique implementations for tracking metrics for WAN Edge health, WAN link health, and application health to derive percentage ratings, which Juniper calls user minutes. User-minute metrics inform the basis for Mist monitoring and Juniper service-level experiences (SLEs). Using critical metrics on application response times, WAN link status, gateway health, and other network conditions, both the SRX Series and Session Smart WAN edge devices gain insights into how these metrics impact end-user experiences and use them to identify the root causes of any service degradation. You can find an overview of all Mist SLEs here: No Link Title.

In this troubleshooting section of the configuration guide, you'll discover SLEs specific to your WAN edge.

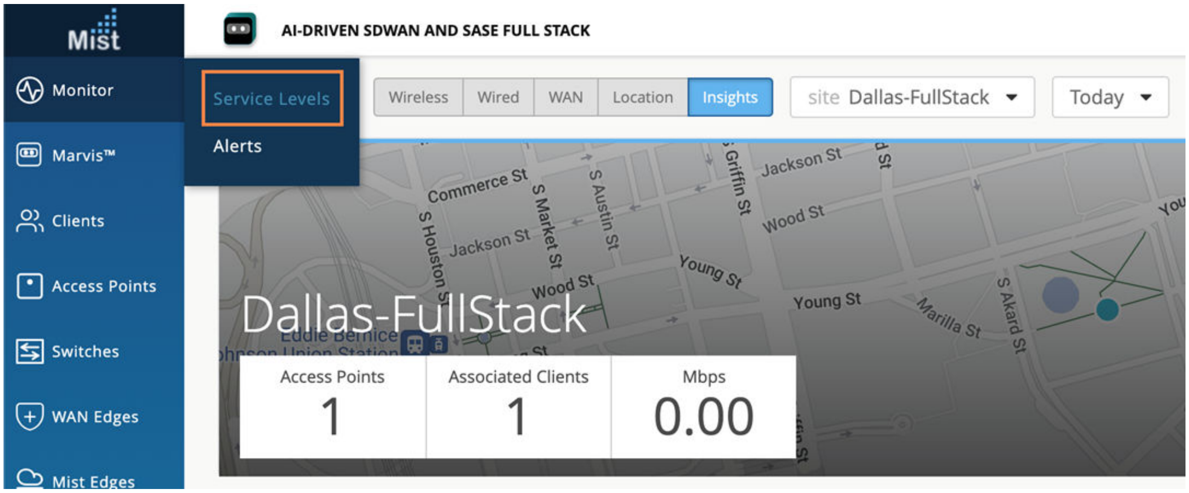
Session Smart WAN Edge SLEs

IN THIS SECTION

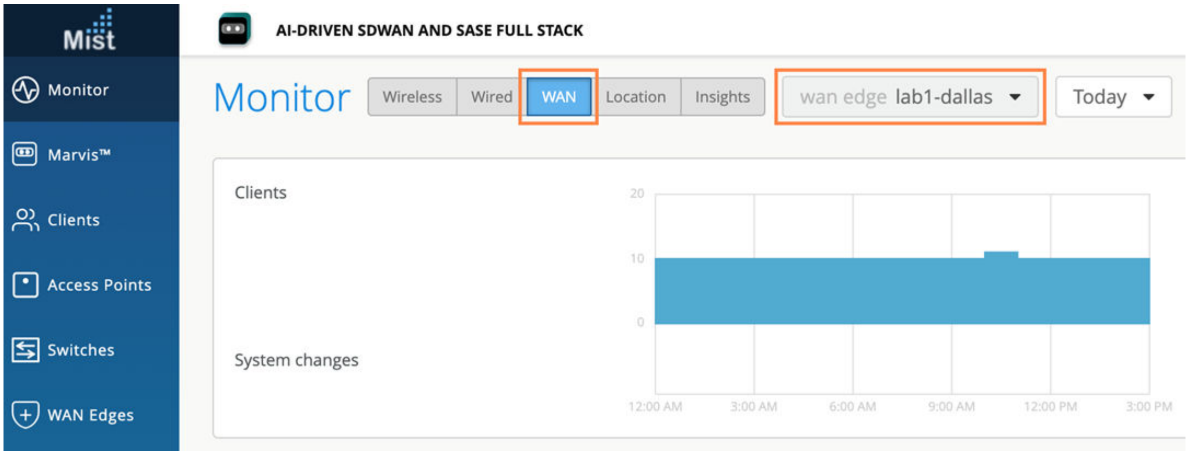
Read the Session Smart WAN Edge SLE guide to learn how to use the Juniper Mist dashboard to efficiently diagnose device and WAN connectivity issues following your initial deployment phase. Let's first focus on WAN edge service-level expectations (SLEs).

Starting at the Juniper Mist dashboard, navigate to Monitor > Service Levels.

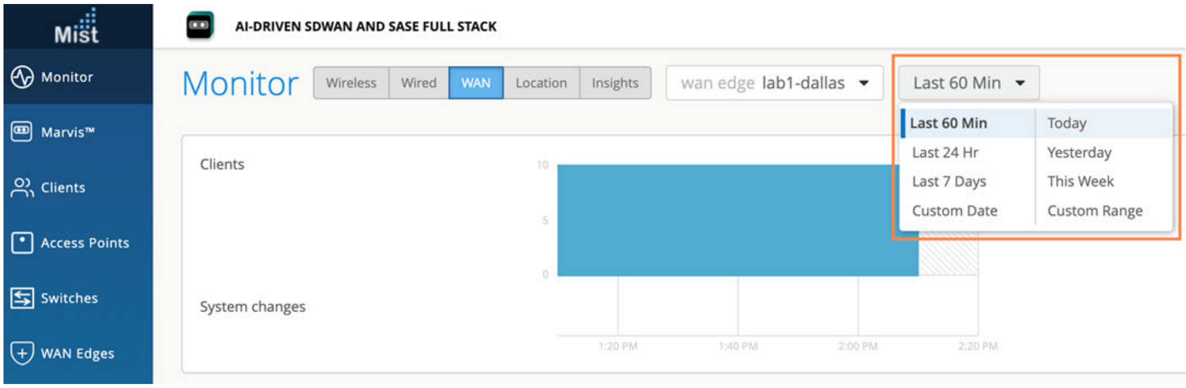
1. Select **Monitor** > **Service Levels** from the Juniper Mist dashboard.



2. From the site list, select a WAN Edge you want to inspect SLEs for. In this example, select Dallas-Fullstack.

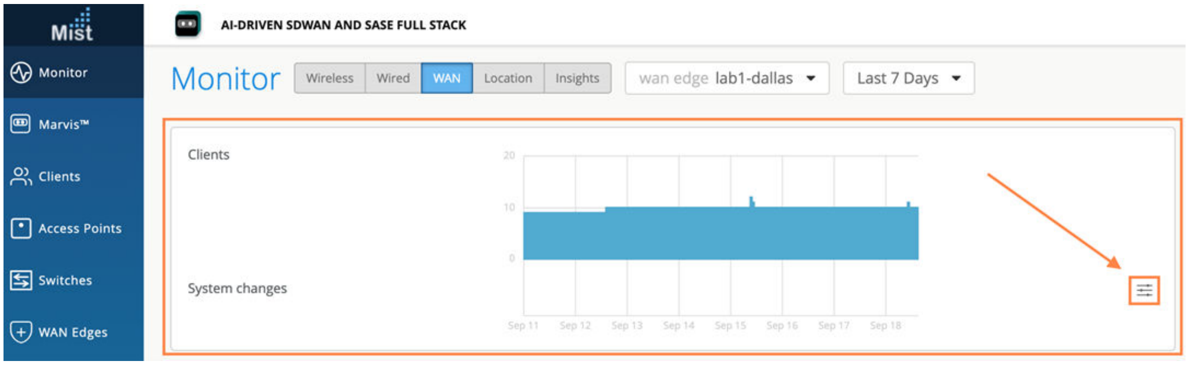


3. Click the WAN tab and select the WAN edge you want to investigate. For example, lab1-dallas.

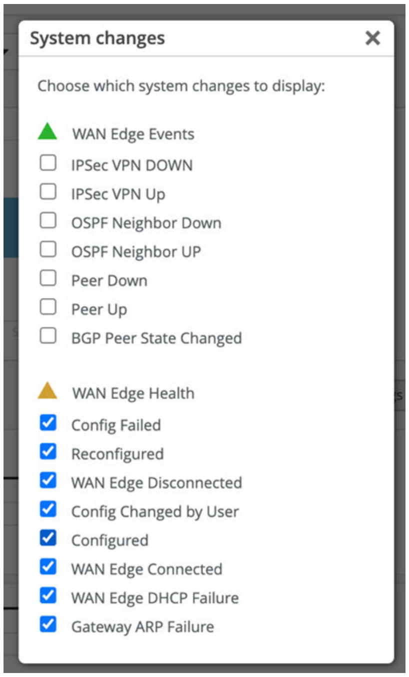


NOTE:
Monitor

The first infographic on your WAN SLE page displays the relationship.



4. Click the toolbox icon to select from a menu in which system changes are displayed.



System changes ✕

Choose which system changes to display:

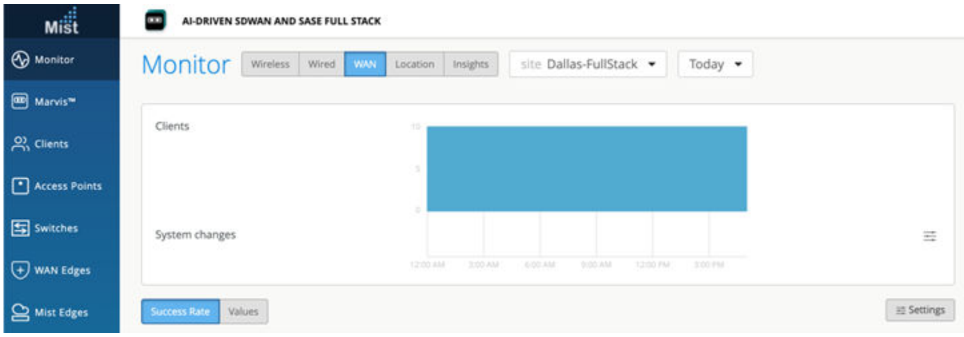
▲ WAN Edge Events

☐ IPSec VPN DOWN
☐ IPSec VPN Up
☐ OSPF Neighbor Down
☐ OSPF Neighbor UP
☐ Peer Down
☐ Peer Up
☐ BGP Peer State Changed

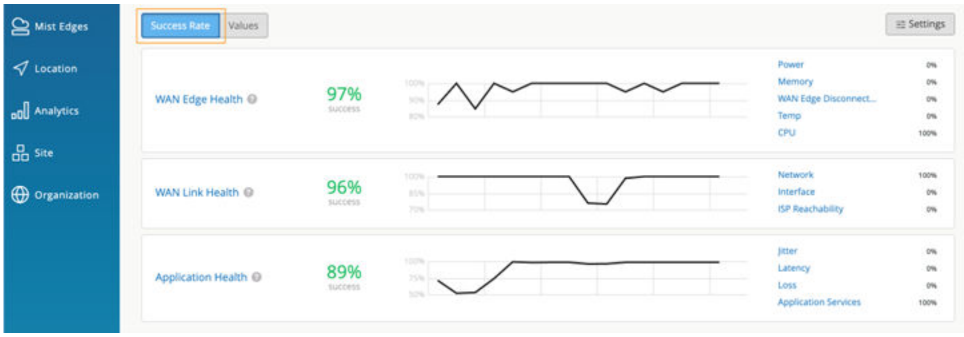
▲ WAN Edge Health

☑ Config Failed
☑ Reconfigured
☑ WAN Edge Disconnected
☑ Config Changed by User
☑ Configured
☑ WAN Edge Connected
☑ WAN Edge DHCP Failure
☑ Gateway ARP Failure

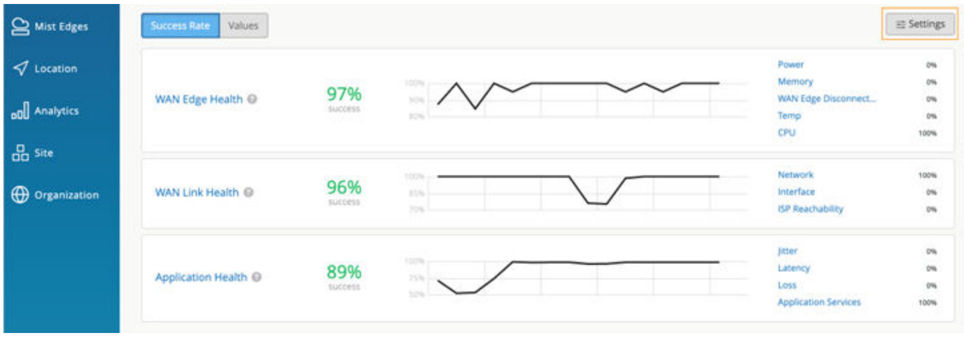
Your WAN edge SLEs are displayed in the SLE Success Rate default view.



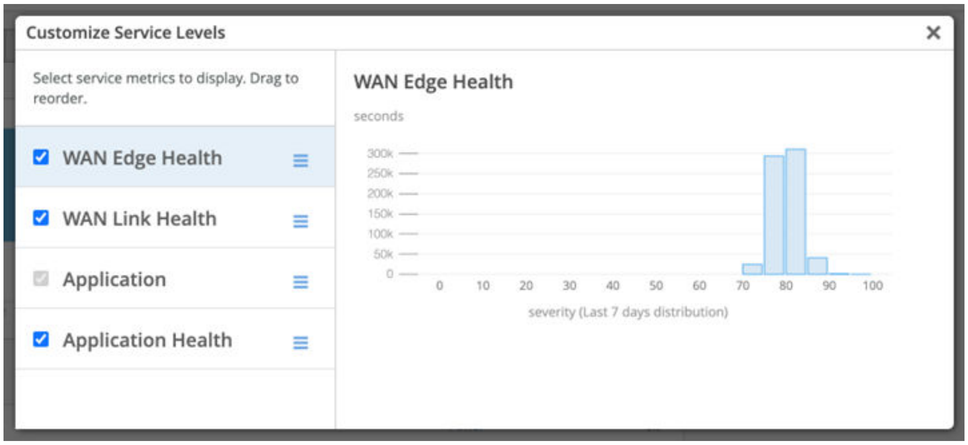
Select a site to inspect and select the WAN **edge** you're investigating. In this example, we're looking at the lab1-dallas WAN edge. The first infographic on your WAN SLE page displays the relationship between collected clients at a point in time and system events that occurred during that same window. The SLE Success Rate default view is just beneath the client insights on your WAN SLE page.



You can also toggle the view to **Values** for a numerical display of SLE metrics. It's important to familiarize yourself with the **Settings** button.



NOTE: There's little customization to this dialog box for **Settings** on the Session Smart Router. The Secure Vector Routing protocol measures these values automatically based on metadata exchanged. You do need SLE Application probes set on SRX Series devices.



Customize Service Levels

Select service metrics to display. Drag to reorder.

☑ WAN Edge Health
☑ WAN Link Health
☐ Application
☑ Application Health

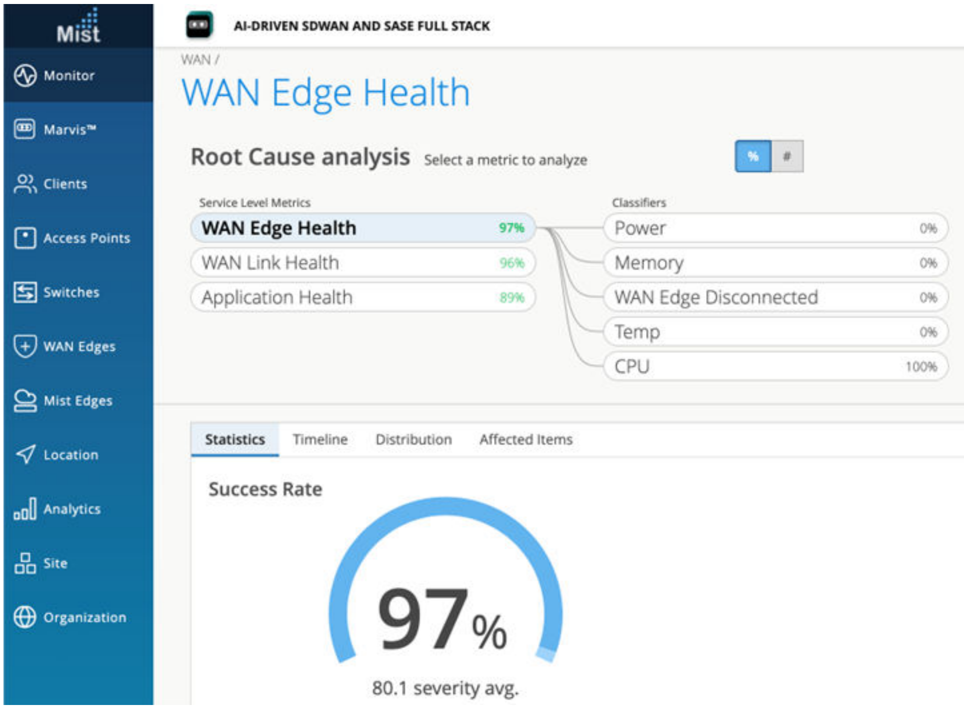
WAN Edge SLEs

For these SLEs, note that the system works to reduce the need for administrators to watch for anomalies. Instead, Juniper(r) Mist WAN Assurance defines threshold levels after which the administrator is notified. This approach contrasts with traditional models where the system administrator would define these values based on a curve or pattern observed.

Our First WAN SLE is WAN Edge Health

WAN Edge Health

The WAN Edge Health SLE provides platform metrics that comprise the root cause analysis for the Service Level metric, including power, CPU and memory utilization, WAN Edge disconnects, and platform temperature.



Service Level Metrics	
WAN Edge Health	97%
WAN Link Health	96%
Application Health	89%

Classifiers	
Power	0%
Memory	0%
WAN Edge Disconnected	0%
Temp	0%
CPU	100%

Success Rate

97%

80.1 severity avg.

WAN Link Heath

Use the WAN Link Health SLE to know more about the interfaces and where or to which devices they connect.

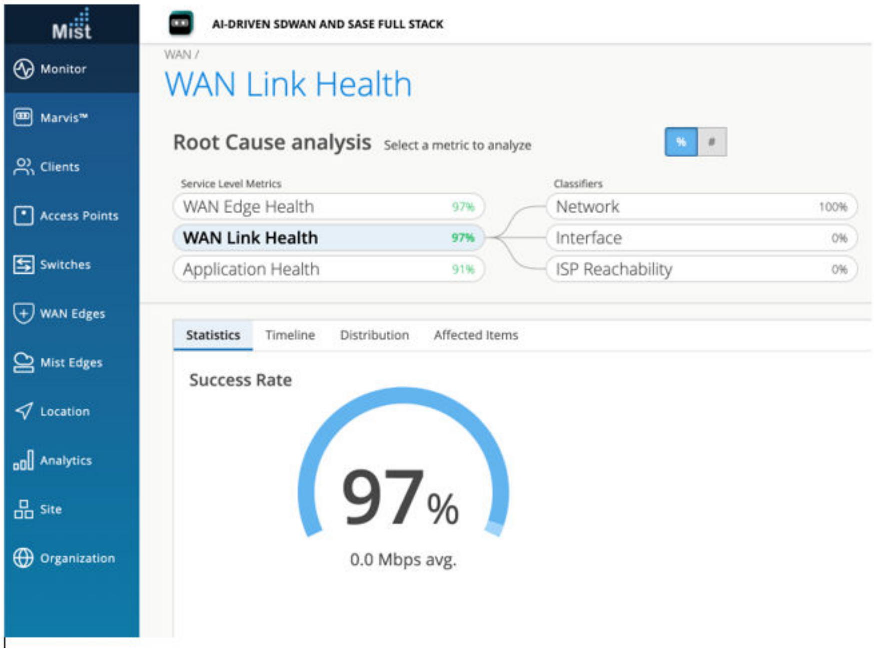
The next WAN SLE is WAN Link Health. Now, we're looking at information on your interfaces and where they connect. These metrics comprise the **Root Cause Analysis** for the **WAN Link Health** metric. Data for **WAN Link Health** comes from these classifiers:

- Network
  - The Session Smart WAN edge monitors **Jitter**, **Loss**, **Latency**, and Session Smart **Peer Path Down** status via **Secure Vector Routing**.
- Interface

  - The Interface category monitors your **LTE Signal** strength, **Cable Issues**, and **Congestion**.

- ISP Reachability

  - ISP Reachability comprises **ARP** and **DHCP** success.



WAN Link Health

Root Cause analysis Select a metric to analyze

Service Level Metrics		Classifiers	
WAN Edge Health	97%	Network	100%
WAN Link Health	97%	Interface	0%
Application Health	91%	ISP Reachability	0%

Success Rate

97%

0.0 Mbps avg.

Application Health

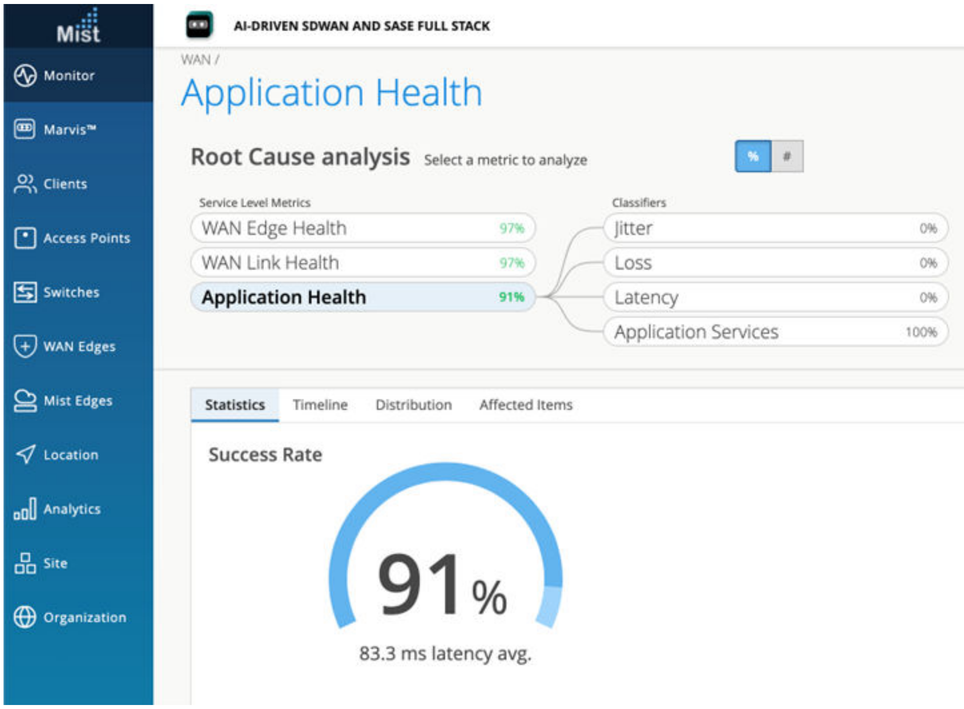
Your last WAN SLE is **Application Health**. Here's where it gets interesting. In this lab environment, **Application Health** has a 79% rating, which means applications hit the service expectations 79% of the time. Like the other values, you can dive into where and why the metrics in the **Root Cause Analysis** comprise a particular **Application Health** score with these classifiers:

- The amount of jitter that contributes to the Root Cause Analysis score.

- The amount of loss that contributes to the Root Cause Analysis score.

- The amount of latency that contributes to the Root Cause Analysis score.

- Failed application health contributes to the Application Services Root Cause Analysis score.



Service Level Metrics
WAN Edge Health 97%
WAN Link Health 97%
Application Health 91%

Classifiers
Jitter 0%
Loss 0%
Latency 0%
Application Services 100%

Success Rate
91%
83.3 ms latency avg.

Troubleshooting the Session Smart WAN Edge with SLE Insights

To troubleshoot the Session Smart WAN edge with SLE insights, select Monitor > Service Levels from the Juniper Mist dashboard, select **Monitor** > **Service Levels**.

Let's learn how to investigate the WAN edge SLEs. We'll dive into Application Health Monitoring for this troubleshooting guide to get detailed metrics. But each SLE menu—**WAN Edge Health**, **WAN Link Health**, and **Application Health**—displays similar tables and tabs related to the SLE. You'll often look at application health while troubleshooting.

NOTE: Remember that you don't need to define Application probes for Application SLEs on your Session Smart WAN edge like you do on an SRX Series device. However, you will need traffic that can be sampled and reported to the Juniper Mist cloud. Juniper Mist AI requires data for suggestions and decisions like any AI-based system. The **best practice** for this is to collect results from an entire week. However, you'll get the first data after 24 hours.

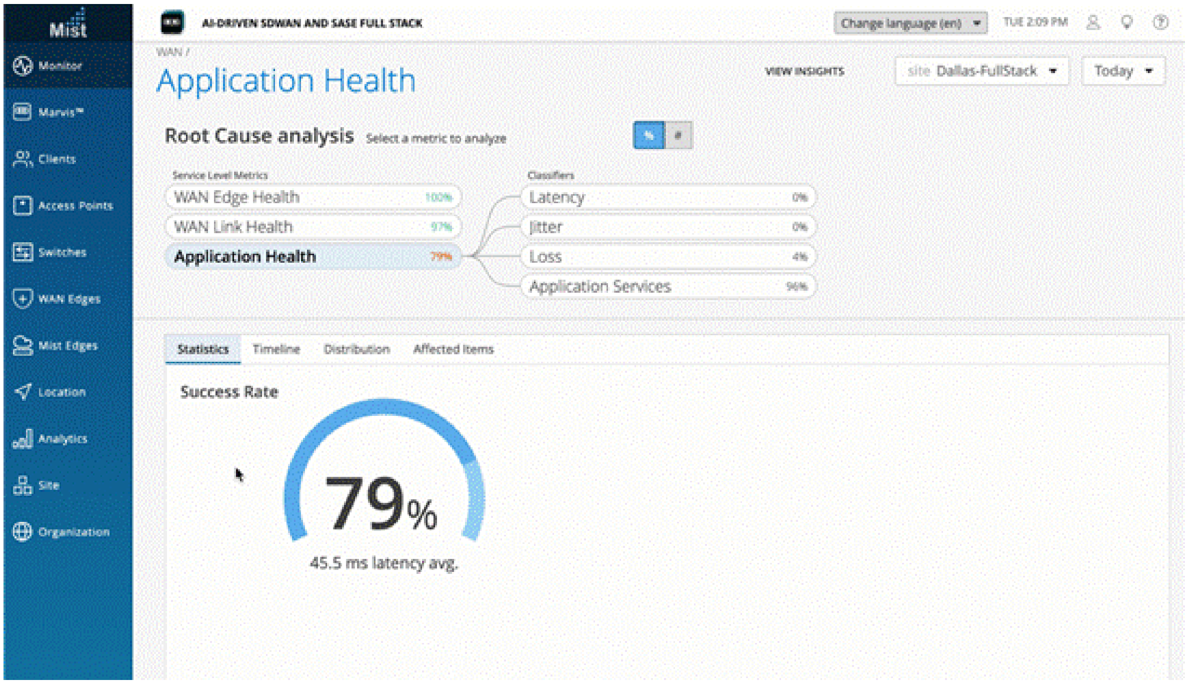
What does a generalized Success Rate of 91% for Application Health mean for your network? The **Application Health** pane reveals a percentage comprised of the Root Cause Analysis that includes all the previously mentioned classifiers (latency, jitter, loss, and application failures) for an overall percentage. When you dig into the menu below, you'll find a few tabs that give you deeper insights into the classifiers that didn't meet expectations.

