Juniper Networks | Engineering Simplicity

Contrail Service Orchestration

Deployment Guide

Published
2020-11-10

Release
5.3.0

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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.

Contrail Service Orchestration Deployment Guide
5.3.0
Copyright © 2020 Juniper Networks, Inc. All rights reserved.

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.

Table of Contents

About the Documentation | vi

Documentation and Release Notes | **vi**

Documentation Conventions | **vi**

Documentation Feedback | **ix**

Requesting Technical Support | **ix**

- Self-Help Online Tools and Resources | **x**
- Creating a Service Request with JTAC | **x**

1 **Solutions Overview**

About this Deployment Guide | 12

Contrail Service Orchestration (CSO) Solutions Overview | 12

- Contrail Software-Defined WAN Solution (SD-WAN) | **14**
- Contrail Software-Defined LAN Solution (SD-LAN) | **15**
- Next Generation Firewall (NGFW) Deployment Model | **16**

2 **Deployment Tools**

Contrail Service Orchestration (CSO) Deployment Tools | 19

Contrail Services Orchestration (CSO) GUIs | 19

Designing and Publishing Network Services | 21

Contrail Service Orchestration (CSO) License Tool | 22

- Overview of the License Pages | **22**

3 **SD-WAN Deployment**

SD-WAN Deployment Overview | 26

Contrail SD-WAN Hardware and Software Requirements | 27

- Contrail SD-WAN Reference Architecture | **27**
- Spoke Devices | **28**
  - On-Premises Spoke Devices | **28**
  - Cloud Spoke Devices | **30**
  - Spoke Redundancy | **30**

Provider Hub Devices | 30

Provider Hubs | 31

Provider Hub Redundancy | 32

Enterprise Hub Sites and Devices | 32

Initial SD-WAN Deployment | 34

Before You Begin | 35

Download Intrusion Protection System (IPS) and Application Signatures | 35

Upload Licenses | 38

Add a New Tenant | 38

Modify Device Templates | 40

Choose a Point of Presence (POP) for the Hub | 44

Add a Provider Hub Device to Your Tenant | 44

Add an Enterprise Hub to Your Tenant | 48

Add an On-Premises Spoke for the Tenant | 52

Install a License on a Device | 58

Install an Application Signature on a Device | 58

Add Firewall and NAT Policies to the Topology | 59

Add SD-WAN SLA-Based Steering Profiles and Policy | 61

4 **SD-LAN Deployment**

SD-LAN Deployment | 64

SD-LAN Deployment Overview | 64

SD-LAN Deployment | 69

5 **Standalone Next-Generation Firewall (NGFW) Deployment**

Next-Generation Firewall (NGFW) Deployment | 74

NGFW Deployment Overview | 74

NGFW Deployment Architecture | 75

NGFW Deployment | 76

6 **Appendix A - Network Function Virtualization in Contrail Service Orchestration**

Network Function Virtualization in the Contrail Service Orchestration Deployments | 81

VNFs Supported by the Contrail Service Orchestration Solutions | 83

7

Appendix B - Manual Staging of NFX

Install Junos OS Software onto an NFX Series Device from a USB Drive | 86

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | vi
- Documentation Conventions | vi
- Documentation Feedback | ix
- Requesting Technical Support | ix

Use this guide to understand the next steps you should take after a successful installation of CSO software (either on-premises or cloud-hosted). This guide describes the solutions available in CSO and the workflows involved in their deployment.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Documentation Conventions

Table 1 on page vii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page vii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

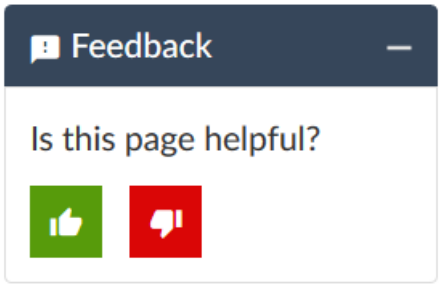
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

1

CHAPTER

Solutions Overview

About this Deployment Guide | 12

Contrail Service Orchestration (CSO) Solutions Overview | 12

About this Deployment Guide

The intent of this deployment guide is to provide an understanding of the available Contrail Service Orchestration (CSO) solutions by:

- Briefly discussing each of the available solutions
- Discussing the tools and devices required to implement the solutions
- Providing an end-to-end walkthrough of each of the solutions and covering the deployment specifics

This guide is available on the Contrail Service Orchestration Documentation page, which includes several other helpful guides:

- *Contrail Service Orchestration Quick Start Guide*
- *Contrail Service Orchestration Administration Portal User Guide*
- *Contrail Service Orchestration Customer Portal User Guide*
- *Contrail Service Orchestration Monitoring and Troubleshooting Guide*
- Contrail SD-WAN and SD-LAN - Design and Architecture Guide
- And more!

Contrail Service Orchestration (CSO) Solutions Overview

IN THIS SECTION

- Contrail Software-Defined WAN Solution (SD-WAN) | **14**
- Contrail Software-Defined LAN Solution (SD-LAN) | **15**
- Next Generation Firewall (NGFW) Deployment Model | **16**

Juniper Networks Contrail SD-WAN, SD-LAN, and NGFW management solutions offer automated branch connectivity while improving network service delivery and agility. CSO is a multi-tenant platform that manages physical and virtual network devices, creates and manages Juniper Networks and third-party virtualized network functions (VNFs), and uses those elements to deploy network solutions for both

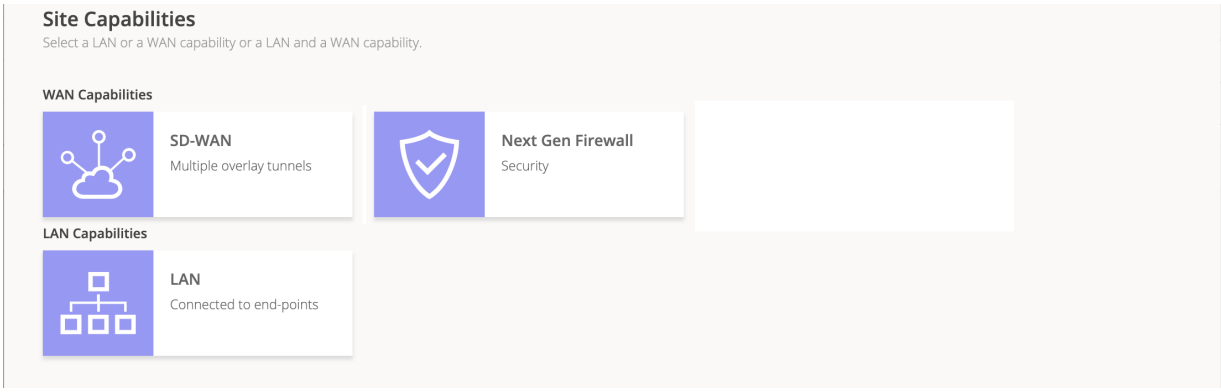
enterprises and service providers (SPs) and their customers. CSO multi-tenancy provides security and tenant isolation that keeps the objects and users belonging to one tenant or operating company (OpCo) from seeing or interacting with those of another tenant or OpCo.

The CSO platform itself can be deployed in one of two ways:

- As a downloadable, on-premises platform in which you (or your company) become the SP administrator (cspadmin user). In an on-premises deployment, the cspadmin user has complete read-write management access and responsibility for the CSO micro-services platforms, orchestration and management infrastructure, and all underlay networks needed to allow access to CSO and its solutions.
- As a software-as-a-service (SaaS) platform, hosted in a public cloud, to which tenants and OpCos subscribe. In an SaaS deployment, Juniper Networks manages the necessary microservices infrastructure, the secure orchestration and management (OAM) infrastructure, and underlay networks needed to allow access to CSO and its solutions.

CSO offers multiple network solutions that benefit enterprise customers and service providers and their customers. The solutions are split into two overall groups, WAN solutions and LAN solutions as shown in Figure 1 on page 13.

Figure 1: WAN and LAN Solutions



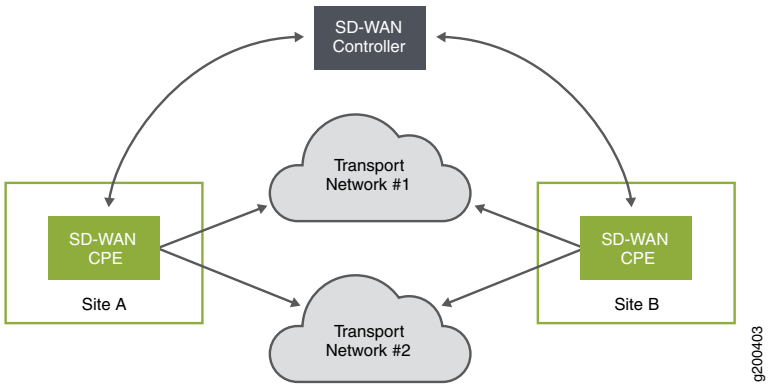
These solutions allow CSO to do the following:

- Provide lifecycle management for devices and services
- Automate physical and virtual device provisioning
- Provide Day 0, Day 1, and Day 2 configuration
- Monitor remote devices
- Provide full lifecycle management of firewall, NAT, and Internet breakout policies for user traffic
- Provide high-level reporting about devices and user traffic

Contrail Software-Defined WAN Solution (SD-WAN)

The Contrail SD-WAN solution offers a flexible and automated way to route traffic through the cloud using overlay networks. It is an overlay network solution that provides an enhanced application user experience. It acts as both a data controller and a management orchestrator. At its most basic, an SD-WAN solution encompasses multiple sites, multiple connections between sites, and a WAN controller as shown in Figure 2 on page 14.

Figure 2: Basic SD-WAN Concept



The CPE devices in a Contrail SD-WAN solution (also known as *on-premises spoke devices*) have a WAN side and a LAN side. On the WAN side, hub-and-spoke and dynamic mesh topologies are supported. The CPE devices use at least one, and up to four, WAN interfaces as connection paths to provider hub devices, enterprise hub devices, other spoke devices, and the Internet. The supported hub devices are shown in Table 3 on page 14:

Table 3: Supported Hub Devices

Hub Device	Used as
vSRX	Enterprise Hub and Provider Hub
SRX1500	Enterprise Hub and Provider Hub
SRX4100	Enterprise Hub and Provider Hub
SRX4200	Enterprise Hub and Provider Hub

The hub devices help to provide the overlay networking needed for the Contrail SD-WAN solution.

CSO allows you to give preference to one WAN path over another for any given traffic through the use of traffic steering and breakout profiles. Thus, business-critical traffic and data can be routed through the

provider hub using MPLS/GRE while non-critical traffic can be routed over the Internet connection through an IPsec tunnel. Each path can have a service level agreement (SLA) profile applied. The SLA profile monitors the path for latency, congestion, and jitter while also accounting for path preference. Should the path fail to meet one or more of the required parameters, traffic is re-routed to another path automatically.

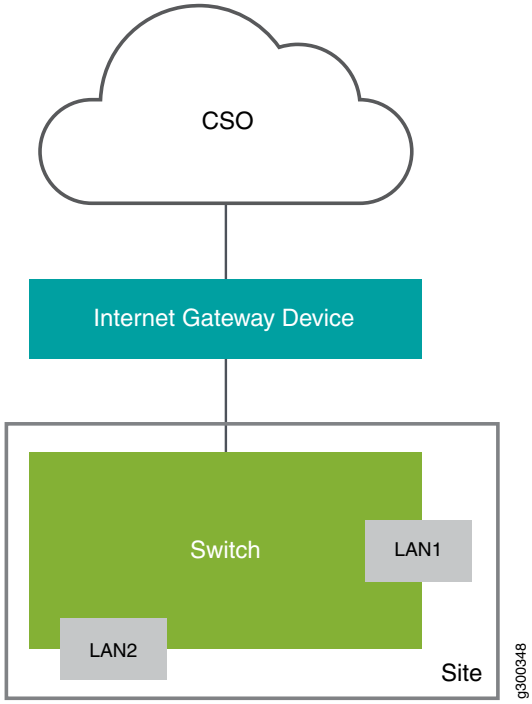
The LAN side of the CPE devices connect to the customer's LAN segments. Multiple departments at the customer site that occupy different LAN segments can have their traffic securely segregated with the use of dedicated IPSec tunnels. NFX Series spoke devices can also provide service chains of network services in addition to the routing flexibility already available.

You can use the solutions as turnkey implementations or connect to other operational support and business support systems (OSS/BSS) through northbound Representational State Transfer (REST) APIs.

Contrail Software-Defined LAN Solution (SD-LAN)

The SD-LAN solution allows CSO to manage and monitor remote LAN devices like certain EX Series LAN switches, Mist WiFi access points, and certain SRX Series next generation firewall (NGFW) devices. This extends the SD-WAN solution to provide visibility into the LANs of remote networks. At its most basic, a managed LAN implementation is as simple as connecting a supported EX switch or SRX firewall at the remote site through an Internet gateway device as shown in Figure 3 on page 16.

Figure 3: Simple SD-LAN Solution

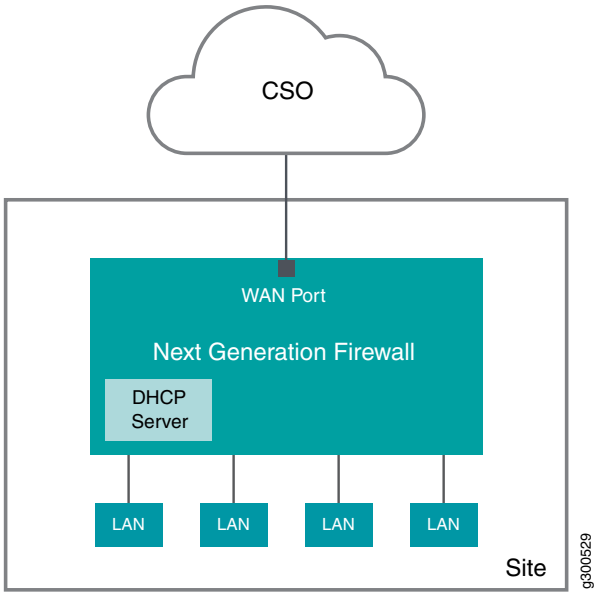


While Figure 3 on page 16 shows a single switch connected behind an Internet gateway device, there are several other deployment options available within the solution. For example, an EX switch can be attached to an existing managed CPE device, or it can be added to CSO as a standalone LAN switch. Similar deployment options are available for the NGFW solution. For more details about switch deployment in a managed LAN solution, see the *Adding and Provisioning Switches to Provide LAN Capability to a Site Overview* and the CSO Design and Architecture Guide.

Next Generation Firewall (NGFW) Deployment Model

The NGFW deployment focuses on providing remote network security through the use of SRX Series NGFW devices as CPE at the spoke site; unlike the SD-WAN deployments which focus on secure site-to-site connectivity and remote VNF deployment. A high-level view of the spoke site with NGFW is shown in Figure 4 on page 17.

Figure 4: NGFW Spoke Site



An NGFW deployment is carried out in the Customer Portal of CSO as a site deployment. The tenant under which the site is deployed must have the NGFW service available. This service is included in the tenant configuration by the tenant administrator during tenant onboarding. The remainder of this document provides a brief discussion of the architecture, and the steps that you need to perform in order to complete a NGFW deployment in CSO.

CHAPTER 2

Deployment Tools

Contrail Service Orchestration (CSO) Deployment Tools | 19

Contrail Services Orchestration (CSO) GUIs | 19

Designing and Publishing Network Services | 21

Contrail Service Orchestration (CSO) License Tool | 22

Contrail Service Orchestration (CSO) Deployment Tools

The following sections describe the deployment tools used by CSO. While these tools are used for deployments, they are also used for other purposes in CSO.

These sections discuss:

- **Administration and Customer Portals**

  These are web-accessible portals and provide work spaces in which CSO administrators and customers can create, view, or change the tenants, sites, devices, policies, and other objects used in CSO deployments.

