JUNIPER NETWORKS | Engineering Simplicity

Contrail Service Orchestration

CSO SD-WAN – Design and Architecture Guide

Published
2025-11-03

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

Contrail Service Orchestration CSO SD-WAN – Design and Architecture Guide

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide

Use this guide to understand the components and capabilities of Juniper Networks SD-WAN and NGFW solutions within the Contrail Service Orchestration platform.

1
CHAPTER

About this Guide

IN THIS CHAPTER

Coverage and Audience

This guide discusses design and architecture elements for Juniper's SD-WAN and NGFW solutions within Juniper's Contrail Service Orchestration (CSO) software. The guide covers features and functionality up to and including CSO Release 5.4.0.

This guide is appropriate for network designers, planners, and architects, as well as network engineers and administrators who need to understand the solution at a higher level.

CSO Terminology

Table 1 on page 2 provides definitions for the terminology used throughout this guide.

Table 1: CSO Terminology

Term	Definition
Branch	A tenant site, connected to other sites in either a full mesh or hub-and-spoke topology. Also known as a *spoke site*.
CPE	Customer-premises equipment—A device placed at a remote customer spoke site that provides services (such as WAN routing or firewall filtering) for the remote site. The CPE allows the remote site to connect with a hub or other spoke sites. Legacy CPE devices provide single services, newer CPE devices (such as the NFX Series and SRX Series Firewalls) provide multiple services to enable the SD-WAN and NGFW solutions. See also *on-premises spoke device*.
CSO	Contrail Service Orchestration—A Juniper Networks software product that facilitates the Contrail SD-WAN and NGFW solutions. You access CSO through a graphical user interface (GUI) to harness its built-in automation capabilities, which enable you to provision, manage, and monitor your WAN, campus, and branch networks.
Dynamic Mesh	A resource conserving method for implementing full-mesh topologies. All of the sites in the full mesh are included in the topology; but the site-to-site VPNs are not brought up until traffic crosses a user-defined threshold called the Dynamic VPN threshold.

Table 1: CSO Terminology *(Continued)*

Term	Definition
Enterprise Hub	A single-tenant on-premises spoke device deployed as a hub at an enterprise hub site. The enterprise hub can serve as the hub portion of a hub-and-spoke topology. When deployed like this, the provider hub (if any) serves as a backup hub to the enterprise hub for site-to-site communications.
Enterprise Hub Site	A special type of spoke site with enhanced capabilities that approximate those of a provider hub site.
Hub Site	A site that acts as a hub for traffic from multiple spokes in a hub-and-spoke topology. In the absence of an enterprise hub, all spoke-to-spoke traffic flows through the provider hub. See also *Provider Hub* and *Enterprise Hub*.
MANO	Management and Orchestration
Mesh Tag	A text-based label for WAN interfaces on CPE devices. Mesh tags enable SLA-based dynamic VPN creation between customer sites. Only interfaces with matching mesh tags can form a VPN.
Microservices	Lightweight, modular building blocks that implement a specific function and communicate with other functions using well defined interfaces (e.g. RESTFul APIs). Can be scaled independently.
MP-BGP	Multiprotocol BGP—A routing protocol used for large-scale, multi-tenancy deployments
NGFW	Next-generation firewall—An SRX Series Services Gateway placed at a remote customer site that acts as a CPE and provides WAN and advanced security services.
NSC	Network Service Controller—The SD-WAN controller layer of CSO, provides topology and CPE lifecycle management functionality, as well as site-to-site routing and reachability.
On-premises spoke device	See *CPE*.

Table 1: CSO Terminology *(Continued)*

Term	Definition
OpCo	Operating Company—Typically a service provider who has multiple large tenants. A single instance of CSO can have multiple OpCos, each with multiple tenants. **NOTE**: An OpCo administrator is the highest level of administrator available for CSOaaS.
PNF	Physical Network Function—Network service provided by a physical device, such as firewall services provided by an SRX Series Services Gateway.
POP	Point of Presence—Typically a physical location where the provider has assets used to deploy one or more of the available solutions. Assets are network devices such as edge routers, provider hubs, and server resources. The POP can also be a data center where the provider can deploy CSO.
Provider Hub	A multitenant hub device located in a POP on the service provider's network. A provider hub can terminate IPsec tunnels for both overlay and secure OAM networks. Provider hub devices can also terminate MPLSoGRE and MPLSoGREoIPsec tunnels. Only an SP administrator or OpCo administrator can add, modify, or delete provider hub devices. **NOTE**: For CSOaaS, an OpCo administrator can add only DATA_ONLY hubs.
SD-WAN	Software-defined wide area network—Uses CSO to provision, manage, and monitor on-premises spoke devices, provider hubs, and enterprise hubs located across a WAN environment. Typically includes the use of NFX Series Network Services Platforms and SRX Series Firewalls.
Secure OAM	Juniper Networks security-focused implementation of operations, administration, and management (OAM) functions within CSO.
Site	Any customer location, such as an on-premises spoke, an enterprise hub, or cloud spoke.
Spoke	A tenant branch site in a hub-and-spoke topology.
Tenant	Typically an enterprise customer with many branches (sites) who subscribes to the offerings provided by the service provider. Sites are provisioned within a tenant. One tenant cannot see the sites or assets of another.

Table 1: CSO Terminology *(Continued)*

Term	Definition
VNF	Virtualized Network Function—Network service provided by software running in a virtual environment, such as the vSRX Virtual Firewall virtual firewall.
ZTP	Zero touch provisioning, also known as autoinstallation.

References

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

- Contrail Service Orchestration Deployment Guide
- Contrail Service Orchestration Installation and Upgrade Guide
- Contrail Service Orchestration Administration Portal User Guide
- Contrail Service Orchestration Customer Portal User Guide
- Contrail Service Orchestration Monitoring and Troubleshooting Guide
- and more

CHAPTER 2

Introduction

IN THIS CHAPTER

Contrail Service Orchestration

IN THIS SECTION

Contrail Service Orchestration (CSO) is an SD-WAN orchestration and management platform that uses automation and virtualization to connect sites together across the wide area, including local breakout where desired. CSO works with SRX Series and NFX Series devices to provide an agile, software-defined approach to site connectivity, supporting both hub-and-spoke and dynamic mesh architectures.

User traffic is routed across logical overlay networks that sit on the physical underlay infrastructure. As long as the remote WAN-facing devices have underlay connectivity, configuring or changing overlay WAN connectivity is as simple as pushing new configuration to the remote devices.

Managed service providers can use CSO to provide WAN connectivity solutions to their enterprise customers. Individual enterprises can use CSO to configure WAN connectivity for their own sites as well as manage and monitor application SLAs with intent-based policies.

CSO is available as a software-as-a-service (SaaS) and as a downloadable on-premises installation:

- **CSO-as-a-Service (CSOaaS)** — A Juniper–provided SaaS installation in AWS. Juniper's highly scalable CSO installation in AWS is available for customers to use by subscription. Juniper provides subscribers with access to a portal where they can log in to CSO to manage their own networks. Managed service providers and individual enterprises subscribe to this cloud-based service.
- **CSO On-Premises** — A software package that you purchase once and install on your own compute infrastructure. Managed service providers and large enterprises who want complete control over their installation choose this option.

NOTE: If you are a managed service provider who wants both the convenience of a CSOaaS solution and the control of a CSO on-premises installation (possibly due to regulatory or compliance requirements), contact Juniper Networks to learn more about a dedicated CSOaaS product.

CSOaaS reduces the complexity and overhead involved in managing the servers, virtual machines, and orchestration and management infrastructures needed to run CSO. As shown in Figure 1 on page 8, Juniper Networks is responsible for the CSO installation and all of the back-end CSO infrastructure.

Managed service providers subscribe to CSOaaS and provide their enterprise customers with an SD-WAN service. Individual enterprises subscribe to CSOaaS to use SD-WAN to manage their own network connectivity.

Figure 1: CSO-as-a-Service

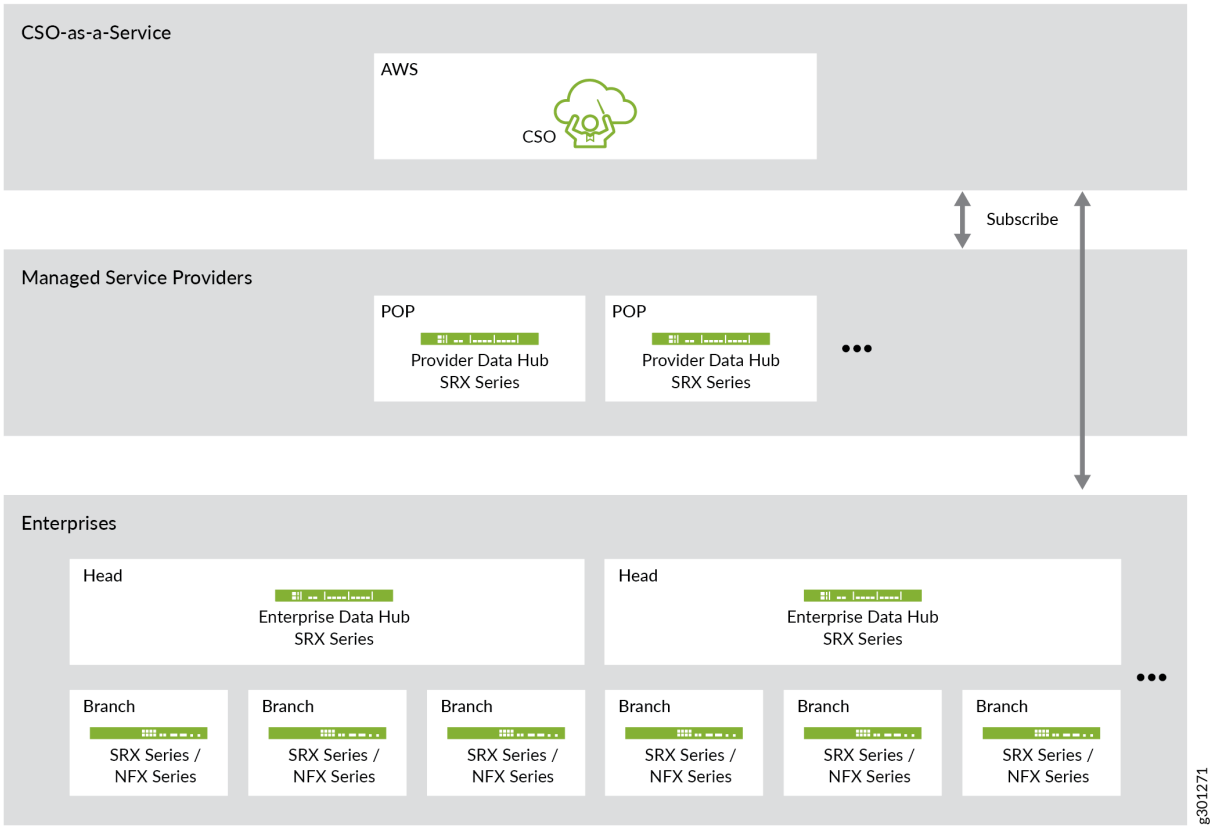
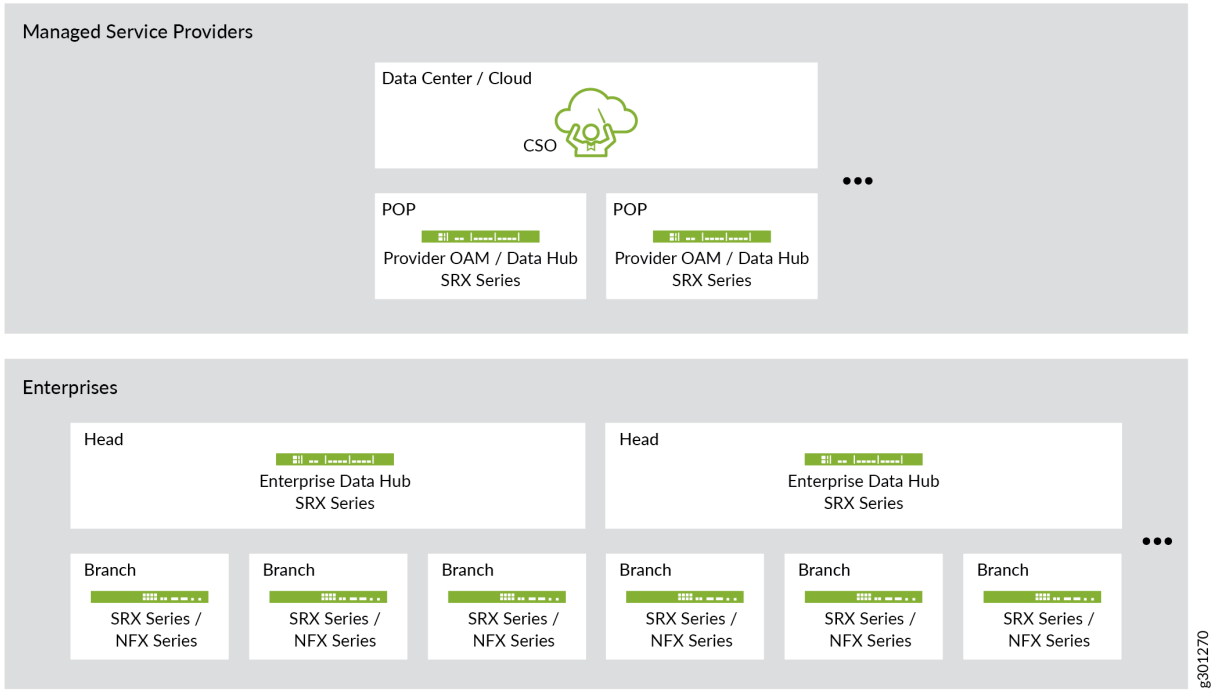


Figure 2 on page 9 shows CSO in an on-premises deployment. The managed service provider who installs and deploys CSO has full control and responsibility for the entirety of the CSO deployment.

Figure 2: CSO On-Premises



In both cases, managed service providers supply their own POP infrastructure including the provider data hub devices that break out customer traffic to the provider network. For the CSO on-premises installation, the managed service provider additionally supplies the provider OAM hub that terminates secure OAM connections from remote sites and forwards the tunneled OAM traffic to CSO. A single SRX Series Firewall can simultaneously support the provider data hub and provider OAM hub roles.

Here are the highlights of the CSO solution:

- End-to-end management and orchestration – Feature rich, horizontally scalable, easy-to-use, microservices-based orchestration platform
- Integrated Security – Full security suite with NGFW, Content Security, and more, with all traffic in encrypted tunnels
- Single Orchestrator – CPE zero touch provisioning, VNF and PNF deployment, managed security, SD-WAN services
- Adherence to open standards – Not book-ended, easily interoperable with existing service provider and enterprise infrastructure and third-party CPEs through open APIs and protocols, with software deployable on public as well as private clouds
- Full routing and MPLS stacks – Support for BGP/OSPF/IS-IS/MPLS/VRRP, etc. on WAN and LAN; scalable architecture with distributed SD-WAN hubs

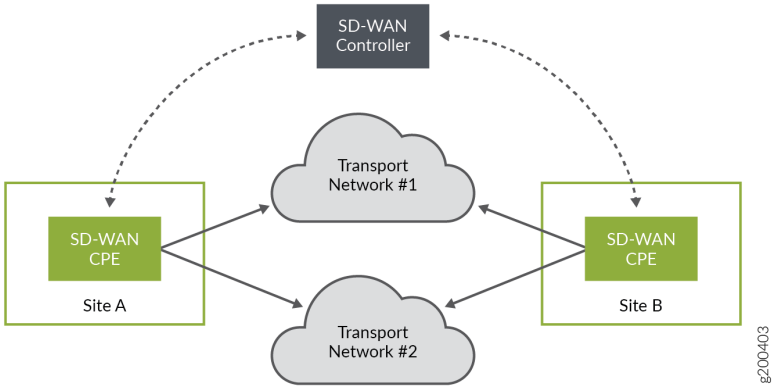
- Carrier grade appliance – Innovative branch device (NFX Series) with service chaining support for 3rd-party VNFs

CSO SD-WAN

CSO provides the automation of Layer 3 connectivity as well as distributed Layer 4 to Layer 7 services. This implementation uses intelligent CPE devices located at branch sites to connect to hub devices as well as other branch sites. Traffic can flow from a branch site to a hub site, between branch sites directly, and break out from a branch or hub site to the Internet.

Figure 3 on page 10 shows a basic SD-WAN model with two sites connected through two different networks, and with the WAN access at both sites controlled by an SD-WAN controller.

Figure 3: SD-WAN



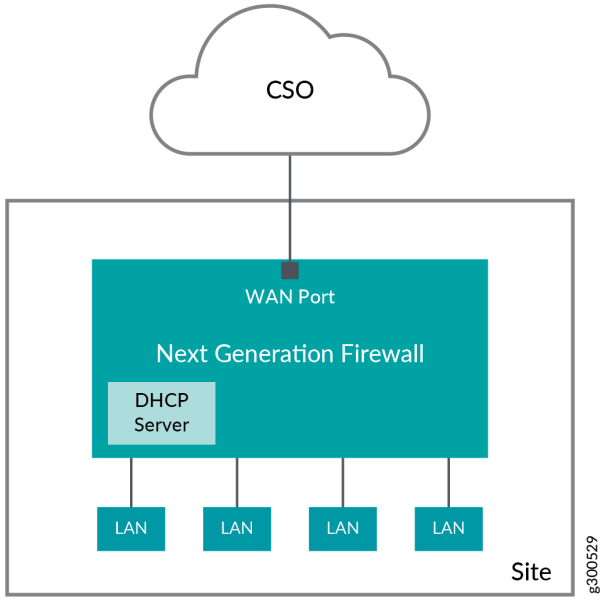
The CSO SD–WAN solution brings SDN–like capabilities to managed service providers and enterprises, offering agility, automation, and rapid automated recovery from failed WAN links, while containing WAN service costs. You can add connectivity options such as broadband or cellular Internet connections to your existing IP/MPLS VPN services, allowing you to prioritize critical traffic across the connections, as well as move traffic proactively to a backup link if the primary link's quality degrades enough to put a service–level agreement (SLA) at risk.

CSO Next Generation Firewall (NGFW)

You can use CSO to deploy a standalone next-generation firewall (NGFW) device at remote branch spoke sites. NGFW deployment provides remote network security through the use of SRX Series

Firewalls as customer-premises equipment (CPE) at a spoke site. This solution offers managed security and LAN visibility to a single location without providing CSO-managed site-to-site connectivity or VNFs, like the CSO SD-WAN solution provides. Figure 4 on page 11 shows a simplified NGFW deployment.

Figure 4: Standalone NGFW



Contrail Service Orchestration Building Blocks

IN THIS SECTION

This section introduces you to some of the main elements and concepts you should understand before using CSO. For a more detailed description of these elements and concepts, see the *Contrail Service Orchestration Administration Portal User Guide* and *Contrail Service Orchestration Customer Portal User Guide* available at https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration.

Administrators

CSO uses a hierarchical, domain-based administration framework. After CSO installation, the first administrator is named *cspadmin* by default. This administrator is also known as the global service provider (SP) administrator. This SP administrator has full read and write access to all of the CSO platform from the global domain. In CSOaaS, the cspadmin role is reserved for Juniper Networks. The SP administrator can create, edit, and delete other administrators and operators who are subject to role-based access controls (RBAC) that assign them privileges to the various objects in CSO.

The next level of administrator is the Operating Company or OpCo administrator. In CSOaaS, the OpCo admin is the highest level of administrator available to managed service provider subscribers. The first administrator for any given OpCo is created by the SP administrator. This user has full administrative privileges within an OpCo domain. In a CSO on-premises installation, an OpCo can be thought of as a region-specific service provider within the global service provider. The OpCo administrator can create other administrators and operators within the OpCo domain and its tenants, but cannot affect elements of the global domain or the domain of other OpCos. Successful login by the OpCo administrator places them into the Administration Portal of their 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 OpCo and tenant operator users. Operator users are created by administrators in their respective domain. By default, operators have read-only access to the elements in their domain.

This is summarized in Table 2 on page 13:

Table 2: Mapping of Users to Portals and Domains

User	Portal	Access	Domain
cspadmin	Administration	read/write	global
OpCo administrator	Administration	read/write	own OpCo domain
OpCo operator	Administration	read only	own OpCo domain
Tenant administrator	Customer	read/write	own Tenant domain
Tenant operator	Customer	read only	own Tenant domain

Domains

Each CSO installation supports a single global domain accessible by the SP administrator. For CSOaaS, this domain is inaccessible to subscribers.

Within the global domain, there can exist multiple OpCo domains. In the CSO on-premises installation, these domains correspond to the regional service providers or to whatever scheme you use to split up administrative responsibilities. A simpler administrative setup may choose to have just a single OpCo domain. For CSOaaS, each OpCo domain corresponds to a single managed service provider subscriber.

Within each OpCo domain are the tenant domains. These are the individual enterprises whose WAN connectivity is being managed. For the CSO on-premises installation, these tenants are the customers of either the regional service provider or the global service provider. For CSOaaS, these tenants can be customers of a managed service provider who subscribes to CSOaaS or the tenants can be direct CSOaaS subscribers themselves.

Portals

CSO provides an Administration Portal for the SP and the OpCos to manage their respective domains, and a Customer Portal for tenants to manage their respective domains. Access to any given portal in any

given domain is controlled by a user's login privileges. If your login does not grant access to the Administration Portal, then you cannot see or access any of the elements of this portal.

Administration portals allow tenant creation and creation of other high-level objects that tenants make use of within the customer portals.

Customer portals provide tenant access to a subset of the objects that exist in administration portals. An OpCo administrator can access the Customer Portal for a tenant by clicking the tenant link on the **Tenants** page in the Administration Portal.

Tenants

CSO uses the tenant element to logically separate one customer from another. An OpCo administrator creates one tenant to represent each customer 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 or OpCo administrator.

Points of Presence (POPs)

A POP is a physical location, usually at the provider network edge, that acts as a demarcation or interchange point between two or more networks. POPs are used in 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.

In CSO, a POP is typically where tenant traffic breaks out of the tenant overlay network into the provider underlay network or Internet. The SP or OpCo administrator is responsible for creating the POP and adding PE routers and provider hub devices to that POP. Once a provider hub device is added, the device becomes available to be selected for use within a tenant network. POPs can be named in whatever way makes the most sense to the SP or OpCo administrator.

Provider Hub

The SP or OpCo administrator adds the provider hub to the POP. The provider hub can have either or both of the following roles:

- OAM - An OAM hub is situated logically between the CPEs and the CSO installation. Its role is to receive OAM traffic from CSO and forward it to the destination CPE devices within secure tunnels. In the other direction, the OAM hub receives OAM traffic from CPE devices within secure tunnels and forwards it to CSO. This role only exists in a CSO on-premises deployment. In CSOaaS, this role is part of the provided service.
- DATA - For tenant traffic staying within the tenant network, the data hub acts as a transit hub for site-to-site traffic. For tenant traffic destined for the provider network, the data hub acts as a demarcation point between the overlay tenant network and the underlay provider network. The provider data hub is optional for tenants that have their own enterprise data hubs. If a tenant has an enterprise data hub as well as an assigned provider data hub, the assigned provider data hub acts as a backup.

After the provider hub is added to the POP, the SP or OpCo administrator can then associate the provider hub site with a tenant.

Sites

Before CSO can build the overlay tenant network, CSO needs to know about all the sites in that network. A site can be a provider hub site, an enterprise hub site, an on-premises spoke site, or a cloud spoke site (Table 3 on page 16).

Table 3: Site Types by Deployment

Available Site Types	Added By	Uses	Service Notes
On-Premises Spoke	The tenant administrator adds the on-premises spoke site.	NFX Series or SRX Series Firewalls placed at branch sites in either a hub–and–spoke or full mesh topology.	An on-premises spoke has the following capabilities: SRX Series • The SRX300 Line of Services Gateways support ADSL and LTE interfaces. • The SRX1500 and SRX300 Line of Services Gateways support PPPoE on WAN Ethernet interfaces. • SRX Series Firewalls deployed as on-premises spoke devices cannot host VNF–based network services. NFX Series • NFX Series devices used as on–premises spoke devices support ADSL, VDSL, and LTE access links, which can also be used for ZTP. The DSL access links allow configuration of PPPoE. Starting with CSO Release 4.0, LTE access links can be used as primary DATA, OAM, or DATA_OAM links. • NFX Series devices support PPPoE on WAN Ethernet interfaces. • Supports local breakout when using a dynamic mesh topology. **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.

Table 3: Site Types by Deployment *(Continued)*

Available Site Types	Added By	Uses	Service Notes
Cloud Spoke	The tenant administrator adds the cloud spoke site.	vSRX Virtual Firewall placed in a tenant's Amazon Web Services (AWS) Virtual Private Cloud (VPC)	A cloud spoke has the following capabilities: • Firewall and Content Security services are available to protect the customer's resources in an AWS VPC. • Connectivity between VPC resources and on-premises sites. • WAN_0, WAN_1, and LAN interfaces need to be predefined in the VPC. • Two elastic IP addresses need to be reserved in the VPC to attach to WAN interfaces later. • VPC should be created and attached to an Internet gateway. • Only a hub-and-spoke topology is supported. • The hub must have public IP addresses on its WAN interfaces. • The hub WAN interface type should be set as **Internet** during onboarding.