- The **Statistics** tab on the Application Health pane displays the generalized percentage of all the classifiers.

- The **Timeline** tab is a chronological display of events comprising the classifiers, listing their failures, connected clients, and system changes. The time frame is influenced by the value at the top of the page, with options for **Today**, **Yesterday**, **TThis Week**, or a **Custom Range**. On the timeline, you can select a specific time, zoom in for details, or select a range. Hovering over a point in time will outline the classifier that failed to meet service expectations.

- The **Distribution** tab analyzes service-level failures by attribute and is sorted by the most disruptive attribute. You can drill down into categories of traffic classes, peer paths (those Session Smart connections between Session Smart Routers), physical interfaces, WAN edges, and zones. Note that WAN Assurance deployments with Session Smart WAN edge devices leverage the **peer path** information, while the SRX Series WAN edge leverage destination **zones** for deeper insights in the **Distribution** tab.

- The **Affected Items** tab categorizes the specific items that failed to meet service-level goals. Here, you'll find a numerical value for the applications, interfaces, clients, WAN edges, or categories that failed.



SEE ALSO

Monitor Session Smart Router Deployed as WAN Edge | 571

Troubleshoot Session Smart Router Deployed as WAN Edge | 613

Troubleshoot Session Smart Router Deployed as WAN Edge

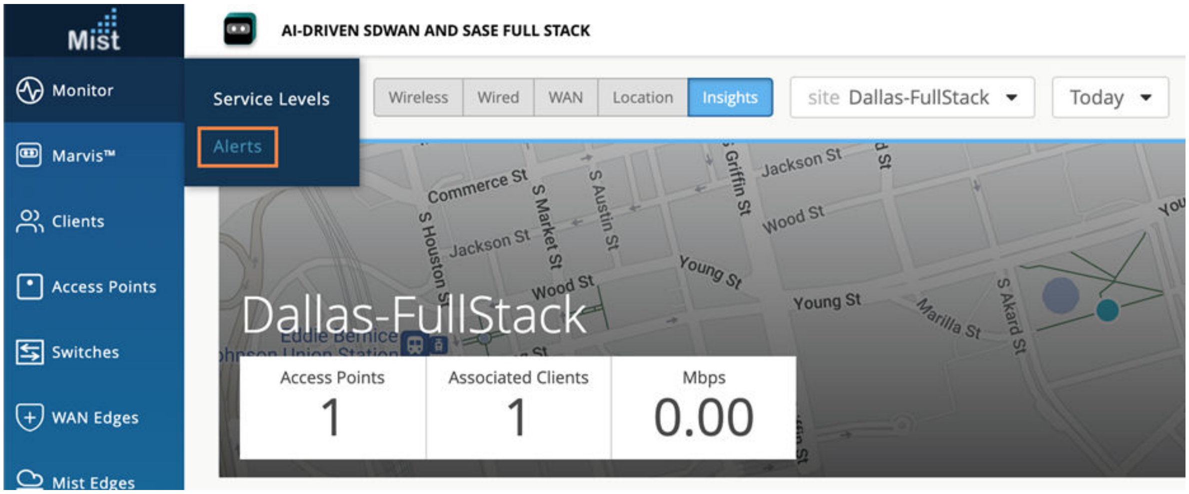
IN THIS SECTION

Discover efficient methods for troubleshooting your WAN edge device in the Juniper Mist™ portal after the initial deployment phase. This topic provides guidance for system administrators and technical support responsible for maintaining enterprise SD-WAN networks.

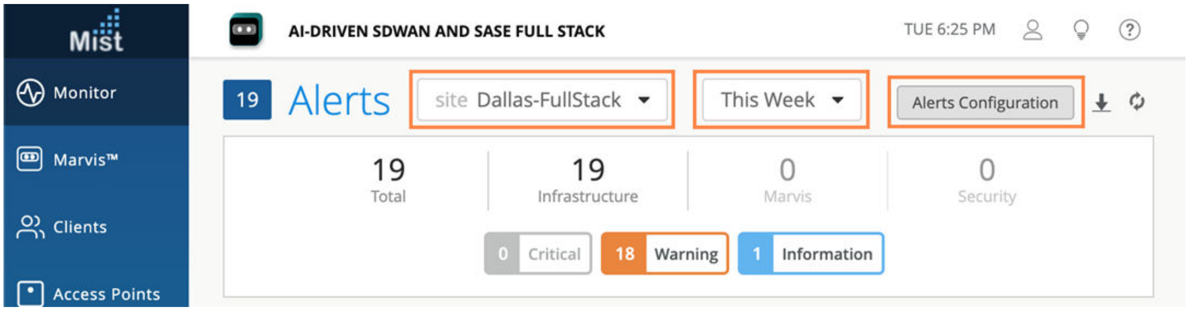
Troubleshooting Session Smart WAN Edge Alarms

In this section you'll configure WAN Edge alarms and e-mail alerts to the administrator.

1. From the Mist dashboard, select **Monitor** > **Alerts**.

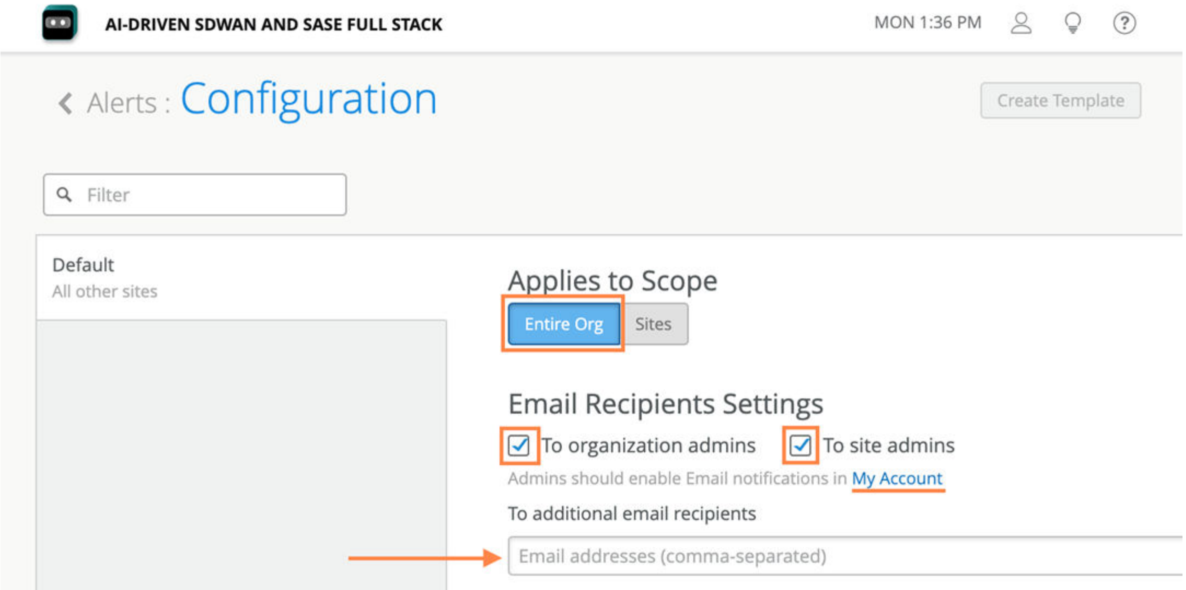


2. Filter the alarms for our lab Site, **Dallas-FullStack**.



3. Set the **Time Range** for **This Week** so we can see some Alerts. Next, we'll select the **Alerts Configuration** to set up e-mail notifications.

> **NOTE**: Under Alerts Configuration, it's best practice for **Applies to Scope** alerts to be set for the Entire Org (as shown in the screenshot below). You can also specify that alerts be sent to organization administrators and site administrators by selecting the relevant check boxes in the Email Recipient Settings section. Enter emails for additional recipients in the **To additional email recipients** field.



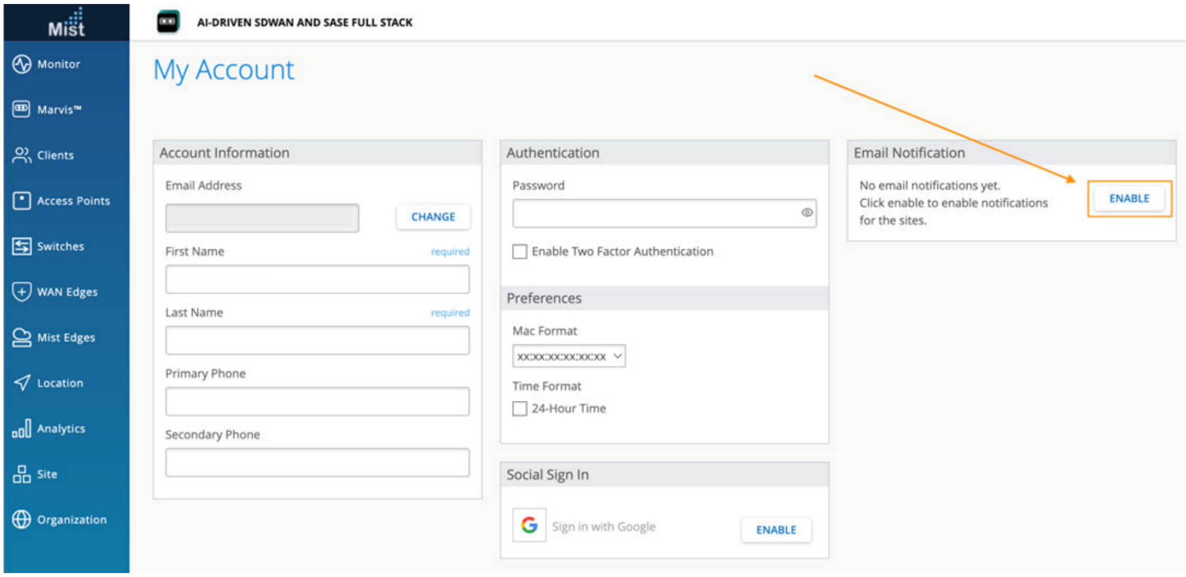
☑ To organization admins ☑ To site admins

Admins should enable Email notifications in My Account

To additional email recipients

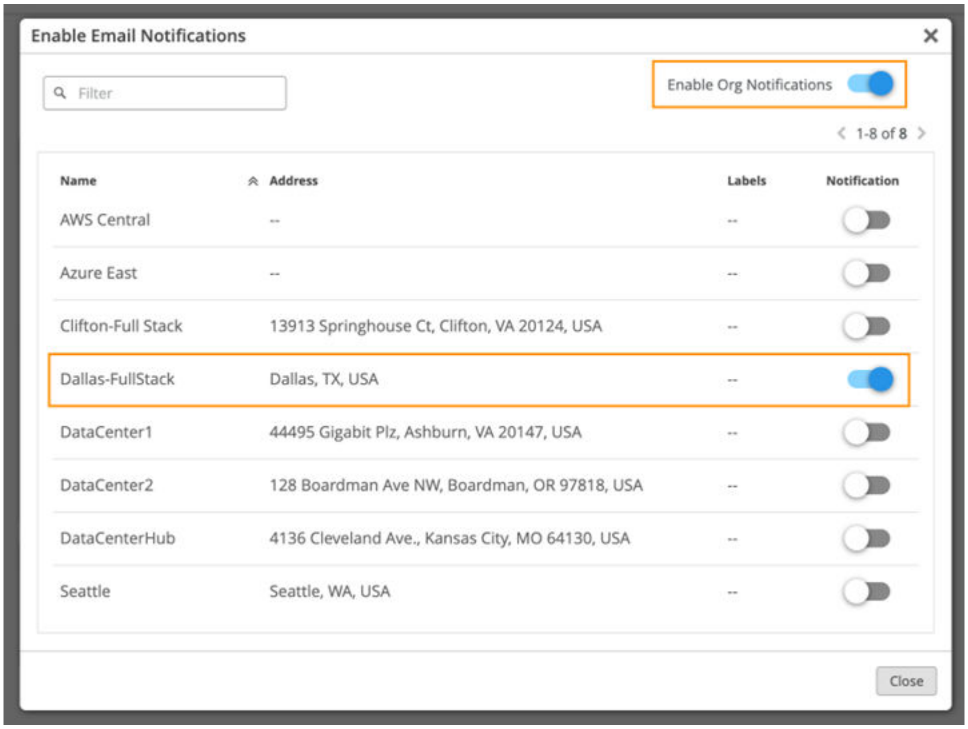
Email addresses (comma-separated)

4. Use **ENABLE** button on the Alerts Configuration in the **Email Notification** section. It's important to note that even for an administrator, e-mails are disabled by default.



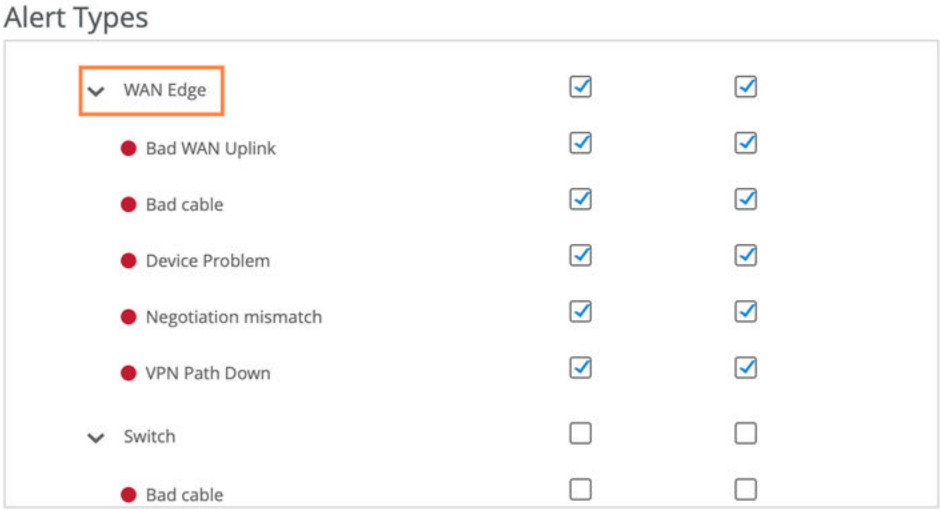
No email notifications yet.
Click enable to enable notifications for the sites.

You're directed to the Enable Email Notifications window where you enable e-mail alerts by selecting the toggle for Enable Org Notifications, and selecting specific sites, in the example below you can see we're getting notifications for our Dallas-FullStack site.



Name	Address	Labels	Notification
AWS Central	--	--	○
Azure East	--	--	○
Clifton-Full Stack	13913 Springhouse Ct, Clifton, VA 20124, USA	--	○
Dallas-FullStack	Dallas, TX, USA	--	●
DataCenter1	44495 Gigabit Plz, Ashburn, VA 20147, USA	--	○
DataCenter2	128 Boardman Ave NW, Boardman, OR 97818, USA	--	○
DataCenterHub	4136 Cleveland Ave., Kansas City, MO 64130, USA	--	○
Seattle	Seattle, WA, USA	--	○

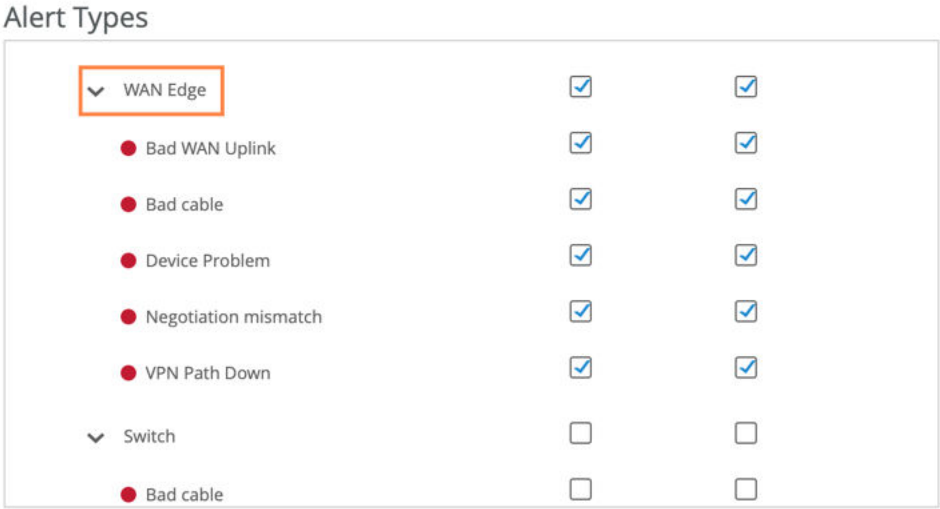
5. Now enable the gateway alerts and e-mail notifications for Infrastructure as shown in the options below:



Alert Types

WAN Edge	☑	☑
● Bad WAN Uplink	☑	☑
● Bad cable	☑	☑
● Device Problem	☑	☑
● Negotiation mismatch	☑	☑
● VPN Path Down	☑	☑
Switch	□	□
● Bad cable	□	□

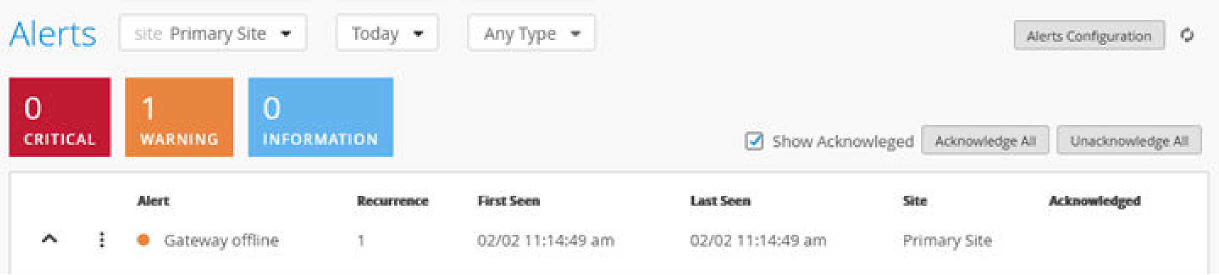
We recommend enabling the WAN edge alerts and e-mail notifications as well.



Alert Types

WAN Edge	☑	☑
● Bad WAN Uplink	☑	☑
● Bad cable	☑	☑
● Device Problem	☑	☑
● Negotiation mismatch	☑	☑
● VPN Path Down	☑	☑
Switch	□	□
● Bad cable	□	□

When a device loses connection to the Juniper Mist cloud, your administrator will receive an e-mail about the event after the issue is resolved. The Alert Details section in the e-mail will direct you to the Alerts page, but you can also look directly at it by seeing the Event reported below:



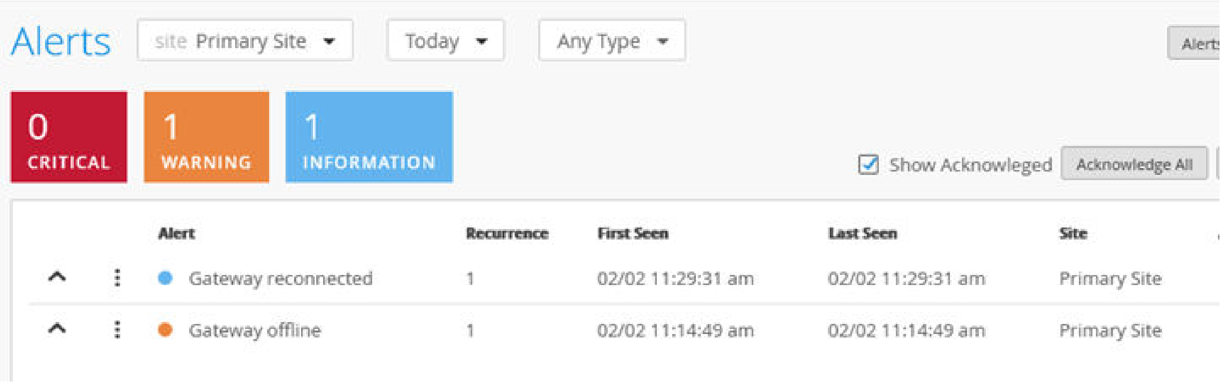
Alerts site Primary Site Today Any Type

0 CRITICAL 1 WARNING 0 INFORMATION

☑ Show Acknowleged

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	

After the connection to the Juniper Mist cloud has been restored, another e-mail will indicate the status change with a link to the Alerts page, with the second event reported.



Alerts

site Primary Site ▾ | Today ▾ | Any Type ▾

0 CRITICAL | 1 WARNING | 1 INFORMATION

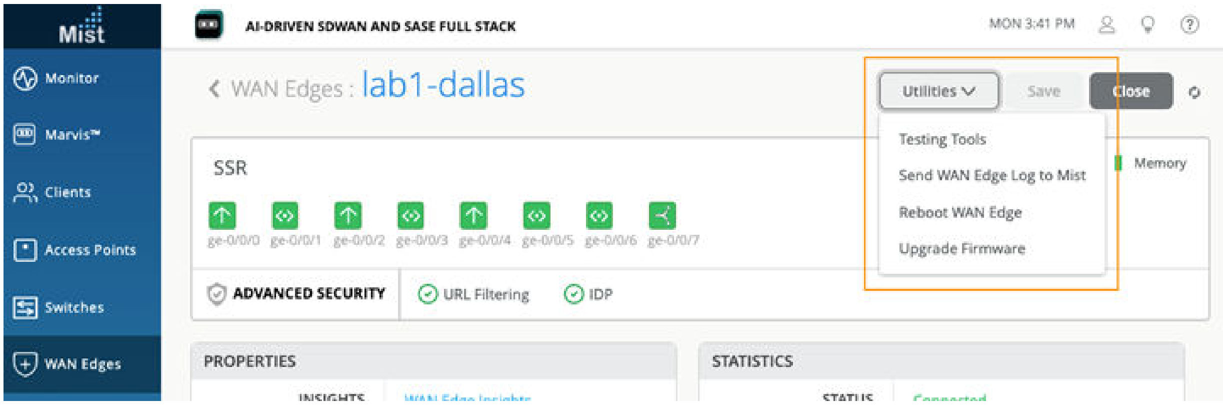
☑ Show Acknowleged | Acknowledge All

		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

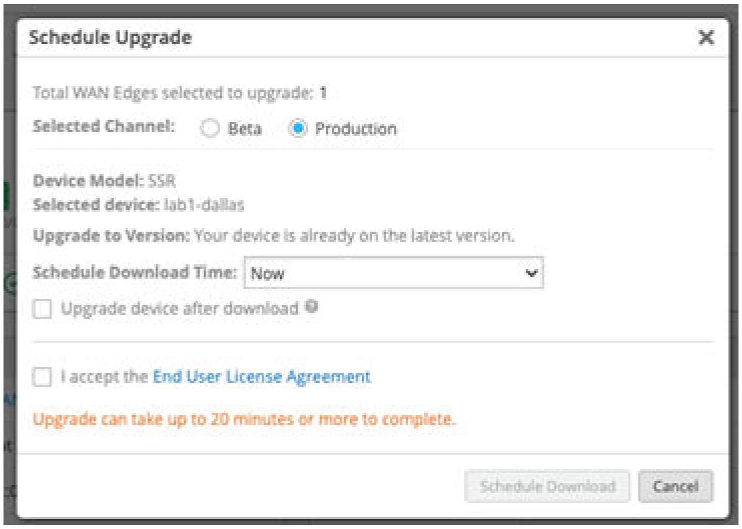
Session Smart Router Testing Tools for Troubleshooting

The Session Smart Router in WAN Assurance relies on SLE and Marvis insights for all your troubleshooting actions. An administrator's ability to see beneath the surface of the GUI is limited to the utilities we'll cover in this section. If you are familiar with the Session Smart Router device and its Programmable CLI (PCLI), which runs the Conductor-based deployments, you'll have a simplified and streamlined experience diagnosing your WAN Edge device using the Mist UI.

First, we'll dive into the **Utilities** button on your selected WAN Edge. Navigate to **WAN Edges** > **WAN Edges**, and we're selecting our Dallas-lab WAN Edge in this example.



In the **Utilities** menu, you'll see the options **Testing Tools**, **Send WAN Edge Log to Mist**, **Reboot WAN Edge**, and **Upgrade Firmware**. Sending the WAN edge device logs to the Juniper Mist cloud and rebooting your selected WAN edge device are straightforward activities. For upgrading firmware, you'll have a few options for scheduling and version, as you can see in the screenshot below:



Schedule Upgrade

Total WAN Edges selected to upgrade: 1

Selected Channel: ○ Beta ● Production

Device Model: SSR

Selected device: lab1-dallas

Upgrade to Version: Your device is already on the latest version.