- **CSO Designer Tools**

  These are tools with which you can create, modify, and deploy network services into CSO. The designer tools allow you to create custom services based on Juniper or third-party virtual network functions (VNFs).

  > **NOTE:** CSO Designer Tools are only available for on-premises CSO deployments.

- **CSO License Tool**

  The license tool allows you to install and maintain software licenses on deployed devices and to track CSO license installation.

Contrail Services Orchestration (CSO) GUIs

Access to CSO's GUI interfaces is achieved using a web browser. This document briefly describes how to access the various CSO GUI interfaces.

> **NOTE:** We recommend that you use Google Chrome (Version 60 or later) or Firefox (Version 78 or later) to access the Contrail Service Orchestration (CSO) GUIs.

See Table 4 on page 20 for information about logging into the Contrail Service Orchestration GUIs.

Table 4: Access Details for the GUIs

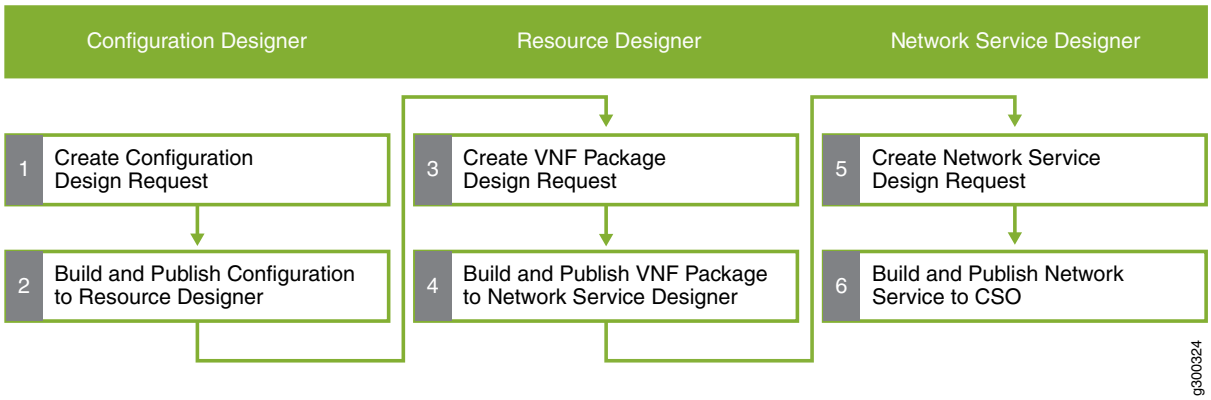
GUI	URL	Login Credentials
Administration Portal	• For cloud-hosted CSO: Login credentials are sent to each Administration Portal user as an e-mail. The address to which the e-mail is sent is the *username* and the e-mail contains a link including an activation code. Clicking the link takes you to the CSO login page which then prompts you to create a password. Once the new password is set, the CSO login URL can be seen in your browser's address bar. • For on-premises CSO: https://central-IP-Address Where: *central-IP-Address* is the IP address of the VM that hosts the microservices for the central POP For example: https://192.0.2.1	• For on-premises CSO: Specify the OpenStack Keystone username and password. The default username is **cspadmin**. Specify the autogenerated cspadmin password that is displayed on the console after the installation is complete. After upgrade, you must specify the cspadmin password of the previously installed version.
Customer Portal	Same as the URL used to access the Administration Portal	Login credentials are sent to each Customer Portal user as an e-mail. The address to which the e-mail is sent is the *username* and the e-mail contains a link including an activation code. Clicking the link takes you to the CSO login page which then prompts you to create a password..
Designer Tools—Log into Network Service Designer and click the menu in the top left of the page to access the other designer tools. **NOTE:** Access to Designer Tools is only available for on-premises deployments of CSO.	https://*central-IP-Address*:83 Where: *central-IP-Address* is the IP address of the VM that hosts the microservices for the central POP For example: https://192.0.2.1:83	Specify the OpenStack Keystone username and password. The default username is **cspadmin**. Specify the autogenerated cspadmin password that is displayed on the console after the installation is complete. After the upgrade, you must specify the cspadmin password of the previously installed version.

Designing and Publishing Network Services

NOTE: This section is only relevant for on-premises deployments of Contrail Service Orchestration (CSO).

The CSO Designer Tools consist of three tools that you use to create VNF templates, packages, and service chains that can be deployed as network services for the CSO solutions. CSO Designer Tools are not available for cloud-hosted deployments of CSO. You access the CSO Designer Tools at the same URL as the CSO Administration Portal, but on port 83. For example, if the IP address of the Administration Portal is 10.2.2.12, then the URL for Designer Tools would be: **https://10.2.2.12:83**. Figure 5 on page 21 shows an overview of the workflow used within the Designer Tools application.

Figure 5: Designer Tools Overview



- First, you use the *Configuration Designer* to create configuration templates for virtualized network functions (VNFs). The configuration templates specify the parameters that the customer can configure for a network service.
- Then, you use the *Resource Designer* to create VNF packages. A VNF package is based on a VNF template and specifies the network functions, function chains, and performance of the package.
- Finally, you use the *Network Service Designer* to:
  - Design service chains for network services using the VNF packages that you created with the Resource Designer.
  - Configure the network services.
  - Publish network services to the network service catalog.

You use the same process to create network services for SD-WAN deployments. The same network service

can not be shared between an on-premises site and the service provider's POP.

> **NOTE:** Currently, SD-WAN deployments support only Layer 2 service chains.

Contrail Service Orchestration (CSO) License Tool

IN THIS SECTION

- Overview of the License Pages | 22

Overview of the License Pages

CSO licenses come in two types: CSO software licenses and CPE platform licenses for hardware and Junos. CSO allows you to manage both the CSO licenses and any devices licenses that you use on your CPE devices. The following sections describe each of the license management pages.

> **NOTE:** For cloud-based CSO, Juniper Networks adds the licenses you have purchased on your behalf. For on-premises CSO, the SP Administrator adds the licenses.

You can use the SRX Series Services Gateways and vSRX Virtual Firewalls as on-premises spoke devices, provider hubs, or enterprise hubs in an SD–WAN solution. These devices require licensing in order to perform the functions needed for those solutions. Contrail Solutions Orchestration (CSO) provides a GUI-based method for loading licenses into CSO and installing them on the devices. The device licensing page is available in the Administration Portal or the Customer Portal by navigating to **Administration > Licenses > Device Licenses**. Licenses must first be purchased through your Juniper Networks account team or reseller. Once purchased, the text of the license is emailed to you.

The license page can be used to push licenses to the following devices.

- vSRX, SRX Series, or NFX Series devices in an SD–WAN solution
- SRX Series or EX Series CPE devices in an SD–LAN (managed branch) solution.

To upload a license to CSO for later push to an SRX, NFX, or EX device:

1. Login to CSO as an authorized user

   License management is available to tenant administrators. Operators can view, but cannot upload licenses to CSO or push them to devices.

2. Navigate to the **Administration > Licenses > Device Licenses** page.

   Here you can see a list of license files that have been uploaded to CSO. The list is empty if there have been no licenses uploaded.

3. Click the Add icon (**+**) at the top-right part of the list.

   The Add License page appears.

4. Click the **Browse** button to locate the license file that was e-mailed to you.

   Each file uploaded should be for one feature only. License files are generally named as the device serial number for which they are intended and have a **.txt** file extension.

5. (Optional) Enter a description of the license file.

   If uploading multiple licenses for a single device, a description can help you know which is which in the license list.

6. Click **OK** once you have filled in the required data.

   The license file will appear in the list along with the upload date, and your login under the **Uploaded By** column.

To install, or push, an uploaded license onto a device:

1. Click on the line or in the checkbox next to the appropriate license file.

2. Click the **Push License** pull-down menu and select **Push**. A pop-up window will appear.

   If you are logged in as a tenant administrator, you will see a list of sites and their assigned devices for your tenant.

3. Select the appropriate device, and click **Push Licenses**.

   Multiple licenses can be pushed to a single device.

The SP Administrator adds CSO licenses to the application. You can assign the added licenses to your tenants. The following procedure describes this process.

1. Click **Administration > Licenses > CSO Licenses**

   The CSO Licenses Page is displayed. All assigned licenses and the license counts appear in the list

2. Click the checkbox next to the license you want to assign.

3. Click the **Update Assignment** button.

   The **Assign CSO License** window appears and shows the quantity for this license and the number available for assignment to tenants

4. From the **Tenants** section, click the Add icon (**+**) button to add a new assignment.

   A new row on the list will appear.

5. From the **Tenant** pull-down menu, select the tenant.

6. Enter the number of licenses to assign to this tenant in the **Quantity** field. Alternatively, you can click the up and down arrows on the right of the field until the appropriate number appears in the field.

7. Click **OK**.

   The window will close and the **CSO Licenses** page will update immediately.

For more information about CSO licenses, see *About the Device License Files Page*.

3

CHAPTER

SD-WAN Deployment

SD-WAN Deployment Overview | **26**

Contrail SD-WAN Hardware and Software Requirements | **27**

Initial SD-WAN Deployment | **34**

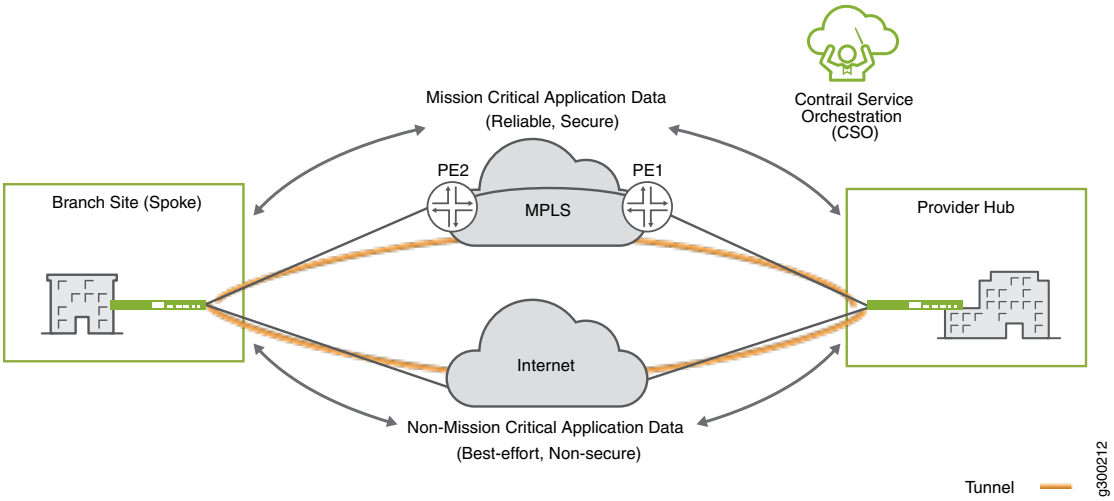
SD-WAN Deployment Overview

This walkthrough highlights the steps that you need to complete to deploy an SD-WAN solution using the hub-and-spoke topology with the provider hub device located in the service provider's cloud. We use an NFX250 Series device as the CPE and an SRX Series device as the provider hub in the SP cloud. We indicate where in the CSO GUI you need to go to complete each step. The document also provides some explanation of the choices that you need to make. It assumes that this is the first SD-WAN deployment you are attempting.

Additional information about using the Administration Portal GUI for any of the steps below can be found in the *Contrail Service Orchestration Administration Portal User Guide*.

The topology shown in Figure 6 on page 26 is a reference for this SD-WAN deployment.

Figure 6: SD-WAN Example Deployment Topology



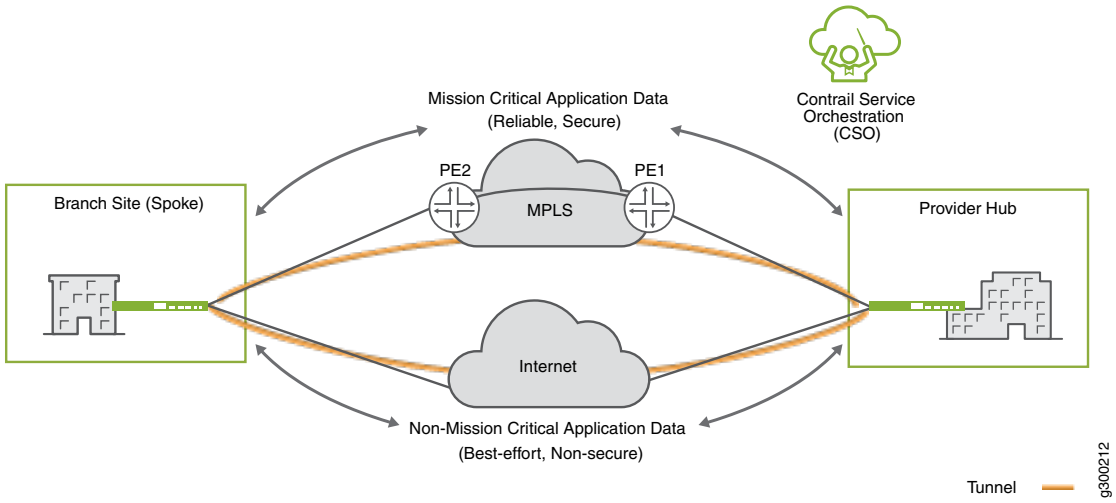
Contrail SD-WAN Hardware and Software Requirements

This topic gives a high level view of the SD-WAN architecture, and then provides specific hardware and software requirements for SD-WAN devices. For more details on the architecture, see the *Contrail SD-WAN Deployment Architectures* section of the CSO SD-WAN and SD-LAN - Design and Architecture Guide.

Contrail SD-WAN Reference Architecture

Juniper Networks Contrail SD–WAN solution architecture, shown in Figure 7 on page 27 uses a hub–and–spoke topology , with on-premises spoke devices located at customer branch sites. On the local side of the site, the on-premises spoke devices connect to LAN segments and participate in dynamic routing protocols with other LAN devices. On the WAN side, the on-premises spoke devices connect across two or more links to a provider hub device. Because the SD-WAN model uses a hub–and–spoke topology, traffic travels from site to site through the provider hub. By default, traffic going to the Internet also flows through the provider hub device.

Figure 7: Contrail SD-WAN Reference Architecture



You can also deploy an enterprise hub device, a special type of spoke device with hub-like properties that can offer Internet breakout services and connect spoke sites to each other over dynamic tunnels.

The SD-WAN orchestrator and controller functions are implemented through Juniper Networks Contrail Service Orchestration (CSO) software. The CSO platform uses policies and SLA parameters to differentiate and direct traffic flows across the available paths as desired.

The following sections describe the hardware and software requirements for devices used in an SD-WAN environment.

Spoke Devices

The CPE device at an enterprise customer's branch site acts as a spoke device in the SD-WAN model. The device also acts as a gateway router, providing connectivity from the branch site to other sites in the tenant network and to the Internet. There are two types of spoke devices: on-premises spoke and cloud spoke.

On-Premises Spoke Devices

On–premises spoke devices can be either NFX Series devices or specific SRX Series devices, as shown in Figure 8 on page 28.

Figure 8: On-Premises Spoke Devices

NFX Series Network Services Platform

The NFX Series Network Services Platform used as an on-premises spoke device differentiates from traditional CPE devices in that it can host a range of multivendor VNFs and support service chaining, managed by orchestration software in the cloud. NFX Series devices eliminate the operational complexities of deploying multiple physical network devices at a customer site.

A key VNF supported on the NFX Series platform is the vSRX Virtual Firewall. In the Contrail SD–WAN solution, the vSRX instance performs the gateway router function, given its routing and switching capabilities. It also provides the same feature-rich security services found on a standard SRX series devices. Table 5 on page 29 shows the supported NFX hardware and required Junos OS software release version for each supported model.

> **NOTE:** The NFX150 features a built–in SRX firewall in place of the vSRX functionality found on other NFX Series devices.

