

Contrail Service Orchestration

Contrail Service Orchestration (CSO) Deployment Guide

Published
2020-11-07

Release
5.0.3

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 Contrail Service Orchestration (CSO) Deployment Guide
5.0.3

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 | vii

Documentation and Release Notes | vii

Documentation Conventions | vii

Documentation Feedback | x

Requesting Technical Support | x

Self-Help Online Tools and Resources | xi

Creating a Service Request with JTAC | xi

1

Solutions Overview

About this Deployment Guide | 13

Contrail Service Orchestration (CSO) Solutions Overview | 13

Building Blocks Used for Contrail Service Orchestration Deployments | 18

Administrators | 18

Portals | 19

Tenants | 20

Topologies | 20

Points of Presence (POPs) | 23

Sites | 24

Customer Premises Equipment (CPE) | 27

Standalone Next-Generation Firewall (NGFW) | 28

Managed LAN Devices | 28

Virtual Route Reflector (VRR) | 28

SLA-Based Steering Profiles and Policies | 29

Path Based Steering Profiles | 30

Intent-based Firewall Policies | 30

Software Image Management | 30

2

Deployment Tools

Contrail Service Orchestration (CSO) Deployment Tools | 33

Contrail Services Orchestration (CSO) GUIs | 33

Designing and Publishing Network Services | 35

Contrail Service Orchestration License Tool | 36

Overview of the License Pages | 36

3

SD-WAN Deployment

SD-WAN Deployment Overview | 40

Contrail SD-WAN Deployment Architectures | 40

Contrail SD-WAN Reference Architecture | 41

Spoke Devices | 42

On-Premise Spoke Devices | 42

Cloud Spoke Devices | 44

Spoke Redundancy | 44

Hub Devices | 45

Hubs | 45

Hub Redundancy | 46

Underlay (Physical) Network | 46

WAN Access Options | 47

WAN Interface Types - Data and OAM | 48

Overlay (Tunnels) Network | 49

Overlay Deployment Topologies | 50

Orchestration and Control | 52

Secure OAM Network | 53

Integration with Deployment Topologies | 54

OAM Hub Design Options | 55

Usage Notes on Provider Hub Design Options | 56

Zero Touch Provisioning | 57

Usage Notes for ZTP | 57

Redirect Server | 58

Design Considerations for CSO and Redirect Server | 58

Bypassing the Redirect Server | 59

Service Chaining in Contrail SD-WAN | 59

Three Planes, Four Layers | 60

Your First SD-WAN Deployment | 61

Before You Begin | 62

Download Application Signatures | 63

Upload Licenses | 64

Create and Configure a New Tenant | 64

View Application Traffic Type Profile | 65

Modify Device Templates | 66

Upload Software Image for vSRX | 67

Choose a Point of Presence (POP) for the Hub Site | 68

Note Your Provider Hub Device | 69

Create and Configure the Tenant's Hub Site | 69

Create and Configure a Spoke Site for the Tenant | 70

Install License on Device | 73

Install Application Signature | 73

Add Firewall and NAT Policies to the Topology | 74

Add SD-WAN SLA-Based Steering Profiles and Policy | 74

4

Hybrid WAN Deployment (uCPE)

Hybrid WAN (Distributed) Deployment Overview | 78

Hybrid WAN (Distributed) Deployment Architecture | 79

Your First Hybrid WAN (Distributed) Deployment | 81

Modify Device Templates | 81

Add and Configure a New Tenant | 82

Add and Configure a Site for the Tenant | 83

5

Standalone Next-Generation Firewall (NGFW) Deployment

Next-Generation Firewall (NGFW) Deployment | 86

NGFW Deployment Overview | 86

NGFW Deployment Architecture | 87

NGFW Deployment | 87

6

LAN Deployment

SD-LAN with EX Switch | 93

LAN Deployment Overview | 93

SD-LAN Deployment | 94

7

Appendix A - Network Function Virtualization in Contrail Service Orchestration

Network Function Virtualization in the Contrail Service Orchestration Deployments | 100

Number of Sites and VNFs Supported in Contrail Service Orchestration | 102

VNFs Supported by the Contrail Service Orchestration Solutions | 103

8

Appendix B - Manual Staging of NFX

Install Junos Software onto NFX from USB Port | 105

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | vii
- Documentation Conventions | vii
- Documentation Feedback | x
- Requesting Technical Support | x

Use this guide to understand the next steps to be taken after successful installation of an on-premise CSO, or subscription to a cloud-hosted CSO. 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 viii](#) 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 viii 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
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

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

Convention	Description	Examples
<i>Italic text like this</i>	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 <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> 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 <i>metric</i> >;
(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 (<i>string1</i> <i>string2</i> <i>string3</i>)
# (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 [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

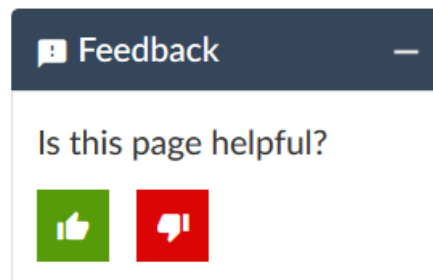
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> 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 | **13**

Conrail Service Orchestration (CSO) Solutions Overview | **13**

Building Blocks Used for Conrail Service Orchestration Deployments | **18**

About this Deployment Guide

The intent of this deployment guide is to provide a comprehensive understanding of the available Contrail Service Orchestration (CSO) solutions. To do that, we will:

- Briefly discuss each of the available solutions
- Discuss the building blocks used in every deployment
- Discuss the tools used to put the blocks together
- Provide an end-to-end walkthrough of each of the solutions that covers the deployment specifics.

This guide is hosted on the Contrail Service Orchestration Documentation page, alongside several other guides, including:

- [CSO Quick Start Guide](#)
- [CSO Administration Portal User Guide](#)
- [CSO Customer Portal User Guide](#)
- [CSO Monitoring and Troubleshooting Guide](#)
- [Contrail SD-WAN and SD-LAN Design and Architecture Guide](#)
- And more

Contrail Service Orchestration (CSO) Solutions Overview

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:

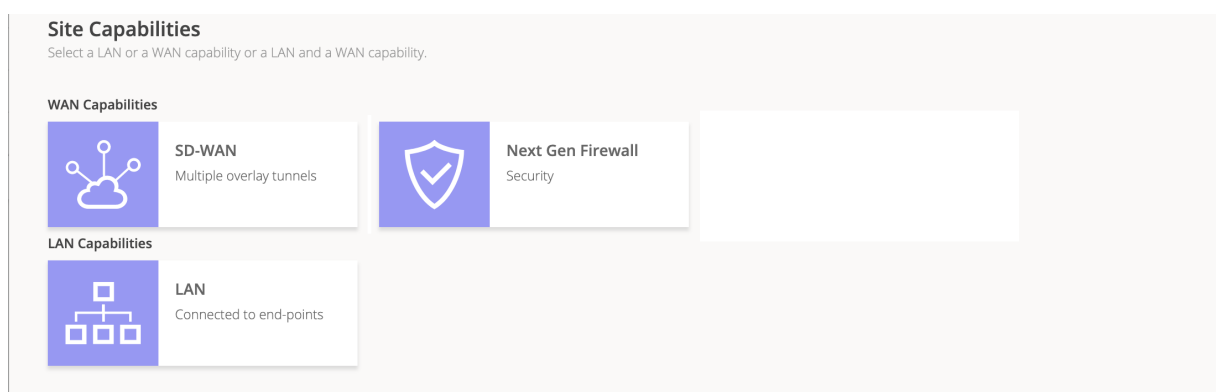
- As a downloadable, on-premise platform in which you (or your company) become the SP administrator (cspadmin user). In an on-premise deployment, the cspadmin user has complete read-write management

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 micro-services 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 14](#).

Figure 1: WAN and LAN Solutions



These solutions allow CSO to provide lifecycle management for devices and services and to:

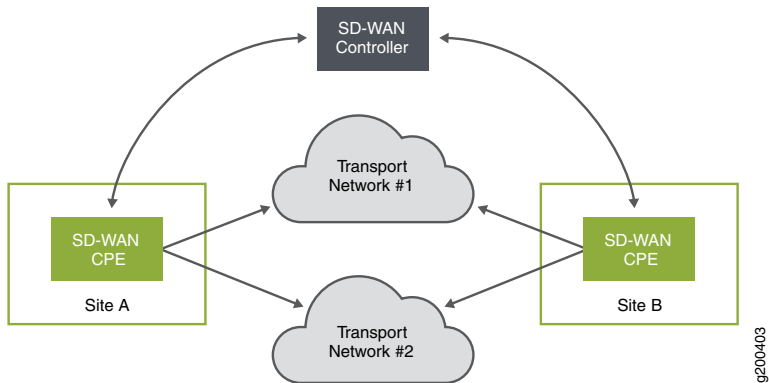
- automate physical and virtual device provisioning
- provide day-0, 1, and 2 configuration
- monitor remote devices
- provide full lifecycle management of firewall, NAT, and Internet breakout policies for user traffic
- provide high-level reporting about devices and user traffic

The following list briefly describes each of the available CSO solutions, or use cases.

Contrail SD-WAN Solution

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 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 15](#).

Figure 2: Basic SD-WAN Concept



The CPE devices, or spokes used in a Contrail SD-WAN solution, 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 15](#):

Table 3: Supported Hub Devices

Hub Device	Used as
vSRX	Enterprise Hub and Provider Hub
SRX1500	Provider Hub
SRX4100	Enterprise Hub and Provider Hub
SRX4200	Enterprise Hub and Provider Hub
MX Series Devices with Services Line Cards	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 (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

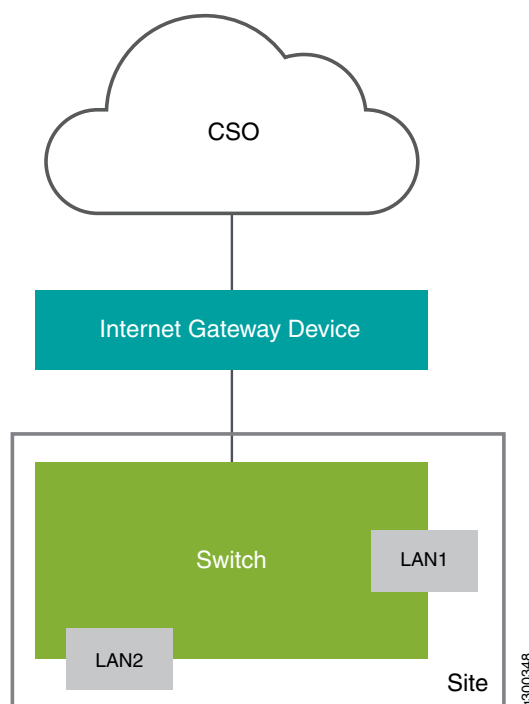
the use of dedicated IPsec tunnels. Starting with CSO Release 4.0.0, NFX Series spoke devices can also provide service chains of network services in addition to the routing flexibility already available.

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 Managed LAN Solution (SD-LAN)

The SD-LAN solution allows CSO to manage and monitor remote LAN devices like certain EX Series LAN switches and Virtual Chassis (VCs), as well as Mist WiFi access points.. 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

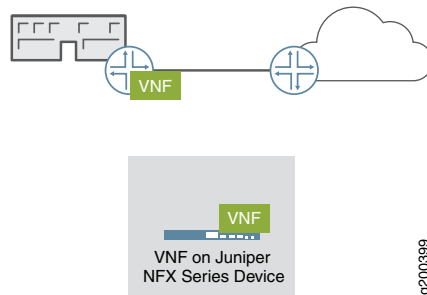


While [Figure 3 on page 16](#) shows a single switch connected behind an Internet gateway device, there are several other deployment options available within the solution. For example, an EX switch, or VC, can be attached to an existing managed CPE device, or it can be added to CSO as a standalone LAN switch. Similar deployment options are available for the NGFW solution. For more details about switch deployment in a managed LAN solution, see the [CSO User Guide](#) and the [CSO Design and Architecture Guide](#).

Hybrid WAN (Distributed CPE) Deployment Model

In a Hybrid WAN deployment, customers access network services from a CPE device, located at the customer's site. These sites are called *on-premise sites* or *spokes* in this documentation. In the workflows used in the CSO GUI, this deployment is known as Hybrid WAN. [Figure 4 on page 17](#) illustrates a simplified Hybrid WAN deployment.

Figure 4: Hybrid WAN Deployment



Initial configuration of the CPE device at the site can be automated through the use of zero touch provisioning (ZTP) that is orchestrated through CSO. CSO also monitors the CPE device and its services, and can push software and configuration updates to the devices remotely, reducing operating expenses. This deployment model is useful in environments where service delivery from the service provider's cloud is costly.

In fact, CSO has been designed to require only modest bandwidth, needing as little as 30kbps for probe and secure OAM traffic over Hybrid WAN connections where there are only a few sessions active. When AppQoe is involved, the bandwidth requirement increases to somewhere between 105kbps and 2Mbps, depending on the number of sessions. During ZTP operations, if new device images are needed, they can be downloaded as part of the ZTP process, or pre-staged on the device. In those circumstances, the bandwidth requirement increases to a maximum of 5Mbps only when device image download is needed. This makes these solutions applicable even in cases where connection bandwidth is limited or noisy.

The Hybrid WAN deployment uses a CPE device such as an NFX Series Network Services platform or SRX Series Services Gateway at the customer site and thus supports private hosting of network services at a site. The distributed deployment can be extended to offer SD-WAN capabilities.

NOTE: If an SRX Series device is used as the CPE device at the customer site, it can not host VNFs.

Building Blocks Used for Contrail Service Orchestration Deployments

IN THIS SECTION

- Administrators | 18
- Portals | 19
- Tenants | 20
- Topologies | 20
- Points of Presence (POPs) | 23
- Sites | 24
- Customer Premises Equipment (CPE) | 27
- Standalone Next-Generation Firewall (NGFW) | 28
- Managed LAN Devices | 28
- Virtual Route Reflector (VRR) | 28
- SLA-Based Steering Profiles and Policies | 29
- Path Based Steering Profiles | 30
- Intent-based Firewall Policies | 30
- Software Image Management | 30

Contrail Service Orchestration (CSO) uses conceptual and logical elements as building blocks to complete deployments in the GUI. This document provides some discussion about those elements and their use in CSO. For more detailed discussions regarding these elements, see the [Contrail Service Orchestration Administration Portal User Guide](#) and [Contrail Service Orchestration Customer Portal User Guide](#).

Administrators

CSO uses a hierarchical, domain-based administration framework. After CSO installation, the first administrator account is named **cspadmin** by default. This administrator is also known as the global service provider administrator or global administrator. This administrator has full read and write access to the entirety of the CSO platform from the global domain in the CSO Administration Portal. In a cloud-hosted CSO deployment, the cspadmin role is reserved for Juniper Networks, thus not available for login by anyone

else. The cspadmin can create, edit, and delete other administrators and operators who are subject to role-based access controls (RBAC) that assign them privileges to the rest of the objects in CSO.

In an on-premise CSO deployment, the next level of administrator is the Operating Company or OpCo administrator. In a cloud-hosted CSO deployment, the OpCo admin is the highest level of administrator available to customers. In this case, the first administrator for any given OpCo is created by the cspadmin user. The OpCo user has full administrative privileges within an OpCo domain of the CSO Administration Portal. An OpCo can be thought of as a region-specific service provider within the global service provider (Juniper Networks). The OpCo administrator can create other administrators and operators within the OpCo domain and its tenants, but can not affect elements of the global domain. Successful login by the OpCo administrator places them into the Administration Portal of their OpCo and they can switch into the Customer Portals of any Tenant of the OpCo.

The other level of administrator is the Tenant administrator. This administrator has full access to all objects within a single tenant and can create other administrator and operator users within that tenant. The tenant administrator's login places them into the Customer Portal for that Tenant.

There are also operator users at both the OpCo and Tenant level. Operator users are not, strictly speaking, administrators. By default, operators have read-only access to the elements in their domain.

Portals

Portals in CSO help to separate the administrators from the customers. CSO has both Administration and Customer Portals available. Access to any given portal is controlled by a user's login. If your login does not grant access to an administration portal, then you cannot see or access any of the elements of the administration portal.

Administration portals allow tenant creation and creation of other high-level objects that customers make use of within the customer portals. The Administration portal is the highest level of portal within CSO.