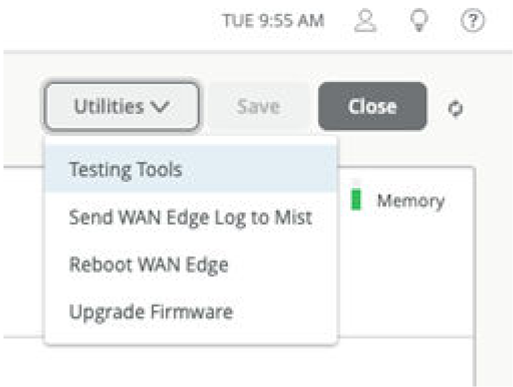
Schedule Download Time: Now

□ Upgrade device after download

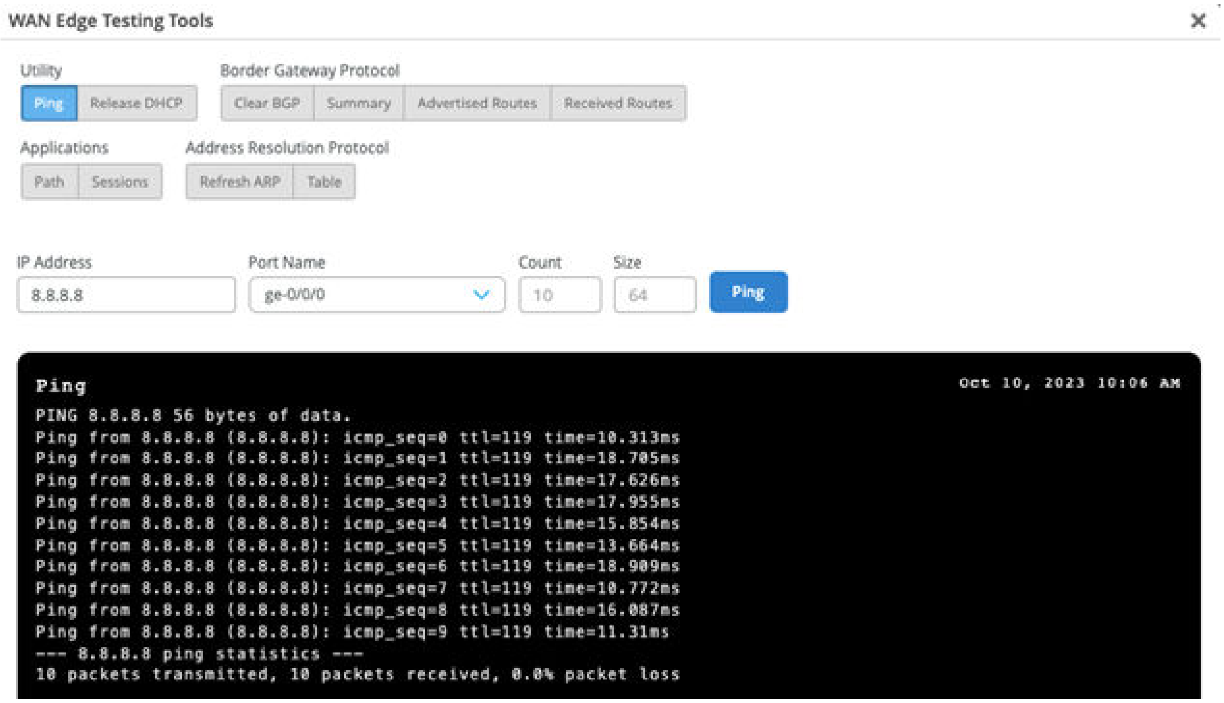
□ I accept the End User License Agreement

Upgrade can take up to 20 minutes or more to complete.

For troubleshooting, let's explore the **Testing Tools** option in the **Utilities** menu.



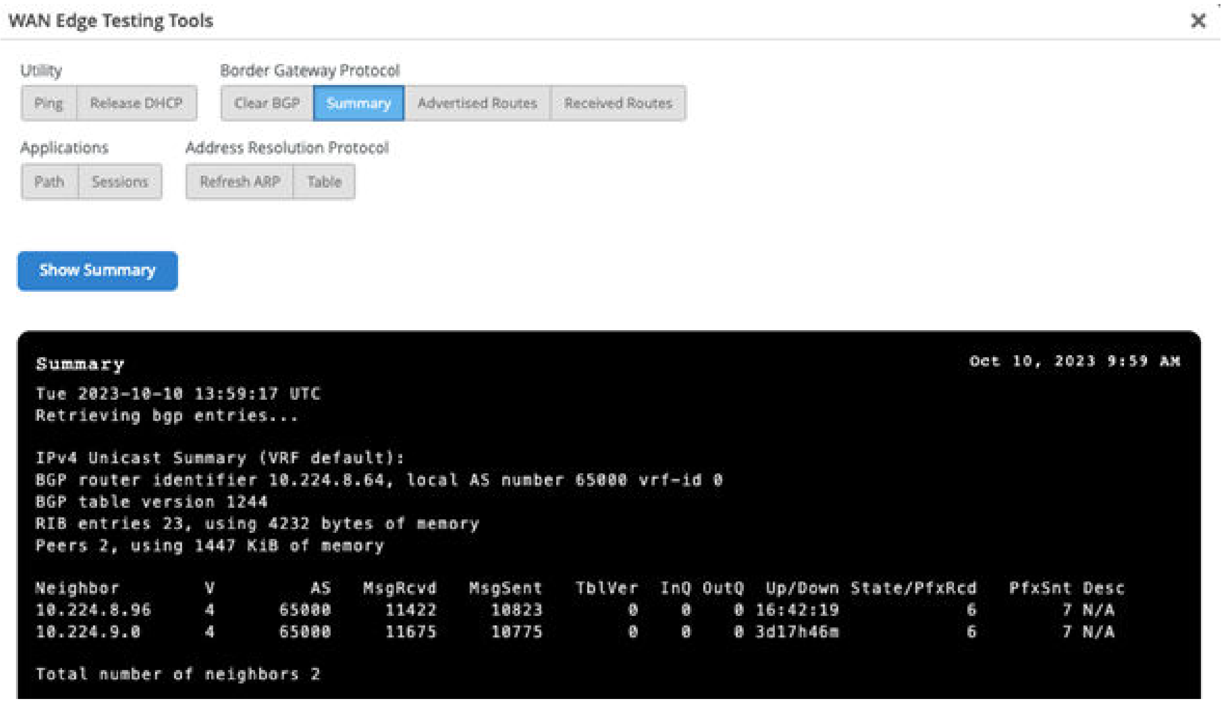
The **Testing Tools** option allows you to issue ICMP-Ping, identify BGP status reviews, sift through Application and Session knowledge, and review Address Resolution Protocol (ARP) tools for your WAN edge. The Mist UI enables quick troubleshooting for device interfaces and connectivity with pings. In this example, we send an ICMP ping to the public DNS 8.8.8.8. After you select Ping from the Utility section, enter an IP address, and specify the port name and the ping count and size, Mist opens an instance of the Session Smart PCLI for you.



IP Address: 8.8.8.8
Port Name: ge-0/0/0
Count: 10
Size: 64

```
Ping                                                          Oct 10, 2023 10:06 AM
PING 8.8.8.8 56 bytes of data.
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=0 ttl=119 time=10.313ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=1 ttl=119 time=18.705ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=2 ttl=119 time=17.626ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=3 ttl=119 time=17.955ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=4 ttl=119 time=15.854ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=5 ttl=119 time=13.664ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=6 ttl=119 time=18.909ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=7 ttl=119 time=10.772ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=8 ttl=119 time=16.087ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=9 ttl=119 time=11.31ms
--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
```

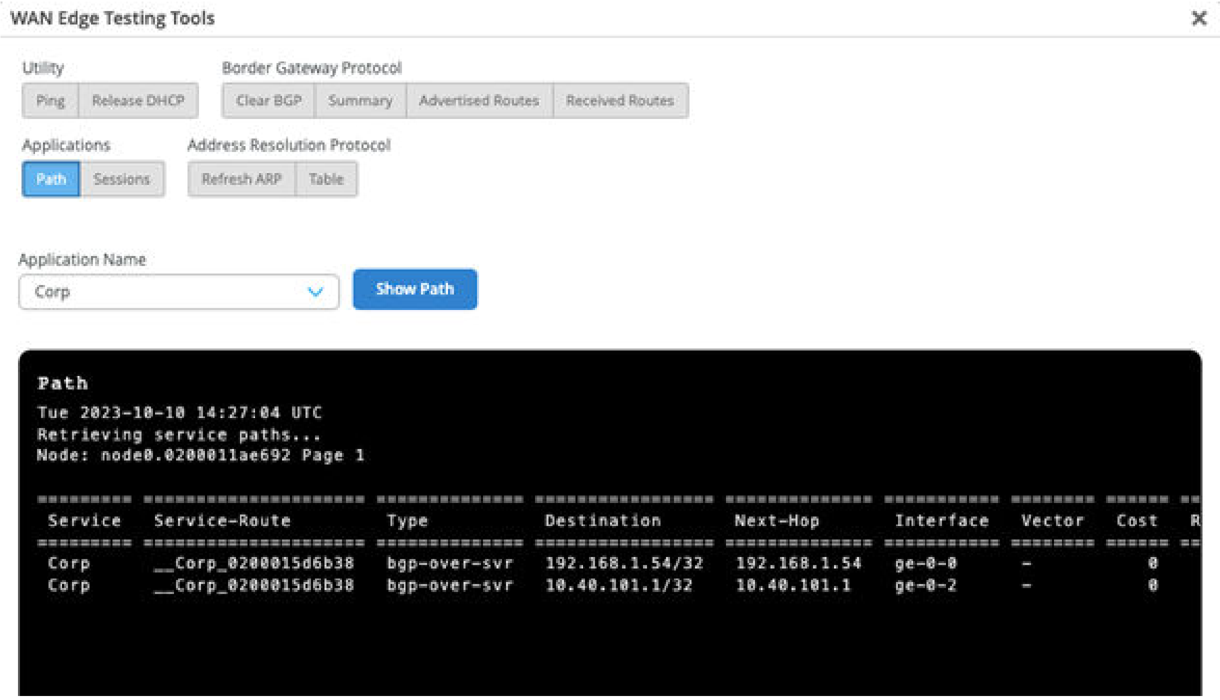
When you select any of the WAN Edge Testing tools for BGP, Mist simplifies the Session Smart PCLI and gathers the information for you. In this example, we see a summary of BGP neighbors and their relevant information by quickly selecting **Summary** under Border Gateway Protocol and then clicking **Show Summary**.



```
Summary                                                                Oct 10, 2023 9:59 AM
Tue 2023-10-10 13:59:17 UTC
Retrieving bgp entries...

IPv4 Unicast Summary (VRF default):
BGP router identifier 10.224.8.64, local AS number 65000 vrf-id 0
BGP table version 1244
RIB entries 23, using 4232 bytes of memory
Peers 2, using 1447 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd   PfxSnt Desc
10.224.8.96     4      65000     11422     10823        0    0    0 16:42:19            6        7 N/A
10.224.9.0      4      65000     11675     10775        0    0    0 3d17h46m            6        7 N/A

Total number of neighbors 2
```

Remember that Mist is intent-driven, and the Session Smart Secure Vector Routing (SVR) protocol leverages the sources and destinations in Mist, the networks, and applications to create point-to-point SVR paths. You can diagnose those paths between Session Smart devices in the **WAN Edge Testing Tools** utility. In this example, we're looking at the Corp Application. In this example, you'll also notice that the actual BGP advertisements are sent through SVR.

> **NOTE**: For SVR, Mist applications are called *services* in the Session Smart paradigm. For more information about the Session Smart platform, refer to the platform considerations, https://www.juniper.net/documentation/us/en/software/mist/mist-wan/topics/concept/mist-wan-platform-consideration.html.

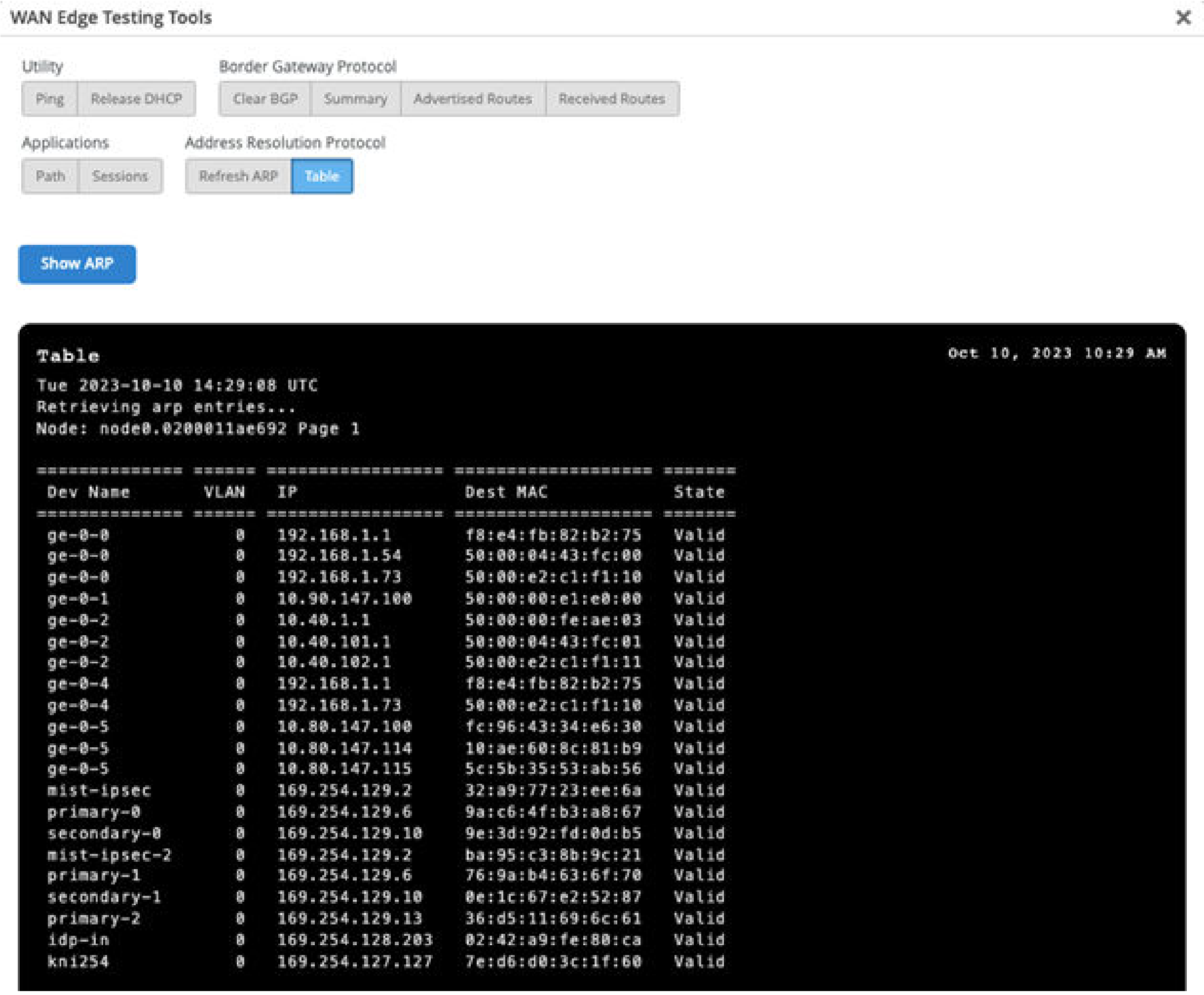


Application Name: Corp

```
Path
Tue 2023-10-10 14:27:04 UTC
Retrieving service paths...
Node: node0.0200011ae692 Page 1

========= ===================== ============== ================= ============== =========== ======== ====== ==
 Service   Service-Route          Type           Destination       Next-Hop       Interface   Vector   Cost   R
========= ===================== ============== ================= ============== =========== ======== ====== ==
 Corp      __Corp_0200015d6b38    bgp-over-svr   192.168.1.54/32   192.168.1.54   ge-0-0      -           0
 Corp      __Corp_0200015d6b38    bgp-over-svr   10.40.101.1/32    10.40.101.1    ge-0-2      -           0
```

Finally, let's explore ARP tools in **WAN Edge Testing Tools**. In our example, we've selected a the table format for displaying the ARP information, and again, the Mist dashboard leverages the Session Smart PCLI for you and generates and generates ARP information for interfaces on node.0.

> **NOTE**: For deeper insights not shown on the output text of the window, select the output from the Utility in your browser and paste it to an ASCII editor for further review.



Table

Oct 10, 2023 10:29 AM

```
Tue 2023-10-10 14:29:08 UTC
Retrieving arp entries...
Node: node0.0200011ae692 Page 1

============== ====== ================= =================== =======
 Dev Name       VLAN   IP                Dest MAC            State
============== ====== ================= =================== =======
 ge-0-0            0   192.168.1.1       f8:e4:fb:82:b2:75   Valid
 ge-0-0            0   192.168.1.54      50:00:04:43:fc:00   Valid
 ge-0-0            0   192.168.1.73      50:00:e2:c1:f1:10   Valid
 ge-0-1            0   10.90.147.100     50:00:00:e1:e0:00   Valid
 ge-0-2            0   10.40.1.1         50:00:00:fe:ae:03   Valid
 ge-0-2            0   10.40.101.1       50:00:04:43:fc:01   Valid
 ge-0-2            0   10.40.102.1       50:00:e2:c1:f1:11   Valid
 ge-0-4            0   192.168.1.1       f8:e4:fb:82:b2:75   Valid
 ge-0-4            0   192.168.1.73      50:00:e2:c1:f1:10   Valid
 ge-0-5            0   10.80.147.100     fc:96:43:34:e6:30   Valid
 ge-0-5            0   10.80.147.114     10:ae:60:8c:81:b9   Valid
 ge-0-5            0   10.80.147.115     5c:5b:35:53:ab:56   Valid
 mist-ipsec        0   169.254.129.2     32:a9:77:23:ee:6a   Valid
 primary-0         0   169.254.129.6     9a:c6:4f:b3:a8:67   Valid
 secondary-0       0   169.254.129.10    9e:3d:92:fd:0d:b5   Valid
 mist-ipsec-2      0   169.254.129.2     ba:95:c3:8b:9c:21   Valid
 primary-1         0   169.254.129.6     76:9a:b4:63:6f:70   Valid
 secondary-1       0   169.254.129.10    0e:1c:67:e2:52:87   Valid
 primary-2         0   169.254.129.13    36:d5:11:69:6c:61   Valid
 idp-in            0   169.254.128.203   02:42:a9:fe:80:ca   Valid
 kni254            0   169.254.127.127   7e:d6:d0:3c:1f:60   Valid
```

The combination of **Marvis insights**, **WAN SLEs**, **WAN edge insights**, and the **WAN Edge Testing Tools** utility make a complete suite for diagnosis at the WAN edge.

SEE ALSO

Monitor Session Smart Router Deployed as WAN Edge | 571

Troubleshoot Session Smart Router Deployed as WAN Edge | 613

Troubleshoot Session Smart Routers Using Packet Captures

IN THIS SECTION

Juniper Session Smart Router (SSR) ports support manual and dynamic packet captures (PCAP). Packet capture is a tool that helps you to analyze network traffic and troubleshoot network problems. It captures real-time data packets traveling over the network for monitoring and logging.

For more information, see "Dynamic and Manual Packet Captures" on page 628.

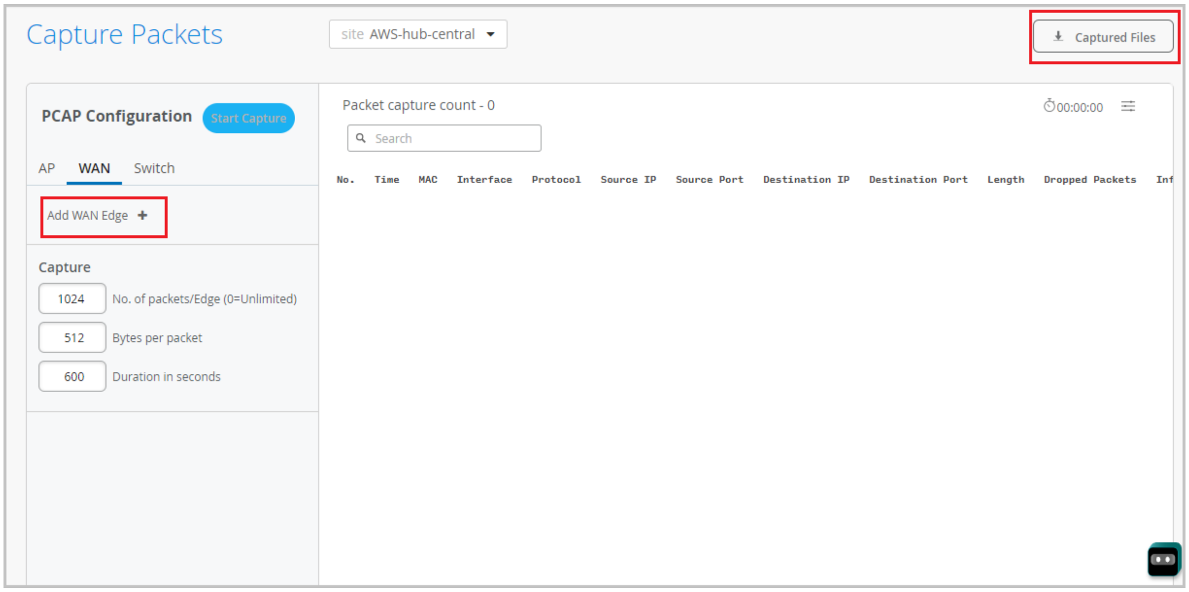
Initiate a Manual Packet Capture

Manual packet captures are initiated by users from the WAN Edge Packet capture page.

To initiate manual PCAP for an SSR device:

1. Go to **Site** > **WAN Edge Packet Captures.**

2. On the WAN tab, click **Add WAN Edge +** and select an SSR device.



Capture

1024 No. of packets/Edge (0=Unlimited)

512 Bytes per packet

600 Duration in seconds

3. Specify the number of packets captured, packet size in bytes, and the duration of the capture session.

You can click **Captured Files** to access a manual PCAP file and analyze it.

Access Dynamic Packet Captures

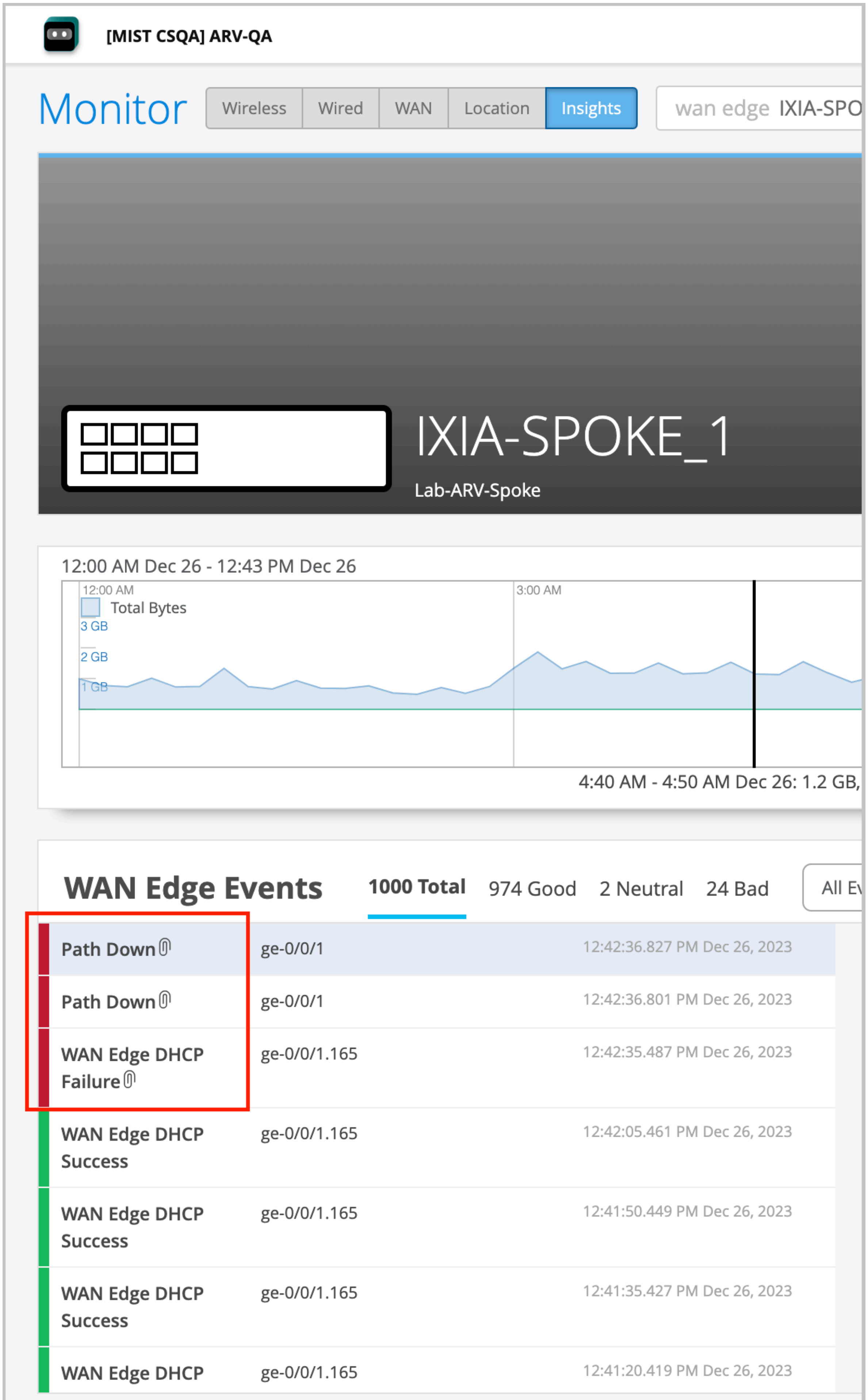
Dynamic packet captures are short-term packet captures automatically triggered by a service impacting event. They are saved to the Mist cloud and are available for you to download in the WAN Edge Events section on the WAN Edge Insights page.

Here are the events which can generate a dynamic packet capture for an SSR device:

- Failure of the ARP request to next-hop gateway
- DHCP address resolution failure
- WAN Edge failure to establish BGP peering based on configuration
- WAN Edge failure to establish SVR peering based on configuration

To download and analyze a dynamic packet capture file:

1. Go to **Monitor** > **Service Levels**. By default, you will land on the Insights tab.
2. Scroll down to WAN Edge Events section. Each event with a dynamic packet capture file available is indicated by a paperclip icon next to the event name.