Table 5: NFX Hardware and Software Matrix for On-Premises Spoke Devices

Platform	Models Supported	Junos OS Software Release Versions
NFX150 Network Services Platform	• NFX150–S1 • NFX150–S1E • NFX150–C–S1 • NFX150–C–S1–AE/AA • NFX150–C–S1E–AE/AA	18.2X85–D12 19.3R2-S3 19.3R2-S4
NFX250 Network Services Platform	• NFX250–LS1 • NFX250–S1 • NFX250–S2	15.1X53–D497 18.4R3-S3

NOTE: When onboarding a new site, ensure your devices at the new site are running the latest specified release version from the above lists. The older release versions listed above are supported for existing devices at existing sites only.

SRX Series Devices and vSRX Virtual Firewalls

A physical SRX device can be used in place of the NFX platform to provide the gateway router function, as can a vSRX instance installed on a server. Table 6 on page 29 shows the supported SRX hardware, vSRX virtual firewalls, and required Junos OS software release versions.

Table 6: SRX Hardware and Software Matrix for On-Premises Spoke Devices

Platform	Models Supported	Junos OS Software Release Versions
SRX Series	• SRX4200 • SRX4100 • SRX550M • SRX345 • SRX340 • SRX320 • SRX300	15.1X49–D172 19.3R2-S3 19.3R2-S4
	SRX1500	19.3R2-S3 19.3R2-S4

Table 6: SRX Hardware and Software Matrix for On-Premises Spoke Devices *(continued)*

Platform	Models Supported	Junos OS Software Release Versions
vSRX Virtual Firewalls	vSRX (standalone)	15.1X49-D172 19.3R2-S3 19.3R2-S4
	vSRX (installed in NFX250)	15.1X49-D172 with NFX running 15.1X53-D497 19.3R2-S3 with NFX running 18.4R3-S3 19.3R2-S4 with NFX running 18.4R3-S3
	vSRX 3.0 (standalone)	19.3R2-S3 19.3R2-S4

NOTE: When onboarding a new site, ensure your devices at the new site are running the latest specified release version from the above lists. The older release versions listed above are supported for existing devices at existing sites only.

NOTE: For the most up to date information on hardware and software support for CSO, see the Contrail Service Orchestration Release Notes.

Cloud Spoke Devices

A Contrail SD–WAN cloud spoke device, in the form of a vSRX, can be located in an AWS VPC. The vSRX serves as a spoke device in the cloud; once the endpoint comes online, it acts like any other spoke device.

Spoke Redundancy

Two redundant CPE devices can be used at spoke sites to protect against device and link failures. For more detail, see the *Resiliency and High Availability* section of the CSO Design and Architecture Guide.

Provider Hub Devices

The Contrail SD–WAN solution supports two deployment topologies: dynamic mesh and hub-and-spoke. In a dynamic mesh deployment, each site has a CPE device that connects to the other sites and the

enterprise hub device. In a hub-and-spoke deployment, there is at least one provider hub device and one or more spoke devices.

The provider hub device terminates both MPLS/GRE and IPsec tunnels from spoke devices.

Provider Hubs

In a service provider (SP) environment, the service provider hosts a *provider hub* device in their network. The provider hub device acts as a point of presence (POP) or connection point. It is typically a shared device, providing hub functionality to multiple customers (tenants) through the use of virtual routing and forwarding instances (VRF). The SP administrator and the OpCo administrator can both manage the provider hub device.

In the cloud-hosted deployment of CSO, the SP administrator role is performed by Juniper Networks as the cspadmin user (or equivalent). The OpCo administrator role can be assigned to a user by the SP administrator, but the OpCo administrator does not have SP administrator privileges.

Figure 9 on page 31 and Table 7 on page 31 show the provider hub devices supported in a CSO SD-WAN environment.

Figure 9: SD-WAN Provider Hub Devices

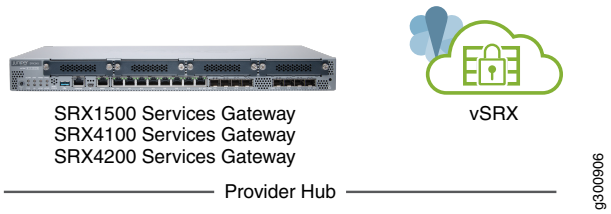


Table 7: Provider Hub Devices and Supported Software

Role	Supported Device Types	Required Junos OS Software Version
Provider Hub	• SRX4200 • SRX4100 • SRX1500	15.1X49–D172 19.3R2-S3 19.3R2-S4
	vSRX	15.1X49–D172 19.3R2-S3 19.3R2-S4
	vSRX 3.0	19.3R2-S3 19.3R2-S4

Table 7: Provider Hub Devices and Supported Software *(continued)*

Role	Supported Device Types	Required Junos OS Software Version
NOTE: When onboarding a new site, ensure your devices at the new site are running the latest specified release version from the above lists. The older release versions listed above are supported for existing devices at existing sites only.		

> **NOTE:** For the most up to date information on hardware and software support for CSO, see the Contrail Service Orchestration Release Notes.

Provider Hub Redundancy

Two redundant provider hub devices can be used at one POP to protect against device and link failures, and to provide upstream multi-homing for spoke sites. For more detail, see the Resiliency and High Availability section of the CSO SD-WAN and SD-LAN - Design and Architecture Guide.

Enterprise Hub Sites and Devices

A special type of spoke device, called an *enterprise hub device*, can be deployed as the CPE at an on-premises spoke site. SRX1500, SRX4100, and SRX4200 devices can serve this function. The spoke site that functions this way, must be configured as an *enterprise hub site* during site creation. Creating an enterprise hub site opens additional functionality for the site:

- Can act as the anchor point for site–to–site communications on the customer's network.
- Can act as the central breakout node for the customer's network.
- Offers a specialized department called the *data–center department*.
- Supports dynamic LAN segments with BGP and OSPF route imports, including default routes, from the LAN–side L3 device.
- Allows for intent-based breakout profiles to create granular breakout behavior based on department, application, site, and so on.

In an enterprise environment, the enterprise hub is owned by the customer (tenant) and usually resides within an enterprise data center. Only the customer's spoke sites can connect to the enterprise hub device. OpCo administrators and tenant administrators can manage the enterprise hub. Figure 10 on page 33 and Table 8 on page 33 show the enterprise hub devices supported in a CSO SD-WAN environment.

Figure 10: SD-WAN Enterprise Hub Devices

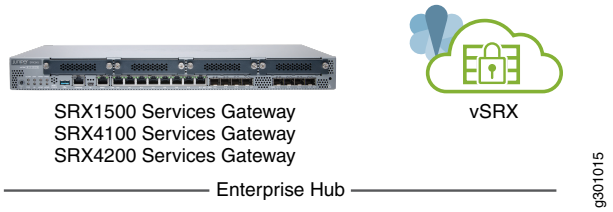


Table 8: Enterprise Hub Devices and Supported Software

Role	Supported Device Types	Required Junos OS Software Versions
Enterprise Hub	• SRX4200 • SRX4100	15.1X49–D172 19.3R2-S3 19.3R2-S4
	SRX1500	19.3R2-S3 19.3R2-S4
	vSRX	15.1X49–D172 19.3R2-S3 19.3R2-S4
	vSRX 3.0	19.3R2-S3 19.3R2-S4
NOTE: When onboarding a new site, ensure your devices at the new site are running the latest specified release version from the above lists. The older release versions listed above are supported for existing devices at existing sites only.		

NOTE: For the most up to date information on hardware and software support for CSO, see the Contrail Service Orchestration Release Notes.

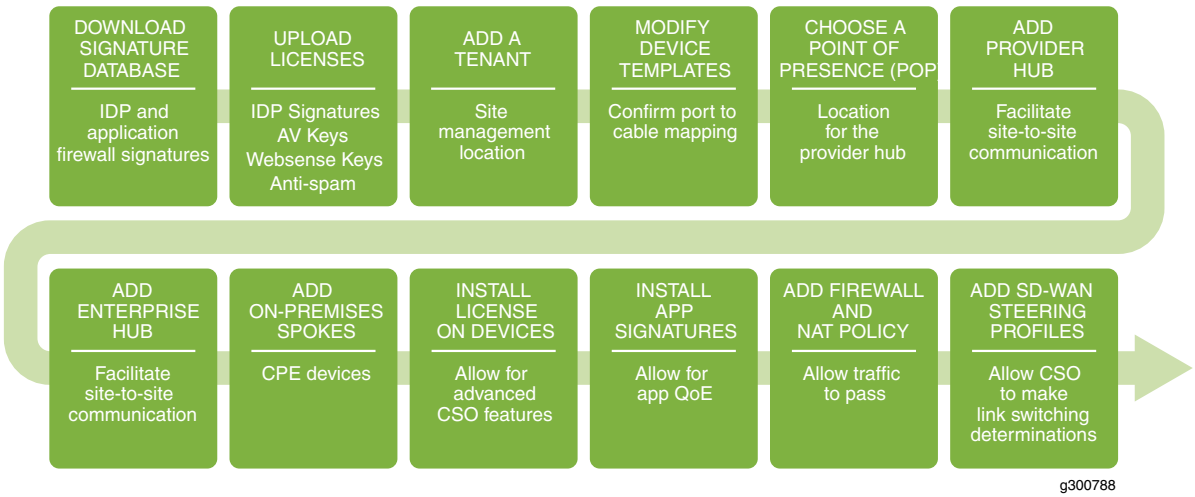
Initial SD-WAN Deployment

IN THIS SECTION

- Before You Begin | 35
- Download Intrusion Protection System (IPS) and Application Signatures | 35
- Upload Licenses | 38
- Add a New Tenant | 38
- Modify Device Templates | 40
- Choose a Point of Presence (POP) for the Hub | 44
- Add a Provider Hub Device to Your Tenant | 44
- Add an Enterprise Hub to Your Tenant | 48
- Add an On-Premises Spoke for the Tenant | 52
- Install a License on a Device | 58
- Install an Application Signature on a Device | 58
- Add Firewall and NAT Policies to the Topology | 59
- Add SD-WAN SLA-Based Steering Profiles and Policy | 61

This document describes the steps required to create a basic SD-WAN deployment. Figure 11 on page 35 shows an overview of the steps that will be covered in this deployment example.

Figure 11: Basic SD-WAN Deployment Workflow



Before You Begin

This example uses hardware-based SRX devices in the roles of provider and enterprise hub and on-premises spoke devices. The vSRX Series of devices could be used in place of either the hub or spoke devices. NFX series devices could also be used for the spoke devices.

CSO makes use of advanced features of the devices used in SD-WAN deployments. In order to use features such as link-switching based on application identification, or remote access IPsec VPNs on vSRX Series devices, you must purchase the required licenses. However, the underlay and overlay networks, and thus SD-WAN connectivity can be established without special licensing.

Download Intrusion Protection System (IPS) and Application Signatures

This section details how to download the IPS and application firewall signature databases from Juniper Networks onto your CSO installation. Downloading the signature databases makes the IPS and application firewall signatures available to install on your hub and CPE device after it has been activated.

From this point on in this deployment example, we assume that you are logged in to CSO as an OpCo administrator.

The user name part of your credentials is the e-mail address that was used when your CSO account was set up. When an account is initially setup, CSO sends an e-mail to that address with a link that includes a one-time activation code. Clicking the link takes you to the CSO login page which then prompts you to set a password. This is a one-time activity. Subsequent logins to the Administration Portal use the e-mail address and your newly-set password as your login credentials.

> **NOTE:** If you are working with an on-premises installation of CSO, you can login as the cspadmin user (or equivalent) to perform all of these steps.

1. Enter the login credentials for the Administration Portal.

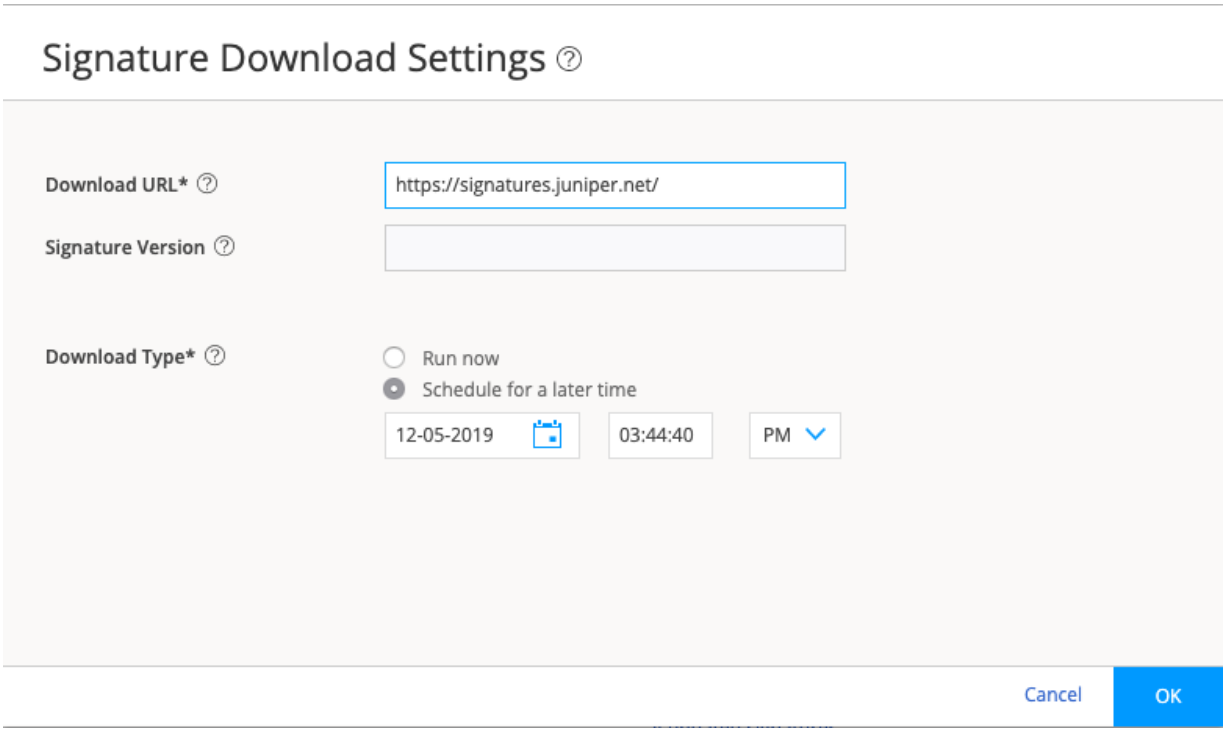
2. Navigate to the **Administration > Signature Database** page.

   On this page, there is a list of available database versions, their publish dates, update summaries, and detector versions. The active database (if there is one) is in its own section at the top of the list. There is a list of available signature databases is in the section below and it is sorted from newest (at the top) to oldest.

3. Click the **Signature Download Settings** button in the upper right corner of the window.

   The **Signature Download Settings** window appears as shown in Figure 12 on page 37.

Figure 12: Signature Download Settings



The **Download URL** field is pre-populated with Juniper's signature download URL. If you have previously downloaded the desired signature pack to another location (URL), enter that URL here.

4. If you are downloading the signature database from a location other than https://signatures.juniper.net, then you must enter the signature version that you want to download. If you are downloading from https://signatures.juniper.net, then you can leave this field empty.

5. Select whether to download the signatures now, or at a later time.

6. Click **OK**.

   A notification will appear at the top of the screen indicating whether the job has been scheduled or is running immediately.

Once the download completes successfully, the new database version number appears in the **Active Database** portion of the page. The new signature database is available to all of your tenants and their sites. To see the application signatures included in the database, navigate to **Configuration > Shared Objects > Application Signatures**.

Starting with CSO Release 5.0.2, you can define your own custom application signatures for use in SD-WAN policy. For more information regarding this optional step, see Contrail Service Orchestration Administration Portal User Guide.

Upload Licenses

The licenses that you upload to CSO using this procedure are available to be pushed to your tenant devices during the ZTP process or after they are provisioned. You need to install licenses on the hub and spoke SRX devices (physical and virtual) that you use in SD-WAN solutions. The licenses allow access to virtual network services such as application-based routing, application monitoring, and vSRX security features.