Table 3: Site Types by Deployment *(Continued)*

Available Site Types	Added By	Uses	Service Notes
Provider Hub	The SP or OpCo administrator adds provider hub sites for a tenant. Adding a provider hub site means associating an existing provider hub device with the tenant. To do this, the SP or OpCo administrator switches to the Customer Portal for the tenant and adds the provider hub site by selecting the POP and the provider hub device from the list of available POPs and provider hub devices. The name of the provider hub site is automatically set to the name of the selected provider hub device.	SRX Series Firewalls placed in a central role in a service provider cloud. The hub devices establish IPSec tunnels with the spoke sites. Provider hub devices are multi-tenant (shared amongst multiple sites) through the use of VRF instances configured on them.	A provider hub has the following capabilities: • Before a provider hub site can be added, the provider hub device must be created. • For CSOaaS, only the OpCo administrator can add provider data hub sites. • A hub device is required for the dynamic mesh topology. • Local breakout is not supported on provider hub sites.

Table 3: Site Types by Deployment *(Continued)*

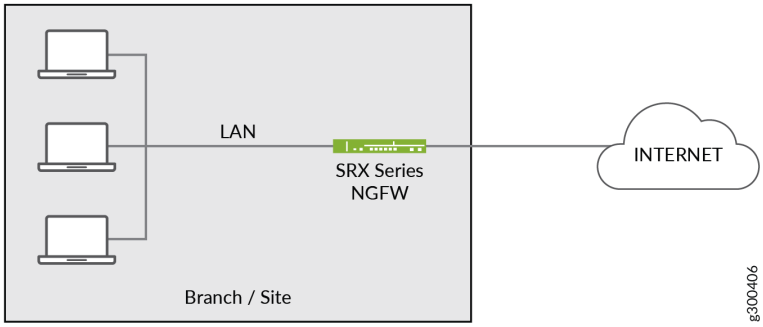
Available Site Types	Added By	Uses	Service Notes
Enterprise Hub	The tenant administrator adds the enterprise hub site.	Provides additional hub-like capabilities to a normal spoke site.	An enterprise hub has the following capabilities: • Can behave as a normal spoke. • Acts as an anchor point for spokes for dynamic VPN creation. • Provides an on-premises central breakout option. • Can host a data center department. • Can import BGP and OSPF routes from the LAN–side L3 device to create a data center dynamic LAN segment. • Automatically meshed with other enterprise hubs that belong to the same tenant. • Regular spoke sites can be assigned to associate with enterprise hubs. • Supports local, central, and cloud breakout profiles with intent-based rules for more granular breakout control.

Topologies

CSO supports the following network topologies:

- **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, such as in the NGFW solution. The NGFW solution provides for remote site security with SRX Series next-generation firewall devices (Figure 5 on page 20).

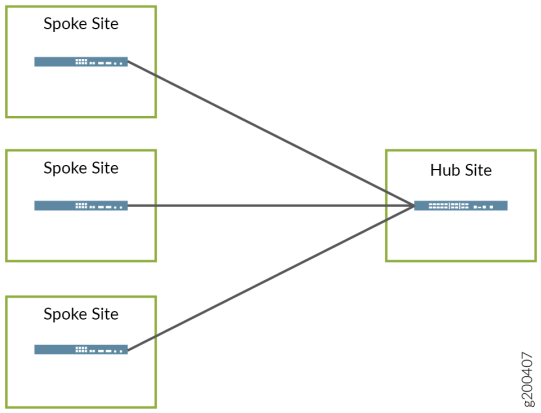
Figure 5: Standalone NGFW



- **Hub–and–Spoke Topology** — This topology is supported for SD–WAN deployments. All traffic, including spoke-to-spoke traffic, passes through the hub site.

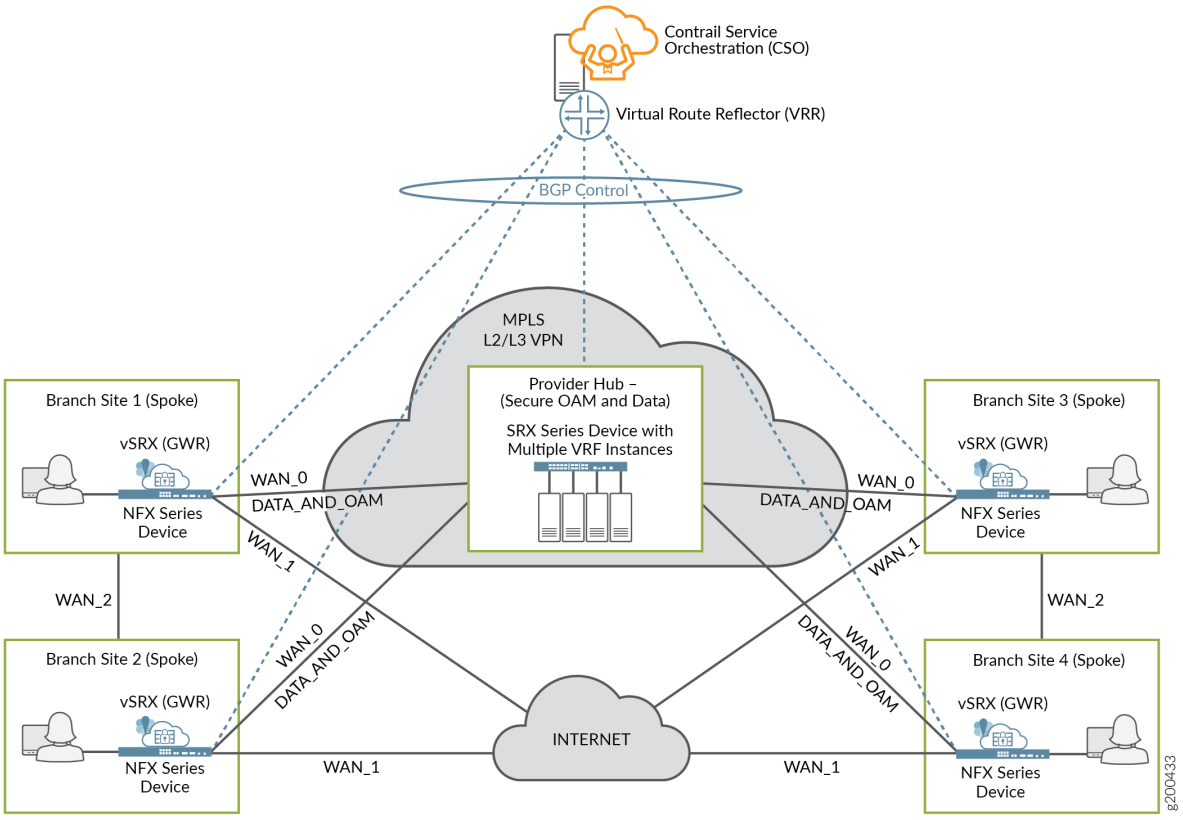
  Figure 6 on page 20 shows the hub–and-spoke concept.

Figure 6: Hub-and-Spoke Topology



- **Dynamic Mesh Topology** — This topology is supported for SD-WAN deployments. Figure 7 on page 21 shows an example of a dynamic mesh topology where traffic can flow directly from any site to any site. Site-to-site tunnels are created dynamically based on traffic thresholds, thereby conserving resources and improving overall performance. Mesh tags are used to determine which sites can connect together.

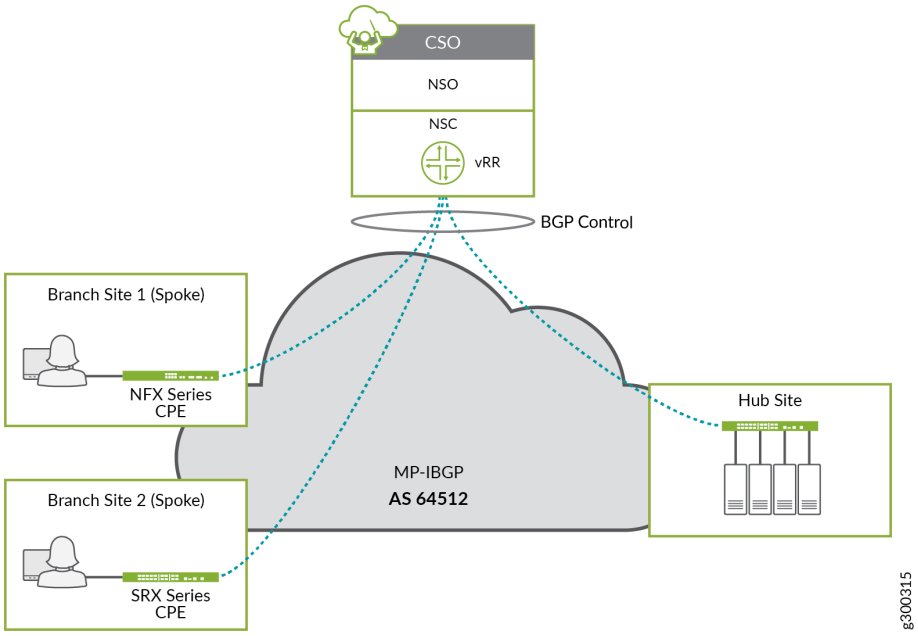
Figure 7: Dynamic Mesh Topology



Virtual Route Reflector (VRR)

The VRR is part of CSO's SD–WAN controller. It is one of the virtual machines that gets provisioned and installed during the installation process. To facilitate the routing needed in the SD–WAN deployment, the VRR forms overlay BGP sessions with CPE spokes and hub devices over the underlay interface designated for OAM capability. You make this selection with the **Configure Site** workflow for site onboarding. Figure 8 on page 22 illustrates the concept of the VRR

Figure 8: VRR Overview



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 and HTTP.

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 SLA Profiles and SD-WAN Policies Overview 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. You must also assign these profiles to an SLA policy before they take effect.

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 (cspadmin) to upload device software images and VNF images on the **Resources > Images** page. The cspadmin user in an on-premises CSO deployment can upload device images for supported SRX Series Firewalls (including vSRX Virtual Firewall), NFX Series devices, and EX Series devices.

For CSOaaS, 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.

3

CHAPTER

SD-WAN Solution

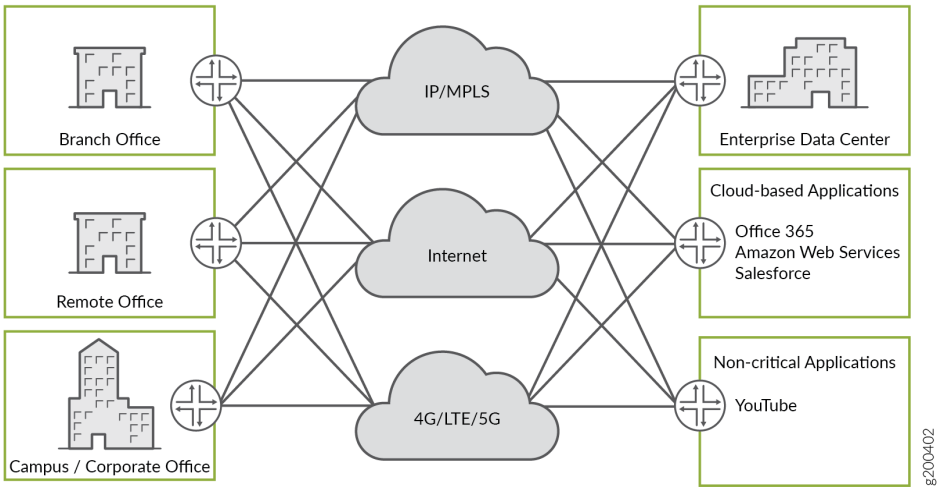
IN THIS CHAPTER

Overview

Typical branch offices can have multiple WAN connection types, including MPLS, Internet (such as LTE and ADSL), and so on. In these traditional networks, the MPLS-based connection typically includes performance guarantees known as *service level agreements* (SLAs) to ensure business-critical applications can function properly. The Internet connection often provides an alternative link for backup and load balancing purposes. However, with Internet access offerings providing ever-increasing bandwidth, many applications can now reasonably be routed over the Internet link.

Software-defined wide area networking (SD-WAN) is primarily thought of as a connectivity solution, implemented as an overlay on top of traditional WAN access. An SD-WAN solution provides the ability to make use of the links in whichever way an enterprise customer wishes, as shown in Figure 9 on page 26.

Figure 9: High-Level View of SD-WAN Interconnectivity



In an SD-WAN environment, low-priority traffic can use the lower-cost Internet link(s), while more important traffic can travel across better quality links (such as those provided by an MPLS network). Link usage can also be assigned per application. With an SD-WAN solution, an enterprise customer can mix and match cost optimization with SLA requirements as they see fit.

Starting in CSO Release 6.0.0, you can choose one of the following SD-WAN service levels for a tenant:

- *Essentials*—Provides the basic SD-WAN services (called Secure SD-WAN Essentials). This service is ideal for small enterprises looking for managing simple WAN connectivity with comprehensive NGFW security services at the branch sites, using link-based application steering. The SD-WAN Essentials service allows Internet traffic to breakout locally, and thus avoids the need to backhaul

web traffic over costly VPN or MPLS links. The sites support features such as intent-based firewall policies, WAN link management and control, CSO-controlled routing between sites connected through the static VPN, and site to site communication through MPLS or internet links behind NAT. A tenant with the SD-WAN Essentials service level can create only SD-WAN Essentials sites. You can upgrade the SD-WAN service level of a tenant from Essentials to Advanced, by editing the tenant information. See Edit Tenant Parameters.

- *Advanced*—Provides the complete SD-WAN service (called Secure SD-WAN Advanced). This service is ideal for enterprises with one or more data centers, requiring flexible topologies and dynamic application steering. Site-to-Site connectivity can be established by using a hub in a hub-and-spoke topology or through static or dynamic full mesh VPN tunnels. Enterprise wide intent based SD-WAN policies and service-level agreement (SLA) measurements allow to differentiate and dynamically route traffic for different applications.

NOTE: SD-WAN sites on CSO Release 5.4 or earlier versions are treated as SD-WAN Advanced sites. You cannot downgrade the SD-WAN service level of a tenant from Advanced to Essentials.

SD-WAN Requirements

The key components of an SD-WAN solution center around application awareness, visibility, and performance. An SD-WAN solution must generally provide the following types of functionality:

- Multiple connection types – MPLS, Internet, LTE, ADSL, etc.
- Secure site-to-site connectivity - tunneling and VPNs
- An intuitive interface for managing WAN connections
- Ability to make use of all available uplink paths
- Ability to optimize use of WAN connection for cost savings
- Application-aware performance monitoring over WAN links
- Dynamic spoke/endpoint learning and reachability

In addition, modern SD-WAN solutions have evolved to offer even broader capabilities, including:

- Automation of end-to-end solution provisioning
- Enterprise network modeling, network definition

- Zero touch provisioning (ZTP) of on-premises devices, including establishing connectivity
- Provisioning of multiple node types (spoke, hub, concentrators, etc.)
- Dynamic path selection, and ability to load balance across multiple WAN connections
- End-to-end, application-level SLAs through continuous path measurement
- Dynamic application steering to counteract link degradation
- End-to-end visibility and monitoring of devices, connectivity, and application performance
- Support for 3rd-party services
- Intent-based policy creation to define traffic treatment
- Security through enterprise-wide policies

Juniper Networks Contrail SD-WAN solution, as described in this document, provides a full, end-to-end solution that aims to offer all of the above functionality.

Contrail SD-WAN Solution Highlights

Highlights of Juniper's Contrail SD-WAN solution include:

- Integrated Security – full security suite with NGFW, Content Security, etc.
- Single Orchestrator – CPE zero touch provisioning, VNF deployment, managed security, SD-WAN services
- Adherence to open standards – not a book-ended solution, easily interoperable with existing SP/enterprise infrastructure and third-party CPEs through open APIs and protocols, with software deployable on public as well as private clouds
- Full routing and MPLS stacks - support for BGP/OSPF/IS-IS/MPLS, etc. on WAN/LAN, scalable architecture with distributed SD-WAN gateways
- Support for BGP on the underlay networks
- Carrier grade appliance – innovative branch device (NFX Series) with service chaining support for 3rd-party VNFs
- End-to-end management/orchestration – feature rich, horizontally scalable, easy-to-use orchestration platform

Target Customers

The Contrail SD-WAN on-premises deployment is architected to address the following types of customers:

- Service providers with existing MPLS networks
    - Offers ways to provide SD-WAN as a value-added offering that leverages existing MPLS core networks
- Managed service providers (also known as OpCos or MSPs), building networks on top of service providers and offering end-to-end solutions (first-mile, middle-mile, last-mile)
    - Provides logical separation from underlay provider using overlay networks
- Large enterprises, trying to build their own end-to-end overlay-based network
    - Enables independence from underlay/transport provider
    - More control and agility to meet network requirements

In addition to the benefits above, the CSOaaS option is designed for broadly distributed enterprise and MSP customers who:

- Prefer a cloud consumption model
- Demand ease of use and quick turn up of cloud enabled branch services
- Don’t have the cloud Infrastructure to host and operate an SD-WAN solution
- Have the business need to consume cloud services in a pay as you grow SaaS model
- Have limited or no IT personnel on-site in remote branches

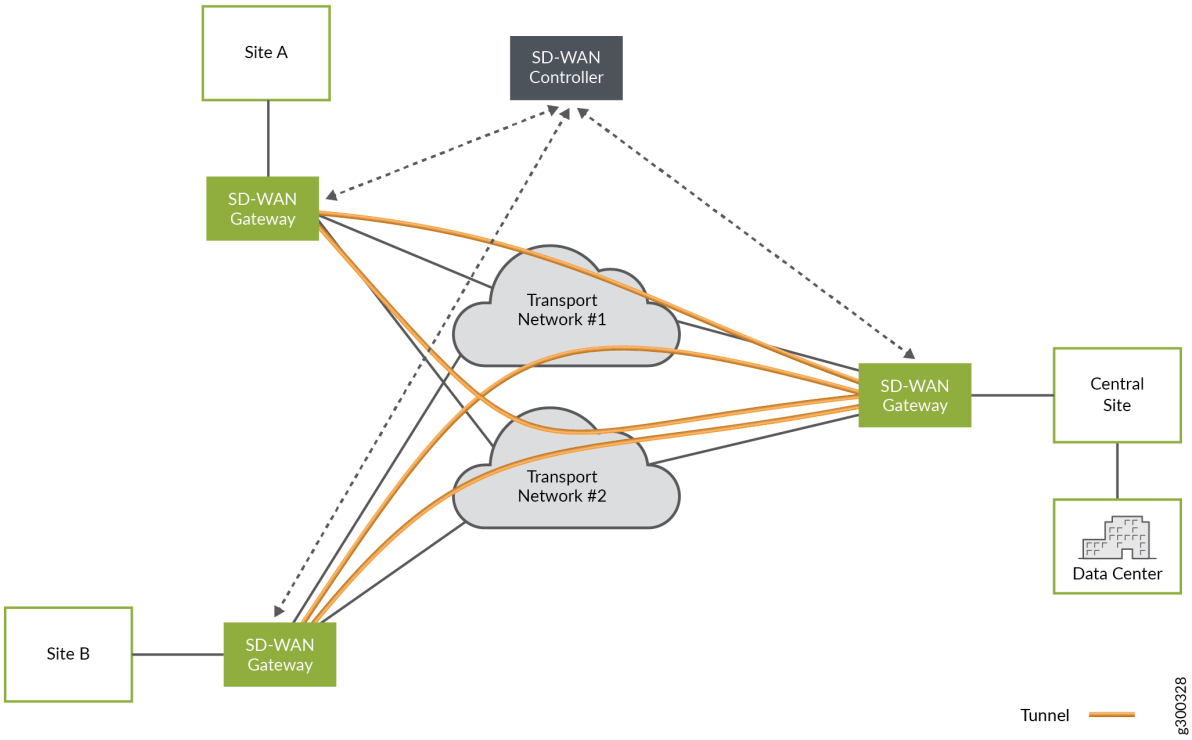
Contrail SD-WAN Deployment Architectures

IN THIS SECTION

An SD–WAN implementation offers a flexible and automated way to route traffic from site to site. As shown in Figure 10 on page 31, 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 10: SD-WAN Architecture

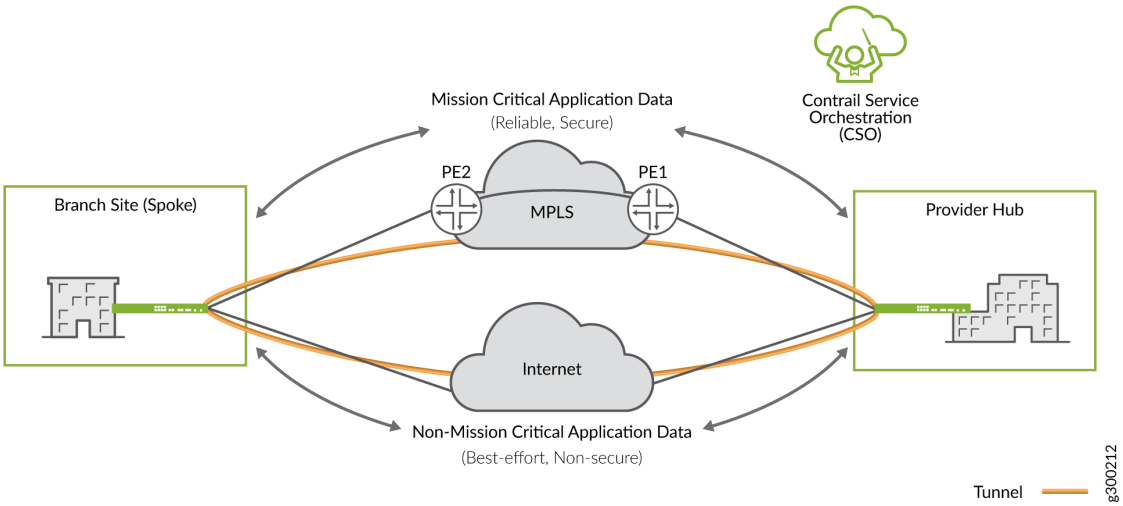


The SD–WAN controller, built in to CSO, acts as an orchestration layer and provides an interface, allowing the operator to setup and manage the devices at the sites.

Contrail SD-WAN Reference Architecture

Juniper Networks Contrail SD–WAN solution architecture, shown in Figure 11 on page 32 uses a hub–and–spoke topology , with CPE devices located at customer branch sites. On the local side of the site, the CPE devices connect to LAN segments and participate in dynamic routing protocols with other LAN devices. On the WAN side, the CPE devices connect across two or more links to a provider hub device. Because the SD-WAN model uses a hub–and–spoke topology, traffic travels from site to site through the provider hub. By default, traffic going to the Internet also flows through the provider hub device.

Figure 11: Contrail SD-WAN Reference Architecture



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

The following sections describe 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 , providing connectivity from the branch site to other sites in the tenant network and to the Internet. There are two types of spoke devices: on-premises spoke and cloud spoke.

On-Premises Spoke Devices

On–premises spoke devices can be either NFX Series devices or specific SRX Series Firewalls.

NFX Series Network Services Platform

An NFX Series Network Services Platform used as an on-premises spoke device can host a range of multivendor VNFs, support service chaining, and be managed by orchestration software in the cloud. NFX Series devices eliminate the operational complexities of deploying multiple physical network devices at a customer site and offer a substantial improvement over traditional, single function CPE devices.

A key VNF supported on the NFX Series platform is the vSRX Virtual Firewall Virtual Firewall. In the Contrail SD–WAN solution, the vSRX Virtual Firewall instance with routing and switching capabilities performs the gateway router function. It also provides the same feature-rich security services found on standard SRX Series Firewalls. Table 4 on page 33 shows the NFX Series hardware that you can implement as an on-premises spoke device.

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

Table 4: NFX Series Hardware – On-Premises Spoke Devices

Platform	Models Supported
NFX150 Network Services Platform	• NFX150–S1 • NFX150–S1E • NFX150–C–S1 • NFX150–C–S1–AE/AA • NFX150–C–S1E–AE/AA
NFX250 Network Services Platform	• NFX250–LS1 • NFX250–S1 • NFX250–S2

SRX Series Devices and vSRX Virtual Firewall Virtual Firewalls

A physical SRX Series security device can be used in place of the NFX Series platform to provide the gateway router function, as can a vSRX Virtual Firewall instance installed on a server. Table 5 on page 34 shows the SRX hardware and vSRX Virtual Firewall virtual firewalls that you can implement as on-premises spoke devices.

Table 5: SRX Series Hardware and vSRX Virtual Firewall Firewalls – On-Premises Spoke Devices

Platform	Models Supported
SRX Series	• SRX4200 • SRX4100 • SRX1500 • SRX550M • SRX380 • SRX345 • SRX340 • SRX320 • SRX300
vSRX Virtual Firewall Virtual Firewalls	vSRX Virtual Firewall vSRX Virtual Firewall 3.0

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

Cloud Spoke Devices

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

Spoke Redundancy

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

Provider 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 provider hub device and one or more spoke devices.

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

Provider Hubs

In a service provider (SP) environment, the service provider hosts a *provider hub* device in their network. The provider hub device acts as a point of presence (POP) or connection point. It is typically a shared device, providing hub functionality to multiple customers (tenants) through the use of virtual routing and forwarding instances (VRF). The SP administrator and the OpCo administrator can both manage the provider hub device.
For CSOaaS, the SP administrator role is performed by Juniper Networks as the cspadmin user (or equivalent). The OpCo administrator role can be assigned to a user by the SP administrator, but the OpCo administrator does not have SP administrator privileges.
Table 6 on page 35 lists the provider hub devices supported in a CSO SD-WAN environment.