WAN Edge Events   1000 Total   974 Good   2 Neutral   24 Bad

Path Down	ge-0/0/1	12:42:36.827 PM Dec 26, 2023
Path Down	ge-0/0/1	12:42:36.801 PM Dec 26, 2023
WAN Edge DHCP Failure	ge-0/0/1.165	12:42:35.487 PM Dec 26, 2023
WAN Edge DHCP Success	ge-0/0/1.165	12:42:05.461 PM Dec 26, 2023
WAN Edge DHCP Success	ge-0/0/1.165	12:41:50.449 PM Dec 26, 2023
WAN Edge DHCP Success	ge-0/0/1.165	12:41:35.427 PM Dec 26, 2023
WAN Edge DHCP	ge-0/0/1.165	12:41:20.419 PM Dec 26, 2023

3. Click an event dynamic packet capture and then click the **Download Packet Capture** button available in the Events Details section on the right.

Speed Tests for Session Smart Router Deployed as a WAN Edge (BETA)

Service Providers (SPs) as well as their end customers install and deploy telecommunication circuits (or paths) to offices, branches, and so on. As Session Smart Routers are deployed at the edge of the customer premise, SPs and customers need to generate traffic to test the speed and performance of these circuits to ensure the quality is being maintained.

From the Juniper Mist™ portal, you can run a speed test for a Session Smart Router deployed as a WAN Edge on your network. Speed tests come in handy, for example, when:

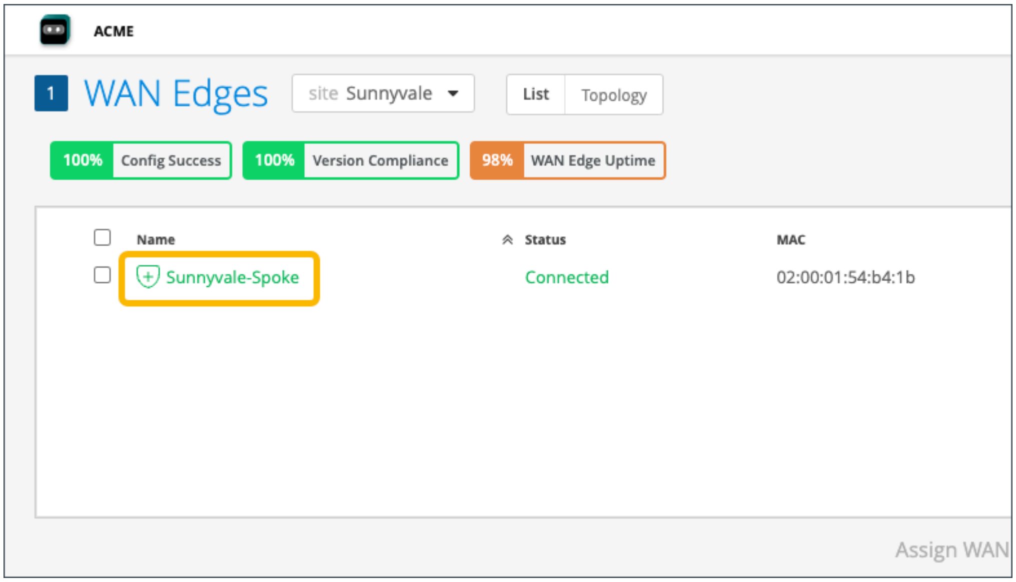
- You need to test the speed and performance of the circuit being delivered to the customer.
- You need to perform new link qualification to verify that speeds are what the service provider and customer have agreed upon.
- You need to perform on-demand speed tests when you suspect a low link speed is causing link issues.
- You need to run scheduled speed tests to re-test link speeds and ensure performance continues to meet expectations on an ongoing basis.

NOTE: The WAN Edge Speed Test tool can reliably validate circuits speeds of 1 megabit per second (Mbps) to 1 gigabit per second (Gbps). Circuits exceeding 1Gbps must rely on other tools for validation.

The WAN Edge Speed Test tool does not measure or validate jitter or loss.

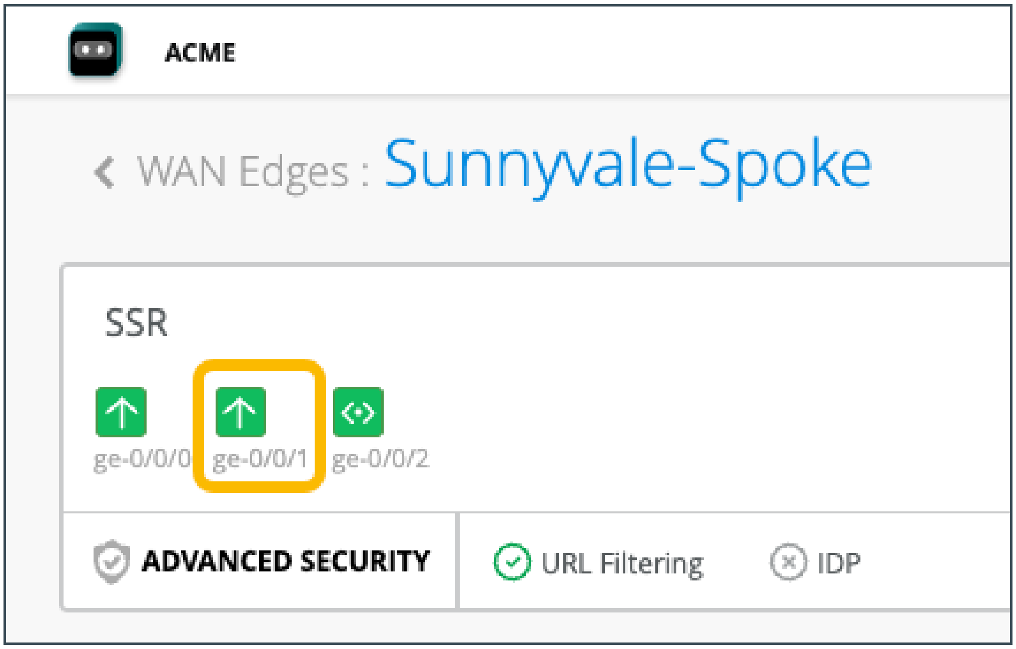
To run a Speed Test for a Session Smart Router deployed as a WAN Edge:

1. Navigate to the Juniper Mist portal, then click **WAN Edges** > **WAN Edges**.
2. Select the WAN Edge name.



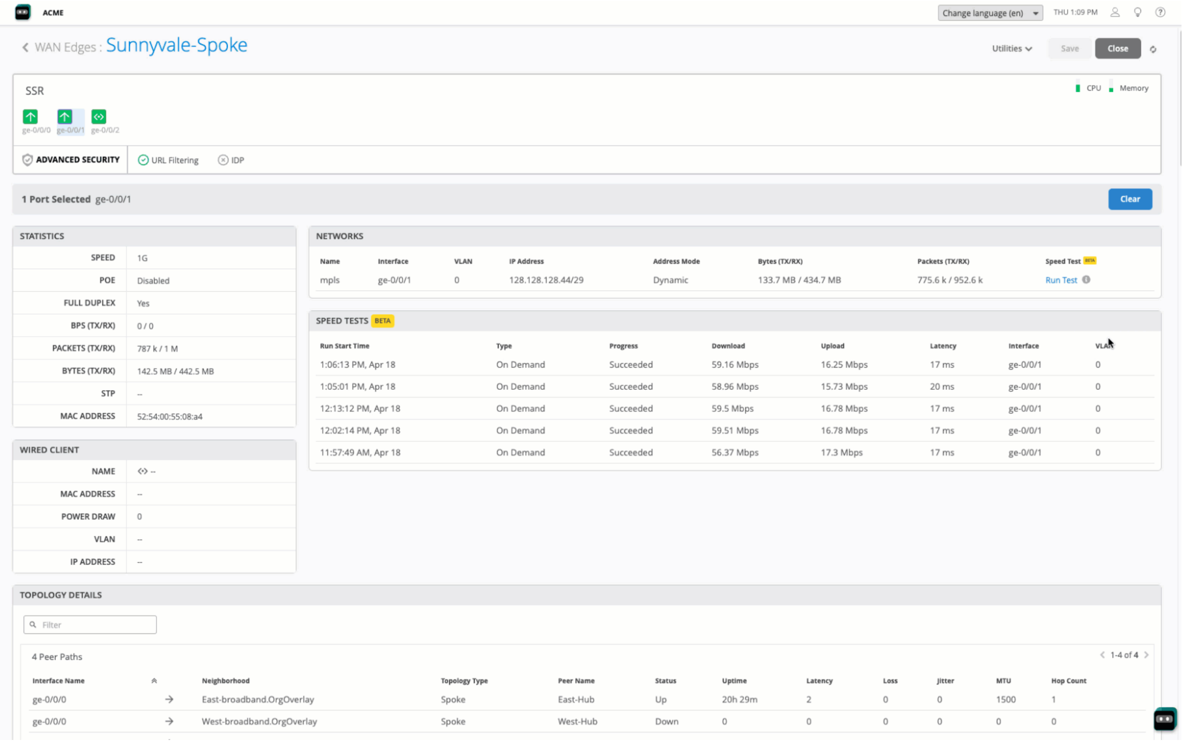
Name	Status	MAC
Sunnyvale-Spoke	Connected	02:00:01:54:b4:1b

3. Select the WAN port from the Port Panel.



4. The Networks section then appears. From the **Networks** section, under the Speed Test column, click **Run Test**.

5. In the Speed Tests section, the test you are currently running is **In Progress**. After a minute or two, the progress of the speed test changes to **Succeeded**, and the results populate in the columns, displaying information such as download speed, upload speed, latency, the interface the test was run on, and the VLAN number.



ACME

Change language (en) THU 1:09 PM

WAN Edges : Sunnyvale-Spoke

Utilities Save Close

SSR

ge-0/0/0 ge-0/0/1 ge-0/0/2

CPU Memory

ADVANCED SECURITY ✓ URL Filtering ⊗ IDP

1 Port Selected ge-0/0/1 Clear

STATISTICS

SPEED	1G
POE	Disabled
FULL DUPLEX	Yes
BPS (TX/RX)	0 / 0
PACKETS (TX/RX)	787 k / 1 M
BYTES (TX/RX)	142.5 MB / 442.5 MB
STP	--
MAC ADDRESS	52:54:00:55:08:a4

WIRED CLIENT

NAME	<·> --
MAC ADDRESS	--
POWER DRAW	0
VLAN	--
IP ADDRESS	--

NETWORKS

Name	Interface	VLAN	IP Address	Address Mode	Bytes (TX/RX)	Packets (TX/RX)	Speed Test BETA
mpls	ge-0/0/1	0	128.128.128.44/29	Dynamic	133.7 MB / 434.7 MB	775.6 k / 952.6 k	Run Test

SPEED TESTS BETA

Run Start Time	Type	Progress	Download	Upload	Latency	Interface	VLAN
1:06:13 PM, Apr 18	On Demand	Succeeded	59.16 Mbps	16.25 Mbps	17 ms	ge-0/0/1	0
1:05:01 PM, Apr 18	On Demand	Succeeded	58.96 Mbps	15.73 Mbps	20 ms	ge-0/0/1	0
12:13:12 PM, Apr 18	On Demand	Succeeded	59.5 Mbps	16.78 Mbps	17 ms	ge-0/0/1	0
12:02:14 PM, Apr 18	On Demand	Succeeded	59.51 Mbps	16.78 Mbps	17 ms	ge-0/0/1	0
11:57:49 AM, Apr 18	On Demand	Succeeded	56.37 Mbps	17.3 Mbps	17 ms	ge-0/0/1	0

TOPOLOGY DETAILS

Filter

4 Peer Paths 1-4 of 4

Interface Name		Neighborhood	Topology Type	Peer Name	Status	Uptime	Latency	Loss	Jitter	MTU	Hop Count
ge-0/0/0	→	East-broadband.OrgOverlay	Spoke	East-Hub	Up	20h 29m	2	0	0	1500	1
ge-0/0/0	→	West-broadband.OrgOverlay	Spoke	West-Hub	Down	0	0	0	0	0	0

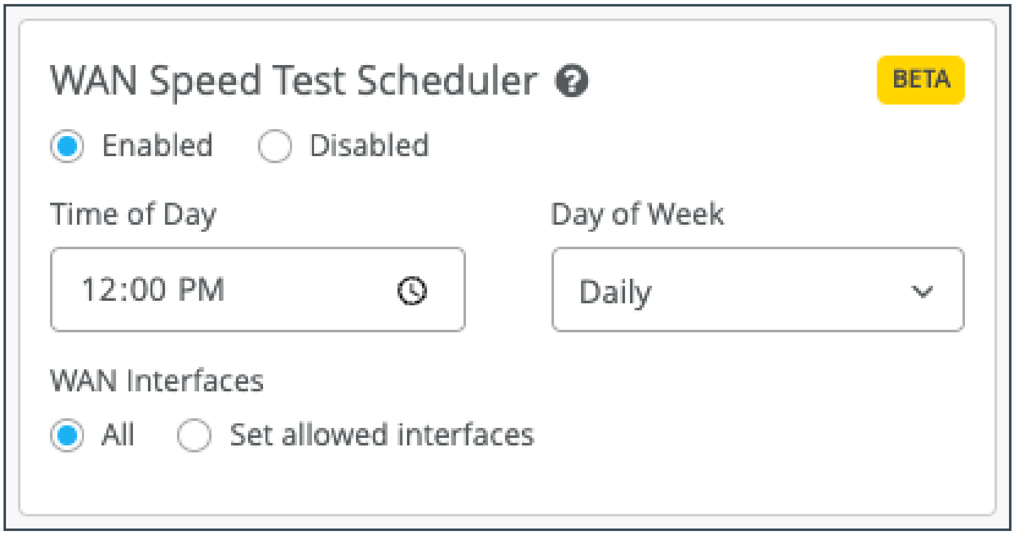
6. If you need to run speed tests on a recurring basis, you can use the WAN Speed Test Scheduler.

   a. Navigate to **Organization** > **Settings**.

   b. In the **WAN Speed Test Scheduler** section, select **Enabled**.

   c. Select the **Time of Day** and **Day of Week** that you want the speed tests to occur.

   d. Select whether you want to run the tests on all WAN interfaces or select WAN interfaces.



WAN Speed Test Scheduler BETA

● Enabled ○ Disabled

Time of Day: 12:00 PM

Day of Week: Daily

WAN Interfaces

● All ○ Set allowed interfaces

Dynamic and Manual Packet Captures

SUMMARY

When investigating communication failures between the client and the access point (AP), you can use the Juniper Mist™ portal to get dynamic and manual packet captures.

IN THIS SECTION

NOTE: Mist does not collect or store any payload data from packets capture. Only transmission and connection data are used.

Dynamic Packet Captures

IN THIS SECTION

Which Events Trigger Dynamic Packet Captures?

Whenever a connection failure event occurs between the wireless client and an access point (AP), it automatically triggers a short-term dynamic packet capture.

These events include:

- DHCP Timeout—When the client sends a broadcast discover packet but does not receive an offer packet from server.

- DHCP Denied—When the server sends a DHCP NAK, indicating that the IP address might already be in use.
- DHCP Terminated—When the Client does not proceed with DHCP request for the offer provided by the server.
- Authorization Failure—This could be caused due to various reasons (MIC failure, Radius server not responding, Access-Reject from Radius server, client failing to complete the auth process).
- 11r FBT Failure—This is caused due to client failing 11r roam.
- OKC Auth Failure—This is caused due to client failing OKC roam.
- Association Failure—This could be caused due to Tx failures or invalid PMKID included by the client during association request.

Finding the Packet Captures

Dynamic packet captures are saved to the cloud. You can download them from the Insights page.

Video Demo

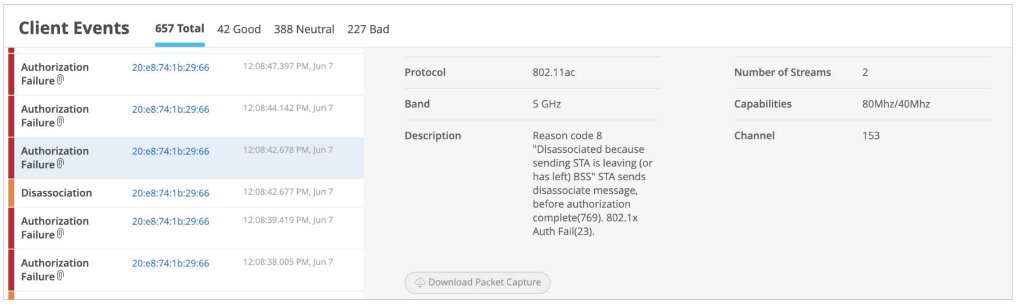
Video: NOW in 60: WAN Assurance - Dynamic Packet Capture

Example

This example shows how easily you can find dynamic packet captures on the Insights page.

1. From the left menu, select **Monitor** > **Service Levels**.
2. Click the **Insights** button to view the Insights page.
3. Scroll down to the **Client Events** section.

   Paperclip icons indicate the events with dynamic packet captures.
4. Click an event to see more details on the right side of the screen.
5. Below the details, click **Download Packet Capture**.



Client Events 657 Total 42 Good 388 Neutral 227 Bad

Authorization Failure	20:e8:74:1b:29:66	12:08:47.397 PM, Jun 7
Authorization Failure	20:e8:74:1b:29:66	12:08:44.142 PM, Jun 7
Authorization Failure	20:e8:74:1b:29:66	12:08:42.678 PM, Jun 7
Disassociation	20:e8:74:1b:29:66	12:08:42.677 PM, Jun 7
Authorization Failure	20:e8:74:1b:29:66	12:08:39.419 PM, Jun 7
Authorization Failure	20:e8:74:1b:29:66	12:08:38.005 PM, Jun 7

Protocol	802.11ac	Number of Streams	2
Band	5 GHz	Capabilities	80Mhz/40Mhz
Description	Reason code 8 "Disassociated because sending STA is leaving (or has left) BSS" STA sends disassociate message, before authorization complete(769). 802.1x Auth Fail(23).	Channel	153

Manual Packet Captures

For manual packet captures, go to **Site** > **Packet Captures**, where you can:

- Choose which network type to capture packets from: wired, wireless, or WAN.

> **NOTE**: Wired packet capture applies to the wired ports of APs (not the switch ports). WAN packet captures support Session Smart Router and SRX WAN edge device ports.

- Restrict the packet capture to specific clients, WLANs, APs, or wireless bands.
- Configure the number of packets captured, packet size in bytes, and the duration of the capture session.
- Configure other capture parameters such as header inclusion and capture filters. See Table 91 on page 632 for details.

After downloading the packet capture to your computer, follow the steps below to view them in Wireshark.

Configure IEEE 802.11 on Wireshark

Packet inspection requires Wireshark. See https://www.wireshark.org for the download file and related information.

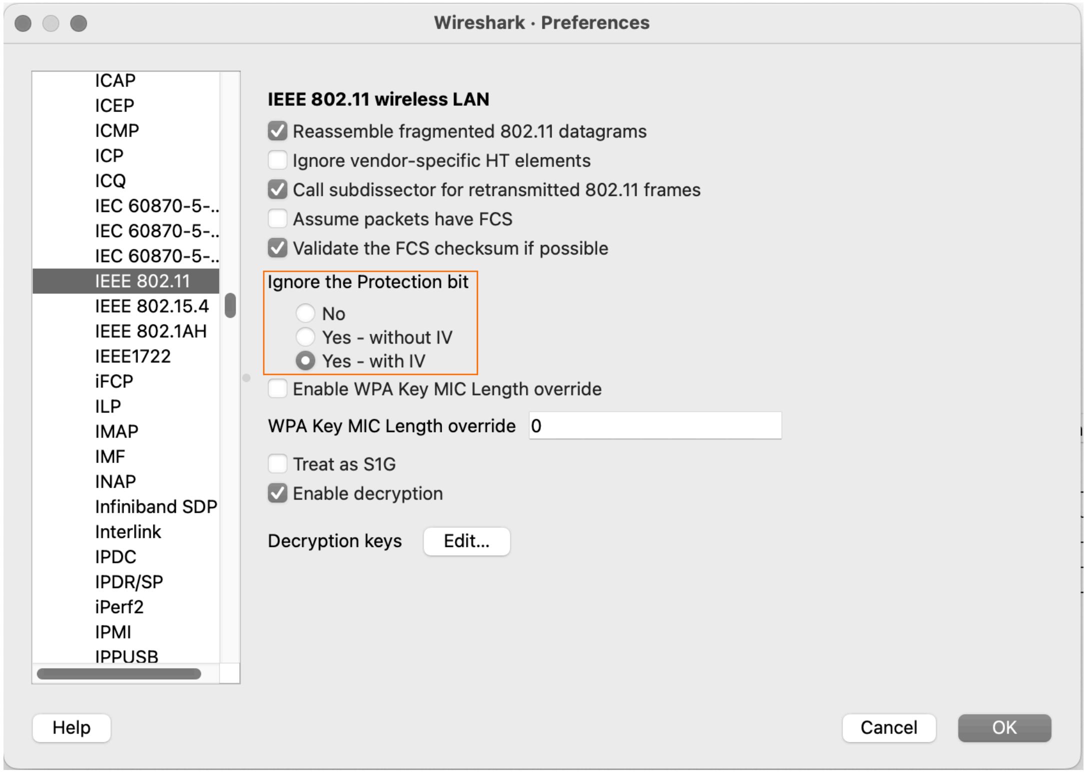
To configure Wireshark to view packets captured from the Juniper Mist portal, follow the steps below:

1. Open the Wireshark application on your computer.
2. Open the Wireshark Preferences window:

   On a Windows computer, navigate to **Edit** > **Preferences**.

   On a Mac computer, navigate to **Wireshark** > **Preferences**.
3. In the Preferences window, expand the **Protocols** menu option and scroll down to **IEEE 802.11**.

   a. Select **Yes - with IV** and then click **OK**, as shown in the following image:



IEEE 802.11 wireless LAN

☑ Reassemble fragmented 802.11 datagrams

□ Ignore vendor-specific HT elements

☑ Call subdissector for retransmitted 802.11 frames

□ Assume packets have FCS

☑ Validate the FCS checksum if possible

Ignore the Protection bit

○ No

○ Yes - without IV

● Yes - with IV

□ Enable WPA Key MIC Length override

WPA Key MIC Length override 0

□ Treat as S1G

☑ Enable decryption

Decryption keys Edit...

View Wireless Packet Captures in Wireshark

You can capture packets from both your wired and wireless networks. The following configuration regards wireless packet, for which you can see:

- Wireless channel information
- Wireless data rate
- Received signal strength indicator (RSSI)

To accomplish this task, you must download and install the Wireshark application on your computer. In a Web browser, navigate to https://www.wireshark.org for Wireshark application downloads and detailed information about Wireshark. For additional information about Wireshark, see https://www.wireshark.org/docs/.

This topic provides minimal guidance about how to configure Wireshark for use in examining wireless packet captures gathered from the Juniper Mist portal.

1. Open the Wireshark application on your computer.
2. Open the Wireshark Preferences window:

   On a Windows computer, navigate to **Edit** > **Preferences**.

On a Mac computer, navigate to **Wireshark** > **Preferences**.

3. In the Preferences window, navigate to **Appearance** > **Columns**.
4. Click the **Add (+)** button to add a new radiotap column to the Wireshark display (radiotap headers include wireless packet frames that would otherwise not be displayed. See: https://www.wireshark.org/docs/dfref/r/radiotap.html.

   Wireshark adds a new line called New Column, and the type Number.

   a. Double-click the **New Column** title and type Channel as the title.

   b. Double-click the **Type** column and select Frequency/Channel from the drop-down menu.

   c. Leave the **Displayed** column selected.
5. Repeat Step 4 two times

   a. The first time, use **Data Rate** for the column title and **IEEE 802.11 TX Rate** for the type.

   b. The second time, use **RSSI** as the column title and **IEEE 802.11 RSSI** for the type.
6. Click **OK** to save your changes.

   Wireshark will display the new columns when you open a packet capture (.pcap) file for viewing.

Manual Packet Capture Options

By default, Juniper Mist streams the packet capture session data, including beacon frames, to the Mist portal. The following table describes the packet capture options that you can use when you create a packet capture session.

Table 91: Packet Capture Options

Option Name	Option Function	Usage Notes	Firmware Notes
Include Network Headers	Include packet headers in addition to the packet data.	Packet capture works by buffering packets locally on the device, meaning there is limited space available for storage. By default, Mist truncates header data from the captured packets to reduce the size of capture files while still providing the most relevant information.	–

Table 91: Packet Capture Options *(Continued)*

Option Name	Option Function	Usage Notes	Firmware Notes
Local Capture	Do not stream the live capture data to the Mist GUI.	Earlier AP firmware did not support live streaming packet captures to the Juniper Mist portal.	Required for AP firmware versions before 0.10.x
Canned Filters	Pre-defined filters that vary based on the type of packet capture you're performing.	The filters available in the list change depending on whether you're capturing wireless, wired, or WAN packets. For example, beacon frames are only available for wireless packet captures.	–
Advanced Filters	Create your own packet filters for the capture session using `tcpdump` syntax.		0.10.x or later
Expression Builder	Interactive GUI tool to build custom filters in `tcpdump` syntax for use in the capture session.	You can let the builder start the filter entry and then add to or delete from the entry manually.	0.10.x or later

Troubleshoot SRX Series Firewalls

IN THIS SECTION

This chapter describes the steps to troubleshoot your SRX Series device that appears as disconnected on the Mist portal. It also discusses the packet capture (PCAP) support available for SRX Series devices deployed as WAN Edges in the Mist cloud.

Troubleshoot SRX Series Firewalls Shown as Disconnected

If the Juniper Mist™ portal shows a Juniper Networks® SRX Series Firewall as disconnected when it is online and reachable locally, you can troubleshoot the issue using the steps listed in this topic. You need console access or SSH access to the firewall to perform the troubleshooting steps.

1. Check if the SRX Series Firewall is running on the supported Junos OS version.

   For WAN Assurance, you need Junos OS version 19.4 and later for SRX300, SRX320, SRX340, SRX345, SRX380, SRX550M, SRX1500, and SRX1600.

   You can use the `show version` CLI command to check the version.