To upload the license for your devices:

1. Navigate to the **Administration > Licenses > Device Licenses** page.

   On this page is a list of all available device licenses. Since you have not installed any licenses yet, the list is empty.

2. Click the Add icon (**+**) button at the top-right part of the list to add a license.

   The **Add License** window appears.

3. Click the **Browse** button.

   This lets you locate the license file on your computer.

4. Select a tenant or *All Tenants* from the Tenant pull-down menu.

   This associates the license file with a particular tenant or all tenants. If the license is associated with a particular tenant, then the licenses can only be applied to devices that belong to that tenant.

5. (Optional) Enter a description of the license file if desired.

You can repeat this procedure to upload as many licenses as you have.

Add a New Tenant

In this section we use the Administration Portal to add a tenant to CSO. OpCo administrators in on-premises or cloud-hosted CSO installations and SP administrators in an on-premises CSO installation can add tenants.

1. Select **Tenants** from the left-navigation panel.

2. If there are no existing tenants, the **Add Tenant** button is displayed on the center of the page.
   Click the **Add Tenant** button, if it is available, to add a new tenant.
   If there are existing tenants, click the Add icon (**+**) at the upper right portion of the window to add a new tenant.

3. In the Add Tenant window that appears:
   - Enter a name for your tenant such as **Tenant1**.
   - Fill in the **Admin User** information.

     The e-mail address is used as the login name (username) for this user.
   - Select the checkbox next to the **Tenant AdminRole Name** in the **Available** list.
   - Click the **Right Arrow** button between the **Available** and **Selected** lists to move the **Tenant Admin** to the **Selected** list.
     If you want to see the access and permissions of the available roles, click the **Tenant Admin** or **Tenant Operator** names.
   - The password expiration default is 180 days.

     You can set any value between 1 and 365.
   - Click **Next**.

     The window advances to the **Deployment Info** tab.
   - In the **Deployment Info** window, select the **SD-WAN** card in the **Services** section.

     This activates the **SD-WAN Mode** section of the window.
   - The **Realtime Optimized** radio button is selected by default with the SD-WAN service.

     You cannot change this selection.
   - Click **Next**.

     The window advances to the **Tenant Properties** tab. For this example, browse the tenant properties but do not make any changes.
     See the CSO Administration Portal User Guide for more information about the settings on the **Tenant Properties** tab.
   - Click **Next**.

     The window advances to the **Summary** section. Review the summary.
   - Click **OK**.

     A pop-up message appears that tells you that the Add Tenant job was started. After some time, your new tenant appears in the list of tenants.

Modify Device Templates

In this section, we examine device templates that we use for this example.

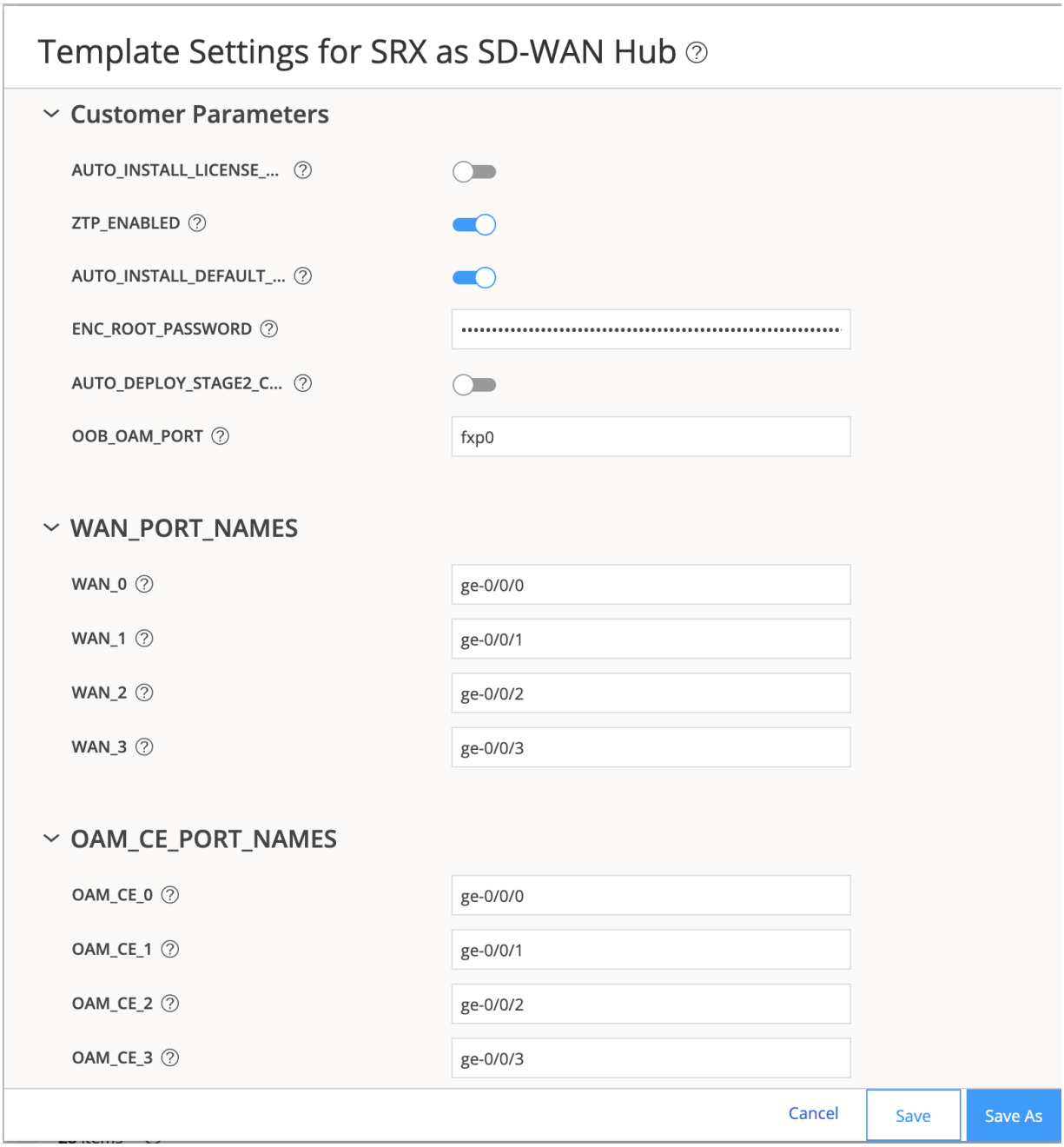
For the SRX in the Enterprise Hub Role

1. Navigate to **Resources > Device Templates**.
2. Find the device template named **SRX as SDWAN Hub**.
3. Select the checkbox next to that template.
4. Click the **Clone** button.
5. Enter a **Display Name** and a **Name** for the cloned template.

   CSO shows the **Display Name** in various workflow locations but uses the **Name** behind the scenes. For this example, we name the template SRX_as_SD-WAN_Hub.
6. Click **OK**.
7. Select the checkbox next to the cloned template and then select **Template Settings** from the **Edit Device Template** pull-down menu.

   A new window titled **Template Settings for *Display Name*** appears as shown in Figure 13 on page 41. You must scroll down to see these particular settings in the template.

Figure 13: Partial Template Settings for SRX as SD-WAN Hub



Note the device port names (**ge-0/0/0**, etc) for the WAN and OAM ports. If your hub device is not cabled to match, then adjust the port names in the template as needed.

8. Select **Save** when finished.

For the SRX in the CPE device role

9. Find the device template named **SRX as SD-WAN CPE** and select the checkbox next to its name.

10. Click the **Clone** button.

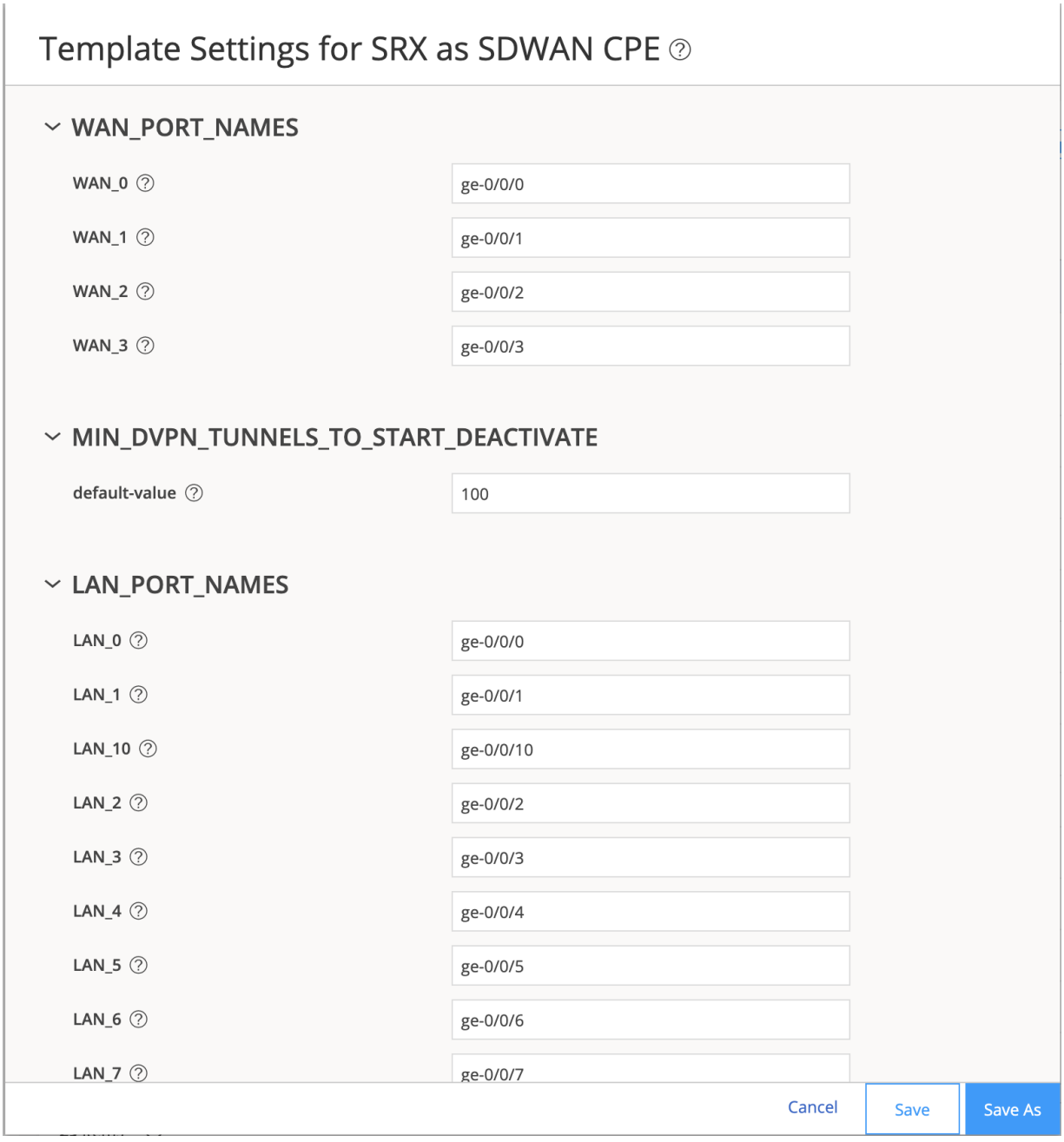
11. Enter a **Display Name** and a **Name** for the cloned template.

    The **Display Name** is whatCSO uses when selecting the template for use.

12. From the **Edit Device Template** pull-down menu, select **Template Settings**.

    The **Template Settings for <*Display Name*>** window appears as shown in Figure 14 on page 43. You must scroll down to see these particular settings in the template.

Figure 14: Partial Template Settings for SRX as SD-WAN CPE



Note the device port names (**ge-0/0/0**, etc) for the WAN and OAM ports. If your CPE device is not cabled to match, then adjust the port names in the template as needed.

13. Click Save when finished.

The templates will be used later when you deploy the enterprise hub and CPE spoke devices.

Choose a Point of Presence (POP) for the Hub

A POP is a location within the service provider's cloud in which PE routers and IPSec Concentrators are located. It is a regionally located access point through which customer sites gain access to provider hub devices that are placed within. The hubs are either DATA_ONLY, OAM_ONLY, or OAM_AND_DATA hubs. SPs often place POPs in their network so that they are geographically close to customer sites.

> **NOTE:** The SP administrator is the only administrator with the privileges to create POPs. In a cloud-hosted CSO deployment, tenants choose the appropriate POP from a list of available POPs created by the SP administrator. In an on-premises CSO deployment, you (as the cspadmin user) create the POP in which the hub device resides.

To choose or add a POP (for cloud-hosted CSO):

1. Navigate to the **Resources > POPs** page.

   Here you can see a list of POPs available to you.

2. Make note of the POP name(s) and location(s) so that you can choose the appropriate one when adding your devices.

To add a POP (for on-premises CSO):

1. Navigate to the **Resources > POPs** page as the SP administrator.

   Here you can see a list of existing POPs.

2. Click on the Add icon (**+**) to add a POP and fill in the information in the **Add POP** window that appears. Currently, all POPs are regional.
   Give the POP a name and, optionally, address information so that its location can be displayed on CSO monitoring maps.

Add a Provider Hub Device to Your Tenant

A provider hub device resides in a regional POP within the service provider network. Provider hub devices are shared amongst multiple tenants through the use of virtual routing and forwarding (VRF) instances configured on the provider hub itself. They allow site-to-site traffic to flow in hub-and-spoke deployments, serve as OAM gateway devices for management traffic between CSO and CPE devices, and serve as backup data hubs when an enterprise hub device is used in a tenant.

Provider hubs come in three varieties: OAM_ONLY, DATA_ONLY, or OAM_AND_DATA. As their names imply, they have different capabilities. At least one of the provider hubs in each tenant must have OAM capabilities. Adding multiple OAM-capable provider hubs helps to balance OAM traffic loads in large CSO deployments. In cloud-hosted versions of CSO, the OAM-capable hubs are clearly labeled.

> **BEST PRACTICE:** It is recommended that all provider hubs be clearly named for their data and OAM capabilities.

The following two procedures describe how to add provider hub devices to your CSO installation and tenant. The first procedure describes adding a provider hub device to an on-premises version of CSO. It can only be done by an SP administrator. In cloud-hosted CSO, the addition of the hub devices to the system is carried out by Juniper Networks.
The second procedure is carried out at the OpCo or tenant level in both on-premises and cloud-hosted CSO versions. It makes the provider hubs added in the first procedure available for use by tenants.

Add Provider Hubs for On-Premises CSO

1. Navigate to the **Resources > Provider Hub Devices** page as the SP administrator user (cspadmin or equivalent).

2. At the top-right part of the page, click the Add icon (**+**).

   A new window appears titled **Add Provider Hub Device**.

3. Fill in the **Site Information** section as follows:
   - **Name**: Name the provider hub something that makes sense, like **PH-OAM-DATA-1**.
   - **Management Region**: **Regional**

     There is currently no other option for this.
   - **Site Capability**: **DATA_AND_OAM**

     This allows both operation, administration, and maintenance (OAM) and user data to traverse this device. It ensures that CSO can manage CPE devices through this provider hub device.
   - **POP**: **Select the POP that you just created from the pull-down menu**.
   - **Authentication Type**: **Pre Shared Key**

     You can choose Public Key Infrastructure if you have the proper certificates set up.
     CSO supports single and multi-level PKI certificates.
   - (Optional) **Advanced Configuration**: Change the information in this section as appropriate for your network.
4. Click **Next**.

The window advances to the **WAN** tab.