Table 6: Provider Hub Devices

Role	Supported Device Types
Provider Hub	• SRX4600 • SRX4200 • SRX4100 • SRX1500 • vSRX Virtual Firewall • vSRX Virtual Firewall 3.0

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

Provider Hub Redundancy

Two redundant provider hub devices can be used at one POP to protect against device and link failures, and to provide upstream multi-homing for spoke sites. For more detail, see the "Resiliency and High Availability" on page 107 topic in this guide.

Enterprise Hub Sites and Devices

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

- Can act as the anchor point for site–to–site communications on the customer's network.
- Can act as the central breakout node for the customer's network.
- Offers a specialized department called the *data–center department*.
- Supports data center dynamic LAN segments with BGP and OSPF route imports, including default routes, from the LAN–side Layer 3 device.
- Allows for intent-based breakout profiles to create granular breakout behavior based on department, application, site, and so on.

In an enterprise environment, the enterprise hub is owned by the customer (tenant) and usually resides within an enterprise data center. Only the customer's spoke sites can connect to the enterprise hub device. OpCo administrators and tenant administrators can manage the enterprise hub. Table 7 on page 37 lists the enterprise hub devices supported in a CSO SD-WAN environment.

Table 7: Enterprise Hub Devices

Role	Supported Device Types
Enterprise Hub	• SRX4600 • SRX4200 • SRX4100 • SRX1500 • SRX380 • vSRX Virtual Firewall • vSRX Virtual Firewall 3.0

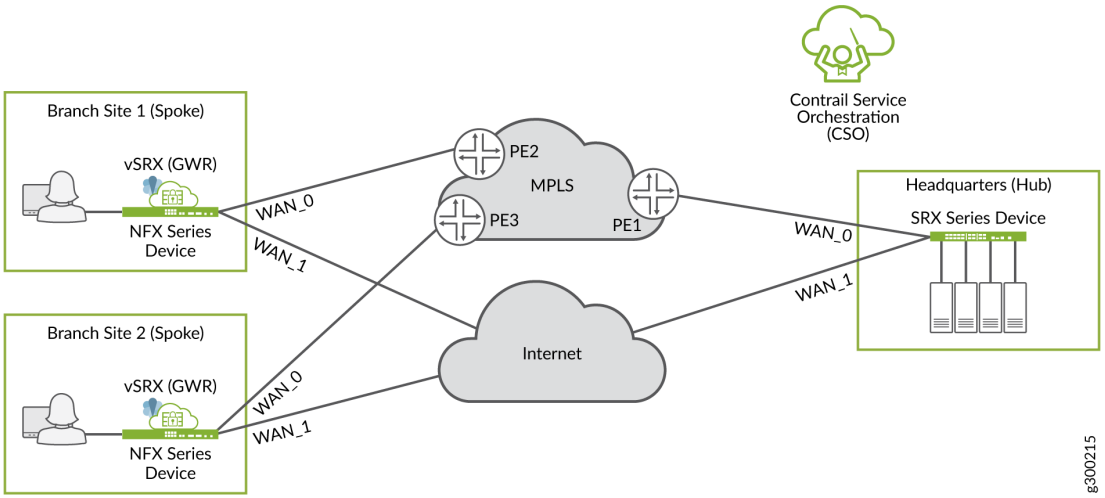
NOTE: For the most up to date information on hardware and software support for CSO, see the Contrail Service Orchestration Release Notes.

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-premises devices.

Figure 12 on page 38 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 12: SD-WAN Underlay Network



Each on-premises 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-premises 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-cone and restrictive NAT deployments are supported.

Dual CPE configurations are not supported.

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

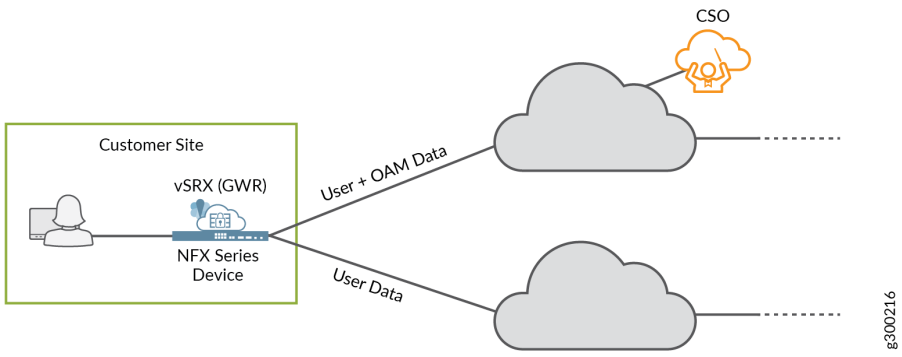
- ADSL/VDSL (ADSL/VDSL support for WAN links and ZTP on NFX Series devices starting in CSO Release 4.0.0, and ADSL support on the SRX300 Line of Services Gateways starting in CSO Release 5.2.0.)
- Broadband
- MPLS and broadband
- Satellite link

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-premises device.

Figure 13 on page 39 illustrates these two interface types.

Figure 13: WAN Interface Types



Note that:

- The on-premises 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-premises device's OAM interface. This ensures that the address is unique within the entire CSO deployment and prevents human error.

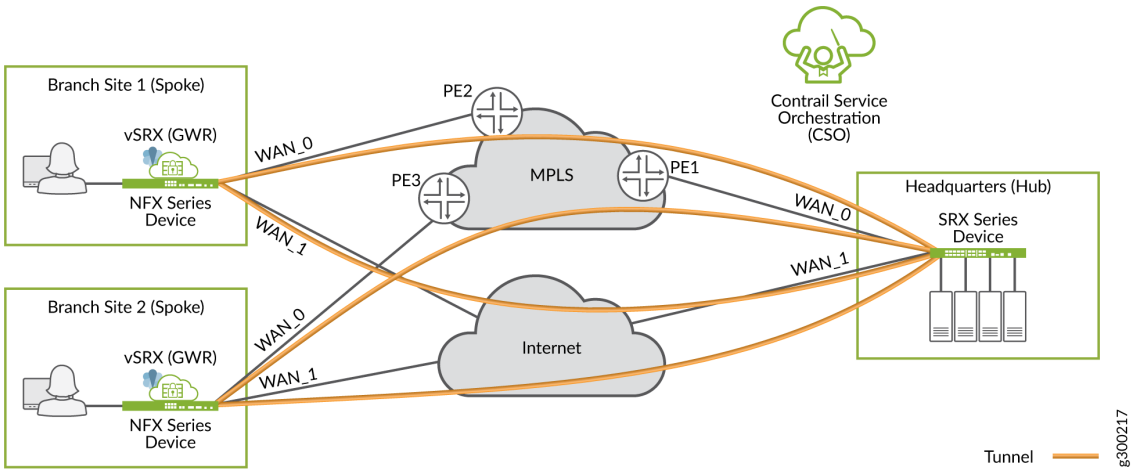
- To ensure secure communication over the WAN, the on-premises device initiates the connection to CSO.
- Device–initiated connections can work across intermediate NAT devices.
- The user-and-OAM-data interface can use a single IP address for both functions.

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 14 on page 40 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 14: 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.

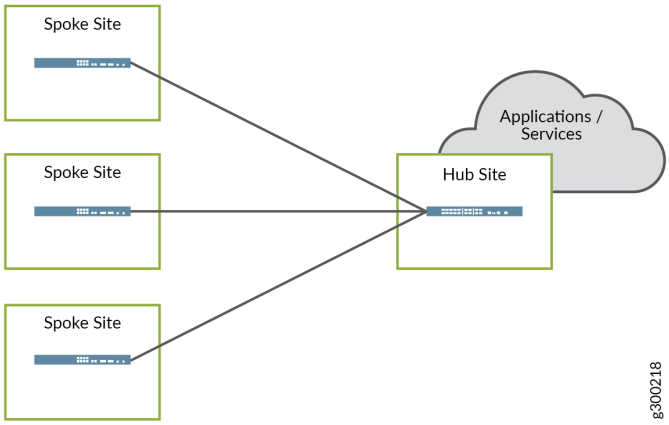
Overlay Deployment Topologies

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 15 on page 41. Spoke sites cannot communicate directly with other spoke sites.

Figure 15: SD-WAN Hub-and-Spoke Topology

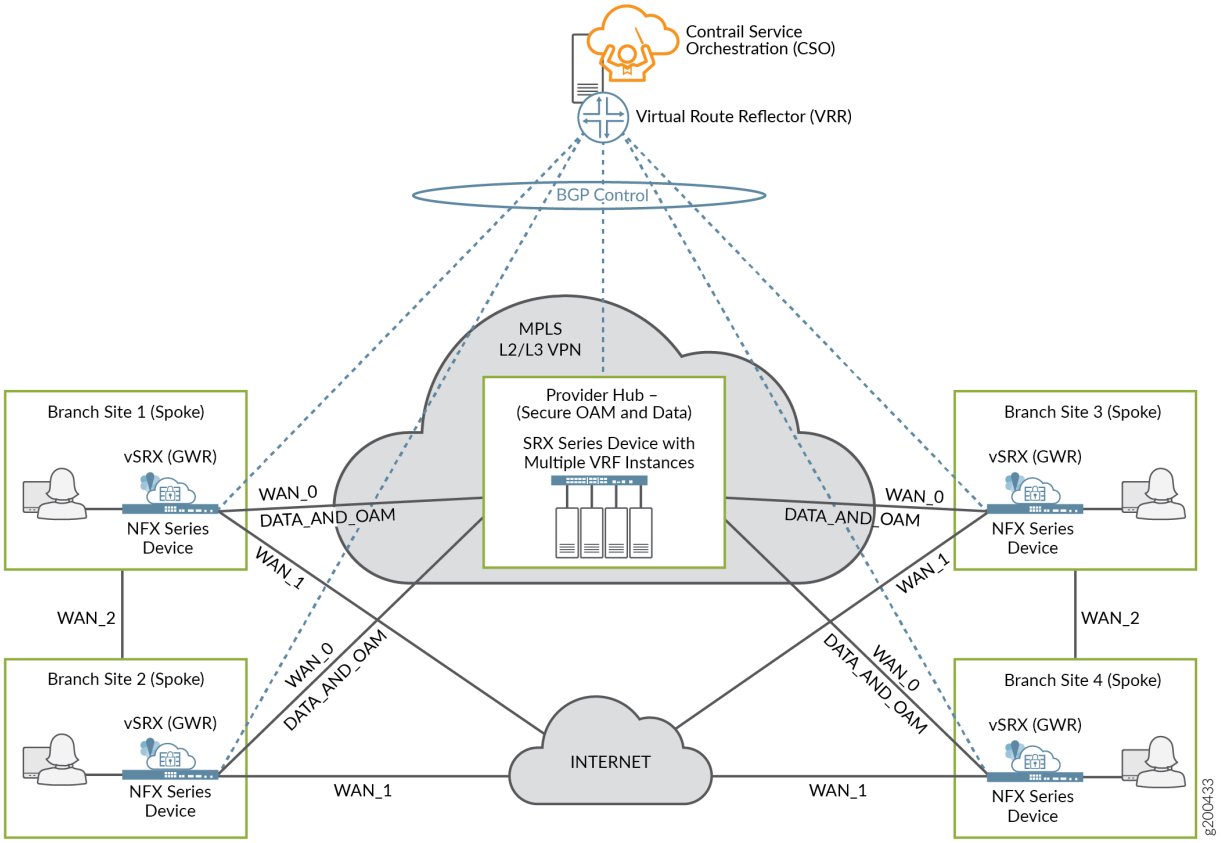


The hub sites used can be either provider hub or enterprise hub sites. When an enterprise hub site is used, the provider hub (if any) is used as backup only. This topology is preferred when applications and services are centralized at the hub site.

Dynamic Mesh

With the dynamic mesh topology, overlay tunnels between participating sites enable the sites to communicate directly with each other, as shown in Figure 16 on page 42. 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 16: 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.

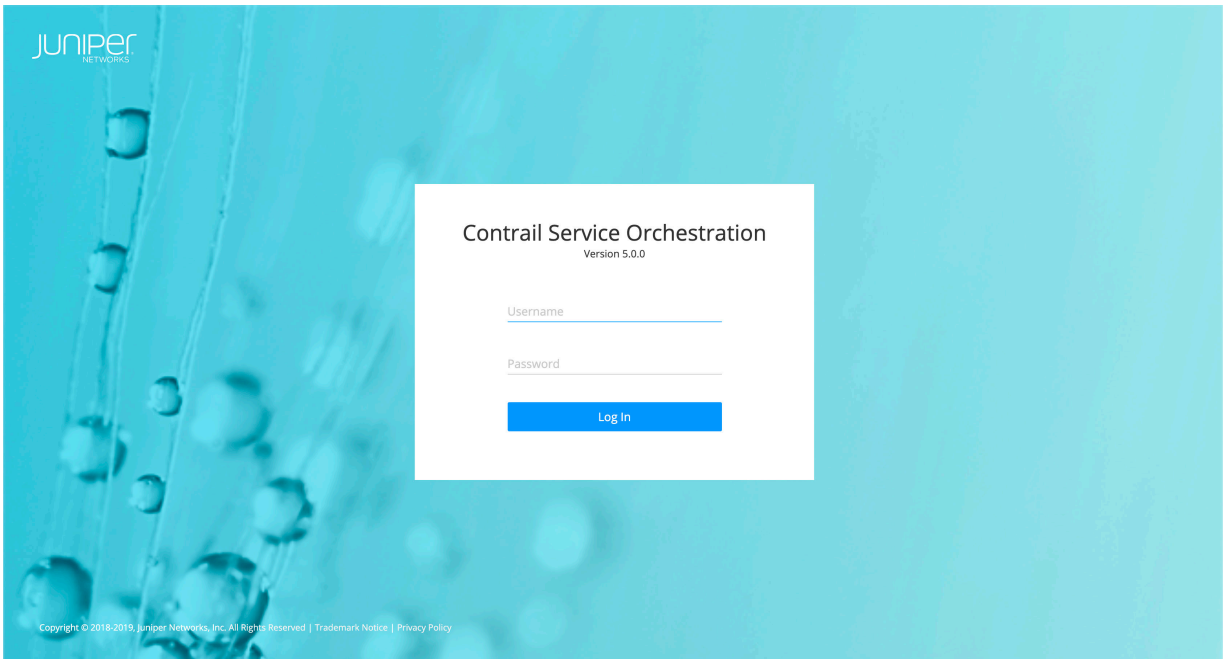
When spoke devices are added to a dynamic mesh topology, the administrator configuring the sites must assign a mesh tag to each WAN interface. Only two devices with matching mesh tags can form the VPN connection to allow communication. Interfaces with mismatched mesh tags can never communicate directly.

Orchestration and Control

Orchestration and controller functions are implemented through Juniper's Contrail Service Orchestration (CSO) software. As shown in Figure 17 on page 43, CSO software offers a Web–based

UI to manage the SD-WAN environment. Figure 17 on page 43 is a sample image and the CSO version number on it is only for reference.

Figure 17: 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-premises (CPE) devices, and provide topology and CPE lifecycle management functionality.

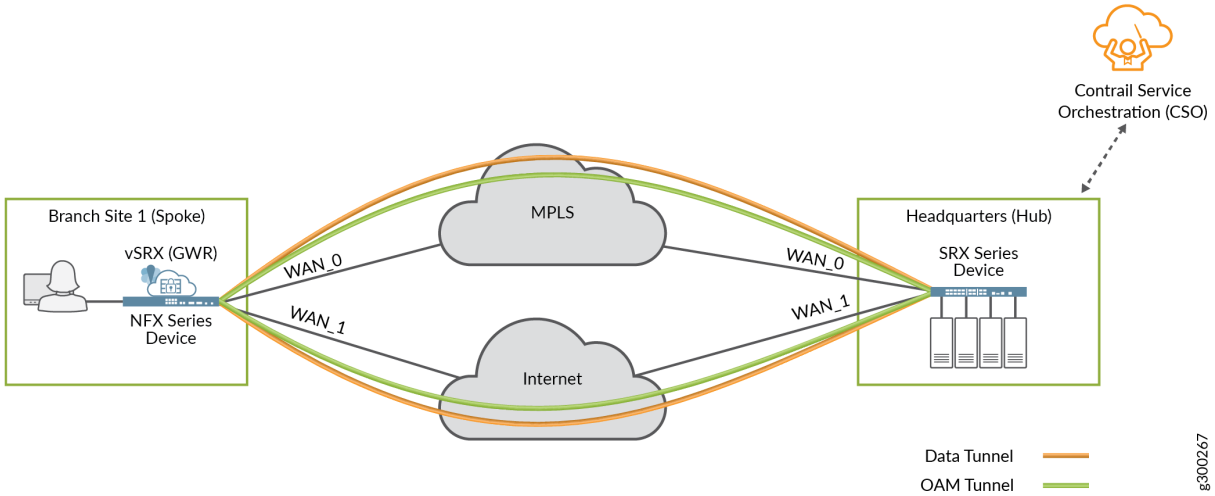
At the user level, CSO provides the interface to deploy, manage, and monitor the devices in the SD–WAN network through the NSC. At the network level, NSC includes a vRR that allows each site to advertise its local routes to remote sites.

Secure OAM Network

SD–WAN deployments include a secure OAM overlay network to provide end-to-end secure communications between on-premises devices and CSO. For CSOaaS, this is automatically provided as part of the service.

As shown in Figure 18 on page 44, dedicated, IPsec-encrypted OAM tunnels enable on-premises devices to send management, routing, and logging traffic securely over the network to a provider hub. The provider hub then forwards the traffic to CSO.

Figure 18: Secure OAM Tunnels



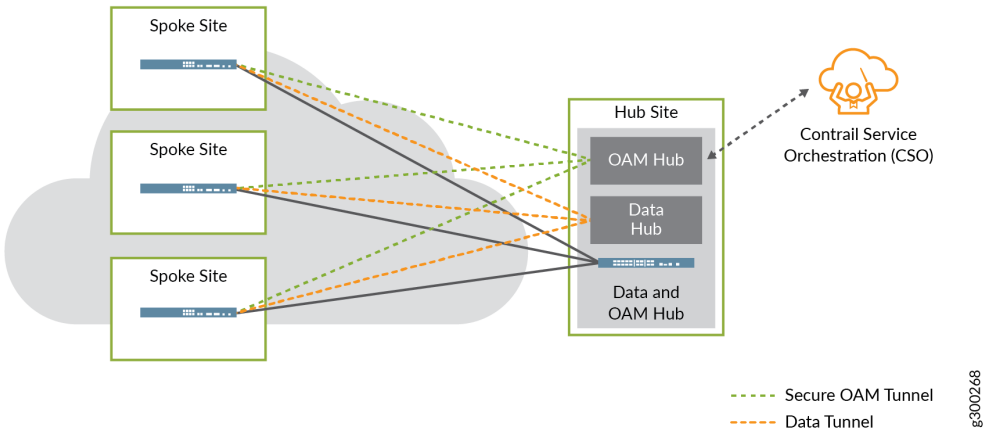
Integration with Deployment Topologies

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 19 on page 45.

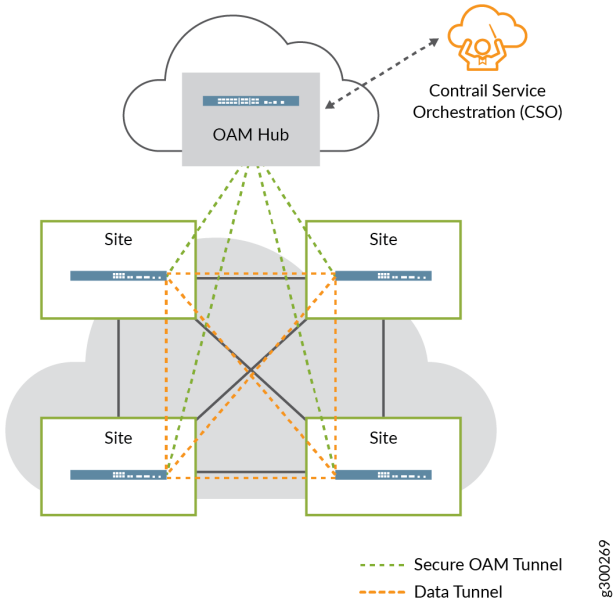
Figure 19: OAM Tunnels in the Hub-and-Spoke Topology



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 20 on page 45, each spoke site has a new connection: a separate, dedicated IPsec overlay tunnel carrying OAM traffic to the provider hub.

Figure 20: OAM Tunnels in the Full Mesh Topology

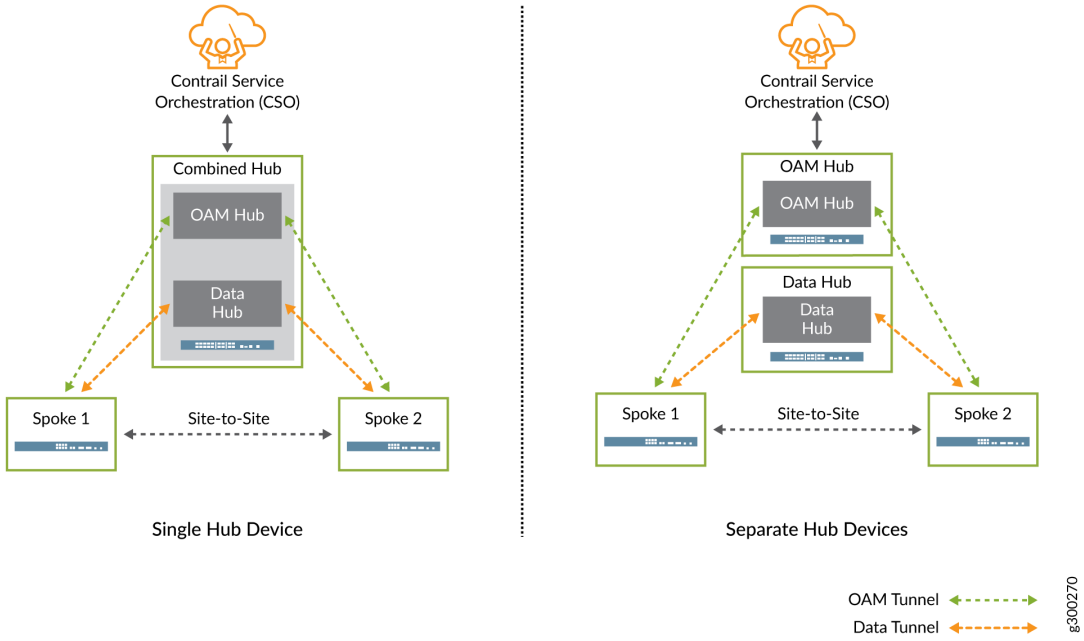


OAM Hub Design Options

There are two ways to implement the OAM hub in an on-premises CSO deployment, depending on design requirements. As shown in Figure 21 on page 46, 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 21: OAM Tunnels - Provider Hub Design Options



NOTE: For CSOaaS, 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-premises devices.

  For CSOaaS, OAM hub redundancy is part of the service.
- When a spoke site is multi-homed to multiple hub devices, one OAM tunnel should terminate on each hub.
- On-premises 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). The following is a high-level list of steps performed during ZTP:

- If you implement the on-premises version of CSO, you need to add the appropriate CSO SSL certificate to the redirect server before performing ZTP.

  NOTE: If you deploy the cloud-delivered version of CSO, Juniper Networks configures the redirect server for you.
- 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 2 Mbps.

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.

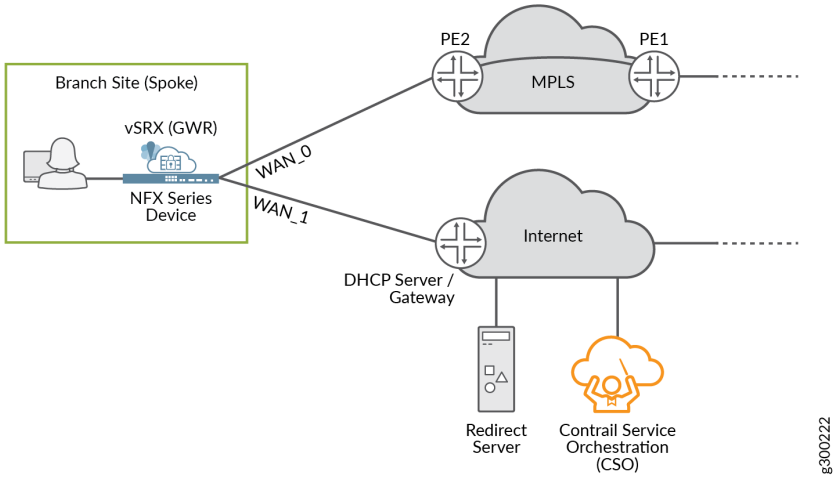
Redirect Server

The redirect server is an Internet–located, Juniper–owned–and–managed server that is integral to the ZTP process. The server enables each spoke device to locate and authenticate with its designated CSO instance. With the assistance of the redirect server, the spoke device can contact CSO and receive its initial configuration, including a Junos OS software update (if required).

For on-premises deployments of CSO, the administrator configures WAN ports on the spoke devices to connect to both the Internet and the redirect server. For cloud-delivered CSO, Juniper Networks handles this configuration for you.

In Figure 22 on page 48, both the redirect server and CSO are located on the Internet. The spoke device obtains and uses IP addressing and other information provided through its Internet–facing interface, and can reach both the redirect server and CSO through that same WAN interface.

