

CONTRAIL SERVICE ORCHESTRATION

Product Overview

Contrail Service Orchestration helps enterprises and communication service providers automate the design, deployment, and management of network services and security in enterprise branch networks.

Intuitive GUIs make it easy to provision, manage, and secure multisite network connectivity services such as VPNs, SD-WAN, and SD-branch, including LAN, CPE, universal CPE (uCPE), virtual CPE (vCPE), and virtual cloud endpoints.

Service design and delivery tools allow seamless integration, deployment, and management of Juniper and third-party VNF-based services such as managed routers, managed security, and more.

Product Description

Multicloud has fundamentally altered the traffic patterns and security postures of enterprise networks. Enterprises need to connect users to cloud-based applications and resources while maintaining a consistent and secure application experience across local and wide area networks.

Juniper® Contrail® Service Orchestration allows enterprise organizations and communication service providers (CSPs) to securely tame the LAN and WAN, and simplify the design, delivery, and management of a broad portfolio of network services. Delivering hybrid WAN, cloud customer premises equipment (CPE), software-defined WAN (SD-WAN), and LAN services, Contrail Service Orchestration is a secure, flexible, and scalable solution that dramatically reduces network complexity.

Contrail Service Orchestration is available as a cloud-based service from Juniper, giving enterprises of all sizes access to its intuitive and simple GUI for WAN and LAN use cases. It can also be deployed on-premises for customers who demand full control over their deployments.

Contrail Service Orchestration is designed to:

- Reduce WAN connectivity costs by effectively managing corporate traffic
- Simplify the deployment, management, and monitoring of branch CPE
- Manage SD-WAN, SD-LAN, and security policies across the enterprise
- Ensure application quality of experience (AppQoE), regardless of WAN connectivity types
- Manage traffic breakouts
- Visualize application traffic flow and security events
- Reduce the cost and complexity of managing remote branch connectivity
- Support virtualized network functions (VNFs) and application-based services
- Centralize end-to-end network management and control through a cloud-based architecture

Contrail Service Orchestration empowers enterprises and service providers to dramatically reduce delivery times for network service deployment and transform a multi-month experience into a near real-time point-and-click operation by automating the entire service delivery life cycle.

