Guided Setup: Juniper Mist WAN Assurance

Guided Setup for Juniper Mist WAN Assurance

IN THIS GUIDE

About Juniper Mist WAN Assurance

Juniper Mist WAN Assurance is a cloud service that brings automated operations and service levels to the enterprise access layer for the WAN edge. It supports both Juniper® SRX Series Services Gateways and Juniper® Session Smart™ Routers to provide near-continuous visibility into application performance and user experiences.

The SRX or SSR devices provide a rich variety of streaming telemetry to the Juniper Mist cloud, upon which you can build WAN Service-Level Experiences (SLEs) and set a baseline for network performance. For example, you can use an SLE for WAN link-health to identify issues on the WAN caused by congestion, IPsec, or ISP availability. You can also get insight into issues such as network latency, jitter, and packet loss as they affect application performance.

Another key part of the WAN Assurance cloud services is the Juniper Mist AI engine and Marvis virtual network assistant. These power the intelligent Self-Driving Network™ by transforming telemetry from the devices into Insights and automated actions, which allows you to shift your IT operations from a stance of being reactive, and troubleshooting based, to one of being proactive and preventive.

All these services are brought together in the Juniper Mist cloud console, which serves as a single pane of glass from which you can manage SLAs and monitor remediations. By virtue of the Juniper Mist cloud, WAN Assurance abstracts away the underlying complex technologies and provides a simplified user experience. Zero Touch Provisioning (ZTP), which is available on all cloud-ready Juniper devices, eliminates the legacy need for skilled and “remote” hands to onboard new equipment, and features such as variable and multi-device configuration that are available through templating brings increased efficiency.

Together, these features allow you to work from a set of common elements that you can apply across the entire Self-Driving Network domain: Wireless, Wired and WAN.

Supported Software and Devices

This example is built using vSRX devices. It is a simple use case with a branch secure router, SD-WAN, and a branch firewall.

You can use the tasks and step-by-step configurations provided to create a proof of concept (POC) in your specific environment using the hardware and software listed here.

Supported Juniper® SRX Series Services Gateways

- vSRX
- SRX300
- SRX320
- SRX340
- SRX345
- SRX380
- SRX550M
- SRX1500
- SRX4100
- SRX4200
- SRX4600

Recommended Junos software releases for the SRX Services Gateways:

- 20.1R3
- 20.2R3-S1
- 20.3R3

- 20.4R3
- 21.1R2
- 21.2R1
- 21.3R1

Supported Juniper® Session Smart™ Routers

- SSR120
- SSR120-AE
- SSR130
- SSR130-AE
- SSR1200

Recommended software releases for the SSR depend on the specific use case.

- To monitor SSRs from the Juniper Mist cloud console (the device is managed through the Conductor platform) you need to be running version 5.4.4 or later.
- • To manage SSRs from the Juniper Mist cloud console you need to be running version 6.0.0.42 or later.

About This Guided Setup

IN THIS SECTION

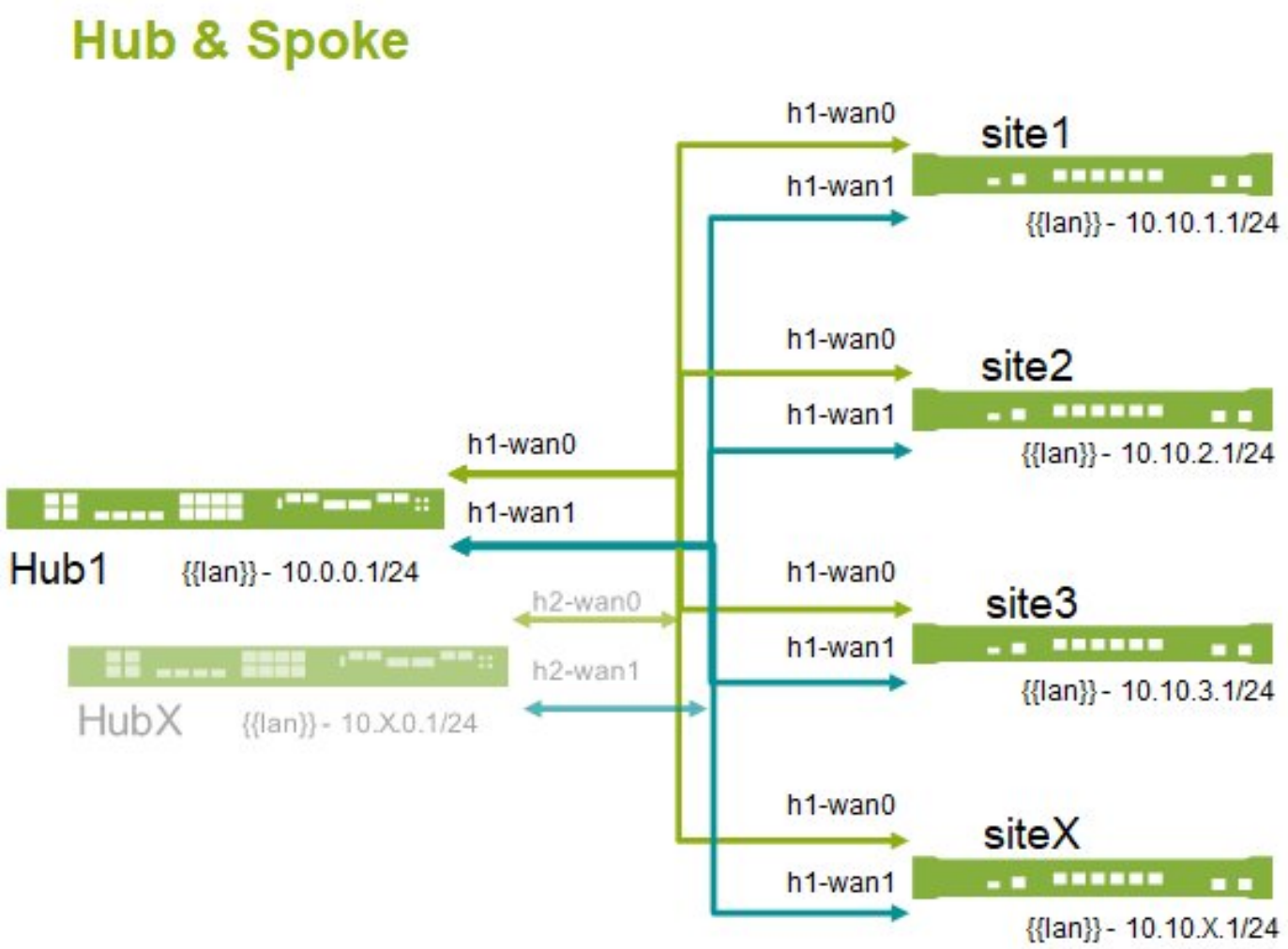
Guided Setup for Juniper Mist WAN Assurance

In this example, we'll use the Juniper Mist cloud console (GUI) to provision a simple hub and spoke network that traverses provider equipment via IPSec tunnels and leverages both access policies and traffic shaping rules to segment users and applications on the network. Conceptually, you can think of it as an enterprise with branch offices connecting over a provider WAN to on-prem data centers. For example, an auto-parts store, a hospital, or 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.

Physically, our example network includes two hubs and two spokes, all with redundant links to the WAN. We assume that you have the hardware already onboarded to the Juniper Mist cloud and that the physical connections needed to

support the configuration are in place (that is, that the cabling is already in place and that you know the interfaces, VLANs, etc. that are in use and/or valid for your sandbox).

Figure 1: Hub and Spoke WAN Assurance Topology



Logically, the Juniper Mist cloud console uses the concepts of sites and templates to vastly simplify the work of provisioning devices. It also supports site-specific variables, which means you can define a given site or network and then clone it to easily expand your network. For the IPsec tunnels running over the WAN between the hub and spokes, the console automates the work of setting up the Public key infrastructure (PKI) so you don't have to configure the certificate authority (CA) and digital signatures and digital certificates.

Essentially, you use the GUI to build up your network overlay on a logical plane, in the form of network elements, applications, and rules. The GUI stores the configuration commands until they are ready to be pushed to the devices. If the device is an SRX, the console will push Junos commands. If it is an SSR device, the console pushes programmable command line interface (PCLI) commands.

All the abstraction provided by the GUI amounts to some 600 to 700 lines of Junos commands, per SRX device.

You can see how Juniper Mist WAN Assurance simplifies network configuration at scale. Once you push the configuration and the network becomes operational under Juniper Mist, streaming telemetry from the SRX or SSR

devices provides the underlying data used in SLAs. The Juniper Mist AI engine takes the automation further by creating Insights into the WAN traffic patterns and automatically providing remediating actions to honor the SLAs when needed.

Using This Guided Setup

IN THIS SECTION

To recreate the network in this example, you'll need an account with admin-level credentials for an organization in the Juniper Mist cloud. You should be able to add a site to the organization.

On the hardware side, you'll need at least two supported SRX Services Gateways. These should be available for you to use in your Organization's Inventory, which means they are already connected to the WAN and have been onboarded to the Juniper Mist cloud (that is, claimed and adopted).

For help getting onboarding and/or claiming your devices, please see the following:

- Claiming A Device
- SSR Onboarding
- SRX Adoption

The Juniper SRX Gateway devices should also be manageable by the Juniper Mist cloud, and you should not make any further configuration changes to the device outside of the Juniper Mist console. This is because any existing configuration will be replaced when the Juniper Mist console pushes its stored configuration to the device. In addition, if you make configuration changes to the device outside of the Juniper Mist console after the initial configuration push, these changes will not be known to the Juniper Mist console. Thus, whenever another cloud-side config push is made to the device, those changes will be lost.

That said, there is an option in the Juniper Mist console to add device-level configuration statements, which will be included in all subsequent cloud-side pushes. This is shown in Task X.

Using The Juniper Mist Console

The GUI typically groups related configuration settings together in a settings panel, identified by a title. In some cases, there are a lot of settings and panels in each screen. In this document, we use the title to help you navigate within the page, but you may need to scroll down the page to find a given panel.

- For screens with a lot of information, you can in some cases display the settings panels in three columns by making the screen wider.
- Some settings panels require an intermediate save action to store the information locally. These are indicated by a blue checkmark at the top of the panel. These saves are not pushed to the device. A gray checkmark means the configuration is not complete or that there is something wrong with one of the settings.
- To push the configuration to the device(s), be sure to scroll to the top of the screen and click the Save button.

Hierarchy in the Juniper Mist Console

The GUI uses an inheritance hierarchy for sites, templates, and devices, in that order. Settings made at the site level will apply to all devices. This is convenient for things like DNS settings, which are global in nature.

Device-level settings, which apply only to that device, are also possible. If the same setting is configured for the device at the template level, the device-level settings will take precedence. This lets you create device-specific exceptions to any settings made at the template level (for example, if you need the device to perform some kind of individual role while at the same time inheriting most of its settings from the parent template).

Settings made in a template can be applied to one or more sites. If you are using site variables in the template, the variables will be replaced by actual values for the site when you apply the template to another site.