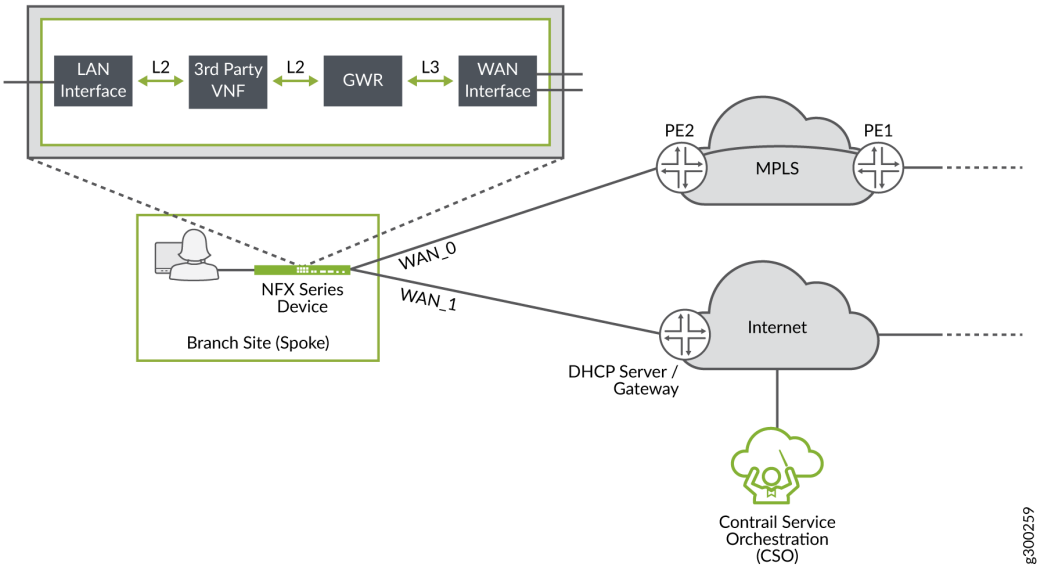
Figure 22: CSO and Redirect Server on Internet



Service Chaining in Contrail SD-WAN

Starting in 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 23 on page 49.

Figure 23: Service Chaining in an SD-WAN Environment



Starting 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:

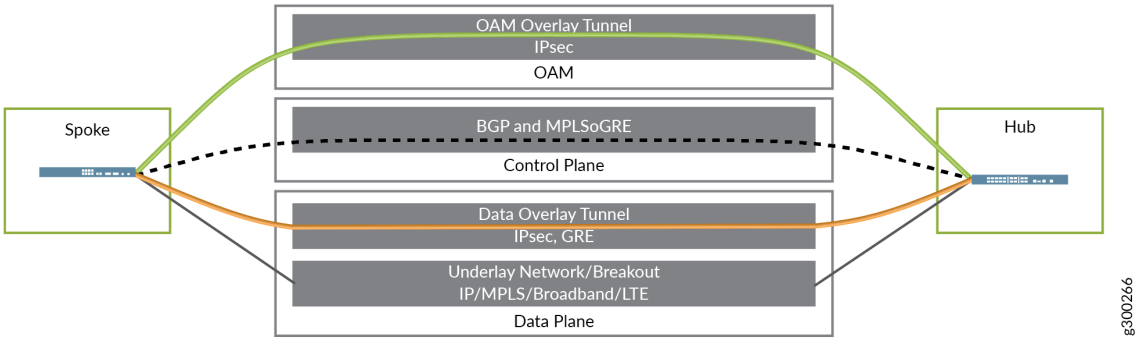
1. Data Plane:

- 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

Figure 24 on page 50 illustrates this concept.

Figure 24: Three Planes, Four Layers



Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
4.0	Starting in CSO Release 4.0, service chaining is available for SD-WAN environments.
4.0	Starting in CSO Release 4.0, the following third-party virtual network functions (VNFs) are supported: *Fortigate-VM* and *Single-legged Ubuntu VM*.

Two Basic SD-WAN Use Cases

IN THIS SECTION

Two SD-WAN use cases are described below. These use cases illustrate variations around which devices constitute the hubs: a separate SRX Series Firewall (in addition to the MX Series PE device providing underlay connectivity) dedicated to providing SD-WAN overlay connectivity for CPE devices; or a dedicated SRX Series Firewall used for terminating overlay connectivity.

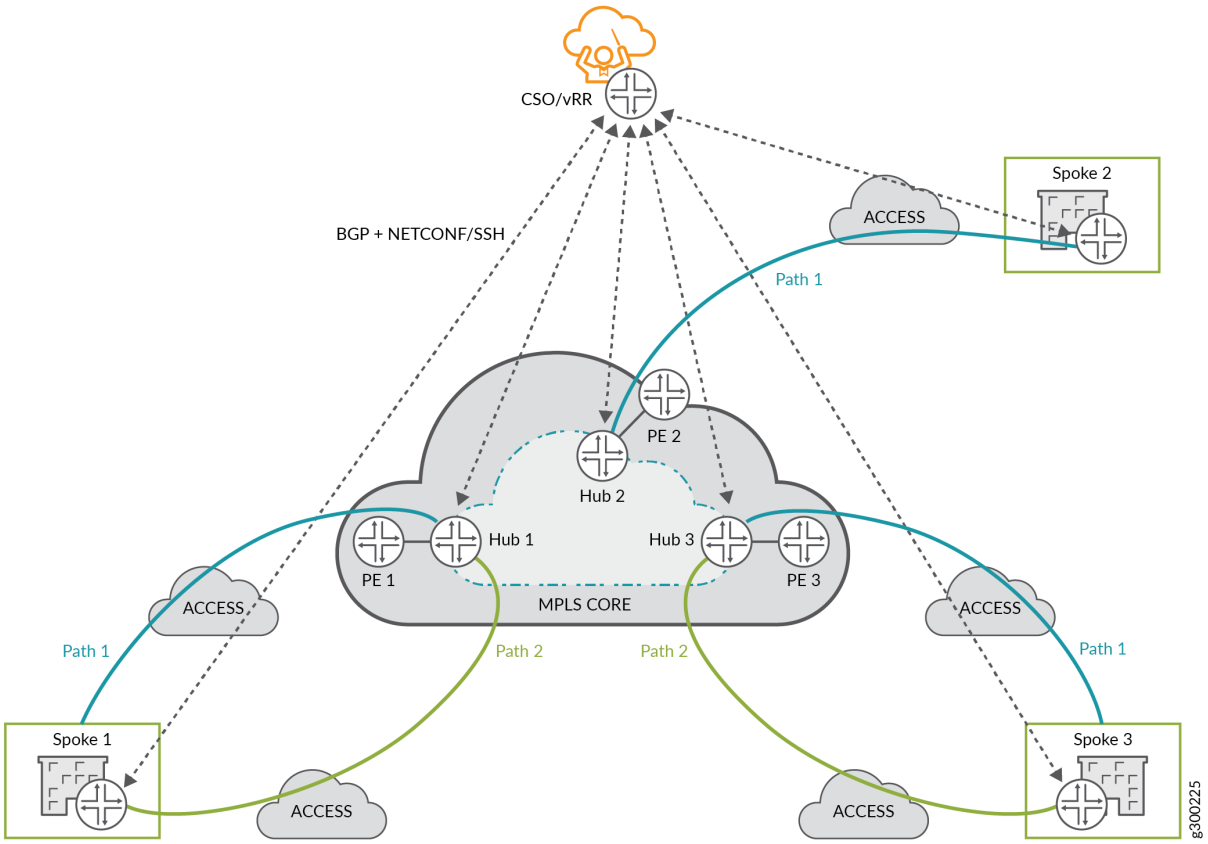
Managed SD-WAN - Overlay Access

This use case is most applicable when the provider wants to take advantage of their existing network, but maintain separation between the existing infrastructure and new SD-WAN infrastructure.

As shown in Figure 25 on page 52, the existing PE devices deployed at POPs remain in place and continue to form that function. In addition, SD-WAN hub devices are deployed at POPs alongside the PE devices to terminate overlay tunnels from the spoke sites.

Again CSO manages the hub and spoke devices. In this use case it also makes use of its vRR to establish BGP sessions with the devices. The vRR advertises reachability information to all devices to provide site-to-site connectivity.

Figure 25: Managed SD-WAN Use Case - Overlay Access



Implementation characteristics:

- The core MPLS infrastructure is managed by the provider.
- The access links can be MPLS or Internet.
- The overlay tunnels extend from the spoke site CPE devices to the dedicated SD-WAN hub devices.
- Multiple overlay encapsulations are supported.
  - MPLSoGRE (CE-PE/MPLS access)
  - MPLSoGREoIPsec (Internet access)
- SRX Series Firewalls are used as provider hubs for IPsec termination.
- The SRX Series Firewalls peer with the PEs for connectivity.
- Provider hubs can be shared across multiple tenants.

Enterprise SD-WAN - Overlay

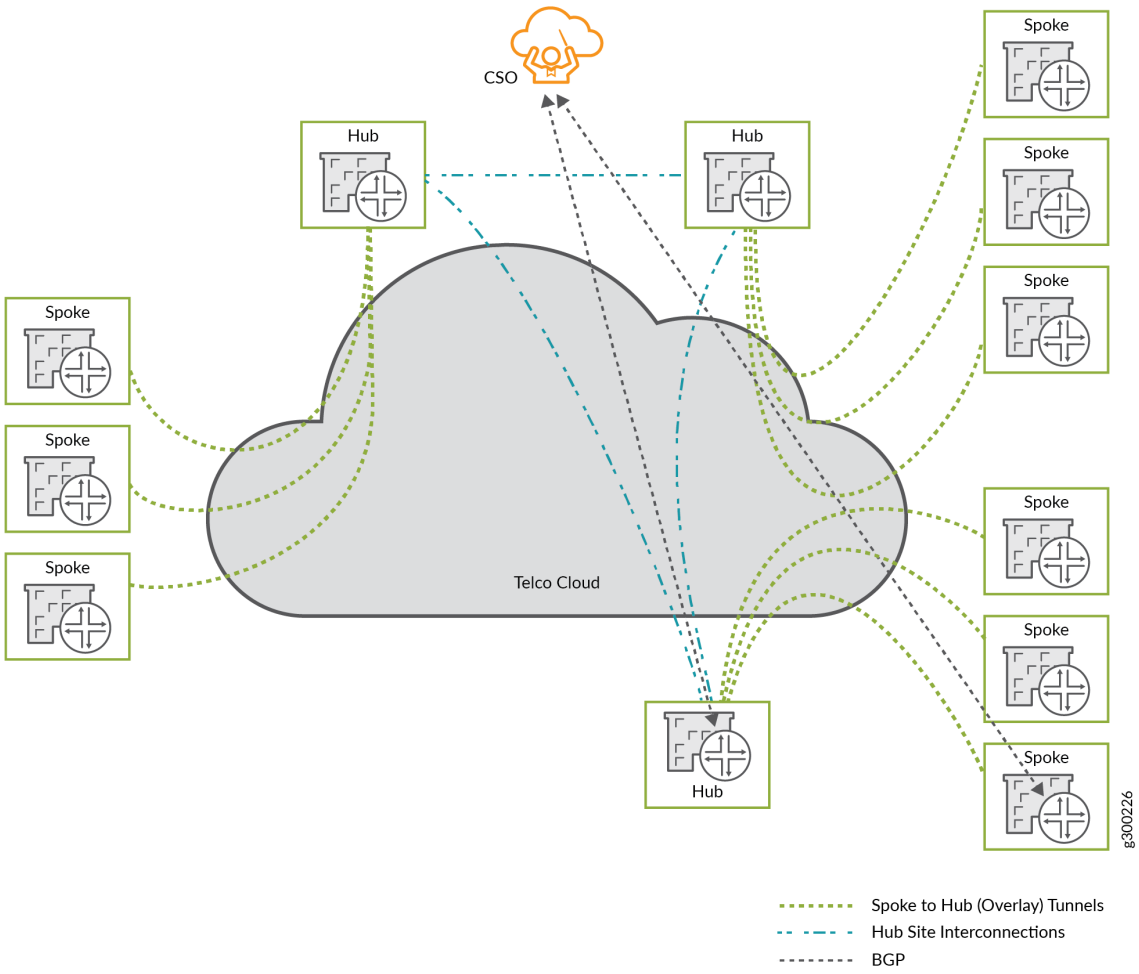
This use case is most applicable to larger enterprises to enable full, end-to-end overlay network connectivity, completely independent of the underlying provider networks.

With this use case, the enterprise customer (tenant or OpCo) owns the hub devices, not the provider. Only spoke sites belonging to this tenant can connect to the enterprise hub devices.

Figure 26 on page 53 illustrates this use case. The enterprise hub devices are located at the customer sites, with overlay tunnels to each of the spoke sites. The hub devices are also interconnected through a provider service such an MPLS VPN, providing full site-to-site connectivity.

Again, CSO manages all hub and spoke devices, and its vRR advertises reachability information to all devices.

Figure 26: Enterprise SD-WAN Use Case - Overlay



Implementation characteristics:

- The overlay tunnels extend from the spoke site CPE devices to the hub devices.
- The overlay tunnels use MPLSoGRE or MPLSoGREoIPsec encapsulation, as appropriate.
- SRX1500, SRX4100, or SRX4200 Series devices can be used as enterprise hubs for IPsec termination.
- Enterprise hub sites are located at customer sites.
- PE resiliency can be implemented by connecting CPE WAN links to primary and secondary PE nodes.

  CSO establishes BGP peering relationships between the CPE and PE nodes. See Adding an On-Premises Spoke Site with SD-WAN Capability for details.

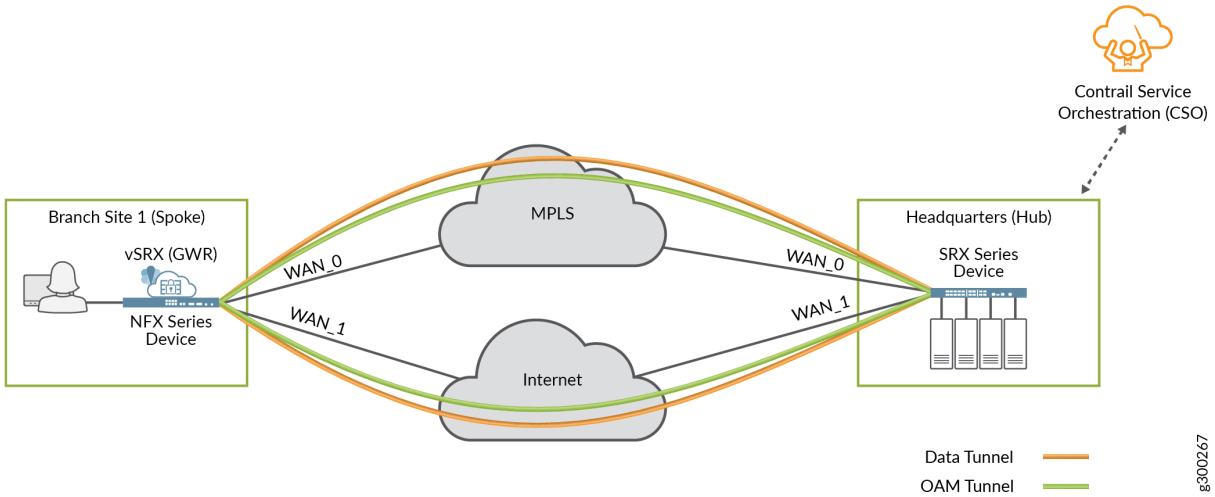
  NOTE: Only supported when local breakout is configured on the CPE WAN link.

- BGP underlay route advertising can be configured to the primary and secondary PE nodes from CPE devices when local breakout is enabled on the WAN interface. See Adding an On-Premises Spoke Site with SD-WAN Capability for details.

Secure and Redundant OAM Network

Contrail SD-WAN deployments include a secure OAM overlay network to provide end-to-end secure communications between on-premises devices and CSO. As shown in Figure 27 on page 55, dedicated, IPsec-encrypted OAM tunnels enable on-premises devices to send management, routing, and logging traffic securely over the network to a provider hub. The hub then forwards that traffic to CSO.

Figure 27: Secure OAM Tunnels

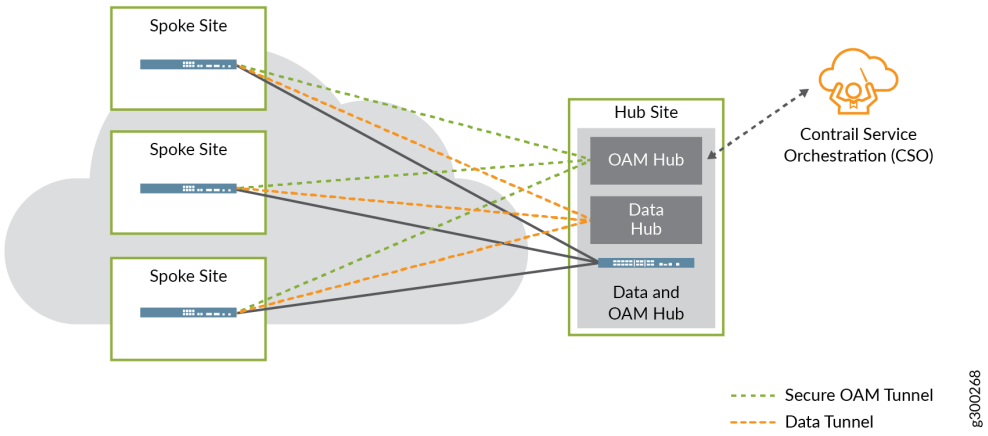


The sites in both the hub-and-spoke and dynamic mesh deployment topologies must use at least one secure OAM tunnel. You accomplish this by setting one of the WAN links for use with OAM during the site onboarding process.

BEST PRACTICE: We recommend having at least two of your WAN links set for use as OAM as shown in Figure 27 on page 55.

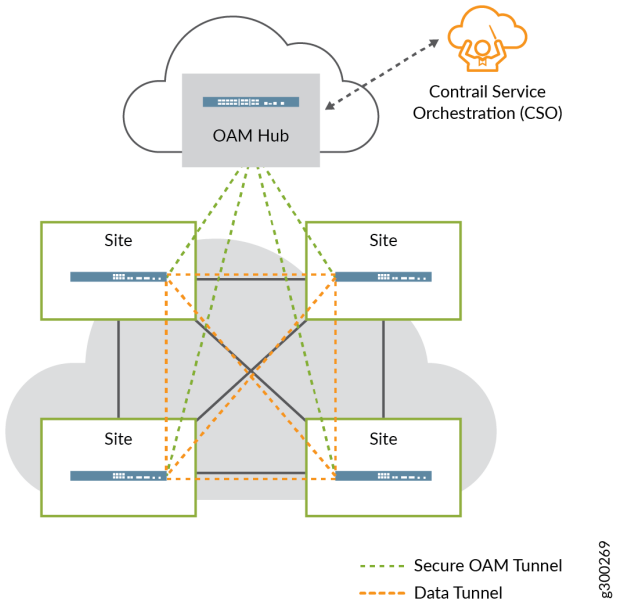
With the hub-and-spoke topology, each spoke site now has two sets of connections to the provider hub site: an overlay tunnel carrying data, and a separate, dedicated IPsec overlay tunnel carrying OAM traffic, as shown in Figure 28 on page 56.

Figure 28: OAM Tunnels in the Hub-and-Spoke Topology



Since a normal dynamic mesh topology would not include a hub device for data traffic, one must be added for the secure OAM traffic. As shown in Figure 29 on page 56, each spoke site has a new connection: a separate, dedicated IPsec overlay tunnel carrying OAM traffic to the provider hub.

Figure 29: OAM Tunnels in the Full Mesh Topology

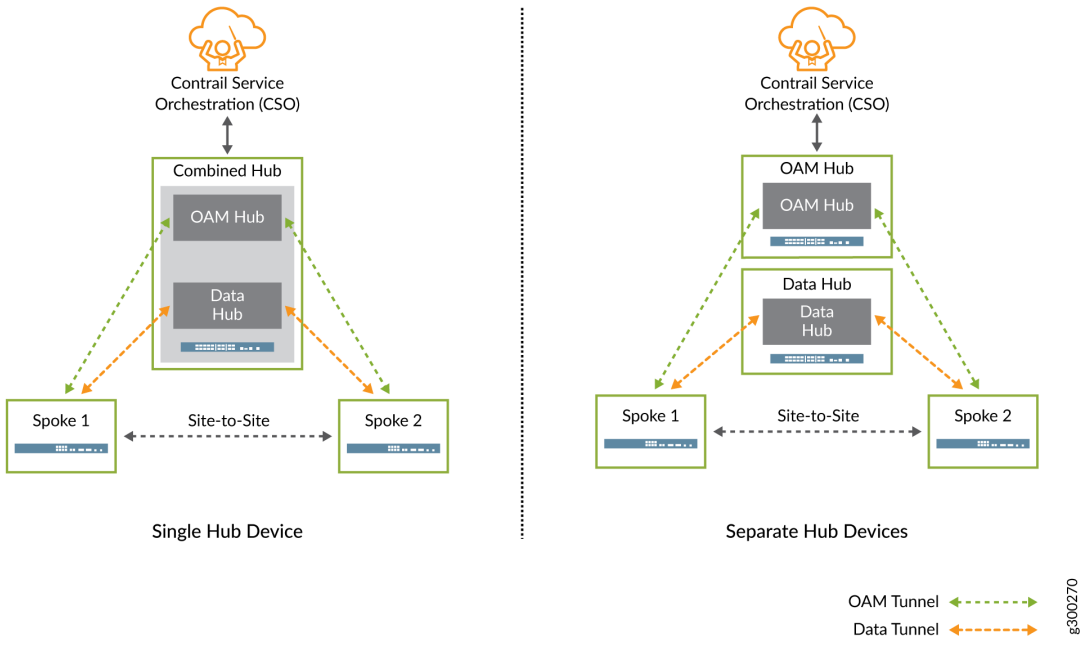


OAM Provider Hub Design Options

There are two ways to implement the OAM hub, depending on design requirements. As shown in Figure 30 on page 57, 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 30: OAM Tunnels - Provider Hub Design Options



Usage Notes on Provider Hub Design Options:

- An OAM provider 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 provider hubs for redundancy and to ensure no loss of management or monitoring of the on-premises devices.
- When a spoke site is multi-homed to multiple hub devices, one OAM tunnel should terminate on each hub. There is no configuration needed in CSO other than configuring multi-homing and specifying the two hubs. CSO automatically terminates one OAM tunnel on each hub device.
- On-premises devices behind NAT are supported for hub-and-spoke and dynamic mesh deployments.

4

CHAPTER

NGFW Solution

IN THIS CHAPTER

NGFW Deployment Architecture

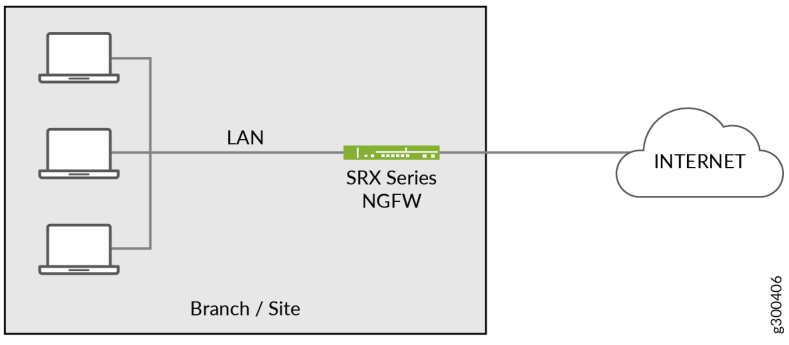
IN THIS SECTION

This topic describes the next-generation firewall (NGFW) deployment architecture for standalone NGFW using SRX Series Security Gateways.

NGFW Architecture

The NGFW architecture offers strong security services for remote sites, along with WAN connectivity. When you use an SRX Series Firewall at an on-premises spoke site as a standalone NGFW, the WAN routing functions are performed on the SRX Series Firewall itself. This architecture allows the SRX Series Firewall to perform all of its built-in security functions (such as firewall and NAT) while providing visibility into the LANs that exist at your spoke sites. Figure 31 on page 59 shows an SRX Series Firewall connected to both the WAN and an onsite LAN.

Figure 31: NGFW



As mentioned previously, an NGFW site can exist on its own or be extended later with the addition of EX Series LAN switches or Virtual Chassis at any time after provisioning and deployment.

NGFW Devices

SRX Series Firewalls can be used as standalone firewalls, managed by CSO in the customer LAN. CSO supports the use of SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, and SRX4200 Security Gateways as well as the vSRX Virtual Firewall for this purpose. In this 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.

NGFW Deployment Usage Notes

With an NGFW deployment you can:

- **Enable WAN connectivity for sites**—When you provision NGFW service capabilities for a tenant, any site belonging to that tenant can use the NGFW device as its WAN link back to CSO.
- **Enable automatic LAN connectivity**—The NGFW device can provide addressing for a connected LAN by using a built-in DHCP server.
- **Create custom application signatures in firewall policies**—CSO supports custom application signatures in firewall policies, in addition to the existing support in SD-WAN policies.
- **Create customized IPS signatures, static groups, and dynamic groups**—You can create, modify, or delete customized intrusion prevention system (IPS) signatures, IPS signature static groups, and IPS signature dynamic groups. In addition, you can clone predefined or customized IPS signatures, static groups, and dynamic groups. You can then use the IPS signatures, static groups, and dynamic groups in an IPS profile that can contain one or more IPS or exempt rules.
- **Import policy configurations**—CSO supports the import of policy configurations from next-generation firewall devices. The following features are supported:
  - Manage next-generation firewall sites for enterprise customers with brown field deployments.
  - Discover existing policy configuration while onboarding NGFW devices (without enabling ZTP).
  - Import policy configurations from Firewall and NAT policy pages.
  - Deploy policies after import into CSO.

