Contrail Service Orchestration

Contrail Service Orchestration (CSO) Deployment Guide

Release
4.0.0

Modified: 2018-07-16

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

Contrail Service Orchestration Contrail Service Orchestration (CSO) Deployment Guide
4.0.0

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://www.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*

Table 2: Text and Syntax Conventions (continued)

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

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

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

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at https://www.juniper.net/documentation/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/documentation/feedback/.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at https://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

CHAPTER 1

Solutions Overview

Contrail Service Orchestration Solutions Overview

The Juniper Networks Cloud Services Orchestration (CSO) provides a flexible and scalable micro-service architecture platform for deploying new service offerings. CSO is a multi-tenant platform that manages physical and virtual network devices, creates and manages Juniper Networks and third-party virtualized network functions (VNFs), and uses those elements to deploy network solutions for both enterprises and service providers and their customers.

CSO offers multiple deployment solutions that benefit both the service providers and their customers. The solutions are split into two overall groups, Cloud CPE solutions and SD-WAN solutions. The Juniper Networks Cloud Customer Premises Equipment (CPE) and the SD-WAN solutions both address the difficulties in traditional CPE deployments like: needing multiple hardware and software platforms to deploy multiple network services, long wait times for service instantiation, network disruption for service instantiation, fixed service offerings, and so on.

CSO uses these deployment solutions to transform traditional branch networks, offering opportunities for highly flexible networks, rapid introduction of new services, automation of network administration, and cost savings. The solutions can be implemented by service providers for their customers or by Enterprise IT departments in a campus and branch environment. In this documentation, service providers and Enterprise IT departments are called *service providers*, the users of their network services are called *customers*, and *solution* and *deployment* are used interchangeably.

The intent of this deployment guide is to provide a comprehensive understanding of the available solutions. In order to do that, we will:

- Briefly discuss each of the available solutions
- Give an overview of the architectures involved in the solutions
- Give an overview of the topologies involved in the solutions
- List and discuss the tasks involved in all of the solutions

Finally, there will be an end-to-end walkthrough of each of the solutions that covers the specifics involved in deploying them.

Juniper Networks Cloud Customer Premises Equipment (CPE) and SD-WAN solutions offer automated service delivery to branch network environments, leading to cost savings over traditional branch networks, while improving network agility and reducing configuration errors.

Traditional branch networks use many dedicated network devices with proprietary software to provide services and require extensive equipment refreshes every 3-5 years to accommodate advances in technology. Both configuration of standard services for multiple sites and customization of services for specific sites are labor-intensive activities. As branch offices rarely employ experienced IT staff on site, companies must carefully plan network modifications and analyze the return on investment of changes to network services.

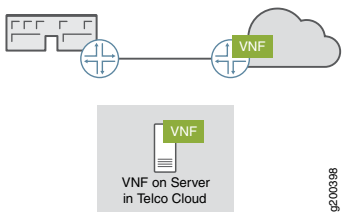
In contrast, the Cloud CPE solutions enable a branch site to access network services based on Juniper Networks and third-party virtualized network functions (VNFs) that run on commercial off-the-shelf (COTS) servers located in a central office (CO) or on a CPE device located at the site. This approach maximizes the flexibility of the network, enabling use of standard services and policies across sites and enabling dynamic updates to existing services. Customization of network services is fast and easy, offering opportunities for new revenue and quick time to market.

The following list briefly describes each of the available Cloud CPE deployments.

- **Cloud CPE Centralized Deployment Model** (centralized deployment or vCPE)

  In the centralized deployment, customers access network services remotely from a service provider's cloud. Sites that access network services in this way are called *service edge sites* in this documentation. Figure 1 on page 16 illustrates a simplified centralized deployment.

Figure 1: Centralized Deployment



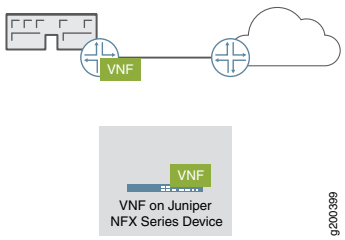
  The only equipment that needs to be configured in this deployment resides at the service provider's cloud. This deployment model is useful when few remote sites are accessing services and cost of traffic back to the CO for service delivery is not an issue.

The centralized deployment offers a fast migration route and this deployment is the recommended model for sites that can accommodate network services, particularly security services, in the cloud. There are no CPE devices deployed at customer sites in a centralized deployment. All network services are deployed in the service provider's cloud.

- **Cloud CPE Distributed Deployment Model** (distributed deployment, Hybrid WAN or uCPE)

  In the distributed deployment, customers access network services from a CPE device, located at the customer's site. These sites are called *on-premises sites* in this documentation. In the deployment workflows used in the CSO GUI, this deployment is known as Hybrid WAN. Figure 2 on page 17 illustrates a simplified distributed deployment.

Figure 2: Distributed or Hybrid WAN Deployment



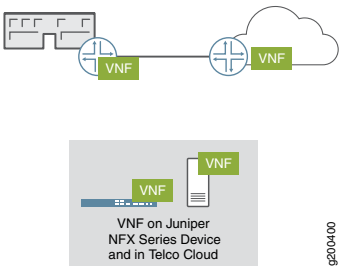
Initial configuration of the CPE device at the site is automated through the use of zero touch provisioning (ZTP) that is orchestrated through CSO. CSO also monitors the CPE device and its services, and can push software and configuration updates to the devices remotely, reducing operating expenses. This deployment model is useful in environments where service delivery from the service provider's cloud is costly. The distributed CPE deployment uses a CPE device such as an NFX Series Network Services platform or SRX Series Services Gateway at the customer site and thus supports private hosting of network services at a site. The distributed deployment can be extended to offer software defined wide area networking (SD-WAN) capabilities.

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

- **A Combined Centralized and Distributed Deployment**

  In this deployment, the network contains both service edge sites and on-premises sites. A customer can access network services from both service edge sites and on-premises sites. However, you cannot use the same network service at both locations. If you require the same network service at both the service edge and on-premises, you must create two identical network services with different names and deploy one at the service edge site and the other at the on-premises site. Figure 3 on page 18 illustrates a simplified combined deployment.

Figure 3: Combined Deployment

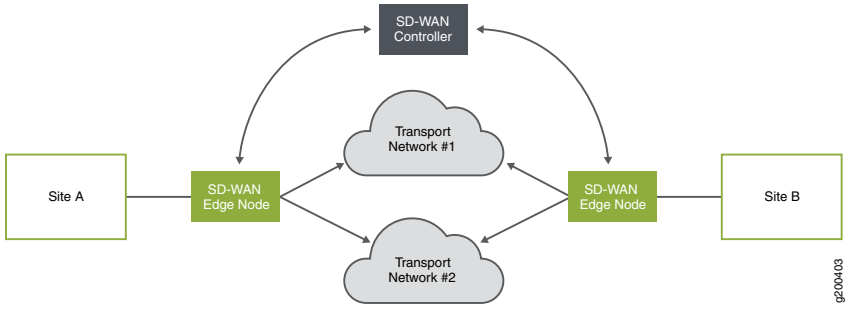


Implementing a combination deployment in which some sites use the centralized deployment and some sites use the distributed deployment provides flexible access based on customer site capabilities and cost factors.

Since the combined deployment is simply a combination of the centralized and distributed deployments, this guide does not provide an end-to-end walkthrough of this deployment option.

The SD-WAN solution offers a flexible and automated way to route traffic through the cloud using overlay networks. Similar to a distributed deployment, this solution uses CPE devices located at on-premises sites. At its most basic, an SD-WAN solution needs multiple sites, multiple connections between sites, and a controller as shown in Figure 4 on page 18.

Figure 4: Basic SD-WAN Concept



The CPE devices, or spokes, have a WAN side and a LAN side. On the WAN side, hub-and-spoke and full mesh topologies are supported. The CPE devices will use at least two and up to four interfaces as connection paths to cloud-based hubs, cloud-based spokes, other on-premises sites, or to the Internet. CSO allows you to give preference to one path over another for any given traffic. Thus, business-critical traffic could be routed through the service provider's cloud-based hub using MPLS/GRE while non-critical traffic could be routed over the Internet connection through an IPSec tunnel. Each path can have a service level agreement (SLA) profile applied which monitors the path for latency, congestion, and jitter and accounts for path preference. Should the path fail to meet one or more of the required parameters, traffic will be re-routed to another path automatically.

The LAN side of the CPE devices connect to the customer's LAN segments. Multiple departments at the customer site that occupy different LAN segments can have their

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

One CSO installation can support a combined centralized and distributed deployment and an SD-WAN solution simultaneously.

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

Related Documentation

- Overview of Solution Architectures on page 43
- Overview of Solution Topologies on page 53

NFV in the Cloud CPE Solution

The Cloud CPE and SD-WAN Solutions use the following components for the Network Functions Virtualization (NFV) environment:

- For the centralized deployment:
  - Network Service Orchestrator provides ETSI-compliant management of the life cycle of network service instances.

    This application includes RESTful APIs that you can use to create and manage network service catalogs.
  - Contrail OpenStack provides the following functionality:
    - Underlying software-defined networking (SDN) to dynamically create logical service chains that form the network services
    - NFV infrastructure (NFVI).
    - Virtualized infrastructure manager (VIM)
- For the distributed CPE and SD-WAN deployments:
  - Network Service Orchestrator, together with Network Service Controller, provides ETSI-compliant management of the life cycle of network service instances.
  - Network Service Controller provides service-chaining and the VIM.
  - The CPE device provides the NFV infrastructure (NFVI).

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

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

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

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

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

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

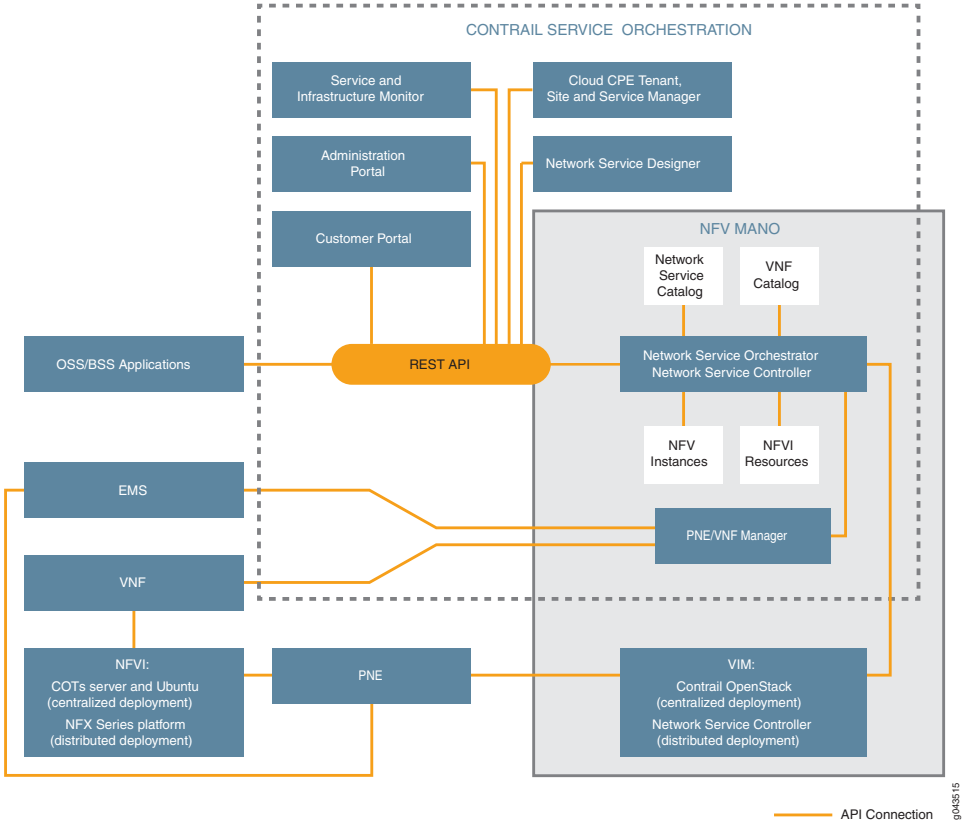
- Service and Infrastructure Monitor, which works with Icinga, an open source enterprise monitoring system to provide real-time data about the Cloud CPE solution, such as the status of virtualized network functions (VNFs), virtual machines (VMs), and physical servers; information about physical servers' resources; components of a network service (VNFs and VMs hosting a VNF); counters and other information for VNFs.

The Cloud CPE solution extends the NFV model through the support of physical network elements (PNEs). A PNE is a networking device in the deployment that you can configure through CSO, but not use in a service chain. Configuration of the PNE through CSO as opposed to other software, such as Contrail or Junos OS, simplifies provisioning of the physical device through automation. Combining provisioning and configuration for PNEs and VNFs provides end-to-end automation in network configuration workflows. An example of a PNE is the MX Series router that acts as an SDN gateway in a centralized deployment.

In the distributed deployment, VNFs reside on a CPE device located at a customer site. The NFX250 and NFX150 are switches that host the vSRX application as a VNF to enable routing and IPSec VPN access with the service provider's POP. MX Series routers, configured as provider edge (PE) routers, provide managed Layer 1 and Layer 2 access and managed MPLS Layer 3 access to the POP. Network Service Controller provides the VIM, NFVI, and device management for the NFX. Network Service Controller includes Network Activator, which enables remote activation of the NFX Series device when the site administrator connects the device and switches it on.

Figure 5 on page 21 illustrates how the components in the Cloud CPE solution interact and how they comply with the ETSI NFV MANO model.

Figure 5: NFV Components of the Cloud CPE Solution



OSS/BSS applications and Contrail Service Orchestration (CSO) components with OSS/BSS capabilities send requests to Network Service Orchestrator through its northbound REST API. Network Service Orchestrator then communicates through its southbound API to the northbound API of the appropriate, directly connected, component. Subsequently, each component in the deployment communicates through its southbound API to the northbound API of the next component in the hierarchy. Components send responses in the reverse direction.

The following process describes the interactions of the components when a customer requests the activation of a network service:

1. Customers send requests for activations of network services through Customer Portal or OSS/BSS applications.

2. Service and Infrastructure Monitor is continuously tracking the software components, hardware components, and processes in the network.

3. Network Service Orchestrator receives requests through its northbound REST API and:

   - For the centralized deployment:

a. Accesses information about the network service and associated VNFs from their respective catalogs, and communicates this information to the VIM, which is provided by Contrail OpenStack.

b. Sends information about the VNF to VNF Manager.

- For the distributed deployment, accesses information about the network service and associated VNFs from their respective catalogs, and communicates this information to the Network Service Controller.

4. The VIM receives information from Network Service Orchestrator and:
   - For the centralized deployment:
     - The VIM creates the service chains and associated VMs in the NFVI, which is provided by the servers and Ubuntu. Contrail OpenStack creates one VM for each VNF in the service chain.
     - VNF Manager starts managing the VNF instances while the element management system (EMS) performs element management for the VNFs.
   - For the distributed deployment, Network Service Controller creates the service chains and associated VMs in the NFVI, which is provided by the CPE device.
5. The network service is activated for the customer.

The PNE fits into the NFV model in a similar, though not identical, way to the VNFs.