2. Check if the SRX Series Firewall has a valid IP address.

   Use the `show interfaces terse` command.

```
user@host >  show interfaces terse 1 match ge-0/0/0
ge-0/0/0      up    up
ge-0/0/0.0    up    up    inet    10.0.0.51/24

user@host > show interfaces terse I match    irb
irb        up    up
irb.0         up    down
irb.2         up    up    inet    192.168.2.1/24
irb.8         up    up    inet    192.168.8.1/24
irb.10        up    up    inet    192.168.10.1/24
irb.24        up    up    inet    192.168.24.1/24
```

   You should see the integrated routing and bridging (IRB) interface (irb.0) with an IP address. You might see multiple IRB interfaces, depending on the SRX Series model (or in the case of a chassis cluster HA configurations).

   At least one IRB interface needs to have a valid IP address. The Firewall can also connect using a management IP address, which you can see on the fxp0 interface. Ensure that either the irb or fxp0 interface has a valid IP address and has its Admin and Link states up.

3. Ensure that the firewall can reach the gateway as shown in the following sample.

```
user@host> ping inet 10.0.0.1
PING 10.0.0.1 (10.0.0.1): 56 data bytes
64 bytes from 10.0.0.1: icmp_seq=0 ttl=64 time=44.967 ms
64 bytes from 10.0.0.1: icmp_seq=l ttl=64 time=1.774 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=41.347 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=1.731 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=1.674 ms
^C
---10.0.0.1 ping statistics---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.674/18.299/44.967/20.329 ms
```

4. Check if your device can reach the Internet. Initiate a *ping* test toward any public server (for example, *8.8.8.8*).

```
user@host> ping inet 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=58 time=9.789 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=5.206 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=4.679 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=4.362 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=4.497 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 4.362/5.707/9.789/2.061 ms
```

5. Check if the firewall can resolve `oc-term.mistsys.net`.

```
user@host> ping oc-term.mistsys.net
PING ab847c3d0fcd311e9b3ae02d80612151-659eb20beaaa3ea3.elb.us-west-1.amazonaws.com
(13.56.90.212): 56 data bytes
```

If the firewall is not resolving `oc-term.mistsys.net`, make sure that the firewall has a DNS server configured.

```
user@host> show configuration | display set | grep name-server
set system name-server 8.8.8.8
set system name-server 8.8.4.4
```

If the firewall doesn't have a DNS server, configure the server as shown in the following example:

```
user@host# set system name-server 8.8.8.8
```

6. Ensure firewall ports are open (for example: tcp port 2200 for oc-term.mistsys.net).

   See the following table to determine which port to enable, depending on your cloud environment:

   Table 92: Ports to Enable in Different Juniper Mist Clouds

Service Type	Global 01	Global 02	Europe 01
SRX Series	redirect.juniper.net (TCP 443)	redirect.juniper.net (TCP 443)	redirect.juniper.net (TCP 443)
	ztp.mist.com (TCP 443)	ztp.gc1.mist.com (TCP 443)	ztp.eu.mist.com (TCP 443)
	oc-term.mistsys.net (TCP 2200)	oc-term.gc1.mist.com (TCP 2200)	oc-term.eu.mist.com (TCP 2200)

   You can check the connections using the following command:

   ```
   user@host> show system connections | grep 2200
   tcp4      0      0      10.0.0.51.49981   54.83.93.93.2200    ESTABLISHED
   ```

7. Check the system time on the firewall to make sure the time is correct.

   ```
   user@host> show system uptime
   Current time: 2021-08-23 19:39:17 UTC
   Time Source: LOCAL CLOCK
   System booted: 2021-07-14 22:40:20 UTC (5w4d 20:58 ago)
   Protocols started: 2021-07-14 22:45:39 UTC (5w4d 20:53 ago)
   ```

```
Last configured: 2021-08-23 19:34:05 UTC (00:05:12 ago) by root
7:39PM up 39 days, 20:59, 2 users, load averages: 0.66, 1.07, 0.92
```

If the system time is not correct, configure it. For more information, see Configure Date and Time Locally.

8. Check `device-id` to make sure it is in the format `<org_id>.<mac_addr>`, as shown below:

```
user@host# show system services outbound-ssh
traceoptions {
   file outbound-ssh.log size 64k files 5;
   flag all;
}
client mist {
   device-id abcd123445-1234-12xx-x1y2-ab1234xyz123.<mac>;
   secret "$abc123"; ## SECRET-DATA
   keep-alive {
      retry 12;
      timeout 5;
   }
   services netconf;
   oc-term-staging.mistsys.net {
      port 2200;
      retry 1000;
      timeout 60;
   }
}
```

See outbound-ssh for more information.

You can also examine the log messages by using the command `show log messages`.

9. Deactivate and then reactivate the outbound SSH, as shown below:

- To deactivate:

```
user@host# deactivate system services outbound-ssh client mist
user@host# commit
```

- To activate again:

```
user@host# activate system services outbound-ssh client mist
user@host# commit
```

10. If you are adding the SRX Series Firewall for the first time, do the following:
    - Delete the present Juniper Mist configuration from the firewall using the delete command.
    - Onboard the firewall again. For details on getting your SRX Series Firewall up and running in the Mist cloud, see Cloud-Ready SRX Firewalls .
    - Verify system service outbound-ssh and system connections using the following commands:
        - `show system services outbound-ssh`
        - `show system connections | grep 2200`

Troubleshoot SRX Series Firewalls Using Packet Captures

SRX Series Firewalls support manual packet captures (PCAP). Packet capture is a tool that helps you to analyze network traffic and troubleshoot network problems. It captures real-time data packets traveling over the network for monitoring and logging.

NOTE: SRX Series Firewalls do not support dynamic packet capture.

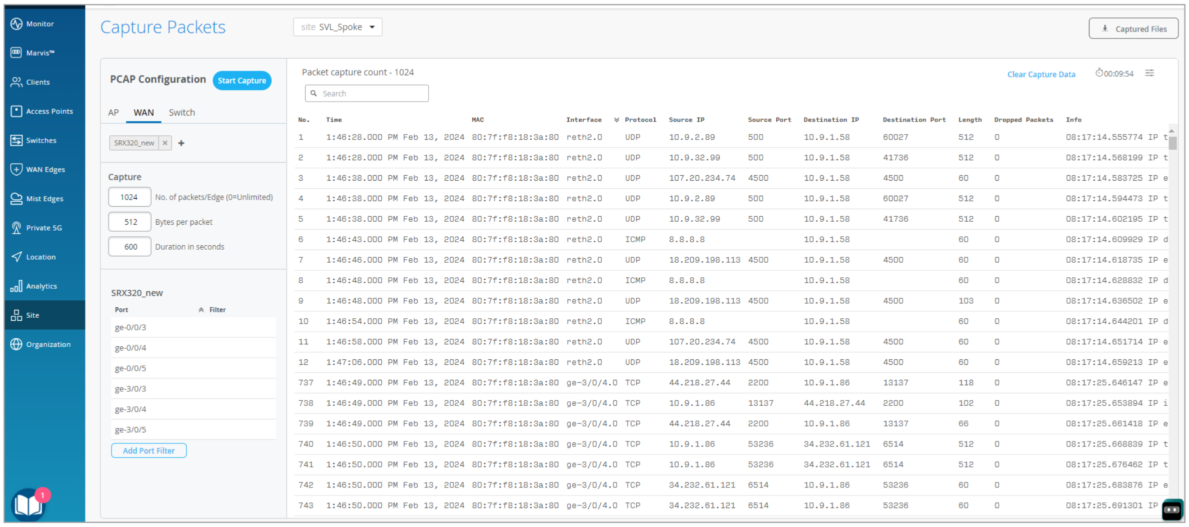
Manual packet captures are initiated by users from the WAN Edge Packet capture page.

To initiate manual PCAP for an SRX Series Firewall:

1. Go to **Site** > **WAN Edge Packet Captures**.

2. On the **WAN** tab, click **Add WAN Edge +** and select an SRX Series Firewall.

Figure 500: WAN Edge Packet Capture



SRX320_new

Capture

1024 No. of packets/Edge (0=Unlimited)

512 Bytes per packet

600 Duration in seconds

SRX320_new

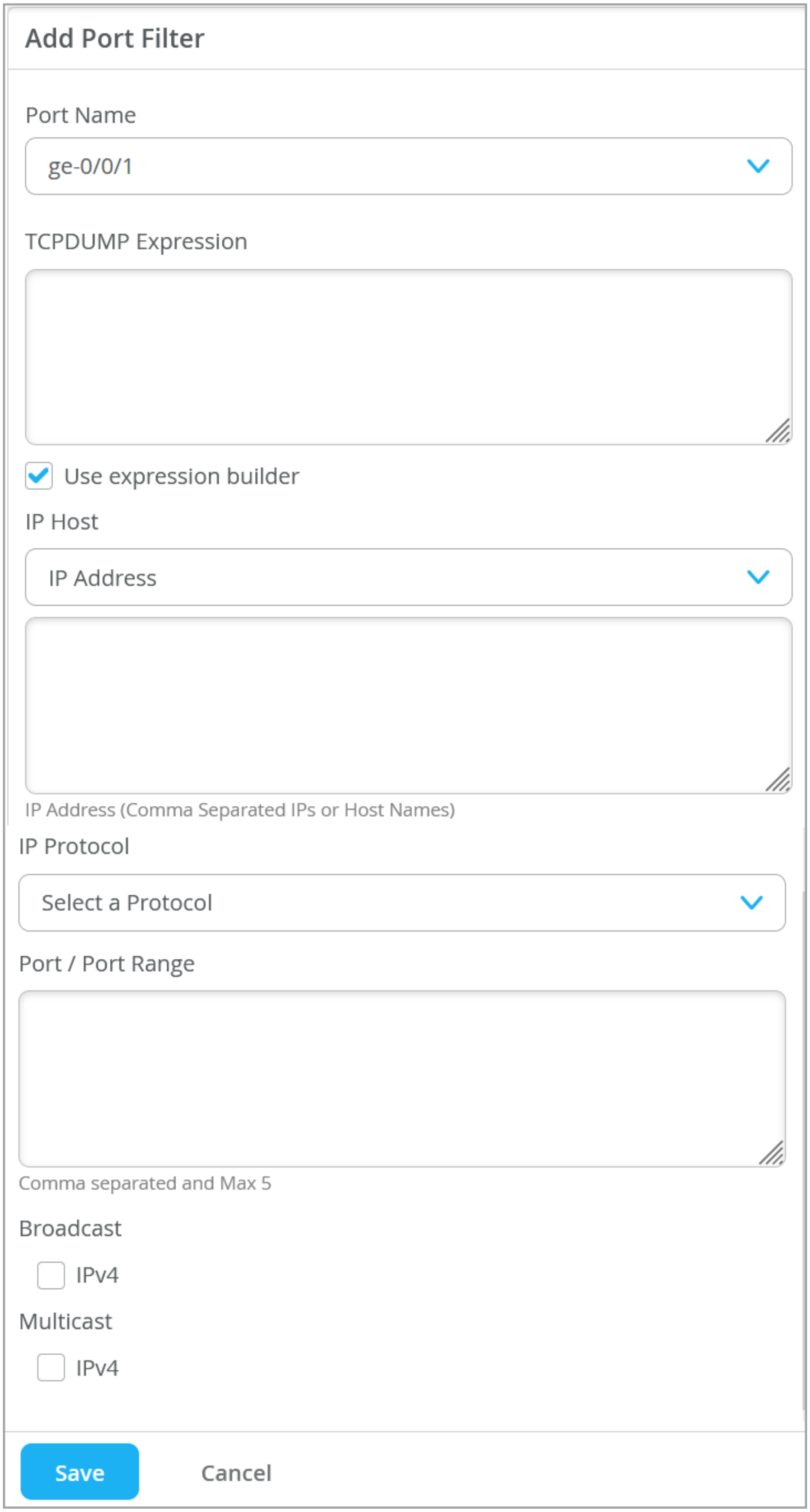
Port	Filter
ge-0/0/3	
ge-0/0/4	
ge-0/0/5	
ge-3/0/3	
ge-3/0/4	
ge-3/0/5	

Packet capture count - 1024

No.	Time	MAC	Interface	Protocol	Source IP	Source Port	Destination IP	Destination Port	Length	Dropped Packets	Info
1	1:46:28.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	reth2.0	UDP	10.9.2.89	500	10.9.1.58	60027	512	0	08:17:14.555774 IP t
2	1:46:28.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	reth2.0	UDP	10.9.32.99	500	10.9.1.58	41736	512	0	08:17:14.568199 IP t
3	1:46:38.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	reth2.0	UDP	107.20.234.74	4500	10.9.1.58	4500	60	0	08:17:14.583725 IP e
4	1:46:38.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	reth2.0	UDP	10.9.2.89	500	10.9.1.58	60027	512	0	08:17:14.594473 IP t
5	1:46:38.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	reth2.0	UDP	10.9.32.99	500	10.9.1.58	41736	512	0	08:17:14.602195 IP t
6	1:46:43.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	reth2.0	ICMP	8.8.8.8		10.9.1.58		60	0	08:17:14.609929 IP d
7	1:46:46.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	reth2.0	UDP	18.209.198.113	4500	10.9.1.58	4500	60	0	08:17:14.618735 IP e
8	1:46:48.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	reth2.0	ICMP	8.8.8.8		10.9.1.58		60	0	08:17:14.628832 IP d
9	1:46:48.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	reth2.0	UDP	18.209.198.113	4500	10.9.1.58	4500	103	0	08:17:14.636502 IP e
10	1:46:54.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	reth2.0	ICMP	8.8.8.8		10.9.1.58		60	0	08:17:14.644201 IP d
11	1:46:58.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	reth2.0	UDP	107.20.234.74	4500	10.9.1.58	4500	60	0	08:17:14.651714 IP e
12	1:47:06.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	reth2.0	UDP	18.209.198.113	4500	10.9.1.58	4500	60	0	08:17:14.659213 IP e
737	1:46:49.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	ge-3/0/4.0	TCP	44.218.27.44	2200	10.9.1.86	13137	118	0	08:17:25.646147 IP e
738	1:46:49.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	ge-3/0/4.0	TCP	10.9.1.86	13137	44.218.27.44	2200	102	0	08:17:25.653894 IP i
739	1:46:49.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	ge-3/0/4.0	TCP	44.218.27.44	2200	10.9.1.86	13137	66	0	08:17:25.661418 IP e
740	1:46:50.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	ge-3/0/4.0	TCP	10.9.1.86	53236	34.232.61.121	6514	512	0	08:17:25.668839 IP t
741	1:46:50.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	ge-3/0/4.0	TCP	10.9.1.86	53236	34.232.61.121	6514	512	0	08:17:25.676462 IP t
742	1:46:50.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	ge-3/0/4.0	TCP	34.232.61.121	6514	10.9.1.86	53236	60	0	08:17:25.683876 IP e
743	1:46:50.000 PM Feb 13, 2024	80:7f:f8:18:3a:80	ge-3/0/4.0	TCP	34.232.61.121	6514	10.9.1.86	53236	60	0	08:17:25.691301 IP

3. Specify the number of packets captured, packet size in bytes, and the duration of the capture session.

4. Use the **Add Port Filter** option to specify the port. In this pane, you can also enter filters in the TCPDUMP Expression text box.



Add Port Filter

Port Name

ge-0/0/1

TCPDUMP Expression

☑ Use expression builder

IP Host

IP Address

IP Address (Comma Separated IPs or Host Names)

IP Protocol

Select a Protocol

Port / Port Range

Comma separated and Max 5

Broadcast

□ IPv4

Multicast

□ IPv4

5. Optionally, select **Use Expression builder** to build the expression for packet capture. Expression builder is an interactive GUI tool to build custom filters in tcpdump syntax for use in the capture session. You can let the builder start the filter entry and then add to or delete from the entry manually. You can specify the following options:

   - IP host
   - Protocols
   - Port and port ranges
   - IP broadcast
   - IP multicast

   When you enter addresses and protocols into the expression builder, the portal automatically generates the tcpdump expression on the page. You can edit the expression if needed.

6. Click **Start Capture**. The packet capture content is streamed on the page.

7. You can download the file for offline analysis by clicking **Captured Files** on the top right side of the page.

See also: "Dynamic and Manual Packet Captures" on page 628.

SEE ALSO

Juniper Mist WAN Assurance Platform Considerations | 10

WAN Assurance Configuration Overview | 166

Juniper Mist WAN Assurance Configuration Hierarchy | 13

WAN Edge Testing Tools

IN THIS SECTION

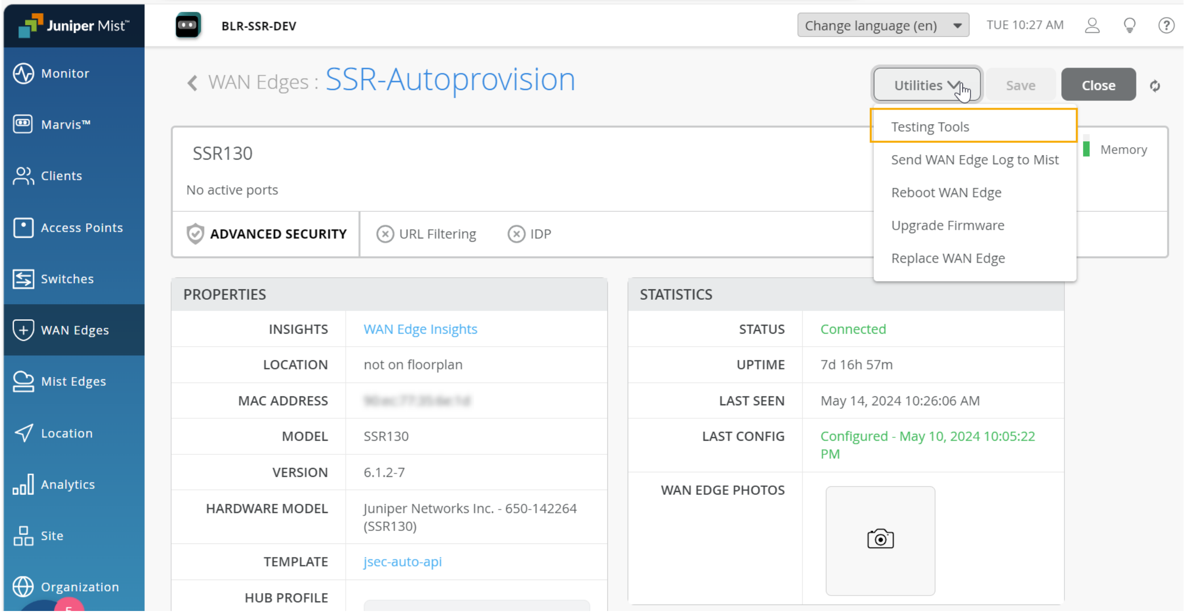
Juniper Mist™ portal provides testing tools that play crucial roles in maintaining network health and diagnosing issues. You can use the tools to:

- Identify network bottlenecks, latency, and packet loss.
- Check connectivity and measuring round-trip time.
- Identify the path taken by network traffic from source to destination for a specific application.
- Monitor BGP peering status and troubleshoot connectivity issues.

To use WAN Edge testing tools:

1. On Juniper Mist portal left navigation bar, select WAN Edges > WAN Edges.
2. On WAN Edge page, select the site from Site dropdown box. The page displays the WAN edge devices in the site.
3. Select the required device and click to open the device details page.
4. Click **Utilities** menu from the top right menu and select testing tool.

Figure 501: WAN Edge Testing Tool - Utilities Option



SSR130

No active ports

PROPERTIES

INSIGHTS	WAN Edge Insights
LOCATION	not on floorplan
MAC ADDRESS	[redacted]
MODEL	SSR130
VERSION	6.1.2-7
HARDWARE MODEL	Juniper Networks Inc. - 650-142264 (SSR130)
TEMPLATE	jsec-auto-api
HUB PROFILE	

STATISTICS

STATUS	Connected
UPTIME	7d 16h 57m
LAST SEEN	May 14, 2024 10:26:06 AM
LAST CONFIG	Configured - May 10, 2024 10:05:22 PM

5. The WAN Edge testing page opens. In this page, you can run tests using the following tools:
   - Ping
   - Traceroute

- BGP options (BGP summary, route advertisement details, and so on)
- Applications
- Address Resolution Protocol
- FIB

Lets learn how to use these tools for testing your WAN edge device connectivity.

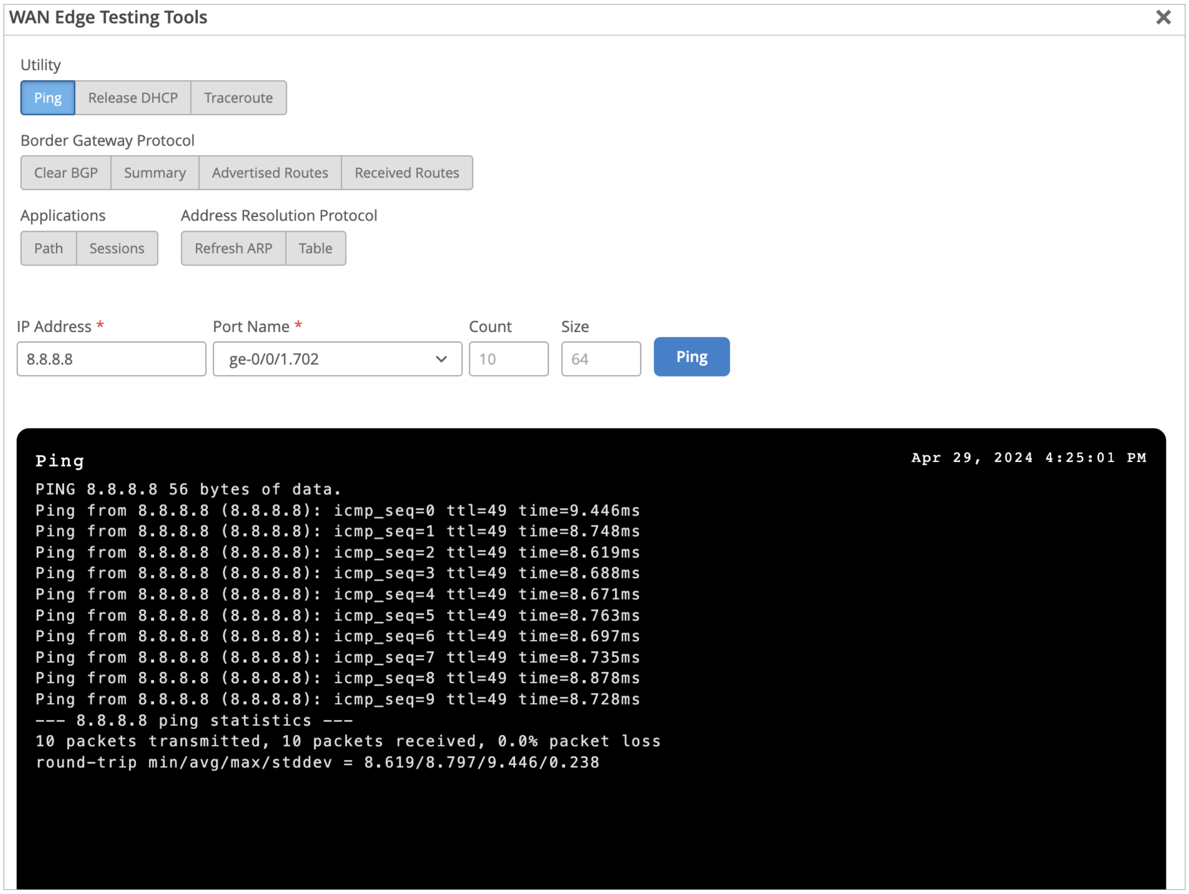
Testing Tools for Session Smart Routers

Ping Tests on Session Smart Routers

Use the Ping tool to send Internet Control Message Protocol (ICMP) echo requests to a specified host. You can use this command to check if a particular host is reachable at a particular IP address.

1. In WAN Edge Testing tools window, click **Ping**.
2. Enter the following options:
   - **IP Address**—Enter the IP address or hostname of the remote system to ping.
   - **Port Name**—Select the port to initiate the ping request.
   - **Count**—Enter the number of ping requests to send. The range of values is `1` through `100`.
   - **Size**—Enter the size of ping request packets. The range of values, in bytes, is `64` through `65,535`.
3. Click **Ping** option.

Figure 502: Check Connectivity to Host Using Ping



IP Address * 8.8.8.8

Port Name * ge-0/0/1.702

Count 10

Size 64

```
Ping                                                                    Apr 29, 2024 4:25:01 PM
PING 8.8.8.8 56 bytes of data.
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=0 ttl=49 time=9.446ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=1 ttl=49 time=8.748ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=2 ttl=49 time=8.619ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=3 ttl=49 time=8.688ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=4 ttl=49 time=8.671ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=5 ttl=49 time=8.763ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=6 ttl=49 time=8.697ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=7 ttl=49 time=8.735ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=8 ttl=49 time=8.878ms
Ping from 8.8.8.8 (8.8.8.8): icmp_seq=9 ttl=49 time=8.728ms
--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 8.619/8.797/9.446/0.238
```

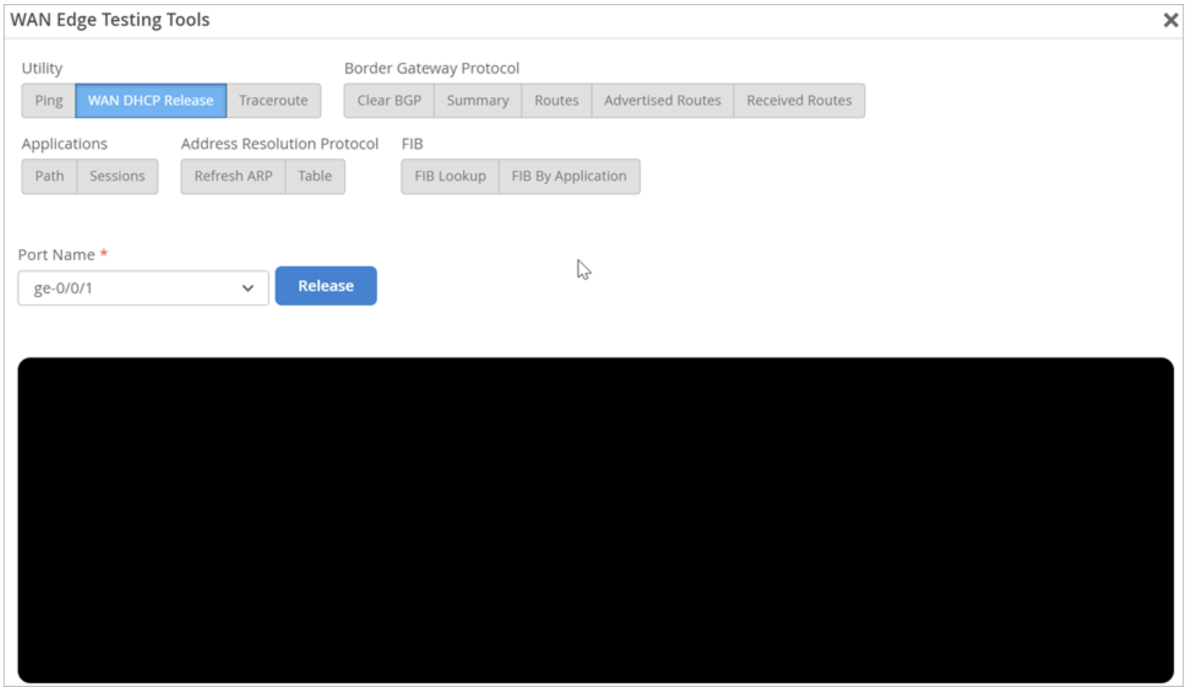
The output displays the details of hops as IP addresses in the path to a given destination.