Variables

Site variables provide a way to use tags (such as “corp_ip”) to represent actual values (such as 10.10.0.1) so that the value can vary according to the context where you use the variable. For example, for Site 1 you can define corp_ip to be 10.10.0.1, while for Site 2 the value you give corp_ip is 192.168.1.10. You can then use the tag to replace the actual IP address for Juniper Mist Cloud configurations such as in the WAN edge template, so that when you attach the template to different sites, the appropriate IP address is automatically used in each site.

To define site variables, use double brackets to format the variable name, like so:

{{site-variable}}

Using These Instructions

The Juniper Mist console does a great job of abstracting much of the network design and configuration details required for the underlay and even automates things like tunnel set up between the hub and spokes. But there is still a fair amount of configuration work to do in the GUI.

In the sections that follow, we break this work into seven tasks, each of which includes required steps. Some tasks are used as objects (or, building blocks) in a later task.

The steps walk you through the configuration for the first instance. For example, creating a site for one of the hubs. If you need to create additional instances of the same task, you’ll see a table that contains the configuration settings needed, such as the remaining hub and two additional spokes.

The idea is for you to follow the steps to complete the first instance of the task and then use the values in the table to go through the steps again to complete the next instance of the task, and so on, rather than cycling through the steps this example again for each set of values.

The tables also make it easier if you need to adapt this example for your own environment. So, for example, if the 10.0.0.1/28 IP addresses we use here are not suitable for your environment, or if you are not using the ge-0/0/1 interface on your device, you can update the tables to include those that are. This is work you should complete before you proceed.

Juniper Mist Live Demo

If you aren't ready to deploy your own network but want to try this out, Juniper has a Live Demo site on the Web where you can access the Juniper Mist cloud console and walk through an existing example of the Juniper Mist WAN Assurance cloud services.

Juniper Mist Live Demo

Please contact your Juniper representative to set up a guided demonstration of all the features covered in this document.

Task Overview

IN THIS SECTION

To help organize the guided setup, we break the configuration into six main tasks.

1. **Create the sites**. In this task, we create a site for the hubs and spokes. We also configure site variables for each site, which are used later in the templates for WAN Edge devices and the hub profile.

2. **Set up the networks**. In this tasks, we define the subnet and configure the network “users” (these are the source addresses you will use later for the access policies). You’ll also create LAN segments here, and you can set up NAT rules if need be.

3. **Configure the applications**. Applications can be selected from a predefined list, selected by category, or defined individually according to IP address or hostname.

4. **Create hub profiles**. These contain the overlay and network paths that are used on the overlay.

   - If you add or remove a WAN link in the hub profile, it will affect the paths on the overlay.
   - The system automatically creates all the necessary AutoVPN tunnels for the hubs and spokes. The Juniper Mist CA will generate and transfer the certificates used for authentication.
   - The system automatically creates a failover probe for each WAN link. You can modify these settings using the API.

5. **Create WAN Edge template for the spoke sites**. The WAN Edge template is where you define the WAN interfaces, select the overlay path (as configure in the hub profile), and define the LAN networks. You can also set up traffic steering preferences, define user service policies, and set up the default routing policies (static, BGP, or OSPF).

6. **Attach the template to the site** to bring the topology together, and then

   Push the configuration to the SRX Services Gateways by saving it.

Task 1: Create the Sites

IN THIS SECTION

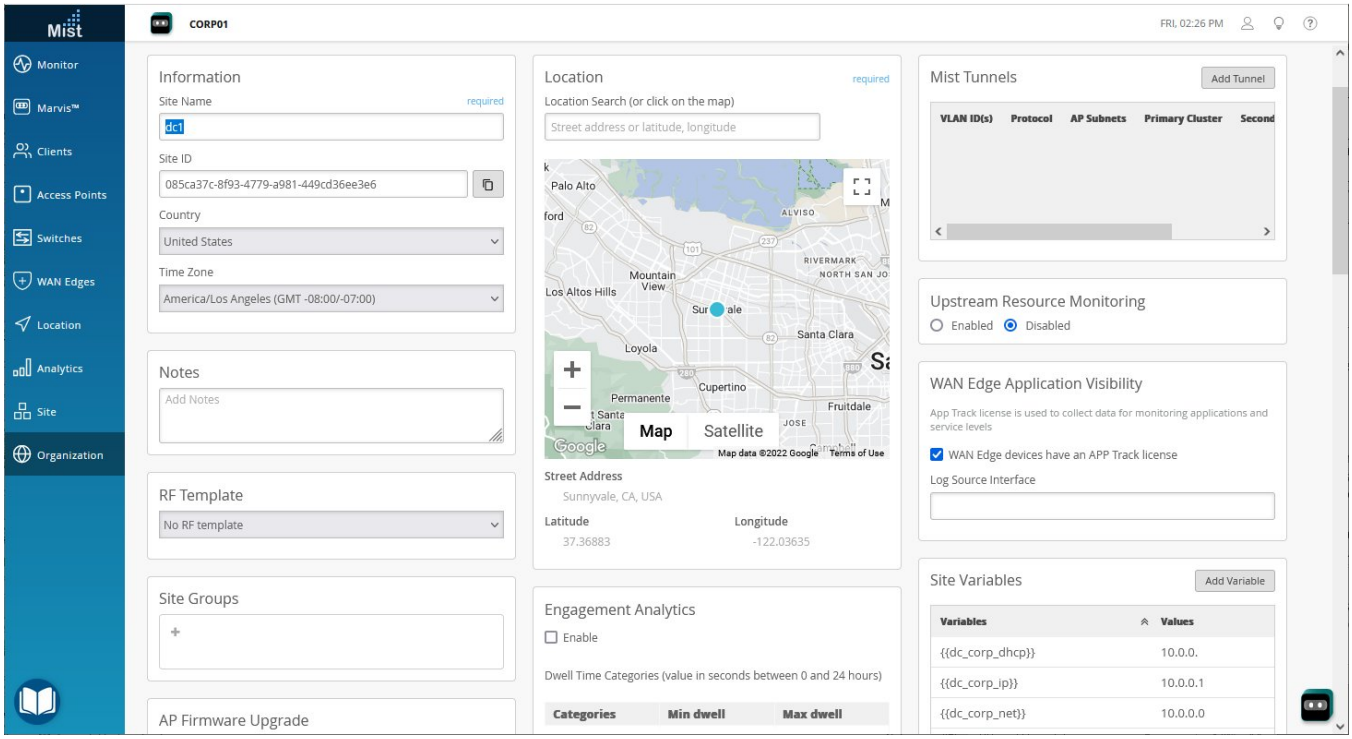
A site is a sub-set of your organization in the Juniper Mist Cloud, available to anyone with sufficient privileges. Likewise, the configuration settings we make for our sites are automatically applied to (or at least available to) all the devices included in the site. In short, the sites we create in this example should be used exclusively for the hub-spoke network we're setting up, as should the devices therein (although, for this example, we will keep the default setting for most of the site level configurations).

In addition, the SRX Series Services Gateway should have an AppSecure 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).

To create a site,

1. In the Juniper Mist menu, click **Organization > Site Configuration**. A list of existing sites, if any, appears. (Although we do not use the feature here, it is worth pointing out that for later instances of this task, you can clone an existing site by selecting it from the list and then in the screen that appears, clicking the **Clone Site** button.)

2. Click the Create Site button in the upper right corner. The New Site window appears.



3. Give the site a name. In our case, we'll use **dc1**, but any name will do.

4. A Site ID is generated automatically.

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

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

7. Scroll down the screen to the **Site Variables** settings panel.

8. Click the **Add Variable** button.

9. In the pop-up screen that appears, type a name for the variable and specify the value it represents. Use Table 1 to complete the list of variable you need to add.

10. For the remaining fields, we'll use the default values except for when we define our site variables.

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

12. Continue by adding the values for **dc2**, **spokes-static**, and**spokes-dhcp** using the information in the following tables.

Site variables for dc1.

Variable	Value
{{dc_corp_dhcp}}	10.0.0.
{{dc_corp_ip}}	10.0.0.1
{{dc_corp_net}}	10.0.0.0
{{dc_corp_subnet}}	24
{{dc_corp}}	10.0.0.
{{dns_1}}	8.8.8.8
{{dns_2}}	1.1.1.1
{{vlan_id}}	10
{{wan0_gw}}	10.11.0.1
{{wan0_ip}}	10.11.0.2
{{wan0_mask}}	30
{{wan1_gw}}	10.11.1.1
{{wan1_ip}}	10.11.1.2
{{wan1_mask}}	30

Site variables for dc2.

Variables	Values
{{dc_corp_dhcp}}	10.0.0.
{{dc_corp_ip}}	10.0.0.1
{{dc_corp_net}}	10.0.0.0

{{dc_corp_subnet}}	24
{{dc_corp}}	10.0.0.
{{dns_1}}	1.1.1.1
{{dns_2}}	8.8.8.8
{{ext_ssh}}	10.11.0.2
{{int_ssh}}	10.0.0.2

Site variables for spokes-static.

Variables	Values
{{corp_vlan_id}}	10
{{dns_1}}	8.8.8.8
{{dns_2}}	1.1.1.1
{{guest_vlan_id}}	200
{{spoke_corp_dhcp}}	10.10.2.
{{spoke_corp_ip}}	10.10.2.1
{{spoke_corp_net}}	10.10.2.0
{{spoke_guest_dhcp}}	172.16.2.
{{spoke_guest_ip}}	172.16.2.1
{{spoke_guest_net}}	172.16.2.0
{{spoke_mask}}	24
{{wan0_gw}}	10.12.0.1
{{wan0_ip}}	10.12.0.2

{{wan0_mask}}	30
{{wan1_gw}}	10.12.1.1
{{wan1_ip}}	10.12.1.2
{{wan1_mask}}	30

Site variables for spokes-dhcp.