You enable an NGFW deployment in CSO by using the Customer Portal to add an NGFW site. A tenant assigned to the NGFW site must have the NGFW service available. To add the NGFW service, a tenant administrator includes the NGFW service in the tenant configuration during the onboarding process.

5
CHAPTER

Network Operation

IN THIS CHAPTER

Network Operation

IN THIS SECTION

When deploying CSO as an on-premises deployment, it is helpful to know how the network operates and what protocols are in use. When working with a cloud-hosted deployment, the concepts are all the same, but the details and control are invisible to subscribers; they are the responsibility of the team that installs CSO in the cloud.

As with most networks, the Contrail SD-WAN solution generally operates in two planes:

- Control plane – OAM and routing traffic
- Data (forwarding) plane - user traffic

Control Plane Operation

The control plane for the Contrail SD-WAN solution centers around the CSO platform. More specifically:

- CSO's Network Service Controller (NSC) layer implements the control plane using vRRs.
- All sites across all tenants establish MP-IBGP peerings with the vRR.
- CSO uses a single private AS number for all tenants, with route targets for tenant separation.
- Tenant route separation is provided both by the vRR and by multi-tenant hub devices using BGP extended communities.

vRR Design

All CSO deployments include one or more vRR instances, which provide control plane functionality for the SD-WAN environment. Figure 32 on page 63 shows a general example where the on-premises devices at each site peer with the vRR.

Figure 32: Control Plane - Single vRR Design

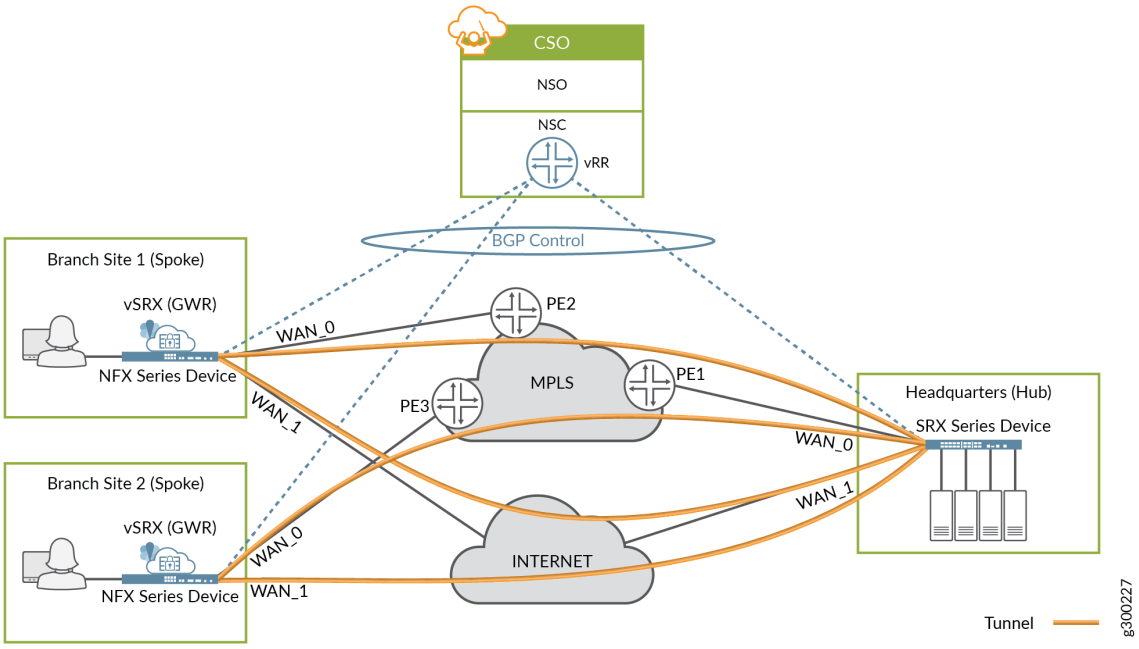
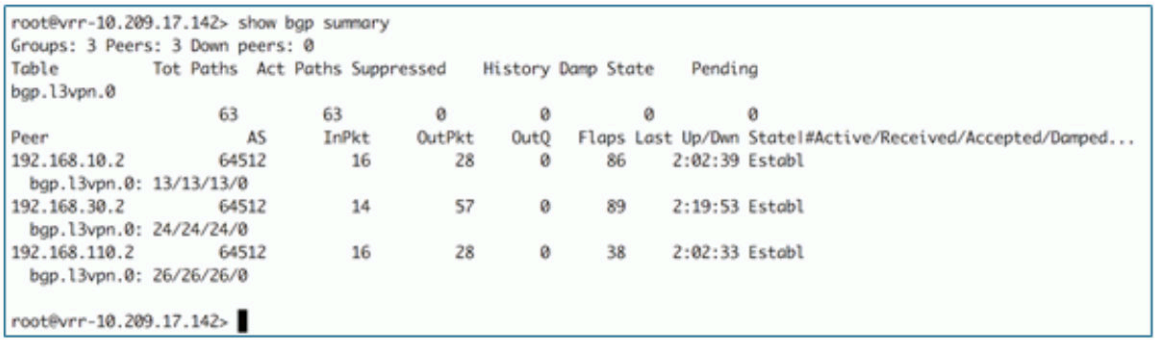


Figure 33 on page 64 shows an example of the CLI output from the vRR.

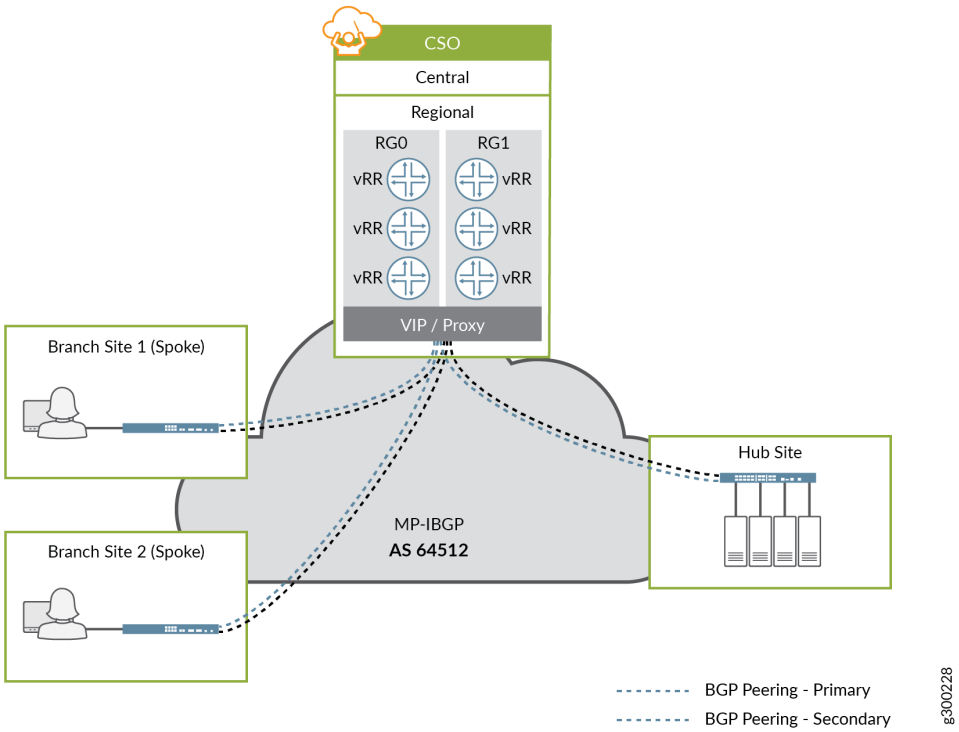
Figure 33: Sample CLI Output from vRR



Control Plane Resiliency

CSO Release 3.3 and later supports the installation of multiple vRRs to provide redundancy and scale. CSO separates the vRRs into two redundancy groups (RGs), and makes a single virtual IP address visible to the network. As part of a site's configuration, CSO establishes BGP peering sessions between the device and a vRR in each RG. If the primary vRR fails or connectivity is lost, the second vRR continues to receive and advertise LAN routes for the connected sites, thereby providing redundancy. This design is illustrated in Figure 34 on page 65.

Figure 34: Control Plane - Multi-vRR Design

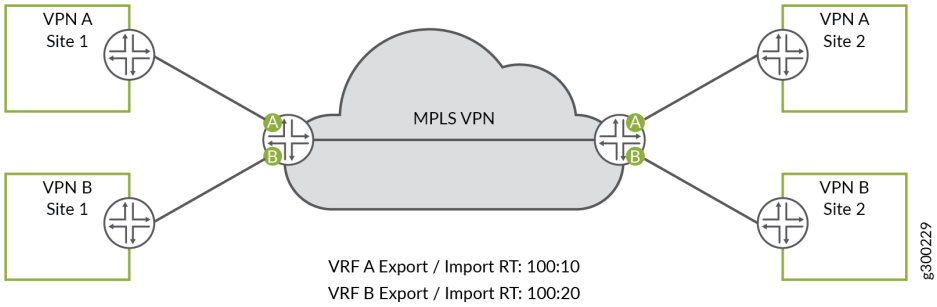


Route Distribution and Separation

The Contrail SD-WAN solution uses Junos OS virtual routing and forwarding (VRF) instances and MP-BGP route targets to provide tenant route separation and enable multi-tenancy.

These concepts can be well illustrated using an MPLS VPN environment as an example. As shown in Figure 35 on page 66, each customer is assigned a unique route target value, and all sites of the customer VPN use that route target value. When a router advertises a customer's routing information it attaches the appropriate route target value based on which customer VRF originated the advertisements. The receiving router uses the attached route target value to identify the customer VRF into which the received routing information should be placed.

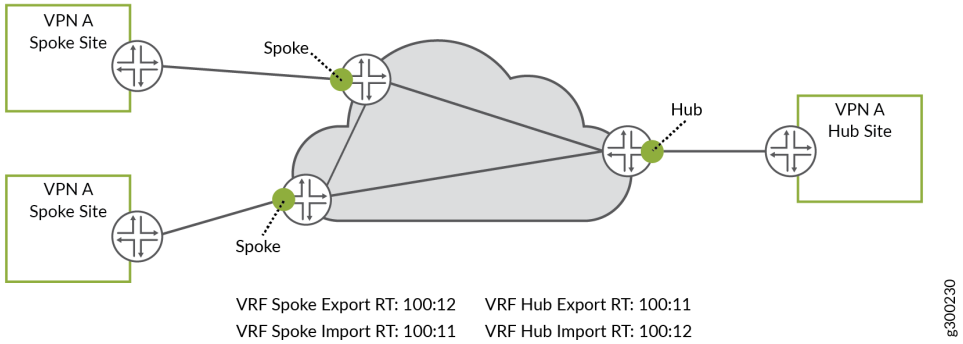
Figure 35: Route Separation Example - MPLS VPNs



An MPLS VPN hub-and-spoke environment uses route targets differently, as shown in Figure 36 on page 66. For each customer, every spoke VRF attaches the same route target value when sending routing information. The receiving router accepts routes with that same route target value and installs them into hub VRF. By contrast, the hub VRF attaches a different route target value when sending routing information, and the receiving routers accept and install routes with that same route target value into spoke VRFs.

With this setup, only the hub VRF accepts routes from the spoke VRFs, and only the spoke VRFs accept routes from the hub VRF. Using this method, the spoke sites need very little routing information (perhaps just a default route) as they only need reachability to the hub site, thereby keeping routing tables small and churn-free.

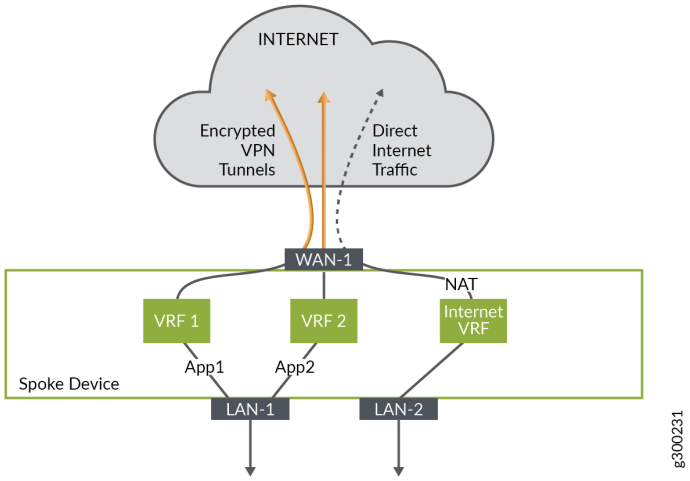
Figure 36: Route Separation Example - Hub-and-Spoke MPLS VPN



The hub and spoke example above serves as a good foundation, as the Contrail SD-WAN solution implements route distribution and separation in the same way when forwarding traffic from one site to another, or when breaking out traffic to the local internet.

Figure 37 on page 67 shows a spoke site example where the spoke device is configured with two overlay tunnels and local breakout, with all traffic flowing out the same interface. Each traffic path has its own VRF, and route targets are assigned appropriately at the spoke and hub sites to ensure proper tenant route separation.

Figure 37: Route Separation - SD-WAN Spoke Site



APBR and SLA Management - Control Plane

Advanced policy-based routing (APBR) enables you to define routing behavior and path selection per application (group). The APBR mechanism classifies sessions based on well-known applications and user-defined application signatures and uses policy intents to identify the best possible route for the application. Dynamic application-based routing makes it possible to define policies that will switch WAN links on the fly based on the application's defined SLA parameters.

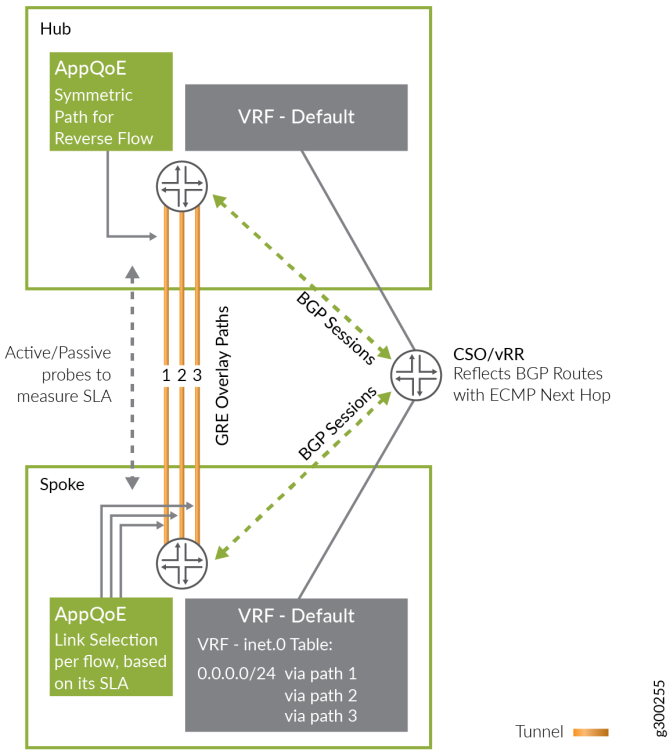
Real-Time Optimized - AppQoE

Starting with Release 3.3.1, CSO supports Application Quality of Experience (AppQoE), a data plane-level mechanism that provides better scalability and faster decision making. Working in conjunction with APBR, AppQoE functions at the device level; that is, the devices themselves perform SLA measurements across the available WAN links, and then dynamically map the application traffic to the path that best serves the application's SLA requirement. This is all done without the need for the CSO controller to distribute SLA-specific routes.

With AppQoE, when an SLA violation occurs, only traffic corresponding to the application that reported the SLA violation is moved to an alternate link; any other traffic using the link is unaffected.

With real-time optimized SLA management only the default VRF is required, as shown in Figure 38 on page 68. The default VRF uses ECMP across all the links. The next hop selection per SLA happens in the data path (described in the data-plane section).

Figure 38: Real-Time Optimized (AppQoE) Routing Architecture



In this case, the MPLS label is used only to identify the tenant.

NOTE: AppQoE is enabled when the SD-WAN mode for the tenant is set to *Real-time Optimized*. This is the default mode for SD-WAN deployments.

Note the following about AppQoE:

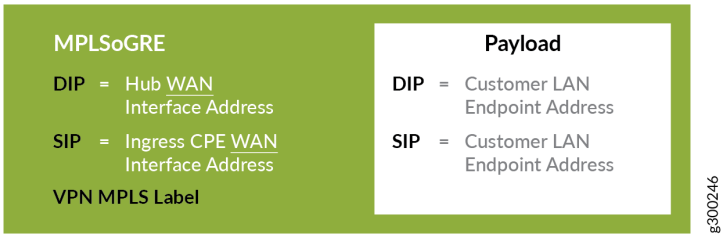
- Only supported on SRX and vSRX Virtual Firewall devices.
- Both ends must use the same Junos OS version and the same configuration.
- Multi-homing is supported.

Data Plane Operation

This section discusses how a packet is forwarded in a hub-and-spoke topology.

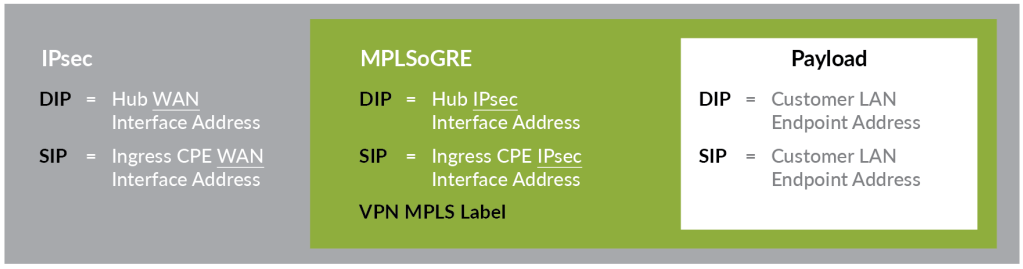
When a user at a spoke site sends traffic through the on-premises CPE device, and the packet is not locally switched or sent direct to the Internet, it is sent over a tunnel to the hub device. This packet from the customer LAN is first encapsulated inside an MPLSoGRE header with the GRE destination as one of the WAN links of the hub device. The MPLS label in the MPLSoGRE header identifies the VRF to be used for forwarding the packet at the hub site. The resulting packet header is shown in Figure 39 on page 69.

Figure 39: Packet Header - MPLSoGRE



If the tunnel between the spoke and hub site is configured to use IPsec, the MPLSoGRE packet is then further encrypted and encapsulated in an IPsec header that uses tunnel mode. The resulting packet header is shown in Figure 40 on page 69.

Figure 40: Packet Header - MPLSoGREoIPsec



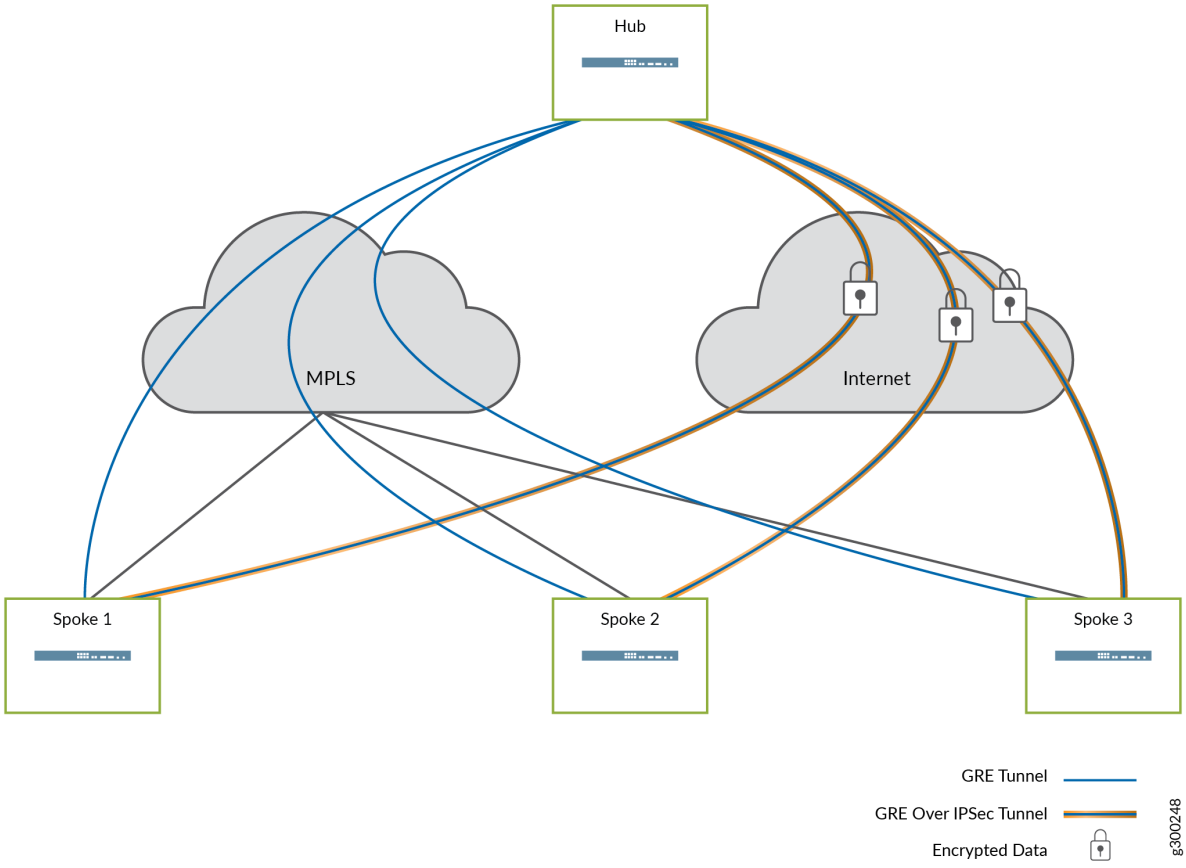
At the hub, the IPsec header is first decrypted. The resulting packet's MPLSoGRE header is used to terminate the GRE tunnel and perform a lookup in the appropriate VRF, as identified using the MPLS label. Based on the route lookup in the VRF, the packet is then either forwarded towards another spoke

site, or out of the SD-WAN environment. If forwarded to another spoke, the hub device encapsulates the packet as described as above.

Design Options

Figure 41 on page 70 illustrates how the tunnels are typically deployed using the packet headers described above. GREoIPSec tunnels are generally used over the Internet path, given the need for secure packet transport over the public network. GRE tunnels are generally used over MPLS paths, though the GREoIPSec option may also be used as appropriate.

Figure 41: Tunnel Design Options



APBR and SLA Management - Data Plane

As noted earlier, tenants can choose one SD-WAN mode of SLA management for application traffic:

- Real-time optimized – Device-level SLA management, using AppQoE

AppQoE is a data plane-level mechanism that provides better scalability and faster decision making. With AppQoE, link switching occurs at the application level in the data path of the devices; the devices

themselves perform SLA measurements across the available WAN links, without the need of the CSO controller.

Link monitoring occurs using two types of inline probes:

- Passive Probes
  - Inline probes that ride along with application traffic
  - Mimic the burstiness of the application flows
  - Enable monitoring of RTT, jitter, packet loss for the application session
  - Used to monitor currently used path for SLA compliance, detect SLA violation
- Active Probes
  - Periodic probes (based on configuration) that gather SLA data on all potential paths
  - Used to determine the original best path for the traffic
  - Used to monitor alternate paths

NOTE: AppQoE is enabled when the SD-WAN mode for the tenant is set to *Real-time Optimized*.

Tunnel Liveliness

To avoid blackholing traffic, appropriate liveness checks are enforced in the overlay network. The Contrail SD-WAN solution uses two mechanisms to ensure liveness:

- IPsec dead peer detection (DPD), where it is used
- GRE keepalives

Mesh Tags and Dynamic Mesh VPNs

As mentioned in the deployment models discussion, dynamic mesh is Juniper's resource-saving implementation of full-mesh VPNs within CSO. This section describes the operation of mesh tags and dynamic mesh VPNs that they enable.

Mesh Tags

Mesh tags are text-based labels applied to the WAN interfaces of CPE and hub devices during the onboarding process in CSO. CSO is shipped with two default mesh tags: Internet and MPLS. You can

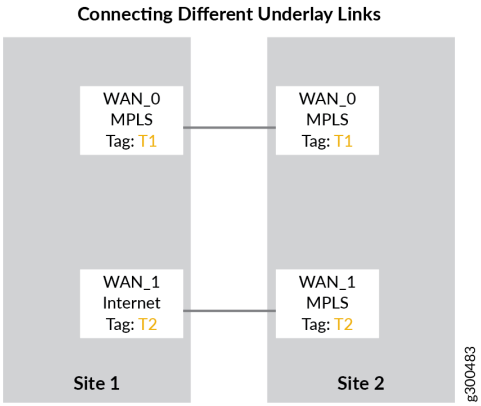
create your own mesh tags using the CSO Administration Portal. On-demand, or dynamic, VPNs can only be formed be formed between WAN interfaces that share the same mesh tag.

The following discussion explains how mesh tags work and some of the use cases to which they apply.

As mentioned above, one mesh tag is applied to each WAN interface of the CPE device at each site. On spoke devices such as the NFX150 and NFX250, and most SRX Series Firewalls, only one mesh tag can be applied to each WAN interface. On provider hub and enterprise hub devices such as the SRX4x00 Series devices, multiple mesh tags can be applied to each interface due to the increased VPN capabilities of the devices.