5. In the **Device Template Section**, select **SRX** as the **Device Series** from the pull-down menu.

6. Select **SRX_as_SDWAN_Hub** from the carousel of available device templates (cards).

7. In the **Device Information** section, enter the device serial number.

8. Leave the **Auto Activate** button active (blue).

9. (Optional) If you want to upgrade the device image for your SRX Series device, select the new boot image from the list. The boot image is the device image that was previously uploaded to the image management system in CSO. The boot image is used to upgrade the device during the ZTP process. If the boot image is not provided, then the device skips the automatic upgrade procedure and uses the image that is present on the device.

10. In the **Management Connectivity** section fill in the form as follows:

    - Leave the **Loopback IP Prefix** blank.
      CSO automatically configures the proper loopback IP during the ZTP process, based on information contained in the device template and CSO databases.
    - OAM Interface: Enter the appropriate interface, such as **ge-0/0/0** as the **OAM Interface** of the provider hub.

      The interface selected must match the device template and your network cabling.
    - OAM VLAN: Leave this field blank.

      > **NOTE:** You can enter a VLAN ID if one is needed in your network. If you specify an OAM VLAN ID, then all in-band OAM traffic reaches the site through the selected OAM interface. The range is 1 through 4050.

    - OAM IP Prefix: Enter an IP address prefix, such as **10.100.100.11/32**.

      This is the IP address prefix for the OAM network. Secure OAM traffic is passed across this network in IPsec tunnels. The OAM IP Prefix must be unique across the entire management network.

      > **NOTE:** For SRX Series services gateways like we are using in this example, always use a **/32** prefix.

    - OAM Gateway: Enter an IP address, such as **10.100.100.1**.

This is the IP address of the next-hop on the management network through which CSO connectivity is established.

- EBGP Peer-AS: Leave this field blank.

  This is the external BGP peer autonomous system number. It is used to peer with a PE router in the SP network (if any).
  Enter a value here if needed in your network.

11. In the **WAN Links** section, fill in the information as follows:

    - Leave the **WAN_0 (ge-0/0/0)** slider button enabled.

      The physical device interface is already chosen from the value in the device template and cannot be altered here.

    - Link Type: Select **MPLS**.
    - Address Assignment: Enter **Static**.
    - Static IP Prefix: Enter an IP address prefix, such as **172.21.22.2/29**.

      This represents the provider hub address of the hub-to-CPE network connection.

    - Gateway IP Address: Enter an IP address, such as **172.21.22.1**.

      This is the IP address of the spoke (SRX or NFX CPE device) at the customer site.

    - Enable the **WAN_1 (ge-0/0/1)** slider button.

      The physical device interface is already chosen from the value in the device template and cannot be changed here.

    - Link Type: Select **Internet**.
    - Address Assignment: Enter **Static**.
    - Static IP Prefix: Enter an IP address prefix, such as **192.0.2.2/29**.

      This represents the provider hub address of the hub-to-CPE network connection.

    - Gateway IP Address: Enter an IP address, such as **192.0.2.1**.

      This is the IP address of the spoke (SRX or NFX CPE device) at the customer site.

    > **NOTE:** Enable the other WAN interfaces for your provider hub device as appropriate.

12. Click **OK** when you're finished.

    The **Activate Device** window pops up.
    The device shows up in the in the **Provisioned** state when this window shows the operation completed successfully.

You can dismiss this window by clicking **OK** before the operation is complete. To track the progress, navigate to **Monitor > Jobs** and click on the job name.

Add a Provider Hub to Your Tenant

1. Navigate to the **Resources > Provider Hub Devices** page.

   Here you can see a list of all cloud hub devices, their assigned POP, site associations, status, model, serial number, and OS version.

2. Make note of the names of the Provider Hub devices available to you.

3. Navigate to the **Resources > Site Management** page.

4. From the **Add** menu, select **Add Provider Hub**.

   The **Add Provider Hub for *Tenant Name*** window appears.

5. Select a **Service POP** from the pull-down menu.

6. Select a **Hub Device Name** from the pull-down menu.

   As mentioned previously, the you must add at least one provider hub with OAM capabilities.
   You can repeat this process to add as many provider hubs as you want from this POP to your tenant.

7. Click **OK**.

   The provider hub device is added to the list.

Add an Enterprise Hub to Your Tenant

Unlike a provider hub which is shared amongst multiple tenants, an enterprise hub acts as the primary hub device for spoke sites belonging to a single tenant. Tenants that have an enterprise hub installed can use it for site-to-site VPNs between spoke sites. In this case, the provider hub becomes a backup hub for the same VPNs. The site-to-site VPNs initially created through the enterprise hub can be dynamically switched to direct site-to-site VPNs based on the (user configurable) dynamic VPN threshold settings for the tenant.

An enterprise hub is added to a tenant by a tenant administrator using the Customer Portal in CSO. To add an enterprise hub to your new tenant:

1. Enter the Customer Portal for your tenant.

   SP and OpCo administrators access the Customer Portal by navigating to **Tenants** and clicking the tenant name from the list. This puts these administrators into the tenant administrator role for that tenant.
   Tenant administrators are automatically placed in their Customer Portal upon successful login.

2. Navigate to **Resources > Site Management**.

   The **Sites** page appears.

3. From the **Add** pull-down menu, select **Enterprise Hub**.

   The **Add Enterprise Hub for *Site Name*** window appears.

4. In the **Site Information** section, enter a name that makes sense for your site.

   Choose site names carefully because they cannot be changed after the site is added.

5. In the **Site Capabilities** section, select the **SD-WAN** card from the **WAN Capabilities** area.

6. In the configuration section, the **Primary Provider Hub** pull-down menu should already be populated with the name of the provider hub added earlier.

   The **On-demand VPN Threshold**, **Address and Contact Information**, and **Advanced Configuration** sections are all optional.

   > **NOTE:** Most settings made while creating sites cannot be changed once the site is provisioned. The exceptions are: **Address and Contact Information** and the NTP settings available in the **Advanced Configuration Settings** section.

7. Click **Next**.

   The page advances to the **WAN** tab.

8. Click the left arrow (**<**) or right arrow (**>**) until you see the **SRX as SD-WAN CPE** card. Click on that card.

9. In the **Device Information** section, enter the device serial number.

10. Leave the **Auto Activate** button active (blue).

11. (Optional) If you want to upgrade the device image for your SRX Series device, select the new boot image from the list. The boot image is the device image that was previously uploaded to the image management system in CSO. The boot image is used to upgrade the device during the ZTP process. If the boot image is not provided, then the device skips the automatic upgrade procedure and uses the image that is present on the device.

12. In the **Management Connectivity** section fill in the form as follows:

    - Leave the **Loopback IP Prefix** blank.
      CSO automatically configures the proper loopback IP during the ZTP process, based on information contained in the device template and CSO databases.
    - OAM Interface: Enter the appropriate interface, such as **ge-0/0/0** as the **OAM Interface** of the provider hub.

      The interface selected must match the device template and your network cabling.
    - OAM VLAN: Leave this field blank.

      > **NOTE:** You can enter a VLAN ID if one is needed in your network. If you specify an OAM VLAN ID, then all in-band OAM traffic reaches the site through the selected OAM interface. The range is 0 through 65535.

    - OAM IP Prefix: Enter an IP address prefix, such as **10.100.100.11/32**.

      This is the IP address prefix for the OAM network. Secure OAM traffic is passed across this network in IPsec tunnels. The OAM IP Prefix must be unique across the entire management network.

      > **NOTE:** For SRX Series services gateways like we are using in this example, always use a **/32** prefix.

    - OAM Gateway: Enter an IP address, such as **10.100.100.1**.

      This is the IP address of the next-hop on the management network through which CSO connectivity is established.
    - EBGP Peer-AS: Leave this field blank.

      This is the external BGP peer autonomous system number. It is used to peer with a PE router in the SP network (if any).
      Enter a value here if needed in your network.

13. In the **WAN Links** section, fill in the information as follows:

- Leave the **WAN_0 (ge-0/0/0)** slider button enabled.

  The physical device interface is already chosen from the value in the device template and cannot be changed here.

- Link Type: Select **MPLS**.
- Address Assignment: Enter **Static**.
- Static IP Prefix: Enter an IP address prefix.

  This represents the hub-side address of the hub-to-CPE network connection.

- Gateway IP Address: Enter an IP address.

  This is the IP address of the spoke (SRX or NFX CPE device) at the customer site.

- Enable the **WAN_1 (ge-0/0/1)** slider button.

  The physical device interface is already chosen from the value in the device template and cannot be changed here.

- Link Type: Select **Internet**.
- Address Assignment: Enter **Static**.
- Static IP Prefix: Enter an IP address prefix.

  This represents the hub-side address of the hub-to-CPE network connection.

- Gateway IP Address: Enter an IP address.

  This is the IP address of the spoke (SRX or NFX CPE device) at the customer site.

> **NOTE:** Enable the other WAN interfaces for your provider hub device as appropriate.

14. Expand the **Advanced Settings** section by clicking on the right arrow **>** icon.

15. Enable the **Use for Full Mesh** slider button (set to blue).

16. Select the **Internet** mesh tag from the **Mesh Tag** pull-down menu.

17. Ensure that the proper **Overlay Peer Interface** is selected.

    This is the interface on the provider hub that this enterprise hub will use as a BGP peer interface.

18. Click **Next**.

    The page advances to the **LAN** tab.

19. Click the **Add LAN Segment** button.

The **Add LAN Segment** window appears.

20. Enter a **Name** for the LAN segment.

21. Ensure that the **Department** pull-down menu has **Default** selected.

22. Enter a valid **Gateway Address/Mask**.

    This value is used as the gateway address for devices deployed on this LAN segment.

23. Select and move the appropriate port(s) from the **Available** list to the **Selected** list.

    Click the blue arrow to the right of a port name to move it from one list to the other.

24. Click **Save**.

    The new LAN segment is listed in the **LAN** tab of the **Add Enterprise Hub for *Site Name*** window.

25. Click **Next**.

    The page advances to the **Summary** tab.

26. Click **OK** when you're finished reviewing the summary tab information.

The **Activate Device** window pops up.
The device shows up in the in the **Provisioned** state when this window shows the operation completed successfully.

You can dismiss this window by clicking **OK** before the operation is complete. To track the progress, navigate to **Monitor > Jobs** and click on the job name.

Add an On-Premises Spoke for the Tenant

In this section, we continue in the Customer Portal for the newly configured tenant to create an on-premises spoke with an SRX CPE device.

This procedure begins in the **Tenants** window of the Administration Portal at the list of tenants.

1. Click on the name of the tenant that you created.

   This will take you to the Customer Portal for that tenant.

2. Navigate to the **Resources > Site Management** page.

3. In the **Site Management** window that appears, select **Add On-Premise Spoke Site (Manual)** from the **Add** pull-down menu.

   The **Add On-Premise Spoke Site for *Tenant*** page appears.

4. In the **Site Information** section, enter a name that makes sense for your site

   Choose site names carefully because they cannot be changed after the site is added.

5. In the **Site Capabilities** section, select the type of WAN and LAN capabilities you want for this site.

   The available site capabilities are based on the tenant capabilities defined during tenant creation. You can choose one WAN capability in addition to one optional LAN capability.

   For this example, choose only **SD-WAN**.

6. In the **Configuration** section, the **Provider Hub** and **Enterprise Hub** pull-down menus are already populated with the previously added hub devices.

   The **On-demand VPN Threshold**, **Address and Contact Information**, and **Advanced Configuration Settings** sections are all optional.

   > **NOTE:** Most settings made while creating sites cannot be changed once the site is provisioned. The exceptions are: **Address and Contact Information** and the NTP settings available in the **Advanced Configuration** section.

7. Click **Next**.

   The page advances to the **WAN** tab.

8. Next to **Device Series**, select **SRX** from the pull-down menu.

   A horizontal list of device template cards applicable to SRX Series devices is shown.

9. Click the left arrow (**<**) or right arrow (**>**) until you see the **SRX as SD-WAN CPE** card. Click on that card.

10. In the **Device Information** section, enter the device serial number.

11. Leave the **Auto Activate** button active (blue).

12. (Optional) If you want to upgrade the device image for your SRX Series device, select the new boot image from the list. The boot image is the device image that was previously uploaded to the image management system in CSO. The boot image is used to upgrade the device during the ZTP process. If

the boot image is not provided, then the device skips the automatic upgrade procedure and uses the image that is present on the device.

13. In the **WAN Links** section, fill in the information as follows:

    - Leave the **WAN_0 (ge-0/0/0)** slider button enabled.

      The physical device interface is already chosen from the value in the device template and cannot be changed here.

    - Link Type: Select **MPLS**.
    - Address Assignment: Enter **Static**.
    - Static IP Prefix: Enter an IP address prefix.

      This represents the hub-side address of the hub-to-CPE network connection.

    - Gateway IP Address: Enter an IP address.

      This is the IP address of the spoke (SRX or NFX CPE device) at the customer site.

    - Enable the **WAN_1 (ge-0/0/1)** slider button.

      The physical device interface is already chosen from the value in the device template and cannot be changed here.

    - Link Type: Select **MPLS**.
    - Address Assignment: Enter **Static**.
    - Static IP Prefix: Enter an IP address prefix.

      This represents the hub-side address of the hub-to-CPE network connection.

    - Gateway IP Address: Enter an IP address.

      This is the IP address of the spoke (SRX or NFX CPE device) at the customer site.

    > **NOTE:** Enable the other WAN interfaces for your provider hub device as appropriate.

14. Expand the **Advanced Settings** section by clicking on the right arrow **>** icon.

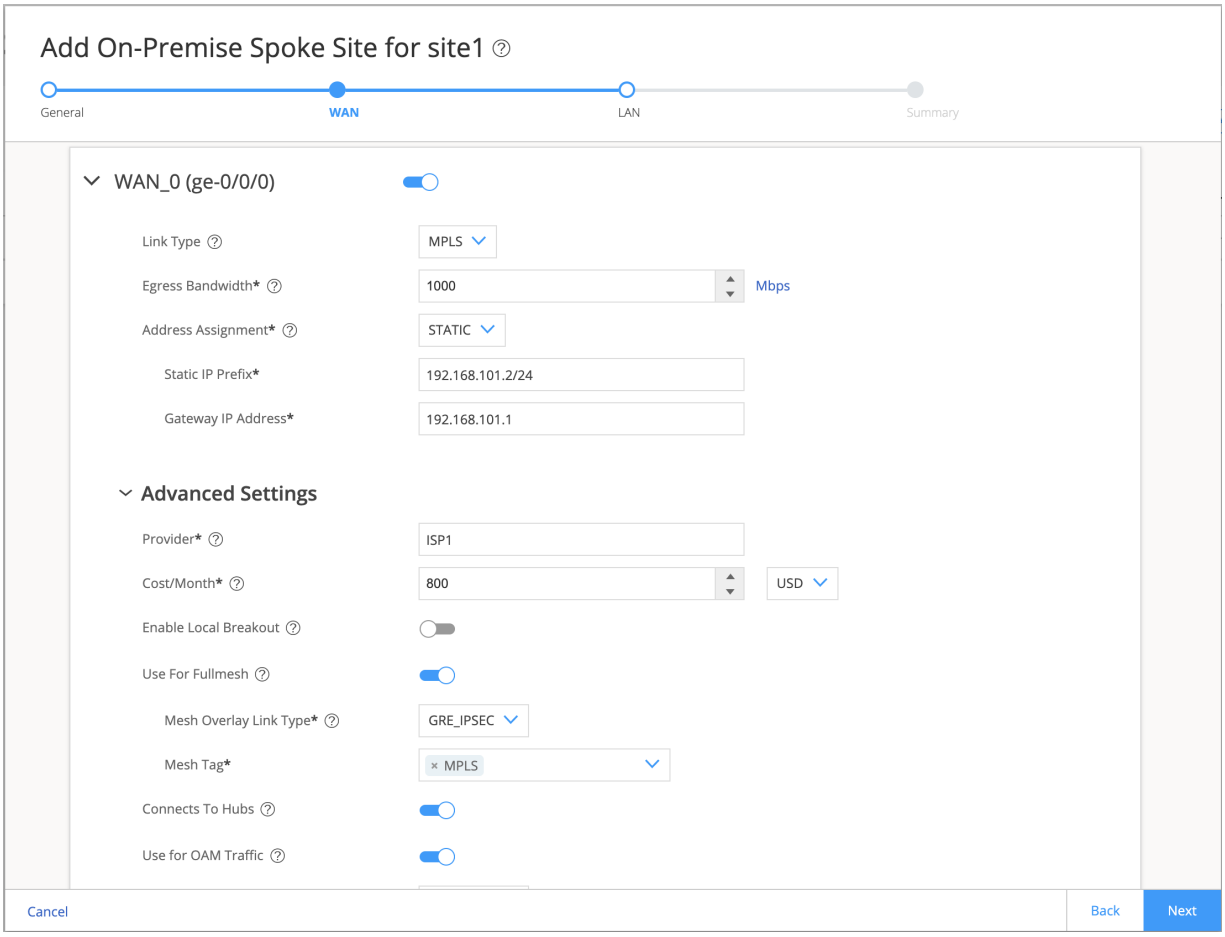
15. Enable the **Use for Full Mesh** slider button (set to blue).