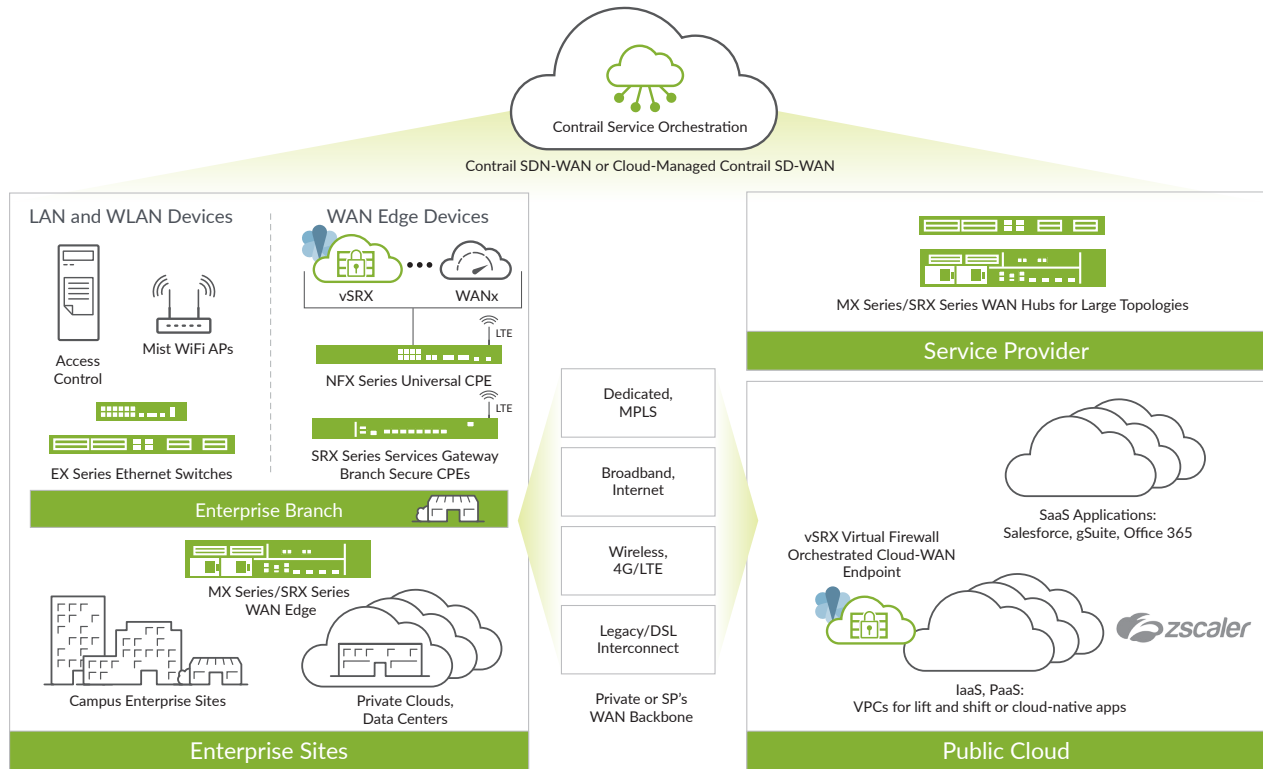


Figure 1: The Contrail Service Orchestration solution.

Architecture and Use Cases

SD-WAN/Hybrid WAN

Contrail Service Orchestration offers a flexible and automated way to connect enterprise locations to each other, as well as to the Internet and multicloud, including Amazon Web Services (AWS) VPC. The SD-WAN deployment model supports Juniper Networks SRX Series Services Gateways and Juniper Networks NFX Series Network Services Platforms as CPE devices, which are located on the customer premises to securely connect LAN segments to the WAN. On the WAN side, the CPE devices connect to a hub in a hub-and-spoke or full mesh VPN. Local breakout support allows lower priority Internet traffic to connect directly to the Internet locally, avoiding the need to transport basic Web traffic across costly VPN or MPLS links. Contrail Service Orchestration uses SD-WAN policies and service-level agreement (SLA) measurements to differentiate and dynamically route traffic for different applications.

SD-LAN/SD-WLAN

Cloud-based Contrail Service Orchestration offers LAN management in the branch with Juniper Networks EX Series Ethernet Switches subtended behind an SRX Series services gateway, NFX Series network services platform, or a third-party Internet gateway. Mist Systems AI-driven wireless LAN is integrated in the Contrail Platform management interface, allowing customers to see operational and analytics data about

the Wi-Fi, including connected host devices. Contrail Service Orchestration enables large enterprises and CSPs to create, deploy, and manage LAN services and also provides visibility into Mist WLAN access points.

NGFW Management

Contrail Service Orchestration offers next-generation firewall (NGFW) management capabilities in the branch with the SRX Series Service Gateways, Juniper Networks vSRX Virtual Firewall running on the NFX Series platform, or standalone vSRX Virtual Firewall running in a cloud footprint. Contrail Service Orchestration enables large enterprises and CSPs to create, deploy, and manage intent-based NGFW services from the cloud.

Key Features

Automated Network Orchestration and Control: Contrail Service Orchestration simplifies branch management, delivering greater network flexibility and agility through dynamic and automated workflows. Zero-touch deployment (ZTD) and zero-touch provisioning (ZTP) greatly simplify branch network turnup and connectivity. Subsequent service updates and policy changes are consistently and dynamically inserted into the existing device, resulting in operational efficiency for service providers and enterprise customers alike by limiting or in some cases eliminating service interruptions and business disruptions. Additionally, it supports VNF management.