Release WAN DHCP

You can release the DHCP lease on a WAN Edge device. This option lets you release client devices from their current DHCP lease.

1. In WAN Edge Testing tools window, click **WAN DHCP Release**.
2. Select the port name from **Port Name** drop-down and click **Release**.

Figure 503: WAN DHCP Release (Session Smart Routers)



Port Name *: ge-0/0/1

The output displays the details of response to your request.

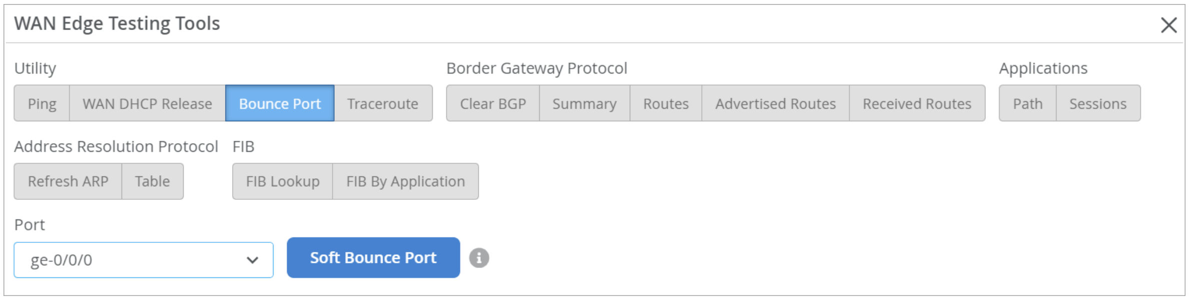
Bounce Port

Use the *Bounce Port* tool to run soft bounce port test on your Session Smart Router.

1. In WAN Edge Testing tools window, click **Bounce Port**.

2. Specify the interface name (example: ge-0/0/0).

Figure 504: Bounce Port (Session Smart Router)



Port: ge-0/0/0

3. Click **Soft Bounce Port**. This test provisionally takes the port down and brings the port up without causing the external physical link to change. The connected devices will not see a link state change.

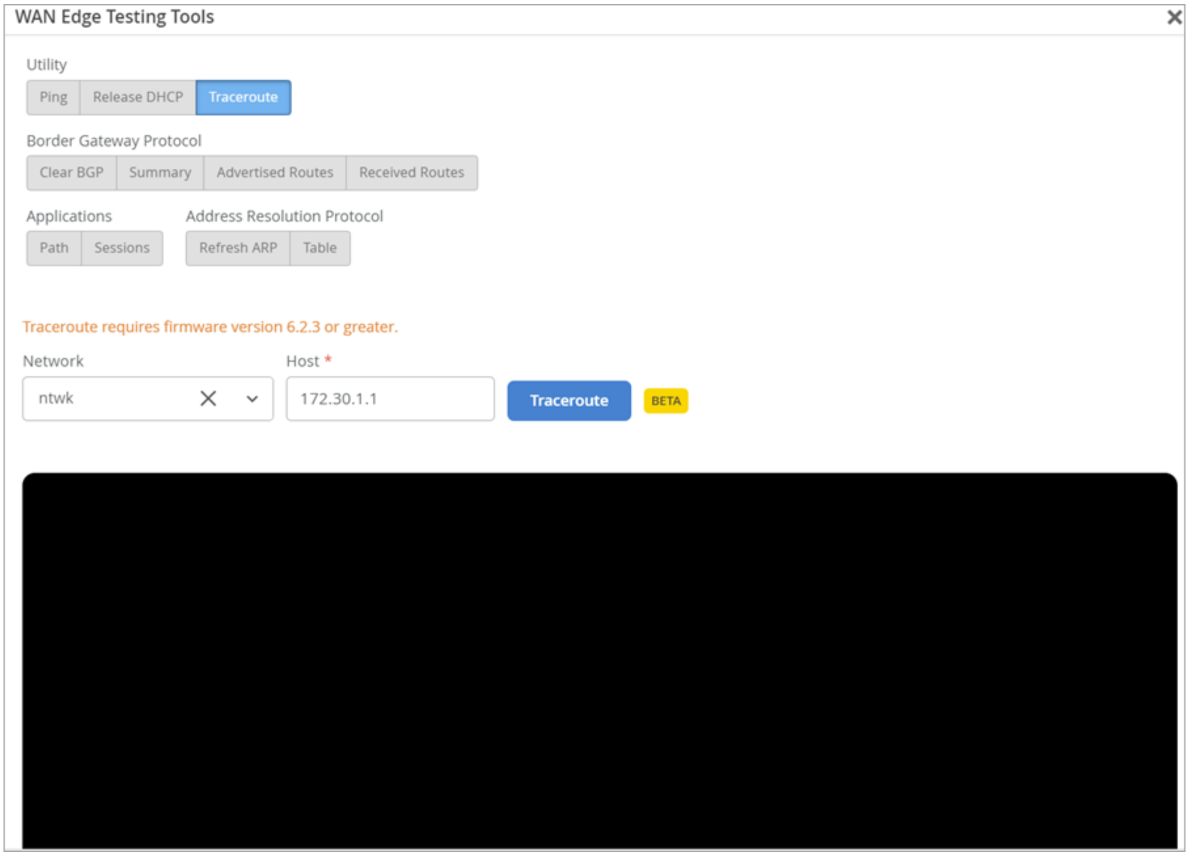
Traceroute on Session Smart Routers

Traceroute is a network diagnostic tool that traces the path an IP packet takes across networks, revealing the sequence of routers (hops) it takes along the way

To initiate traceroute utility:

1. In WAN Edge Testing tools window, click **Traceroute**.
2. Enter the following options:
   - Network—Select the source network from where you want to trace packet.
   - Host—Enter the IP address for the destination site.
3. Click **Traceroute** option.

Figure 505: Initiate Traceroute (Session Smart Routers)



Traceroute requires firmware version 6.2.3 or greater.

Network: ntwk

Host *: 172.30.1.1

The output displays the details of hops as IP addresses in the path to a given destination.

Border Gateway Protocol Test Tools for Session Smart Routers

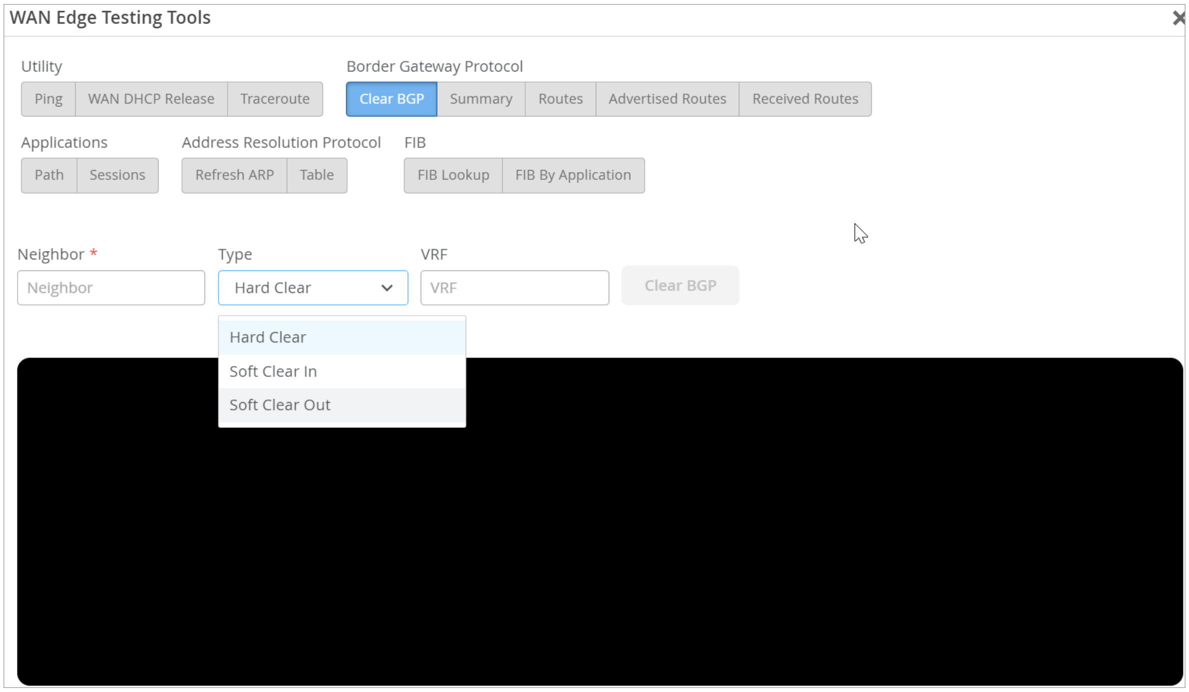
You can perform the following testing related to a BGP session:

- Display BGP routes advertised
- Display BGP routes received
- Display BGP summary
- Display BGP Routes
- Clear BGP routes

Use the following options to perform tests:

- Use **Clear BGP** option to clear sessions with all BGP neighbors or with specific BGP peer.

Figure 506: Clear BGP Sessions (Session Smart Routers)

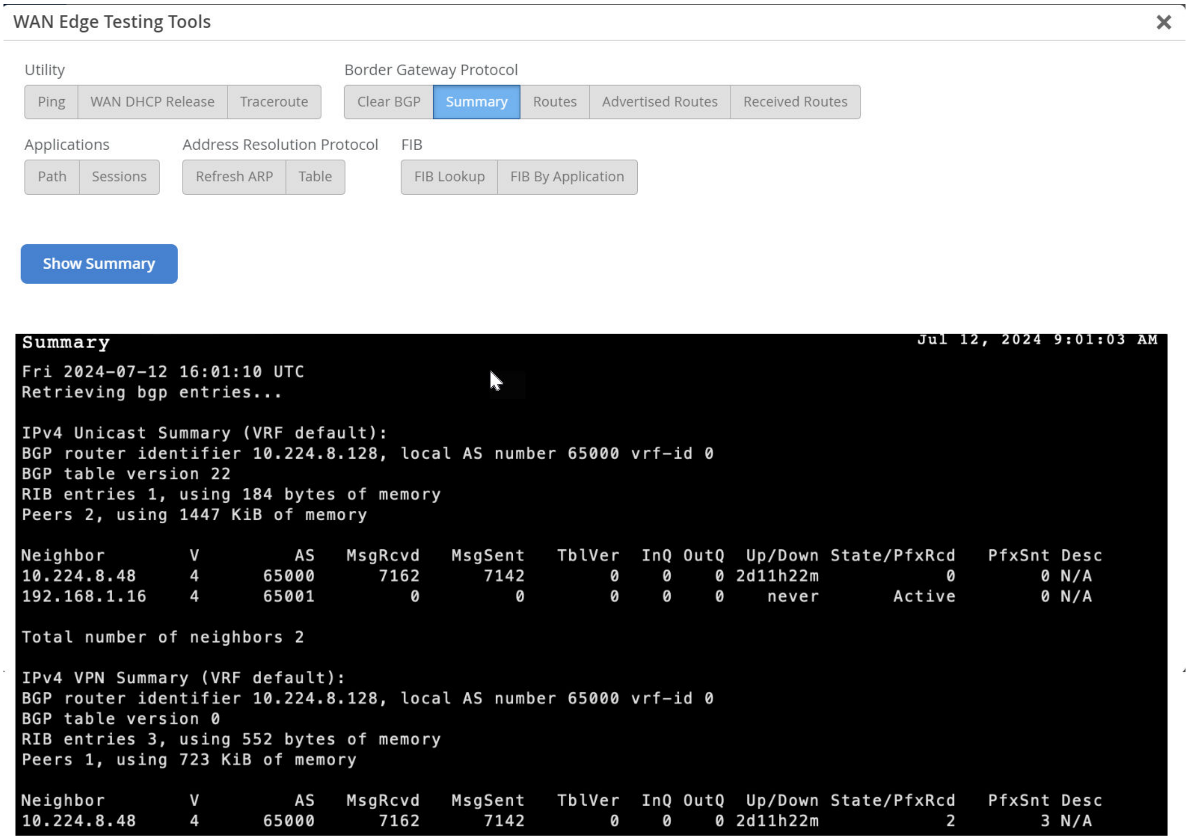


You have the following options when clearing BGP routes:

- **Neighbor**—Select all to or IP address of a BGP peer. Apply this command only to the specified neighbor.
- **Type**—Specify how you want to reset a BGP session.

    - **Hard Clear**—A hard reset terminates the specified peering sessions. This action drops the TCP connection to the neighbors. This setting is not recommended.
    - **Soft Clear In**—Inbound soft reset on the connections
    - **Soft Clear Out**—Outbound soft reset on the outgoing connections
  - **VRF**—(Optional) Specify virtual routing and forwarding (VRF). The action applies only to neighbors for the specified routing instance.
- Use **Summary** option to display summary information about BGP and its neighbors.

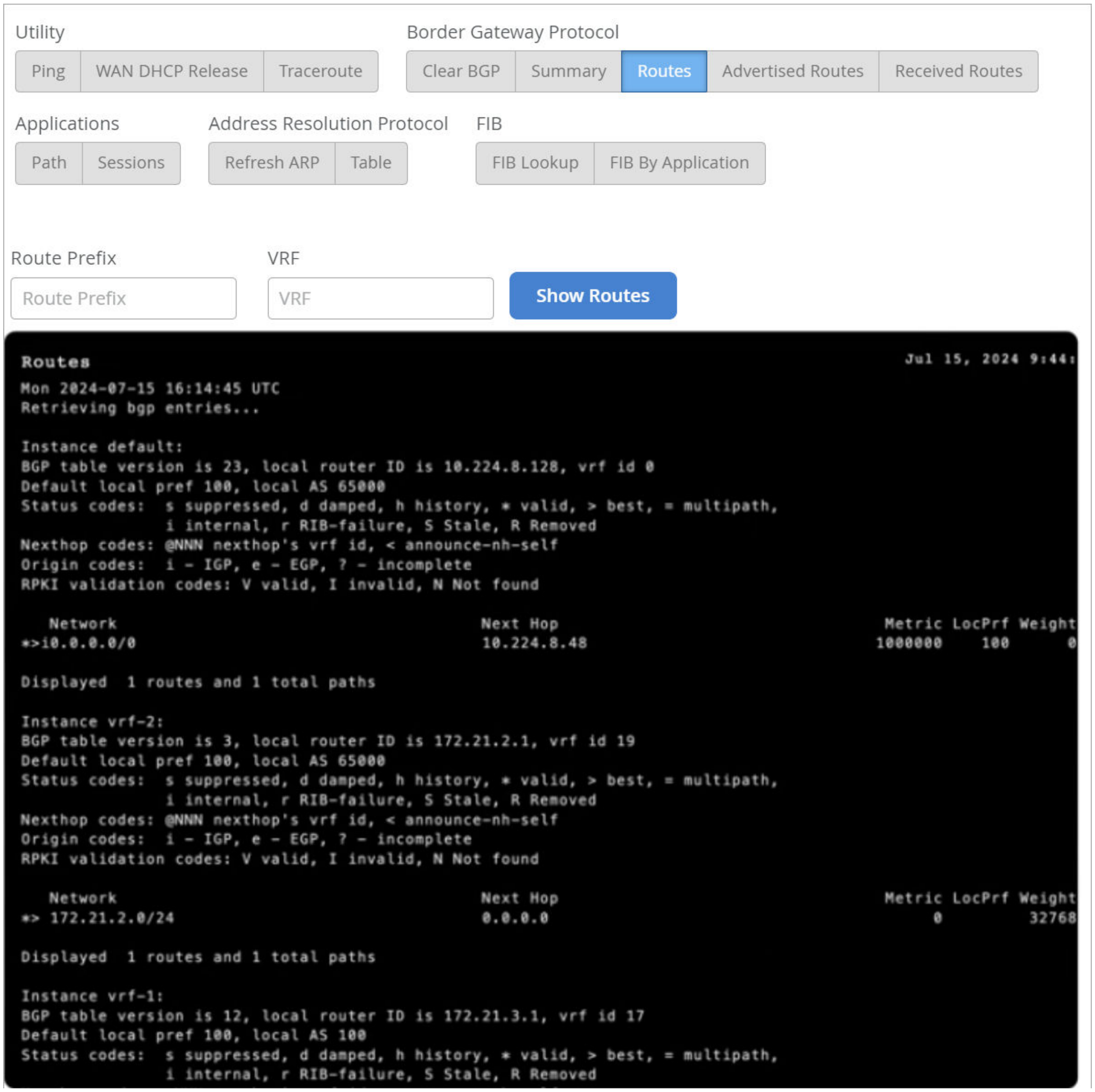
Figure 507: View BGP Summary (Session Smart Routers)



```
Summary                                                                         Jul 12, 2024 9:01:03 AM
Fri 2024-07-12 16:01:10 UTC
Retrieving bgp entries...

IPv4 Unicast Summary (VRF default):
BGP router identifier 10.224.8.128, local AS number 65000 vrf-id 0
BGP table version 22
RIB entries 1, using 184 bytes of memory
Peers 2, using 1447 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd   PfxSnt Desc
10.224.8.48     4      65000      7162      7142        0    0    0 2d11h22m            0        0 N/A
192.168.1.16    4      65001         0         0        0    0    0    never       Active        0 N/A

Total number of neighbors 2

IPv4 VPN Summary (VRF default):
BGP router identifier 10.224.8.128, local AS number 65000 vrf-id 0
BGP table version 0
RIB entries 3, using 552 bytes of memory
Peers 1, using 723 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd   PfxSnt Desc
10.224.8.48     4      65000      7162      7142        0    0    0 2d11h22m            2        3 N/A
```

- Use **Routes** option to display BGP routes details. You can use this option to debug the BGP routing table. It shows how the sent or received prefixes from various neighbors are being handled and processed in the BGP table.

Figure 508: View BGP Routes (Session Smart Routers)



Route Prefix: Route Prefix

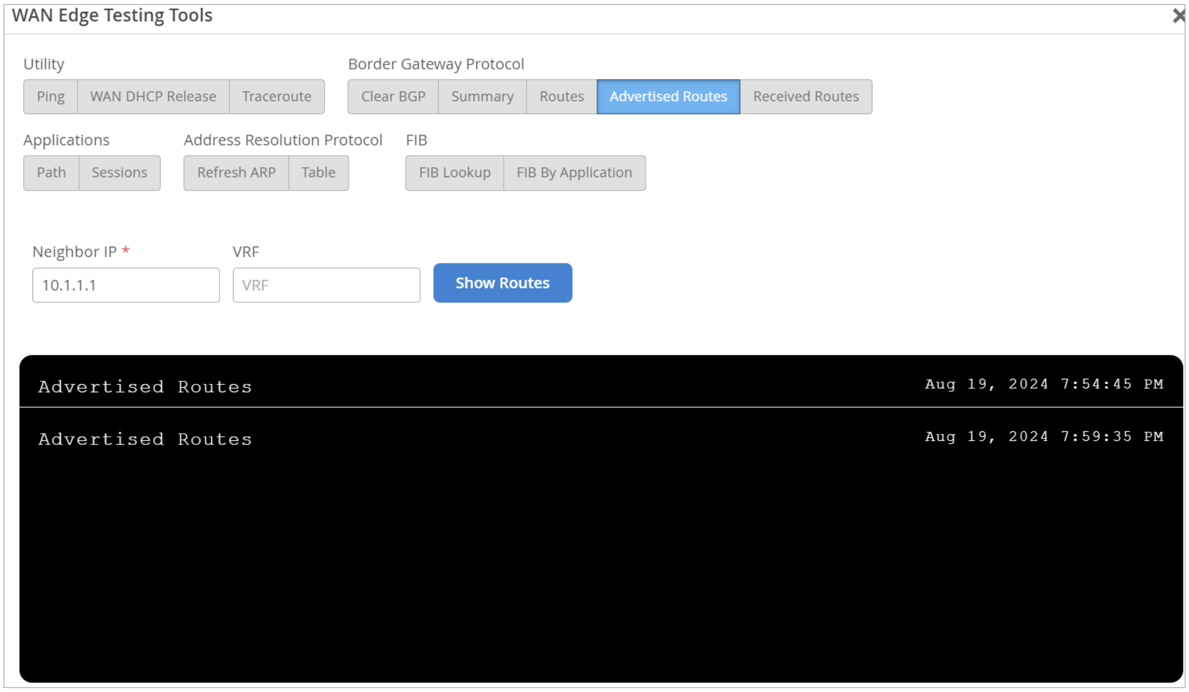
VRF: VRF

```
Routes                                                                                  Jul 15, 2024 9:44:
Mon 2024-07-15 16:14:45 UTC
Retrieving bgp entries...

Instance default:
BGP table version is 23, local router ID is 10.224.8.128, vrf id 0
Default local pref 100, local AS 65000
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network                                      Next Hop                                  Metric LocPrf Weight
*>i0.0.0.0/0                                    10.224.8.48                              1000000    100      0

Displayed  1 routes and 1 total paths

Instance vrf-2:
BGP table version is 3, local router ID is 172.21.2.1, vrf id 19
Default local pref 100, local AS 65000
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network                                      Next Hop                                  Metric LocPrf Weight
*> 172.21.2.0/24                                0.0.0.0                                        0         32768

Displayed  1 routes and 1 total paths

Instance vrf-1:
BGP table version is 12, local router ID is 172.21.3.1, vrf id 17
Default local pref 100, local AS 100
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
```

Enter the route prefix or VRF (optional) and click **Show Routes**. The output display the routing information as it was received through a particular neighbor using BGP.

- Use **Advertised Routes** option to display all routes that have been advertised to the specified neighbor.

Figure 509: BGP Advertized Routes (Session Smart Routers)



Neighbor IP * 10.1.1.1

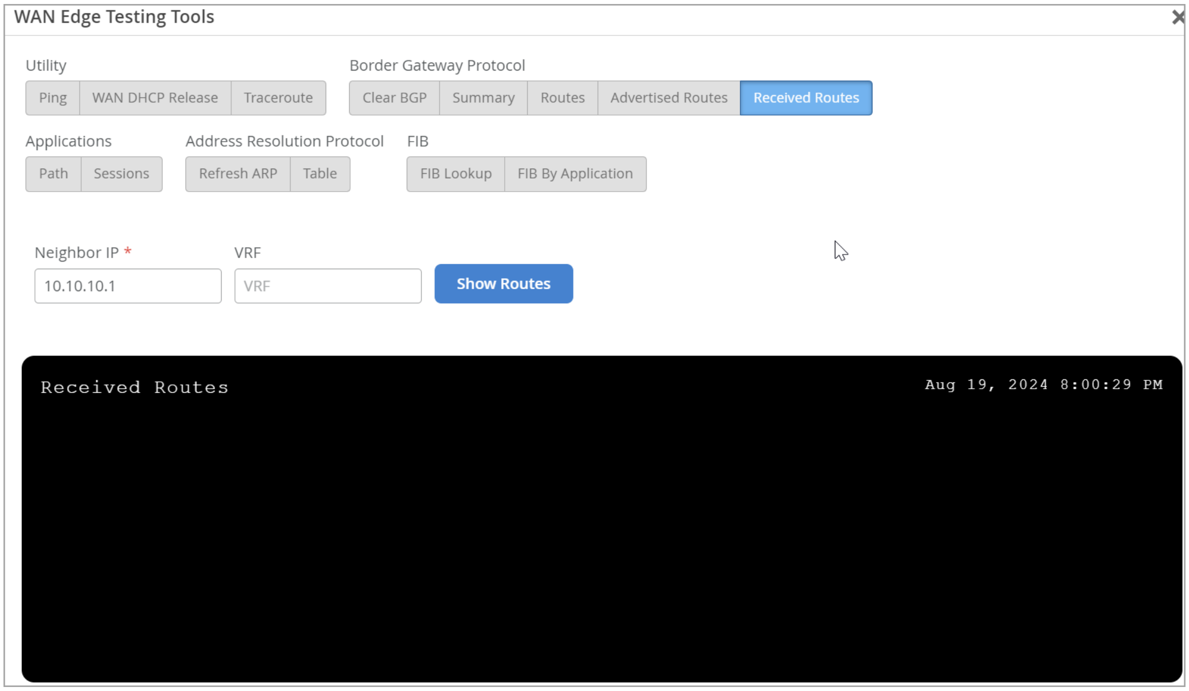
VRF

```
Advertised Routes                                    Aug 19, 2024 7:54:45 PM
Advertised Routes                                    Aug 19, 2024 7:59:35 PM
```

Enter the IP address of neighbor router and click **Show BGP Advertised Routes**. Output displays the routes that your device has advertised to the peer router during the current BGP session.

- Use **Received Routes** option to display all received routes from the specified neighbor.