16. Select the **MPLS** mesh tag from the **Mesh Tag** pull-down menu.

17. Enable the **Use for OAM Traffic** slider button (set to blue).

    Figure 15 on page 55 below shows an example of the settings described above.

Figure 15: WAN_0 Configuration Example



18. Select the **Enable** button next to **Wan_1**.

    The physical device interface is already chosen from the value in the device template and cannot be changed here.

    - Link Type: Select **Internet**.
    - Address Assignment: Enter **Static**.
    - Static IP Prefix: Enter an IP address prefix.

      This represents the hub-side address of the hub-to-CPE network connection.

      NOTE: Enable the other WAN interfaces for your provider hub device as appropriate.

19. Expand the **Advanced Settings** section by clicking on the right arrow **>** icon.

20. Enable the **Enable Local Breakout** button (set to blue).

Leave the **Breakout Options** pull-down menu set to **Use for breakout and WAN traffic**.

21. Enable the **Autocreate Source NAT Rule** button (set to blue).

    Leave the **Translation** pull-down menu set to **Interface**.

22. Enable the **Use for Full Mesh** slider button (set to blue).

23. Select the **Internet** mesh tag from the **Mesh Tag** pull-down menu.

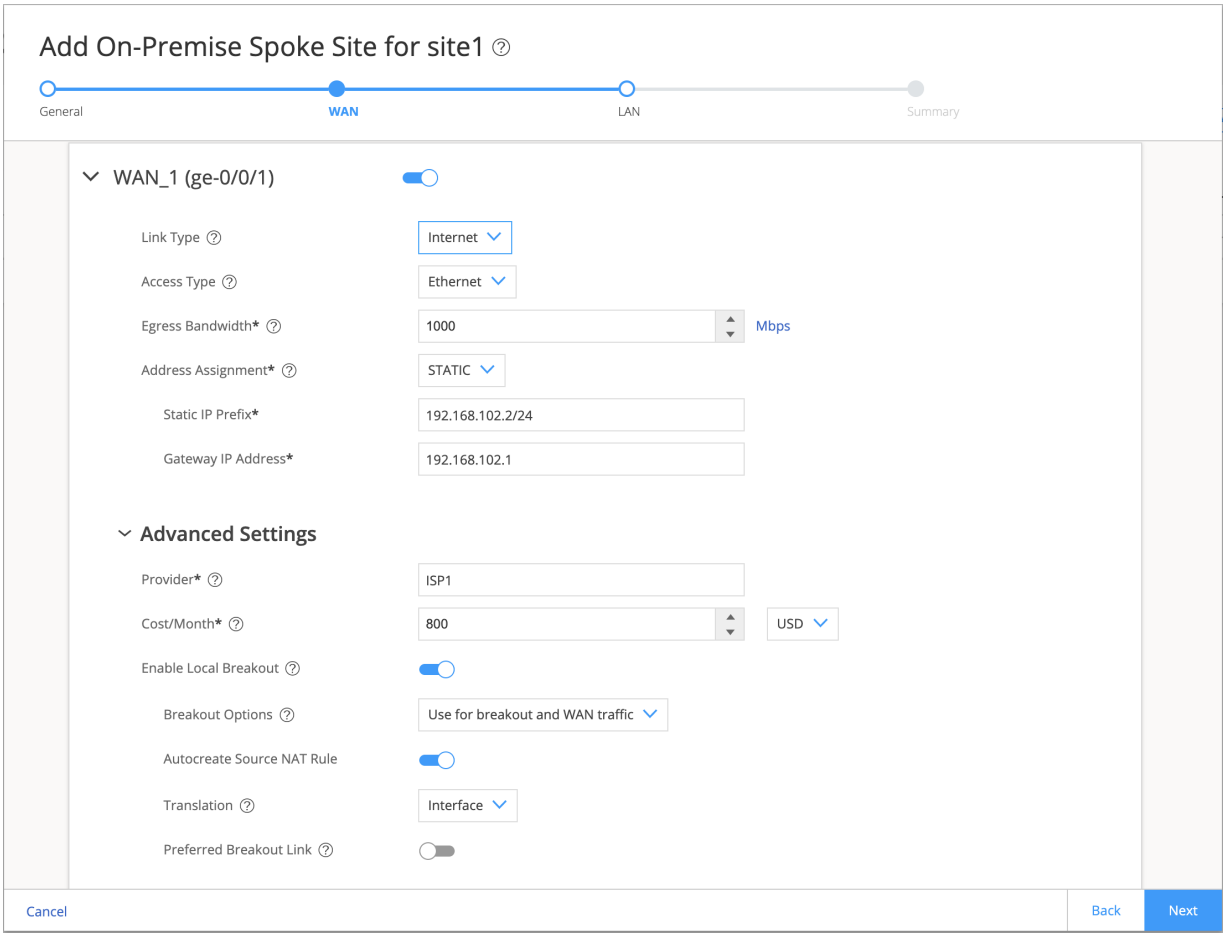
24. Enable the **Use For OAM Traffic** slider button (set to blue).

25. The **Overlay Peer Device** is automatically set to the provider hub device.

    Ensure that the **Overlay Peer Interface** pull-down menu is set to the proper interface.

    Figure 16 on page 56 below shows an example of the WAN_1 configuration as described above.

Figure 16: WAN_1 Configuration Example



26. Click **Next** when finished.

    The window advances to the **LAN** section.

27. Click the **Add LAN Segment** button.

    A new window appears titled **Add LAN Segment**.

    Fill in the following information in this window:

    - Name: **LAN2**

      > **NOTE:** This can be any name that makes sense in your deployment.

    - VLAN ID: Leave this field blank.

      > **NOTE:** Enter a VLAN ID if required at the remote site.

    - Department: Leave this field as **Default**.

      In CSO, spoke site departments equate to security zones on the CPE device. In this example, the Default security zone will be used later when we create security policies. Creating multiple departments for the spoke site creates multiple security zones with the same names on the CPE device.

      If you have departments set up already and the proper department is not shown, you can create one by clicking on the **Create Department** link.

    - Gateway Address/Mask: Enter an IP address and mask.

      Specify a unique and valid IPv4 address with subnet mask. This address is the default gateway for endpoints in this LAN segment.

    - DHCP: **Off**

      The An SRX Series device can provide DHCP server services for the remote LAN. For this example, leave DHCP set to off.

    - CPE Ports: Select **LAN_2 (ge-0/0/2)** by clicking the checkbox next to it.

    - Click the right arrow **>** icon to move **LAN_2 (ge-0/0/2)** from the available list to the selected list.

28. Click **Save** when finished.

    The **Add LAN Segment** window closes.

29. Click **Next**.

    The window advances to the **Summary** section.

30. Review the **Summary** section.

31. Click **OK** when you're finished reviewing this section.

    A device activation window pops up and displays the progress of your site deployment.

Install a License on a Device

To install a license on a device, use the Administration Portal.

1. Navigate to **Administration > Licenses > Device Licenses**.

   In the pop-up window that appears,

2. Click the checkbox next to the license file that you uploaded in Step 3.

3. Click the **Push License** button at the upper-right part of the list and select **Push**.

   The **Push License** window appears.

4. Select the name of the tenant that you created previously from the **Tenant** pull-down menu.

   Your sites and devices appear under **Sites and Devices**.

5. Select the checkbox next to your tenant site to push the license to the CPE device at that site.

Install an Application Signature on a Device

This step allows the CPE device to obtain the signature database needed for application identification.

To install an application signature:

1. Navigate to **Adminstration > Signature Database**.

   From the signature download you completed previously, you can now see the **Active Database** section has the number of the downloaded database listed.

2. Click the **Install on Device** link under the **Actions** column.

   In the new window that appears, you can elect to push the signatures to any device listed.

3. Select the checkbox next to the NFX250 device.

4. Click **OK**.

Add Firewall and NAT Policies to the Topology

In this section, we use the Customer Portal to add and deploy an intent-based firewall policy that allows the CPE-side LAN segments to pass traffic between each other and to the Internet. This requires adding two intents to the policy. One for department–to–department, and one for department–to–any address.

1. In the Customer Portal for your tenant, navigate to **Configuration > Firewall > Firewall Policy**.

   This brings up the **Firewall Policy** page with a list of existing policies.

2. Click the Add icon (**+**) to add a new policy.

   The **Add Firewall Policy** page appears.

3. Give the policy a name that makes sense, like FirstFirewallPolicy.

4. Click the checkbox to enable the policy for all sites.

   The new policy is added to the list.

5. Click on the policy name in the list to bring up the **Intents** for that policy.

   It shows that there are no **Enterprise Intenets** or **Zone-based Intents** for this policy.

   Allow Site-to-Site Traffic

6. Click the Add icon (**+**) to add a new intent.

   The window changes to reveal the intent editor page.

7. Click the Add icon (**+**) in the **Select Source** field.

   A list of possible sources appears.

8. Select **Default** from the **Departments [DEPT]** section of the list.

   Your choice is added to the source section.

9. Click the Add icon (**+**) labeled **Select Action**.

   A list containing available actions is shown. Select **Allow** from that list.

10. Your action choice is added between the source and destination sections.

11. Click the Add icon (**+**) in the **Destination** section.

    A list of possible destinations appears.

12. Select **Default** from the **Departments [DEPT]** section of the list.

    Your choice is added to the destination section.

13. (Optional) Enable the **Logging** slider switch (turns blue).

    We recommend that you log all deny or drop actions within firewall intents. Turning logging on for an accept action creates a lot of logs.

14. Click the **Save** button.

    The new intent is shown under the policy.

    Allow Outgoing Site Traffic

15. Click the Add icon (**+**) to add a second intent to the policy.

    The window changes to reveal the intent editor page.

16. Click the Add icon (**+**) in the **Select Source** field.

    A list of possible sources appears.

17. Select **Default** from the **Departments [DEPT]** section of the list.

    Your choice is added to the source section.

18. Click the Add icon (**+**) labeled **Select Action**.

    A list containing available actions is shown. Select **Allow** from that list.

19. Your action choice is added between the source and destination sections.

20. Click the Add icon (**+**) in the **Destination** section.

    A list of possible destinations appears.

21. Select **Any** from the **Addresses [ADDR]** section of the list.

    Your choice is added to the destination section.

22. (Optional) Enable the **Logging** slider switch (turns blue).

It is recommended to log all deny or drop actions within firewall intents. Turning logging on for an accept action creates a lot of logs.

23. Click the **Save** button.

24. Click the **Deploy** button.

    This brings up a **Deploy** window. Here you can select to run the policy deployment now or schedule it to run later.

25. Click **Deploy**.

    Deployment progress bars appear as CSO deploys the policy.

Add SD-WAN SLA-Based Steering Profiles and Policy

In this section, we use the Customer Portal to select a path-based steering profile and apply it to the SD-WAN Policy to specify that You Tube traffic should pass over the WAN_1 overlay link rather than the default link, WAN_0.

1. Navigate to **Configuration > SD-WAN > Path-Based Steering Profiles**.

2. Click the Add icon (**+**) to create a new profile.

   This brings up a **Add PathProfile** window.

   In the new window, fill in the following information.

   - Name: Enter a name for the profile, such as **Internet-Path**.
   - Traffic Type Profile: Select **INTERNET**.
   - Path Preference: Enter **Internet**.

     Priority value 1 is the highest priority. Higher priority profiles (lower numbers) take precedence over lower priority ones during SD-WAN events.

3. Click **OK**.

   The window closes and the new policy appears in the list.

4. Navigate to **Configuration > SD-WAN > SD-WAN Policy**.

   This brings up the SD-WAN policy page which includes a list of all SD-WAN policies.

5. Click the Add icon (**+**) at the upper right part of the list to create a new policy.

The policy builder screen appears with the **Source** section activated.

The default value for Source is **All Sites**.

The default value for Application is **Any**.

Use the default values for these fields.

6. Click the **+ Select Destination** field.

7. Type **YouTube** at the text-insertion point.

   This brings up a list of available applications.

8. Select **YouTube** from the list.

9. Click **+ Select Profile**.

   This brings up a list of available profiles.

10. Select **Internet-Path** from the **Path-Based Profiles [SLA]** section of the list.

11. Click **Save**.

    This closes the builder window and shows the list of SD-WAN Policies.

12. Click the **Deploy** button.

    This brings up a **Deploy** window. Here you can select to run the policy deployment now or schedule it to run later.

13. Click **Deploy**.

    Deployment progress bars appear as CSO deploys the policy. When it finishes, the **Total Intents** count increases from 0 to 1.

4

CHAPTER

SD-LAN Deployment

SD-LAN Deployment | 64

SD-LAN Deployment

IN THIS SECTION

- SD-LAN Deployment Overview | 64
- SD-LAN Deployment | 69

SD-LAN Deployment Overview

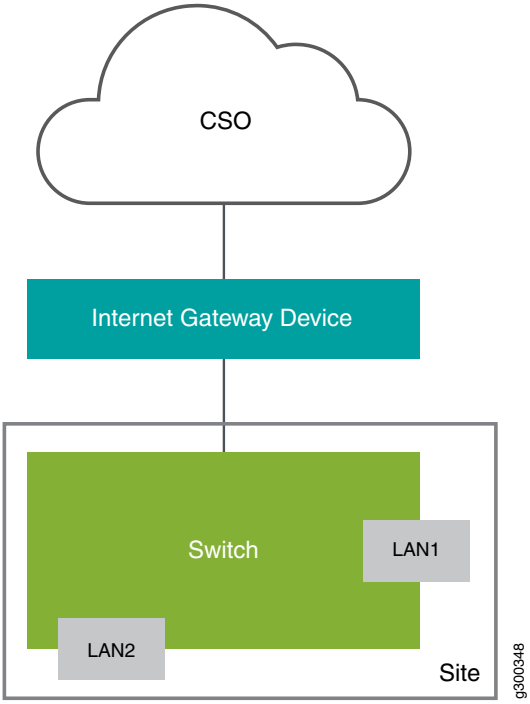
The SD-LAN deployment focuses on branch site LAN connectivity using specific EX Series switches, Virtual Chassis, and Mist wireless LAN access points. Once deployed, you can manage the connected branch site LANs through the EX switch. You can also manage many aspects of the EX switch or Virtual Chassis itself.

> **NOTE:** For more information on SD-LAN, see *Contrail SD-LAN: Manage Branch and Campus Switching* available from the Contrail Service Orchestration Documentation page.