Application SLA Policy Management and Routing: Policy-based application routing automates application and resource provisioning across multiple network connections and paths. It supports more than 4000 application signatures; applications are routed dynamically across multiple network connections to meet user-specified SLAs.

VNF Management: The Network Service Designer tool, a component of Contrail Service Orchestration, supports end-to-end life-cycle management for VNFs. The Network Service Designer GUI allows product managers and network engineers to design, create, manage, and configure VNF-based network service templates. VNFs can be more easily provisioned and service chained on the CPE. Contrail Service Orchestration supports both Juniper and third-party VNFs.

Integrated Security: Contrail Service Orchestration is integrated with the SRX Series gateways and the vSRX Virtual Firewall, high-performance NGFWs that provide advanced security capabilities such as unified threat management (UTM) and Network Address Translation (NAT). The Contrail Service Orchestration administration portals also support security management and reporting.

Integrated Wi-Fi Access Point Monitoring: Contrail Service Orchestration is integrated with Mist Systems in the cloud to provide visibility into Mist access points. Visibility into wireless endpoints, switches, and associated WAN analytics, as well as into Mist Cloud, is also supported.

Fully Redundant Platform: Contrail Service Orchestration is a fully redundant platform. It supports both redundant and non-redundant installation options, as well as spoke redundancy, hub site redundancy through its support for multihoming, and high controller availability.

Multitenant Support: Contrail Service Orchestration supports multiple tenants, allowing CSPs to serve and manage multiple customers with one instance. Multitenant support simplifies the management of multiple WANs, LANs, uCPE, and NGFW for service providers, and it reduces the complexity of managing multiple sites and departments for IT managers at large enterprises. Contrail Service Orchestration's multitenant capability offers the CSP or enterprise IT manager a single Network Service Designer and administration portal while delivering secure segmentation to end users. End users have their own separate WAN, LAN, uCPE, and NGFW that can be configured, secured, monitored, and managed to meet their unique business requirements.

Key Components

Contrail Service Orchestration includes the following components:

Network Service Orchestrator

The Network Service Orchestrator is the interface to Contrail Service Orchestration. Its portfolio of GUI-based design, integration, and management tools enables the onboarding and integration of VNFs, supports the design and management of network services such as SD-WAN, and provides status monitoring and analytics.

Contrail Service Orchestration GUI portals automate network and service design, deployment, monitoring, management, security, and reporting, reducing the complexity of network management for enterprise IT organizations and CSP network engineering, operations, and product management teams. The portals support role-based access control, giving network administrators full access to the tools and resources needed to design, deploy, manage, and monitor network services while providing limited access to other users.

The Network Service Orchestrator integrates with existing operations/business support systems (OSS/BSS) through its northbound REST API and also offers multitenant customer portals, pushing user-defined policies southbound to the Network Service Controller that manages the required network devices.

The Network Service Orchestrator consists of the following portals:

Network Service Designer: The Network Service Designer provides product managers and network architects with an intuitive point-and-click solution for performing the service definition that is part of service life-cycle management for both Juniper and third-party VNFs. An easy step-by-step service design implementation wizard walks you through the service definition process, specifying the VNF onboarding process, VNF version control, VNF description, and more. The Network Service Designer also assists with service configuration parameters, service chaining templates, and customer-specific service catalogs that get exposed through the customer portal. The entire service definition is saved in a database via standard YANG data models, providing easy integration with third-party operations support systems (OSS) and business support systems (BSS).