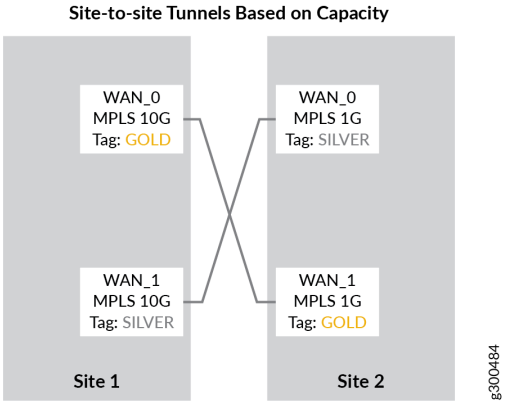
The following list helps to illustrate the various use cases in which mesh tags and dynamic mesh VPNs come into play.

- **Connecting Different Underlay Links**



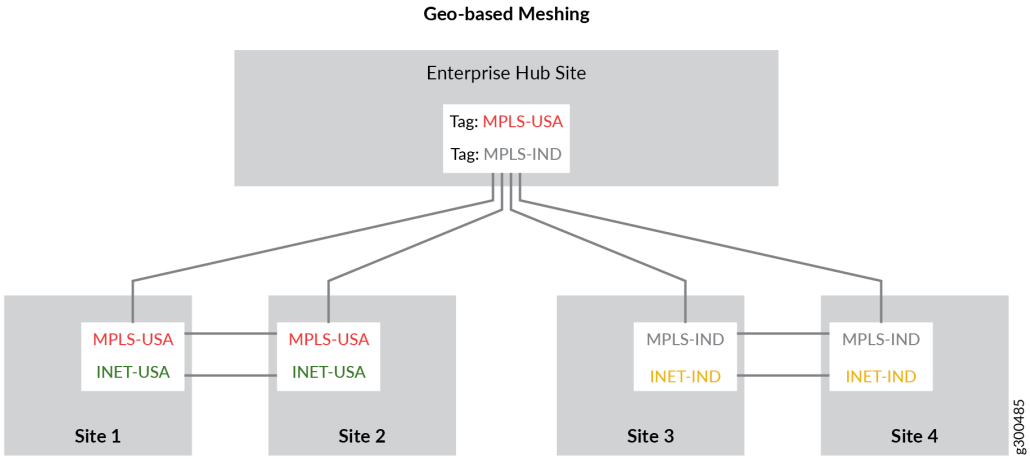
Overlay tunnel on WAN links WAN_1 on two sites can be created, even though they are of different underlay types (MPLS, Internet).

- **Site-to-Site Tunnels Based on Capacity**

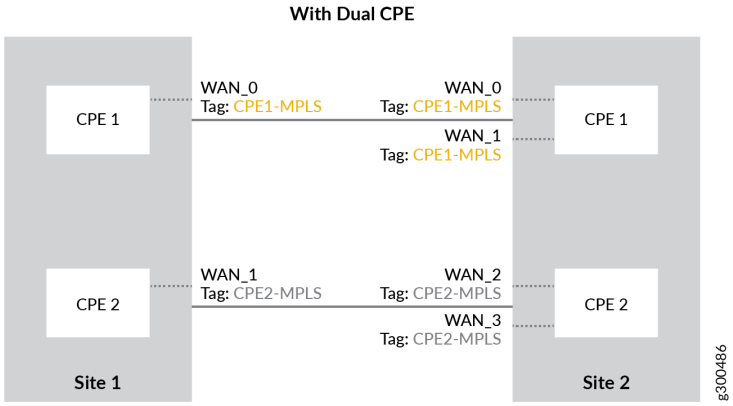


WAN links with the same capacity can be tagged with the same mesh tags.

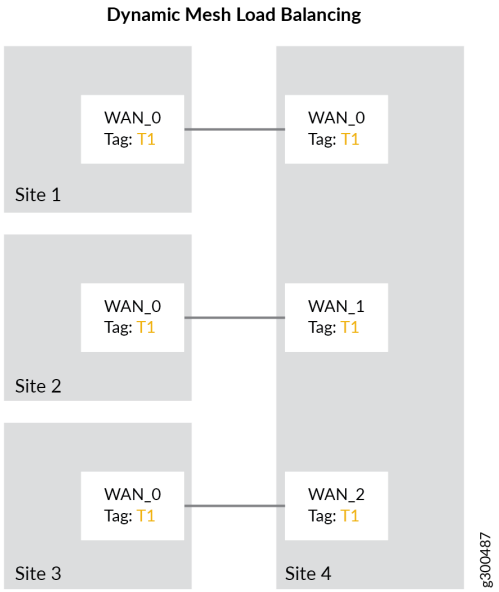
- **Geo-Based Meshing**



- **With Dual CPE**

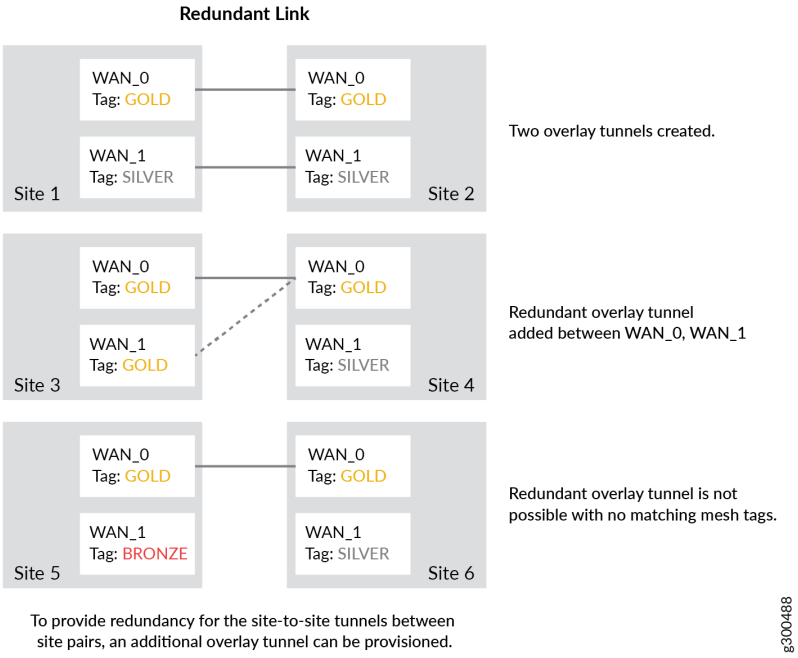


- **Dynamic Mesh Load Balancing**



If a site has multiple WAN interfaces with the same mesh tag, CSO will auto load-balance tunnels across those interfaces.

- **Redundant Link**

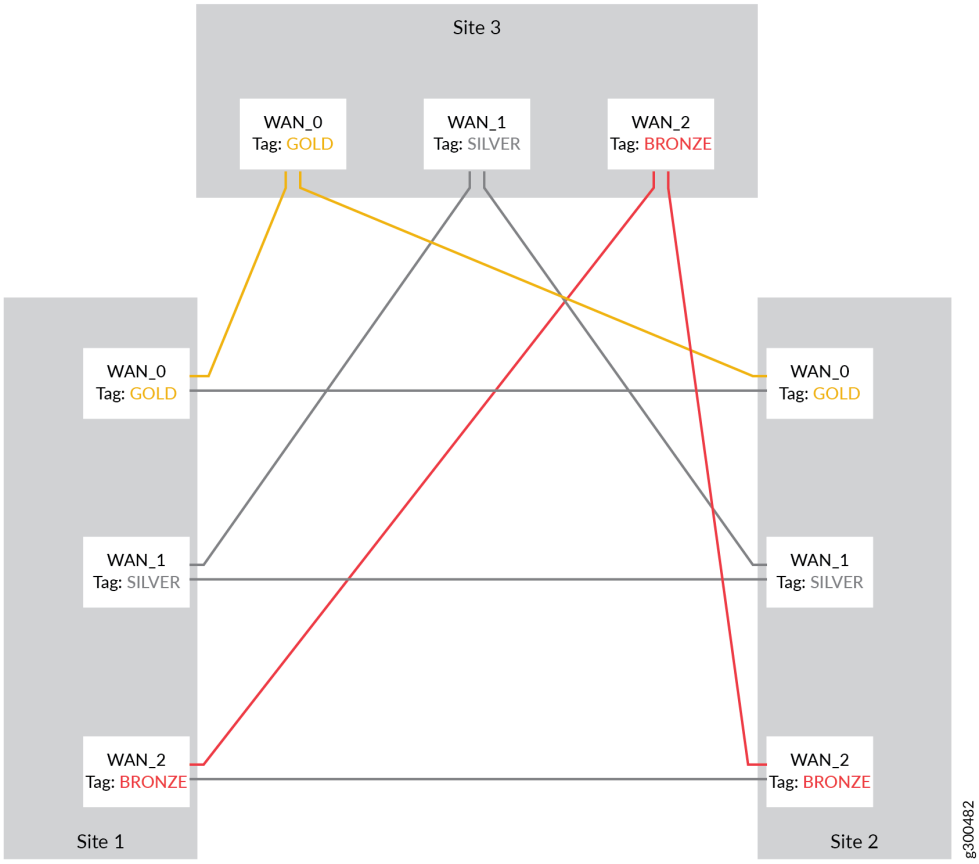


To provide redundancy for the site-to-site tunnels between site pairs, an additional overlay tunnel can be provisioned.

Dynamic Mesh VPNs

Figure 42 on page 75 shows a dynamic mesh VPN topology between three spoke sites and describes how the site-to-site VPN is brought up.

Figure 42: Dynamic Mesh Operation



1– Sites and tunnels to Hub sites provisioned using ZTP. Site to site traffic goes through the site to hub data tunnels.	4– CSO configures on-demand site-to-site tunnels between the site-pairs.
2– CSO receives syslog messages from the devices containing details about traffic rates.	5– Site-to-site traffic now switches to the newly formed site-to-site tunnels.
3– CSO recognizes that the traffic between Phoenix Site 1 and Houston Site 2 exceeds KPI thresholds.	

NOTE: Tunnel deletion is also controlled and automated by CSO using traffic thresholds and syslog messaging.

Internet Breakout

While traffic destined for the Internet can be sent across the overlay tunnels and through a central site, the tunnels are more typically intended to support site-to-site traffic. For non-SD-WAN destinations, local breakout provides the option to send the traffic out of the local on-premises device directly to the Internet. Local breakout allows the tenant to use its network bandwidth optimally at each site and to avoid incurring the cost of carrying all traffic to the central site.

Local breakout is an important feature in SD-WAN deployments, as many enterprises nowadays use SaaS services that are hosted outside the corporate network. Since most of these SaaS apps use SSL as the transport and also support single sign-on with the enterprise AAA systems, security concerns are addressed despite sending traffic directly over the Internet.

WAN Interface Options

An on-premises device's WAN (MPLS and Internet) interfaces can support tunneled and local breakout traffic in any combination:

- Tunneled traffic only
- Tunneled and local breakout traffic
- Local breakout traffic only

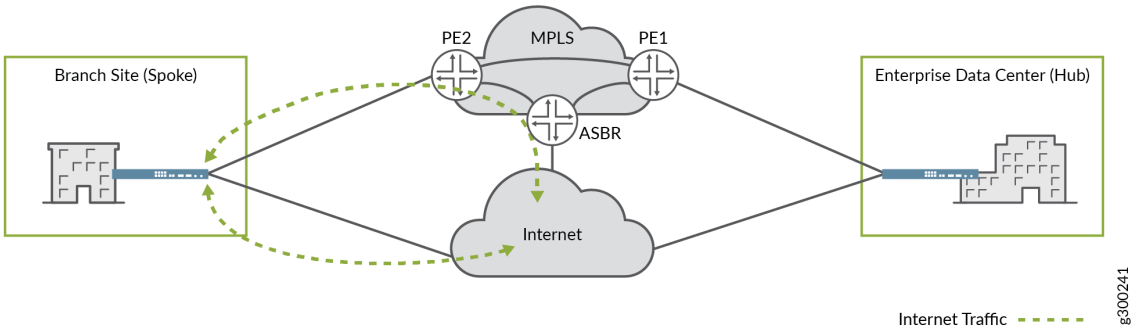
Design Options

There are multiple ways to implement local breakout, depending on design requirements.

Breakout at Spoke

Local breakout at spoke sites allows users to access the Internet directly without having to send traffic over the overlay network towards the hub, thus helping to conserve tunnel bandwidth. This option can be implemented on either the Internet or MPLS WAN links. Figure 43 on page 77 illustrates this concept.

Figure 43: Local Breakout at Spoke

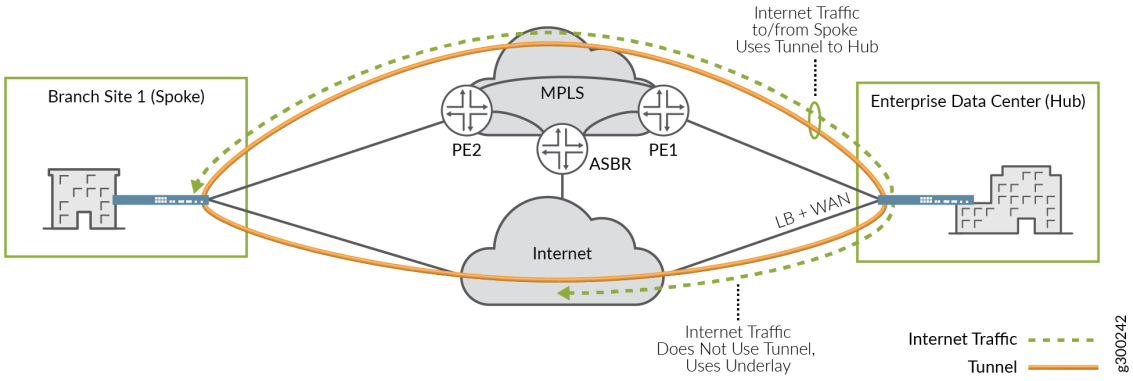


When using local breakout, you can specify either interface-based or pool-based NAT.

Breakout at Provider Hub (Central Breakout)

Central breakout at a provider hub site enables hub-and-spoke deployments where spoke sites forward Internet-destined traffic through the overlay network to the provider hub device, which then forwards the traffic out to the Internet as shown in Figure 44 on page 77.

Figure 44: Local Breakout at Hub



Central breakout at the hub site is enabled differently than at a spoke site. It can be configured manually in CSO through Stage 2 templates.

Central breakout can also be provided to spoke sites through an Enterprise Hub site. In this scenario, the enterprise hub can eithe rperform local breakout using an underlay network for forwarding or it can receive the default route from the Datacenter department and propagate it to the spokes.

When central breakout is offered at both the provider hub and enterprise hub through the default route method, the default route from the enterprise hub is preferred using BGP local preference.

Cloud Breakout

Another breakout option for Internet-destined traffic, Cloud Breakout, is available to spoke and enterprise hub sites. When cloud breakout is enabled, the spoke site or the enterprise hub site forwards Internet-destined traffic to Zscaler for further security-related processing before it is sent to the Internet. The Zscaler account must be active and accessible prior to sending traffic through the breakout.

Usage Notes for Cloud Breakout

- Generic routing encapsulation (GRE) tunnels that use public IP addresses for the WAN links are supported for cloud breakout.
- When using GRE tunnels, the CPE devices cannot be behind NAT.
- When you configure cloud breakout settings, you can specify IPsec phase 1 parameters, phase 2 parameters, and domain name.
- You can specify IP address or hostname validation for cloud breakout nodes.
- CSO auto-populates FQDN, preshared keys, and WAN link information and provides the option to change the auto-populated values.
- CSO supports high-availability between the WAN links of an SD-WAN spoke site and the cloud breakout node.
- WAN link nodes can be configured as active/passive or active/active.
- A maximum of two WAN links can be defined between the SD-WAN spoke site and the cloud breakout node.

Order of Preference for Scenarios with Multiple Breakout Options

If multiple breakout options are available to the CPE at the spoke site and there is no breakout policy specified, then the order of preference for breakout is:

1. Datacenter department/enterprise hub
2. Local breakout/Cloud breakout
3. Provider hub (Central)

If multiple breakout options are available to an enterprise hub site, the order of preference for breakout traffic is:

Without SD-WAN policy:

1. Datacenter department
2. Hub

With SD-WAN policy:

1. Local breakout/Cloud breakout
2. Datacenter department
3. Provider hub (Central)

Use Cases for Local Breakout

Some use cases for local breakout are described below.

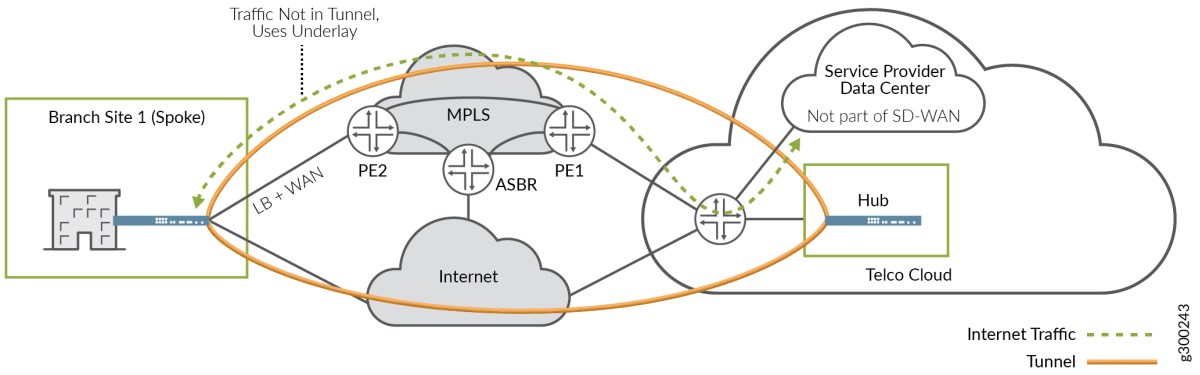
Service Provider Data Center

In this use case, the Enterprise customer uses the service provider's SD-WAN service for site-to-site inter-connectivity. The customer also uses value-added services hosted out of the service provider's data center.

At the spoke site, the on-premises device's MPLS-facing WAN interface is configured to support both tunneled and local breakout traffic. As shown in Figure 45 on page 79, traffic flows across the network as follows:

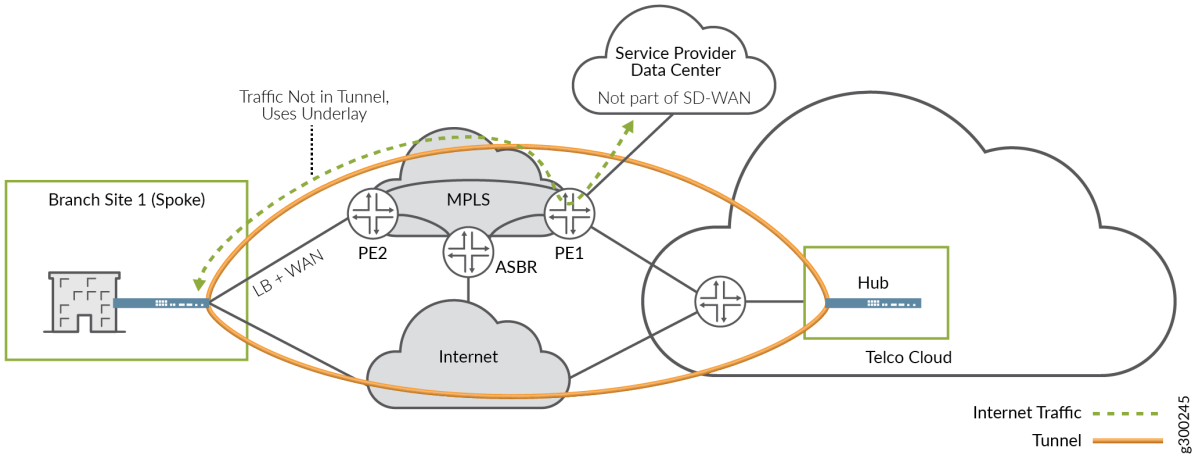
- Inter-site (SD-WAN) traffic travels across the MPLS network using the overlay tunnel.
- DC-destined traffic uses local breakout and travels directly across the underlay MPLS network.

Figure 45: Local Breakout at Spoke to DC Located in Telco Cloud



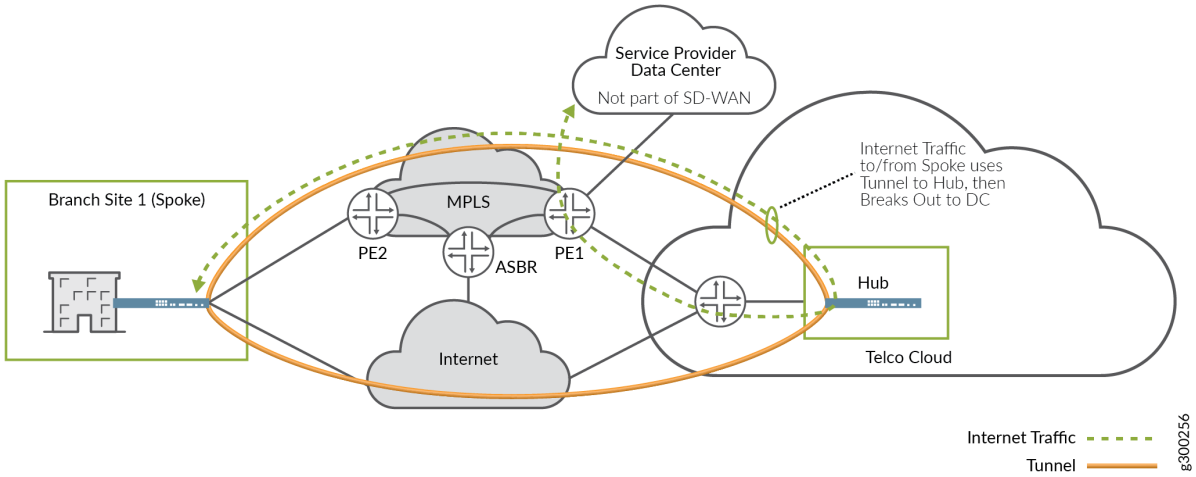
As a variation on this scenario, the data center could be located elsewhere on the MPLS network, perhaps at a POP, as shown in Figure 47 on page 80. in this case, traffic flows remain generally the same as above.

Figure 46: Local Breakout at Spoke to DC Located at POP



As another variation on this scenario, DC-destined traffic could use the overlay tunnel, breakout at the hub device, and double back to the DC, as shown in Figure 47 on page 80.

Figure 47: Local Breakout at Hub to DC Located at POP



This option has some drawbacks:

- It uses more tunnel bandwidth.
- It may increase latency as the on-premises device at the spoke site processes and encapsulates more traffic.

- It increases the load on the hub device.
- It creates a suboptimal path, causing traffic to flow through the tunnels to the hub device, only to have to double back to get to the DC.

However, it also has some advantages:

- Using the overlay tunnels, DC-destined traffic can take advantage of SLA services and choose the best path dynamically, thus improving network performance for those applications.
- Additional security functions can be offered centrally.

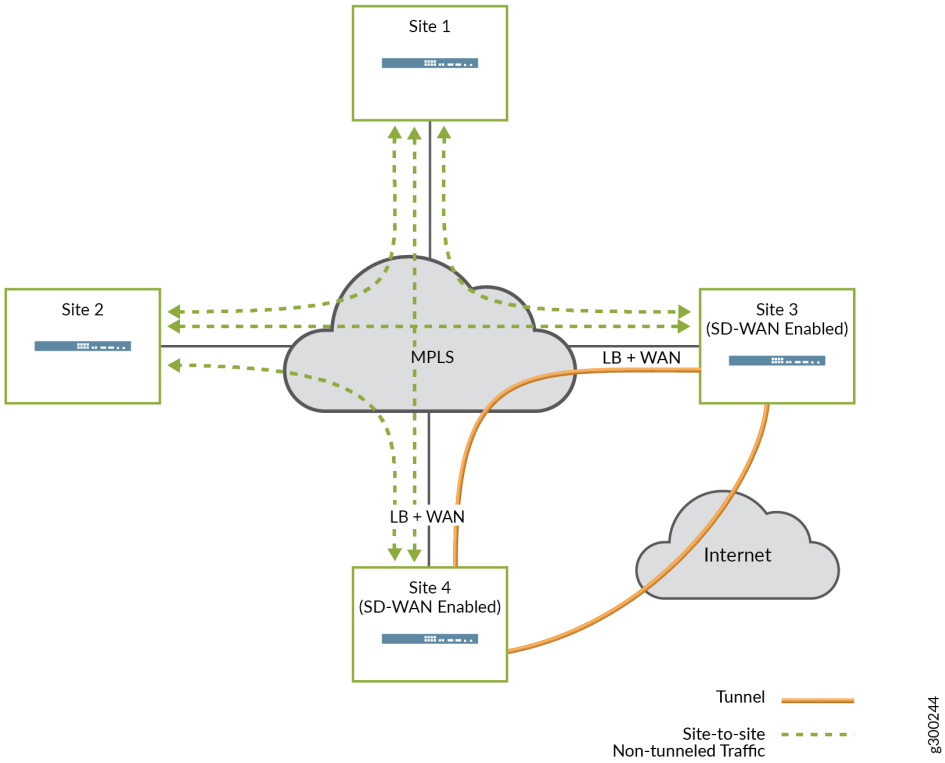
Migration to SD-WAN

In this use case, the enterprise customer has multiple large locations and uses the service provider's existing MPLS service to provide a full mesh between sites. The customer wants to migrate to SD-WAN, and the implementation is likely to be incremental. Nevertheless, it is critical to maintain connectivity between sites at all times.