Customer portals provide users access to a subset of the objects that exist in administration portals. The primary example of this is that an OpCo administrator can see the **Tenants** page in the Administration Portal. Each tenant name on that page is a link that, when clicked, takes you to the customer portal for that tenant.

For more information about Administrator and Customer Portals, see the [Contrail Service Orchestration Administration Portal User Guide](#) and [Contrail Service Orchestration Customer Portal User Guide](#).

Tenants

CSO uses the tenant element to logically separate one customer from another. An OpCo administrator creates one tenant to represent each customer, or site, for which they will provide network services.

Using RBAC and other means, such as virtual routing and forwarding (VRF) instances within the network, CSO keeps all tenant and OpCo objects walled within their own space. This ultimately includes the traffic that traverses the customer networks. No individual tenant, its administrators, operators, or customers can see or interact with the objects of another tenant or customer. Tenants can be named in whatever way makes most sense to the SP.

Topologies

There are, essentially, four network topologies supported in CSO. When defining a tenant, the OpCo administrator must decide if that tenant will be able to use:

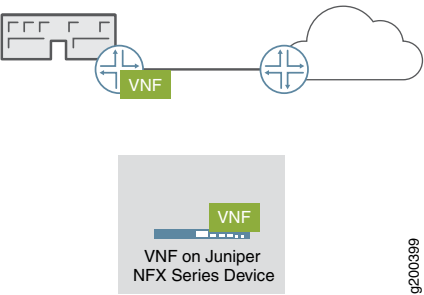
- **The Service Provider (SP) Cloud Topology**—This is generally assumed to be a traditional MPLS topology including provider edge (PE) routers, provider routers (P) and other resources that are owned and managed by the SP.

NOTE: In cloud-hosted CSO releases, the OpCo administrator may have no access or read-only access to the SP Cloud and any of its components.

- **Standalone Topology**—This topology is one in which the customers, or users of network services remain separate from each other with no means of communication amongst themselves.

This is the topology of the Hybrid WAN, solution wherein the SP provides network services to its on-premise customers but does not allow them to communicate with one another. [Figure 5 on page 21](#) shows an example where the virtual network functions (VNFs) are located at an on-premises site, but the site has no access to other sites belonging to the tenant.

Figure 5: Distributed CPE (or Hybrid WAN)



NOTE: For more information regarding network function virtualization (NFV) and VNF, see [“Appendix A - Network Function Virtualization in Contrail Service Orchestration” on page 100](#)

It is also the topology of the NGFW and LAN solutions. The NGFW solution provides for remote site security with SRX Series next-generation firewall devices. The LAN solution provides for remote site LAN management with EX Series LAN access switches. [Figure 6 on page 21](#) and [Figure 7 on page 22](#) below show high-level examples of these two solutions.

Figure 6: Standalone NGFW

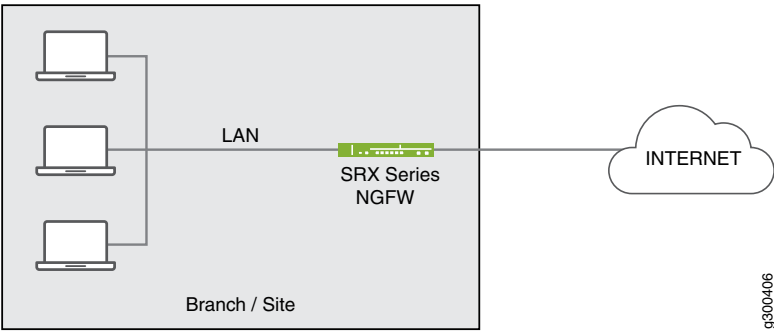
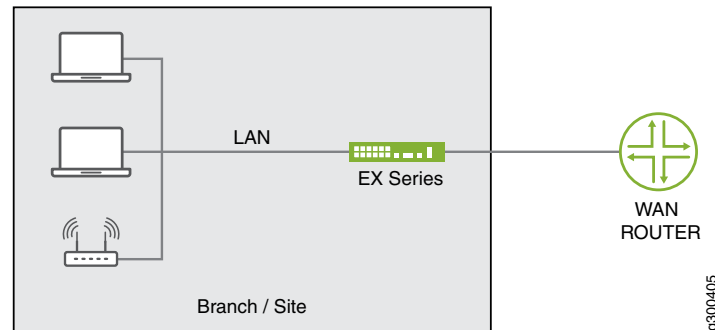
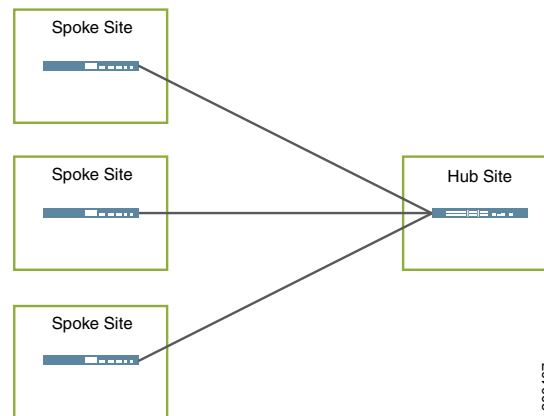


Figure 7: SD-LAN Solution with EX Switch



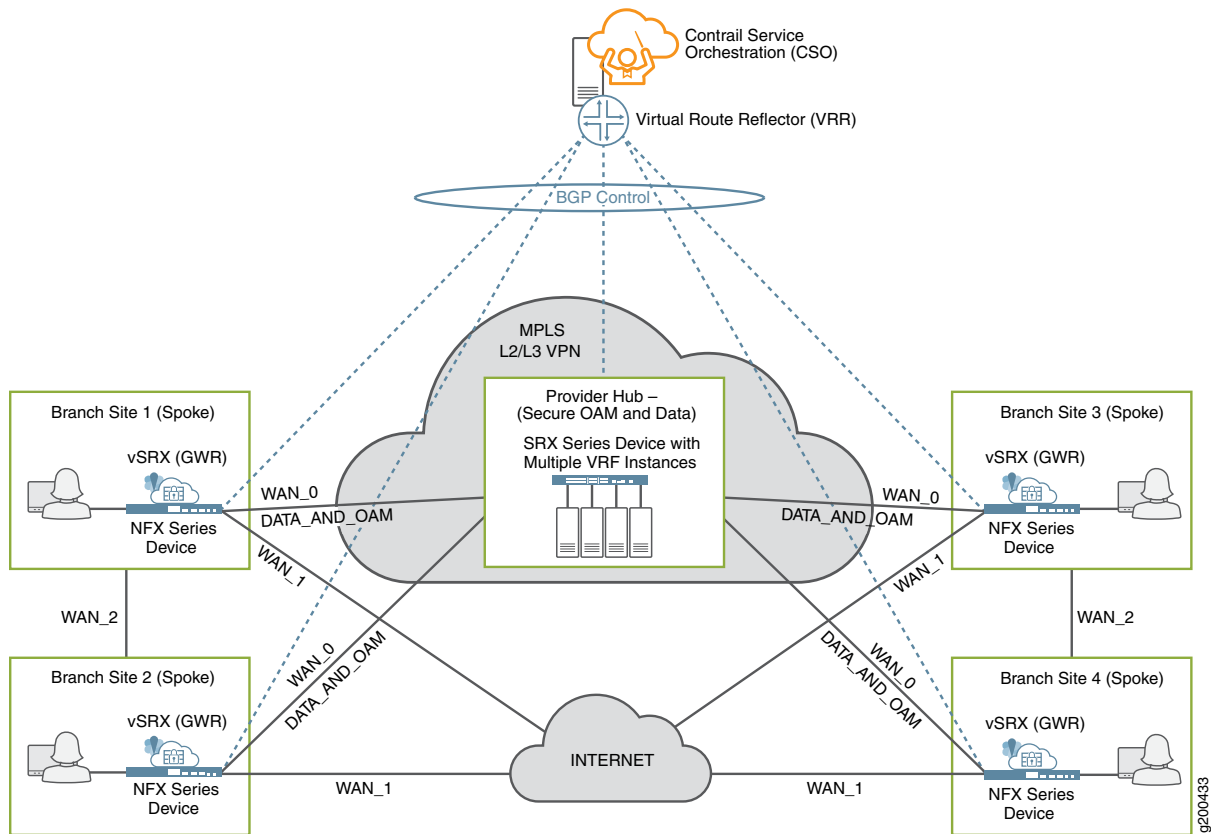
- Hub-and-Spoke Topology**–This topology is available for SD-WAN deployments. Given that SD-WAN is intended specifically to enable and enhance the efficacy of WAN communication using network overlays, this topology does allow for communication from site to site. Specifically, if one site needs to communicate with another site, that communication goes through the hub on its way to the other site. [Figure 8 on page 22](#) shows a very basic example of hub-and-spoke topology. VNFs can be deployed at any of the locations shown.

Figure 8: Hub-and-Spoke Topology



- Dynamic Mesh Topology**–This topology is also available for SD-WAN deployments. Direct site-to-site communication is allowed and every site is considered a hub site. [Figure 9 on page 23](#) shows a very basic example of a full mesh topology. VNFs can be deployed at any of the locations shown. This topology requires more overlay networks than the hub-and-spoke topology so CSO allows for the creation of a full mesh topology as a construct, but the tunnels from one site to another are created dynamically, (or on-demand) based on traffic thresholds thereby conserving resources and improving overall performance.

Figure 9: Dynamic Mesh Topology

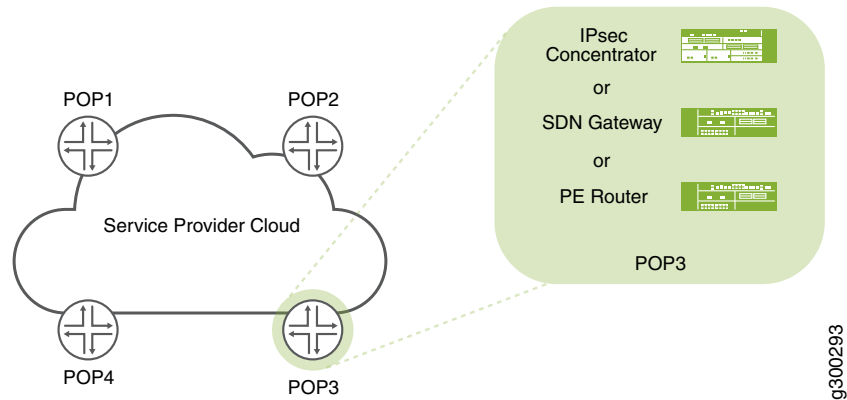


In addition, tunnelling requires the use of mesh tags. Each WAN interface on a CPE device in a dynamic mesh topology is configured with a mesh tag. Tunnels can only be formed between interfaces with matching mesh tags.

Points of Presence (POPs)

A POP is a placeholder, usually at the telco edge or enterprise datacenter, where network services can be deployed and underlay network connections are made to remote sites. POPs can have PE routers and Provider Hubs (both data and OAM type).

Figure 10: Points of Presence (POPs)



POPs are used in Hybrid WAN and SD-WAN deployments as a way to locate network access and network services closer to the users who need them. Different network services and different connection types can be offered at each POP, depending on need and availability. POPs can be named in whatever way makes the most sense to the SP administrator.

Sites

Sites are the branch offices or remote locations from which customers access the network services provided by the CSO solutions. A site is assigned to a POP and the type of sites available for creation depend on the type of deployment you are creating: SD-WAN, Hybrid WAN, Next Gen Firewall, or SD-LAN. Sites are created by the Tenant administrator or by an OpCo administrator by accessing the **Resources > Site Management** page. Sites can be named whatever makes sense for the Tenant. [Table 4 on page 25](#) lists what types of sites can be created within each deployment.

Table 4: Site Types by Deployment

Deployment	Available Site Types	Uses	Service Notes
SD-WAN	On-premise Spoke	Use this site type for locating NFX Series or SRX Series devices at customer sites in either a hub-and-spoke or full mesh topology.	<p>SRX Series devices deployed as on-premises spoke devices can not host VNF-based network services.</p> <p>NFX devices used as on-premise spoke devices can support ADSL, VDSL, and LTE access links, which can also be used for ZTP. The DSL access links allow configuration of PPPoE. LTE access links can be used as primary DATA, OAM, or OAM and Data links.</p> <p>NOTE: ZTP using an xDSL interface will not work if the link is PPPoE. If the link is bridged and uses DHCP, then ZTP will work on xDSL interfaces.</p> <p>Local breakout is supported on this type of site when using the dynamic mesh topology.</p>
	Cloud Spoke	This type of site is specifically for deploying a vSRX in a tenant's Amazon Web Services (AWS) Virtual Private Cloud (VPC)	<p>Firewall and UTM services are available to protect the customer's resources in the AWS VPC.</p> <p>WAN_0, WAN_1, and LAN interfaces need to be predefined in VPC.</p> <p>Two elastic IP addresses need to be reserved in VPC to attach to WAN interfaces later.</p> <p>VPC should be created and attached to an Internet gateway.</p> <p>Only hub-and-spoke topology is supported.</p> <p>Hub needs to have public IPs on in its WAN interfaces.</p> <p>Hub WAN interface type should be set as Internet during onboarding.</p>
	Provider Hub		

Table 4: Site Types by Deployment (*continued*)

Deployment	Available Site Types	Uses	Service Notes
		<p>Use this type of site for locating MX Series or SRX series devices in a SP cloud. The hub devices are used for establishment of IPSec tunnels. Hub devices are multi-tenant (shared amongst multiple sites) through the use of VRF instances configured on them.</p> <p>In a cloud-hosted CSO deployment, an OpCo or Tenant admin can create Provider Hub sites, but not the hub devices themselves. In this case, available hub devices are created by the cspadmin user and made available to the lower-level administrators.</p>	<p>You must specify the capability of the hub devices when setting up the site. Specifying OAM capabilities (OAM Hub) allows the hub to help create secure OAM networks between CSO and the CPE devices. This option is only available for on-premise CSO deployments.</p> <p>For cloud-hosted CSO, only data-only provider hub sites can be added by an OpCo administrator.</p> <p>A hub device is required for the dynamic mesh topology.</p> <p>Local breakout is not supported on Hub sites.</p>
	Enterprise Hub	Use this type of site, along with SRX4x00 Series Services Gateway devices, to provide additional capabilities to those of a normal spoke site.	<p>This type of site has the following capabilities:</p> <ul style="list-style-type: none"> • Can behave as a normal spoke • Anchor point for spokes for dynamic VPN creation • Provides on-premise central breakout option • Can host a data center department. Can import BGP and OSPF routes from the LAN-side L3 device. Thus creating a dynamic LAN segment. • Automatically meshed with other enterprise hub sites that belong to the same tenant. • Regular spoke sites can be assigned to associate with a gateway site. • Supports local, central and cloud breakout profiles with intent-based rules for more granular breakout control.

Table 4: Site Types by Deployment (*continued*)

Deployment	Available Site Types	Uses	Service Notes
Hybrid WAN/Distributed CPE	On-premise Spoke	Use this site type for locating NFX Series or SRX Series devices at customer sites.	<p>SRX Series devices deployed as on-premises spoke devices can not host VNF-based network services.</p> <p>NFX devices used as on-premise spoke devices can support ADSL, VDSL, and LTE access links, which can also be used for ZTP. The DSL access links allow configuration of PPPoE. LTE access links can be used as primary DATA, OAM, or DATA_OAM links.</p> <p>NOTE: ZTP using an xDSL interface will not work if the link is PPPoE. If the link is bridged and uses DHCP, then ZTP will work on xDSL interfaces.</p> <p>Local breakout is supported on this type of site.</p>

Customer Premises Equipment (CPE)

CPE devices are those devices that are placed at remote locations in the site types mentioned previously. CPE devices serve their functions as on-premise spoke devices in Hybrid WAN or SD-WAN deployments. [Figure 11 on page 27](#) shows available CPE device types.

Figure 11: CPE Devices



NFX250 and NFX150 Series Network Services Platforms, SRX300, SRX 550M, SRX4100, SRX4200, and vSRX Series Services Gateways can all be deployed as CPE devices. The NFX series devices provide the ability to host VNFs that can be deployed within the Hybrid WAN and SD-WAN solutions. The SRX Series devices cannot host VNFs but can provide their built-in security functions of firewall, UTM, and NAT as protection for the customer sites. In these cases, VNFs can still be deployed behind the SRX, but those VNFs cannot be managed by CSO.