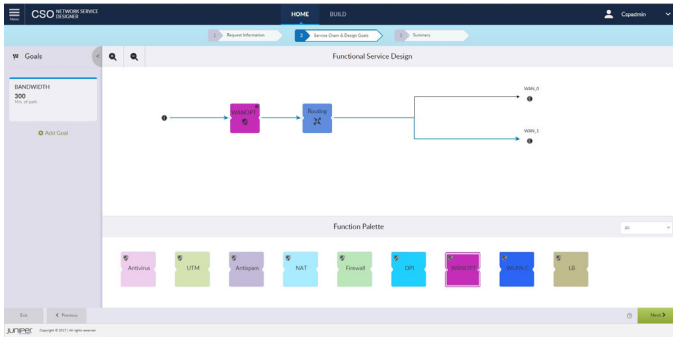


Figure 2: Contrail Service Orchestration Network Service Designer

Administration Portal: The Administration Portal gives network administrators simultaneous visibility into customers' on-premises and hybrid cloud-based services, enabling them to easily monitor and troubleshoot service health and status. Detailed service information is readily accessible for monitoring virtual or physical CPE, SLAs, CPE resource diagnostic reports, service catalog resources, and other administrative functions. The Administration Portal supports role-based access control (RBAC), as well as both local authentication and Security Assertion Markup Language (SAML)-based authentication for single sign-on (SSO). Administrators can also create more users with specific roles and access privileges.

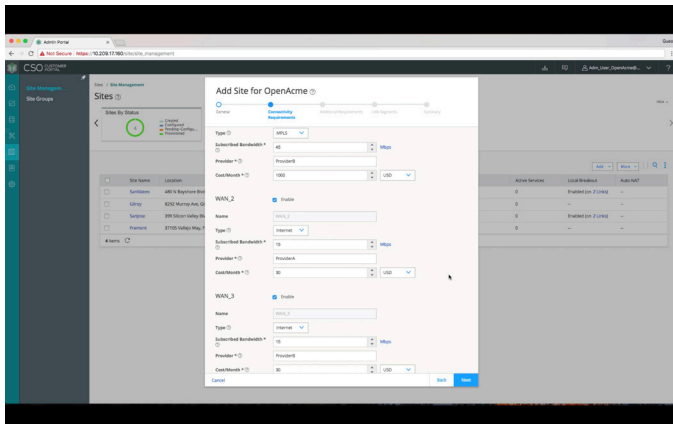


Figure 3: Contrail Service Orchestration Administration Portal

Multitenant Customer Portal: The Customer Portal is provided through a unified portal with access to functions governed by an RBAC to fill a per-tenant admin and tenant operator role (read-only access). Tenants, such as service provider customers, have the freedom to self-select the services that best fit their business needs. The portal can be customized by the service provider or the enterprise owner/operator to align with their corporate brand and identity. They can also select the appropriate service deployment model on-premises or in the cloud, with the flexibility to determine when to deploy, change, or delete a service in near real time. Service providers can choose to develop their own customer portal GUI using REST APIs.

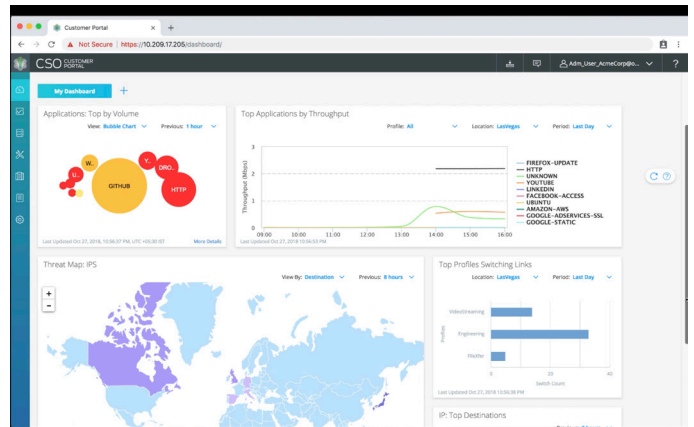
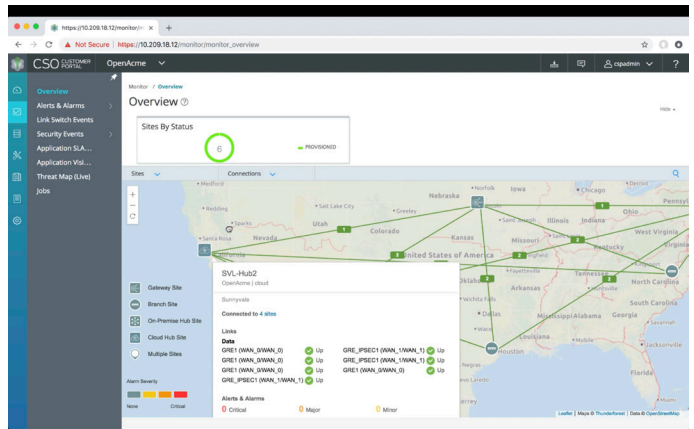