Variables	Values
{{corp_vlan_id}}	10
{{dns_1}}	8.8.8.8
{{dns_2}}	1.1.1.1
{{guest_vlan_id}}	200
{{spoke_corp_dhcp}}	10.10.3.
{{spoke_corp_ip}}	10.10.3.1
{{spoke_corp_net}}	10.10.3.0
{{spoke_guest_dhcp}}	172.16.3.
{{spoke_guest_ip}}	172.16.3.1
{{spoke_guest_net}}	172.16.3.0
{{spoke_mask}}	24
{{wan0_gw}}	10.13.0.1
{{wan0_ip}}	10.13.0.2
{{wan0_mask}}	30
{{wan1_gw}}	10.13.1.1

{{wan1_ip}}	10.13.1.2
{{wan1_mask}}	30

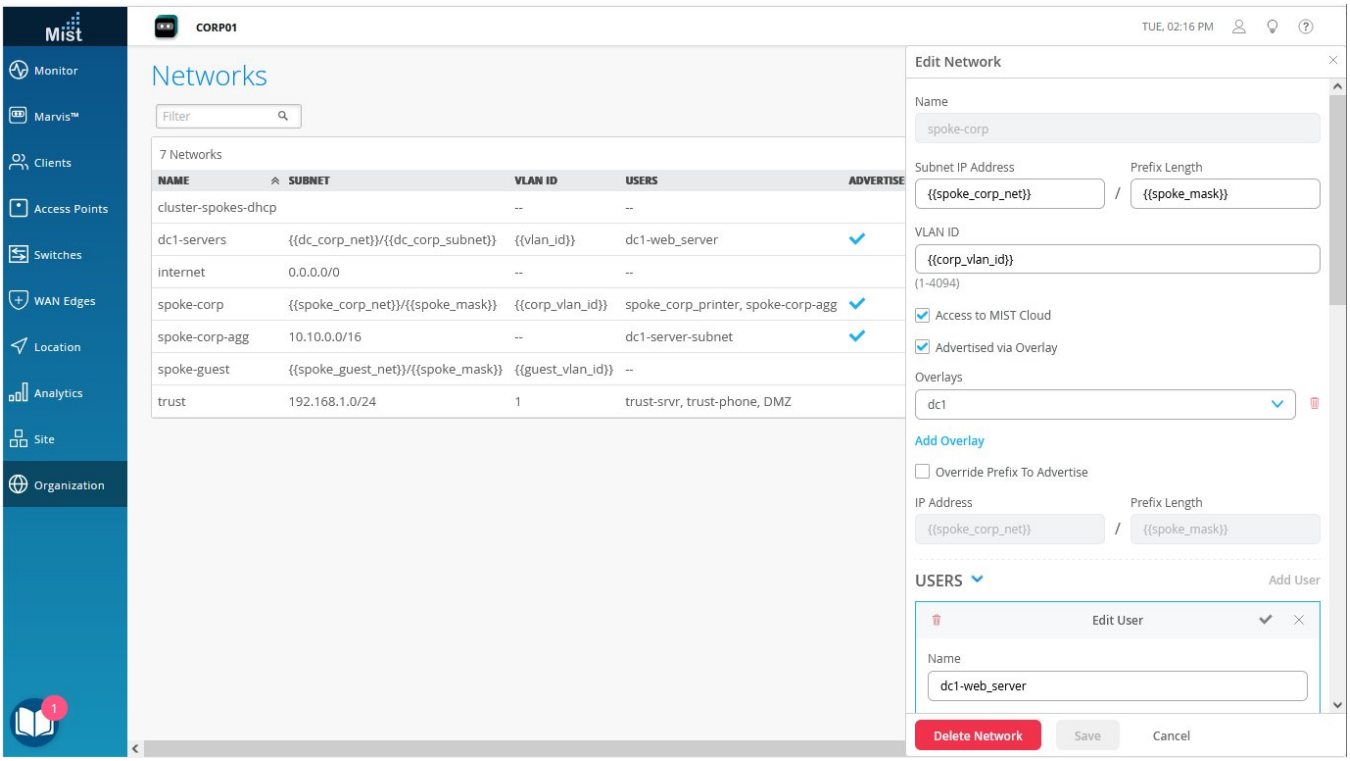
Task 2: Set Up Networks

IN THIS SECTION

In this task we create our LAN segments and set up “users,” which are source addresses that will be used later in the service policies. The network can be advertised on the overlay, and you can set up Network Address Translation (NAT) for the source and/or destination if needed.

To configure the network,

1. In the Juniper Mist menu click **Organization > WAN | Networks**. A list of existing networks, if any, appears.
2. Click the **Add Networks** button in the upper right corner. The Add Network window appears.



3. Give the network a name. Here, we'll use **spoke-corp**.
4. We'll use variables for both the **Subnet IP Address** and **Prefix Length** fields.
   - For Subnet IP Address, type **{{spoke_corp_net}}**
   - For Prefix Length, type **{{spoke_mask}}**
5. For VLAN ID, type **{{corp_vlan_id}}**. Note that we're using a variable for the VLAN ID. If your device is an SRX Services Gateway that is using an untagged interface, you should use 1 as the VLAN ID instead of the variable shown here.
6. Enable the following options:
   - **Access to MIST Cloud** (this permits services to access the Juniper Mist cloud)
   - **Advertised via Overlay** (this announces the network via iBGP). The IP Address and Prefix Length fields below the option are filled in automatically.
7. Under the **Users** section, click the **Add User** button and create the following users:

User	IP_Prefix
spoke_corp_printer	{{spoke_corp_net}}10
spoke-corp-agg	10.10.0.0/16
Phones	192.168.1.0/24
corp-any	0.0.0.0/0

8. Under the **Destination NAT** section, click the **Add Destination Nat** button configure it with the values shown in the table.

Destination_NAT	Values
Name	spoke-corp-ssh
External IP	{{wan0_ip}}
External Port	22
Internal IP	{{spoke_corp_dhcp}}10
Internal Port	22

9. For the option **Apply to Incoming traffic from**, select **Underlay**.
10. Click the **Add** button.

11. Continue by adding the values for **spoke-guest, spoke-corp-agg**, and **dc1-servers** networks using the information in the table.

Values for the spoke-guest network.

Subnet_IP_Address	**__spoke_guest_net__**
Prefix Length	{{spoke_mask}}
VLAN ID	{{guest_vlan_id}}
Access to MIST Cloud	Checked
Users	None configured
Static Source NAT	Not configured
Destination NAT	Not configured

Values for the spoke-corp-agg network.

Name	**spoke-corp-agg**
Subnet IP Address	101.0.0.0
Prefix Length	/16
VLAN ID	<default>
Source NAT Pool Prefix	Not configured
Access to MIST Cloud	Checked
Advertised via Overlay	Checked
Override Prefix to Advertise	Not checked
Users > Name	dc1-server-subnet
Users > IP Prefixes	10.0.0.0/24

Static Source NAT	Not configured
Destination NAT	Not configured

Values for the dc1-servers network.

Name	**dc1-servers**
Subnet IP Address	10.0.0.0
Prefix Length	/24
VLAN ID	10
Access to MIST Cloud	Checked
Advertised via Overlay	Checked
Override Prefix to Advertise	Not checked
Users > Name	dc1-web_server
Users > IP Prefixes	10.0.0.254/32
Users > Name	dc1-web_server2
Users > IP Prefixes	10.0.0.253/32
Static Source NAT	Not configured
Destination NAT > Name	public-ssh
Destination NAT > External IP	10.11.0.2
Destination NAT > External Port	22
Destination NAT > Internal IP	10.0.0.10
Destination NAT > Internal Port	22
Destination NAT > Apply to Incoming traffic from	Underlay

Task 3: Configure Applications

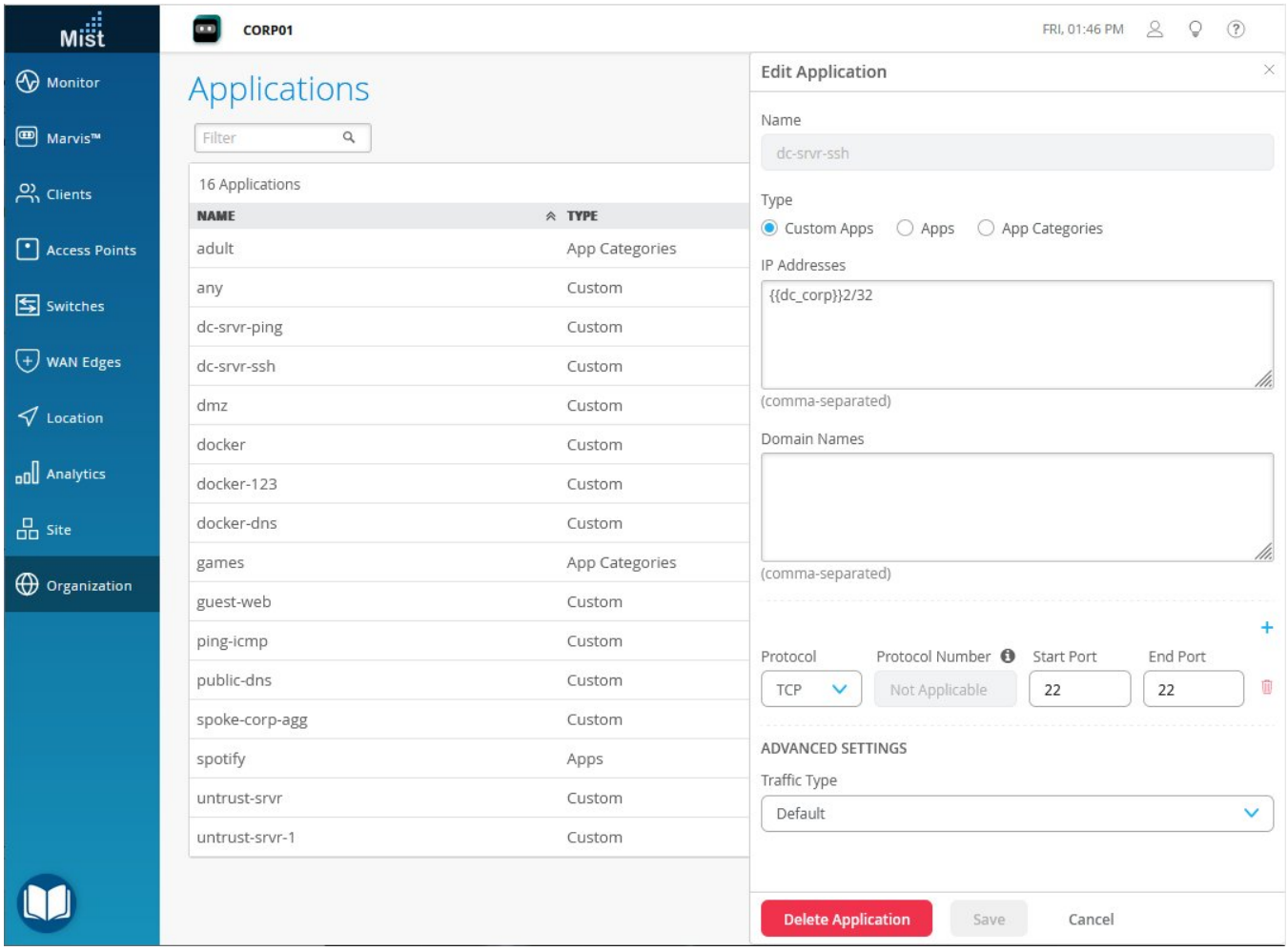
IN THIS SECTION

Applications are the services or apps that your network users will connect to. You can select applications by category (such as Social Media), select individual applications (such as Microsoft Teams) from a list, or create a custom application to describe anything that is not otherwise available. For the latter, you define the app by specifying a combination of its IP address, port (or port range), and protocol (TCP or UDP). We will associate these applications with the users/networks that we set up in Task 2, and assign a traffic steering policy and access rule (Allow/Deny).

To set up applications,

1. In the Juniper Mist menu, click **Organization > WAN | Applications**. A list of existing applications, if any, appears.