When using SRX4000 Series Services Gateways, you can create an Enterprise Hub site that helps implement the on-demand IPsec tunnels used in dynamic mesh topologies.

Standalone Next-Generation Firewall (NGFW)

SRX Series devices can be used as standalone firewalls in the customer LAN and managed by CSO. CSO supports the use of the SRX300, SRX550M, SRX4100, and SRX4200 Lines for this purpose. In the next-generation firewall (NGFW) scenario, the SRX acts as a CPE device but provides no site-to-site or site-to-hub communications as with an SD-WAN solution.

You can add LAN capabilities along with or after the deployment of an NGFW site.

Managed LAN Devices

EX Series LAN access switches can be used as CPE devices to provide managed LAN services in branch/spoke sites. This SD-LAN solution supports the use of EX2300, EX3400, and EX4300 Series switches, in either standalone or virtual chassis (VC) configurations, for providing CSO managed LAN capabilities.

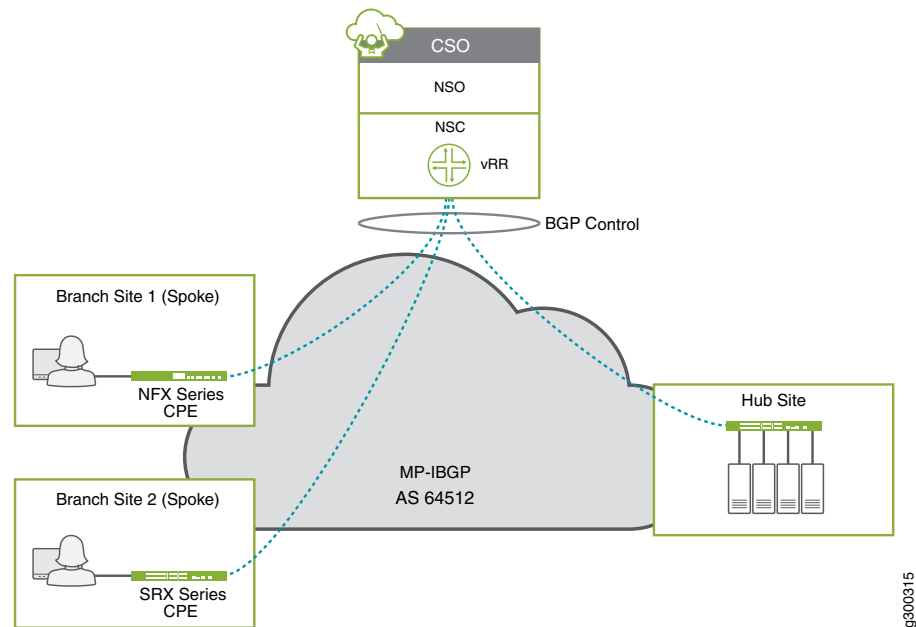
In addition, CSO supports dynamic routing protocols such as BGP and OSPF in the local LAN. Therefore, when SD-LAN is configured using any of the above devices, routes to the site LANs can be updated dynamically with BGP or OSPF.

In addition, SD-LAN sites can be extended to include Mist WiFi Access Points. If your Mist AP is connected to the EX switch at the time that the SD-LAN is provisioned, the Mist AP will be automatically accessible for management in CSO.

Virtual Route Reflector (VRR)

The VRR is part of CSO's SD-WAN controller. It is one of the virtual machines that get provisioned and installed during the on-premise CSO installation process. To facilitate the routing needed in the SD-WAN deployment, the VRR forms BGP sessions with CPE spokes and hub devices using the underlay interface designated as OAM or OAM_AND_DATA in the configure site GUI workflow for site onboarding. The OAM interfaces can be implemented using dedicated IPsec tunnels which allows CPE and hub devices to be behind NAT. [Figure 12 on page 29](#) illustrates the concept of the VRR

Figure 12: VRR Overview



g300315

SLA-Based Steering Profiles and Policies

CSO allows for the creation of SLA-Based steering profiles that can be mapped to SD-WAN policy intents for traffic management in an SD-WAN deployment. The profiles are designed to steer traffic to a specific WAN link based on SLA parameters such as packet loss, round trip time (rtt), and jitter thresholds. SLA steering profiles are created for global application traffic types for all tenants. An SLA profile consists of a set of configurable constraints that can be defined in the Administration Portal.

You can set:

- path preference for each of the connection paths from site-to-site
- path preference for each of the connection paths from site-to-hub
- threshold parameters for throughput
- threshold parameters for packet loss
- threshold parameters for latency
- threshold parameters for jitter
- class of service for various types of traffic
- rate limiters to control upstream and downstream traffic rates and burst sizes

Once the steering profile exists, an intent-based SD-WAN policy can be created that applies that profile to specific sites or departments and against specific types of application traffic such as ssh, http, etc.

NOTE: When creating an SLA profile, you must set either path preference or one of the SLA parameters. Both fields cannot be left blank at the same time.

See [Configuring Application SLA Profiles](#) in the [CSO Administration Portal User Guide](#) for more details.

Path Based Steering Profiles

Path based steering profiles are a simplified way to steer global application traffic types onto a specific WAN path. With these profiles, you do not need to configure any SLA parameters. All you need to do is specify which available path you want a specific traffic type to take. Just as with SLA steering profiles, you can set rate limiting parameters for these profiles. These profiles must also be assigned to an SLA Policy prior to

Intent-based Firewall Policies

Accessed through the Customer Portal, CSO presents firewall policies as *intent-based* policies. Firewall policies provide security functionality by enforcing intents on traffic that passes through a device. Traffic is permitted or denied based on the action defined as the firewall policy intent. If your intention is to block HTTP-based traffic from social media sites, but allow HTTP-based traffic from Microsoft Outlook, you can create an intent policy to do that.

See [Firewall Policy Overview](#) for more information.

Software Image Management

The CSO Administration Portal allows SP administrators to upload device software images and VNF images on the **Resources > Images** page. The cspadmin user in an on-premise CSO deployment can upload device images for supported SRX Series devices (including vSRX), NFX Series devices, and EX Series devices. He or she can also upload VNF images created in the Designer Tools applications.

For cloud-hosted versions of CSO, an OpCo administrator can see the images that have been uploaded to CSO by Juniper Networks. He or she can also stage and deploy uploaded device images to CPE devices and EX Series access switches.

Release History Table

Release	Description
5.0	SRX Series devices can be used as standalone firewalls in the customer LAN and managed by CSO. CSO supports the use of the SRX300, SRX550M, SRX4100, and SRX4200 Lines for this purpose.

2

CHAPTER

Deployment Tools

Contrail Service Orchestration (CSO) Deployment Tools | 33

Contrail Services Orchestration (CSO) GUIs | 33

Designing and Publishing Network Services | 35

Contrail Service Orchestration License Tool | 36

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-premise 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 to access the Contrail Service Orchestration (CSO) GUIs.

See [Table 5 on page 34](#) for information about logging into the Contrail Service Orchestration GUIs.

Table 5: Access Details for the GUIs

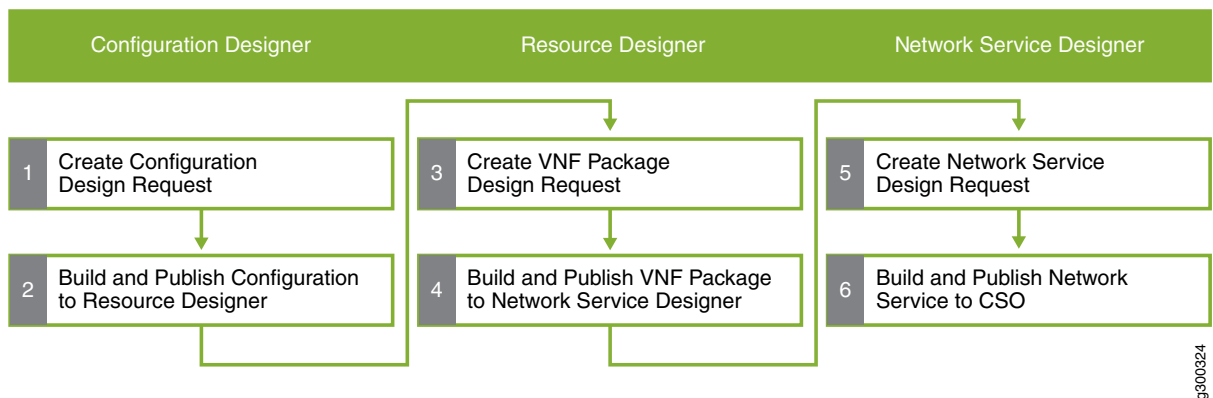
GUI	URL	Login Credentials
Administration Portal	<ul style="list-style-type: none"> For cloud-hosted CSO: Login credentials are sent to each Administration Portal user as an e-mail. The address to which the e-mail is sent is the <i>username</i> and the e-mail contains a link including an activation code. 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-premise CSO: <code>https://central-IP-Address</code> Where: <i>central-IP-Address</i> is the IP address of the VM that hosts the microservices for the central POP For example: <code>https://192.0.2.1</code> 	<ul style="list-style-type: none"> For on-premise 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	<p>Login credentials are sent to each Customer Portal user as an e-mail.</p> <p>The address to which the e-mail is sent is the <i>username</i> 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..</p>
<p>Designer Tools—Log into Network Service Designer and click the menu in the top left of the page to access the other designer tools.</p> <p>NOTE: Access to Designer Tools is only available for on-premise deployments of CSO.</p>	<p><code>https://central-IP-Address:83</code></p> <p>Where: <i>central-IP-Address</i> is the IP address of the VM that hosts the microservices for the central POP</p> <p>For example: <code>https://192.0.2.1:83</code></p>	<p>Specify the OpenStack Keystone username and password.</p> <p>The default username is cspadmin.</p> <p>Specify the autogenerated cspadmin password that is displayed on the console after the installation is complete.</p> <p>After the upgrade, you must specify the cspadmin password of the previously installed version.</p>

Designing and Publishing Network Services

NOTE: This section is only relevant for on-premise 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 13 on page 35](#) shows an overview of the workflow used within the Designer Tools application.

Figure 13: Designer Tools Overview



- First, you use *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.
- First, you use *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 *Network Service Designer* to:
 - Design service chains for network services using the VNF packages that you created with Resource Designer.
 - Configure the network services.
 - Publish network services to the network service catalog.

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

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

NOTE: Currently, SD-WAN deployments support only layer 2 (L2) service chains while Hybrid WAN deployments can support L2 and L3 service chains.

Contrail Service Orchestration License Tool

IN THIS SECTION

- [Overview of the License Pages | 36](#)

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.

SRX and vSRX Series devices can be used in both the Hybrid WAN and SD-WAN solutions as CPE devices or as provider or enterprise hubs. 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.

- The following items in a Hybrid WAN solution:
 - vSRX gateway router on an NFX Series device
 - vSRX or SRX Series CPE devices
- vSRX, SRX Series, or NFX Series CPE 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 **+** 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 **check box** 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 + button to add a new assignment.

A new row on the list will appear.

5. From the **Tenant** pull-down, 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.

See [Contrail Service Orchestration User Guide](#) for additional details about the CSO license pages.

3

CHAPTER

SD-WAN Deployment

SD-WAN Deployment Overview | **40**

Contrail SD-WAN Deployment Architectures | **40**

Your First SD-WAN Deployment | **61**

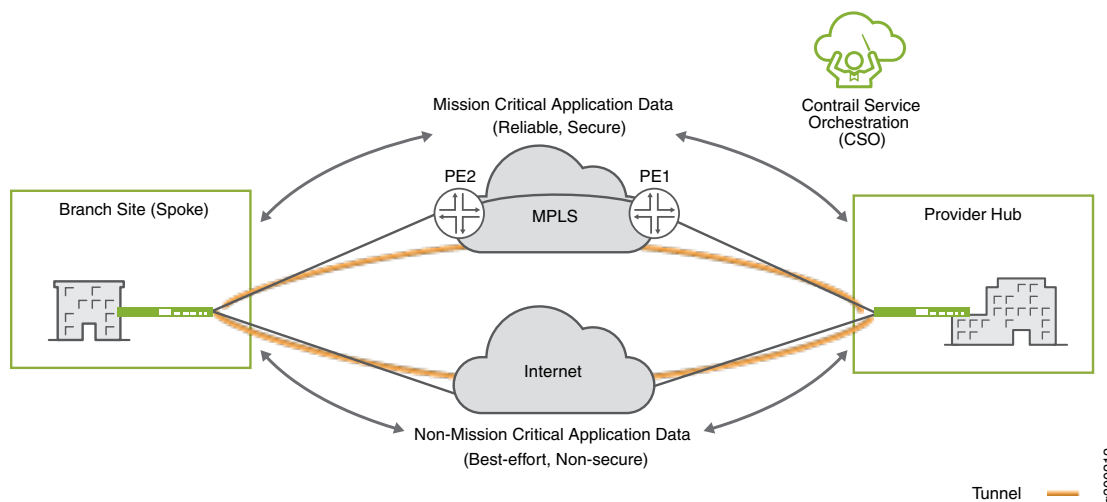
SD-WAN Deployment Overview

This walkthrough highlights the steps, or workflows, that you need to complete in order to deploy an SD-WAN solution using the hub-and-spoke topology with the 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. 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 at each step. It assumes that this is the first 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](#).

We use the topology shown in [Figure 14 on page 40](#) as a reference for this SD-WAN deployment.

Figure 14: SD-WAN Example Deployment Topology



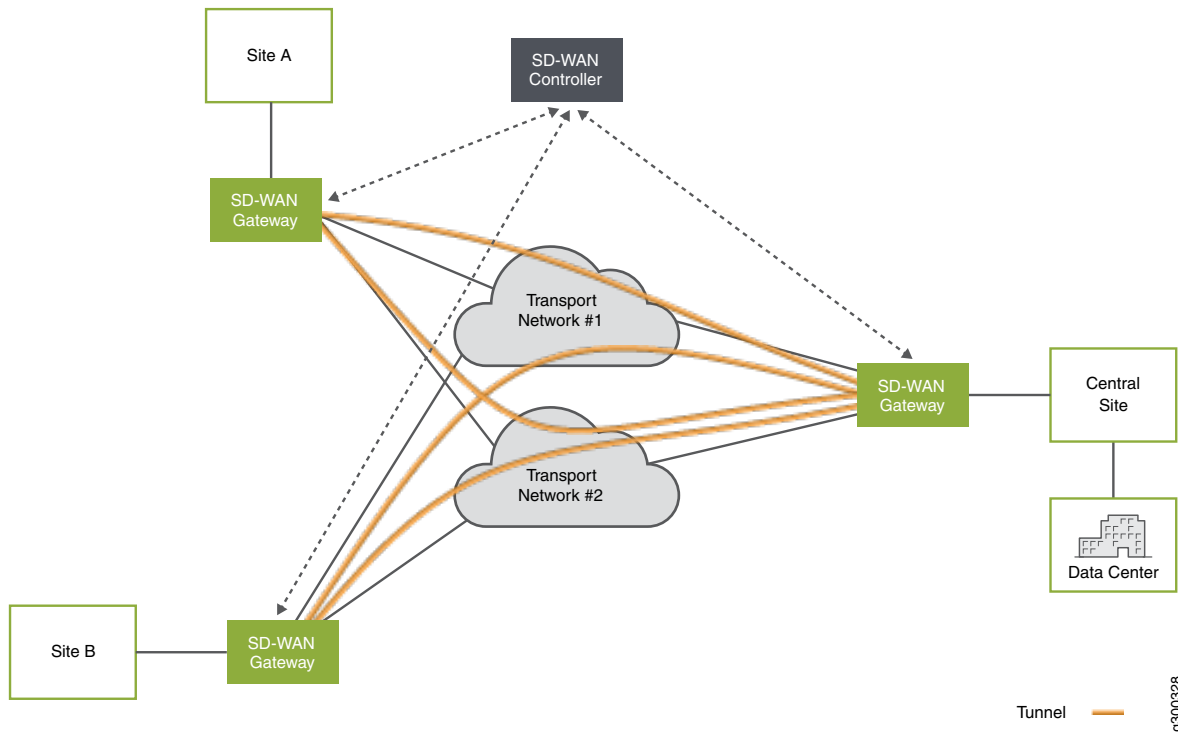
Contrail SD-WAN Deployment Architectures

An SD-WAN implementation offers a flexible and automated way to route traffic from site to site. As shown in [Figure 15 on page 41](#), a basic SD-WAN architecture includes just a few basic elements

- Multiple sites
- Multiple connections between sites that form the underlay network

- Multiple overlay tunnels
- A controller

Figure 15: SD-WAN Architecture

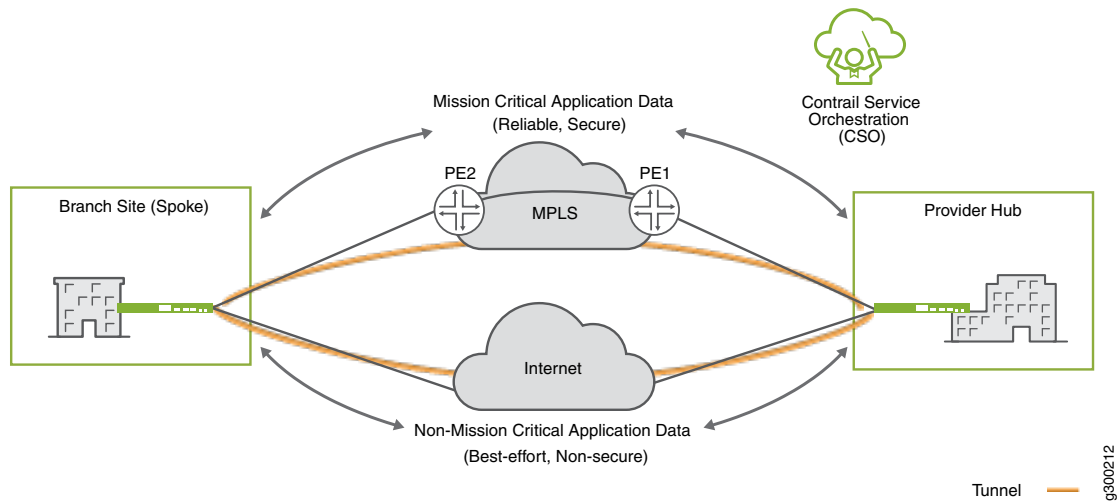


The SD-WAN controller, built-in to CSO, acts as an orchestration layer and provides an interface, allowing the operator to setup and manage the devices at the sites.