Figure 4: Contrail Service Orchestration Customer Portal

Security Management: Contrail Service Orchestration includes the ability, through the same management platform, to orchestrate managed security services as part of the suite of network services. You can manage NAT policy or intent-based firewall policy to ensure security across Layer 4 transport rules through Layer 7 application rules. Policy automation allows for consistent and easy deployment across the network. Integrated security dashboards and alerts provide visibility into which sites are secure. With security management built in, pervasive and always-on security is part of every deployment.

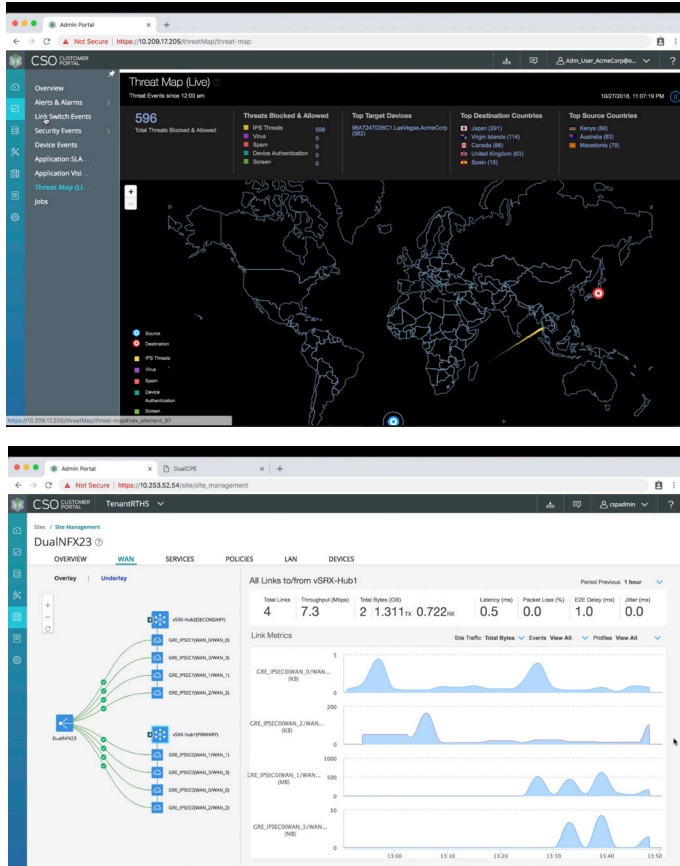


Figure 5: Integrated secure SD-WAN

LAN Management: Cloud-based Contrail Service Orchestration lets you manage EX Series Ethernet Switches as part of branch management. This includes ZTP support, device software upgrade, VLAN, STP, 802.1x and Power over Ethernet (PoE) configuration, and switch monitoring. In addition, Mist access points can be monitored via Contrail Service Orchestration.