2. Click the **Add Application** button in the upper right corner. The Add Application window appears, as shown here.



3. Give the application a name. In our case, we'll create an application called **guest-web** to allow guest access to the Internet.
4. For **Type**, choose the **Custom Apps** option.
5. Skip the IP Address and Domain Names field for this case.
6. Click the **Protocol** drop down and select **TCP**.
7. Type **80** for both the **Start Port** and **End Port**.
8. Click the blue + icon and type **443** for both the **Start Port** and **End Port**.
9. For **Traffic Type**, under **Advanced Settings**, keep **Default**.
10. Click **Save**.
11. Use the table below to add the remaining applications we need for this example.
    - Click the **Add Application** button to open a new screen, and the **Add** button to add it to the application list.
    - To add more than one protocol, click the blue + icon.
    - For Advanced Settings, use Default for all the applications.

Applications

Name	IP_Address	Protocol	Start_Port	End_Port
Any	0.0.0.0/0	any	<null>	<null>
dc-srvr-ping	10.11.0.2/32	ICMP	<null>	<null>
dc-srvr-ssh	10.0.0.10/32	TCP	22	22
public-dns	8.8.8.8/32,8.8.4.4/32,1.1.1.1/32,1.0.0.1/32	UDP	53	53
spoke-corp-agg	10.10.0.0/16	any	<null>	<null>
trust-srvr1	192.168.1.10/32	TCP	22	22
untrust-srvr	8.8.8.8/32,1.1.1.1/32	TCP TCP	80 443	80 443
untrust-srvr1	8.8.8.8/32,1.1.1.1/32	any	<null>	<null>

Task 4: Configure Hub Profiles

IN THIS SECTION

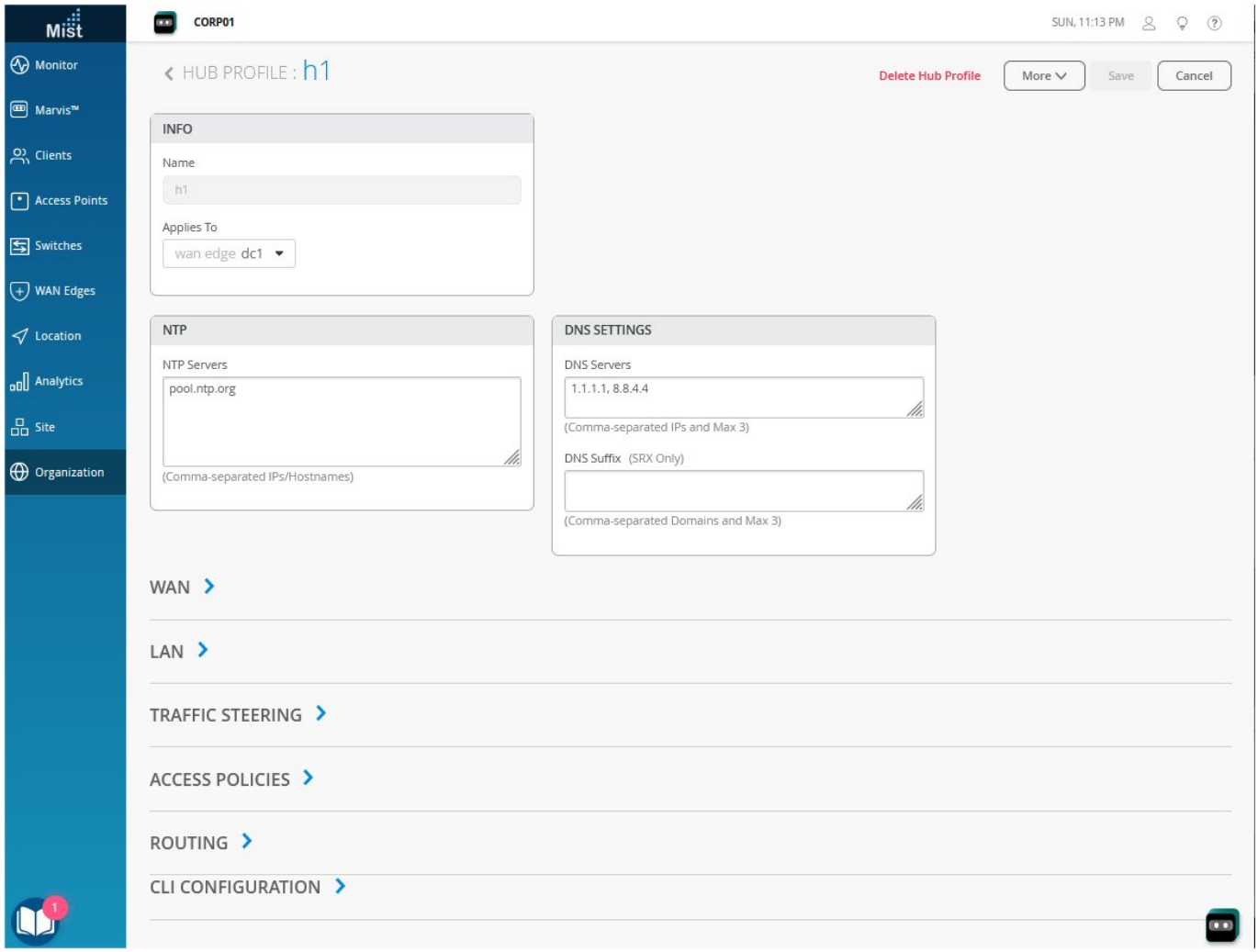
Hub profiles are a convenient way to create an overlay and assign a path for each WAN link on that overlay. Each hub device in a topology should have its own profile. When you create a hub profile for a device, the system will automatically generate and install the SSL certificates. It also setup up WAN-link probes for failover detection.

In this task, we'll create a hub profile and apply it to the **dc1** WAN Edge device.

To create a hub profile,

1. In the Juniper Mist menu, click **Organization > WAN | Hub Profiles**. A list of existing profiles, if any, appears.
2. Click the **Create Profile** button in the upper right corner and give the profile a name. For this example, we'll use **h1**, but anything will do.

3. The Hub Profile screen appears, as shown here.



4. In the **Info** settings panel, click the **Applies To** dropdown to show a list of the WAN Edge devices that have been added to the inventory of the current site. In our case, the site is named **dc1**, and the WAN Edge device also happens to have the same name. Select **dc1**.
   - WAN Edge devices are assigned to a site from the Inventory page, typically at the time when the device was onboarded and claimed.
   - If your organization has multiple sites, the **Applies To** dropdown will include a sub-dropdown of available sites, and a list of WAN Edge devices available in the site is displayed.
   - Although we are not using this method here, you can also assign the hub profiles to a device from the device page once the device is assigned to a site.
5. In the **NTP Settings** panel, enter the hostname or IP address of the NTP server(s) you want the Hub to use. In this example, we use **pool.ntp.org**, a virtual, global cluster of public time servers.
6. In the **DNS Settings** panel, enter the hostname or IP address of the DNS server(s) you want the Hub to use. In this example, we use **8.8.4.4** and **1.1.1.1**, which are public DNS servers, for the domain name resolution of hosts on the Internet.

7. (Optional) Specify up to three domain suffixes. These will be automatically appended, in the order specified, to accommodate unqualified computer names in DNS query.

Hub Profiles: WAN

IN THIS SECTION

We'll add two WAN links to this hub profile. The hub profile will automatically create overlay endpoints for each WAN interface, which can then be referenced when building the WAN Edge template.

1. Under the **WAN** section, click the **Add WANs** button to open the Add WAN Configuration panel.
2. Give the WAN a name. For this example, we'll use **wan0**, which automatically becomes the **Overlay Hub Endpoint**.
3. For **WAN Type**, choose **Ethernet** (this appears as "**broadband**" in the WAN list).
4. For **Interface**, specify the hub port that connects to the WAN. Because in this example we are configuring an SRX Service Gateway, we must specify **ge-0/0/0** as the interface to connect to the Juniper Mist cloud.
5. To configure the IP address of the hub interface, use the following values:
   - **IP Address**: **10.11.0.2**
   - **Prefix Length**: **30**
   - **Gateway**: **10.11.0.1**
6. For most deployments **Source NAT** will be **Enabled**. Although we do not use the feature in this example, you can override the IP address used to terminate the overlay by selecting the **Override** option and then entering an IP address in the **Public IP** field.
7. Click **Save** to apply the settings.
8. Continue by adding the values for the remaining WAN using the information in the table.

Values for wan1 in the Hub Profiles

Name	Value
Name	WAN1
WAN Type	Ethernet
Interface	ge-0/0/1

Port Aggregation	Not selected
Redundant	Not selected
VLAN ID	<null>
IP address	10.11.1.2
Prefix Length	/30
Gateway	10.11.1.2
Source NAT	Enabled
Public IP	default (10.11.1.2)
Overlay	Not selected

Hub Profiles: LAN

We'll add one LAN to this hub profile.

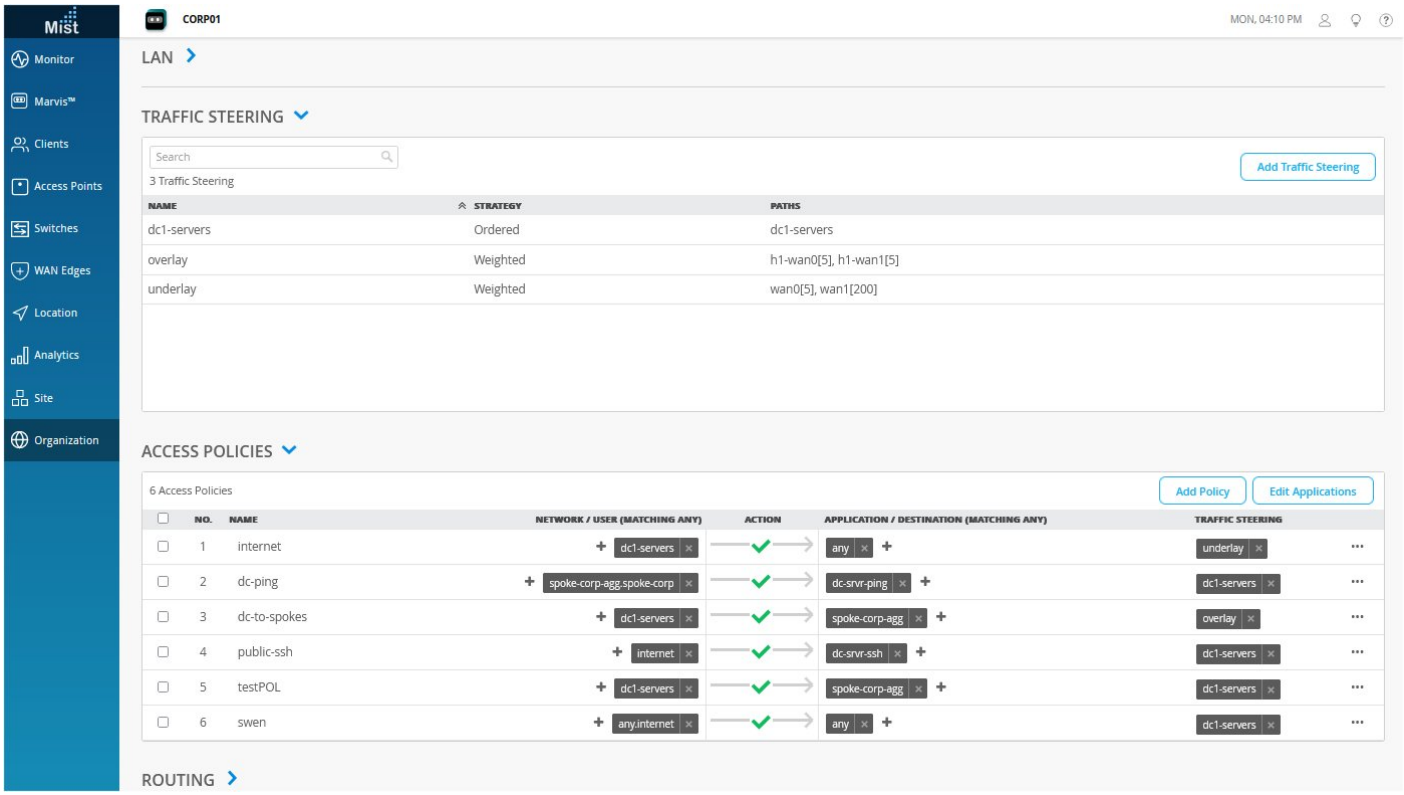
1. Under the LAN section, click the **Add LANs** button to open the Add LAN Configuration panel.
2. Click the drop-down under **Network** and select **dc1-servers** from the list of networks that appears.
3. For **Interface**, specify the hub port that connects to the LAN. For the network used in this example, that interface is **ge-0/0/2**.
4. To configure the IP address of the interface, use the following values:
   - **IP Address**: **{{dc_corp_ip}}**
   - **Prefix Length**: **{{dc_corp_subnet}}**
   - **Under Untagged VLAN**, select **Yes**.
5. For **DHCP**, select **Server** and specify the following:
   - **IP Start**: **{{dc_corp_dhcp}}20**
   - **IP End**: **{{dc_corp_dhcp}}254**
   - **Gateway**: **{{dc_corp_dhcp}}1**
   - **DNS Servers**: **{{dns_1}}, {{dns_2}}**
   - **DNS Suffix**: **<null>**
6. Click **Save**.