- For the centralized deployment:
  1. Network Service Orchestrator receives the request through its northbound REST API and sends information about the PNE to PNE/VNF Manager.
  2. PNE/VNF Manager receives information from Network Service Orchestrator and sends information about the PNE to the EMS.
  3. VNF Manager starts managing the VNF instances and the EMS starts element management for the VNFs.
  4. The PNE becomes operational.
- For the distributed deployment:
  1. Network Service Orchestrator receives the request through its northbound REST API.
  2. Network Service Controller receives information from Network Service Orchestrator and starts managing the PNE.
  3. The PNE becomes operational.

Related Documentation

- Contrail Service Orchestration Solutions Overview on page 15
- Overview of Solution Topologies on page 53

Hardware and Software Used in Contrail Service Orchestration Solution Deployments

Contrail Service Orchestration makes use of various hardware and software-based network devices. running specific software versions. The following tables list devices and software versions that were tested in the various deployment models.

- Network Devices and Software Tested in the Centralized Deployment on page 23
- Network Devices and Software Tested in the Hybrid WAN (Distributed CPE) and SD-WAN Deployments on page 24

Network Devices and Software Tested in the Centralized Deployment

The centralized deployment makes use of Contrail Cloud

Table 3 on page 23 shows the network devices that have been tested as part of a reference architecture for the centralized deployment.

Table 3: Network Devices Tested for the Centralized Deployment

Function	Device
SDN gateway router	Juniper Networks MX Series 3D Universal Edge Router
Management switch	Juniper Networks EX Series Ethernet Switch
Data switch	Juniper Networks QFX Series Switch

Table 4 on page 23 shows the software tested for the centralized deployment. You must use these specific versions of the software when you implement a centralized deployment.

Table 4: Software Tested in the Centralized Deployment

Function	Software and Version
Operating system for MX Series router	Junos OS Release 14.2R3
Operating system for QFX Series switch	Junos OS Release 13.2X51-D38
Software defined networking (SDN), including Contrail Analytics, for a centralized deployment	Contrail Release 3.2.5 with OpenStack Mitaka
Virtualized infrastructure manager (VIM) and virtual machine (VM) orchestration	OpenStack Mitaka
Authentication and Authorization	OpenStack Mitaka
Network Functions Virtualization (NFV)	CSO Release 4.0.0

Network Devices and Software Tested in the Hybrid WAN (Distributed CPE) and SD-WAN Deployments

Table 5 on page 24 shows the network devices that have been tested for the distributed deployment and the SD-WAN implementation.

Table 5: Network Devices Tested for the Distributed Deployment and SD-WAN Implementation

Function	Device	Model
PE router and IPsec concentrator (Hybrid WAN distributed deployment only)	Juniper Networks MX Series 3D Universal Edge Router	• MX960, MX480, or MX240 router with a Multiservices MPC line card • MX80 or MX104 router with Multiservices MIC line card • Other MX Series routers with a Multiservices MPC or Multiservices MIC line card See MPCs Supported by MX Series Routers and MICs Supported by MX Series Routers for information about MX Series routers that support Multiservices MPC and MIC line cards.
Cloud hub device (SD-WAN implementation only)	Juniper Networks MX Series 3D Universal Edge Router Juniper Networks SRX Series Services Gateway	• MX104, MX240, MX480, or MX960 router with an Multiservices MIC line card. See MPCs Supported by MX Series Routers and MICs Supported by MX Series Routers for information about MX Series routers that support Multiservices MPC and MIC line cards. • SRX1500 Services Gateway • SRX4100 Services Gateway • SRX4200 Services Gateway
On-premise hub device (SD-WAN implementation only)	Juniper Networks SRX Series Services Gateway vSRX on an x86 server	• SRX1500 Services Gateway • SRX4100 Services Gateway • SRX4200 Services Gateway • vSRX

Table 5: Network Devices Tested for the Distributed Deployment and SD-WAN Implementation (continued)

Function	Device	Model
CPE device (Hybrid WAN deployment) or spoke device (SD-WAN implementation)	• NFX Series Network Services Platforms • SRX Series Services Gateways • vSRX on an x86 server	• NFX250-LS1 device • NFX250-S1 device • NFX250-S2 device • NFX150-S1 device • NFX150-S1E device • NFX150-C-S1 device • NFX150-C-S1-AE/AA device • NFX150-C-S1E-AE/AA device • SRX300 Services Gateway • SRX320 Services Gateway • SRX340 Services Gateway • SRX345 Services Gateway • vSRX

Table 6 on page 25 shows the software tested for the Hybrid WAN (distributed CPE) and SD-WAN deployment. You must use these specific versions of the software when you implement a distributed deployment.

Table 6: Software Tested in the Distributed Deployment and SD-WAN Solution

Function	Software and Version
NFX250 Operating System Software	Junos OS Release 15.1X53-D490
NFX150 Operating System Software	Junos OS Release 18.2R1.6
vSRX VNF on NFX device	vSRX KVM Appliance 15.1X49-D143
Operating system for vSRX used as a CPE device on an x86 server	vSRX KVM Appliance 15.1X49-D143
Operating system for SRX Series Services Gateway used as a CPE device or spoke device	Junos OS Release 15.1X49-D140
Operating system for MX Series router used as PE router	Junos OS Release 16.1R3.00
Operating system for MX Series Router used as a hub device for an SD-WAN implementation	Junos OS Release 16.1R5.7
Operating system for SRX Series Services Gateway used as a hub device for an SD-WAN implementation	Junos OS Release 18.2R1

Related Documentation

- Contrail Service Orchestration Solutions Overview on page 15

Number of Sites and VNFs Supported in Contrail Service Orchestration

The Cloud CPE solution supports three environment types: small, medium, and large. The small environment does not include any high availability features. Table 7 on page 26 shows the number of sites and VNFs supported for each environment.

Table 7: Number of Sites and VNFs Supported

Deployment Type	Number of VNFs Supported for a Centralized Deployment	Number of Sites and VNFs Supported for a Distributed Deployment	Number of Sites Supported for an SD-WAN Deployment	
			Hub and Spoke Sites	Full Mesh Sites
Small	10 VNFs	Up to 450, 2 VNFs per site	Up to 450	Up to 100
Medium	100 VNFs, 20 VNFs per Contrail compute node	Up to 3500, 2 VNFs per site	Up to 3500	Up to 200
Large	500 VNFs, 20 VNFs per Contrail compute node	Up to 5000, 2 VNFs per site	Up to 5000	Up to 200

Each environment has different requirements for:

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

Related Documentation

- *Minimum Requirements for Servers and VMs*
- *Provisioning VMs on Contrail Service Orchestration Nodes or Servers*

VNFs Supported by the Contrail Service Orchestration Solutions

Contrail Service Orchestration (CSO) supports Juniper Networks and third-party VNFs listed in .

Table 8: VNFs Supported by Contrail Service Orchestration

VNF Name	Version	Network Functions Supported	Deployment Model Support	Element Management System Support
Juniper Networks vSRX	vSRX KVM Appliance 15.1X49-D143	• Network Address Translation (NAT) • Demonstration version of Deep Packet Inspection (DPI) • Firewall • Unified threat management (UTM)	• Centralized deployment • Hybrid WAN and SD-WAN deployments supports NAT, firewall, and UTM.	Element Management System (EMS) microservice, which is included with CSO
LxCIPtable (a free, third party VNF based on Linux IP tables	14.04	• NAT • Firewall	Centralized deployment	EMS microservice
Cisco Cloud Services Router 1000V Series (CSR-1000V)	3.15.0	Firewall	Centralized deployment	Junos Space Network Management Platform
Riverbed SteelHead	9.2.0	WAN optimization	Hybrid WAN deployment–NFX250 and NFX150 platforms.	EMS microservice
Fortinet	5.6.3	Firewall	Hybrid WAN and SD-WAN deployments–NFX250 and NFX150 platforms.	EMS microservice
Single-legged Ubuntu	16.04	Firewall	Hybrid WAN and SD-WAN deployments–NFX250 and NFX150 platforms.	EMS microservice

Immediately after installation, CSO does not contain any VNFs. You have to upload the VNFs to the CSO platform through the Administration Portal or through API calls.

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

Related Documentation

- *Uploading the vSRX VNF Image for a Centralized Deployment*
- *Uploading the LxCIPtable VNF Image for a Centralized Deployment*
- *Uploading the Cisco CSR-1000V VNF Image for a Centralized Deployment*

CHAPTER 2

Common Elements in All Deployments

Building Blocks Used for Contrail Service Orchestration Deployments

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

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 administrator or global admin. This administrator has full read and write access to the entirety of the CSO platform from the global domain. He or she can create, edit, and delete other administrators and operators who are subject to role-based access controls (RBAC) that assign them privileges to the rest of the objects in CSO. Successful login as cspadmin places the user in the Administration Portal of the global domain; the user can switch into the Customer Portal of any OpCo or Tenant.

The next level of administrator is the Operating Company or OpCo administrator. This user has full administrative privileges within an OpCo domain. 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 can not affect elements of the global domain. Successful login by the OpCo administrator places them into the Administration Portal of their OpCo and they can switch into the Customer Portals of any Tenant of the OpCo.

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

There are also operator users at all three levels, Global, OpCo, and Tenant. While operator users are not, strictly speaking, administrators, they can be created by administrators at each level. By default, operators have read-only access to the elements in their domain.

Portals

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

Administration portals allow tenant creation, OpCo creation, and creation of other high-level objects that customers make use of within the customer portals. Administration portals are the highest level of portal within a domain.

Customer portals provide users access to a subset of the objects that exist in administration portals. The primary example of this is that global administrators can see the **Tenants** page in the Administration Portal

For more information about Administrator and Customer Portals, see the *Contrail Service Orchestration User Guide*.

Tenants

CSO uses the tenant element to logically separate one customer from another. A global service provider (SP) administrator creates one tenant to represent each customer for which they will provide network services. If the global SP is logically split up into multiple OpCos, then the individual OpCo administrators can create tenants that represent their customers.

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 SP and customer networks. No individual tenant, its administrators, operators or customers can see or interact with the objects of another tenant or customer. Tenants can be named in whatever way makes most sense to the SP.

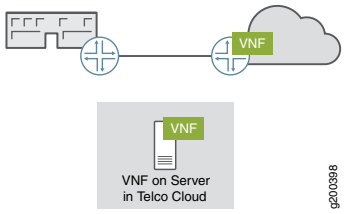
Topologies

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

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

  It is within this topology that a Centralized CPE solution and its network services are deployed. Figure 6 on page 31shows an example where the VNFs used in the Centralized CPE are deployed in the SP cloud.

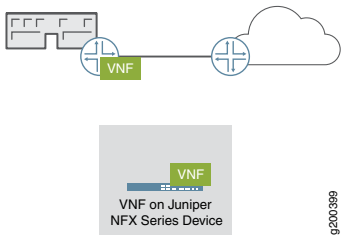
Figure 6: Centralized CPE



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

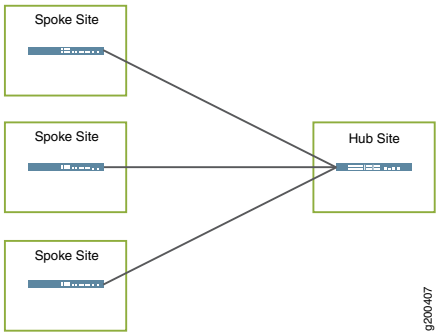
  This is the topology of Distributed CPE, or Hybrid WAN solutions wherein the SP provides network services to its on-premises customers but does not allow them to communicate with one another. Figure 7 on page 31 shows an example where the VNF functions are located on-premises, but the on-premises site has no access to other sites.

Figure 7: Distributed CPE (or Hybrid WAN)



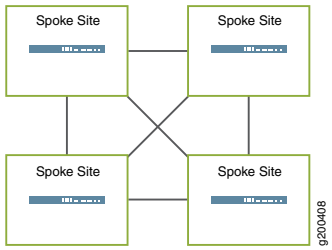
- **Hub-and-Spoke Topology–** This topology is available for SD-WAN deployments. Given that SD-WAN is intended specifically to enable and enhance the efficacy of WAN communication using network overlays, this topology does allow for communication from site to site. Specifically, if one site needs to communicate with another site, that communication goes through the hub on its way to the other site. Figure 8 on page 32 shows a very basic example of hub-and-spoke topology. VNFs can be deployed at any of the locations shown.

Figure 8: Hub-and-Spoke Topology



- **Full Mesh Topology–** This topology is also available for SD-WAN deployments. Direct site-to-site communication is allowed and every site is considered a hub site. Figure 9 on page 32 shows a very basic example of a full mesh topology. VNFs can be deployed at any of the locations shown. This topology requires more overlay networks than the hub-and-spoke topology so consideration must be given where resources are constrained.

Figure 9: Full Mesh Topology



Points of Presence (POPs)

A POP is a place, usually at the SP Cloud edge, where network services can be deployed and underlay network connections are made to remote sites. POPs can have PE router, IPSec concentrator, and SDN Gateway devices assigned to them.

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

Sites

Sites are the branch offices or remote locations from which customers access the network services provided by the CSO solutions. A site is assigned to a POP and the type of sites available for creation depend on the type of deployment you are creating: Centralized CPE, Distributed CPE, or SD-WAN. Sites can be created by the Global administrator, the OpCo administrator, or the Tenant administrator. Sites can be named whatever makes

sense for the SP or Tenant. Table 9 on page 33 lists what types of sites can be created within each deployment.

Table 9: Site types by Deployment

Deployment	Available Site Types	Uses	Service Notes
Centralized CPE	Local Service Edge	The local service edge is the automation point in the network closest to the customer location (SDN gateway) where centralized service VNFs can be attached. Use this site type for customers who access the Internet through a VPN in the SP cloud.	Site acts as a service attachment point. During site creation, an optional VRF can be created on the gateway router to handle routing and forwarding specifically for the centralized service attachment point. If a PNE is configured, then it must be associated with a site and a VNF must be created on the PNE for each associated site.
	Regional Service Edge	Automation point deeper in the service provider network that performs centralized services for many branches, for example: a hub router deep inside the enterprise network. Use this site type for each branch location in the customer network. For use with customers who access the Internet from their local site.	The end-point is identified only by route-target. The centralized VNF (network-service) connectivity is orchestrated only by peering using BGP routing protocols. No configuration changes are made to the hub router.
Hybrid WAN/Distributed CPE	Local Service Edge	Automation point in the network closest to the customer CPE location, for example: the PE-Router, where centralized service VNFs can be attached. Use this site type for customers who access the Internet through a VPN in the SP cloud.	The Local Service Edge site acts as a service attachment point. During site creation, an optional VRF can be created on the gateway router to handle routing and forwarding specifically for the centralized service attachment point.
	Regional Service Edge	Automation point deeper in the service provider network that performs centralized services for many branches, for example: a hub router deep inside the enterprise network. Use this site type for each branch location in the customer network. For use with customers who access the Internet from their local site.	The end-point is identified only by route-target. The centralized VNF (network-service) connectivity is orchestrated only by peering using BGP routing protocols. No configuration changes are made to the hub router.