There are several options for deploying an SD-LAN solution:

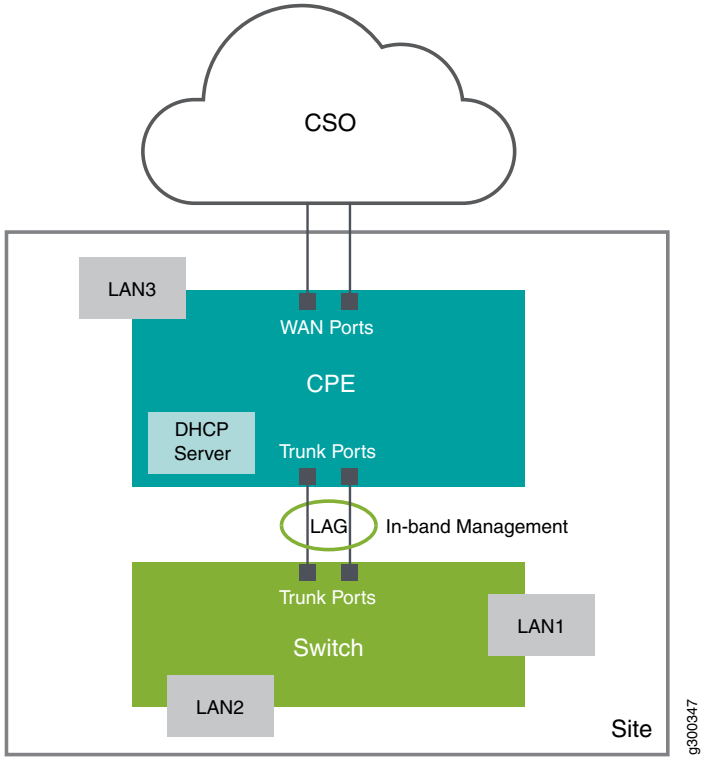
- Behind an Internet Gateway device as a standalone LAN switch in a new SD-LAN deployment, as shown in Figure 17 on page 65.

Figure 17: SD-LAN Behind an Internet Gateway Device



- As a switch, Virtual Chassis, or set of multiple switches located behind a CSO-managed on-premises spoke device—You can implement this style of SD-LAN as part of a new SD-WAN deployment or an extension of an existing SD-WAN deployment, as shown in Figure 18 on page 66.

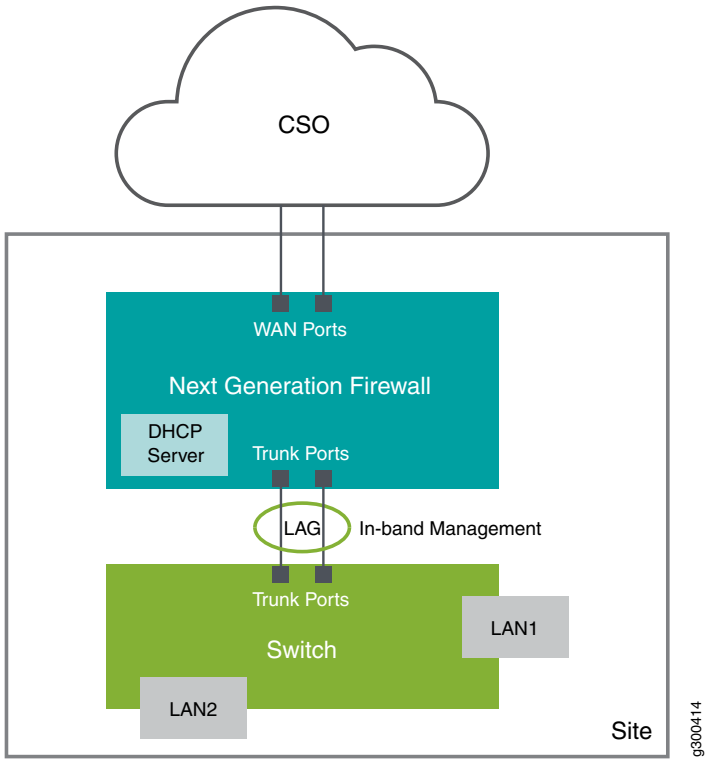
Figure 18: SD-LAN Behind a CPE Device



NOTE: You cannot deploy an EX Series LAN switch behind an NFX150 Series CPE device.

- As a switch, Virtual Chassis, or set of multiple switches located behind a CSO-managed NGFW device—You can implement this style of SD-LAN as part of a new NGFW deployment or as an extension of an existing NGFW deployment, as shown in Figure 19 on page 67.

Figure 19: SD-LAN Behind NGFW



It is important to note the Internet Gateway Device and the CPE device shown in Figure 17 on page 65 and Figure 18 on page 66. The LAN switch deployed at a branch site must be deployed behind an Internet gateway device that is capable of routing traffic to CSO.

An SD-LAN deployment is carried out in the Customer Portal of CSO as a site deployment. The tenant under which the site is deployed must have the LAN service available. This service is included in the tenant configuration by the tenant administrator during tenant onboarding. The remainder of this document provides the steps that you need to perform in order to complete an SD-LAN deployment in CSO.

Table 9 on page 68 shows the switching and WiFi platforms currently supported for SD-LAN.

Table 9: Hardware and Software Matrix for Devices in an SD-LAN Deployment

Role	Platform	Models Supported	Software Release Versions
SD-LAN Devices	EX Series Switches	• EX2300 • EX3400 • EX4300 • EX4600 • EX4650	Junos OS 18.4R2 Junos OS 18.4R3-S3
	Mist Access Points	• AP41 • AP43 • AP61	Mist AP Firmware 0.3.x and later

NOTE: For the most up to date information on hardware and software support for CSO, see the Contrail Service Orchestration Release Notes.

For those tenants with LAN service capabilities, you can add an SD-LAN site using EX Series Virtual Chassis. CSO supports EX2300, EX3400, EX4300, EX4600, and EX4650 switches.The number of members supported in a Virtual Chassis are shown in Table 10 on page 68.

Table 10: EX Series Virtual Chassis Member Count by Switch

Switch Model	Maximum Virtual Chassis Member Count
EX2300	4
EX3400	10
EX4300	10
EX4600	10
EX4650	2

The Virtual Chassis must be fully formed prior to provisioning in CSO. CSO only requires the primary member's serial number. Other member devices are automatically discovered during provisioning.

SD-LAN Deployment

The procedure you follow to complete this task varies slightly depending on whether you are in the role of a CSO tenant administrator or OpCo administrator. A note is used where needed to account for these variances.

This procedure makes the following assumptions:

- You have already established your login credentials for CSO.
- The tenant for which you are creating the LAN site is called **ExampleCo**, and has already been created.
- The **ExampleCo** tenant was added with LAN service capabilities.

If any of these things are not true, see *Accessing Administration Portal*, *Accessing Customer Portal*, or *Adding a Single Tenant* as needed.

This example demonstrates deploying a standalone SD-LAN behind an Internet gateway device.

The steps to deploy an SD-LAN site are as follows:

1. Log in to CSO using your login credentials.

   > **NOTE:** If you are an OpCo administrator, navigate to **Tenants** in the left-nav bar and select **ExampleCo** from the list of tenants on the tenants page. If you are the tenant administrator, you will be placed in the Customer Portal for **ExampleCo** upon successful login.

2. In the Customer Portal for **ExampleCo**, Navigate to **Resources > Site Management**.

   The **Sites** page appears.

3. Click the **Add** button and select **Add On-Premise Spoke (Manual)** from the list of options.

   The **Add On-Premise Spoke Site for ExampleCo** page appears.

4. In the **Site Information** section, give the site a name such as **LAN-Site1**.

5. In the **Site Capabilities** section, click the **LAN** icon.

   Depending on the configuration of the **ExampleCo** tenant, there may be other icons available. Only select **LAN** for this example.

6. Click the right arrow icon **>** next to **Address and Contact Information** to expand this section.

   None of the fields are required, but adding address information for the site allows CSO to place an icon for the site on maps on the monitoring page and show how it is linked to CSO.

7. Click the right arrow icon **>** next to **Advanced Configuration**.

   The two required fields, **Name Server IP List** and **NTP Server** are both pre-populated for you. Make changes as needed for your network to any of the fields.

8. Click **Next**.

   The wizard skips past the **WAN** page to the **LAN** page.

9. In the **Device Profile** section, fill in the **Device Name**.

10. Select the appropriate **Device Type** from the pull-down menu.

11. (Optional) Select the appropriate **Device Model** from the pull-down menu.

12. In the **Switch Details** section, enable the **Virtual Chassis** slider button if you are deploying a Virtual Chassis at the remote site. Otherwise, leave the slider off.

    Enter the **Serial Number** of the switch or the primary member of the Virtual Chassis in the field.

13. The **Auto Activate** button is turned on by default. Turn it off if you want to disable auto-activation and use an activation code instead.

    If you left **Auto Activate** turned on, skip to step 16.

14. (Optional) If you turned off **Auto Activate**, enter an activation code in the field that appears.

    The code can be any combination of letters and numbers.

    Remember this code.

15. The **Zero Touch Provisioning** (ZTP) button is turned on by default. Turn it off if the switch is not upgraded to a Junos OS image version with support for a Phone-Home Client. If ZTP is disabled, you must manually copy (by using CLI), the Stage-1 configuration on to the switch.

    ZTP, if left on, begins immediately after the activation procedure.

16. (Optional) Enter LAN information for the branch site.

    This optional step allows you to define where the remote site LANs are connected to the EX switch. You can define as many LANs as needed by following the next 5 steps.

    a. Click the Add icon (**+**).

       The **Add LAN Segment** window appears.

    b. Enter a name for the LAN segment, such as **LAN1**, in the field provided.

c. (Optional) Enter a **VLAN ID** for the LAN segment.

   If no VLAN ID is needed, you can safely remove the pre-populated value from the field.

d. Click **Save** when finished.

   You can add as many LAN segments as you need by repeating this procedure.

17. Click **Next**.

    The wizard advances to the **Summary** page.

18. Review the configuration on the **Summary** page.

19. Click **OK** when satisfied, or click **Back** as needed to make any changes

    If you need to edit anything, you can click the **Edit** links within the summary to go directly to that page of the wizard.

    If you left auto-activate turned on, the activation procedure begins at this point. The **Site Activation** page appears. Skip to Step 20.

    (Optional) If you turned off auto-activate, your site appears in the list with a status of **Configured** and you are now ready to activate the site:

    a. Click the *site name* link.

       This takes you to the site page for this site with the **Overview** tab highlighted.

    b. Click the **Devices** tab.

    c. Click the **Check-box** next to the device name.

       The **Stage1 Config** button becomes active.

    d. Click the **Stage1 Config** button.

       A new window appears containing the stage 1 configuration for this device.

    e. Click the **Copy to Clipboard** button.

    f. Click **OK**.

       The window closes.

    g. Using a console or SSH connection, install the copied configuration on the EX switch and commit it.

Assuming that the required network connectivity is in place from the EX switch, the switch connects back to CSO using an outbound SSH connection. When this connection is completed, the device will be activated in CSO; its status changes from **Expected** to **Provisioned**.

20. The **Site Activation** window proceeds through **Prestage Device** to **Detect Device** to **Bootstrap Device** and, finally to **Provision Device**.

Each stage will report success as it completes its operation. The window can be closed at any point. While the activation process is running, the **Site Status** column in the site list reports **Activating** and provides a link to **View** the activation wizard's progress. The **Site Status** changes to **Provisioned** once all the steps are successfully completed.

> **NOTE:** In the event of an error or delay, you can open a read-only SSH session to the device from CSO. This will allow you to troubleshoot connection or other issues.

Once deployed, you can monitor and manage the switch through the Customer Portal's Switch Port Operational View.

5

CHAPTER

Standalone Next-Generation Firewall (NGFW) Deployment

Next-Generation Firewall (NGFW) Deployment

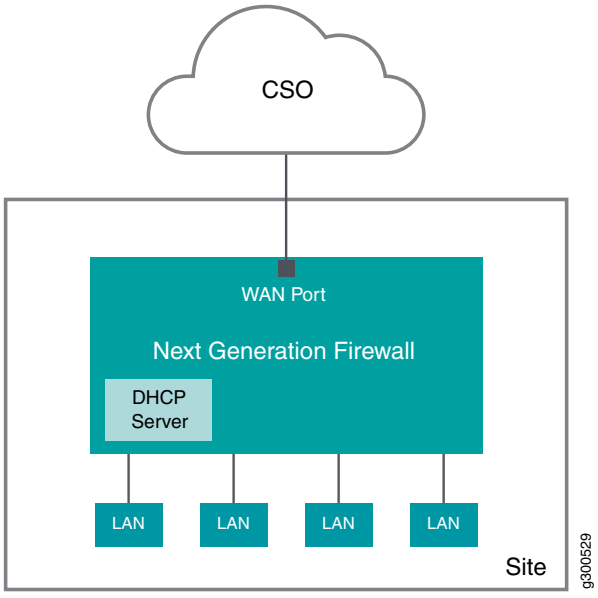
IN THIS SECTION

- NGFW Deployment Overview | 74
- NGFW Deployment Architecture | 75
- NGFW Deployment | 76

NGFW Deployment Overview

The NGFW deployment focuses on providing remote network security through the use of SRX Series NGFW devices as CPE at the spoke site; unlike the SD-WAN WAN deployment that focuses on secure site-to-site connectivity and remote VNF deployment. A high-level view of the spoke site with NGFW is shown in Figure 4 on page 17.

Figure 20: NGFW Spoke Site



An NGFW deployment is carried out in the Customer Portal of CSO as a site deployment. The tenant under which the site is deployed must have the NGFW service available. This service is included in the tenant configuration by the tenant administrator during tenant onboarding. The remainder of this document

provides a brief discussion of the architecture, and the steps that you need to perform in order to complete a NGFW deployment in CSO.

NGFW Deployment Architecture

The architecture used in this example is described below.

The architecture for a cloud-hosted, CSO-managed NGFW deployment is very similar to any standalone firewall deployment as shown in Figure 4 on page 17. There is only one WAN port needed for communication with CSO. This port must get its IP address and gateway information from an available DHCP server. The gateway must provide a path to the Internet so that the NGFW can communicate with Juniper's redirect server.

CSO provisions the device and adds logging functionality. Optionally, default FW and NAT policies can be added during the initial provisioning process. After provisioning the site administrator can push additional GE, NAT, UTM, or IPS policies to the device.

Device monitoring is supported via the CSO GUI where you can view application and security logging data.

The remaining ports on the NGFW can be used for LAN communication at the site. Additionally, an EX Series access switch can be added after the NGFW deployment. This addition allows for further LAN management within the site, including the ability to add CSO-managed Mist WiFi access points to the site.

Table 11 on page 75 shows the security devices supported in an NGFW deployment.

Table 11: Hardware and Software Matrix for Devices in an NGFW Deployment

Role	Platform	Models Supported	Junos OS Software Release Versions
NGFW Devices	SRX Series Security Gateways	• SRX300 • SRX320 • SRX340 • SRX345 • SRX550M • SRX1500 • SRX4100 • SRX4200	18.4R1 19.3R2-S3

NOTE: For the most up to date information on hardware and software support for CSO, see the Contrail Service Orchestration Release Notes.

NGFW Deployment

The procedure you follow to complete this task varies slightly depending on whether you are in the role of a CSO tenant administrator or OpCo administrator. A note is used where needed to account for these variances.

This procedure makes the following assumptions:

- You have already established your login credentials for CSO.
- The tenant for which you are creating the NGFW site is called **Example_Company**, and has already been created.
- The **Example_Company** tenant was added with NGFW WAN services capabilities.
- There is a working DHCP server available from which the WAN port of the NGFW device will obtain:
  - IP address
  - Address of a gateway router that can route traffic to the Internet

If any of these things are not true, see *Accessing Administration Portal*, *Accessing Customer Portal*, or *Adding a Single Tenant* as needed.

The steps to deploy an NGFW site are as follows:

1. Login to CSO using your login credentials.

   NOTE: If you are an OpCo administrator, navigate to **Tenants** in the left-navigation panel and select **Example_Company** from the list of tenants on the tenants page. If you are the tenant administrator, you will be placed in the Customer Portal for **Example_Company**.

2. In the Customer Portal for **Example_Company**, Navigate to **Resources > Site Management**.

   The **Sites** page appears.