Contrail SD-WAN Reference Architecture

Juniper's Contrail SD-WAN solution architecture, shown in [Figure 16 on page 42](#) using a hub-and-spoke topology, is based on the Hybrid WAN model, with CPE devices located at customer branch sites. On the local side of the site, the CPE devices connect to LAN segments and can participate in dynamic routing protocols with other LAN devices. On the WAN side, the CPE devices connect across two or more links to a hub device. With the SD-WAN model (in a hub-and-spoke topology), traffic travels from site to site through the hub. By default, traffic going to the Internet also flows through the hub device.

Figure 16: Contrail SD-WAN Reference Architecture



The SD-WAN orchestrator and controller functions are implemented through Juniper's 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 these architectural elements in more detail.

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 (GWR), 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-premise spoke and cloud spoke.

On-Premise Spoke Devices

On-Premise spoke devices can be either NFX series devices or specific SRX series devices.

[Table 6 on page 43](#) shows the supported NFX hardware and required Junos OS software release version for each supported model.

Figure 17: On-Premise Spoke Devices



NFX Network Services Platform

The NFX Network Services Platform 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 GWR function, given its routing and switching capabilities. It also provides the same feature-rich security services found on a standard SRX series devices.

NOTE: The NFX150 includes SRX functionality natively built in.

Table 6: NFX Hardware and Software Matrix for On-Premise Spoke Devices

Platform	Models Supported	Junos OS Software Release Version
NFX150 Network Services Platform	<ul style="list-style-type: none"> NFX150-S1 NFX150-S1E NFX150-C-S1 NFX150-C-S1-AE/AA NFX150-C-S1E-AE/AA 	18.2X85-D12
NFX250 Network Services Platform	<ul style="list-style-type: none"> NFX250-LS1 NFX250-S1 NFX250-S2 	15.1X53-D497.0

SRX Series Devices and vSRX Virtual Firewall

A physical SRX device can be used in place of the NFX platform to provide the GWR function, as can a vSRX instance installed on a server. [Table 7 on page 44](#) shows the supported SRX hardware and required Junos OS software release version.

Table 7: SRX Hardware and Software Matrix for On-Premise Spoke Devices

Platform	Models Supported	Junos OS Software Release Version
SRX Series	<ul style="list-style-type: none"> • SRX4100 • SRX4200 • SRX300 • SRX320 • SRX340 • SRX345 • SRX550M 	15.1_X49_D172
vSRX Virtual Firewall	vSRX	15.1_X49_D172

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-premise spoke site. Only SRX4100 and SRX4200 devices can serve this function. The spoke site that functions this way, must be configured as a nEnterprise Hub site during site creation. Creating an Enterprise Hub site with an SRX4x00 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
- Provides for a new, 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, etc.

Cloud Spoke Devices

A Contrail SD-WAN spoke device, in the form of a vSRX, can be located in an AWS VPC. The vSRX serves as the cloud spoke device; 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 [Contrail SD-WAN Design and Architecture Guide](#).

Hub Devices

The Contrail SD-WAN solution supports two deployment topologies (discussed later in this guide): 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 hub device and one or more spoke devices.

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

Hubs

In a service provider (SP) environment, a Provider Hub is owned by the service provider and the Provider Hub device resides within the service provider's network (POP). 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 SaaS deployment of CSO, the SP administrator role is performed by the operating company (OpCo) administrator. In an on-premise CSO deployment, either the cspadmin user or an OpCo administrator can perform the SP administrator role.

In an enterprise environment, the enterprise hub is owned by the customer (tenant) and the hub device resides within the enterprise data center. Only the customer's spoke sites can connect to its hub device. OpCo administrators and tenant administrators can manage the Enterprise Hub.

Figure 18: SD-WAN Hub Devices



As of CSO Release 5.0, the supported hub devices are shown in [Table 8 on page 46](#)

Table 8: Hub Devices

Role	Supported Device Types	Required Junos OS Software Version	Usage Notes
Hub	<ul style="list-style-type: none"> • MX Series Devices with Services Line Cards • SRX1500 • SRX4100 • SRX4200 • vSRX 	<p>For MX Series Devices: 16.1R5.7</p> <p>For SRX Series Devices: 15.1X49-D172</p> <p>For vSRX: 15.1X49-D172</p>	<p>The requirement for the Services Line Card (MIC or MPC) is there so that the MX can terminate IPsec tunnels.</p> <p>See MPCs Supported by MX Series Routers and MICs Supported by MX Series Routers for information about MX Series routers that support Multiservices MPC and MIC line cards</p>

Hub Redundancy

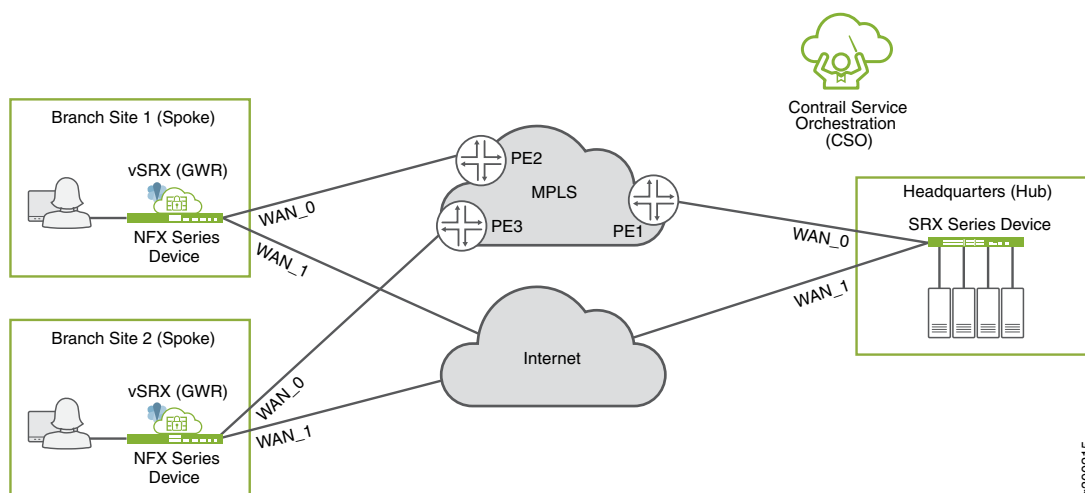
Starting with CSO Release 3.3, two redundant hub devices can be used at one POP to protect against device and link failures, and to provide upstream multihoming for spoke sites. For more detail, see the Resiliency and High Availability section of the [Contrail SD-WAN Design and Architecture Guide](#).

Underlay (Physical) Network

The underlay network includes the physical connectivity between devices in the SD-WAN environment. This layer of the network has no awareness of the customer LAN segments, it simply provides reachability between on-premise devices.

[Figure 19 on page 47](#) shows a sample underlay network for a hub-and-spoke SD-WAN deployment (the details apply equally to a dynamic mesh setup). Each spoke site typically has multiple paths to the hub site; in this case, one through the private MPLS cloud, and one over the Internet.

Figure 19: SD-WAN Underlay Network



Each on-premise device (or site) can have up to four WAN links, including a satellite link that can be used for OAM. During configuration, CSO identifies the devices' WAN-facing interfaces as WAN_0 through WAN_3.

Note that:

- The WAN interfaces can be VLAN tagged or untagged, as per design requirements.
- The on-premise devices' Internet-facing interfaces can be attached to different service provider networks.

WAN Access Options

Each WAN access type listed below can be used for ZTP, data, or OAM traffic. All the links can be leveraged for data traffic simultaneously.

- MPLS
- Ethernet
- LTE

NOTE: LTE WAN access supported using a dongle on NFX250 Series devices.

LTE WAN access supported using a built-in interface on NFX150 Series devices.

LTE WAN access supported using a mini-PIM in slot 1 of SRX300 Series devices.

All of the previously mentioned LTE interfaces are supported for ZTP.

Only supported for Hub-and-Spoke SD-WAN deployments with single CPE.

Full/Dynamic Mesh deployments are not supported.

Dual CPE configurations are not supported.

LTE APN settings can be localized for the installation region during the ZTP process.

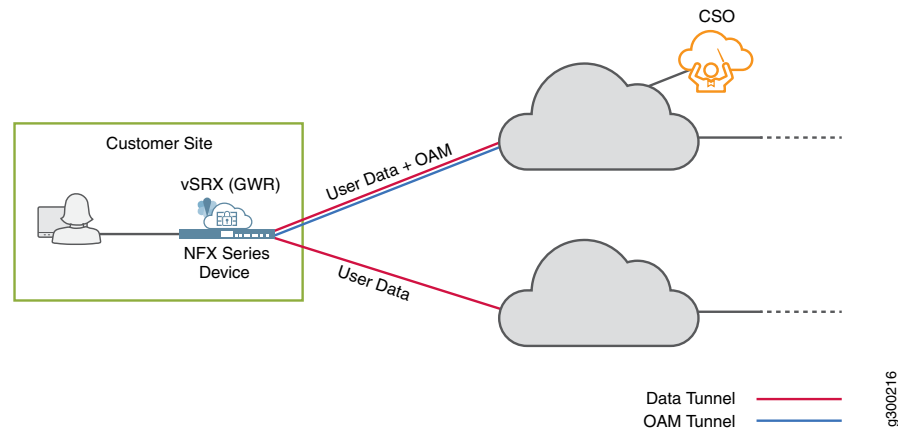
- ADSL/VDSL (ADSL/VDSL support for WAN links and ZTP on NFX Series devices starting in CSO Release 4.0.0 and on SRX300 Series devices starting in CSO Release 5.0.3.)
- Broadband
- MPLS and broadband
- Satellite link

WAN Interface Types - Data and OAM

The WAN interfaces are used primarily to send and receive user traffic (data). At least one of the WAN interfaces must also be used for management (OAM) traffic. The OAM interface is used to communicate with CSO, and allows CSO to manage the on-premise device.

[Figure 20 on page 49](#) illustrates these two interface types.

Figure 20: WAN Interface Types



Note that:

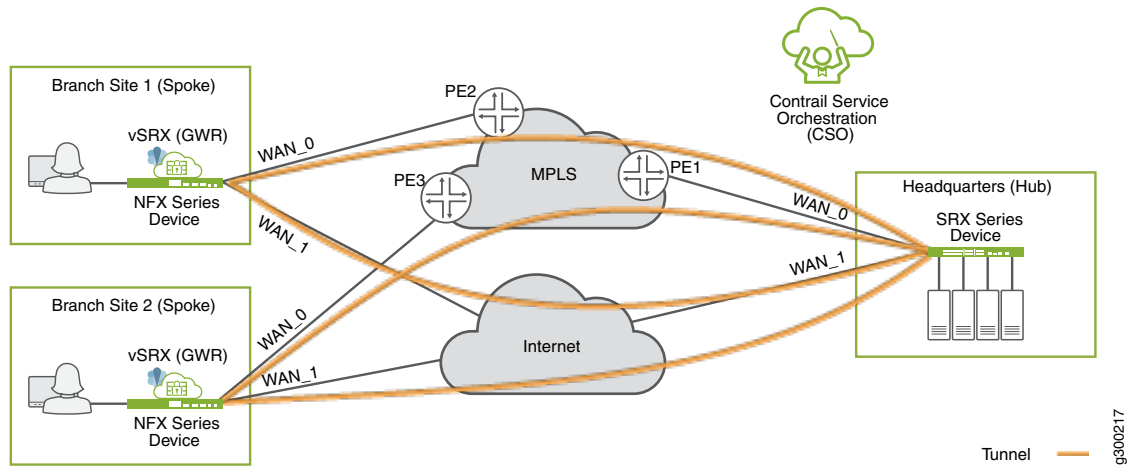
- The on-premise device's OAM interface must be able to reach CSO. The connectivity can be supplied strictly using CSO-orchestrated overlay networks. You do not need pre-existing underlay network connectivity for this. Starting in CSO release 5.0.1, CSO automatically selects an IP address for the on-premise device's OAM interface. This ensures that the address is unique within the entire CSO deployment and prevents human error.
- To ensure secure communication over the WAN, the on-premise device initiates the connection to CSO.
- Device-initiated connections can work across intermediate NAT devices.
- The user-and-OAM-data interface can use a single IP address for both functions.

Overlay (Tunnels) Network

The overlay network includes the logical tunnel connectivity between devices in the SD-WAN environment. This layer of the network has awareness of the customer LAN segments, and is responsible for transporting customer traffic between sites.

[Figure 21 on page 50](#) shows an overlay network for a hub-and-spoke environment. Each spoke site has two tunnels to carry traffic to the hub site: one through the private MPLS cloud, and one over the Internet.

Figure 21: SD-WAN Hub-and-Spoke Overlay



The tunnels have two encapsulation options: MPLSoGRE or MPLSoGREoIPsec. CSO automatically provisions and establishes these tunnels as part of the deployment process.

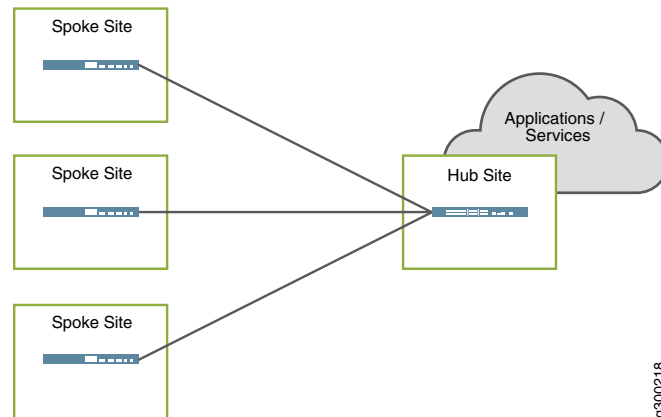
Overlay Deployment Topologies

The SD-WAN solution supports hub-and-spoke or dynamic mesh deployment topologies. A dynamic mesh topology is similar to a full mesh topology wherein every site is capable of connecting directly to any other site. But with dynamic mesh, the connections (tunnels) are brought up on-demand, thereby reducing the continual load on any one site. A single tenant can support both hub-and-spoke and dynamic mesh topologies.