Table 9: Site types by Deployment (continued)

Deployment	Available Site Types	Uses	Service Notes
SD-WAN	On-premise Hub	Use this site type for locating SRX Series devices at customer sites.	Local breakout of Internet traffic is supported when using the hub-and-spoke topology.
	On-premise Spoke	Use this site type for locating NFX Series or SRX Series devices at customer sites in either a hub-and-spoke or full mesh topology.	SRX Series devices deployed as on-premises spoke devices can not host VNF-based network services. NFX devices used as on-premise spoke devices can support ADSL, VDSL, and LTE access links, but cannot 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. Local breakout is supported on this type of site when using the full mesh topology.
	Cloud Hub	Use this type of site for locating MX Series or SRX series in a SP cloud. The cloud hub devices are used for establishment of IPSec tunnels. Cloud hub devices are multi-tenant (shared amongst multiple sites) through the use of VRF instances configured on them.	You must specify the capability of the cloud hub devices when setting up the site. Specifying OAM capabilities allows the hub to help create secure OAM networks with the CPE devices. A cloud hub device is required for the full mesh topology. Local breakout is not supported on Cloud Hub sites.
	Cloud Spoke	This type of site is specifically for deploying a vSRX in a tenant's Amazon Web Services (AWS) Virtual Private Cloud (VPC)	Firewall and UTM services are available to protect the customer's resources in AWS VPC. Connectivity between VPC resources and on-premise sites. WAN_0, WAN_1, and LAN interfaces need to be predefined in VPC. Two elastic IP addresses need to be reserved in VPC to attach to WAN interfaces later. VPC should be created and attached to an Internet gateway. Only hub-and-spoke topology supported. Hub needs to have public IPs on in its WAN interfaces. Hub WAN interface type should be set as Internet during onboarding.

Customer Premises Equipment (CPE)

CPE devices are those devices that are placed at remote locations in the site types mentioned previously. CPE devices serve their functions in Hybrid WAN deployments or as on-premises spoke devices in SD-WAN deployments.

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

Virtual Route Reflector (VRR)

The VRR is part of CSO's SD-WAN controller. It is one of the virtual machines that get provisioned and installed during the installation process. To facilitate the routing needed in the SD-WAN deployment , the VRR forms BGP sessions with CPE spokes and hub devices using the underlay interface designated as OAM or OAM_AND_DATA during the configure site GUI workflow for site onboarding. Starting in CSO Release 4.0.0, the OAM interfaces can be implemented using dedicated IPSec tunnels which allows CPE and hub devices to be behind NAT.

Service-Level Agreement (SLA) Profiles and Policies

CSO allows for the creation of SLA profiles that can be mapped to SD-WAN policies for traffic management in an SD-WAN deployment. SLA profiles are created for applications or groups of applications for all tenants. An SLA profile consists of a set of configurable constraints that can be defined in the unified portal for both the Administration and Customer Portals.

You can set path preference for each of the connection paths from site-to-site or from site-to-hub, set SLA parameters for throughput, packet lost, latency, and jitter, set class of service for various types of traffic, and set rate limiters to control upstream and downstream rates and burst sizes.

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

See Configuring Application SLA Profiles in the *Contrail Service Orchestration User Guide* for more details.

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.

Related Documentation

- Installing and Setting Up CPE Devices on page 78

Accessing the Contrail Services Orchestration GUIs

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

See Table 10 on page 36 for information about logging into the Contrail Service Orchestration GUIs.

Table 10: Access Details for the GUIs

GUI	URL	Login Credentials
Administration Portal	https://*central-IP-Address* Where: *central-IP-Address*—IP address of the VM that hosts the microservices for the central POP For example: https://192.0.2.1	Specify the OpenStack Keystone username and password. The default username is **cspadmin**. Specify the autogenerated cspadmin password that is displayed on the console after the installation is complete. After the upgrade, you must specify the cspadmin password of the previously installed version.
Customer Portal	Same as the URL used to access the Administration Portal	Specify the credentials when you create the Customer either In Administration Portal or with API calls.
Designer Tools—Log into Network Service Designer and click the menu in the top left of the page to access the other designer tools.	https://*central-IP-Address*:83 Where: *central-IP-Address*—IP address of the VM that hosts the microservices for the central POP For example: https://192.0.2.1:83	Specify the OpenStack Keystone username and password. The default username is **cspadmin**. Specify the autogenerated cspadmin password that is displayed on the console after the installation is complete. After the upgrade, you must specify the cspadmin password of the previously installed version.

Table 10: Access Details for the GUIs (continued)

GUI	URL	Login Credentials
Kibana This tool provides a visual representation of log files. You can use it to monitor: • Network services in a central or regional POP • Microservices in the deployment	http://*infra-vm-IP-Address* | *ha-proxy-IP-Address*:5601 Where: *infra-vm-IP-Address*—IP address of the VM that hosts the infrastructure services for a central or regional POP. Use this option to monitor network services. *ha-proxy-IP-Address*—IP address of high availability (HA) proxy. Use this option to monitor the microservices. • For a deployment without HA, use the IP address of the VM that hosts the microservices for the central POP. • For an HA deployment, use the virtual IP address that you provide for the HA proxy when you install CSO. For example: http://192.0.2.2:5601	Login credentials are not needed.
Grafana and Prometheus These tools provide monitoring and troubleshooting for the infrastructure services in CSO. You use Prometheus to create queries for the infrastructure services and Grafana to view the results of the queries in a visual format.	• Prometheus—*ha-proxy-IP-Address*:30900 • Grafana—*ha-proxy-IP-Address*:3000 Where: *ha-proxy-IP-Address*—IP address of HA proxy • For a deployment without HA, use the IP address of the VM that hosts the microservices for the central POP. • For an HA deployment, use the virtual IP address that you provide for the HA proxy when you install CSO. For example: http://192.0.2.2:30900	For Grafana, specify the username and password. The default username is **admin** and the default password is **admin**. For Prometheus, the login credentials are not needed. After the upgrade, to login to the Administration Portal, you must specify the cspadmin password of the previously installed version.

Related Documentation

- Setting Up a Centralized Deployment on page 59
- Setting Up a Distributed Deployment on page 71
- Designing and Publishing Network Services on page 38
- Setting Up Customers' Networks on page 40
- Contrail Service Orchestration Solutions Overview on page 15

Designing and Publishing Network Services

The Contrail Service Orchestration (CSO) Designer Tools consist of three tools that you use to create VNF templates, packages, and service chains that can be deployed as network services for all of the Cloud CPE and SD-WAN solutions. You access the CSO Designer Tools at the same URL as the CSO Administration Portal, but on port 83. For example, if the IP address of the Administration Portal is 10.2.2.12, then the URL for Designer Tools would be: **https://10.2.2.12:83**.

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

You use the same process to create network services for centralized CPE, Hybrid WAN, and SD-WAN deployments. You cannot, however, share network services between a centralized deployment and a distributed deployment that are managed by one Contrail Service Orchestration installation. In this case, you must create two identical services, one for the centralized deployment and one for the Hybrid WAN deployment. The same is true for SD-WAN deployments, the same network service can not be shared between an on-premise site and the service provider's POP.

You can also use *Configuration Designer* to create workflows for device templates.

For detailed information about using the Designer Tools, see the Contrail Service Orchestration User Guide.

Related Documentation

- Accessing the Contrail Services Orchestration GUIs on page 36
- Setting Up a Centralized Deployment on page 59
- Setting Up a Distributed Deployment on page 71

Contrail Service Orchestration License Tool

- Overview of the License Page on page 39

Overview of the License Page

SRX and vSRX Series devices can be used in both the distributed cloud CPE and SD-WAN solutions as CPE devices or as cloud or site hubs. These devices require licensing in order to perform the functions needed for those solutions. Contrail Solutions Orchestration (CSO) provides a GUI-based method for loading licenses into CSO and installing them on the devices. The licensing page is available in the Administration Portal or the Customer Portal by navigating to **Administration > Licenses**. Licenses must first be purchased through your Juniper Networks account team or reseller. Once purchased, the text of the license is emailed to you.

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

- vSRX VNFs in a centralized deployment
- The following items in a distributed deployment:
  - vSRX gateway router on an NFX Series device
  - vSRX or SRX Series CPE devices
- vSRX or SRX Series CPE devices in an SD-WAN deployment

To upload a license to CSO for later push to an SRX device:

1. Login to CSO as an authorized user–License management is available to both tenant administrators and the global administrator. Operators can not upload licenses to CSO or push them to devices.

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

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

3. Click the **+** at the top-right part of the list.

   This brings up a pop-up window in which you locate and describe the new license file.

4. Click the **Browse** button to locate the license file that was emailed to you. Each file uploaded should be for one feature only. License files are generally named as the device serial number for which they are intended and have a **.txt** file extension.

5. (Optional) Enter a description of the license file. If uploading multiple licenses for a single device, a description can help you know which is which in the license list.

6. Click **OK** once you have filled in the required data. The license file will appear in the list along with the upload date, and your login under the **Uploaded By** column.

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

1. Click on the line or in the **check box** next to the appropriate license file.

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

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

   If you are logged in as the global administrator, you will see a pull-down list of tenants. Below that will be the sites and devices to which you can push the license files.

3. Select the appropriate device, and click **Push Licenses**. Multiple licenses can be pushed to a single device.

See *Contrail Service Orchestration User Guide* for additional details about the CSO license page.

NOTE: **For releases prior to CSO Release 3.3.0, there is a CLI-based license tool that allows you to upload and install licenses. Information about the CLI-based license tool can be found in the** Overview of the License Tool.

See Also

- Accessing the Contrail Services Orchestration GUIs on page 36
- Designing and Publishing Network Services on page 38

Setting Up Customers' Networks

After you have set up the network for a customer with Administration Portal, that customer can view, configure, and manage their network through Customer Portal. Customer Portal is actually customer-specific view of Administration Portal. Customers have their own login credentials, which provide role-based access control to the information for their networks. Customers see only their own networks, and cannot view other customers' networks. You can also view and manage each customer's network from Administration Portal, by accessing the view for a specific customer.

With Customer Portal, customers can:

- Add, activate and delete sites in the network.

BEST PRACTICE: **Service providers often add sites for customers. Customers typically activate and deactivate sites in their networks.**

- Configure CPE devices.
- Deploy and manage available network services for a hybrid WAN deployment.

- Add and configure network services.
- Disable and remove network services.
- Monitor network services.

For detailed information about using Customer Portal, see the *Contrail Service Orchestration User Guide.*

Related Documentation

- Accessing the Contrail Services Orchestration GUIs on page 36
- Designing and Publishing Network Services on page 38
- Contrail Service Orchestration Solutions Overview on page 15

CHAPTER 3

Architecture Overview

Overview of Solution Architectures

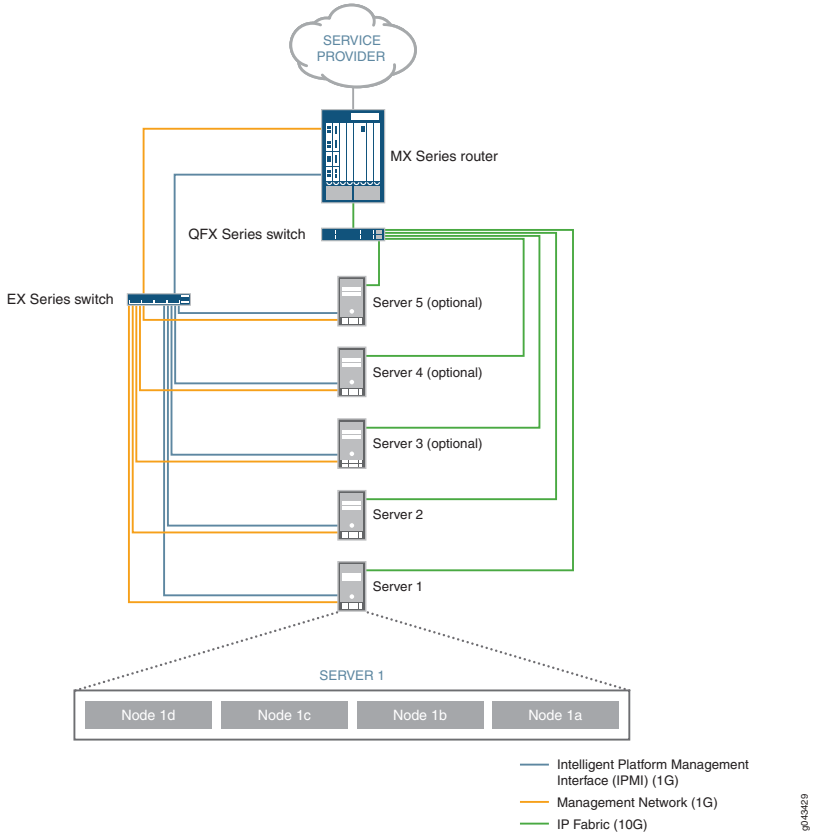
Architecture of the Contrail Cloud Implementation in the Centralized Deployment

This section describes the architecture of the components in the Contrail Cloud implementation used in the centralized deployment.

Architecture of the Contrail Cloud Implementation

The centralized deployment uses the Contrail Cloud implementation to support the service provider's cloud in a network point of presence (POP). The Contrail Cloud implementation consists of the hardware platforms, including the servers, and Contrail OpenStack software. Figure 10 on page 44 illustrates the Contrail Cloud implementation. The Contrail Service Orchestration (CSO) software is installed on one or more servers in the Contrail Cloud implementation to complete the deployment.

Figure 10: Architecture of Contrail Cloud Implementation



In the Cloud CPE Centralized Deployment Model:

- The MX Series router provides the gateway to the service provider's cloud.
- The EX Series switch provides Ethernet management and Intelligent Platform Management Interface (IPMI) access for all components of the Cloud CPE Centralized Deployment Model. Two interfaces on each server connect to this switch.
- The QFX Series switch provides data access to all servers.
- The number of servers depends on the scale of the deployment and the high availability configuration. You must use at least two servers and you can use up to five servers.
- Each server supports four nodes. The function of the nodes depends on the high availability configuration and the type of POP.

Architecture of the Servers

The configuration of the nodes depends on whether the Contrail Cloud implementation is in a regional POP or central POP and on the high availability configuration. Each node is one of the following types:

- Contrail Service Orchestration node, which hosts the Contrail Service Orchestration software.

- Contrail controller node, which hosts the Contrail controller and Contrail Analytics.
- Contrail compute node, which hosts the Contrail Openstack software and the virtualized network functions (VNFs).

The Contrail Cloud implementation in a central POP contains all three types of node. Figure 11 on page 45 shows the configuration of the nodes in the Contrail Cloud implementation in the central POP for a deployment that offers neither Contrail nor Contrail Service Orchestration high availability:

- Server 1 supports one Contrail controller node, two Contrail compute nodes, and one Contrail Service Orchestration node.
- Server 2 and optional servers 3 through 5 each support four Contrail compute nodes.