Hub Profiles: Traffic Steering

IN THIS SECTION

Traffic steering is where you define the different paths that application traffic can take to traverse the network. Destination zone is also determined by the paths configured within traffic steering.

We will set up three traffic steering policies, one for the overlay, one for the underlay, and one for **dc1-servers**, which is detailed here. The figure below shows the policies in the context of a screenshot.



To set up Traffic Steering,

1. Under the **Traffic Steering** section, click the **Add Traffic Steering** button to display the Traffic Steering configuration screen.
2. Give your policy a name. For this example we'll use **dc1-servers**, but any name will do.
3. Select the **Strategy** you want to apply. For this example, choose **Ordered**.
   - **Ordered**
   - **Weighted**—Distribute traffic across links according to a weighted bias, as determined by the configure cost.
   - **ECMP**-- Equal-cost multipath; distributed traffic equally across multiple paths (for links with similar capacity and utilization)

4. Click **Add Paths** to expose the **Add Path** drop-down.
   - For **Type**, choose **LAN**
   - For **Name**, choose **dc1-servers**.
5. Click the blue checkmark in the corner of the panel to apply these settings.
6. Click **Save** to add the policy to the list.
7. Continue by adding the site variables for the remaining WAN using the information in the table.

Values for the Traffic Steering Policies in the WAN Edge template

Name	Field	Value	Paths	Value	Value
dc1-servers	Strategy:	Ordered			
			spoke-corp	Type:	LAN
				Network:	dc1-servers
Overlay	Strategy:	Weighted			
			h1-wan0	Type:	Overlay
				Name:	h1-wan0
				Cost:	5
			h1-wan1	Type:	Overlay
				Name:	h1-wan1
				Cost:	5
Underlay	Strategy:	Weighted			
			wan0	Type:	WAN
				Name:	wan0
				Cost:	5
			wan1	Type:	WAN
				Name:	wan1

Cost: 200

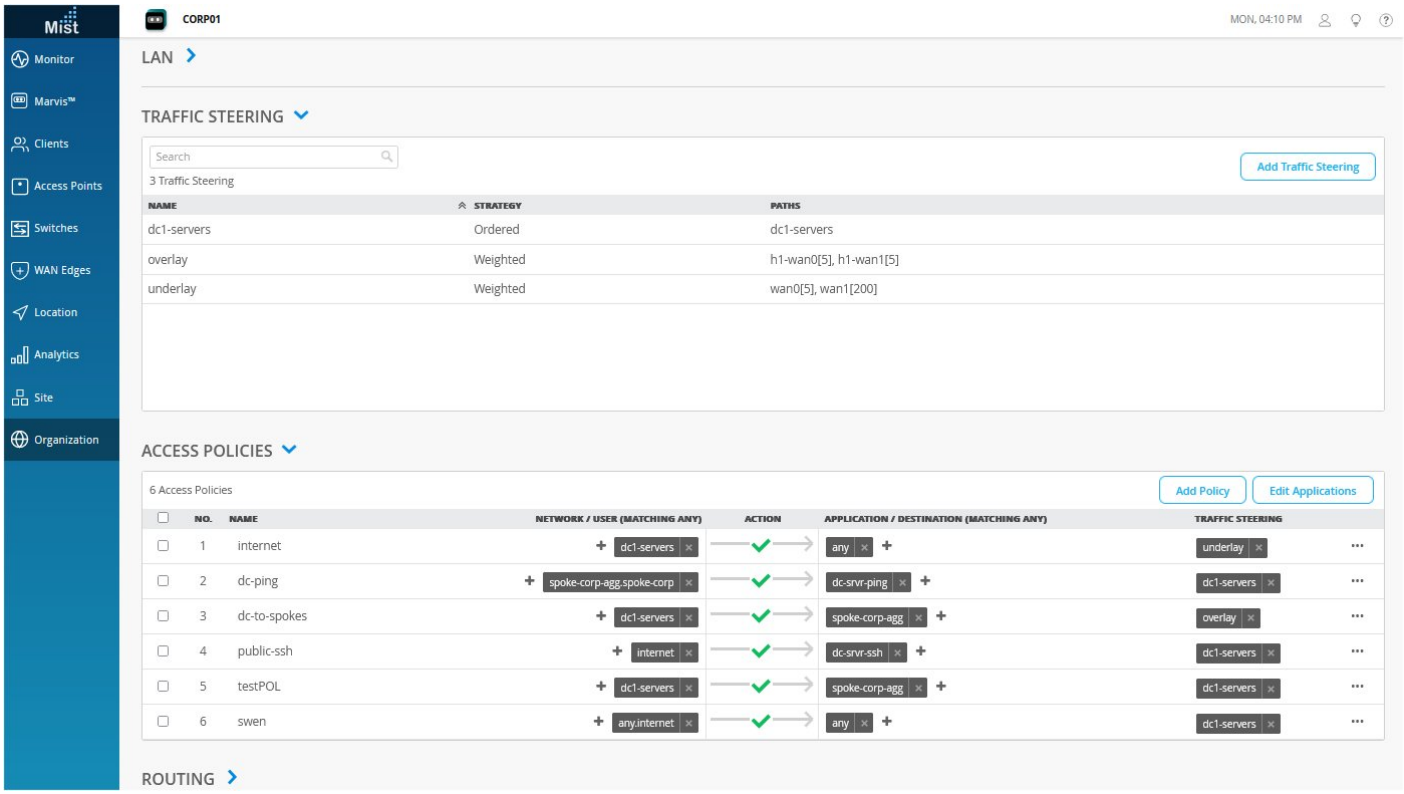
Hub Profiles: Access Policy

IN THIS SECTION

Access policies are where you define which network/users can access which applications, and according to which traffic steering policy. The source zone is determined by the Networks/Users and the destination zone is determined by the Application + Traffic Steering path. Additionally, you can assign an action of Permit or Deny. Access policies are evaluated and applied in the order listed.

- You can move a given policy up or down in the order by clicking the ellipsis **...** button.
- Likewise, you can delete a policy by clicking the ellipsis and then **Delete**
- Steering policies are required when used with SRX series devices.
- To add applications from the Access Policies section, click the **Edit Applications** button.

For our current hub-spoke example, we will create five access policies, listed below. The figure below shows them in the context of a screenshot.



Steps for the first access policy are provided, after which you can use the details in the table to complete the others.

Access Policies

- **Policy 1**—**internet**. This policy provides an Internet breakout through the underlay at the hub.
- **Policy 2** —**dc-ping**. This policy provides a local breakout through the underlay for guest users (TCP ports 80 and 443, and UDP port 53) only.
- **Policy 3**—**dc-to-spokes**. This policy allows inbound and outbound traffic over the aggregate network attached to the overlay.
- **Policy 4**—**publish-ssh**. This policy allows inbound and outbound spoke-to-spoke traffic over the aggregate network attached to the overlay.
- **Policy 5**—**TestPOL**.

To create an access policy,

1. Under the **Access Policy** section, click the **Add Policy** button to create a new rule in the policy list.
2. Click the new field under the **Name** column and give the policy a name. Here, we will use **internet**, then click the blue checkmark to apply your changes.
3. Click the **+** icon in the **Network/User** column and in the drop-down that appears, select **dc1-servers** from the list of network/user combos that appears.
4. Select **Allow** for the **Action**. This controls the network/users' access to the application over the given path.
5. Click the **+** icon in the **Application/Destination** column, and then any from the list of applications that appears.
6. Click the **+** icon in the **Traffic Steering** column and in the drop-down that appears, select underlay from the list of policies that appears.