Hub and Spoke

With the hub-and-spoke topology, all spoke sites are connected to at least one hub site, as shown in [Figure 22 on page 51](#). Spoke sites cannot communicate directly with other spoke sites.

Figure 22: SD-WAN Hub-and-Spoke Topology

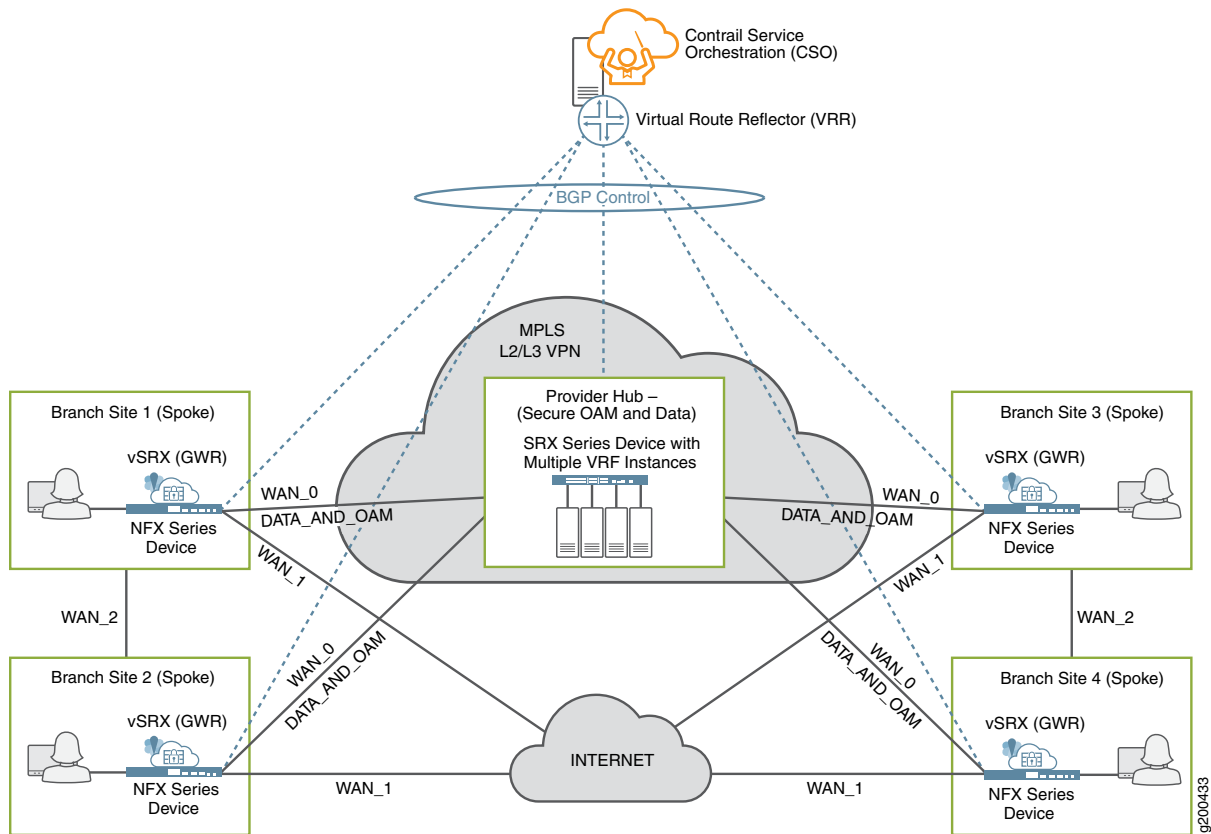


The hub sites used can be either provider hub or enterprise hub sites. When an enterprise hub site is used, the provider hub (if any) is used as backup only. This topology is preferred when applications and services are centralized at the hub site.

Dynamic Mesh

With the dynamic mesh topology, all sites are interconnected using overlay tunnels, as shown in [Figure 23 on page 52](#), and each site can communicate directly with every other site through the tunnels. Although the figure shows the DATA_AND_OAM connection on the MPLS link, WAN_0, this function can be performed on either the MPLS or Internet links.

Figure 23: SD-WAN Dynamic Mesh Topology



This topology is well suited for deployments where applications and services are not centralized.

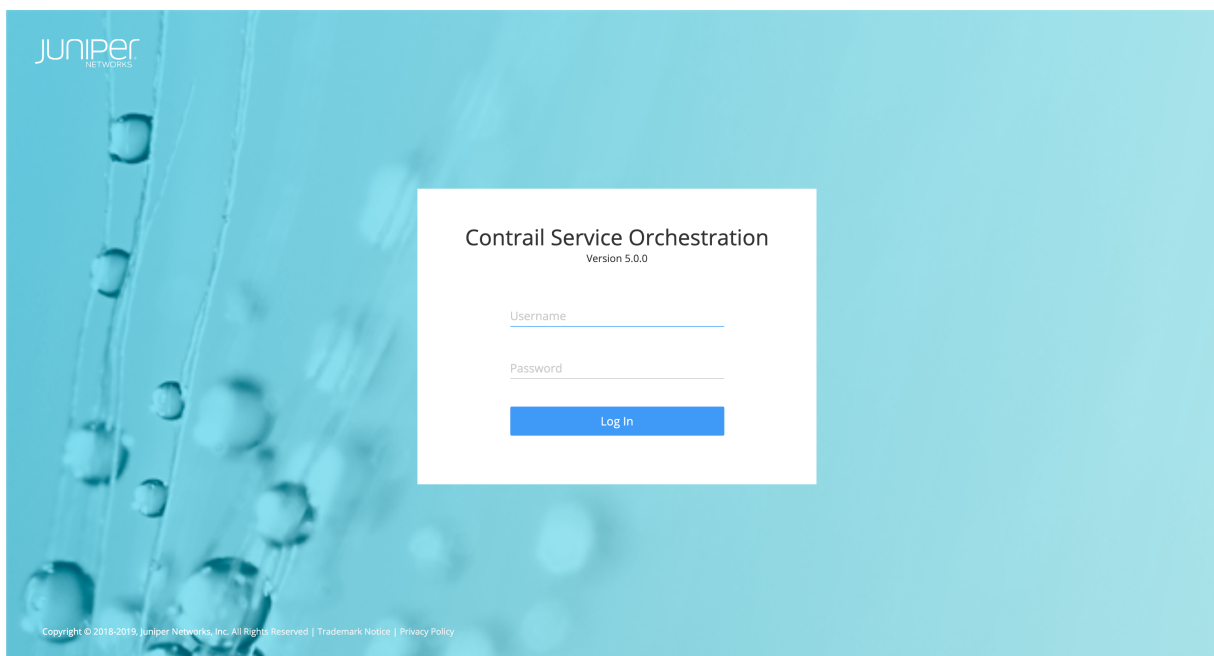
NOTE: Both hub-and-spoke and full mesh topologies require adding a secure OAM network overlay, and thus an OAM Hub, to the deployment.

When spoke devices are added to a dynamic mesh topology, the administrator configuring the sites must assign a mesh tag to each WAN interface. Only two devices with matching mesh tags can form the VPN connection to allow communication. Interfaces with mismatched mesh tags can never communicate directly.

Orchestration and Control

Orchestration and controller functions are implemented through Juniper's Contrail Service Orchestration (CSO) software. CSO software offers a Web-based UI to manage the SD-WAN environment, as shown in [Figure 24 on page 53](#).

Figure 24: CSO Login Screen



The Service Orchestration Layer contains the Network Service Orchestrator (NSO). The orchestration software has a global view of all resources and enables tenant management, providing end-to-end traffic orchestration, visibility, and monitoring. The Domain Orchestration Layer contains the Network Service Controller (NSC). The orchestration software works together with the controller to manage on-premise (CPE) devices, and provide topology and CPE lifecycle management functionality.

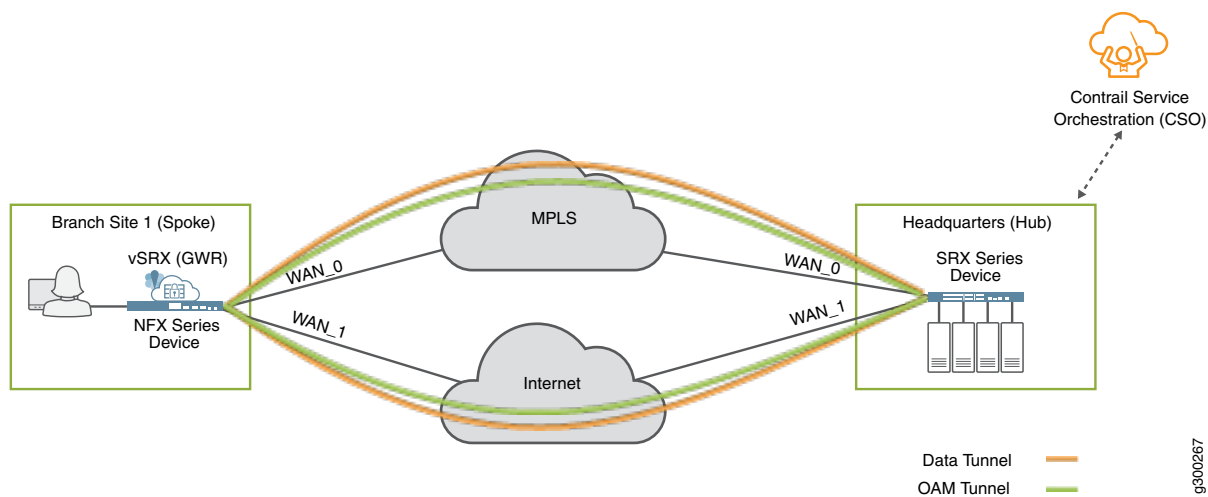
At the user level, CSO provides the interface to deploy, manage, and monitor the devices in the SD-WAN network through the NSC. At the network level, NSC includes a vRR that allows each site to advertise its local routes to remote sites.

For more information regarding SD-WAN architecture, see [Contrail SD-WAN Design and Architecture Guide](#).

Secure OAM Network

SD-WAN deployments include a secure OAM overlay network to provide end-to-end secure communications between on-premise devices and CSO. This is true regardless of whether your CSO software is deployed on-premise or as a SaaS deployment. In an SaaS deployment, the Provider hub devices, and thus, one end of the OAM network is owned and managed by the SP. As shown in [Figure 25 on page 54](#), dedicated, IPsec-encrypted OAM tunnels enable on-premise devices to send management, routing, and logging traffic securely over the network to a provider hub. The hub then forwards the traffic to CSO.

Figure 25: Secure OAM Tunnels



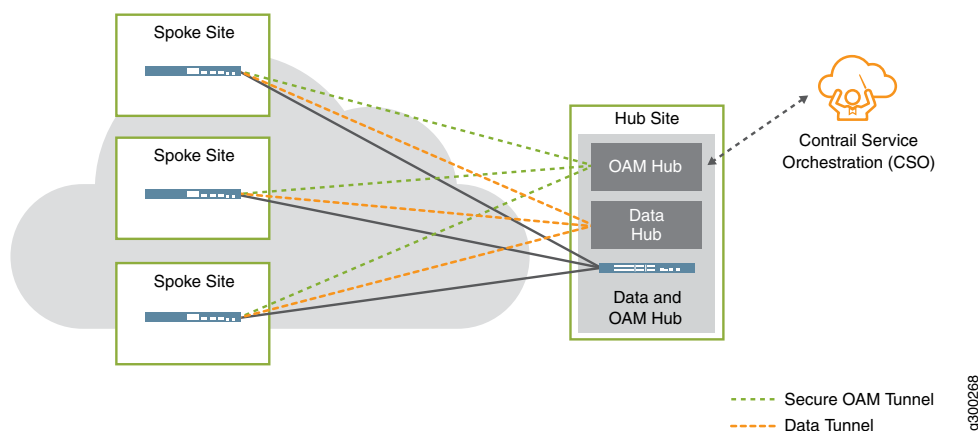
Integration with Deployment Topologies

Both the hub-and-spoke and dynamic mesh deployment topologies must use secure OAM tunnels.

Hub and Spoke

With the hub-and-spoke topology, each spoke site now has two sets of connections to the provider hub site: an overlay tunnel carrying data, and a separate, dedicated IPsec overlay tunnel carrying OAM traffic, as shown in [Figure 26 on page 54](#).

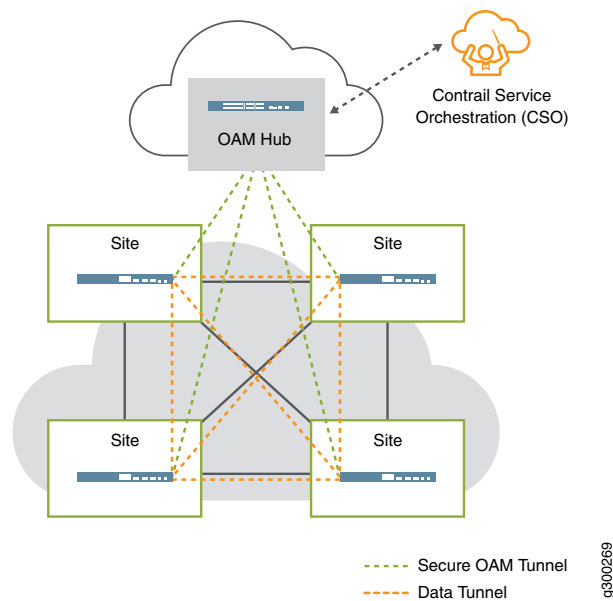
Figure 26: OAM Tunnels in the Hub-and-Spoke Topology



Dynamic Mesh

Since a normal full mesh topology would not include a hub device for data traffic, one must be added. As shown in [Figure 27 on page 55](#), each spoke site has a new connection: a separate, dedicated IPsec overlay tunnel carrying OAM traffic to the provider hub.

Figure 27: OAM Tunnels in the Full Mesh Topology

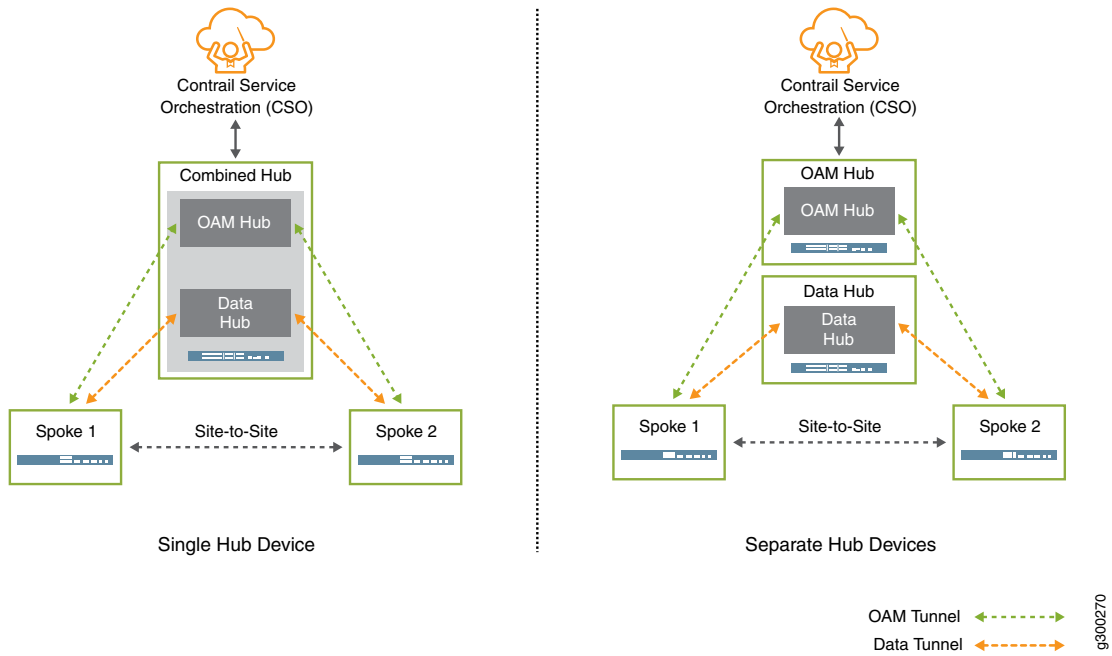


OAM Hub Design Options

There are two ways to implement the OAM hub in an on-premise CSO deployment, depending on design requirements. As shown in [Figure 28 on page 56](#), the options are as follows:

- Data and OAM tunnels terminate on same provider hub device—this is a good option for small deployments, where the single hub device can handle both the data and OAM traffic.
- Data and OAM tunnels terminate on separate provider hub devices—this option can be useful for larger deployments where the main hub device's resources are needed to service the overlay tunnels carrying data traffic; a second hub device can be used to terminate the OAM tunnels.