Figure 11: Architecture of Servers in the Central POP for a Non-Redundant Installation

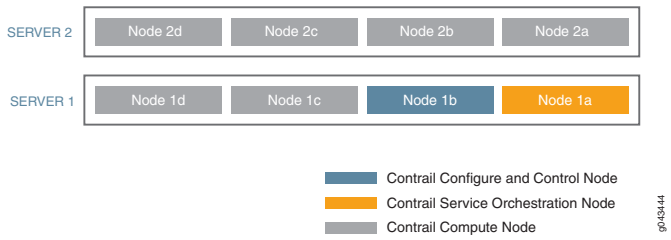
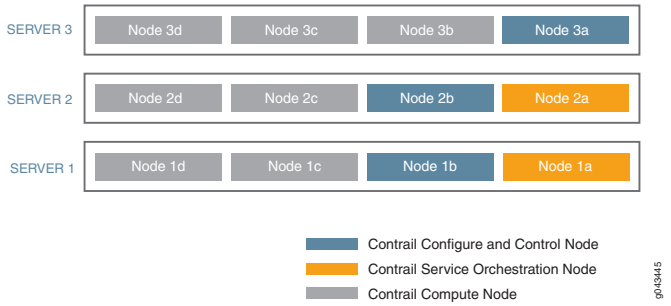


Figure 12 on page 45 shows the configuration of the nodes in the Contrail Cloud implementation in the central POP for a deployment that offers both Contrail and Contrail Service Orchestration high availability:

- Servers 1, 2, and 3 each support one Contrail controller node for Contrail redundancy.
- Servers 1 and 2 each support one Contrail Service Orchestration node for Contrail Service Orchestration redundancy.
- Other nodes on servers 1, 2, and 3 are Contrail compute nodes. Optional servers 4 through 7 also support Contrail compute nodes.

Figure 12: Architecture of Servers in the Central POP for a Redundant Installation



The Contrail Cloud implementation in a regional POP contains only Contrail nodes and not Contrail Service Orchestration nodes. In a deployment that does not offer Contrail high availability, the regional Contrail Cloud implementations support:

- One Contrail controller node and three Contrail compute nodes on server 1.
- Four Contrail compute nodes on server 2 and on optional servers 3 through 5.

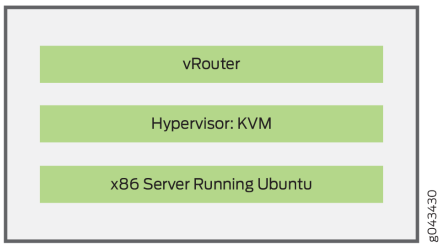
In a deployment that offers Contrail high availability, the regional Contrail Cloud implementations support:

- One Contrail controller node for Contrail redundancy on servers 1, 2, and 3.
- Three Contrail compute nodes on servers 1, 2, and 3.
- Four Contrail compute nodes on optional servers 4 through 7.

Architecture of the Contrail Nodes

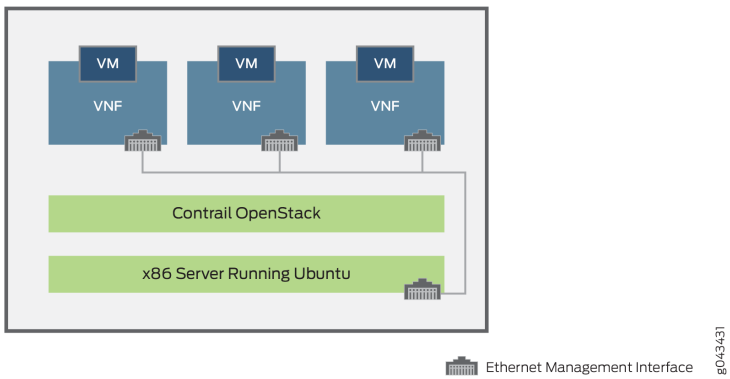
Each Contrail controller node uses Contrail vRouter over Ubuntu and kernel-based virtual machine (KVM) as a forwarding plane in the Linux kernel. Use of vRouter on the compute node separates the deployment's forwarding plane from the control plane, which is the SDN Controller in Contrail OpenStack on the controller node. This separation leads to uninterrupted performance and enables scaling of the deployment. Figure 13 on page 46 shows the logical representation of the Contrail controller nodes.

Figure 13: Logical Representation of Contrail Controller Nodes



A Contrail compute node hosts Contrail OpenStack, and the VNFs. Contrail OpenStack resides on the physical server and cannot be deployed in a VM. Each VNF resides in its own VM. Figure 14 on page 46 shows the logical representation of the Contrail compute nodes.

Figure 14: Logical Representation of Contrail Compute Nodes



See Also

- Overview of Solution Topologies on page 53
- Resiliency in Contrail Service Orchestration on page 50
- NFV in the Cloud CPE Solution on page 19

Architecture of the Hybrid WAN or Distributed CPE Deployment

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

Figure X shows a simple diagram of the distributed CPE solution. The cloud represents the service provider network to which the customer site is connected.

As mentioned previously, the distributed Cloud CPE deployment makes use of on-premises CPE devices in order to localize the delivery of network services and provide gateway router (GWR) functionality. In this case, the Juniper Networks NFX Series or SRX Series devices act as the CPE devices. In the case of NFX as CPE, the GWR function is provided by a built-in vSRX VNF and network services are hosted and provided from within the NFX that is located at the customer site. This makes the network services extremely responsive from the point of view of the customer LAN, while negating the need for customer traffic to traverse the WAN in order to access the services. In the case of an SRX Series device as the managed CPE device, only services native to the SRX, firewall, NAT, and UTM, can be provisioned and managed at the customer site by CSO. Other services, such as WAN optimization must be provisioned and managed separately from the SRX and cannot be managed by CSO.

The distributed Cloud CPE deployment also makes use of a provider edge (PE) router in the service provider cloud. The PE router acts as a IPSec concentrator, terminating IPSec tunnels, and a PE router, providing policy-based access to the service provider's MPLS network. The PE and CPE devices communicate over one or more WAN links and make use of MPLS/GRE or IPSec tunnels.

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

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

See Also

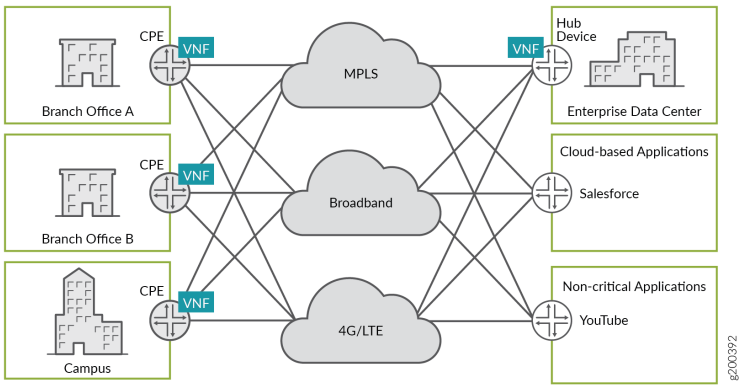
- Overview of Solution Topologies on page 53

Architecture of the SD-WAN Deployment

While the Cloud CPE deployments focus on network service delivery to customer sites, the SD-WAN deployment differs in that its primary goal is cost effective, efficient, and secure transfer of data from site to site, through the cloud, over multiple connections. At its most basic, SD-WAN includes multiple sites, multiple connections between sites, and a controller as shown in figure

The SD-WAN solution makes use of existing branch and WAN connection types (underlay networks) combined with on-premises CPE devices and hubs, service provider cloud-based hubs and routers, and overlay networking to provide network flexibility, traffic management, and cost effective routing across whichever connection makes the most sense.

At a customer site, there are often separate MPLS and multiple Internet connections over various transports and ISPs. The SD-WAN solution allows you to create software-defined overlay networks that take advantage of the differences in these connection types. For example, business-critical applications can be routed through L3 VPN tunnels over secure MPLS connections that typically include service level agreements (SLAs), while non-critical applications can be routed through IPSec tunnels overlaid on various Internet connection types. Figure shows a simplified underlay network without the overlays.



Traffic is routed across one link as a primary link while other links remain as backups in case of failure, degradation, or congestion. The SD-WAN solution can monitor traffic across all the link types and automatically re-route traffic that is in danger of missing an SLA. Primary links are designated for a given type of traffic or specific application.

Starting with Release 4.0.0, CSO supports multiple broadband connection types including LTE, ADSL and VDSL. LTE can now be used as a primary link and function as DATA, OAM, or DATA_AND_OAM link. An LTE link can also be used for zero-touch provisioning (ZTP) of the devices. For LTE support, the NFX150 has support built-in while the NFX250 uses a USB dongle for LTE connectivity. Both the NFX150 and NFX 250 Series use SFP connectors to support ADSL or VDSL. ADSL and VDSL cannot be used for ZTP.

For redundancy and resiliency, the SD-WAN solution supports multi-homed hubs in the service provider cloud and dual CPE in on-premises sites. In both instances, one device

(hub or CPE) is the primary device while the second device is a backup device. The backup devices remain idle as long as the primary devices are working.

Network services like statefull firewall, unified threat management, and WAN optimization can be created as VNFs and deployed as service chains in whatever order needed on any of the links at each customer site.

NOTE: When using an NFX Series devices as CPE, service chains can not include WAN optimization, APPQoE, or APBR.

The SD-WAN deployment also supports two distinct topologies: full-mesh and hub-and-spoke. In the hub-and-spoke topology, customer sites can communicate with one another, provided the proper policies are in place, by going through the hub device at the service provider cloud. In the full-mesh topology, all CPE devices are spoke devices. Starting with CSO Release 4.0.0, a cloud hub device is required in the full mesh topology in order to support secure OAM.

For more details on SD-WAN architecture, see the *SD-WAN Design and Architecture Guide*

See Also

- Overview of Solution Topologies on page 53

Authentication and Authorization in CSO

Contrail Service Orchestration (CSO) uses OpenStack Keystone to authenticate and authorize the network operations. You can implement the Keystone in several different ways, and you specify which method you use when you install CSO:

- A CSO Keystone, which is integrated with CSO and resides on the central CSO server.

  This option offers enhanced security because the Keystone is dedicated to CSO and is not shared with any other applications. Consequently, this option is generally recommended.

- An external Keystone, which resides on a different server to the CSO server:
  - The Contrail OpenStack Keystone in the Contrail Cloud Implementation for a centralized deployment is an example of an external Keystone.

    In this case, customers and Cloud CPE infrastructure components use the same Keystone token.
  - You can also use an external Keystone that is specific to your network.

See Table 11 on page 50 for guidelines about using the Keystone options with different types of deployments.

Table 11: Guidelines for Keystone Options for Different Deployments

	Centralized Deployment	Distributed and SD-WAN Deployments	Combined deployment
The CSO Keystone (recommended)	• Installation of the Keystone occurs with the CSO installation. • After installation, you must use Administration Portal or the API to configure a service profile for each virtualized infrastructure monitor (VIM).	• Installation occurs with the CSO installation. • You do not need to perform any configuration after installation.	• Installation occurs with the CSO installation. • You do not need to perform any configuration after installation for the distributed portion of the deployment. • After installation, you must configure service profiles for VIMs in the centralized portion of the deployment.
The Contrail OpenStack Keystone on the Contrail Cloud Platform (external Keystone)	• Installation occurs with Contrail OpenStack • You specify the IP address and access details for the Contrail OpenStack Keystone when you install CSO.	Not available	• Available for the centralized portion of the deployment. • Installation occurs with Contrail OpenStack. • You specify the IP address and access details for the Contrail OpenStack Keystone when you install CSO.
An external Keystone that is specific to your network.	You specify the IP address and access details for your Keystone when you install CSO.		

Related Documentation

- Contrail Service Orchestration Solutions Overview on page 15

Resiliency in Contrail Service Orchestration

The Contrail Services Orchestration (CSO) software offers robust deployment implementations with resiliency for the following features:

- High availability of CSO infrastructure services and microservices in medium and large installations

  Each infrastructure service or microservice resides on multiple hosts and if an application on the primary host fails, a corresponding application on another host takes over. Current operations for an application do not recover if a failure occurs; however, any new operations proceed as normal.

- A Contrail OpenStack instance configured for high availability can be used with the centralized Cloud CPE deployment

  The Contrail OpenStack instance, which is used for the centralized deployment, includes three Contrail controller nodes in the Contrail Cloud Platform, and provides resiliency for virtualized infrastructure managers (VIMs), virtualized network functions (VNFs), and network services.

- CSO provides additional resiliency for virtualized network functions (VNFs) and network services in the centralized Cloud CPE solution.

  You can enable or disable automatic recovery of a network service in a centralized deployment. If a network service becomes unavailable due to a connectivity issue with a VNF, Network Service Orchestrator maintains existing instances of the network service in end users' networks and initiates recreation of the VNFs. During this recovery process, the end user cannot activate the network service on additional network links. When the problem is resolved, normal operation resumes and end users can activate the network service on additional network links.

  Enabling automatic recovery improves reliability of the implementation. Conversely, disabling automatic recovery for a network service allows you to quickly investigate a problem with the underlying VNF. By default, automatic recovery of a network service is enabled.

Related Documentation

- Architecture of the Contrail Cloud Implementation in the Centralized Deployment on page 43
- Contrail Service Orchestration Solutions Overview on page 15
- NFV in the Cloud CPE Solution on page 19

CHAPTER 4

Topology Overview

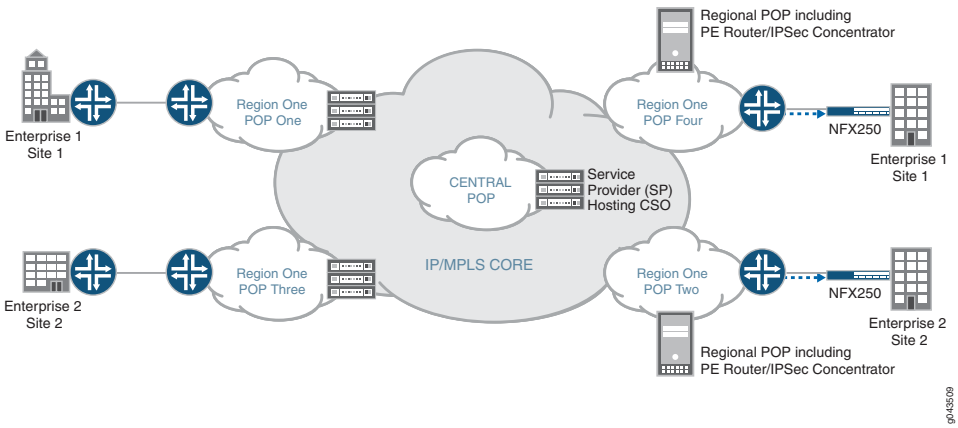
Overview of Solution Topologies

This section discusses the topologies of the various solutions.

Figure 15 on page 53 shows the topology of the Cloud customer premises equipment (CPE) and SD-WAN solutions. You can use one Contrail Service Orchestration (CSO) installation for any or all of the supported solution deployments:

- Cloud CPE solutions
  - Centralized deployment (vCPE)
  - Distributed (uCPE or Hybrid WAN) deployment
  - Combined centralized and distributed deployment
- SD-WAN solution

Figure 15: Cloud CPE and SD-WAN Solutions Topology



Different sites for an enterprise might connect to different regional POPs, depending on the geographical location of the sites. Within an enterprise, traffic from a site that connects to one regional POP travels to a site that connects to another regional POP through the

central POP. A site can connect to the Internet and other external links through either the regional POP or the central POP.