Values for Access Policies in Hub Profiles

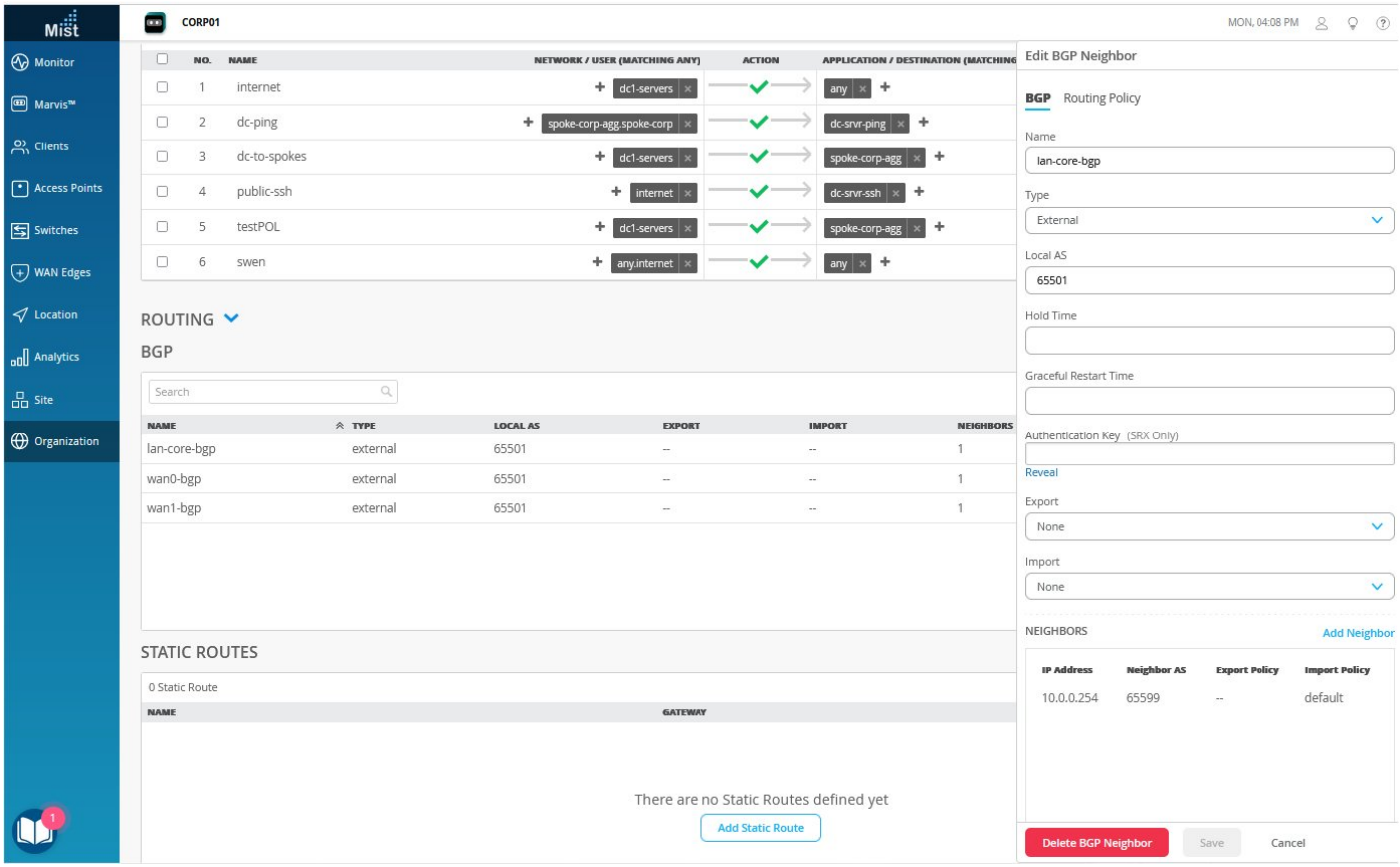
Order	Name	Network/User	Action	Application/Destination	Traffic Steering
1	internet	dc1-servers	Allow	any	underlay
2	dc-ping	spoke-corp-agg.spoke-corp	Allow	dc-srvr-ping	dc1-servers
3	dc-to-spokes	dc1-servers	Allow	spoke-corp-agg	overlay
4	public-ssh	internet	Allow	dc-srvr-ssh	dc1-servers
5	testPOL	dc1-servers	Allow	spoke-corp-agg	dc1-servers

Hub Profiles: Routing

IN THIS SECTION

The Juniper Mist cloud uses Border Gateway Protocol (BGP) for routing traffic between the hub and spokes.

We will set up three routing instances, one for the LAN, and two for the WAN links. The figure below shows the BGP routes in the context of a screenshot.



To set up BGP Routing,

1. Under the **Routing** section, click the **Add BGP Neighbors** button to display the Add BGP Neighbor configuration screen.
2. Give the instance a name. In this example we'll use **lan-core-bgp** but any name will do.
3. For **Type**, choose **External** from the dropdown.
4. For **Local AS**, enter **65501** (or whatever is appropriate for your environment).
5. Under **Neighbors**, click **Add Neighbor** and then populate the screens as follows:
   - IP Address: **10.0.0.254**

- Neighbor AS: **65599**
- Hold time: **<null>**
- Export: **none**
- Import: **default**

6. Click the blue checkmark in the upper corner of the box to apply your changes.
7. Next, select the **Routing Policy** tab at the top of the screen.
8. In the **Routing Policy** panel, click **Create Policy**, and then give the policy a name. For this first policy, we'll use **default** as the name.
9. Click **Add Term** and then populate the screens with the values from the table.

default policy	Terms
Prefix	0.0.0.0/0
AS path	64510
Protocol	BGP
Community	<null>
Then	Accept

10. Click the blue checkmark in the upper corner of the box to apply your changes.
11. Click **Create Policy**, and then give this new policy a name. For this example, we'll use **export** as the name.
12. We'll add three terms to the export policy. For each, click **Add Term** and populate the screens using the values from the table.

export policy_term_1	export policy_term_2	export policy_term_3
Prefix: 10.11.0.0/30	Prefix: 10.11.1.0/30	Prefix: 0.0.0.0/0
AS path: <null>	AS path: <null>	AS path: <null>
Protocol: None	Protocol: None	Protocol: None
Community: <null>	Community: <null>	Community: <null>
Then: Accept	Then: Accept	Then: Reject

13. Click the blue checkmark in the upper corner of the box to apply your changes.

14. Add the two remaining BGP neighbors using values from the table and the table.
15. When creating the BGP neighbors, for the **Routing Policy** tab, use values from the table to create the associated routing policies and terms. The same terms apply to every instance of the export policy used in this example, that is, those shown in the figure.
16. When done, click the **Save** button.

BGP Neighbors

Name: lan-core-bgp	**Name: wan0-bgp**	**Name: wan1-bgp**
Type: External	Type: External	Type: External
Local AS: 65501	Local AS: 65501	Local AS: 65501
Hold Time: <null>	Hold Time: <null>>	Hold Time: <null>
Graceful Restart Time: <null>	Graceful Restart Time: <null>	Graceful Restart Time: <null>
Authentication Key: <null>	Authentication Key: <null>	Authentication Key: <null>
Export: None	Export: None	Export: None
Import: None	Import: None	Import: None
Add Neighbors >	**Add Neighbors >**	**Add Neighbors >**
IP Address: 10.0.0.254	IP Address: 10.11.0.1	IP Address: 10.11.1.1
Neighbor AS: 65999	Neighbor AS: 64510	Neighbor AS: 64511
Hold Time: <null>	Hold Time: <null>	Hold Time: <null>
Export: None	Export: export	Export: export
Import: default	Import: default	Import: default

Hub Profiles: CLI Configuration

Not all Junos OS commands are available through the Juniper Mist cloud console. Instead, you can use the CLI Configuration window to include any additional configuration settings that you need to run on the SRX Services Gateway.

Junos OS commands entered here will be merged with rest of the configuration that you've made through the Juniper Mist cloud console.

We recommend that when adding commands, you use the “groups” configuration, where applicable, so the statements are easier to maintain.

Use the Junos OS “set” command format for all commands entered in the window.

To include custom CLI commands along with the hub profile configuration,

- Copy and paste the following commands in the **CLI Configuration** field:

```
set system root-authentication encrypted-password "$6$BOH8DxtT$wIakTFwjtQEffPUlCMzXYd9eA1if/
KKrIyXz2a.yovJWMvYHwbSCje1ixTgs8C4i/S/MlFLvvZsaxUL30dFpM/"
delete apply-groups mist_add_cli
delete groups mist_add_cli
set apply-groups mist_add_cli
delete system max-configuration-rollbacks
delete system max-configurations-on-flash
set groups mist_add_cli system max-configurations-on-flash 15
set groups mist_add_cli system max-configuration-rollbacks 15
set security zones security-zone wan0 host-inbound-traffic system-services ping
set security zones security-zone wan1 host-inbound-traffic system-services ping
set groups top routing-instances vpn_OrgOverlay protocols bgp group OrgOverlay_overlay bfd-liveness-detection
minimum-interval 1500
set groups top routing-instances vpn_OrgOverlay protocols bgp group OrgOverlay_overlay bfd-liveness-detection
multiplier 6
set groups top routing-instances vpn_OrgOverlay protocols bgp group OrgOverlay_overlay bfd-liveness-detection
session-mode automatic
```

Hub Profiles: Save

IN THIS SECTION

It has been a big day, we know. Before you go home, there’s one more ask for the new branch office. You'll need to establish a secure IPsec VPN tunnel to the remote corporate office. This tunnel allows members of the *trust* zone to securely reach specific corporate resources on the 172.16.200.0/24 subnet over the Internet.

Secure tunnels are a key feature of SRX platforms. Being able to send sensitive traffic over the public Internet without concern for eavesdropping, or data theft, is no small task. An IPsec VPN lets you securely tunnel traffic through the public Internet. Because the traffic is tunneled, there's no need to perform source NAT.

- IPsec tunnel
- Use the Junos CLI to verify IPsec VPN operation

In this example, traffic sent from the *trust* zone to 172.16.200.0/24 uses the IPsec tunnel. This traffic bypasses source NAT and exits the remote end with the original source IP from the 192.168.2.0/24 *trust-vlan* subnet.

Task 5: Configure WAN Edge Templates

IN THIS SECTION

The WAN Edge template is where you connect the various elements we've constructed so far, as well as define common spoke characteristics including WAN interfaces, DHCP servers, traffic steering rules, and access policies, and then apply these configurations to the WAN Edge devices.

In this task, we'll set up two templates for the WAN Edge spokes. We'll bind both to our site, where they will pick up the overlay, application, and user information we configured. At the same time, the site will resolve the variables we use in the template.