Figure 28: OAM Tunnels - Provider Hub Design Options



NOTE: In a cloud-hosted CSO deployment the OAM hub is provided as part of the service.

However, an OpCo administrator can deploy a DATA_ONLY or an OAM_AND_DATA hub. In the case of a DATA_ONLY hub, the DATA hub has an IPsec secured tunnel to the OAM_HUB. In the case of an OAM_AND_DATA hub, the OpCo administrator is required to set up the IPsec secured connection between the OAM_AND_DATA HUB and CSO.

Usage Notes on Provider Hub Design Options

- An OAM hub can support multiple tenants, or can be dedicated to a single tenant.
- Connectivity from the provider hub(s) to CSO should be private and secured, as it is not covered by the OAM tunnels.
- We recommended that you implement multiple OAM hubs for redundancy and to ensure no loss of management or monitoring of the on-premise devices.

For a cloud-hosted CSO deployment, OAM hub redundancy is handled by the SP Administrator so cannot be addressed by an OpCo or tenant administrator.

- When a spoke site is multi-homed to multiple hub devices, one OAM tunnel should terminate on each hub.
- On-Premise devices using NAT are supported for hub-and-spoke deployments.

Zero Touch Provisioning

One of the key features of the Contrail SD-WAN solution is the ability to “plug-and-play” new spoke devices using ZTP (autoinstallation). In CSO, the ZTP process is implemented with the help of an Internet-located redirect server. For true ZTP, the use of the redirect server is required. The redirect server itself is discussed in the next section.

A high-level list of steps performed during ZTP looks like:

- Before performing ZTP, add the appropriate CSO SSL certificate to the redirect server.
- When a spoke device first comes online, it uses a local DHCP server to obtain an IP address and name server information.
- The spoke device then contacts the redirect server, which provides the DNS name and certificate for the CSO installation.
- The spoke device then contacts the CSO server to obtain its initial configuration and Junos OS software update (if required).

NOTE: CSO Release 4.1 and later include enhancements that reduce the bandwidth required for ZTP to 2mbps.

Usage Notes for ZTP

- At least one of the device's WAN interfaces must obtain its IP address from a DHCP server in order to also be assigned a DNS name server and a default route.
- Both CSO and the redirect server must be reachable over the same WAN interface.
- The ZTP process can be run from any WAN interface on the spoke device, including a satellite link.
- The download of the initial configuration can require significant amount of time, especially on slow links, due to the size of configuration and Junos OS software.

Redirect Server

The redirect server is an Internet-located, Juniper-owned-and-managed server that is integral to the ZTP process. The function of the server is to hold and distribute the DNS names and SSL certificates of all CSO instances so that newly installed spoke devices can locate and authenticate to their designated CSO instance.

During site configuration, the serial number of the spoke device is entered into CSO. This leaves the specific CSO instance in a state where it is expecting contact from a device with this serial number. When the redirect server is contacted by the spoke device, it uses the serial number to:

- Pair the device with the proper instance of CSO
- Pass the proper SSL certificate to the spoke device
- Pass the DNS name of the proper CSO instance to the spoke device

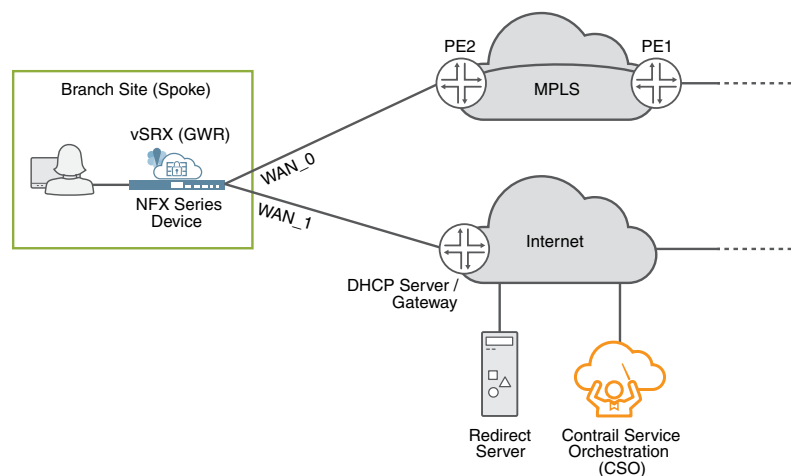
With the above information, the spoke device can contact CSO and receive its initial configuration, including Junos OS software update (if required).

Design Considerations for CSO and Redirect Server

The redirect server is located on the Internet, and cannot be moved.

In [Figure 29 on page 58](#), both the redirect server and CSO are located on the Internet. In this case, the spoke device obtains and uses IP addressing and other information provided through its Internet-facing interface, and can then reach both the redirect server (first) and CSO (second) through that same interface. This is the only CSO deployment option available for the Juniper-hosted CSO instance in release version 5.0.

Figure 29: CSO and Redirect Servers on Internet



g300222

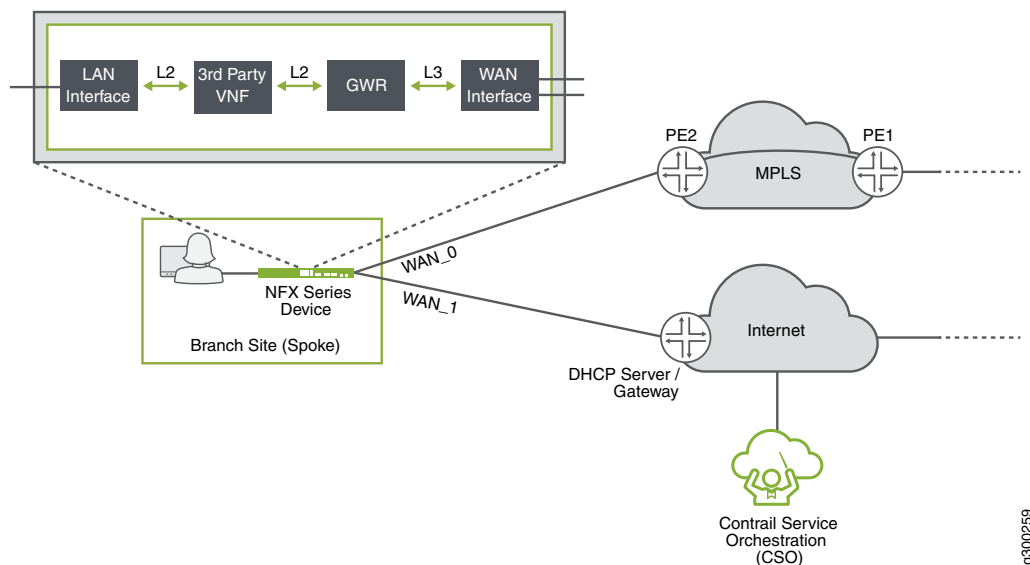
Bypassing the Redirect Server

In some cases, it may not be desirable or practical to use the Juniper redirect server. In these cases, a spoke device can be pre-staged to include reachability information for the CSO server before being shipped to the customer location.

Service Chaining in Contrail SD-WAN

As of CSO Release 4.0, service chaining is available for SD-WAN environments. Service chaining is a concept wherein multiple network services instantiated in software and running on x86 hardware are linked, or chained together in an end-to-end fashion. This allows the one physical device to provide the services normally provided by multiple devices. Service chaining can be performed on NFX Series devices, as shown in [Figure 30 on page 59](#).

Figure 30: Service Chaining in an SD-WAN Environment



In CSO release 4.0, the following third-party virtual network functions (VNFs) are supported: *Fortigate-VM* and *Single-legged Ubuntu VM*.

NOTE: Currently only Layer 2 VNF mode is supported in SD-WAN service chains.

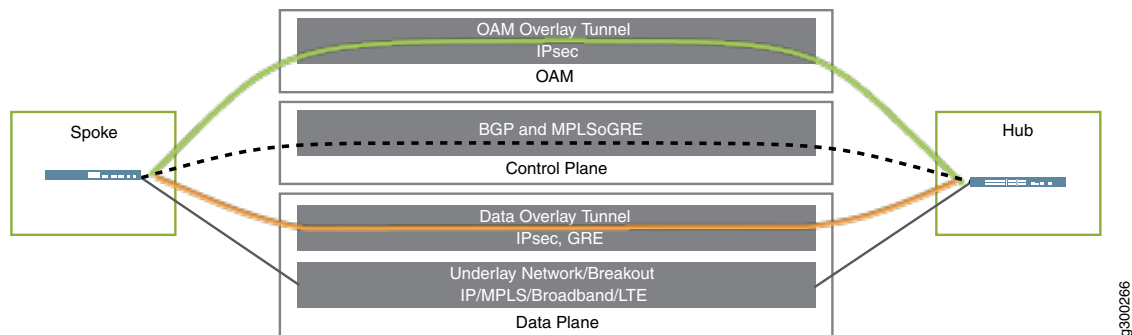
Three Planes, Four Layers

To bring all of the above elements together, the Contrail SD-WAN Architecture can be thought of in three planes, comprised of four functional layers:

1. Data Plane:
 - Includes the underlay network; provides physical connectivity
 - Includes the overlay network; provides tunnels for tenant data traffic
2. Control Plane—includes the routing protocols which flow through the OAM tunnels
3. Management Plane—includes the overlay tunnels for the secure OAM network

The graphic in [Figure 31 on page 60](#) illustrates this concept.

Figure 31: Three Planes, Four Layers



Release History Table

Release	Description
5.0	
4.1	A special type of spoke device, called an Enterprise Hub Device, can be deployed as the CPE at an on-premise spoke site. Only SRX4100 and SRX4200 devices can serve this function.
4.0	As of CSO Release 4.0, service chaining is available for SD-WAN environments.
4.0	In CSO release 4.0, the following third-party virtual network functions (VNFs) are supported: <i>Fortigate-VM</i> and <i>Single-legged Ubuntu VM</i> .
3.3.0	Starting with CSO Release 3.3, two redundant hub devices can be used at one POP to protect against device and link failures, and to provide upstream multihoming for spoke sites.

Your First SD-WAN Deployment

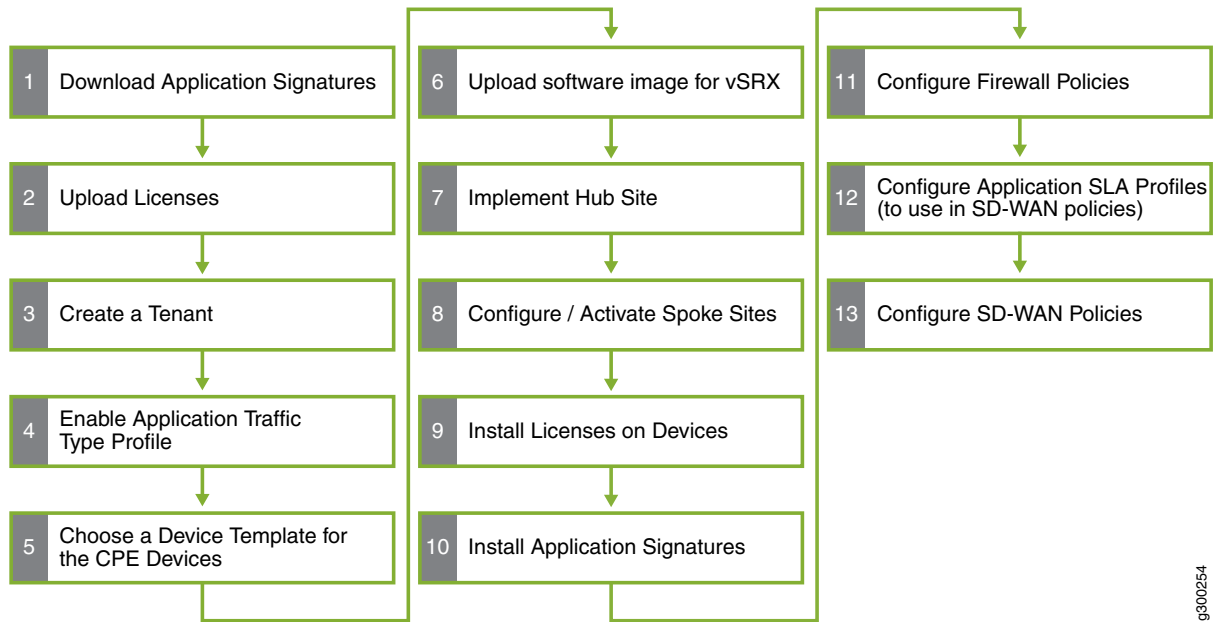
IN THIS SECTION

- Before You Begin | 62
- Download Application Signatures | 63
- Upload Licenses | 64
- Create and Configure a New Tenant | 64
- View Application Traffic Type Profile | 65
- Modify Device Templates | 66
- Upload Software Image for vSRX | 67
- Choose a Point of Presence (POP) for the Hub Site | 68
- Note Your Provider Hub Device | 69
- Create and Configure the Tenant's Hub Site | 69
- Create and Configure a Spoke Site for the Tenant | 70
- Install License on Device | 73
- Install Application Signature | 73
- Add Firewall and NAT Policies to the Topology | 74
- Add SD-WAN SLA-Based Steering Profiles and Policy | 74

This document describes the steps required in order to create your first SD-WAN deployment.

[Figure 32 on page 62](#) shows an overview of the steps that will be covered in this deployment example.

Figure 32: SD-WAN Deployment Workflow



g300254

Before You Begin

- Purchase an Advanced Policy-based Routing license for a vSRX. You must purchase a license that includes the **appid-sig** feature.
- Download the required vSRX KVM appliance software image to your workstation. You can find the URLs for CSO-related software downloads in the [Contrail Service Orchestration Release Notes](#). For CSO Release 5.0.0, the required version for vSRX is **15.1X49-D172** and you can download the image here: [vSRX Software for KVM - Junos OS 15.1X49-D172](#). You'll need this software image to bring up a vSRX VNF on the NFX device later in the deployment.

NOTE: Make note of the physical interfaces that you select for use throughout this deployment example. These interfaces need to be connected to form the underlay networks over which the data and management traffic will travel.

Download Application Signatures

This section details how to download application signatures from Juniper onto your CSO installation. Downloading the signature database makes the application signatures available to install on your CPE device after it has been activated in a later step. These signatures are used for application identification within CSO.

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 an 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 email address as the username and your newly-set password.

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 newest database is at the top of the list.

3. Click the **Full Download** link under the **Actions** column.

A pop-up window appears that shows the progress of the download. You can watch the progress here or dismiss the window by clicking OK. If you dismiss the progress window before the job completes, you can still access the job information by looking in **Monitor > Jobs**. The download job appears at the top of the list.

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 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 using this procedure are available to be pushed to your tenant devices during the ZTP process.

To upload the license for your vSRX gateway router (GWR) device:

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. This brings up a window in which you click the **Browse** button to locate the license file that you purchased for the vSRX.

2. Click the + 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 it 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.

Create and Configure a New Tenant

In this section we use the Administrator Portal to add a tenant to CSO.

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

2. Click the **Add Tenant** button

If there are no tenants created an Add Tenant is displayed on the center of the page. If there are tenants, click the "+" to create 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

- Select the check-boxes next to both **Roles** in the **Available** section and click the arrow link to move them to the **Selected** section
- The password expiration defaults to 180 days.
You can set any value between 1 and 365.
- Click Next

- In the **Deployment Info** window, select the **SD-WAN** icon.

Depending on how your tenant was configured, you may see one or more of the following in addition to the SD-WAN icon: Hybrid WAN, Next Gen Firewall, and LAN. For this example, select only SD-WAN.

This activates the **SD-WAN Mode** section of the window.