Figure 48 on page 82 illustrates a scenario where the migration is underway. SD-WAN functionality has been added to Site 3 and Site 4, while the other sites have not yet been migrated. At each SD-WAN-enabled site, the on-premises device's MPLS-facing WAN interface is configured to support both tunneled and local breakout traffic. Traffic flows across the network as follows:

- Traffic between the SD-WAN-enabled sites can use the overlay tunnel.
- Traffic between an SD-WAN-enabled site and a legacy site uses local breakout and travels directly across the underlay MPLS network.

Figure 48: Local Breakout to Support Migration to SD-WAN



In this case, local breakout is the key to maintaining connectivity between the migrated sites and legacy sites.

Local breakout and NAT

When traffic flows from a tenant VRF to the Internet, NAT must typically be used to translate from the tenant's private network space to the Internet (public) network space.

At spoke sites, the on-premises devices can use Auto-NAT to automatically perform source NAT on all local breakout traffic. At hub sites, Auto-NAT is not available; however, the CSO UI supports manual creation of NAT rules for these on-premises devices.

Local Breakout and DNS

Configuring an on-premises device as a DHCP server for LAN segments allows you to specify DNS server information for end hosts. For a site with local breakout enabled, it is generally recommended to specify more than than one name server: an internal server for corporate domain name resolution, and a public or ISP server for Internet-destined local breakout traffic.

Network Security

One of the important security considerations for SD-WAN architectures is providing security for data not only at rest, but also in motion. Data security has been enhanced to allow for the use of multi-level PKI for the data and OAM tunnels. This allows CSO to receive multi-level CA certificates from a CA server, push multiple CA certificates to CPE devices, renew and revoke mulitple CA certificates on CPE devices.

CSO supports simple certificate enrollment protocol (SCEP), starting with CSO release 4.1. This allows CSO to:

- Act as SCEP server
- Act as SCEP cllient
  - Certificate revocation
  - Certificate auto-renew
- Deploy certificates to a CPE/site
- Manage certificates on CPE (site)
- Provide GUI support for CA Server information
- Site/CPE certificate renewals
- Microsoft CA/NDES support
- Broker certificates for each site/CPE

A back-end API is provided for programmatic access to PKI features.

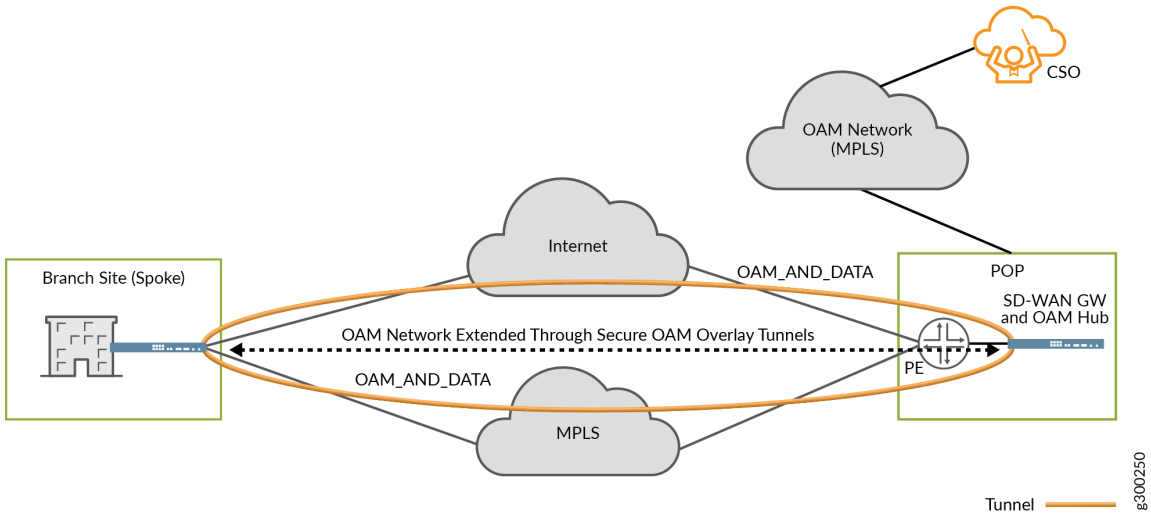
Data Plane

Data plane connections can be configured to use IPsec with PKI-based authentication. When used, the local on-premises device encrypts traffic before transmitting it over the network to the remote site and authentication is handled with public-private key pairs.

Management and Control Plane

CSO connects to and configures on-premises devices using SSH for console and NETCONF connections. Starting with CSO Release 4.0, dedicated OAM overlay tunnels help to enhance secure, end-to-end communications between on-premises devices and CSO. IPsec-encrypted and PKI authenticated OAM tunnels, shown in Figure 49 on page 84, enable on-premises spoke 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 49: Management and Control Plane Security - Secure OAM Network



For more detail, see the "Secure and Redundant OAM Network" on page 54 section earlier in this guide.

CHAPTER 6

Orchestration and Management Within CSO

IN THIS CHAPTER

Orchestration and Management Using CSO

IN THIS SECTION

The following management and orchestration information pertains to the hardware, software, and services of the CSO platform itself. Therefore, this discussion pertains mostly to those who are implementing an on-premises deployment of CSO. While the same elements exist in CSOaaS, subscribers generally have little need to understand the concepts discussed in these sections.

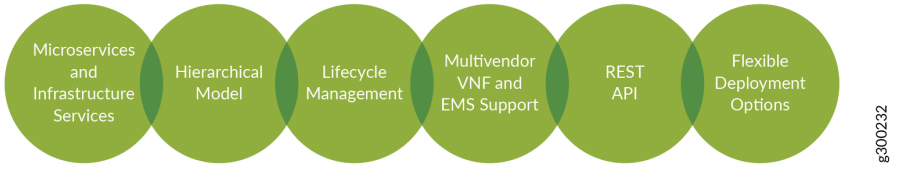
The Contrail Service Orchestration software implements SD-WAN and NGFW management and orchestration solutions. CSO is a scalable and cloud deployable multi-tenant software platform that abstracts the complexity involved in creating and managing network services. Essentially, CSO provides the automation and integration framework for the various components of the solution.

The CSO platform is metadata-driven and uses templates to represent network and resource services. It uses *intent-based policies*, designed to translate the higher-level business rules such as, “send traffic type a, destined for endpoint b, across link c” into repeatable actionable tasks and executes them under the control of a flexible orchestration engine.

Architecture

Some key characteristics of the CSO architecture are shown in Figure 50 on page 86.

Figure 50: CSO Architecture Characteristics



These characteristics include:

- Container-based, microservices architecture that allows each functional component to be independently deployed and scaled
- Hierarchical central-regional services that can support a large number of network elements (VNFs, PNFs, etc.) across multiple geographical locations
- An orchestration platform to allow full lifecycle management of network devices and virtualized network services, as well as monitoring and visualization
- Open, plugin-based, multi-vendor VNF and EMS support
- Standards-based REST API for OSS/BSS integration
- Flexible deployment options such as on-premises, public cloud, and private cloud.

Orchestration Layers

CSO software is built with multiple layers of abstraction for usability and scalability, as shown in Figure 51 on page 87. The platform implements these layers using orchestration software and controller software.

Figure 51: CSO Orchestration Layers

The Service Orchestration Layer contains the Network Service Orchestrator. The orchestration software has a global view of all resources, including both virtual network functions as well as physical devices.

The orchestration software also enables tenant management, providing end-to-end traffic orchestration, visibility, and monitoring. In addition, Enterprise customers can login to a Customer Portal to enable and manage their own set of services on demand.

The Domain Orchestration Layer contains the Network Service Controller. The orchestration software works together with the controller to manage on-premises (CPE) devices. The controller provides

topology and CPE lifecycle management functionality; it also monitors device and link status, and passes this information to the orchestration layer.

The two layers are connected using standard Web-based REST APIs, and both the orchestration layer and the controller layer expose their own sets of APIs, which can be used by any external OSS system to integrate with CSO.

Infrastructure Services and Microservices

CSO uses a fully distributed, docker container-based microservices architecture. The platform consists of several infrastructure services and microservices, which are deployed across the central and regional nodes. Each of these microservices can be independently scaled and deployed, to enable the overall system to scale as needed.

For HA deployments, multiple sets of microservices can be deployed to allow for the failure of orchestrator components. An overlay connection is used between the sets of services to allow for seamless communication of microservices.

Some important microservices include:

- **Tenant site and service management (TSSM)**: Provides APIs for tenant, site and service management
- **VNF manager**: Provides APIs to manage virtualized networking services
- **Intent-based Policy and SLA management (PSLAM)**: Provides policy and SLA profile object management service to enable SD-WAN functions.
- **Routing manager**: Provides APIs to manage routing operations such as creating VPNs, interfaces to vRRs, enabling routing on CPE devices, etc.
- **Telemetry**: Provides APIs used by fault monitoring and performance monitoring system for collecting service check results from telemetry agents.
- **Activation service**: Provides network activation functions to enable zero touch provisioning of devices.

NOTE: Installation and upgrade of CSO do not apply to CSOaaS. The information on microservices can be found in the CSO Installation and Upgrade Guide which is specific to the latest on-premises version of CSO which is 5.1.0

Platform Characteristics

IN THIS SECTION

Multitenancy with RBAC

The CSO platform has built-in multitenancy support, enabling multiple tenants to coexist on the system. Multitenancy is based on the OpenStack Keystone model. In this model, each object in the database belongs to a specific tenant and is assigned a tenant ID. When an administrator is granted certain roles to a specific tenant, he or she is authorized with certain rights to all objects belonging to that tenant.

The server enforces multitenancy RBAC at the API level. A user must authenticate with CSO's Identity and Access Management (IAM) microservice to acquire the access token first before any CSO APIs can be invoked. On each API call, the API server enforces the multitenancy RBAC by making sure the object's tenant ID matches the assigned tenant IDs in the access token, and the REST URI is defined in the assigned roles.

RBAC in CSO is object-based. To simplify RBAC application, CSO has pre-defined user roles which provide users assigned to those roles read-only or read-and-write access to specific objects. Custom roles allow administrators to grant users additional access privileges to those or other specific objects.

High Availability and Scale

As noted above, the CSO installation architecture for small environments does not provide HA. The small setup includes one instance each of a central VM and a regional VM; any VM failure renders CSO non-operational. CSO can also scale out for larger environments, using multiple servers with load balancing between them. These servers typically work in active/active HA mode, and services are duplicated across servers. The loss of a server does not impact CSO functionality.

A key design principle is that there is no in-memory state. All the states are transactional and maintained in a database using a Job Manager. CSO ensures that if a node fails, the Job Manager automatically detects the incomplete job and assigns the process to an alternate server for processing.

All CSO infrastructure services, such as database services and message buses, use proven open source software that supports multi-node clustering for HA and scale. These infrastructure service clusters are fine tuned for large scale deployment. The primary CSO configuration and analytics database is built on Cassandra, which is known for its scalability and fault tolerance on commodity hardware and in cloud environments.

All CSO microservices are stateless and do not hold any state between API calls. The application states are kept in the database. Microservices communicate with each other only through RESTful APIs or the highly available message bus. Microservice RESTful APIs are designed to be idempotent (making the same call repeatedly produces the same result) and highly fault tolerant over commodity hardware or cloud environments. CSO microservices are packaged as Docker containers and orchestrated by Kubernetes. Because of the stateless nature and idempotent APIs, each microservice can scale linearly and independently. Kubernetes allows each microservice to scale up and down automatically based on CPU usage. Kubernetes can also monitor the health of CSO microservice instances, and auto-heal failed instances.

The CSO platform can be deployed on-premises, or in a hybrid or public cloud infrastructure. When deployed across multiple availability zones of the public or private cloud, the platform can survive power and network failures across centers.

Programmability and Integration

All CSO microservices make their functionality accessible via RESTful APIs. Some of these APIs are meant for consumption by other microservices or applications running on CSO, but most are exposed to be consumed by external systems, such as northbound OSS/BSS applications. This allows providers and end customers to automate various tasks, processes, and workflows by invoking these APIs from scripts or backend systems. All microservice APIs are generated from data model descriptions in YANG and can be categorized at a high level as:

- CRUD APIs to create, read, update, and delete resources in the system. These are synchronous APIs that return status and details using HTTP. The caller can define a tenant topology, add or delete sites to this topology, enable no-touch activation of devices at the customer site, setup network connections defined in the topology, enable end user configuration of on-premises devices, monitor device and link status, and more.
- RPC (Remote Procedure Call) APIs to perform operations on these resources. These are typically asynchronous APIs that return completion status and results using Advanced Message Queuing Protocol (AMQP) notifications. The caller can specify an exchange and a routing key for the response message, and the CSO microservice will publish the result notification to that exchange using the specified routing key.

CSO microservices also publish various messages to certain documented exchanges created in the AMQP server, including various resource state change events and alerts. External systems can consume these messages and perform various tasks, thus allowing them to create event-driven automation tasks. One can configure new rules in the FMPM microservice to generate specific alerts and also post alerts on different message buses like Kafka.

The APIs exposed by CSO can be categorized as shown in Table 8 on page 91.

Table 8: CSO APIs

Catalog management	APIs to manage network service descriptors and VNFs
VIM/POP Management	APIs to create define and manage VIM and POP data centers
Topology Management	API to insert and manage end-to-end CPE service topology (logical)
Site/Customer Creation	APIs to manage customer/site objects and association with service topology nodes.
Network Design APIs	APIs to define virtualized services and service chains
Site Activation	APIs to notify vCPE/uCPE device deployment, topology and service placement.
Identity Management	APIs to manage Identity for both enterprise and service provider users
Bootstrap Service	APIs for configuration and management device activation service

Service Placement/Instantiation	APIs to position and manage service chains in customer topology
Device and Service Monitoring	APIs to monitor status of devices, network services, and services topology
Root Cause Analysis/ Troubleshooting	APIs trace and correlation engine for events, alarms and logs
Zero touch and Device Management	APIs for activating, provisioning and managing NFX/SRX
Image Management	APIs to manage NFX, SRX, EX, and EX VC software images
SD-WAN	APIs for link provisioning, auto-VPN, discover-VPN, distributed routing
Abstracted Routing	APIs for creating L2/L3 service chains
Public Key Infrastructure (PKI)	APIs for working the PKI security features

For detailed list of APIs, see Contrail Service Orchestration API Reference.

Extensibility and Customization

CSO is architected to allow easy extension and customization of its microservices. These capabilities can be categorized into three main building blocks:

- **Plugin-based architecture:** Various microservices, such as EMS, FMPM, VNFM, Flex, etc., have a plugin-based architecture to allow their behavior to be extended and customized using plugins that can be created and installed without requiring any code changes in the microservice itself. These microservices ship with a certain set of plugins, and new plugins can be created and added in the field.
- **Customization of site connectivity topology and activation workflows:** For every site, the WAN-side connection topology, as well as the configuration deployed to the on-premises device(s) during its activation are modeled as device templates. These templates can be modified, or new ones created, in the field to customize the activation workflows and configurations based on each service provider's unique requirements.

Telemetry and Analytics Capability

An important capability of the CSO platform is its ability to collect telemetry data from different devices/VNFs and use it to:

- Store as time series data and make the data query-able from Northbound Applications and the CSO UI to display as charts and graphs.
- Create events for microservices to be able to react to. For example, SLA metrics collected from the devices are published to analyze for link SLA violations, so that the relevant applications can take the appropriate action.
- Publish selected data to Northbound listening applications over Kafka and RabbitMQ.

CSO uses Contrail Analytics nodes to store time series data. Contrail Analytics by itself is a horizontally scalable component that provides high availability as well as the ability to query data through REST APIs. The data from the time series is exposed through CSO APIs to the UI and Northbound applications.

Intent-Based Policies

CSO's user interface puts a strong focus on simplifying and automating many of the main functions an operator needs to perform. This simplification is enabled by modeling enterprise objects and using intent-based policies to configure them.

Intent-based policies allow an operator to configure policies using constructs such as departments, sites, site groups, and application groups. The policy is applied to all relevant devices that match the parameters specified in the matching construct; the operator does not have to worry about configuring the policy explicitly on the devices.

Intents can be expressed as part of various workflows, as described below:

- **Site Onboarding**–During site or hub onboarding, the following intents can be specified:
  - Default link - tenant admin can choose a default link; used as the default overlay path for all traffic which doesn't have a policy saying otherwise.
  - Application breakout - enables site administrators to designate that certain application traffic be routed directly to the Internet from the spoke site.
  - Central breakout - enables Internet-destined traffic to break out directly to the Internet at the enterprise hub.
  - Department breakout - enables site administrators to designate that all Internet-destined traffic from a specific local department be routed directly to the Internet from the spoke site.

- Hub breakout - enables site administrators to designate that all Internet-destined traffic be route directly to the Internet from the provider hub device.
- Site group - allows the same policies to be deployed across a group of sites with similar characteristics.
- Site local Internet breakout - enables site administrators to designate that all Internet-destined traffic be routed directly to the Internet from the spoke site.
- Zscaler breakout - Allow all Internet-destined traffic to be routed to a Zscaler implementation prior to going to the Internet. This breakout can be done locally, centrally, or at the provider hub.

NOTE: Although the above intents can be specified during the site onboarding process, they are not applied until after ZTP.

- **SD-WAN Intent Policy Creation**–Steering and breakout profiles can be created to be used in SD-WAN policies.

  Two types of profiles are supported:

  - Path-Based Steering Profile – operator explicitly specifies a preferred path for traffic. Traffic matching an SD-WAN policy using this profile will take the preferred path.
  - Breakout Profile - operator specifies a breakout type of either, local breakout using underlay networking, backhaul using hub sites for breakout traffic, or local breakout using a cloud-based platform such as Zscaler. The operator also specifies a traffic type profile and preferred path for the breakout traffic. If a WAN link type that matches the preferred path is available at the CPE and enabled for breakout, then the traffic will use that link for breakout traffic. If *any* is selected as the preferred path, then CSO will use all available links that are enabled for breakout in a load-balancing fashion.

An SD-WAN policy can be created by specifying the following elements:

- Source endpoint(s) - site groups, departments
- Destination endpoint(s) - application/application groups
- Action - Steering profile or breakout profile

The operator simply needs to select these high-level elements from the available drop-down menus, and then deploy the policy. CSO takes care of translating these intents into configurations that are pushed to the relevant network devices.

Security Intent-Based Policies

To create firewall policies, the operator does not need to specify the location and connectivity information of the endpoints; instead, CSO uses existing topology information to determine how the relevant endpoints are connected and creates the appropriate security policies to be deployed to the appropriate policy enforcement points.

Firewall policy intents can be defined using the following elements as source and destination identifiers:

- Site
- Department (SRX security zone: Up to 25 departments supported starting in CSO version 4.1)
- Application (L7: signature based)
- Services (protocol based)
- Address objects representing hosts, networks, IP ranges, etc.

Firewall intents are order insensitive, meaning the operator does not have to arrange the intents in the proper order. CSO analyzes all firewall intents and converts them to security policies statements in correct order.

Upgrade and Backward Compatibility

CSO supports seamless upgrades from previous versions, including infrastructure services and microservices upgrade, data migration, device connectivity, and configuration.

The upgrade procedure is an 'offline' activity; all microservices are shut down while the upgrade is in progress. However, network devices (CPEs, hubs, etc.) and the SD-WAN environment overall continue to function normally.

The CSO data model and APIs maintain backward compatibility such that latest version of all CSO microservices support (read/write) data created by previous versions. Migration scripts/additional workflows can also be executed as part of the upgrade process.

Element Management

CSO includes a set of microservices that provide scalable, multi-vendor element management capabilities. These capabilities are used to provide SD-WAN services by managing, orchestrating, and controlling the physical and virtual networking devices that make up the overall solution.

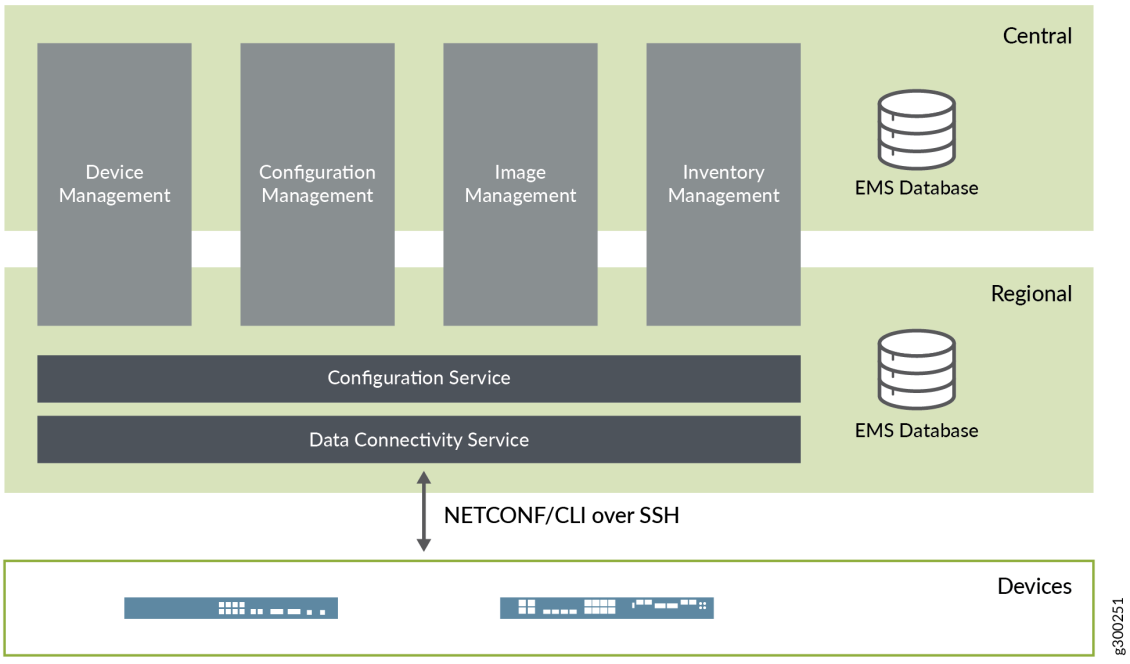
These devices can generally be brought under CSO management in two ways:

- If the device is already provisioned, it can be discovered by CSO and brought under its management by providing the device's management IP address and admin account credentials. A provider hub device located in a service provider POP is typically discovered using this option.
- For devices that need to be automatically brought online and provisioned, CSO employs a zero-touch mechanism to bring the device under its management. By providing the serial number of the expected device at each site, CSO creates a device object in its database corresponding to each device and prepares the image and configuration that needs to be delivered to it. When the device arrives at the site and is racked up and powered on, it will reach out to the Juniper redirect service (https://redirect.juniper.net) to learn how to reach its regional CSO instance. Upon contacting the CSO server, the device receives an assigned software image and initial configuration. Once up and running, CSO performs further actions on the device, such as bringing up required VMs, provisioning overlay tunnels, installing a telemetry agent, etc.

CSO interacts with network devices using NETCONF or CLI sessions over SSH, thus ensuring that all management communications use a secure, encrypted channel. CSO supports both password-based authentication as well as SSH key-based authentication to the device.

Figure 52 on page 96illustrates the various microservices that work together to provide CSO's element management capabilities, and how they are distributed across central and regional servers.

Figure 52: CSO Microservices for Element Management



Microservice	Description
Activation Service	Supports secure zero-touch activation of CPE devices through draft-ietf-netconf-zerotouch.
Device Management Service	Manages the lifecycle of devices; devices include VNFs, PNFs, CPEs, PEs, IPsec concentrators, etc.
Config Management Service	Manages the lifecycle of configuration objects, including their versioning as well as their deployment onto devices.
Image Management Service	Maintains a repository of device images and other software packages, and manages the deployment and installation of these onto devices.
Inventory Service	Takes care of discovering and managing physical and logical inventory resources on devices.
Template Service	Manages all templates on-boarded into the system, and provides APIs for rendering them using different template engines via plugins; templates can be used to generate configuration or operational commands.
FMPM Provider Service	Centralized service that maintains all FM and PM data, and provides APIs for collecting and querying the data.
FMPM Collector Service	Distributed service that is responsible for collection of FM and PM data from managed entities.
Config Service	Provides APIs to execute commands on managed devices, and acts as the gateway between all microservices and managed devices; has a plugin-based architecture to support multiple management protocols, such as NETCONF/SSH, CLI/SSH, and REST/HTTP.
Device Connectivity Service	Takes care of transport connection establishment and authentication between CSO and the managed devices.

CSO Behind NAT

CSO can be installed behind a NAT gateway. When used, managed devices can reach CSO through a publicly exposed IP address. This option is specified during initial CSO installation, and requires some additional manual configuration of NAT rules once setup is complete.