Figure 510: BGP Received Routes (Session Smart Routers)



WAN Edge Testing Tools

Neighbor IP *: 10.10.10.1

VRF: VRF

```
Received Routes                                    Aug 19, 2024 8:00:29 PM
```

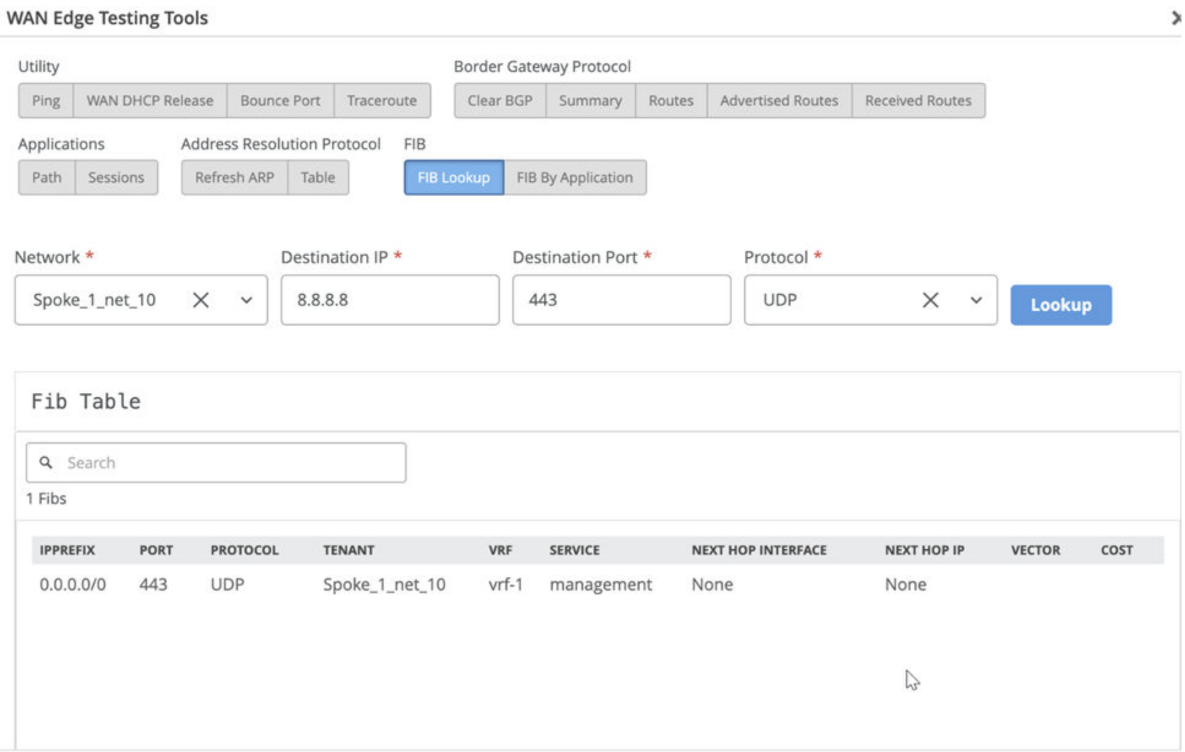
Enter the IP address of neighbor router and click **Show BGP Received Routes**. The output display the routing information as it was received through a particular neighbor using BGP.

FIB Testing Tool

Use this information to look up the forwarding information base (FIB) data associated with the selected WAN Edge device. You can also look up the FIB data by application.

- In WAN Edge Testing tools window, click **FIB Lookup**.
- Enter the following options and click **Show FIB**:
  - **Network**—Name of the network to perform the FIB lookup.
  - **Destination Port**—Destination port of the route.
  - **Destination IP**—Destination IP address of the route.
  - **Protocol**—Transport protocol of the packet.

Figure 511: FIB Lookup



Network * Spoke_1_net_10

Destination IP * 8.8.8.8

Destination Port * 443

Protocol * UDP

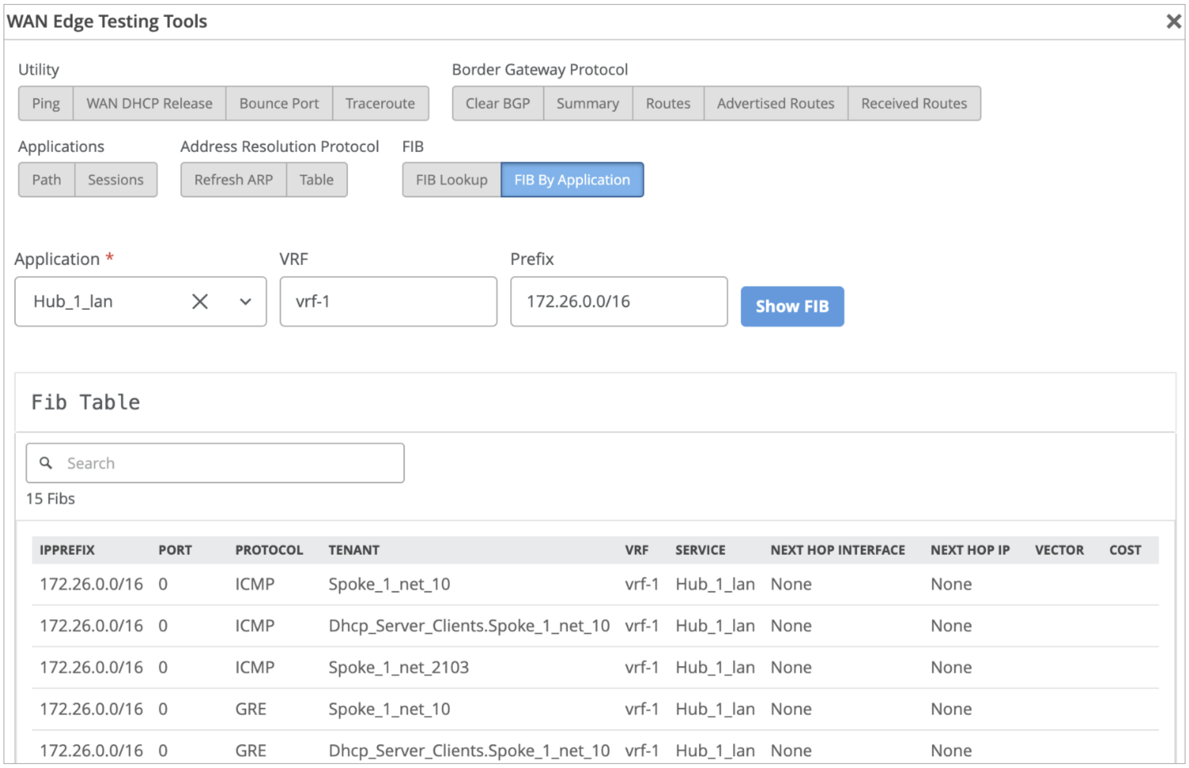
Fib Table

1 Fibs

IPPREFIX	PORT	PROTOCOL	TENANT	VRF	SERVICE	NEXT HOP INTERFACE	NEXT HOP IP	VECTOR	COST
0.0.0.0/0	443	UDP	Spoke_1_net_10	vrf-1	management	None	None		

- If you select **FIB By Application**, enter the following details to filter by and click **Show FIB**:
  - **Application**—Name of the application to perform the FIB lookup for. Applications represent traffic destinations.
  - **VRF**—Virtual routing and forwarding instance.
  - **Prefix**—IP address prefix.

Figure 512: FIB By Applications



Application * Hub_1_lan

VRF vrf-1

Prefix 172.26.0.0/16

Fib Table

15 Fibs

IPPREFIX	PORT	PROTOCOL	TENANT	VRF	SERVICE	NEXT HOP INTERFACE	NEXT HOP IP	VECTOR	COST
172.26.0.0/16	0	ICMP	Spoke_1_net_10	vrf-1	Hub_1_lan	None	None		
172.26.0.0/16	0	ICMP	Dhcp_Server_Clients.Spoke_1_net_10	vrf-1	Hub_1_lan	None	None		
172.26.0.0/16	0	ICMP	Spoke_1_net_2103	vrf-1	Hub_1_lan	None	None		
172.26.0.0/16	0	GRE	Spoke_1_net_10	vrf-1	Hub_1_lan	None	None		
172.26.0.0/16	0	GRE	Dhcp_Server_Clients.Spoke_1_net_10	vrf-1	Hub_1_lan	None	None		

The table displays entries matching the specified application, VRF, or IP address prefix.

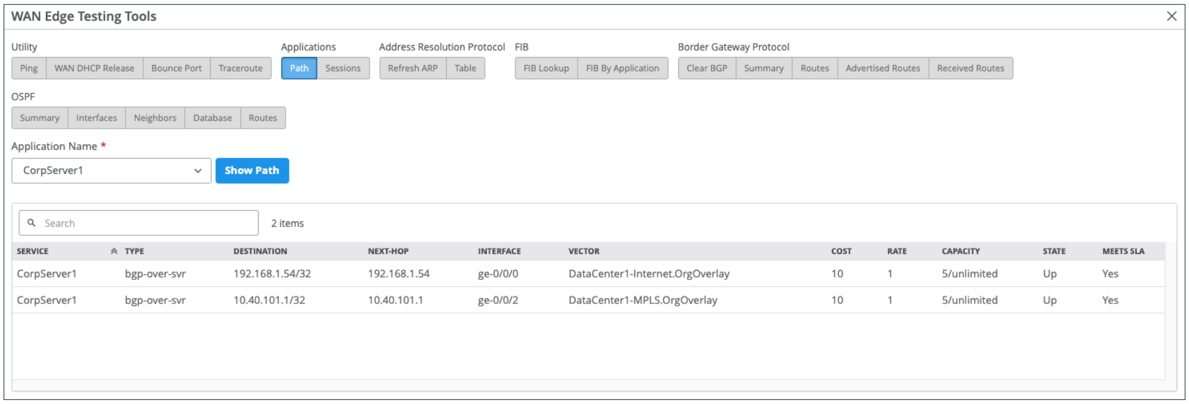
Applications for Session Smart Routers

You can use the Applications section to see the Path information for the selected application. You can also display the sessions for an application, as well as delete them.

1. In the WAN Edge Testing Tools window, under Applications, select **Path**.

2. Select the appropriate Application Name, then select **Show Path**.

Figure 513: Show Path



Application Name * CorpServer1

2 items

SERVICE	TYPE	DESTINATION	NEXT-HOP	INTERFACE	VECTOR	COST	RATE	CAPACITY	STATE	MEETS SLA
CorpServer1	bgp-over-svr	192.168.1.54/32	192.168.1.54	ge-0/0/0	DataCenter1-Internet.OrgOverlay	10	1	5/unlimited	Up	Yes
CorpServer1	bgp-over-svr	10.40.101.1/32	10.40.101.1	ge-0/0/2	DataCenter1-MPLS.OrgOverlay	10	1	5/unlimited	Up	Yes

The following information about the path will display:

Table 93: Show Path

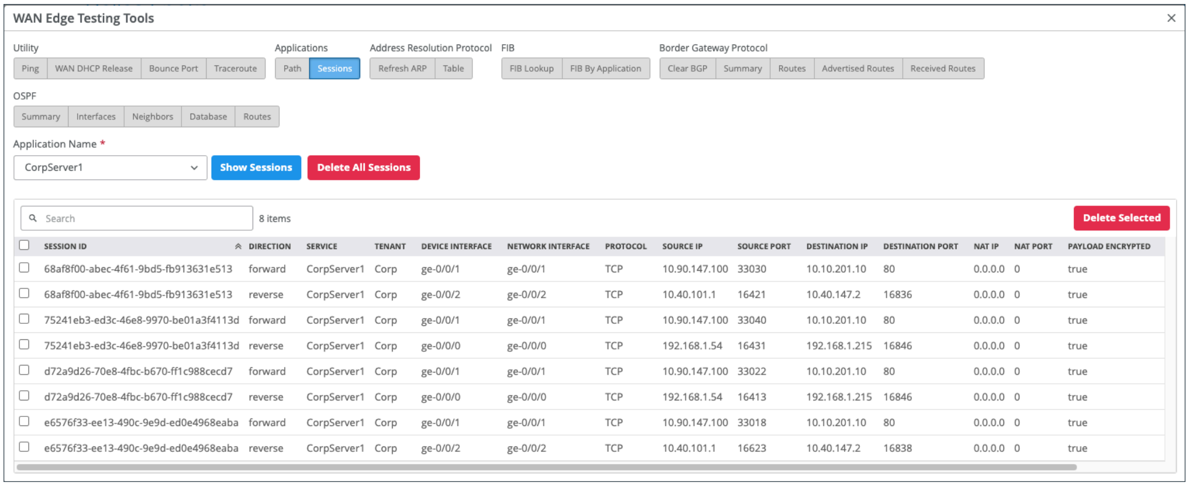
Column	Definition
Service	The selected application name.
Type	The type of path.
Destination	The destination IP address for packets traveling on the path.
Next-hop	The next hop address where the Session Smart Router will route the session.
Interface	The name of the network interface that will be used to send the route along the path.
Vector	The name of the vector assigned to the path. The vector is associated with a cost that indicates path preference.
Cost	Indicates path preference.

Table 93: Show Path *(Continued)*

Column	Definition
Rate	A snapshot of the rate at which sessions are created for the service.
Capacity	The load balancing capacity that has been set for the path.
State	The current state of the path (Up or Down).
Meet SLA	Whether the path is meeting the minimum required Service Level Agreement (Yes or No).

The Sessions testing tool has been enhanced with options to view session details. You can also delete sessions if needed. Deleting a session may be useful in situations where a stuck session was created and traffic is not able to be sent in both directions on the path due to upstream problems. These options help in debugging scenarios.

1. In the WAN Edge Testing tools window, under Applications, select **Sessions**.
2. Select an Application Name, then select **Show Sessions**.



Application Name *
CorpServer1

8 items

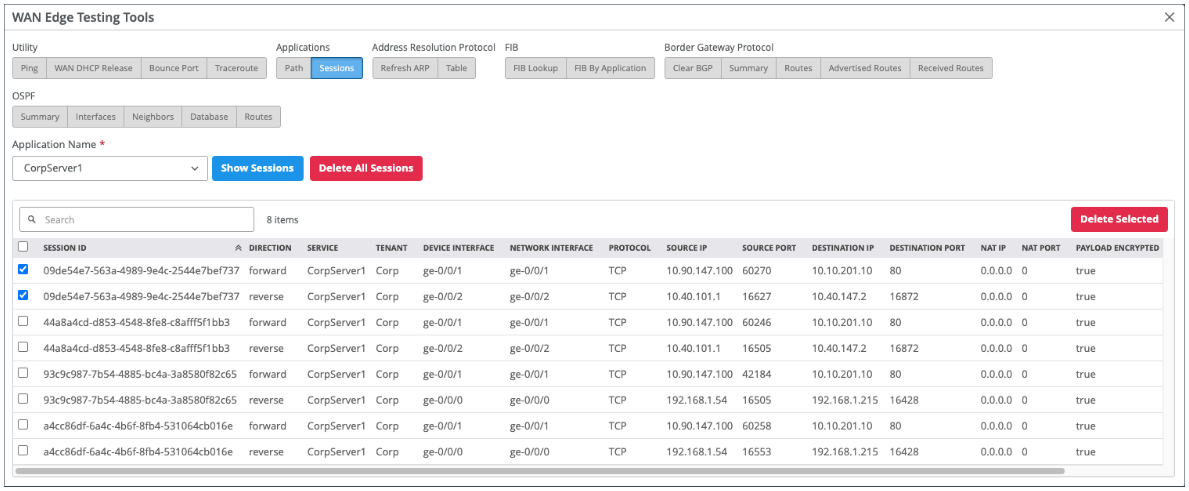
□	SESSION ID	DIRECTION	SERVICE	TENANT	DEVICE INTERFACE	NETWORK INTERFACE	PROTOCOL	SOURCE IP	SOURCE PORT	DESTINATION IP	DESTINATION PORT	NAT IP	NAT PORT	PAYLOAD ENCRYPTED
□	68af8f00-abec-4f61-9bd5-fb913631e513	forward	CorpServer1	Corp	ge-0/0/1	ge-0/0/1	TCP	10.90.147.100	33030	10.10.201.10	80	0.0.0.0	0	true
□	68af8f00-abec-4f61-9bd5-fb913631e513	reverse	CorpServer1	Corp	ge-0/0/2	ge-0/0/2	TCP	10.40.101.1	16421	10.40.147.2	16836	0.0.0.0	0	true
□	75241eb3-ed3c-46e8-9970-be01a3f4113d	forward	CorpServer1	Corp	ge-0/0/1	ge-0/0/1	TCP	10.90.147.100	33040	10.10.201.10	80	0.0.0.0	0	true
□	75241eb3-ed3c-46e8-9970-be01a3f4113d	reverse	CorpServer1	Corp	ge-0/0/0	ge-0/0/0	TCP	192.168.1.54	16431	192.168.1.215	16846	0.0.0.0	0	true
□	d72a9d26-70e8-4fbc-b670-ff1c988cecd7	forward	CorpServer1	Corp	ge-0/0/1	ge-0/0/1	TCP	10.90.147.100	33022	10.10.201.10	80	0.0.0.0	0	true
□	d72a9d26-70e8-4fbc-b670-ff1c988cecd7	reverse	CorpServer1	Corp	ge-0/0/0	ge-0/0/0	TCP	192.168.1.54	16413	192.168.1.215	16846	0.0.0.0	0	true
□	e6576f33-ee13-490c-9e9d-ed0e4968eaba	forward	CorpServer1	Corp	ge-0/0/1	ge-0/0/1	TCP	10.90.147.100	33018	10.10.201.10	80	0.0.0.0	0	true
□	e6576f33-ee13-490c-9e9d-ed0e4968eaba	reverse	CorpServer1	Corp	ge-0/0/2	ge-0/0/2	TCP	10.40.101.1	16623	10.40.147.2	16838	0.0.0.0	0	true

The following information about the path will display:

Column	Definition
Session ID	The session identifier.
Direction	The direction the flow is heading (forward or reverse).
Service	The selected application name.
Tenant	The name of the tenant attempting to access the service.
Device Interface	The name of the device interface the flow is arriving on.
Network Interface	The name of the network interface the flow is arriving on.
Protocol	Which routing protocol the flow is using (TCP, UDP, etc).
Source IP	The source IP address for the flow.
Source Port	The source port for the flow.
Destination IP	Represents the destination IP address of the flow.
Destination Port	Represents the destination port for the flow.
NAT IP	The Network Address Translated destination IP address.
NAT Port	The Network Address Translated destination port.
Payload Encrypted	True or False.

3. To delete a session, select the checkbox to the left of the session, then click the **Delete Selected** button.

Figure 514: Show Sessions and Delete Sessions



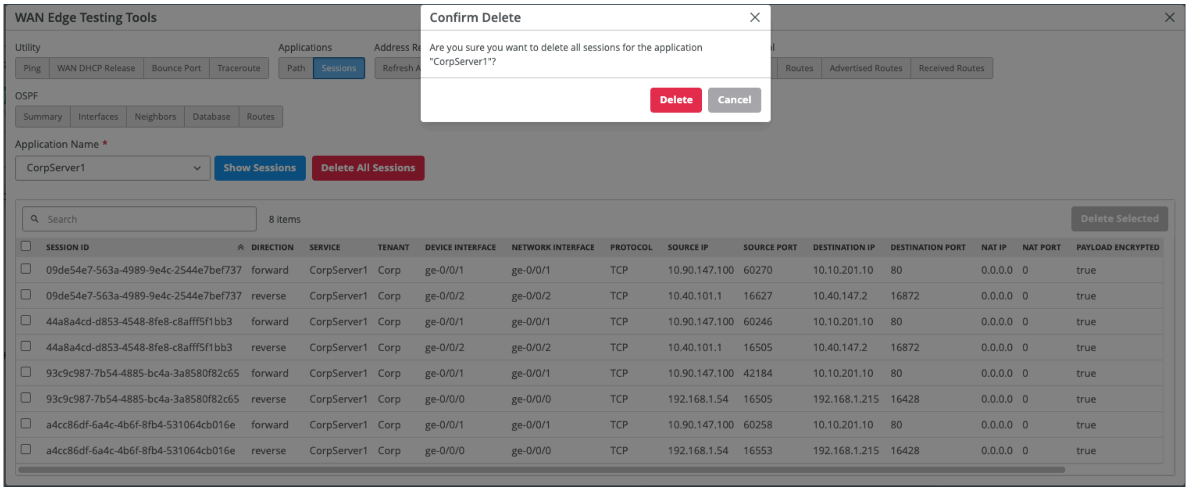
Application Name * CorpServer1

8 items

☐	SESSION ID	DIRECTION	SERVICE	TENANT	DEVICE INTERFACE	NETWORK INTERFACE	PROTOCOL	SOURCE IP	SOURCE PORT	DESTINATION IP	DESTINATION PORT	NAT IP	NAT PORT	PAYLOAD ENCRYPTED
☑	09de54e7-563a-4989-9e4c-2544e7bef737	forward	CorpServer1	Corp	ge-0/0/1	ge-0/0/1	TCP	10.90.147.100	60270	10.10.201.10	80	0.0.0.0	0	true
☑	09de54e7-563a-4989-9e4c-2544e7bef737	reverse	CorpServer1	Corp	ge-0/0/2	ge-0/0/2	TCP	10.40.101.1	16627	10.40.147.2	16872	0.0.0.0	0	true
☐	44a8a4cd-d853-4548-8fe8-c8afff5f1bb3	forward	CorpServer1	Corp	ge-0/0/1	ge-0/0/1	TCP	10.90.147.100	60246	10.10.201.10	80	0.0.0.0	0	true
☐	44a8a4cd-d853-4548-8fe8-c8afff5f1bb3	reverse	CorpServer1	Corp	ge-0/0/2	ge-0/0/2	TCP	10.40.101.1	16505	10.40.147.2	16872	0.0.0.0	0	true
☐	93c9c987-7b54-4885-bc4a-3a8580f82c65	forward	CorpServer1	Corp	ge-0/0/1	ge-0/0/1	TCP	10.90.147.100	42184	10.10.201.10	80	0.0.0.0	0	true
☐	93c9c987-7b54-4885-bc4a-3a8580f82c65	reverse	CorpServer1	Corp	ge-0/0/0	ge-0/0/0	TCP	192.168.1.54	16505	192.168.1.215	16428	0.0.0.0	0	true
☐	a4cc86df-6a4c-4b6f-8fb4-531064cb016e	forward	CorpServer1	Corp	ge-0/0/1	ge-0/0/1	TCP	10.90.147.100	60258	10.10.201.10	80	0.0.0.0	0	true
☐	a4cc86df-6a4c-4b6f-8fb4-531064cb016e	reverse	CorpServer1	Corp	ge-0/0/0	ge-0/0/0	TCP	192.168.1.54	16553	192.168.1.215	16428	0.0.0.0	0	true

4. To delete all sessions, select the **Delete All Sessions** button. You will be asked to confirm the delete action. **Click Delete.**

Figure 515: Delete All Sessions



Are you sure you want to delete all sessions for the application "CorpServer1"?

Application Name * CorpServer1

8 items

☐	SESSION ID	DIRECTION	SERVICE	TENANT	DEVICE INTERFACE	NETWORK INTERFACE	PROTOCOL	SOURCE IP	SOURCE PORT	DESTINATION IP	DESTINATION PORT	NAT IP	NAT PORT	PAYLOAD ENCRYPTED
☐	09de54e7-563a-4989-9e4c-2544e7bef737	forward	CorpServer1	Corp	ge-0/0/1	ge-0/0/1	TCP	10.90.147.100	60270	10.10.201.10	80	0.0.0.0	0	true
☐	09de54e7-563a-4989-9e4c-2544e7bef737	reverse	CorpServer1	Corp	ge-0/0/2	ge-0/0/2	TCP	10.40.101.1	16627	10.40.147.2	16872	0.0.0.0	0	true
☐	44a8a4cd-d853-4548-8fe8-c8afff5f1bb3	forward	CorpServer1	Corp	ge-0/0/1	ge-0/0/1	TCP	10.90.147.100	60246	10.10.201.10	80	0.0.0.0	0	true
☐	44a8a4cd-d853-4548-8fe8-c8afff5f1bb3	reverse	CorpServer1	Corp	ge-0/0/2	ge-0/0/2	TCP	10.40.101.1	16505	10.40.147.2	16872	0.0.0.0	0	true
☐	93c9c987-7b54-4885-bc4a-3a8580f82c65	forward	CorpServer1	Corp	ge-0/0/1	ge-0/0/1	TCP	10.90.147.100	42184	10.10.201.10	80	0.0.0.0	0	true
☐	93c9c987-7b54-4885-bc4a-3a8580f82c65	reverse	CorpServer1	Corp	ge-0/0/0	ge-0/0/0	TCP	192.168.1.54	16505	192.168.1.215	16428	0.0.0.0	0	true
☐	a4cc86df-6a4c-4b6f-8fb4-531064cb016e	forward	CorpServer1	Corp	ge-0/0/1	ge-0/0/1	TCP	10.90.147.100	60258	10.10.201.10	80	0.0.0.0	0	true
☐	a4cc86df-6a4c-4b6f-8fb4-531064cb016e	reverse	CorpServer1	Corp	ge-0/0/0	ge-0/0/0	TCP	192.168.1.54	16553	192.168.1.215	16428	0.0.0.0	0	true

Address Resolution Protocol for Session Smart Routers

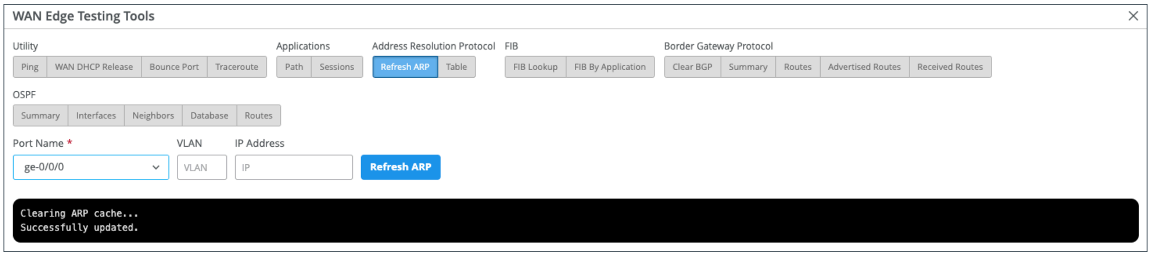
The Refresh ARP tool is typically used during troubleshooting scenarios to remove Address Resolution Protocol (ARP) entries from a Session Smart Router or node's ARP cache. The tool has multiple filters, allowing administrators to specify which entry to remove.