- Select the **Realtime Optimized** radio button

Selecting **Bandwidth Optimized** allows for hub-and-spoke deployments. Selecting **Real-time Optimized** allows for dynamic mesh deployments as well as hub-and-spoke.

- Click Next

The window advances to the **Tenant Properties** section. For this example, browse the Tenant properties but do not make any changes

- 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.

The preceding steps show only one of many possible settings that can be used to create an SD-WAN tenant

View Application Traffic Type Profile

You can customize class-of-service and probe parameters with traffic type profiles. Only profiles with the enabled status can be used in policy intents. The CSO SP administrator can enable and disable existing profiles. They can also create new profiles upon request.

Modify Device Templates

In this section, we modify an existing device template so that it works for this example.

1. Navigate to **Resources > Device Templates**

2. Find the device template named **NFX250 as SD-WAN CPE**.

3. Select the check-box next to that template

4. Click the **Clone** button

Since an OpCo administrator cannot

5. Enter a display name and a name for the cloned template

CSO shows the display name in various workflow locations but uses the entered name behind the scenes.

6. Select the check-box next to the cloned template and then select **Template Settings** from the **Edit Device Template** pull-down menu.

A new window titled Template Settings appears

7. In the Template Settings window, ensure that the following things are set:

- **ACTIVATION_CODE_ENABLED: ON**

By requiring an activation code, a CPE device will not be allowed to communicate with CSO until the tenant has activated a site using the activation code. The value of the activation code will be set later in the process.

- **AUTO_DEPLOY_STAGE2_CONFIG: OFF**

Stage 2 configurations are configurations that can be added to a device after the initial, stage 1, provisioning of the device. This setting prevents the automatic deployment of a stage 2 configuration.

- **OOB_MGMT_ENABLED: OFF**

This setting ensures that the **jmgmt0** interface is not enabled on the NFX device. Since this is a managed Internet service and the NFX device will be sitting on the customer's premise, this might be a useful setting to prevent unwanted login by the tenant.

- **USE_SINGLE_SSH_TO_NFX: ON**

Do not change any other settings.

8. Select Save when finished.

9. Find the device template named **SRX as SDWAN Hub** and select the check-box next to its name.

10. Click the **Clone** button

11. Enter a display name and a name for the cloned template

The template name is what is used in CSO when selecting the template for use.

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

13. In the **Template Settings** window that appears, make sure the following options are set:

- ACTIVATION_CODE_ENABLED: **Off**
- ZTP_ENABLED: **Off**
- WAN_0: ge-0/0/3
- WAN_1: ge-0/0/1
- WAN_2: ge-0/0/0
- WAN_3: ge-0/0/2

Leave all the other settings at their default.

14. Click Save when finished.

Upload Software Image for vSRX

The NFX appliance that you are using as a CPE will be in factory-default state. Therefore it will not have any vSRX images to instantiate. During the zero touch provisioning (ZTP) process, the NFX downloads the GWR (vSRX) image from CSO.

To upload a software image:

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

Here you can see the software images that have been uploaded to CSO.

2. Click the + button to create a new image.

The **Upload Image** page that pops up requires that you fill in all of the fields except Description and Supported Platform.

3. Name the image **vsrx-vmdisk-15.1.qcow2**

4. Select **VNF Image** as the image type.
5. Click **Browse** and select the **.qcow2** software image that you downloaded previously.
6. Select **Juniper** as the Vendor.
7. Select **juniper-vsrx** as the Family.
8. Fill in the Major Version Number, Minor Version Number, and Build Number as **15**, **1**, and **X49-D161**, respectively.
9. Click **Upload**. CSO displays a progress window as the file is uploaded.

Choose a Point of Presence (POP) for the Hub Site

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 hub devices that are placed within. The hubs are either data hubs, OAM hubs, or both. SPs often place POPs in their network so that they are geographically close to customer sites.

NOTE: The SP Administrator is the only one with the privileges to create POPs. In a cloud-hosted CSO deployment, the SP Administrator links your tenant with an appropriate POP.

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 onboarding CPE devices.

Note Your Provider Hub Device

A provider hub device resides in a regional POP within the service provider's network or cloud. Provider hub devices can be shared amongst multiple tenants through the use of virtual routing and forwarding (VRF) instances configured on the hub itself.

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

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

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

Create and Configure the Tenant's Hub Site

In this section, we continue in the Customer Portal for your new tenant to create a provider hub site that will connect with the spoke site that we created in the previous section.

A provider hub site is the site on the SP's network at which the provider hub device resides. The provider hub site is associated with a POP.

Ensure that you are on the **Resources > Site Management** page in the Customer Portal of your new tenant.

1. From the **Add** pull-down menu on the **Sites** page, select **Provider Hub Site**

A new window, titled **Add Provider Hub for <tenant-name>**, appears.

2. Fill in the information requested in this window as follows:

- In the **Configuration** section, select the **POP** and **Hub Device Name**

The POP must exist and the hub device must be activated for it to show up in the list. The POP and Hub device are provided by the SP Administrator. In the case of cloud-hosted CSO, this is Juniper Networks.

3. Click **OK** when finished

Create and Configure a Spoke Site for the Tenant

In this section, we continue in the Customer Portal for the newly configured tenant in order to create an On-Premise Spoke site.

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 just created

This will take you to the Customer Portal for that tenant. The **Dashboard** is displayed

2. Select **Resources > Site Management** link from the left-nav bar

3. In the **Site Management** window that appears, click the **Add On-premise Spoke Site**

A new window titled **Add On-Premise Spoke Site for Tenant** appears.

4. Fill out the information in the **Site Information** section.

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, choose the appropriate **Provider Hub** from the pull-down menu.

7. Click Next

This brings up the **WAN** section.

8. Next to **Device Series**, select **NFX 250** from the pull-down menu.

A horizontal list of device template boxes applicable to the NFX250 series devices appears.

9. Click the left (<) or right (>) arrow until you see the **NFX250 as SD-WAN CPE** box. Click on that box.

10. In the **Device Information** section:

- Fill in the Serial Number for the NFX250 device
- Leave **Auto Activate** selected
- For the **Boot Image**, select the NFX series software image that you previously uploaded to CSO.

The **Boot Image** tells CSO whether to update the device with a software image from the image management system or to use the image that exists on the device.

11. In the **WAN Links** section, select the **Enable** button next to **Wan_0**

Fill in the following

- Link Type: **MPLS**
- Access Type: **Ethernet**
- Egress Bandwidth: **1000** Mbps
- Click the > button next to **Advanced Settings** and fill in the following information:
- Provider: **MPLS-Service-Provider**

This can be any provider name, but it is a required field.

- Cost/Month: **1000**

Use a realistic value for this cost per month. This number is used in SD-WAN link-switch calculations.

- Local Breakout: Off

For this example, leave the other settings at their default.

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

Fill in the following

- Type: **Internet**
- Access Type: **Ethernet**
- Egress Bandwidth: **25** Mbps

Use the appropriate bandwidth number for your network. 25 is simply an example.

- Click the > button next to **Advanced Settings** and fill in the following information:
- Provider: **Internet-Service-ProviderA**

This can be any provider name, but is a required field.

- Cost/Month: **100**

Use a realistic value for this cost per month. This number is used in SD-WAN link-switch calculations.

- Local Breakout: Off

For this example, leave the other settings at their default.

13. Click Next when finished

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

14. (Optional) Click the Add LAN Segment button

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

Fill in the following information in this window:

- Name: **LAN2**

This can be any name that makes sense in your deployment.

- VLAN ID: <Leave blank>

Enter a VLAN ID if required at the remote site. For this example, leave VLAN ID blank.

- Department: <Leave as Default>

In CSO, spoke site departments equate to security zones on the GWR. 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 GWR.

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: 10.0.2.1/24

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

- DHCP: Off

The NFX250 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 **check-box** next to it.
- Click the -> button to move **LAN_2 (ge-0/0/2)** from the available list to the selected list

15. Click Save when finished

The **Add LAN Segment** window closes

16. Click Next

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

17. Review the **Summary** section

18. Click **OK** when you're finished reviewing

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

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.

Install License on Device

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

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

In the pop-up window that appears,

2. Click the check box 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 **check box** next to your tenant site to push the license to the CPE device at that site.

Install Application Signature

This step allowsthe 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 **check box** next to the NFX250 device
4. Click **OK**

Add Firewall and NAT Policies to the Topology

In this section, we use the Customer Portal for your new tenant and create an intent-based firewall policy that blocks **icmp-ping** traffic.

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

This brings up the **Firewall Policy** page. Here you can see a list of policies. You will see the **Default_FW_Policy** which has 1 intent associated with it.

2. (Optional) Click the **Default_FW_Policy** link.

The page changes to show the intents associated with this firewall policy. You can see that the policy allows any traffic originating from any address in the trust zone to any address in the untrust zone. To get back to the list of firewall policies, navigate to **Configuration > Firewall > Firewall Policy**

3. Click the **Check-box** next to **Default_FW_Policy**

4. 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.

5. Click **Deploy**

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

The policy can be implemented at any time for any device within this tenant that works with zone-based firewall policies.

Add SD-WAN SLA-Based Steering Profiles and Policy

In this section, we use the Customer Portal to select an Path-Based Steering Profile and apply it to the SD-WAN Policy to specify that Microsoft Outlook traffic should pass over the WAN_0 overlay link rather than the default link, WAN_1.

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

2. Click the **+** 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: **INTERNET**
- Path Preference: **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**

This causes the window to close. The new policy shows 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 **+** at the upper right part of the list to create a new policy

This brings up a policy builder with the **Source** section activated.

The Source defaults to **All Sites**.

The Application section defaults to **Any**.

Leave the source field at its default.

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

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.

Release History Table

Release	Description
5.0.2	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 .

4

CHAPTER

Hybrid WAN Deployment (uCPE)

Hybrid WAN (Distributed) Deployment Overview | 78

Hybrid WAN (Distributed) Deployment Architecture | 79

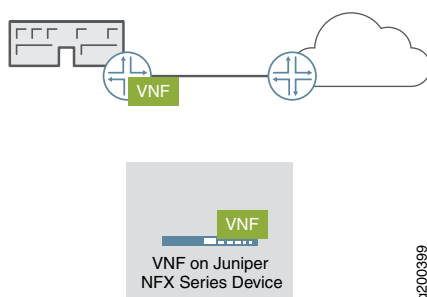
Your First Hybrid WAN (Distributed) Deployment | 81

Hybrid WAN (Distributed) Deployment Overview

This walkthrough highlights the steps, or workflows, that you need to complete in order to deploy a Hybrid WAN solution. We use an NFX250 Series device as the CPE and an SRX Series device as the Hub which is located 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 at each step. It assumes that this is the first deployment you are attempting.

In the distributed deployment, customers access network services from a CPE device located at the customer's site. These sites are called on-premise sites in this documentation. In the deployment workflows used in the CSO GUI, this deployment is known as Hybrid WAN. [Figure 33 on page 78](#) illustrates a simplified distributed deployment.

Figure 33: Simplified Hybrid WAN Deployment



Initial configuration of the CPE device at the site is automated through the use of zero touch provisioning (ZTP) that is orchestrated through CSO. CSO also monitors the CPE device and its services, and can push software and configuration updates to the devices remotely, reducing operating expenses.

This deployment model is useful in environments where service delivery from the service provider's cloud is costly. In fact, CSO has been designed to require only modest bandwidth, needing as little as 30kbps for probe and OAM traffic over Hybrid WAN connections where there are only a few sessions active. When AppQoe is involved, the bandwidth requirement increases to somewhere between 105kbps and 2Mbps, depending on the number of sessions.

During ZTP operations, if new device images are needed, they can be downloaded as part of the ZTP process, or pre-staged on the device. In those circumstances, the bandwidth requirement increases to a maximum of 5Mbps only when device image download is needed. This makes these solutions applicable even in cases where connection bandwidth is limited or noisy.

The Hybrid WAN deployment uses a CPE device such as an NFX Series Network Services platform or SRX Series Services Gateway at the customer site and thus supports private hosting of network services at a site. The Hybrid WAN deployment can be extended to offer software defined wide area networking (SD-WAN) capabilities.

NOTE: If an SRX Series device is used as the CPE device at the customer site, it can not host VNFs. It can still offer all of the built-in services inherent in an SRX Series device.

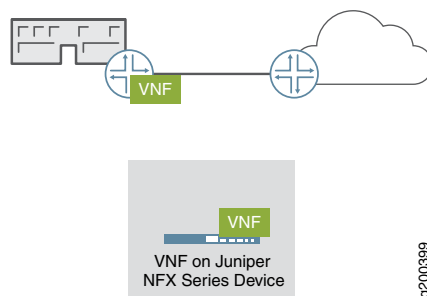
In the Hybrid WAN deployment model, there is typically only one path from the on-premise site back to headquarters or the service provider cloud. The following sections describe the high-level architecture of a Hybrid WAN deployment and provide a walkthrough of how to set up CSO for Hybrid WAN.

Hybrid WAN (Distributed) Deployment Architecture

In the Hybrid WAN deployment the Contrail Services Orchestration (CSO) software resides in the service provider's cloud, and is operated by the service provider in order to provide network services, hosted on CPE devices, at customer sites.

Figure 34 on page 79 shows a simple diagram of the Hybrid WAN solution. The cloud represents the service provider network to which the customer site is connected.

Figure 34: Hybrid WAN Solution



As mentioned previously, the Hybrid WAN deployment makes use of on-premise CPE devices in order to localize the delivery of network services and provide gateway router (GWR) functionality. In this case, the Juniper Networks NFX Series or SRX Series devices act as the CPE devices.

In the case of NFX as CPE, the GWR function is provided by a built-in vSRX VNF and network services are hosted and provided from within the NFX that is located at the customer site. This makes the network services extremely responsive from the point of view of the customer LAN, while negating the need for customer traffic to traverse the WAN in order to access the services.

In the case of an SRX Series device as the managed CPE device, only services native to the SRX— firewall, NAT, and UTM, can be provisioned and managed at the customer site by CSO. Other services, such as

WAN optimization must be provisioned and managed separately from the SRX and cannot be managed by CSO.

In addition to the CPE devices, the Hybrid WAN solution also makes use of a provider edge (PE) router in the service provider cloud. The PE router terminates IPsec tunnels and provides policy-based access to the service provider's MPLS network. The PE and CPE devices communicate over one or more WAN links and make use of MPLS/GRE or IPsec tunnels for secure transport. Supported device types for a Hybrid WAN deployment are shown in while the device roles and required software versions are shown in [Table 9 on page 80](#).

Table 9: Hardware and Software Matrix for CPE Devices in a Hybrid WAN Deployment

Role	Platform	Models Supported	Junos OS Software Release Version
PE Router and IPsec Concentrator (Hybrid WAN deployment only)	MX Series 3D Universal Edge Router	<ul style="list-style-type: none"> MX960, MX480, or MX240 router with a Multiservices MPC line card MX80 or MX104 router with Multiservices MIC line card Other MX Series routers with a Multiservices MPC or Multiservices MIC line card <p>See MPCs Supported by MX Series Routers and MICs Supported by MX Series Routers for information about MX Series routers that support Multiservices MPC and MIC line cards.</p>	Junos OS Release 16.1R3.00
CPE device	<ul style="list-style-type: none"> NFX Series Network Services Platforms SRX Series devices vSRX on an x86 server 	<ul style="list-style-type: none"> NFX250-LS1 device NFX250-S1 device NFX250-S2 device NFX150-S1 device NFX150-S1E device NFX150-C-S1 device NFX150-C-S1-AE/AA device NFX150-C-S1E-AE/AA device SRX300 SRX320 SRX340 SRX345 SRX4100 SRX4200 vSRX 	<p><i>For NFX250:</i> Junos OS Release 15.1X53-D496</p> <p><i>For NFX150:</i> Junos OS Release 18.3X85-D11</p> <p><i>For SRX Series:</i> Junos OS Release 15.1X49-D172</p> <p><i>For vSRX:</i> Junos OS Release 15.1X49-D172</p>

Selection of services, and some service management capabilities can be allocated to the customer by the service provider using the CSO Administration Portal. The customer would then access the allowed services and management capabilities by using the Customer Portal.

CSO manages the lifecycle of the VNFs hosted on the NFX CPE devices from creation in Network Designer, through instantiation, deployment, and finally through replacement or retirement.

NOTE: Designer tools such as Network Designer are only available for on-premise deployments of CSO.