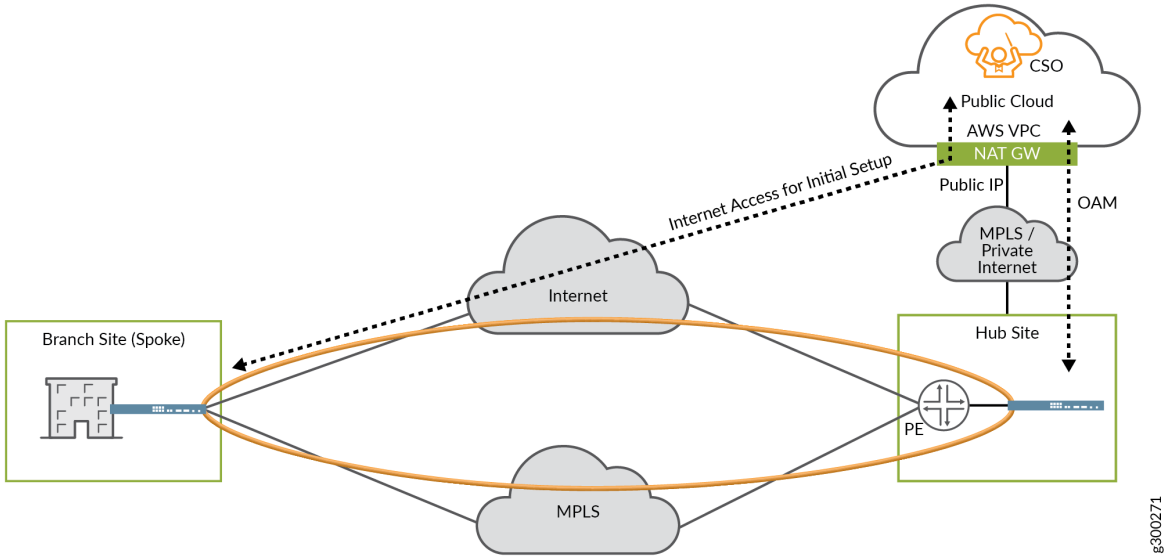
CSO in the Cloud

While CSO is often installed within the service provider's network, it can also be installed in the cloud, depending on design requirements.

CSO in Public Cloud

Figure 53 on page 98 shows CSO located in an AWS VPC and accessible through a private connection. This is known as a cloud-hosted CSO deployment. CSOaaS is based on this model.

Figure 53: CSO in Public Cloud



Implementation characteristics:

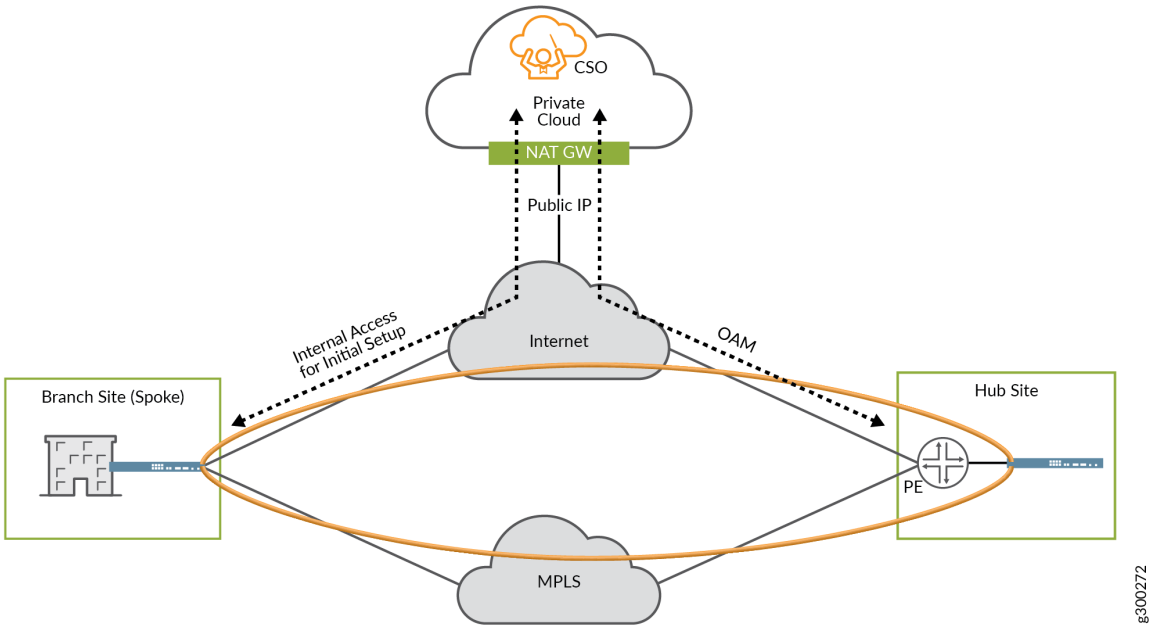
- The CSO installation uses private IP addressing.
- The NAT gateway provides a public-facing IP address for CSO.
- The connection between CSO and the hub device uses an MPLS network or a private Internet connection, such as AWS Direct Connect.
- The hub device must use a public IP address for OAM.
- The hub device's IP address must be directly reachable from CSO.

- The spoke device initiates its connection to CSO using the public IP address on the NAT gateway.

CSO on Internet

Figure 54 on page 99 shows CSO located at some other on-Internet location, such as in a private cloud, and accessible directly over the Internet.

Figure 54: CSO on Internet



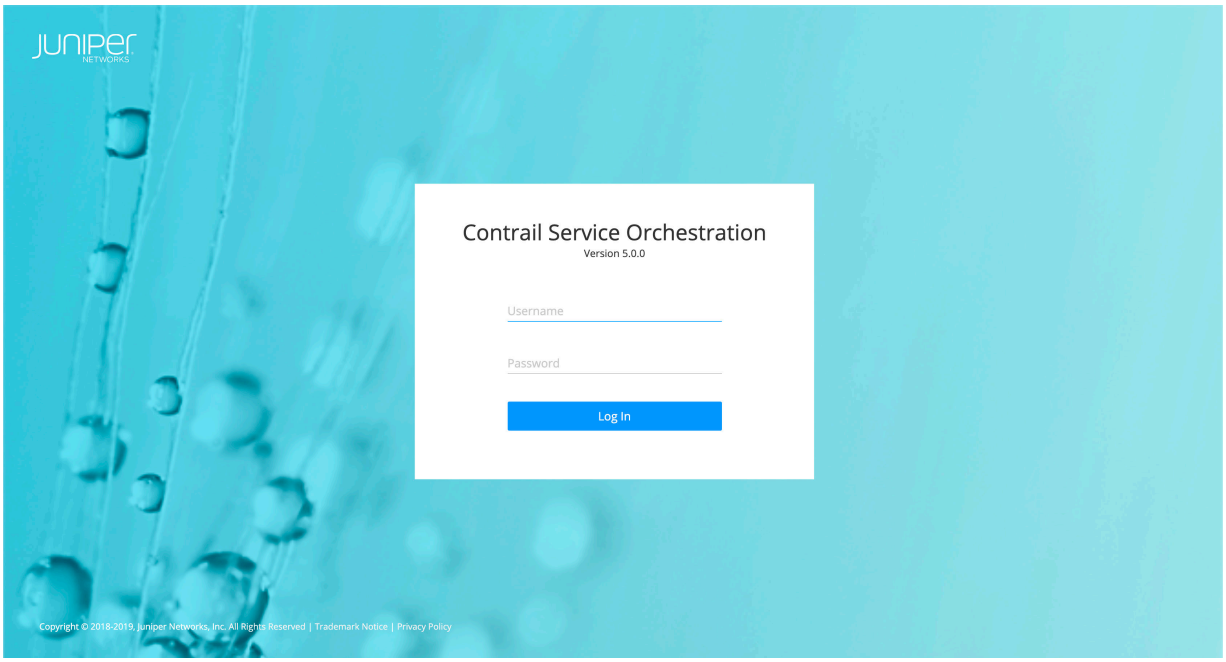
Implementation characteristics:

- The CSO installation uses private IP addressing.
- The NAT gateway provides a public-facing IP address for CSO.
- The connection between CSO and the hub device uses the public Internet.
- The hub device must use a public IP address for OAM.
- The hub device's IP address must be directly reachable from CSO.
- The spoke device initiates its connection to CSO using the public IP address on the NAT gateway.

CSO User Interface

CSO software offers a single Web-based UI to create, configure, and monitor tenants, sites, devices, network topologies, and security and SD-WAN policies. A sample screenshot of the dashboard is shown in Figure 55 on page 101.

Figure 55: CSO User Interface - Dashboard View



Web UI Architecture

The CSO Web UI uses a lightweight framework for building single-pane-of-glass user interfaces in a decoupled way. The UI allows workflows to be dynamically created from independently developed and deployed plugins, which allow the UI to be extended dynamically in a customer environment without any impact on existing functionality.

The UI architecture supports a single, unified dashboard that hosts monitoring widgets. A thumbnail view of the widgets is provided by the framework, and the operator can drag and drop the widgets to compose customized monitoring views. The UI includes a "preferences" API that can be used to read and write UI-related user preferences, such as a preferred sort order or visible subset of columns for a grid instance. These preferences are preserved across user sessions.

Personas

There are two main personas in the Web UI:

- **Service Provider admin**—global access to all operating companies, tenants, and customers; access CSO through the Administration Portal
- **Tenant admin**—customer-specific access; access CSO through the Customer Portal

Operating Companies (OpCos)

CSO Release 4.0 and later supports operating companies (OpCos) in a service provider environment.

In cases where a global service provider is required to have regional business entities to manage customers on a regional basis (for regulatory, billing, or operational reasons), the OpCo construct enables the service provider to extend their CSO platform to enable each regional entity to independently offer SD-WAN services to its own tenants and customers.

When supporting OpCos, the CSO multitenant hierarchy has three levels:

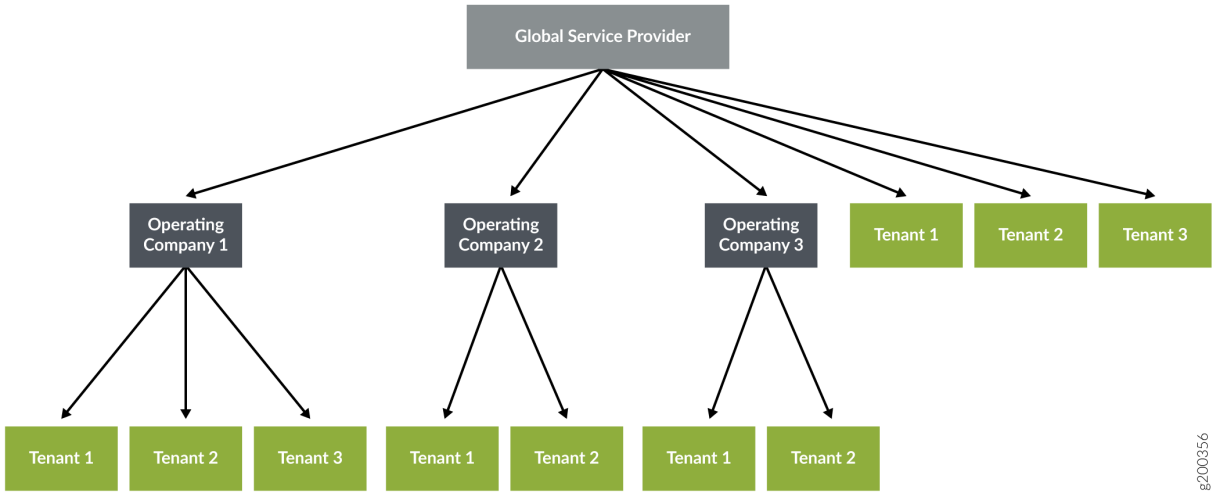
- **Global service provider**—Contains one or more operating companies and its tenants, manages resources at the service provider level, and shares common resources with operating companies and tenants.

  NOTE: In CSOaaS, there is no user access to the Global Service Provider role/hierarchy.

- **Operating company**—A region-specific service provider that can manage its tenants and provide services to them. Tenants managed by one OpCo are isolated from tenants of another OpCo.
- **Tenant**—Uses the resources provided by the global service provider or OpCo.

Figure 56 on page 103 shows the relationship between the global service provider, operating companies, and tenants.

Figure 56: CSO Multitenant Hierarchy



For more details on CSO portals, user types, and personas, see the CSO Administration Portal User Guide and CSO Customer Portal User Guide for Release 5.0.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
4.1	Up to 25 departments supported starting in CSO version 4.1
4.0	CSO Release 4.0 and later supports operating companies (OpCos) in a service provider environment.

7

CHAPTER

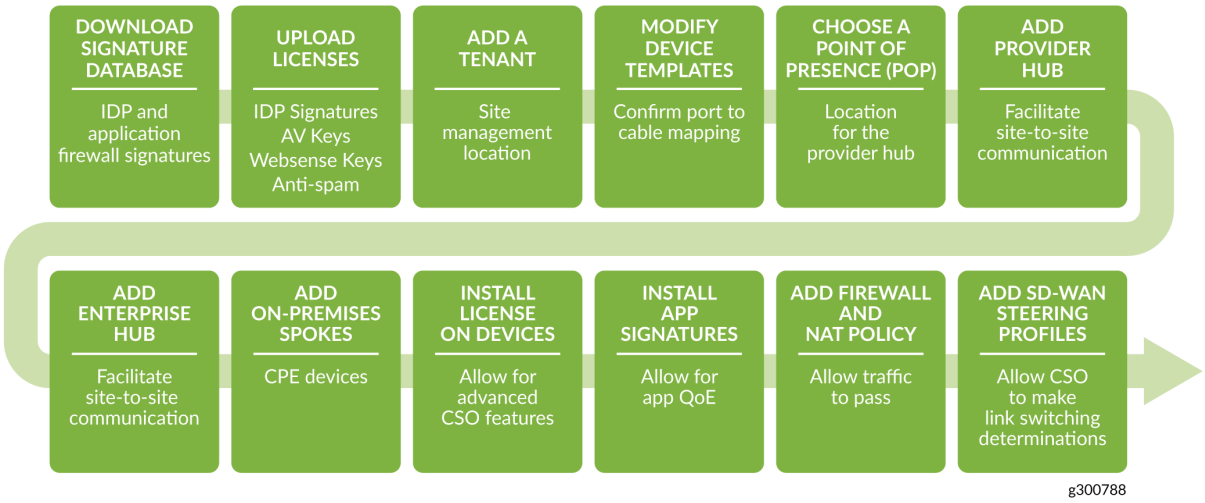
Operational Workflows - Overview

IN THIS CHAPTER

Operational Workflows

While this guide does not cover deployment, Figure 57 on page 105 provides a brief description of an end-to-end workflow that the operator might be expected to follow for SD-WAN.

Figure 57: SD-WAN Workflow



For more details on SD-WAN deployment workflows, see the CSO Deployment Guide.

8
CHAPTER

Resiliency and High Availability

IN THIS CHAPTER

Resiliency and High Availability

IN THIS SECTION

The Contrail SD-WAN solution is resilient and highly available at all layers. As a result, the network works seamlessly across failures with as little downtime as possible. The following sections discuss high availability at each layer.

Network Control Plane

The control plane itself is a distributed entity in the Contrail SD-WAN solution. The control plane is enabled using vRRs, which peer with the on-premise devices and set up routing dynamically based on information from the Routing Manager and Policy/SLA Manager microservices.

Route reflectors are deployed in a hierarchical structure. The on-premise devices peer with their closest regional route reflector, which itself peers with the other route reflectors.

Headless Forwarding

If on-premise devices lose connectivity to the route reflector in the SD-WAN controller, the devices are still able to continue forwarding traffic. This is referred to as headless operation. This situation will be sub-optimal as the controller cannot monitor and suggest new routes, but the paths still continue to exist and traffic will be forwarded in a best effort manner.

In headless mode, no new configuration or policy changes are made to the device, and no new data is reported from the device. Once connectivity is restored, the device checks in with the controller to ensure it has the latest routing and configuration information.

Data Plane

CSO Release 3.3 and later support on-premise device redundancy. A site can include a cluster of two nodes, acting as primary and secondary, to protect against device and link failures. If the primary node fails, or the links to it are down, traffic will flow through the secondary node.

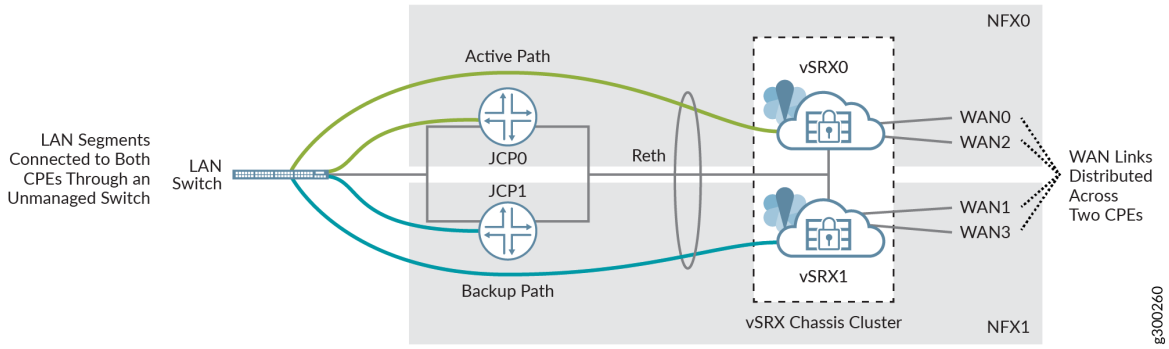
Spoke Redundancy

Spoke sites can include redundancy by interconnecting two CPE devices to create a single, logical, secure router. NFX Series or SRX Series Firewalls can be used.

Using NFX Series Devices

Figure 58 on page 108 shows a spoke redundancy setup using NFX Series devices, each with a vSRX Virtual Firewall Virtual Firewall installed. The two CPE devices are interconnected by creating an SRX chassis cluster to form a single logical node. The cluster uses a redundant Ethernet (reth) interface to connect to the Junos Control Plane (JCP) component, which acts as a switch to provide connectivity in and out of the devices.

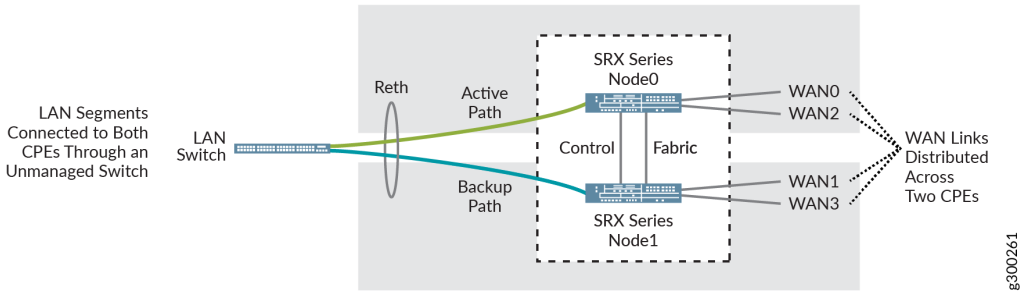
Figure 58: Dual CPE Devices - NFX Series Network Services Platforms



Using SRX Series Firewalls

Figure 59 on page 109 shows a spoke redundancy setup using SRX Series Firewalls. The two CPE devices are interconnected using chassis clustering to form a single logical node.

Figure 59: Dual CPE Devices - SRX Series Firewalls



Again, multiple connections on both sides of the devices provide link redundancy, The LAN side uses active/backup links, which are bundled as a reth interface on the SRX cluster. The WAN side uses all four active WAN links, distributed across the two devices.

Failover Scenarios

Table x describes how a spoke redundancy setup will react to various failure scenarios.

Scenario	NFX Behavior	SRX Behavior
Device failure	Node failover of vSRX Virtual Firewall cluster	Node failover of SRX chassis cluster
GWR vSRX Virtual Firewall VM failure	Node failover of vSRX Virtual Firewall cluster	N/A
LAN-side link failure	JCP - LAG based protection for individual link failures vSRX Virtual Firewall - Reth failover to the other cluster node if all LAN links to a node fail	LAG based protection for individual link failures Reth failover to the other cluster node if all LAN links to a node fail
WAN-side link failure	Same as single-CPE - ECMP across remaining links until SLA enforcement from SD-WAN controller	

(Continued)

Scenario	NFX Behavior	SRX Behavior
Interconnect physical link failure	JCP - LAG based protection	None built in; can add LAG based protection using two interconnected switches between the nodes

Usage Notes

You must use the same device model of NFX Series or SRX Series Firewall and the devices (primary and secondary) must have the same version of Junos OS installed.

The following SD-WAN features are not supported when using spoke redundancy:

- LTE WAN backup link
- Service chain support

For more information on spoke redundancy, see Device Redundancy Support Overview in the CSO User Guide.

Hub Redundancy (CPE Multihoming)

For hub-and-spoke topologies, redundancy can also be provided on the hub side by deploying two hub devices in an active/backup setup. If the primary hub goes down, or all overlay tunnels to the primary hub fail, traffic switches over to the secondary hub. When the primary hub comes up again and tunnels are established, traffic moves back to the primary hub.

Dual hub mode can also be used in primary/secondary mode. For example, a hub may be primary for half of the spokes, and secondary for the other half. This way the load is distributed in an active/active manner across all pairs of hub devices. Note that this mode requires meshing the hub devices to maintain flow symmetry across the network.

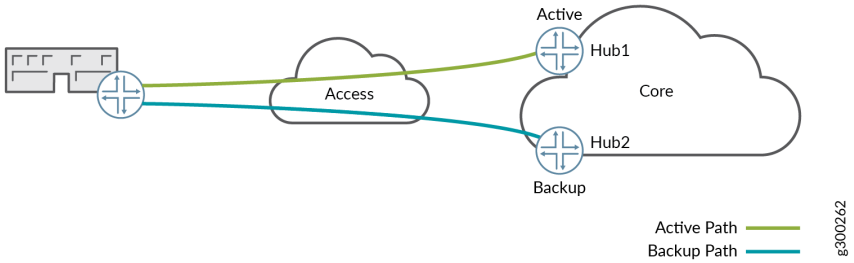
Design Options

There are several ways to implement redundancy between hub and spoke devices, depending on design requirements:

- **Single Spoke Device Multihomed to Dual Hub Devices; Single Access**

Figure 60 on page 111 shows how a single spoke device could be multihomed to dual hub devices with single access.

Figure 60: One Spoke Device, One Tunnel to Each Hub

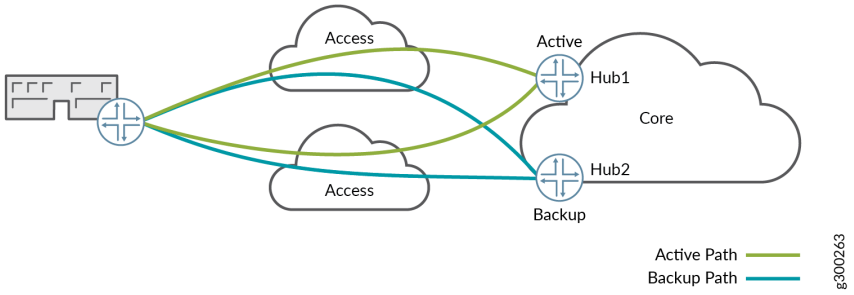


In this scenario, the hub devices are in an active/backup configuration, and spoke site prefixes are routed to the active hub.

- **Single Spoke Device Multihomed to Dual Hub Devices; Multiple Access**

  Figure 61 on page 111 shows how a single spoke device could be multihomed to dual hub devices with multiple access.

Figure 61: One Spoke Device, Two Tunnels to Each Hub

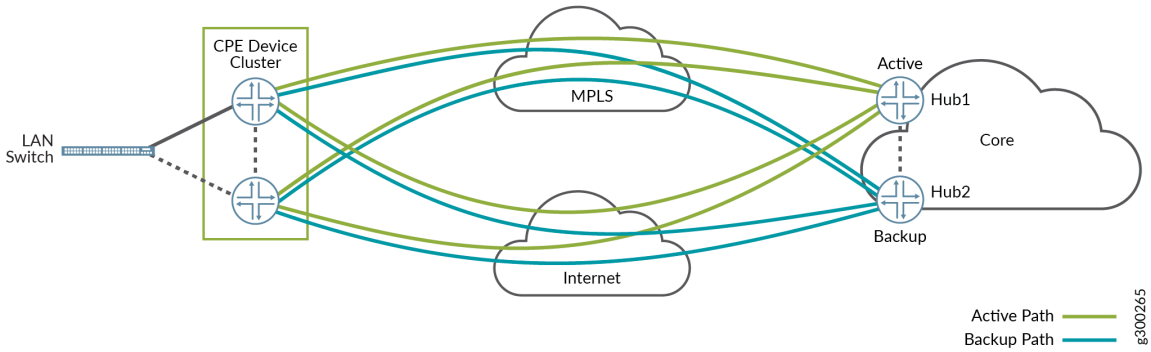


As in the previous scenario, the hub devices are in an active/backup configuration, and spoke site prefixes are routed to the active hub. In addition, the spoke site has overlay links to each hub through each access network. APBR routes traffic from CPE device to active hub over all possible overlays.

- **Clustered Spoke Devices Multihomed to Dual Hub Devices; Multiple Access**

  Figure 62 on page 112 shows how dual CPE devices could be multihomed to dual hub devices with multiple access from each CPE device.

Figure 62: Spoke Cluster, One Tunnel to Each Hub



As in the previous scenario, the hub devices are in an active/backup configuration, spoke site prefixes are routed to the active hub, and APBR routes traffic from active CPE device to active hub over all possible overlays. In this scenario, the CPE devices are also in an active/passive configuration.

The spoke site has eight overlay tunnels:

- Active CPE to active hub - two active links
- Active CPE to backup hub - two backup links
- Backup CPE to active hub - two active links
- Backup CPE to backup hub - two backup links

NOTE: Both hubs to which a CPE device is multihomed must be the same type of device.

NOTE: If using NAT, a hub switchover due to a primary hub failure may cause site-to-Internet and site to cloud application sessions to flap, as the NAT behavior adjusts to the change. Site-to-site sessions will continue to work through the switchover.