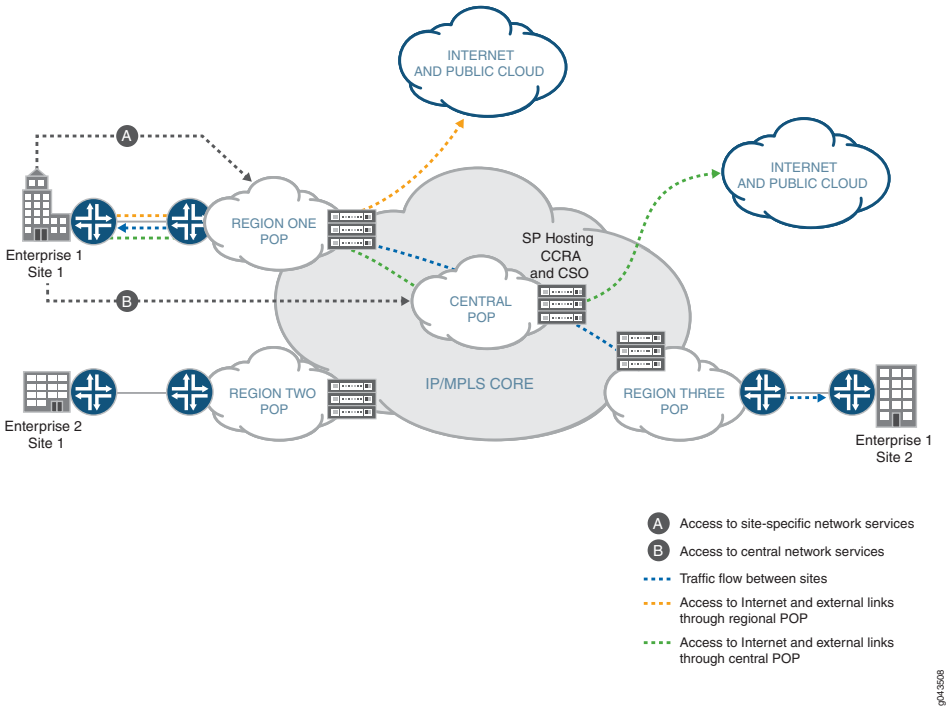
Service providers use the central server to set up the Cloud CPE solution through the Administration Portal. Similarly, customers activate and manage network services through their own dedicated view of the Customer Portal on the central server.

Topologies of the Specific Deployments

Centralized Deployment

Figure 16 on page 54 illustrates the topology of a centralized deployment. Customers access network services in a regional cloud through a Layer 3 VPN.

Figure 16: Centralized Deployment Topology



The central and regional POPs contain one or more Contrail Cloud implementations. VNFs reside on Contrail compute nodes and service chains are created in Contrail. You can choose whether to use the CSO OpenStack Keystone on the central infrastructure server or the OpenStack Keystone on the Contrail controller node in the central POP to authenticate CSO operations. The Contrail Cloud implementation provides Contrail Analytics for this deployment.

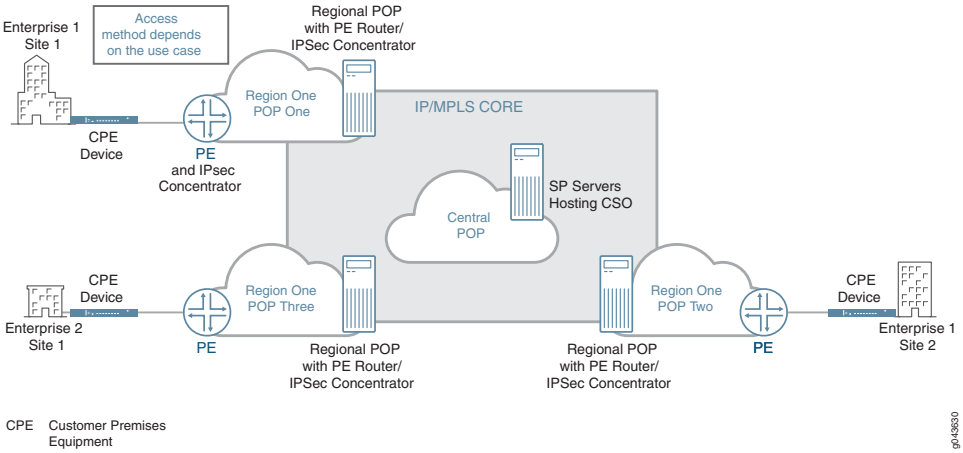
The MX Series router in the Contrail Cloud implementation is an SDN gateway and provides a Layer 3 routing service to customer sites through use of virtual routing and forwarding (VRF) instances, known in Junos OS as Layer 3 VPN routing instances. A unique routing table for each VRF instance separates each customer's traffic from other customers' traffic. The MX Series router is a PNE.

Sites can access the Internet directly, through the central POP, or both. Data traveling from one site to another passes through the central POP.

Distributed Deployment

Figure 17 on page 55 illustrates the topology of a distributed deployment.

Figure 17: Distributed Deployment Topology



Each site in a distributed deployment hosts a CPE device on which the vSRX application is installed to provide security and routing services. The Cloud CPE solution supports the following CPE devices:

- NFX250 Network Services Platform
- NFX150 Network Services Platform
- SRX Series Services Gateway
- vSRX

  The vSRX CPE device can reside at a customer site or in the service provider cloud. In both cases, you configure the site in CSO as an on-premise site. Authentication of the vSRX as a CPE device takes place through SSH.

An MX Series router in each regional POP acts as an IPsec concentrator and provider edge (PE) router for the CPE device. An IPsec tunnel, with endpoints on the CPE device and MX Series router, enables Internet access from the CPE device. Data flows from one site to another through a GRE tunnel with endpoints on the PE routers for the sites. The distributed deployment also supports SD-WAN functionality for traffic steering, based on 5-tuple (source IP address, source TCP/UDP port, destination IP address, destination TCP/UDP port and IP protocol) criteria.

Network administrators can configure the MX Series router, the GRE tunnel, and the IPsec tunnel through Administration Portal. Similar to the centralized deployment, the MX Series router in the distributed deployment is a PNE.

The CPE device provides the NFVI, which supports the VNFs and service chains. Customers can configure sites, CPE devices, and network services with Customer Portal.

The OpenStack Keystone resides on the central infrastructure server and Contrail Analytics resides on a dedicated VM or server.

SD-WAN Solution

The SD-WAN solution supports hub-and-spoke and full mesh VPN topologies.

Figure 18 on page 56 shows the SD-WAN solution using a hub and spoke topology. The figure shows two sites, each with two underlay connections, WAN_0 and WAN_1, and overlay tunnels across those connections to the hub device, or cloud hub. CSO, as the orchestration layer, along with BGP control connections is shown for reference.

Figure 18: SD-WAN Hub-and-Spoke Topology

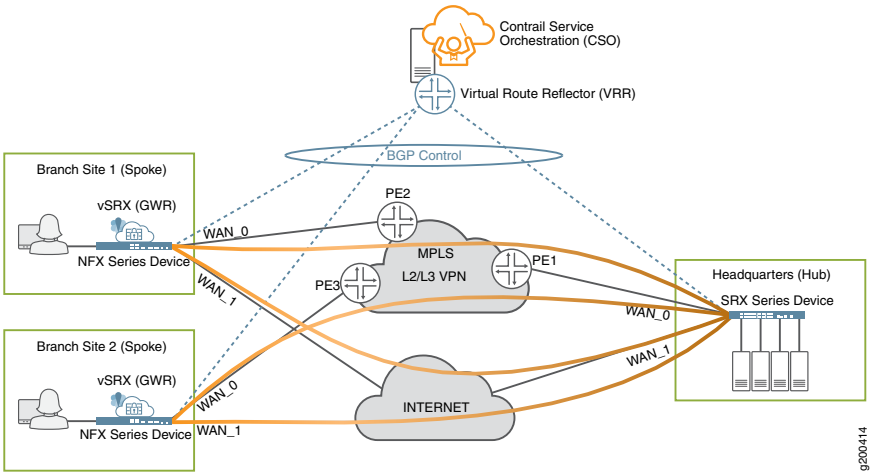
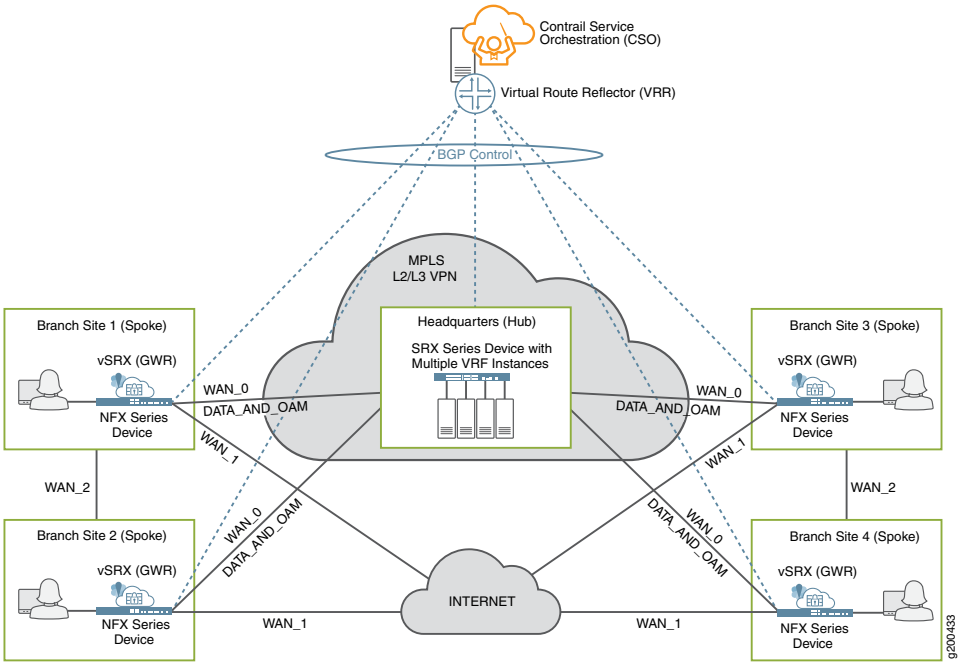


Figure 19 on page 57 shows a similar SD-WAN solution using a full mesh topology without the VPN overlays. Note that although the figure shows the DATA_AND_OAM connection on the MPLS link, WAN_0. this function can be performed on either the MPLS or Internet links.

Figure 19: SD-WAN Full Mesh Topology



The SD-WAN implementation supports a hub-and-spoke VPN topology, in which CPE devices reside at the spoke sites. The CPE devices are the same as those used in a distributed deployment. The hub device, which is an SRX Series gateway, typically serves all the spoke sites for all the customers in a POP. You can, however, dedicate a hub device to a specific tenant. In the hub-and-spoke topology, all traffic from a LAN segment passes through the hub, whether it is traveling to another of the customer's sites in the same POP or to the Internet.

A virtual route reflector (VRR) resides on a VM on each regional microservices server. During the CSO installation, a VRR is installed on the regional servers. The VRR has a fixed configuration that you cannot modify. Use of a VRR enhances scaling of the BGP network with low cost and removes the need for hardware-based route reflectors that require space in a data center and ongoing maintenance.

For VRR redundancy, you need to create at least two VRRs for a region. We recommend that you create VRRs in even numbers and assign these VRRs equally in different redundancy groups. Each hub or spoke device establishes a BGP peering session with two VRRs that are in different redundancy groups. If the primary VRR fails or connectivity is lost, the BGP peering session remains active because the secondary VRR continues to receive and advertise LAN routes to a device, thereby providing redundancy.

Redundancy groups are formed by logically separating VRRs based on following parameters:

- Physical server affinity—VRRs that reside on a same physical server should not belong to different redundancy group.

- Network affinity—VRRs that reside on a same network should not belong to different redundancy group.

There can be only two redundancy groups—group 0 and group 1. If you do not specify the redundancy group for VRRs, all VRRs are placed in the default redundancy group—group 0—and hub or spoke devices establish a BGP session with only one VRR.

Related Documentation

- Contrail Service Orchestration Solutions Overview on page 15

CHAPTER 5

Walkthrough of a Centralized CPE Deployment

Setting Up a Centralized Deployment

Before you set up a centralized deployment, complete the following tasks:

- Configure network devices and servers for the deployment. See the following topics:
  - Cabling the Hardware for the Centralized Deployment on page 61
  - Configuring the EX Series Ethernet Switch for the Contrail Cloud Implementation in a Centralized Deployment on page 63
  - Configuring the QFX Series Switch for the Contrail Cloud Implementation in a Centralized Deployment on page 64
  - Configuring the MX Series Router for the Contrail Cloud Implementation in a Centralized Deployment on page 67
  - Configuring the Physical Servers and Nodes for the Contrail Cloud Implementation in a Centralized Deployment on page 69
- Install Contrail Service Orchestration. See the following topics:
  - *Removing a Previous Deployment*
  - *Provisioning VMs on Contrail Service Orchestration Nodes or Servers*
  - *Setting Up the Installation Package and Library Access*

  - *Installing and Configuring Contrail Service Orchestration*
  - *Configuring Contrail OpenStack for a Centralized Deployment*
- Upload VNF images. See the following topics:
  - *Uploading the vSRX VNF Image for a Centralized Deployment*
  - *Uploading the LxCIPtable VNF Image for a Centralized Deployment*
  - *Uploading the Cisco CSR-1000V VNF Image for a Centralized Deployment*
- Install VNF licenses.

  You can use the **Licenses** page to install vSRX licenses. See "Contrail Service Orchestration License Tool" on page 38.
- Publish network services with Network Service Designer.

To set up a centralized deployment.

1. Log in to Administration Portal as a service provider operator.
2. Create the POPs and associated resources.
   - You must create a (Virtualized Infrastructure Manager) VIM for each POP.
   - You can add an MX Series router as a physical network element (PNE) to provide a Layer 3 routing service to customer sites through use of virtual routing and forwarding (VRF) instances.
   - You add the Junos Space element management system (EMS) if you use a VNF that requires this EMS.
3. Add or import customers (tenants) in Administration Portal.
4. Access Contrail and add the following rule to the default security group in the Contrail project.

   ```
   Ingress IPv4 network 0.0.0.0/0 protocol any ports any
   ```

5. Allocate network services to each customer.
6. Upload licenses for other VNFs.
7. Access the view for a specific customer.
8. Create cloud sites for the customer.
   a. Create a regional service edge site for each branch site in the customer's network.
   b. Create a local service edge site if customers access the Internet through the corporate VPN
9. If you configured a PNE, then associate the PNE with the site and configure a VRF for each customer site.

For detailed information about using Administration Portal, see the *Contrail Service Orchestration User Guide*.

Related Documentation

- Accessing the Contrail Services Orchestration GUIs on page 36
- Designing and Publishing Network Services on page 38
- Setting Up Customers' Networks on page 40

Cabling the Hardware for the Centralized Deployment

This section describes how to connect cables among the network devices and servers in the Contrail Cloud implementation. See Architecture of the Contrail Cloud Implementation in the Centralized Deployment for more information.

To cable the hardware:

1. Connect cables from the EX Series switch to the other devices in the network.

   See Table 12 on page 61 for information about the connections for the EX Series switch.

2. Connect cables from the QFX Series switch to the other devices in the network.

   See Table 13 on page 62 for information about the connections for the QFX Series switch.

3. Connect cables from the MX Series router to the other devices in the network.

   See Table 14 on page 63 for information about the connections for the MX Series router.