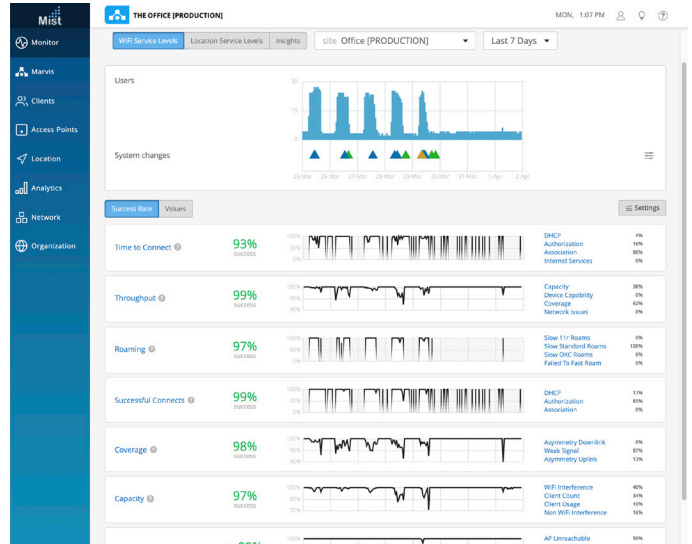


Figure 6: Integrated branch SD-LAN management

Network Service Controller

The Network Service Controller provides life-cycle management of VNFs deployed by Contrail Service Orchestration. It includes the virtualized infrastructure manager (VIM), Network Functions Virtualization Infrastructure (NFVI), and device management for supported CPE endpoints, including deployment, activation, scaling, updating, and terminating VNFs. It also manages service chains on the CPE endpoint, as well as the chaining of end users to services located in the cloud.

In SD-WAN deployments, the Network Service Controller becomes the SD-WAN controller, simplifying network provisioning, supporting multiple network topology architectures, and executing network control and management capabilities. As an SD-WAN controller, it manages key activities such as configuration, ZTP, installing updates, pushing new policies onto CPE devices and network-based hub gateways, maintaining network connections, and gathering application performance and network and device telemetry data.

Policy Manager

Contrail Service Orchestration’s Policy Manager provides intuitive policy management capabilities across enterprise and specific sites for WAN, LAN, and security services. The policy manager abstracts complex policy management, providing a simple and intuitive user interface.

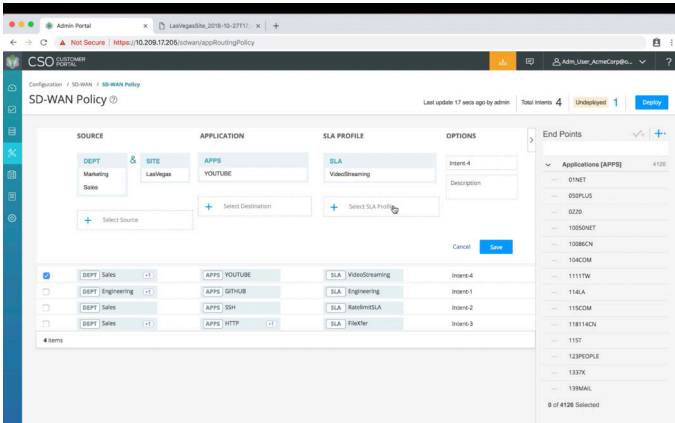
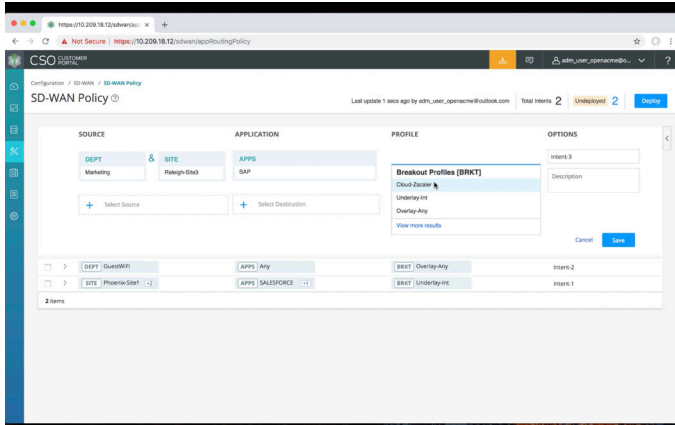
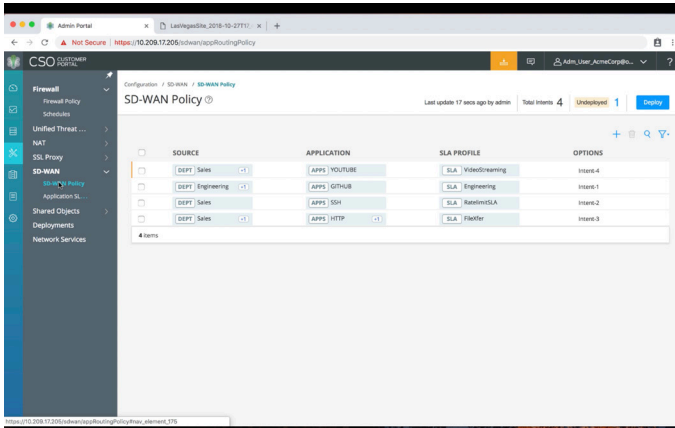
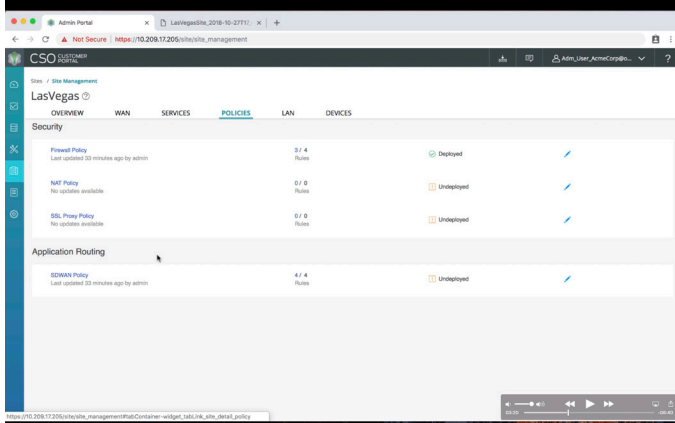