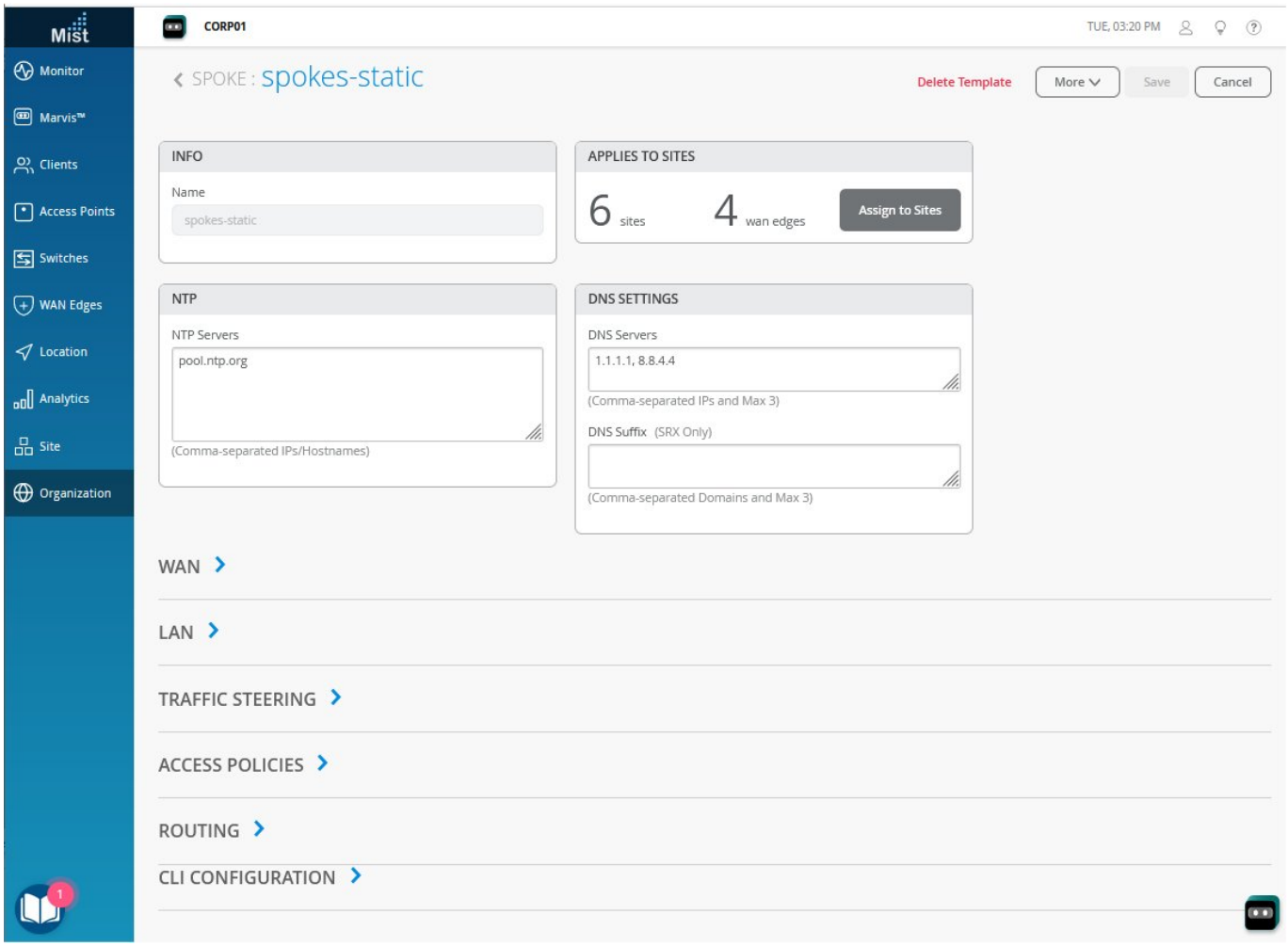
Many of the template elements will be familiar from the Hub Profiles we just created – LAN, WAN, Traffic Steering, and Access Rules. The difference is that whereas the hub profile attaches to a specific hub only, we create the WAN Edge Template for the spoke devices, and attach them to the site.

At the end of this task, we'll have connected the various spoke users to the applications they can access on the hub (with its separately defined WAN links and overlay), defined the path that the network traffic will take between the spoke and hub, and applied our security policies to those flows.

To configure a template for the WAN Edge,

1. In the Juniper Mist menu, 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.
3. In the box that appears, give your template a name (we use **spokes-static** in this example) and select **Spoke** as the type.

4. Click the **Create** button. The WAN Edge template appears, as shown in the figure below.



5. Under **NTP**, enter the hostname or IP address of the NTP server(s) you want the spoke to use. Here, we use **pool.ntp.org** , a virtual, global cluster of public times servers.

6. Likewise, under **DNS Settings**, enter the hostname or IP address of the DNS server(s) you want the spoke to use for the domain name resolution of hosts on the Internet. Here, we use **8.8.4.4** and **1.1.1.1**, which are public DNS servers.

7. (Optional) Specify up to three domain suffixes. These will be automatically appended, in the order specified, to accommodate unqualified computer names in DNS query.

WAN Edge Templates: WAN

IN THIS SECTION

We'll add two WAN links to the template.

1. Under the WAN section, click the **Add WANs** button to open the **Add WAN Configuration** panel.
2. Give the WAN a name. Here, we'll use **wan0**.
3. For **WAN Type**, choose **Ethernet** (this appears as "broadband" in the WAN list).
4. For **Interface**, type **ge-0/0/0**.
5. To configure the IP address of the WAN link, use the following values:
   - IP Address: **{{wan0_ip}}**
   - Prefix Length: **{{wan0_mask}}**
   - Gateway: **{{wan0_gw}}**
6. For **Source NAT**, select **Enabled**.
7. Below the **Overlay Hub Endpoints** panel, click the **Endpoints** dropdown and select **h1-wan0** from the list that appears.
8. For **BDF Profile**, choose **None**.
9. Click **Save** to add this to the WAN list.

Values for wan1 in the WAN Edge template

Name	Value
Name	wan1
WAN Type	Ethernet
Interface	ge-0/0/1
Port Aggregation	Not selected
Redundant	Not selected
VLAN ID	<null>
IP address	{{wan1_ip}}
Prefix Length	{{wan1_mask}}
Gateway	{{wan1_gw}}
Source NAT	Enabled

Traffic Shaping	Disabled
Endpoint	h1-wan1
BDF Profile	None

WAN Edge Templates: LAN

IN THIS SECTION

We'll add two LANs to this WAN Edge template by selecting them from the Network list.

1. Under the **LAN** section, click the **Add LANs** button to open the **Add LAN Configuration** panel.
2. Click the drop-down under **Network** and select **spoke-corp** from the list of networks that appears. When you do, the remaining configuration will be automatically filled in.
3. Use the table to review the LAN settings and click **Add** to add it to the list of LANs.

LAN Configurations for the WAN Edge Template

Name: spoke-corp	**Name: spoke-guest**
Interface: ge-0/0/2	**Interface**: ge-0/0/3
Port Aggregation: not selected	**Port Aggregation**: not selected
Redundant: not selected	**Redundant**: not selected
IP Address: {{spoke_corp_ip}}	**IP Address**: {{spoke_guest_ip}}
Prefix Length: {{spoke_mask}}	**Prefix Length**: {{spoke_mask}}
Redirect Gateway: <null>	**Redirect Gateway**: <null>
Untagged VLAN: Yes	**Untagged VLAN**: Yes
DHCP: Server	**DHCP**: Server
IP Start: {{spoke_corp_dhcp}}2	**IP Start**: {{spoke_guest_dhcp}}1

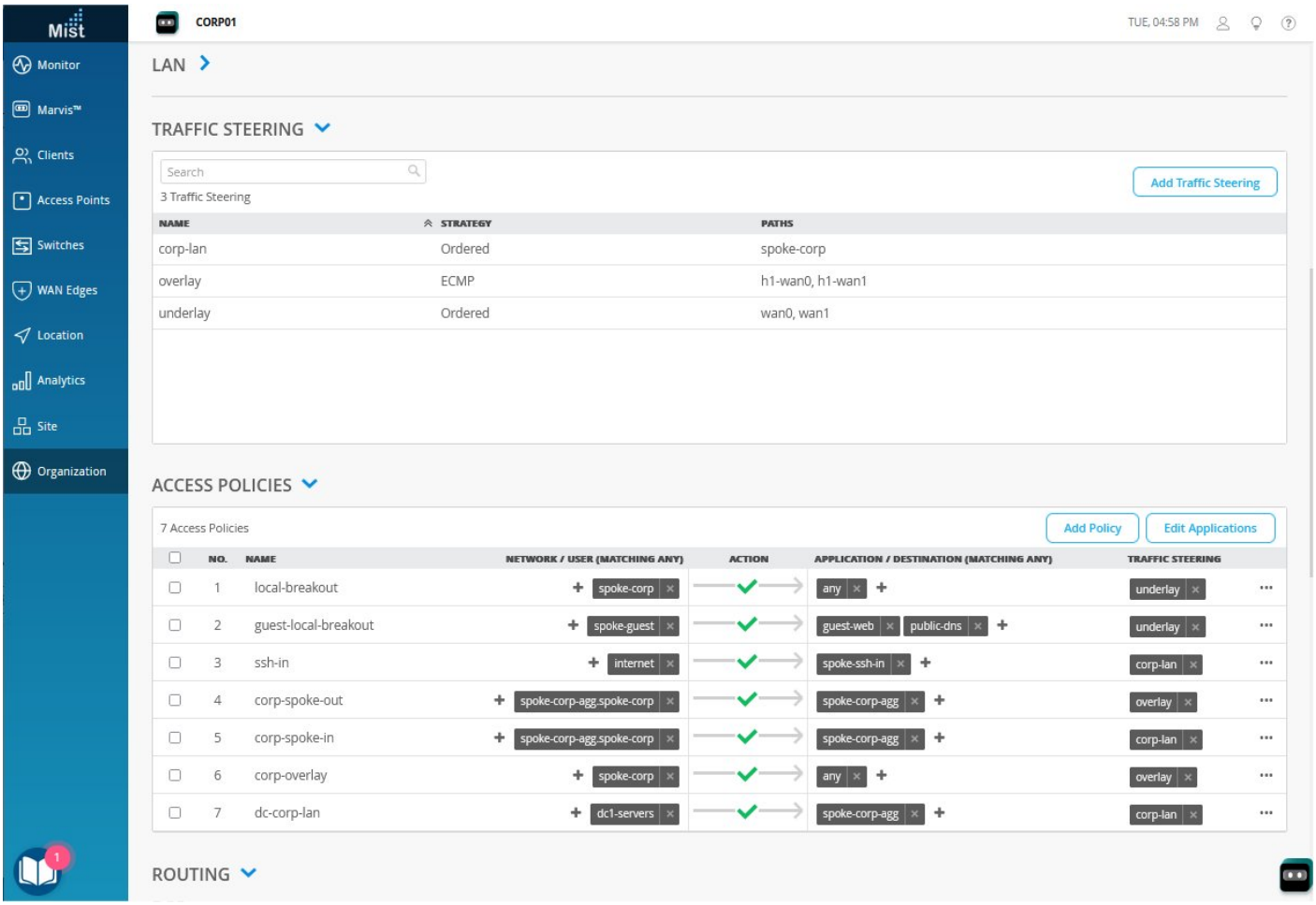
IP End: {{spoke_corp_dhcp}}254	**IP End**: {{spoke_guest_dhcp}}253
Gateway: {{spoke_corp_dhcp}}1	**Gateway**: {{spoke_guest_dhcp}}254
DNS Servers: {{dns_1}}, {{dns_2}}	**DNS Servers**: {{dns_1}}, {{dns_2}}
DNS Suffix: <null>	**DNS Suffix**: <null>

WAN Edge Templates: Traffic Steering

IN THIS SECTION

Just like with hub profiles, traffic steering is where you define the different paths that application traffic can take to traverse the network. Destination zone is also determined by the paths configured within traffic steering.

We will set up three traffic steering policies, one for the *overlay*, one for the *underlay*, and one for the *corporate LAN*, which is detailed here. The figure below shows the policies in the context of a screenshot.



To set up Traffic Steering,

1. Under the **Traffic Steering** section, click the **Add Traffic Steering** button to display the **Traffic Steering** configuration screen.
2. Give your policy a name. Here, we'll use **corp-lan**, but any name will do.
3. For **Strategy**, choose **Ordered**.
4. Click **Add Paths** to expose the **Add Path d**rop-down.
   - For **Type**, choose **LAN**.
   - For **Name**, choose **spoke-corp**.
5. Click the blue checkmark in the corner of the panel to post these settings to the Juniper Mist cloud.
6. Click **Save** to add the policy to the list.