Table 12: Connections for EX Series Switch

Interface on EX Series Switch	Destination Device	Interface on Destination Device
eth0 (management interface)	EX Series switch	ge-0/0/41
ge-0/0/0	Server 1	IPMI
ge-0/0/1	Server 2	IPMI
ge-0/0/2	Server 3	IPMI
ge-0/0/3	Server 4	IPMI
ge-0/0/4	Server 5	IPMI
ge-0/0/5	Server 6	IPMI
ge-0/0/6	Server 7	IPMI
ge-0/0/20	Server 1	eth0
ge-0/0/21	Server 2	eth0

Table 12: Connections for EX Series Switch (continued)

Interface on EX Series Switch	Destination Device	Interface on Destination Device
ge-0/0/22	Server 3	eth0
ge-0/0/23	Server 4	eth0
ge-0/0/24	Server 5	eth0
ge-0/0/25	Server 6	eth0
ge-0/0/26	Server 7	eth0
ge-0/0/41	EX Series switch	eth0 (management interface)
ge-0/0/42	QFX Series switch	eth0 (management interface)
ge-0/0/44	MX Series router	fxp0
ge-0/0/46	MX Series router	ge-1/3/11
ge-0/0/47	Server 1	eth1

Table 13: Connections for QFX Series Switch

Interface on QFX Series Switch	Destination Device	Interface on Destination Device
eth0 (management interface)	EX Series switch	ge-0/0/42
xe-0/0/0	Server 1	eth2
xe-0/0/1	Server 2	eth2
xe-0/0/2	Server 3	eth2
xe-0/0/3	Server 4	eth2
xe-0/0/4	Server 5	eth2
xe-0/0/5	Server 6	eth2
xe-0/0/6	Server 7	eth2
xe-0/0/20	Server 1	eth3
xe-0/0/21	Server 2	eth3
xe-0/0/22	Server 3	eth3

Table 13: Connections for QFX Series Switch (continued)

Interface on QFX Series Switch	Destination Device	Interface on Destination Device
xe-0/0/23	Server 4	eth3
xe-0/0/24	Server 5	eth3
xe-0/0/24	Server 6	eth3
xe-0/0/25	Server 7	eth3
xe-0/0/46	MX Series router	xe-0/0/0
xe-0/0/47	MX Series router	xe-0/0/1

Table 14: Connections for MX Series Router

Interface on MX Series Router	Destination Device	Interface on Destination Device
fxp0 (management interface)	EX Series switch	ge-0/0/44
ge-1/3/11	EX Series switch	ge-0/0/46
xe-0/0/0	QFX Series switch	xe-0/0/46
xe-0/0/1	QFX Series switch	xe-0/0/47
ge-1/0/0 and ge-1/0/1 or xe-0/0/2 and xe-0/0/3, depending on the network	Service provider's device at the cloud	–

Related Documentation

- Configuring the EX Series Ethernet Switch for the Contrail Cloud Implementation in a Centralized Deployment on page 63
- Configuring the QFX Series Switch for the Contrail Cloud Implementation in a Centralized Deployment on page 64
- Configuring the MX Series Router for the Contrail Cloud Implementation in a Centralized Deployment on page 67
- Configuring the Physical Servers and Nodes for the Contrail Cloud Implementation in a Centralized Deployment on page 69

Configuring the EX Series Ethernet Switch for the Contrail Cloud Implementation in a Centralized Deployment

Before you configure the EX Series switch, complete any basic setup procedures and install the correct Junos OS software release on the switch.

To configure the EX Series switch:

1. Define VLANs for the IPMI ports. For example:

```
user@switch# set interfaces interface-range ipmi member-range ge-0/0/0 to
  ge-0/0/19
user@switch# set interfaces interface-range ipmi unit 0 family ethernet-switching
  port-mode access
user@switch# set interfaces interface-range ipmi unit 0 family ethernet-switching
  vlan members ipmi
user@switch# set interfaces vlan unit 60 family inet address 172.16.60.254/24
user@switch# set vlans ipmi vlan-id 60
user@switch# set vlans ipmi l3-interface vlan.60
```

2. Define a VLAN for the management ports. For example:

```
user@switch# set interfaces interface-range mgmt member-range ge-0/0/20 to
  ge-0/0/46
user@switch# set interfaces interface-range mgmt unit 0 family ethernet-switching
  port-mode access
user@switch# set interfaces interface-range mgmt unit 0 family ethernet-switching
  vlan members mgmt
user@switch# set interfaces vlan unit 70 family inet address 172.16.70.254/24
user@switch# set vlans mgmt vlan-id 70
user@switch# set vlans mgmt l3-interface vlan.70
```

3. Define a static route for external network access. For example:

```
user@switch# set routing-options static route 0.0.0.0/0 next-hop 172.16.70.253
```

Related Documentation

- Hardware and Software Used in Contrail Service Orchestration Solution Deployments on page 23
- Configuring the QFX Series Switch for the Contrail Cloud Implementation in a Centralized Deployment on page 64
- Configuring the MX Series Router for the Contrail Cloud Implementation in a Centralized Deployment on page 67

Configuring the QFX Series Switch for the Contrail Cloud Implementation in a Centralized Deployment

Before you configure the QFX Series switch, complete any basic setup procedures and install the correct Junos OS software release on the switch.

To configure the QFX Series switch:

1. Configure the IP address of the Ethernet management port. For example:

```
user@switch# set interfaces vme unit 0 family inet address 172.16.70.251/24
```

2. Configure integrated routing and bridging (IRB). For example:

```
user@switch# set interfaces irb unit 80 family inet address 172.16.80.254/24
```

3. Configure a link aggregation group (LAG) for each pair of server ports. For example:

```
user@switch# set interfaces xe-0/0/0 ether-options 802.3ad ae0
user@switch# set interfaces xe-0/0/20 ether-options 802.3ad ae0
user@switch# set interfaces ae0 mtu 9192
user@switch# set interfaces ae0 aggregated-ether-options lacp active
user@switch# set interfaces ae0 aggregated-ether-options lacp periodic fast
user@switch# set interfaces ae0 unit 0 family ethernet-switching interface-mode
  access
user@switch# set interfaces ae0 unit 0 family ethernet-switching vlan members data

user@switch# set interfaces xe-0/0/1 ether-options 802.3ad ae1
user@switch# set interfaces xe-0/0/21 ether-options 802.3ad ae1
user@switch# set interfaces ae1 mtu 9192
user@switch# set interfaces ae1 aggregated-ether-options lacp active
user@switch# set interfaces ae1 aggregated-ether-options lacp periodic fast
user@switch# set interfaces ae1 unit 0 family ethernet-switching interface-mode
  access
user@switch# set interfaces ae1 unit 0 family ethernet-switching vlan members data

user@switch# set interfaces xe-0/0/2 ether-options 802.3ad ae2
user@switch# set interfaces xe-0/0/22 ether-options 802.3ad ae2
user@switch# set interfaces ae2 mtu 9192
user@switch# set interfaces ae2 aggregated-ether-options lacp active
user@switch# set interfaces ae2 aggregated-ether-options lacp periodic fast
user@switch# set interfaces ae2 unit 0 family ethernet-switching interface-mode
  access
user@switch# set interfaces ae2 unit 0 family ethernet-switching vlan members data

user@switch# set interfaces xe-0/0/3 ether-options 802.3ad ae3
user@switch# set interfaces xe-0/0/23 ether-options 802.3ad ae3
user@switch# set interfaces ae3 mtu 9192
user@switch# set interfaces ae3 aggregated-ether-options lacp active
user@switch# set interfaces ae3 aggregated-ether-options lacp periodic fast
user@switch# set interfaces ae3 unit 0 family ethernet-switching interface-mode
  access
user@switch# set interfaces ae3 unit 0 family ethernet-switching vlan members data

user@switch# set interfaces xe-0/0/4 ether-options 802.3ad ae4
user@switch# set interfaces xe-0/0/24 ether-options 802.3ad ae4
user@switch# set interfaces ae4 mtu 9192
user@switch# set interfaces ae4 aggregated-ether-options lacp active
user@switch# set interfaces ae4 aggregated-ether-options lacp periodic fast
user@switch# set interfaces ae4 unit 0 family ethernet-switching interface-mode
  access
user@switch# set interfaces ae4 unit 0 family ethernet-switching vlan members data

user@switch# set interfaces xe-0/0/5 ether-options 802.3ad ae5
user@switch# set interfaces xe-0/0/25 ether-options 802.3ad ae5
user@switch# set interfaces ae5 mtu 9192
user@switch# set interfaces ae5 aggregated-ether-options lacp active
user@switch# set interfaces ae5 aggregated-ether-options lacp periodic fast
user@switch# set interfaces ae5 unit 0 family ethernet-switching interface-mode
  access
user@switch# set interfaces ae5 unit 0 family ethernet-switching vlan members data
```

```
user@switch# set interfaces xe-0/0/6 ether-options 802.3ad ae6
user@switch# set interfaces xe-0/0/26 ether-options 802.3ad ae6
user@switch# set interfaces ae6 mtu 9192
user@switch# set interfaces ae6 aggregated-ether-options lacp active
user@switch# set interfaces ae6 aggregated-ether-options lacp periodic fast
user@switch# set interfaces ae6 unit 0 family ethernet-switching interface-mode
  access
user@switch# set interfaces ae6 unit 0 family ethernet-switching vlan members data

user@switch# set interfaces xe-0/0/7 ether-options 802.3ad ae7
user@switch# set interfaces xe-0/0/27 ether-options 802.3ad ae7
user@switch# set interfaces ae7 mtu 9192
user@switch# set interfaces ae7 aggregated-ether-options lacp active
user@switch# set interfaces ae7 aggregated-ether-options lacp periodic fast
user@switch# set interfaces ae7 unit 0 family ethernet-switching interface-mode
  access
user@switch# set interfaces ae7 unit 0 family ethernet-switching vlan members data

user@switch# set interfaces xe-0/0/8 ether-options 802.3ad ae8
user@switch# set interfaces xe-0/0/28 ether-options 802.3ad ae8
user@switch# set interfaces ae8 mtu 9192
user@switch# set interfaces ae8 aggregated-ether-options lacp active
user@switch# set interfaces ae8 aggregated-ether-options lacp periodic fast
user@switch# set interfaces ae8 unit 0 family ethernet-switching interface-mode
  access
user@switch# set interfaces ae8 unit 0 family ethernet-switching vlan members data
```

4. Configure a VLAN for data transmission. For example:

```
user@switch# set vlans data vlan-id 80
user@switch# set vlans data l3-interface irb.80
```

5. Configure OSPF routing. For example:

```
user@switch# set interfaces irb unit 80 family inet address 172.16.80.254/24
user@switch# set protocols ospf area 0.0.0.0 interface irb.80 passive
```

6. Configure the interface that connects to the MX Series router. For example:

```
user@switch# set interfaces xe-0/0/46 ether-options 802.3ad ae9
user@switch# set interfaces xe-0/0/47 ether-options 802.3ad ae9

user@switch# set interfaces ae9 aggregated-ether-options lacp active
user@switch# set interfaces ae9 aggregated-ether-options lacp periodic fast
user@switch# set interfaces ae9 unit 0 family inet address 172.16.10.253/24

user@switch# set protocols ospf area 0.0.0.0 interface ae9.0
```

Related Documentation

- Configuring the EX Series Ethernet Switch for the Contrail Cloud Implementation in a Centralized Deployment on page 63
- Configuring the MX Series Router for the Contrail Cloud Implementation in a Centralized Deployment on page 67

Configuring the MX Series Router for the Contrail Cloud Implementation in a Centralized Deployment

Before you configure the MX Series router, complete any basic setup procedures and install the correct Junos OS software release on the switch.

To configure the MX Series router:

1. Configure interfaces, IP addresses, and basic routing settings. For example:

```
user@router# set interfaces ge-1/0/0 unit 0 family inet address 10.87.24.77/28
user@router# set interfaces lo0 unit 0 family inet address 172.16.100.1/32
user@router# set routing-options route-distinguisher-id 172.16.100.1
user@router# set routing-options autonomous-system 64512
user@router# set protocols ospf area 0.0.0.0 interface lo0.0

user@router# set interfaces ge-1/0/0 unit 0 family inet service input service-set s1
  service-filter ingress-1
user@router# set interfaces ge-1/0/0 unit 0 family inet service output service-set s1
  service-filter ingress-1
```

2. Configure the interfaces that connect to the QFX Series switch. For example:

```
user@router# set chassis aggregated-devices ethernet device-count 2
user@router# set interfaces xe-0/0/0 gigether-options 802.3ad ae0
user@router# set interfaces xe-0/0/1 gigether-options 802.3ad ae0
user@router# set interfaces ae0 aggregated-ether-options lacp periodic fast
user@router# set interfaces ae0 unit 0 family inet service input service-set s1
  service-filter ingress-1
user@router# set interfaces ae0 unit 0 family inet service output service-set s1
  service-filter ingress-1
user@router# set interfaces ae0 unit 0 family inet address 172.16.10.254/24
user@router# set protocols ospf area 0.0.0.0 interface ae0.0
```

3. Configure BGP and tunneling for the service provider's cloud. For example:

```
user@router# set chassis fpc 0 pic 0 tunnel-services
user@router# set chassis fpc 0 pic 0 inline-services bandwidth 1g
user@router# set routing-options dynamic-tunnels dynamic_overlay_tunnels
  source-address 172.16.100.1
user@router# set routing-options dynamic-tunnels dynamic_overlay_tunnels gre
user@router# set routing-options dynamic-tunnels dynamic_overlay_tunnels
  destination-networks 172.16.80.0/24
user@router# set protocols mpls interface all
user@router# set protocols bgp group Contrail_Controller type internal
user@router# set protocols bgp group Contrail_Controller local-address 172.16.100.1
user@router# set protocols bgp group Contrail_Controller keep all
user@router# set protocols bgp group Contrail_Controller family inet-vpn unicast
user@router# set protocols bgp group Contrail_Controller neighbor 172.16.80.2
user@router# set protocols bgp group Contrail_Controller neighbor 172.16.80.3
user@router# set protocols ospf export leak-default-only
```

4. Set up routing. For example:

```
user@router# set routing-options static rib-group inet-to-public
user@router# set routing-options static route 0.0.0.0/0 next-hop 10.87.24.78
user@router# set routing-options static route 0.0.0.0/0 retain
user@router# set routing-options static route 10.87.24.64/26 next-table public.inet.0
user@router# set routing-options rib-groups inet-to-public import-rib inet.0
user@router# set routing-options rib-groups inet-to-public import-rib public.inet.0
user@router# set routing-options rib-groups inet-to-public import-policy
  leak-default-only
user@router# set policy-options policy-statement leak-default-only term default
  from route-filter 0.0.0.0/0 exact
user@router# set policy-options policy-statement leak-default-only term default then
  accept
user@router# set policy-options policy-statement leak-default-only then reject
user@router# set routing-instances public instance-type vrf
user@router# set routing-instances public interface lo0.10
user@router# set routing-instances public vrf-target target:64512:10000
user@router# set routing-instances public vrf-table-label
user@router# set routing-instances public routing-options static route 10.87.24.64/26
  discard
```