Figure 7: SD-WAN policy management screens

Contrail Analytics

The Contrail Analytics component is a scalable data management system that supports large numbers of tenants, devices, and services data. Contrail Analytics also supports a number of Contrail Service Orchestration system capabilities, including device and service status, real-time service performance, and alert and notification for overall system maintenance.

This system collects and analyzes the large amounts of data required for SD-WAN, SD-LAN, and security use cases. The data also supports visualization and monitoring of services across WAN, LAN, and security, as well as historic time series data for past performance and reporting.

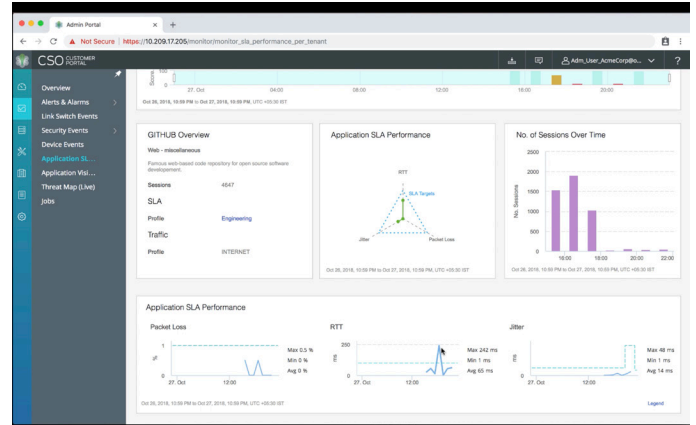
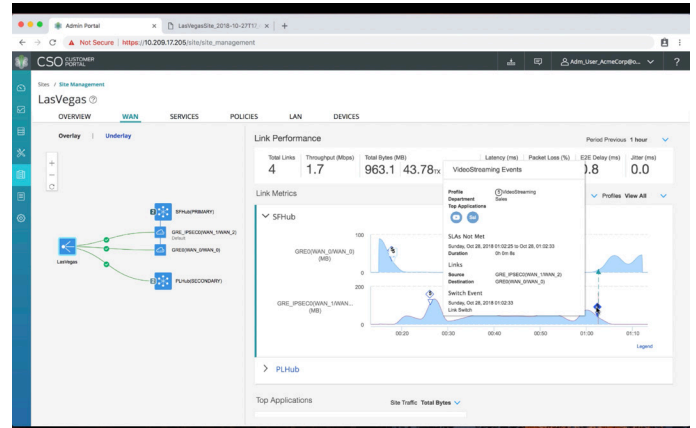