Values for the Traffic Steering Policies in the WAN Edge template

Name	Field	Value	Paths	Value	Value
corp-lan	Strategy:	Ordered			

			spoke-corp	Type:	LAN
				Network:	spoke-corp
Overlay	Strategy:	ECMP			
			h1-wan0	Type:	Overlay
				Name:	h1-wan0
			h1-wan1	Type:	Overlay
				Name:	h1-wan1
Underlay	Strategy:	Ordered			
			wan0	Type:	WAN
				Name:	wan0
			wan1	Type:	WAN
				Name:	wan1

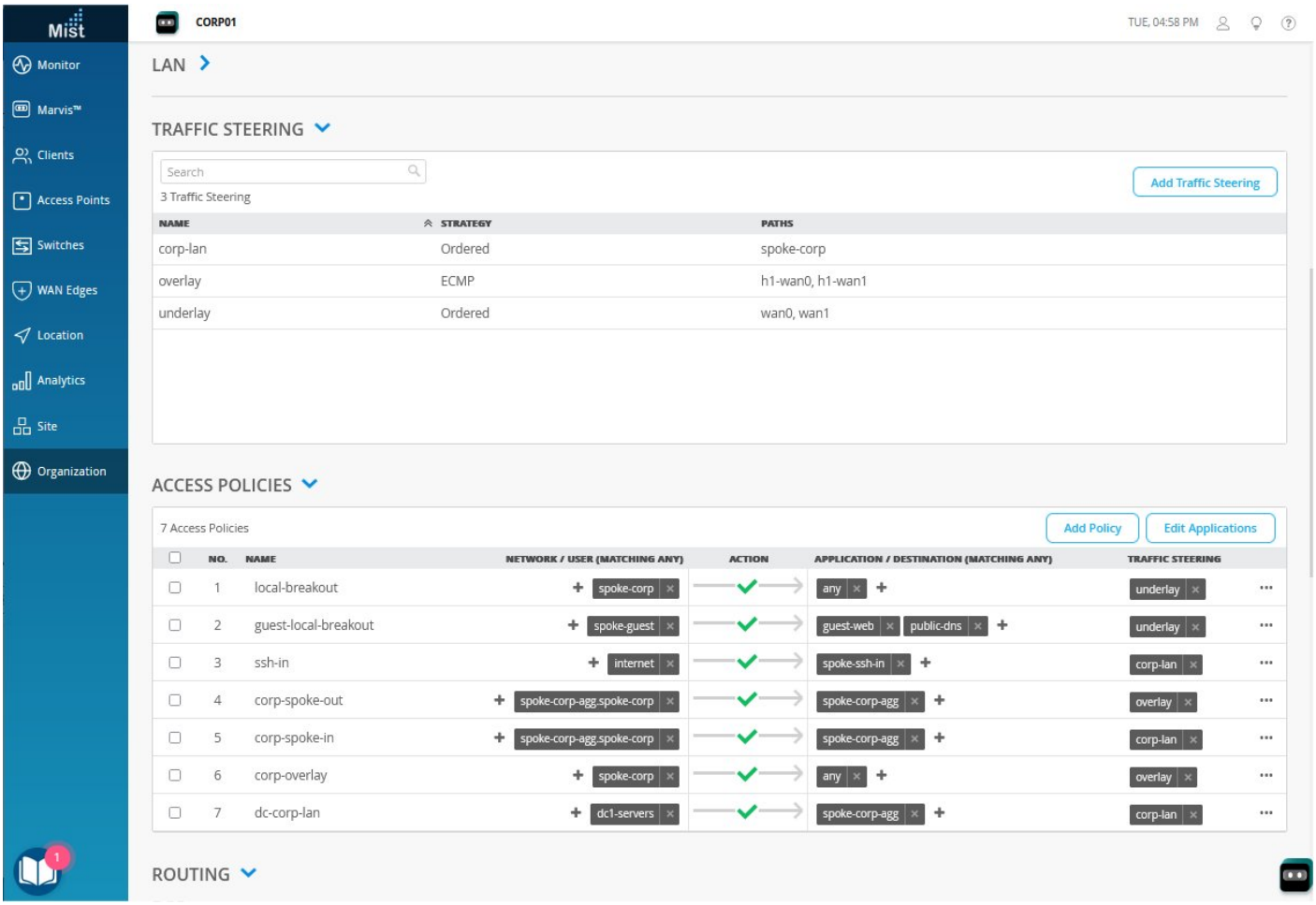
WAN Edge Templates: Access Policy

IN THIS SECTION

Access policies are where you define which network/users can access which applications, and according to which traffic steering policy. The source zone is determined by the Networks/Users and the destination zone is determined by the Application + Traffic Steering path. Additionally, you can assign an action of *Permit* or *Deny*. Access policies are evaluated and applied in the order listed.

- You can move a given policy up or down in the order by clicking the ellipsis **...** button.
- Likewise, you can delete a policy by clicking the ellipsis and then **Delete**
- Steering policies are required when used with SRX series devices.
- To add applications from the Access Policies section, click the **Edit Applications** button.

For our current hub-spoke example, we will create seven access policies, listed below. The figure below shows them in the context of a screenshot.



Steps for the first access policy are provided, after which you can use the details in the table to complete the others.

Spoke Policies

- **Policy 1— local-breakout**. Provides a local breakout through the underlay.
- **Policy 2 —guest-local-breakout**. Provides a local breakout through the underlay for guest users (TCP ports 80 and 443, and UDP port 53) only.
- **Policy 3— ssh-in**. Allows inbound traffic to the hub from the spokes through the corporate LAN.
- **Policy 4— corp-spoke-out**. Allows outbound spoke-to-spoke traffic over the aggregate network attached to the overlay.
- **Policy 5— corp-spoke-in**. Allows inbound spoke-to-spoke traffic over the aggregate network attached to the overlay.
- **Policy 6— corp-overlay**. Provides an Internet breakout through the overlay at the Hub
- **Policy 7—dc-corp-lan**.

To create an access policy,

1. Under the **Access Policy** section, click the **Add Policy** button to add a new rule in the policy list.

2. Click the new field under the **Name** column and give the policy a name. Here, we will use **local-breakout**, then click the blue checkmark to apply your changes.
3. Click the **+** icon in the **Network/User** column and in the drop-down that appears, select **spoke-corp** from the list of network/user combos that appears.
4. Select **Allow** for the **Action**. This controls the network/users' access to the application over the given path.
5. Click the **+** icon in the **Application/Destination** column, and then **any** from the list of applications that appears.
6. Click the **+** icon in the **Traffic Steering** column and in the drop-down that appears, select **underlay** from the list of policies that appears.

Values for Access Policies in the WAN Edge Template

Order	Policy Name	Network/User	Action	Application/Destination	Traffic Steering
1	local-breakout	spoke-corp	Allow	any	underlay
2	guest-local-breakout	spoke-guest	Allow	guest-web pulbic-dns	underlay
3	ssh-in	internet	Allow	spoke-ssh-in	corp-lan
4	corp-spoke-out	spoke-corp-agg.spoke-corp	Allow	spoke-corp-agg	overlay
5	corp-spoke-in	spoke-corp-agg.spoke-corp	Allow	spoke-corp-agg	corp-lan
6	corp-overlay	spoke-corp	Allow	any	overlay
7	dc-corp-lan	dc1-servers	Allow	spoke-corp-agg	corp-lan

WAN Edge Templates: Routing

There are no BGP neighbors or routing policies to set up for the WAN Edge template.

There are no static routes to set up for the WAN Edge template.

WAN Edge Templates: CLI Configuration

Junos OS commands entered here will be merged with rest of the configuration that you've made through the Juniper Mist cloud console.

We recommend that when adding commands, you use the "groups" configuration, where applicable, so the statements are easier to maintain.

Use the Junos OS "set" command format for all commands entered in the window.

To include custom CLI commands along with the hub profile configuration,

- Copy and paste the following commands in the **CLI Configuration** field:

```
delete apply-groups mist_add_cli
delete groups mist_add_cli
set apply-groups mist_add_cli
delete system max-configuration-rollbacks
delete system max-configurations-on-flash
set groups mist_add_cli system max-configurations-on-flash 15
set groups mist_add_cli system max-configuration-rollbacks 15
set groups top routing-instances vpn_OrgOverlay protocols bgp group OrgOverlay_overlay bfd-liveness-detection
minimum-interval 1500
set groups top routing-instances vpn_OrgOverlay protocols bgp group OrgOverlay_overlay bfd-liveness-detection
multiplier 6
set groups top routing-instances vpn_OrgOverlay protocols bgp group OrgOverlay_overlay bfd-liveness-detection
session-mode automatic
```

WAN Edge Templates: Save

The WAN Edge template is complete. To save it, scroll to the top of the page and click the **Save** button to push the configuration to the device.

For SRX Service Gateways, the configuration settings are Junos commands. For SSR devices, the configuration settings are programmable command line interface (PCLI) commands.

Task 6: Attach Template To Site

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).

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

1. Scroll to the top of the WAN Edge Templates page and click the **Assign to Sites** button. The Assign Template to sites window appears.
2. Select the **dc1 site** we created in our first task from the list of available sites.
3. Click the **Apply** button.

Final Step: What's Next

Congratulations! You've got your hub and spoke network configured for WAN Assurance on the Juniper Mist cloud.

We showed you how to use the Juniper Mist cloud console to provision a sample hub and spoke network. The network traverses provider equipment via IPSec tunnels, and leverages both access policies and traffic shaping rules to segment users and applications on the network.

Here are some additional resources you might want to check out next.

Table 1: What's Next

If you want to	Then
Create a Mist Account and Organization	See Create a Mist Account and Organization
Learn about WAN Assurance for the SSR, which is available for Mist Cloud users.	See Staging.
Onboard and adopt an SSR Router Into The Mist Cloud	See Onboarding.
Learn More About WAN Assurance	See WAN Assurance
Learn How to Automate Juniper Mist Using the API	See Automation with APIs
Set up your SRX device with advanced security measures to protect and defend your network	See SRX Series Up and Running with Advanced Security Services
See the Junos OS documentation	Visit the Junos OS documentation page
View the WAN Assurance Datasheet	See Juniper Mist WAN Assurance Datasheet

Our video library continues to grow! We've created many, many videos that demonstrate how to do everything from install your hardware to configure advanced Junos OS network features. Here are some great video and training resources that will help you expand your knowledge of Junos OS and branch SRX devices.

Table 2: Learn With Videos

If you want to	Then
View a Video on Provisioning for WAN Assurance	See Provisioning for WAN Assurance

Table 2: Learn With Videos *(Continued)*

If you want to	Then
View a Web-based training video which provides an overview of the SRX320 and describes how to install and configure it	Visit the SRX300 and SRX320 Services Gateways Overview and Deployment (WBT) page
View a list of the many free technical trainings we offer at Juniper	Visit the Getting Started page on the Juniper Learning Portal