5. Configure NAT. For example:

```
user@router# set services service-set s1 nat-rules rule-napt-zone
user@router# set services service-set s1 interface-service service-interface si-0/0/0.0
user@router# set services nat pool contrailui address 10.87.24.81/32
user@router# set services nat pool openstack address 10.87.24.82/32
user@router# set services nat pool jumphost address 10.87.24.83/32
user@router# set services nat rule rule-napt-zone term t1 from source-address
  172.16.80.2/32
user@router# set services nat rule rule-napt-zone term t1 then translated source-pool
  openstack
user@router# set services nat rule rule-napt-zone term t1 then translated
  translation-type basic-nat44
user@router# set services nat rule rule-napt-zone term t2 from source-address
  172.16.80.4/32
user@router# set services nat rule rule-napt-zone term t2 then translated source-pool
  contrailui
user@router# set services nat rule rule-napt-zone term t2 then translated
  translation-type basic-nat44
user@router# set services nat rule rule-napt-zone term t3 from source-address
  172.16.70.1/32
user@router# set services nat rule rule-napt-zone term t3 then translated source-pool
  jumphost
user@router# set services nat rule rule-napt-zone term t3 then translated
  translation-type basic-nat44
user@router# set firewall family inet service-filter ingress-1 term t1 from source-address
  172.16.80.2/32
user@router# set firewall family inet service-filter ingress-1 term t1 from protocol tcp
user@router# set firewall family inet service-filter ingress-1 term t1 from
  destination-port-except 179
user@router# set firewall family inet service-filter ingress-1 term t1 then service
user@router# set firewall family inet service-filter ingress-1 term t2 from source-address
  172.16.80.4/32
user@router# set firewall family inet service-filter ingress-1 term t2 then service
```

```
user@router# set firewall family inet service-filter ingress-1 term t3 from source-address
  172.16.70.1/32
user@router# set firewall family inet service-filter ingress-1 term t3 then service
user@router# set firewall family inet service-filter ingress-1 term end then skip
```

Related Documentation

- Hardware and Software Used in Contrail Service Orchestration Solution Deployments on page 23
- Configuring the EX Series Ethernet Switch for the Contrail Cloud Implementation in a Centralized Deployment on page 63
- Configuring the QFX Series Switch for the Contrail Cloud Implementation in a Centralized Deployment on page 64

Configuring the Physical Servers and Nodes for the Contrail Cloud Implementation in a Centralized Deployment

For a centralized deployment, you must configure the physical servers and nodes in the Contrail Cloud implementation and install Contrail OpenStack on the server cluster before you run the installer.

To install Contrail OpenStack:

1. Configure hostnames for the physical servers and nodes.
2. Configure IP addresses for the Ethernet management ports of the physical servers and nodes.
3. Configure DNS on the physical servers and nodes, and ensure that DNS is working correctly.
4. Configure Internet access for the physical servers and nodes.
5. From each server and node, verify that you can ping the IP addresses and hostnames of all the other servers and nodes in the Contrail Cloud implementation.
6. Using Contrail Server Manager, install Contrail OpenStack on the server cluster and set up the roles of the Contrail nodes in the cluster.

   You configure an OpenStack Keystone on the primary Contrail controller node in the central Contrail Cloud implementation, and also use this Keystone for:

   - Regional Contrail configure and control nodes
   - Redundant configure and control nodes in the central Contrail Cloud implementation

Refer to the Contrail documentation for information about installing Contrail OpenStack and configuring the nodes.

7. For each node, use the ETCD keys to specify the same username and password for Contrail.

   CSO uses the BASIC authentication mechanism to establish a connection to Contrail.

Related Documentation

CHAPTER 6

Walkthrough of a Distributed CPE Deployment

Setting Up a Distributed Deployment

The following workflow describes the steps required to set up a Hybrid WAN (distributed CPE) deployment.

Before you can start a deployment, complete the following tasks:

- Provision your VMs according to the steps discussed in Contrail Service Orchestration Install and Upgrade Guide

  NOTE: If you are provisioning your VMs on a KVM-based hypervisor, you must complete the steps in Creating a Data Interface for a Distributed Deployment prior to provisioning. This step creates a required bridge interface for the VMs to communicate with the CPE devices.

- Complete the CSO installation as per the CSO Install and Upgrade Guide.
- Publish network services with Network Service Designer.

  Publishing the VNFs as network services allows them to be seen in the CSO Administration portal under the **Allocate Network Services** links for installed tenants. See "Designing and Publishing Network Services" on page 38 and the *Contrail Service Orchestration User Guide* for details.

After you have installed Contrail Service Orchestration and published network services with Network Service Designer, you use Administration Portal to set up the distributed deployment. The following workflow describes the process:

1. Log in to Administration Portal.
2. Add or import customers (tenants) in Administration Portal.

   Tenants in the Cloud CPE solution represent customers who accesses virtualized network functions (VNFs) in a service provider's cloud through a Layer 3 VPN. Create one tenant for each customer who will use your network services

   For distributed CPE deployments, choose Hybrid WAN topology after entering the tenant administrator information in the add tenant pop-up. See The Contrail Service Orchestration User Guide for more information about adding and importing tenants
3. Allocate networks services to each customer.

   All of the published network services are listed in the pop-up window that comes up when you click **Allocate Network Services** under the **Assigned Services** column of the tenants list. The number of services assigned to a particular tenant is shown for those tenants which have services assigned. The **Allocate Network Services** link is only shown if no services have been allocated for that tenant.
4. Access the tenant view for the first customer by clicking the tenant name link from the list of tenants.
5. Add an on-premises spoke site for each site in the customer's network.

   NOTE: **Alternatively customers can add the spoke sites themselves.**

   For this deployment guide, we will focus on the spoke sites. Information about Local Service Edge Sites and Regional Service Edge Sites can be found in the *Contrail Service Orchestration User Guide*.
6. Repeat Step 3 for each customer in the network.
7. Access the All Tenants view for the customers.
8. Add data for the POPs and provider edge (PE) router.
9. Upload images for devices used in the deployment, such as the vSRX gateway, NFX250 CPE devices or NFX150 CPE devices, to the central activation server.
10. Configure activation data for CPE devices.

    NOTE: **You must send an activation code to the customer for each NFX250 or NFX150 device. The customer's administrative user must provide this code during the NFX installation and configuration process. The Juniper Networks Redirect Service uses this code to authenticate the device.**
11. Upload VNF images.
12. Upload and install licenses:
    1. Upload licenses for vSRX and SRX devices and VNFs with the using the
    2. Upload licenses for other VNFS with Administration Portal.

3. Manually install licenses for other VNFs.

13. Allocate network services to customers.
14. Activate CPE devices at customer sites.

NOTE: **Alternatively customers can activate the devices themselves.**

When an administrator installs and configures the NFX devices at a customer site, the device automatically interacts with the Redirect Service. The Redirect Service authenticates the device and sends information about its assigned regional server. The device then obtains a boot image and configuration image from the regional server and uses the images to become operational.

Customers activate SRX Series Services Gateways and vSRX instances acting as CPE devices through Customer Portal.

For detailed information about using Administration Portal, see the *Contrail Service Orchestration User Guide.*

Related Documentation

- Accessing the Contrail Services Orchestration GUIs on page 36
- Installing and Setting Up CPE Devices on page 78

Configuring the Physical Servers in a Distributed Deployment

For a distributed deployment, you must configure the Contrail Service Orchestration (CSO) and Contrail Analytics servers (or nodes, if you are using a node server) before you run the installer.

To configure the servers:

1. Configure hostnames for the physical servers.
2. Configure IP addresses for the Ethernet management ports of the physical servers.
3. Configure DNS on the physical servers, and ensure that DNS is working correctly.
4. Configure Internet access for the physical servers and nodes.
5. From each server and node, verify that you can ping the IP addresses and hostnames of all the other servers and nodes in the distributed deployment.
6. For a medium or large environment, install Contrail OpenStack on the Contrail Analytics server.

   Refer to the Contrail documentation for information about installing Contrail OpenStack.

Related Documentation

- Hardware and Software Used in Contrail Service Orchestration Solution Deployments on page 23

Configuring the MX Series Router in a Distributed Deployment

You need to configure interfaces, virtual routing and forwarding instances (VRFs), and DHCP on the MX Series router with Junos OS. You can, however, use Administration Portal to specify configuration settings for both endpoints of the required IPSec tunnel between the MX Series router and the NFX250 with Administration Portal. When the NFX250 becomes operational, Contrail Service Orchestration (CSO) components set up the tunnel.

To configure the MX Series router in Junos OS:

1. Configure the interfaces on the MX Series router.

   For example:

```
ge-0/3/7 {
        description "to nfx wan0 i.e. ge-0/0/10";
        vlan-tagging;
        unit 10 {
            description "NFX WAN_0 data";
            vlan-id 10;
            family inet {
                address 195.195.195.1/24;
            }
        }
        unit 20 {
            description "NFX WAN_0 OAM";
            vlan-id 20;
            family inet {
                address 196.196.196.254/24;
            }
        }
    }
    ge-0/3/8 {
        description "to nfx wan1 i.e. ge-0/0/11 FOR IPSEC";
        unit 0 {
            family inet {
                address 198.198.198.1/24;
            }
        }
    }
```

2. Configure a VRF for Operation, Administration, and Maintenance (OAM) traffic between Contrail Service Orchestration and the NFX250.

For example:

```
nfx-oam {
        instance-type vrf;
        interface ge-0/0/0.220;
        vrf-target target:64512:10000;
        vrf-table-label;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 192.168.220.2;
            }
        }
    }
```

3. Configure a VRF for data traffic that travels over the wide area network (WAN).

   Data that travels through the IPSec tunnel also uses this VRF. When you configure the MX endpoint of the IPSec tunnel in Administration Portal, you specify these VRF settings.

   For example:

```
nfx-data {
        instance-type vrf;
        interface ge-0/3/7.10;
        vrf-target target:64512:10001;
        vrf-table-label;
        protocols {
            bgp {
                group nfx-gwr-bgp-grp {
                    type external;
                    family inet {
                        unicast;
                    }
                    export send-direct;
                    peer-as 65000;
```

```
                    neighbor 195.195.195.2;
                }
            }
        }
    }
```

4. Configure DHCP on the MX Series router.

```
System{
    Services {
        dhcp-local-server {
            group 8-csp-gpr {
                interface ge-0/3/8.0;
            }
        }
    }


access {
    address-assignment {
        pool 8-csp-gpr-pool {
            family inet {
                network 198.198.198.0/24;
                range valid {
                    low 198.198.198.5;
                    high 198.198.198.250;
                }
                dhcp-attributes {
                    domain-name juniper.net;
                    name-server {
                        8.8.8.8;
                    }
                }
```

```
                }
            }
        }
    }
```

Related Documentation

- Hardware and Software Used in Contrail Service Orchestration Solution Deployments on page 23
- Overview of Solution Topologies on page 53
- Configuring the Physical Servers in a Distributed Deployment on page 73

Installing and Setting Up CPE Devices

- Preparing for CPE Device Activation on page 78
- Installing and Configuring an NFX Series Device on page 78
- Installing and Configuring an SRX Series Services Gateway or vSRX Instance as a CPE Device on page 78

Preparing for CPE Device Activation

Before customers can activate a CPE device, you must complete the following tasks:

- Specify activation data with Administration Portal or the API for each CPE device, such as:
  - The name of the site for the device
  - The serial number
  - The activation code (NFX250 and NFX150 devices only)

Installing and Configuring an NFX Series Device

An administrator at the customer's site installs the NFX device and performs the initial software configuration for the NFX. These are straightforward tasks that involve a limited amount of hardware installation, cabling, and software configuration. See the NFX Series documentation for more information.

When the administrator completes the initial configuration process, the NFX device obtains a boot image and configuration image from its regional server and becomes operational.

Installing and Configuring an SRX Series Services Gateway or vSRX Instance as a CPE Device

An administrator at the customer's site installs and configures an SRX Series Services Gateway or a vSRX instances as a CPE device using the following workflow:

1. Install the hardware and cable the device.

2. Power on the device and access the device console.
3. Log in to Customer Portal and perform the following tasks:
   - Add the site to the network.
   - Apply the initial configuration to the device.
   - Activate the CPE device.

Related Documentation

- Setting Up a Distributed Deployment on page 71
- NFX Series documentation
- SRX Series documentation
- vSRX documentation

CHAPTER 7

Walkthrough of an SD-WAN Deployment

Setting Up an SD-WAN Deployment

About This SD-WAN Deployment

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

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

Setting Up an SD-WAN Deployment

- Provision your VMs according to the steps discussed in Contrail Service Orchestration Install and Upgrade Guide

  NOTE: If you are provisioning your VMs on a KVM-based hypervisor, you must complete the steps in Creating a Data Interface for a Distributed Deployment prior to provisioning. This step creates a required bridge interface for the VMs to communicate with the CPE devices.

- Complete the CSO installation as per the CSO Install and Upgrade Guide.
- Purchase an Advanced Policy-based Routing license for a vSRX. You must purchase a license that includes the **appid-sig** feature.
- Download the required vSRX KVM appliance software image from the Juniper Networks Software Download site. For CSO Release 4.0.0, the required version is **15.1X49-D143**. Other hardware and software versions can be found in "Hardware and Software Used in Contrail Service Orchestration Solution Deployments" on page 23.

To set up an SD-WAN deployment:

1. **Access the Administration Portal by logging into Contrail Service Orchestration (CSO) with the Administrator login.**

   See "Accessing the Contrail Services Orchestration GUIs" on page 36 for details.

2. **Download Application Signatures**

   To download the application signatures, navigate to the **Administration > Signature Database** page.

   On this page, there is a list of available database versions, their publish dates, update summaries, and detector versions. The newest database is at the top of the list. Downloading the signature database makes the application signatures available to install on your CPE device after it has been activated in a later step.

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

3. **Upload License**

   To upload the license for your vSRX gateway router (GWR) device, navigate to the **Administration > Licenses** page.

   On this page is a list of all available device licenses. Since you have not installed any licenses yet, the list is empty. Click the **+** icon at the top-right part of the list to add a license. This brings up a window in which you click the **Browse** button to locate the license file that you purchased for the vSRX.

   License files are associated with specific tenants because the devices that they install on are exclusive to the tenant. If you had already created tenants, you could specify to which tenant this license file belonged. Since you don't have any, leave the tenant field blank. You assign the tenant in a later step when you push the license to the device.

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

4. **Create Tenant**

   To create a CSO tenant, or customer, navigate to the **Tenants** page.

   On this page, you can view a list of information about all installed tenants. Since you don't have any tenants the list is empty. Click the **+** icon at the top-right part of the list to add a tenant. This brings up a window in which you fill out information regarding the new tenant including its name, information about the tenant administrator, and the roles that the administrator will have. All of the information is required. Service providers (SPs) in an enterprise environment may want to name the tenants after branch office locations or retail store locations. Name the tenant something that makes sense for your deployment. Assign roles to the tenant admin as needed by

selecting the check box next to the role and then clicking the > button to move the role from available to selected. For this example, select all of the roles. Detailed information about the different roles can be found in the *Contrail Service Orchestration User Guide*.