3. Click the **Add** button and select **Add On-Premise Spoke (Manual)** from the list of options.

   The **Add On-Premise Spoke Site for Example_Company** page appears.

4. In the **Site Information** section, give the site a name such as **NGFW-Site1**.

5. In the **Site Capabilities** section, click the **Next Gen Firewall** icon.

   Depending on the configuration of the **Example_Company** tenant, there may be other icons available. Only select **Next Gen Firewall** for this example.

6. Click the right arrow icon > next to **Address and Contact Information** to expand this section.

   None of the fields are required, but adding address information for the site allows CSO to place an icon in the correct location for the site on maps on the monitoring page and show how it is linked to CSO. Without an address, CSO will place an icon at a default site.

7. Click the right arrow icon > next to **Advanced Configuration**.

   The two required fields, **Name Server IP List** and **NTP Server** are both pre-populated for you. Make changes as needed for your network to any of the fields.

8. Click **Next**.

   The wizard advances to the **WAN** page.

9. In the **Device Information** section, fill in the serial number of the SRX device you are onboarding.

10. The **Auto Activate** button is turned on by default. Turn it off if you want to disable auto-activation and use an activation code instead.

    Auto-activation, if left on, begins immediately after this add spoke site procedure is completed.

11. The **Zero Touch Provisioning** (ZTP) button is turned on by default. Turn it off if you want to pre-stage the device.

    ZTP, if left on, begins immediately after the activation procedure, if enabled.

12. Select the appropriate **In-Band Management** port from the pull-down list.

    NOTE: In-Band Management refers to management traffic that uses a connection that also carries non-management traffic. In this case, the in-band management port is the WAN port over which the device communicates with both CSO and the Internet.

13. Select a firewall policy from the pull-down list.

    CSO has a built-in firewall policy called **Default_Fw_Policy** that is provided for you. This policy is a zone-based policy intent that allows all traffic from any address in the trust zone to reach any address in the untrust zone.

14. Select a NAT policy from the pull-down list.

    CSO has a built-in NAT policy called **Default_NAT_Policy** that is provided for you. This policy is a Source-NAT policy that translates the source IP address of any traffic originating in the trust zone to the IP address of the trust-zone interface.

15. Click **Next**.

    The wizard advances to the **Summary** page.

16. Review the configuration on the **Summary** page as shown in Figure 21 on page 78.

Figure 21: NGFW Add Site Summary

The summary lists in text everything could be set in the wizard's GUI.

> **NOTE:** At the bottom of the summary page a **Save JSON** link is shown that allows you to download a JSON file of this site configuration. This JSON configuration can be modified for other sites so that they can be quickly imported without using the wizard workflow.

17. Click **OK** when satisfied, or click **Back** as needed to make any changes.

    If you need to edit anything, you can click the **Edit** links within the summary to go directly to that page of the wizard.

    The **Site Activation** wizard appears when you click **OK**.

18. If you left auto-activate turned on, the activation procedure begins at this point with the **Site Activation** page appearing.

If you turned off ZTP, you must copy the set commands from the **Pre-Stage Device** section of the **Site Activation** wizard. If you left ZTP on, it will begin as part of the site activation wizard.

19. The **Site Activation** window proceeds through **Prestage Device** to **Detect Device** to **Bootstrap Device** and, finally to **Provision Device**.

Each stage will report success as it completes its operation. The window can be closed at any point. While the activation process is running, the **Site Status** column in the site list reports **Activating** and provides a link to **View** the activation wizard's progress. The **Site Status** changes to **Provisioned** once all the steps are successfully completed.

CHAPTER 6

Appendix A - Network Function Virtualization in Contrail Service Orchestration

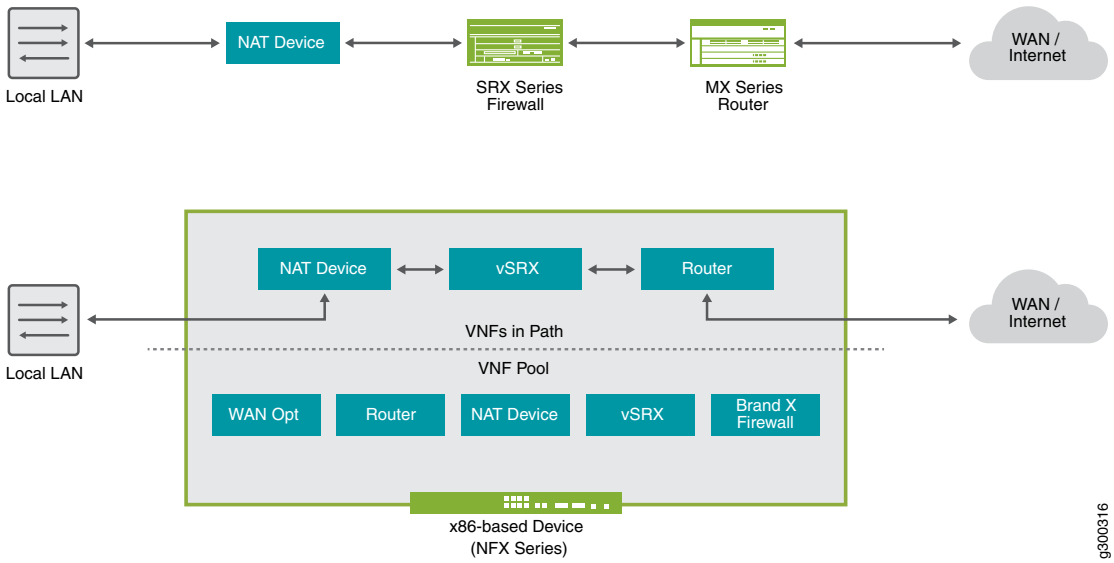
Network Function Virtualization in the Contrail Service Orchestration Deployments | **81**

VNFs Supported by the Contrail Service Orchestration Solutions | **83**

Network Function Virtualization in the Contrail Service Orchestration Deployments

Network Function Virtualization (NFV) is a concept in which network functions traditionally performed by dedicated hardware devices are performed by software that runs on virtual machines in various network locations. The virtual machines run software that performs traditional functions like routing, firewall, or network address translation (NAT). These functions are known as virtual network functions (VNFs). In Figure 22 on page 81, the upper part of the diagram shows conventional physical network devices chained together to provide network services. The lower part of the diagram shows how the same service chain can be created from a pool of VNFs available on an NFX Series device.

Figure 22: Network Function Virtualization



Juniper's CSO solutions comply with European Telecommunications Standards Institute (ETSI) standards for lifecycle management of network service instances.

The Contrail SD-WAN Solution uses the following components for the Network Functions Virtualization (NFV) environment:

- For SD-WAN deployments:
  - The Network Service Orchestrator, together with the Network Service Controller, provides ETSI-compliant management of the life cycle of network service instances.
  - The Network Service Controller provides service-chaining and the VIM.

- The CPE device provides the NFV infrastructure (NFVI).

Other CSO components connect to the Network Service Orchestrator through its REST API:

- Administration Portal, which you use to set up and manage your virtual network and customers through a graphical user interface (GUI).

  Administration Portal offers role-based access control for administrators and operators. Administrators can make changes; however, operators can only view the portal.

- Customer Portal, a GUI that your customers use to manage sites, CPE devices, and network services for their organizations.

  Customer Portal offers role-based access control for administrators and operators. Administrators can make changes; however, operators can only view the portal.

- Designer Tools:
  - Configuration Designer, which you use to create configuration templates for virtualized network functions (VNFs). When you publish a configuration template, it is available for use in Resource Designer.
  - Resource Designer, which you use to create VNF packages. A VNF package consists of a configuration template and specifications for resources. You use configuration templates that you create with Configuration Designer to design VNF packages. When you publish a VNF package, it is available for use in Network Service Designer.
  - Network Service Designer, which you use to create a network service package. The package offers a specified performance and provides one or more specific network functions, such as a firewall or NAT, through one or more specific VNFs.

> **NOTE:** In CSO Release 5.1.1 and later, the functionality of these *Designer Tools* (used for on-premises CSO deployments) is available in *Configuration Templates* (used for cloud-delivered CSO deployments).

CSO solutions extend the NFV model through the support of physical network elements (PNEs). A PNE is a networking device in the deployment that you can configure through CSO, but not use in a service chain. Configuration of the PNE through CSO as opposed to other software, such as Contrail or Junos OS, simplifies provisioning of the physical device through automation. Combining provisioning and configuration for PNEs and VNFs provides end-to-end automation in network configuration workflows. An example of a PNE is a vSRX device serving as a provider hub for the termination of IPsec and GRE data tunnels.

OSS/BSS applications and CSO components with OSS/BSS capabilities send requests to Network Service Orchestrator through its northbound REST API. Network Service Orchestrator then communicates through its southbound API to the northbound API of the appropriate, directly connected, component. Subsequently,

each component in the deployment communicates through its southbound API to the northbound API of the next component in the hierarchy. Components send responses in the reverse direction.

VNFs Supported by the Contrail Service Orchestration Solutions

Contrail Service Orchestration (CSO) supports Juniper Networks and third-party VNFs listed in Table 12 on page 83.

Table 12: VNFs Supported by Contrail Service Orchestration

VNF Name	Version	Network Functions Supported	Deployment Model Support
Juniper Networks vSRX	vSRX KVM Appliance 15.1X49-D123	• Network Address Translation (NAT) • Demonstration version of Deep Packet Inspection (DPI) • Firewall • Unified threat management (UTM)	SD-WAN deployments support NAT, firewall, and UTM.
Fortinet FortiGate NGFW	5.6.3	Firewall	SD-WAN deployments on NFX250 and NFX150 platforms. **NOTE:** Use *Fortinet-oam* in the NFX250 device profile when you set USE_SINGLE_SSH_TO_NFX as *False*, and use *Fortinet-no-oam* when you set USE_SINGLE_SSH_TO_NFX as *True*.
Single-legged Ubuntu	16.04	Firewall	SD-WAN deployments on NFX250 and NFX150 platforms.

An on-premises version of CSO is not shipped with any VNFs. Immediately after installation you have to upload any desired VNFs to the CSO platform using the Administration Portal.

You can use VNFs in service chains and configure some settings for them in Network Service Designer. You can then view those network service configuration settings in the Administration Portal. Customers can also configure some settings for the VNFs in their network services through Customer Portal. VNF

configuration settings that customers specify in the Customer Portal override VNF configuration settings specified in Network Service Designer, which is not available in a cloud-hosted CSO deployment.

> **NOTE:** Currently, SD-WAN deployments support only Layer 2 service chains.

In a cloud-hosted deployment, CSO only contains those VNFs installed by Juniper Networks' administrators. Requests for additional VNFs must be made through your account manager and Professional Services.

7

CHAPTER

Appendix B - Manual Staging of NFX

Install Junos OS Software onto an NFX Series Device from a USB Drive | 86

Install Junos OS Software onto an NFX Series Device from a USB Drive

This section details how to install Junos OS software onto an NFX Series device from a USB drive. Doing this sets the device to the factory-default state. We also perform some confirmation steps and obtain the device's serial number.

Before You Begin

In order for this procedure to succeed, be sure that you have the following:

- Physical access to the USB port of the NFX Series device
- A USB drive of at least 4GB containing the Junos OS software image inserted into the USB port of the NFX Series device
- Access to the console port of the NFX Series device (This can be physical access or access over a terminal server.)
- A DHCP server that is reachable from the **ge-0/0/11** interface of the NFX Series device. This DHCP server must be able to provide IP address, name server, and default gateway to the NFX Series device upon request.

To install Junos OS software onto an NFX Series device by using a USB drive:

1. Ensure that the USB drive containing the Junos OS software image is inserted in the USB port of the NFX Series device.

   This allows you to boot the NFX Series device from the USB drive.

2. Access the NFX Series device console either directly or using a terminal server.

   You do not need to login; just ensure that you are actively connected.

3. Power off the NFX Series device.

4. Power on the NFX Series device.

5. Immediately return to the session that you have open to the console port of the nfx1 device.

   From the console of the nfx1 device, press the ESC key every second until the following message appears: **Esc is pressed. Go to boot options.**

> **NOTE:** If you do not see this message in the console and the NFX appears to be booting normally, you need to wait for the boot to complete and then go back to step 1.

6. A menu appears after a brief time. Use the down arrow key to select **Boot Manager**, then press **Enter**.

7. When the **Boot Manager** menu appears, press **Enter** to boot from the **USB00** drive.

8. When the **GNU GRUB** menu appears, use the up or down arrow keys to select **Install Juniper Linux with secure boot support** and then press **Enter**.

At this point, the NFX Series device installs the software contained on the USB drive. Installation takes some time. You can keep your console connection active to watch the installation process.

The NFX Series device is made up of multiple components that load and boot in a specific order. See NFX250 Overview for details. The PFE of the NFX Series device may take a few minutes to complete the boot and allow the **jsxe0** interface to obtain its address from DHCP.

Log in to the console of the NFX Series device as the **root** user and confirm that the **jsxe0** interface has received its address using the following procedure:

1. Press **Enter** to refresh the login prompt.

2. At the **jdm login** prompt, type **root** and press **Enter**.

> **NOTE:** There is no password assigned to the root user at this point. For the purposes of this deployment exercise, do not set a root password at this time.

3. At the **root@jdm:~#** prompt, type **cli** and press **Enter**.

4. Type **show interfaces jsxe0** and press **Enter**.

The **jsxe0** interface has a number of logical interfaces used internally by the NFX Series device for different purposes. Look for the **jsxe0.0** logical interface. Confirm that the DHCP server has provided an address in the proper range before continuing.

```
root@jdm:~# show interfaces jsxe0
Logical interface jsxe0.1 (Index 4)
  Flags: Up
```

```
  Input packets : 0
  Output packets: 252
  Protocol inet, MTU: 1500

Logical interface jsxe0.2 (Index 5)
  Flags: Up
  Input packets : 3
  Output packets: 274
  Protocol inet, MTU: 1500

Logical interface jsxe0.0 (Index 3)
  Flags: Up
  Input packets : 7097
  Output packets: 8722
  Protocol inet, MTU: 1500
   Destination: 172.26.133.0/24, Local: 172.26.133.106,
   Broadcast: 172.26.133.255
```

At this point, you can confirm that the DNS name server and default gateway are working by issuing the **ping** command to some host on the Internet.

```
root@jdm:~ # cli
root@jdm:~ > ping www.juniper.net count 1
PING e1824.dscb.akamaiedge.net (23.223.165.73) 56(84) bytes of data.
64 bytes from a23-223-165-73.deploy.static.akamaitechnologies.com (23.223.165.73):
icmp_seq=1 ttl=56 time=2.67 ms

--- e1824.dscb.akamaiedge.net ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.670/2.670/2.670/0.000 ms
```

The last part of this procedure is to login to the Junos Control Plane (jcp) to obtain the device serial number which will be used later in the SD-WAN deployment.

```
root@jdm:~ > ssh vjunos0
Last login: Tue Jan 22 06:28:51 2019
--- JUNOS 15.1X53-D40.3 Kernel 32-bit FLEX
JNPR-10.1-20160217.114153_fbsd-builder_stable_10
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ #cli
root> show chassis hardware
```

```
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                DXXXXXXXXXX3
Pseudo CB 0
Routing Engine 0          BUILTIN      BUILTIN           RE-NFX250-S2
FPC 0            REV 04   650-066113   DXXXXXXXXXX3
  CPU                     BUILTIN      BUILTIN           FPC CPU
  PIC 0          REV 04   BUILTIN      BUILTIN           10x10/100/1000 Base-T-2x1G
 SFP-
Power Supply 0
Fan Tray 0                                               fan-ctrl-0 0, Front to Back
 Airflow - AFO
Fan Tray 1                                               fan-ctrl-0 1, Front to Back
 Airflow - AFO
```

The device serial number is listed on the **Chassis** line of the output. In this example, it is partly obscured for security purposes. Make note of the serial number for later use.

RELATED DOCUMENTATION

SD-WAN Deployment Overview | 26