Your First Hybrid WAN (Distributed) Deployment

IN THIS SECTION

- [Modify Device Templates | 81](#)
- [Add and Configure a New Tenant | 82](#)
- [Add and Configure a Site for the Tenant | 83](#)

Modify Device Templates

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 an 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.

In this section, we modify an existing device template so that it works for this example.

1. Enter the login credentials for the Administration Portal.
2. Navigate to **Resources > Device Templates**
3. Find the device template named **NFX250 as Managed Internet CPE**.

4. Select the check-box next to the template and then select **Template Settings** from the **Edit Device Template** pull-down menu.

A new window titled Template Settings appears

5. In the Template Settings window, ensure that the following things are set:

- **ACTIVATION_CODE_ENABLED: ON**

By requiring an activation code, a CPE device will not be allowed to communicate with CSO until the tenant has activated a site using the activation code. The value of the activation code will be set later in the process.

- **AUTO_DEPLOY_STAGE2_CONFIG: OFF**

Stage 2 configurations are configurations that can be added to a device after the initial, stage 1, provisioning of the device. This setting prevents the automatic deployment of a stage 2 configuration.

- **OOB_MGMT_ENABLED: OFF**

This setting ensures that the **jmgmt0** interface is not enabled on the NFX device. Since this is a managed Internet service and the NFX device will be sitting on the customer's premise, this might be a useful setting to prevent unwanted login by the tenant.

- **WAN_Oge-0/0/11**

Do not change any other settings.

6. Select Save when finished.

Add and Configure a New Tenant

In this section we use the Administrator Portal to add a tenant to CSO.

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

2. Click the **Add Tenant** button

If there are no tenants created yet, 'Add Tenant' will be a button. If there are tenants, click the "+" to create 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

- Select the check-boxes next to both **Roles** in the **Available** section and click the arrow link to move them to the **Selected** section
- The password expiry defaults to 180 days
You can set any value from 1 to 365 days.
- Click Next
- In the **Deployment Info** window, select the **Hybrid WAN** icon
- Click Next
The window advances to the **Tenant Properties** section. For this example, browse the Tenant properties but do not make any changes
- 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.

Add and Configure a Site for the Tenant

In this section, we move to the Customer Portal for the newly configured tenant in order to create a site.

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 just created

This will take you to the Customer Portal for that tenant. The **Dashboard** is displayed

2. Select **Resources > Site Management** link from the left-nav bar

3. In the **Sites** window that appears, click the **Add On-Premise Spoke (Manual)**

A new window titled **Add On-Premise Spoke Site for <Tenant>** appears.

4. Fill out the information in the **Site Information** section.

Enter a site name that makes sense, like: **site1**

If you fill in the address information, CSO will use it to display the site on maps on some of the monitoring pages.

5. Click Next

This brings up the **WAN** section.

6. Under **Device Template**, select the **NFX250** from the **Device Series** pull-down menu.

This displays the device templates for NFX250 Series devices.

7. Select **NFX250 as Managed Internet CPE**

8. Fill out the information In the **Device Information** section

9. Disable **Auto Activate**

This enables the **Activation Code** field.

NOTE: If you leave **Auto Activate** enabled, CSO will attempt to connect with the device as soon as the site configuration is complete.

10. Enter an activation code for the NFX250.

This code must be entered when the device is powered-on for the first time in its final location.

NOTE: You cannot modify any settings for the WAN_0 interface because there are strict requirements for this device template that the WAN_0 must be an Internet-facing interface.

11. Click Next when finished

The window advances to the **Summary**

12. Review the **Summary** section

13. Click **OK** when you're finished reviewing

You will see pop-up messages appear for site-creation job start and site-creation job finished.

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.

5

CHAPTER

Standalone Next-Generation Firewall (NGFW) Deployment

Next-Generation Firewall (NGFW) Deployment | 86

Next-Generation Firewall (NGFW) Deployment

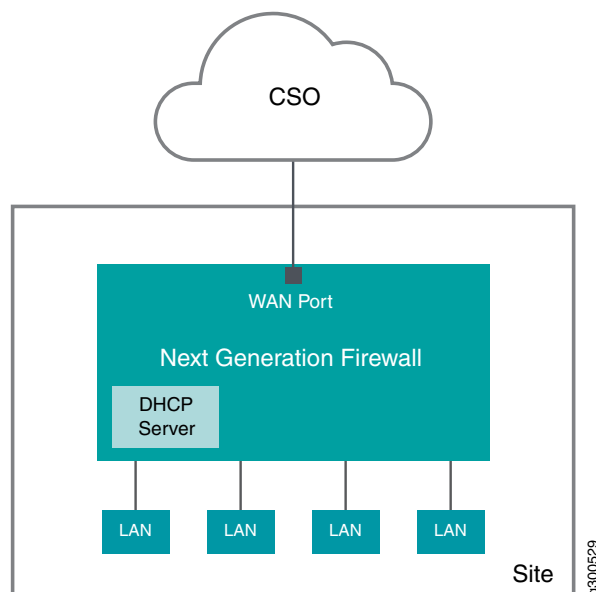
IN THIS SECTION

- [NGFW Deployment Overview | 86](#)
- [NGFW Deployment Architecture | 87](#)
- [NGFW Deployment | 87](#)

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 and Hybrid 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 35 on page 86](#).

Figure 35: 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 stand alone firewall deployment as shown in [Figure 35 on page 86](#). 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.

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 [Creating a Single Tenant](#) as appropriate.

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-nav bar 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 > 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 > 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 36 on page 90](#)

Figure 36: NGFW Add Site Summary

Add On-Premise Spoke Site for JNPR_IX

General Add LAN Summary

General Information [Edit](#)

Site Name	NGFW Site
Site Type	SPoke
Home Server	0.0.0.0/0.0.0.0
NTP Server	time.google.com
WAN Capability	STANDALONE
LAN Capability	N/A
Street Address	NONE
City	NONE
State/Province	NONE
ZIP/Postal Code	NONE
Country	US
Contact Name	NONE
Email Address	NONE
Phone Number	NONE

WAN Information [Edit](#)

WAN Device Template	NAC_Security_Policy_Signed_ZTP
In-Band Management Port	gi0/0/1
Firewall Policy	Default_NGFW_Policy
NAT Policy	Default_NGFW_Policy

Cancel Back OK

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.

- 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**.

- 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.

- 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.

6

CHAPTER

LAN Deployment

SD-LAN with EX Switch | 93

SD-LAN with EX Switch

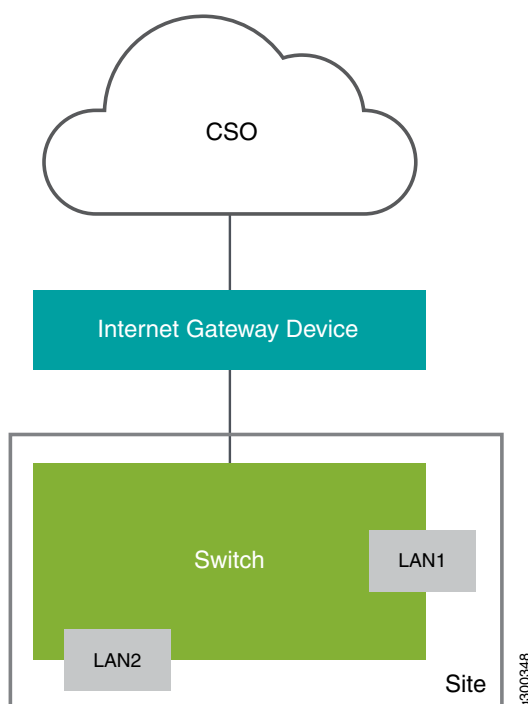
IN THIS SECTION

- LAN Deployment Overview | 93
- SD-LAN Deployment | 94

LAN Deployment Overview

The SD-LAN deployment focuses on spoke site LAN connectivity using specific EX Series switches and Virtual Chassis (VC). Once deployed, you can manage the connected spoke site LANs through the EX switch or VC. You can also manage many aspects of the EX switch or VC itself. [Figure 35 on page 86](#) shows a high-level view of an SD-LAN spoke site. It is important to note the Internet Gateway Device depicted in the diagram. The LAN switch at a spoke site must be deployed behind a router or CPE that is capable of routing traffic to CSO.

Figure 37: SD-LAN Spoke Site



In addition to the SD-LAN deployment shown above, you can deploy EX Series access switches behind existing CPE devices that act as the routers to allow the switch to communicate with CSO. You can deploy EX Series LAN switches and VCs behind SRX Series and NFX250 Series CPE devices. You cannot deploy an EX Series LAN switch or VC behind an NFX150 Series CPE device.

An SD-LAN deployment is performed in the Customer Portal of CSO as an on-premise 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.

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 you are deploying a Virtual Chassis (VC) as the LAN switching device, the VC must be up and running prior to beginning this procedure. You must have the serial number of the primary switch in the VC.

If any of these things are not true, see [Accessing Administration Portal](#), [Accessing Customer Portal](#), or [Creating a Single Tenant](#) as appropriate.

The steps to deploy an SD-LAN 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-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**

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 > 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 > 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, enter the **Serial Number** of the switch 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 off by default. Turn it on if the switch is upgraded to a Junos OS image version with support for Phone-Home-Client. If ZTP is disabled, you must manually copy and paste the Stage-1 configuration (by using CLI) on to the switch.

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

16. (Optional) Enter LAN information for the branch/spoke 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 +

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. Select the switch ports to which the LAN segment is connected by clicking the **Check-box** next to the port name and then clicking the right-arrow (->) between the **Available** and **Selected** lists.

Alternatively, you can select the **Check-box** for the desired port and then click the right-arrow (->) directly to the right of the port name.

- e. 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.

If you turned off auto-activate, then your site appears in the list with a status of **Configured**. Go to next step.

(Optional) If you turned off auto-activate, and 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. After that, 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 or VC through the Customer Portal's Switch Port Operational View.

7

CHAPTER

Appendix A - Network Function Virtualization in Contrail Service Orchestration

Network Function Virtualization in the Contrail Service Orchestration
Deployments | **100**

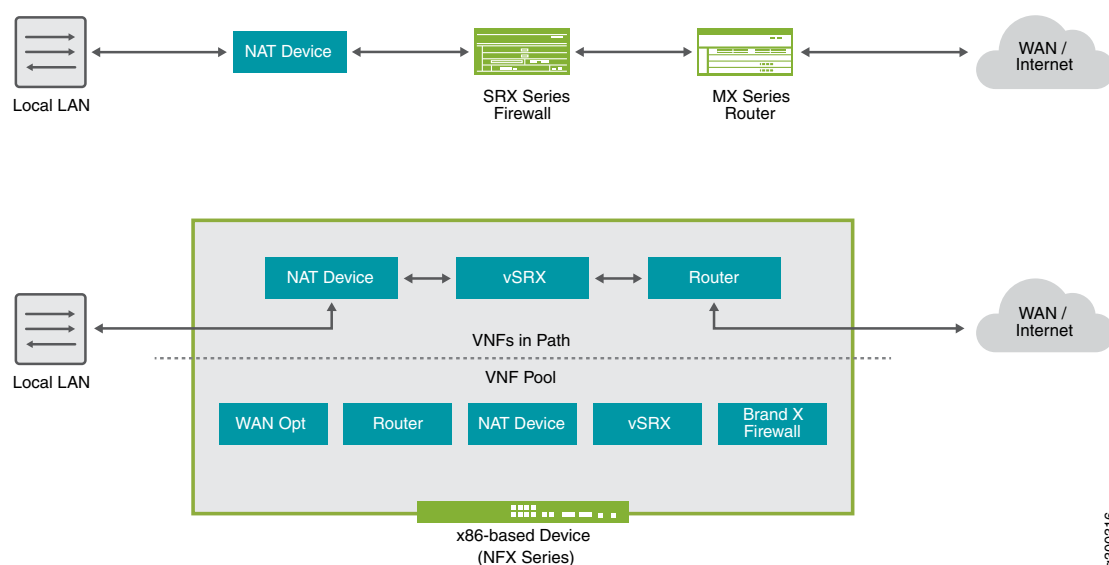
Number of Sites and VNFs Supported in Contrail Service Orchestration | **102**

VNFs Supported by the Contrail Service Orchestration Solutions | **103**

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 38 on page 100](#) 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 38: 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 the Hybrid WAN and SD-WAN deployments:
 - Network Service Orchestrator, together with Network Service Controller, provides ETSI-compliant management of the life cycle of network service instances.
 - Network Service Controller provides service-chaining and the VIM.

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

Other CSO components connect to 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: Designer Tools are only available in on-premise 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.

Number of Sites and VNFs Supported in Contrail Service Orchestration

Cloud-hosted CSO 5.0 supports up to 6000 sites and 2 VNFs for a Hybrid WAN deployment and up to 6000 sites for a Hub and Spoke SD-WAN deployment.

An on-premise CSO deployment supports three environment types: small, medium, and large. The small environment does not include any high availability features for the CSO platform itself, while medium and large deployments do support HA for the CSO platform. [Table 10 on page 102](#) shows the number of sites and VNFs supported for each environment.

Table 10: Number of Sites and VNFs Supported

Deployment Type	Number of VNFs Supported for a Centralized Deployment	Number of Sites and VNFs Supported for a Distributed Deployment	Number of Sites Supported for a Hub and Spoke SD-WAN Deployment
Small	10 VNFs	Up to 500, 2 VNFs per site	Up to 500
Medium	100 VNFs, 20 VNFs per Contrail compute node	Up to 3500, 2 VNFs per site	Up to 3500
Large	500 VNFs, 20 VNFs per Contrail compute node	Up to 6000, 2 VNFs per site	Up to 6000

Each environment has different requirements for:

- The number and specification of node servers and servers. See *Minimum Requirements for Servers and VMs*
- The number and specification of virtual machines (VMs). *Provisioning VMs on Contrail Service Orchestration Nodes or Servers*

NOTE: For a cloud-hosted CSO deployment all of the node server and VM details are handled by Juniper Networks. The links above point to CSO 4.1 on-premise installation information.

VNFs Supported by the Contrail Service Orchestration Solutions

Contrail Service Orchestration (CSO) supports Juniper Networks and third-party VNFs listed in [Table 11 on page 103](#).

Table 11: VNFs Supported by Contrail Service Orchestration

VNF Name	Version	Network Functions Supported	Deployment Model Support
Juniper Networks vSRX	vSRX KVM Appliance 15.1X49-D123	<ul style="list-style-type: none"> • Network Address Translation (NAT) • Demonstration version of Deep Packet Inspection (DPI) • Firewall • Unified threat management (UTM) 	Hybrid WAN and SD-WAN deployments supports NAT, firewall, and UTM.
Fortinet	5.6.3	Firewall	Hybrid WAN and SD-WAN deployments—NFX250 and NFX150 platforms.
Single-legged Ubuntu	16.04	Firewall	Hybrid WAN and SD-WAN deployments—NFX250 and NFX150 platforms.

An on-premise 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 (L2) service chains while Hybrid WAN deployments can support L2 and L3 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.

8

CHAPTER

Appendix B - Manual Staging of NFX

[Install Junos Software onto NFX from USB Port | 105](#)

Install Junos Software onto NFX from USB Port

This section details how to install Junos OS software version 15.1X53-D496.0 onto an NFX250 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. This procedure is for an NFX250 device.

Before You Begin

In order for this procedure to succeed, you must have the following

- Physical access to the USB port of the NFX device
- A USB drive of at least 4GB containing the Junos OS Software image, 15.1X53-D496.0, inserted into the USB port of the NFX
- Access to the console port of the NFX 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 NFX250. This DHCP server must be able to provide IP address, name server, and default gateway to the NFX upon request.

The following procedures contain comments that are added to clarify the steps that are discussed.

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

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

2. Access the NFX 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 device.

4. Power on the NFX 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 will install 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 is made up of multiple components that load and boot in a specific order. See [NFX 250 Overview](#) for details. The PFE of the NFX may take a few minutes to complete the boot and allow the **jsxe0** interface to obtain its address from DHCP.

You can login to the console of the NFX as **root** 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 for different purposes. You are looking 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) in order 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

[Building Blocks Used for Contrail Service Orchestration Deployments | 18](#)

[Hybrid WAN \(Distributed\) Deployment Overview | 78](#)

[SD-WAN Deployment Overview | 40](#)