Click Next. This changes the window to display the available topologies for deployment. The tenant can have a Hybrid WAN deployment, an SD-WAN deployment, or both. Leaving either of the boxes unchecked restricts this tenant from ever building a deployment based on the unchecked deployment type. Un-check the box next to Hybrid WAN since you are only deploying SD-WAN in this example. With an SD-WAN deployment, you have two topology options: Full Mesh and Hub-and-Spoke. You can only select one topology per deployment. For this example, click the Hub-and-Spoke topology.

Click Next. This changes the window to display available tenant properties, each with a brief description of what they do. Clicking the > icon to the left of each property expands it to show what information is needed for that property. For this example, click the > next to **SD-WAN Mode**. This shows two radio buttons that allow the SD-WAN mode to be set as **Bandwidth Optimized** or **Real-time Optimized**. The **Compare** link below the radio buttons brings up information regarding what can and cannot be done with each mode.

For this example, select the **Bandwidth Optimized** radio button.

Click Next. This changes the window to the summary page. Review what you have input and click Ok. A pop-up display indicates a job has been created. Another pop-up will display when the job completes. Then the list of tenants refreshes.

NOTE: When the tenant is created, an email is sent to the tenant administrator's email address that you entered. This email contains the username (email address) and password (auto-generated) for the tenant.

5. **Enable Application Traffic Type Profile**

   You can customize class-of-service and probe parameters with traffic type profiles. All traffic type profiles are disabled by default A maximum of six traffic type profiles can be enabled at one time.

   To enable application traffic type profiles, navigate to the **Configuration > Application Traffic Type Profiles** page. Here you can see the built-in application traffic type profiles.

   Click the check box next to Internet, then click the **Pencil** icon at the upper right part of the list to edit the profile.

   In the new window that appears, you can see the parameters that make up this profile. Click the **Toggle Switch** next to **Status**. This enables the profile for use in an Application SLA Profile that you create later.

   Click **OK**.

6. **Choose a Device Template for the CPE Device**

To choose the proper device template, navigate to the **Resources > Device Templates** page. Here you can see the pre-installed device templates in CSO. Scroll through the list and click the check box next to the appropriate template for your CPE device. For example, if you are using an NFX250 as the CPE device in your SD-WAN deployment, you would click: **NFX250 as SD-WAN CPE**. At the top-right part of the list select the drop-down menu **Edit Device Template** and select **Template Settings**.

A pop up window appears in which all of the settings for the selected template are pre-populated. Make note of the exact name in the field **GWR_VSRX_IMAGE_CNAME_IN_CSO**. This is the name of the software image that the CPE device need in order to instantiate the vSRX GWR. In the case of the vSRX GWR in an NFX250, it is **vsrx-vmdisk-15.1.qcow2**. Feel free to check out the other available settings, but for this example, do not make any changes. Click **Cancel**.

7. **Upload Software image for vSRX**

   To upload a software image, navigate to the **Resources > Images** page. Here you can see the software images that have been uploaded to CSO.

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

   In the top-right part of the list, click the **+** icon to create a new image. The page that pops up requires that you fill in all of the fields except Description and Supported Platform.

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

   Select **VNF Image** as the image type.

   Click **Browse** and select the **.qcow2** software image that you downloaded previously.

   Select **Juniper** as the Vendor.

   Select **juniper-vsrx** as the Family.

   Fill in the Major Version Number, Minor Version Number, and Build Number as **15**, **1**, and **X49-D130**, respectively.

   Click **Upload**. CSO displays a progress window as the file is uploaded.

8. **Create Point of Presence (POP) for Cloud Hub Device**

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

   To create a POP, navigate to the **Resources > POPs** page. Here you can see a list of POPs. Since you have not created any POPs, the list is empty.

   At the top-right part of the list, click the **+** icon to create a new POP.

A pop-up window appears that requires you to enter basic information about the POP such as POP name and Address Information.

In CSO Release 4.0.0, all POPs are regional.

Give the POP a name that makes sense, like **bay-area-pop**, and enter the appropriate address information. CSO uses this information to place the POP on a map in certain monitoring screens.

Click **Next**. The workflow window changes to allow you to add optional device information. The lower portion of the window allows you to create a device to put in the POP during this workflow, but for this example just click **Next** on this and the next two pages. At the summary page, click **Enter**.

9. **Create Cloud Hub Device**

   A cloud hub device resides in a regional POP within the service provider's network or cloud. To create a Cloud Hub, navigate to the **Resources > Cloud Hub Devices** page. Here you can see a list of all cloud hub devices, their POP, and site associations, status, model, serial number, and OS version.

   At the top-right part of the list, click the **+** icon to add a cloud hub device. A pop-up workflow window appears in which you define the cloud hub device.

   Name the hub something that makes sense, like **srx-1500-1**. Cloud hub devices can be shared amongst multiple tenants through the use of virtual routing and forwarding (VRF) instances configured on the hub itself.

   regional is the only choice for **Management Region**.

   Pull down the list of POPs and select the POP that you just created.

   Select **DATA_AND_OAM** for **Capability**. This allows both operation, administration, and maintenance (OAM) and user data to traverse this device. It ensures that CSO can manage on-premises CPE devices through this hub device.

   Select **SRX as SDWAN Hub** for **Device Template**. Other options for the hub device also populate the list. The list is built from the Device Templates list that you looked at in step 6. Multiple tenants can share this hub. There is usually one hub per POP.

   In the **Configuration** section on the **Connectivity** tab, fill in the **Management Connectivity** section.

   - Enter a 32-bit IP address prefix such as **10.10.10.123/32** as the **Loopback IP Prefix** for the CPE device. Be sure to use an address that works within your network. This address is used for BGP peering. The IP address prefix must be a /32 IP address prefix and must be unique across the entire management network.
   - Select an appropriate interface, such as **ge-0/0/3** as the OAM Interface of the CPE device.

   NOTE: The device template that was selected in step 6, contained interface assignments for WAN_0 and WAN_1 interfaces. You must choose an unused

- Leave the OAM VLAN ID blank

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

- Enter an IP address prefix, such as **10.100.100.11/32**, for the **OAM IP Prefix**. The OAM IP Prefix must be unique across the entire management network.

NOTE: For NFX Series services gateways like we are using in this example, specify the IP address prefix as /32 if USE_SINGLE_SSH is set on the NFX. If USE_SINGLE_SSH is not set, then use a /29 or higher prefix. For SRX series CPE devices, always use a /32 prefix.

- Enter an IP address, such as **10.100.100.1**, for the **OAM Gateway**. This is the IP address of the next-hop on the management network through which CSO connectivity must be established.

Click the check box under the WAN_0 section to enable the WAN_0 interface of the CPE device. The physical device interface is already chosen from the value in the device template and cannot be altered here.

Leave the Link Type as MPLS.

NOTE: Internet is the other available link type. Since there is usually only one MPLS connection to any given service provider, any other WAN connections that you set up will likely have the link type set to Internet.

Select **Static** for the **Address Assignment**.

Enter an IP address prefix, such as **172.21.22.1/29**, for the **Static IP Prefix**. This represents the hub-side address of the hub-to-cpe network connection.

Enter an IP address, such as **172.21.22.2**, for the **Gateway IP Address**. This is the IP address of the GWR on the NFX250 at the customer site.

Select the Devices tab. Under **Device Details**, Enter the serial number of the hub device and the name of the boot image that you uploaded previously.

When you have finished, click **OK** and a pop-up message telsl you that the device is being added. When the add completes, the list refreshes and shows the new cloud hub device in **EXPECTED** state under **Management Status.**

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

10. **Activate Cloud Hub Device**

    To activate the cloud hub device, navigate to the **Resources > Cloud Hub Devices** page. Click the **Activate Device** button at the top-right of the list. A new window appears that shows the stages of activation. The stages should flow from EXPECTED to DEVICE_DETECTED to Stage-one configuration applied to Bootstrap successful to Device Active.

    Click **Ok**. The **Activate Device** window closes and your device is listed as PROVISIONED in the **Management Status** column. Once your cloud hub device is in the PROVISIONED state, you can proceed to the next step.

11. **Create Site for Cloud Hub**

    To add a site for the cloud hub you assume the role of the tenant administrator. To do this, navigate to the **Global** menu and select the tenant that you created in step 5.

    Navigate to the **Sites > Site Management** page. Here you see an empty list of sites.

    Click the **Add** button at the top-right of the list. Select **Cloud Hub** from the list.

    The only required fields in the new window that pops up are **Site Name**, **Service POP**, and **Hub Device Name**. You can fill in the other fields as appropriate.

    Give the site a name that makes sense, such as naming it after the POP that its in, like **bay-area-pop-site1**.

    Select your previously created POP from the **Service POP** list.

    Select your previously created hub device from the **Hub Device Name** list.

    Click **OK**. A pop-up message tells you that the add site job has been created. When it finishes, the list refreshes and shows the new site.

12. **Configure Spoke Site**

    A CSO spoke site is needed to contain the CPE device that gets shipped the customer site. To do this, click the **Add** button and select **On-premise Spoke**.

    In the workflow window that appears, fill in the name of the on-premise site such as **Site1** and click **Next**.

    In Connectivity Requirements, select the appropriate connection plan for your CPE device, such as **NFX250 as SD-WAN CPE** for an NFX250. The WAN Underlay Links appear below the Connection Plan.

    Click the check box next to WAN_0 to enable this link.

    Leave the **Connection Type** as MPLS.

    Leave the **Access Type** as Ethernet for an MPLS connection. You can select ADSL, Ethernet, LTE, or VDSL as appropriate when using an Internet **Connection Type**.

    Set the **Subscribed Bandwidth** to the appropriate setting for this link, such as**15**.

    Enter the **Provider** name as the name of the service provider, like **Juniper**.

Enter the **Cost/Month** as the cost per month for using this link. This number is used in SD-WAN link-switch calculations.

Click the check box next to WAN_1 to enable this link.

Set the **Connection Type** as Internet.

Set the **Access Type** to the appropriate type: ADSL, Ethernet, LTE, or VDSL

Set the **Subscribed Bandwidth** to the appropriate value for this link.

Enter the **Provider** name as the name of the service provider, like **Comcast**.

Enter the **Cost/Month** as **40**.

Click **Next**. The workflow proceeds to Additional Requirements. Here you select the default and backup links for the connection.

Set **Default Link** to whichever link **WAN_0 (MPLS)**.

Set **Backup Link** to **WAN_1 (Internet)**.

Click **Next**. The workflow proceeds to LAN Segments. Here you must add at least one LAN segment for the on-premise site.

NOTE: Additional LAN segments can be added. CSO provides the ability to set up multiple LAN segments for the customer based on departments. In this case, each department gets its own IPSec VPN in order to keep traffic separated.

Name the LAN segment to something that makes sense, like **Site1-LAN**.

Assign one or more **Ports** to be used on the CPE device for this LAN segment, like **LAN_0 (ge-0/0/0)**.

Set the **IP Address Prefix** to something that meets the requirements of the customer LAN, such as **172.20.13.0/24** or whatever is required at the site.

Leave the **Department** as **Default**. In case you have set up multiple departments during the tenant creation phase, you can choose the appropriate

If you toggle the **DHCP** switch, you can have the NFX provide DHCP Services for the site on that LAN segment.

Click **Save**, then click **Next**.

The workflow proceeds to Summary. Review the summary and click **OK**. A pop up message appears telling you that the Create Site job was created.

13. **Activate Spoke Site Device**

    The activate spoke site operation allows you to control when the ZTP of a device can proceed to completion. If a CPE device is powered on at a customer site, and you have not performed this activation procedure, the device continuously tries to start the ZTP process.

To activate your spoke site device, click the **check box** next to the site name then click the **Activate Device** button at the top-right part of the list. This brings up a window in which you enter the activation code for the device.

Install License on Device

To install a license on a device, you switch back to the Global Administrator role. Navigate to the pull-down menu **Tenant1** on the left side of the grey bar at the top of the GUI, next to **CSO Customer Portal**, and select **Global**.

Once back in the Administration Portal, navigate to **Administration > Licenses**.

Click the check box next to the license file that you uploaded in step 3.

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

In the pop-up window that appears, select name of the tenant that you created in step 4 from the **Tenant** pull-down menu. Your sites and devices appear under **Sites and Devices**.

Select the check box next to your tenant site to push the license to the CPE device at that site.

14. **Install Application Signature**

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

    To install an application signature, navigate to **Adminstration > Signature Database** in the Administration Portal. From the signature download you completed in step 2, you can now see the **Active Database** section has the number of the downloaded database listed.

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

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

    Select the check box next to the NFX250 device, then click **OK**.

15. **Configure Firewall Policy**

    To configure a firewall policy, you switch again to the tenant administrator role. To do this, navigate to the **Global** pull-down menu and select **Tenant1** that you created in step 4.

    Once in the Customer Portal, navigate to **Configuration > Firewall > Firewall Policy**.

    Click the **+** icon on the right side of the window to add an intent-based firewall policy.

    The window changes to reveal a policy builder with the **Source** area selected. You can select a source address, department, users, or a combination as Source.

    Select **Any** and click the icon for **Action**.

    Select **Deny** from the list of actions, then click in the **Destination** field.

Click the **View More Results** link from the list of destinations. A slide-out appears on the right of the screen where you can select from many destinations.

Click the **>** next to **Services [SVCS]** to expand the list of services. Click the check box next to **icmp-ping**. Then hover over the **...** icon and click **Add**. This adds the **icmp-ping** service to the destination field. Click **Save**.

The intent policy is listed. Click the **Deploy** button.

Pop-up messages indicate that the deployment is in progress. When it is finished, the **Total Intents** counter changes from 0 to 1. This indicates successful deployment of a firewall policy to block the **ICMP-PING** service. This policy can be implemented at any site.

16. **Configure SD-WAN Application SLA Profile**

    To configure an SD-WAN Application SLA Profile, navigate to the **Configuration > SD-WAN > Application SLA Profiles** page. Here you see a blank list of profiles. Click the **+** icon at the upper-right part of the list.

    The Create SLA Profile workflow window appears.

    Name the profile as **Internet-SLA**.

    In the **Priority** field, enter 5 for fairly high priority.

    From the **Traffic Type Profile** pull-down menu, select **INTERNET**.

    From the **Path Preference** pull-down menu, select **Internet**.

    Set the **Packet Loss** slider to **20%**.

    Set the **RTT**, **Jitter**, and **Throughput** fields to **20**, **10,** and **5**, respectively.

    Leave all other settings at their default, and click **OK**. The profile is listed on the page and is available for use in an SD-WAN policy.

17. **Configure SD-WAN Policy**

    To configure and SD-WAN Policy, switch again to the Tenant Administrator role in the **Customer Portal**. To do this, navigate to the **Global** pull-down menu and select the tenant that you created in step 4.

    Once in the Customer Portal, navigate to the **Configuration > SD-WAN > SD-WAN Policy** page.

Once your SD-WAN deployment is up and running, a logical next step might be to look into the *Contrail Service Orchestration Monitoring and Troubleshooting Guide*

This walkthrough has examined the major workflows involved in deploying an SD-WAN solution using a hub-and-spoke topology. As you can see by going through this, there are many other modes of deployment and options available when deploying an SD-WAN solutions. A good resource for proceeding with other SD-WAN solutions is the *SD-WAN Design and Architecture Guide*.

See Also

- *Contrail Service Orchestration Installation and Upgrade Guide*