1. In the WAN Edge Testing Tools window, under Address Resolution Protocol, select **Refresh ARP**.

2. Enter the following details to filter by and click **Refresh ARP:**:

- **Port Name**—If you select a port name and then click Refresh ARP, it refreshes all ARP Entries for that port.
- **VLAN**—By specifying a VLAN tag in addition to the Port Name, this enables you to refresh any ARP entries with that port and VLAN tag.
- **IP Address**—You can also enter an IP address here and then click Refresh ARP to refresh only that single ARP entry.

Figure 516: Refresh ARP



Port Name *: ge-0/0/0

VLAN: VLAN

IP Address: IP

```
Clearing ARP cache...
Successfully updated.
```

Testing Tools for SRX Series Firewalls

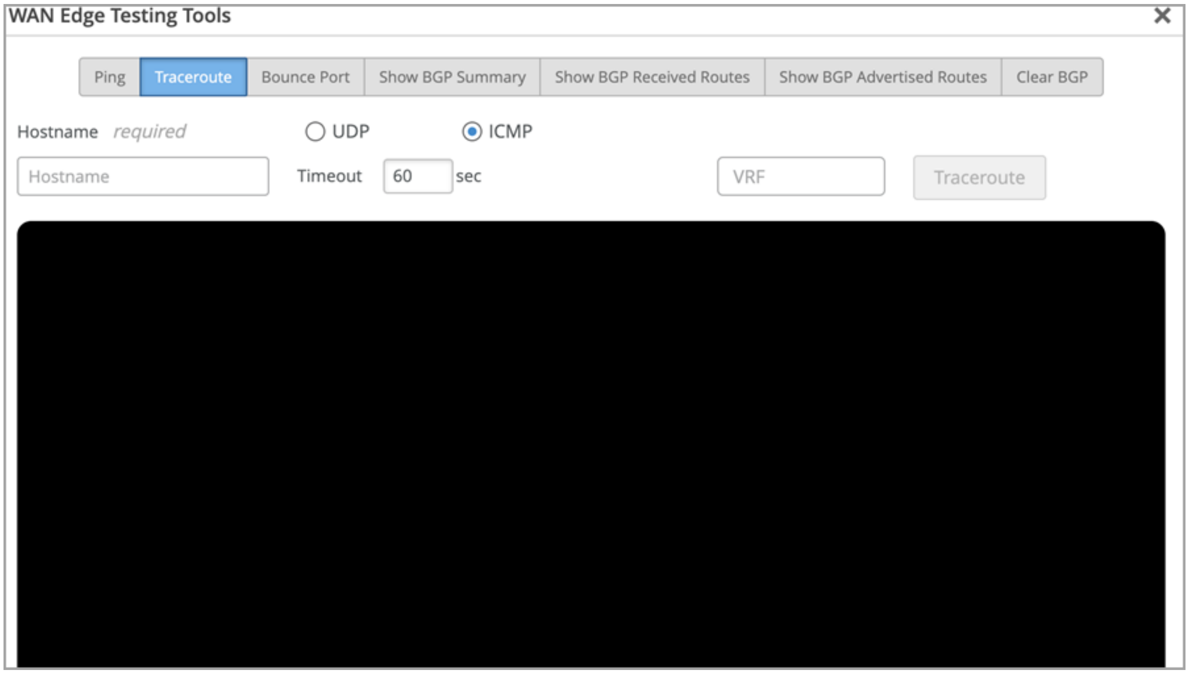
Traceroute on SRX Series Firewalls

Traceroute is a network diagnostic tool that traces the path an IP packet takes across networks, revealing the sequence of routers (hops) it takes along the way

To initiate Traceroute utility on SRX Series Firewalls:

1. In WAN Edge Testing tools window, click **Traceroute** and select one of the following options:
   - UDP
   - ICMP
2. Enter the following details for ICMP:

Figure 517: ICMP-Based Traceroute



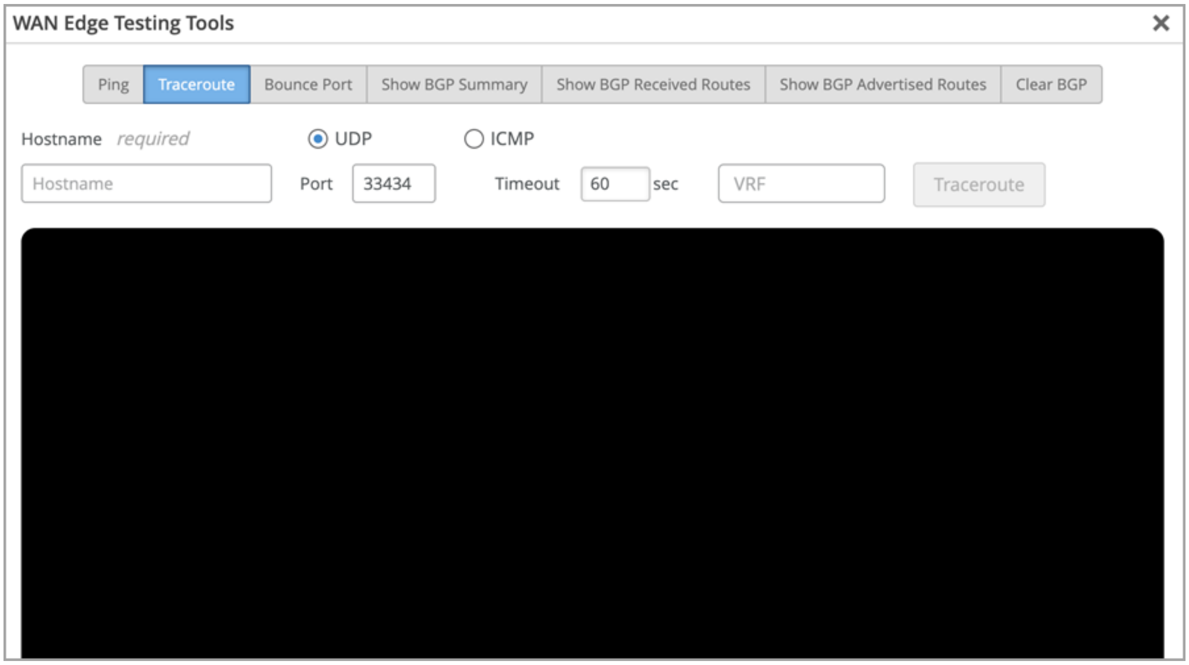
○ UDP ● ICMP

Timeout 60 sec

- **Hostname**—Enter the IP address or hostname of the remote system to ping.
- **Timeout**—Enter the time until which the device waits for a response from the remote host to a packet sent before considering timeout. The range of values is `60` through `3600` seconds. Default value is 60 seconds.
- **VRF**—Name of the routing instance present on the device.

3. Enter the following details for UDP:

Figure 518: UDP-Based Traceroute



WAN Edge Testing Tools

Hostname *required* ● UDP ○ ICMP

Hostname | Port 33434 | Timeout 60 sec | VRF

- **Hostname**—Enter the IP address or hostname of the remote system to ping.
- **Port**—Base port number to use in traceroute probes. The range is 1 through 65535. Default value is 33434.
- **Timeout**—Enter the time until which the device waits for a response from the remote host to a packet sent before considering timeout. The range of values is `60` through `3600` seconds. Default value is 60 seconds.
- **VRF**—Name of the routing instance present on the device.

4. Click **Traceroute**.

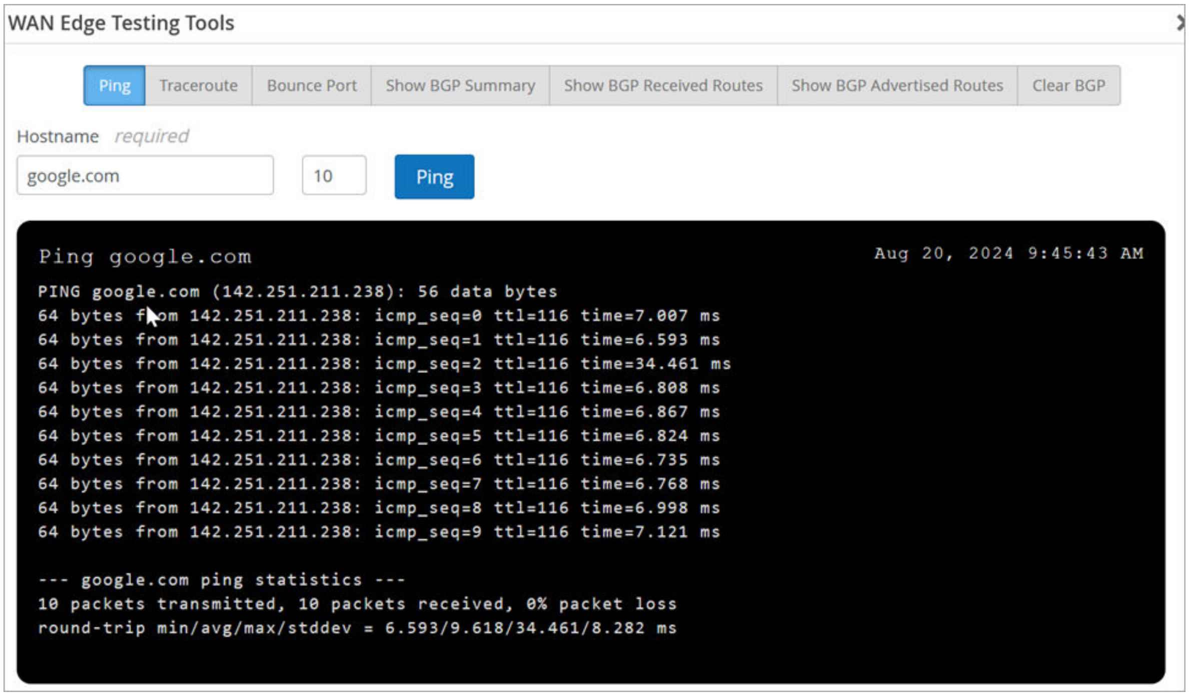
   The output displays the details of hops as IP addresses in the path to a given destination.

Ping Tests on SRX Series Firewall

Use the Ping tool to send Internet Control Message Protocol (ICMP) echo requests to a specified host. You can use this command to check if a particular host is reachable at a particular IP address.

1. In WAN Edge Testing tools window, click **Ping**.
2. Enter the following options:

Figure 519: Check Connectivity to Host Using Ping (SRX Series Firewall)



Hostname: google.com

Count: 10

```
Ping google.com                                            Aug 20, 2024 9:45:43 AM
PING google.com (142.251.211.238): 56 data bytes
64 bytes from 142.251.211.238: icmp_seq=0 ttl=116 time=7.007 ms
64 bytes from 142.251.211.238: icmp_seq=1 ttl=116 time=6.593 ms
64 bytes from 142.251.211.238: icmp_seq=2 ttl=116 time=34.461 ms
64 bytes from 142.251.211.238: icmp_seq=3 ttl=116 time=6.808 ms
64 bytes from 142.251.211.238: icmp_seq=4 ttl=116 time=6.867 ms
64 bytes from 142.251.211.238: icmp_seq=5 ttl=116 time=6.824 ms
64 bytes from 142.251.211.238: icmp_seq=6 ttl=116 time=6.735 ms
64 bytes from 142.251.211.238: icmp_seq=7 ttl=116 time=6.768 ms
64 bytes from 142.251.211.238: icmp_seq=8 ttl=116 time=6.998 ms
64 bytes from 142.251.211.238: icmp_seq=9 ttl=116 time=7.121 ms

--- google.com ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max/stddev = 6.593/9.618/34.461/8.282 ms
```

- **Hostname**—Enter the hostname of the remote system to ping.
- **Count**—Enter the number of ping requests to send. The range of values is `1` through `100`.

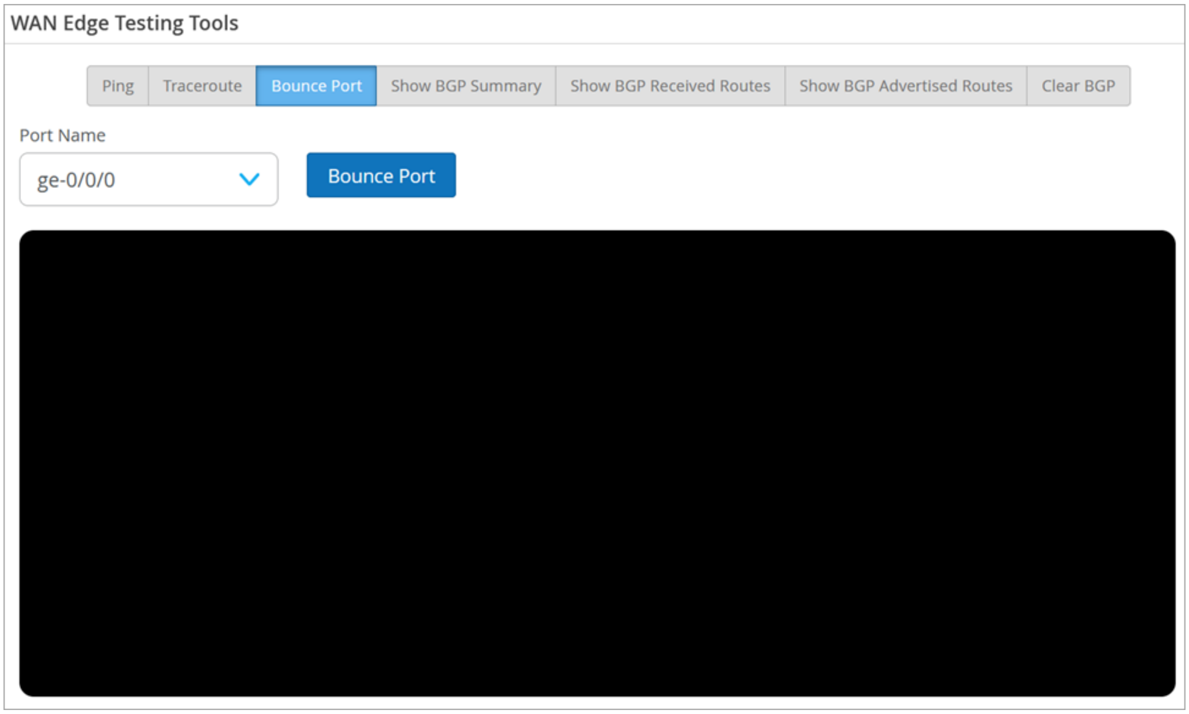
3. Click **Ping**. The output displays the details of hops as IP addresses in the path to a given destination.

Bounce Port

Use the *Bounce Port* tool to restart any unresponsive ports on your firewall.

1. In WAN Edge Testing tools window, click **Bounce Port**.
2. Specify the interface name (example: ge-0/0/0) and then click **Bounce Port**.

Figure 520: Bounce Port (SRX Series Firewall)



Port Name

ge-0/0/0

Border Gateway Protocol Test Tools for SRX Series Firewalls

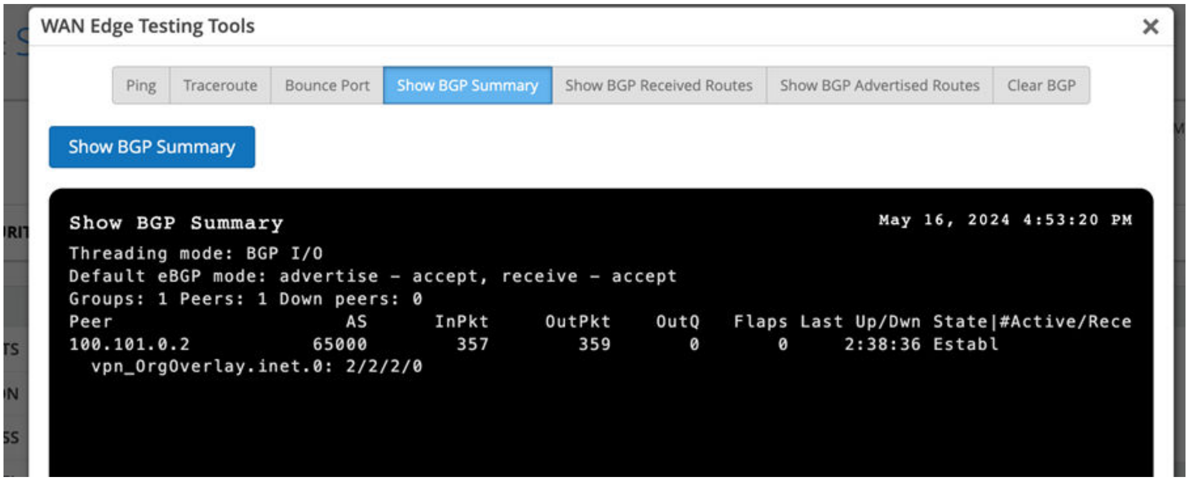
You can perform the following testing related to a BGP session:

- Display BGP summary
- Display BGP routes received
- Display BGP routes advertised
- Clear BGP routes

Use the following options to perform tests:

- Use **Show BGP Summary** option to display summary information about BGP and its neighbors.

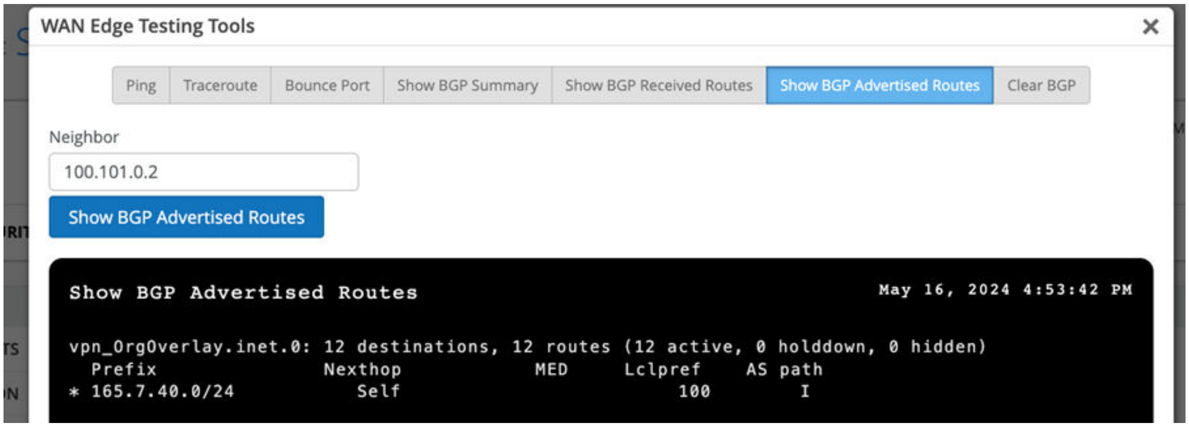
Figure 521: View BGP Summary (SRX Series Firewalls)



```
Show BGP Summary                                                  May 16, 2024 4:53:20 PM
Threading mode: BGP I/O
Default eBGP mode: advertise - accept, receive - accept
Groups: 1 Peers: 1 Down peers: 0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|#Active/Rece
100.101.0.2           65000        357        359       0       0     2:38:36 Establ
  vpn_OrgOverlay.inet.0: 2/2/2/0
```

- Use **Advertised Routes** option to display all routes that have been advertised to the specified neighbor.

Figure 522: BGP Advertized Routes (SRX Series Firewalls)



Neighbor

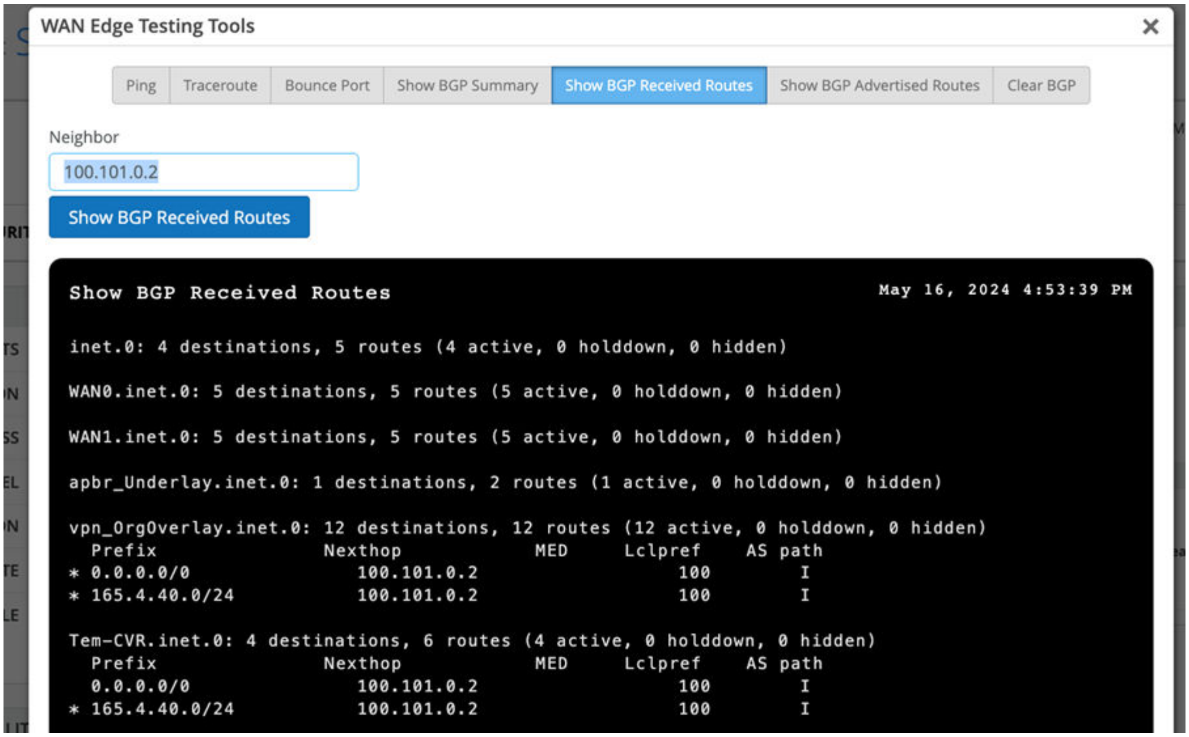
100.101.0.2

```
Show BGP Advertised Routes                                        May 16, 2024 4:53:42 PM

vpn_OrgOverlay.inet.0: 12 destinations, 12 routes (12 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 165.7.40.0/24              Self                         100        I
```

Enter the IP address of neighbor router and click **Show BGP Advertised Routes.** Output displays the routes that your device has advertised to the peer router during the current BGP session.

- Use **Received Routes** option to display all received routes from the specified neighbor.

Figure 523: BGP Received Routes (SRX Series Firewalls)



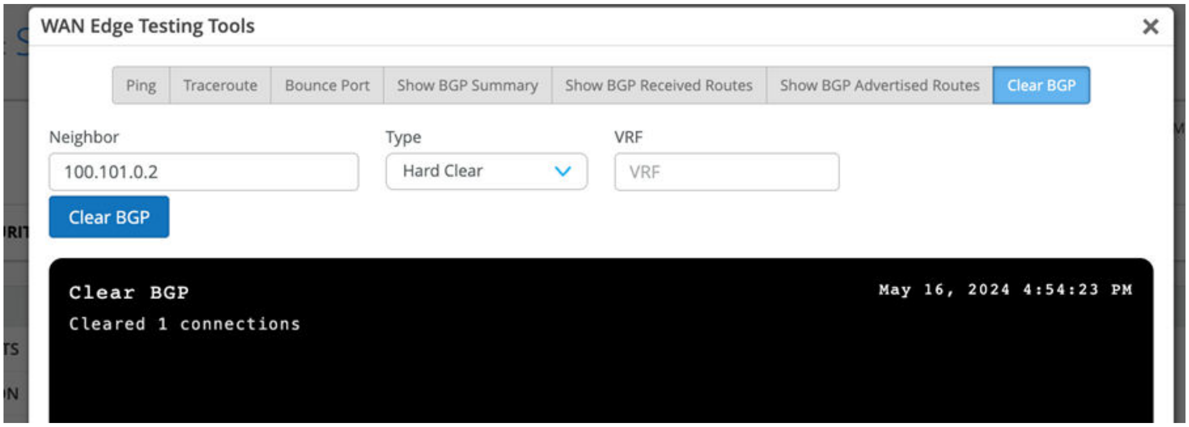
Neighbor: 100.101.0.2

```
Show BGP Received Routes                                    May 16, 2024 4:53:39 PM

inet.0: 4 destinations, 5 routes (4 active, 0 holddown, 0 hidden)

WAN0.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

WAN1.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

apbr_Underlay.inet.0: 1 destinations, 2 routes (1 active, 0 holddown, 0 hidden)

vpn_OrgOverlay.inet.0: 12 destinations, 12 routes (12 active, 0 holddown, 0 hidden)
  Prefix                Nexthop           MED     Lclpref    AS path
* 0.0.0.0/0                100.101.0.2                100        I
* 165.4.40.0/24            100.101.0.2                100        I

Tem-CVR.inet.0: 4 destinations, 6 routes (4 active, 0 holddown, 0 hidden)
  Prefix                Nexthop           MED     Lclpref    AS path
  0.0.0.0/0                100.101.0.2                100        I
* 165.4.40.0/24            100.101.0.2                100        I
```

Enter the IP address of neighbor router and click **Show BGP Received Routes**. The output display the routing information as it was received through a particular neighbor using BGP.

- Use **Clear BGP** option to clear sessions with all BGP neighbors or with specific BGP peer.

Figure 524: Clear BGP Sessions (SRX Series Firewalls)



Neighbor: 100.101.0.2

Type: Hard Clear

VRF: VRF

```
Clear BGP                                                   May 16, 2024 4:54:23 PM
Cleared 1 connections
```

You have the following options when clearing BGP routes:

- **Neighbor**—Select all to or IP address of a BGP peer. Apply this command only to the specified neighbor.
- **Type**—Specify how you want to reset a BGP session.
  - **Hard Clear**—A hard reset terminates the specified peering sessions. This action drops the TCP connection to the neighbors. This setting is not recommended.
  - **Soft Clear In**—Inbound soft reset on the connections
  - **Soft Clear Out**—Outbound soft reset on the outgoing connections
- **VRF**—(Optional) Specify virtual routing and forwarding (VRF). The action applies only to neighbors for the specified routing instance.

RELATED DOCUMENTATION

WAN Assurance Monitoring, SLE, and Troubleshooting Overview | **535**

Troubleshoot Session Smart Router Deployed as WAN Edge | **613**

Troubleshoot SRX Series Firewalls | **633**