Figure 8: Detailed analytics views

Reports and Audit Logs

Contrail Service Orchestration features a built-in reporting capability to generate WAN, security, and audit log reports. Users can schedule reports at predefined intervals or generate custom reports on demand.

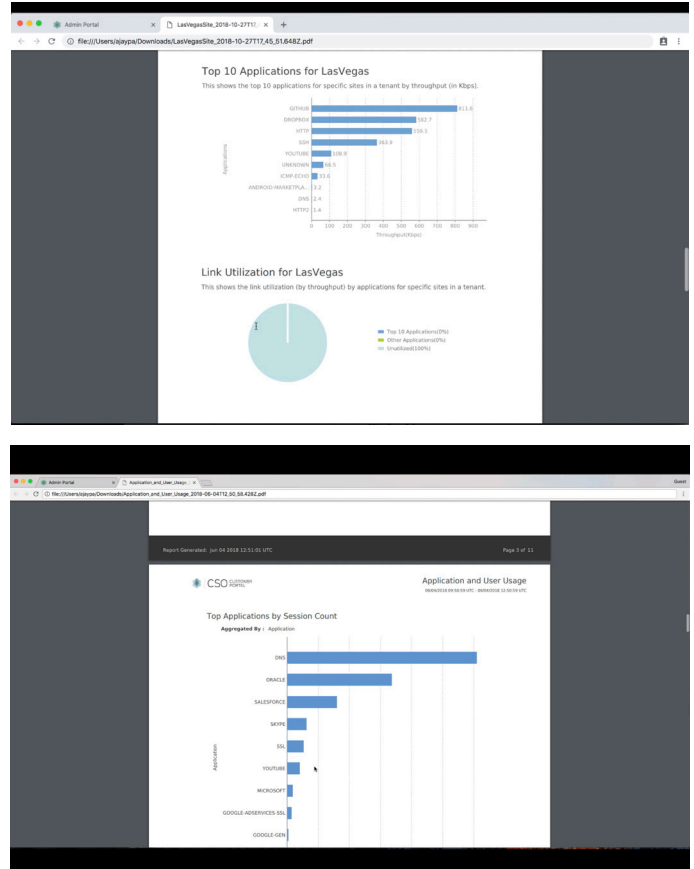


Figure 9: Reporting views

Contrail Service Orchestration Features and Benefits

Features	Benefits
Available as a cloud-hosted service from Juniper or in on-premises deployment mode	Contrail Service Orchestration is offered as a cloud-hosted centralized management service from Juniper, reducing capital and operational expenses for large enterprises and CSPs. It can also be deployed on-premises for enterprises and CSPs that want full control.
Supports multiple CPE and access switching platforms	NFX Series Network Services Platforms allow you to design, develop, and deliver a portfolio of managed services from one orchestration solution. Contrail Service Orchestration and the NFX Series support a number of Juniper and third-party VNF solutions, and Juniper Professional Services can help customers integrate additional VNFs as needed. SRX Series Services Gateways and EX Series Ethernet Switches let you easily deploy a high-performance, orchestrated, and fully automated access switching solution and NGFW-based managed security solution from a centralized management platform.
Supports zero-touch provisioning (ZTP)	Supports zero-touch provisioning (ZTP) Contrail Service Orchestration delivers a fully automated deployment experience for supported CPE and select EX Series switches. Simply take the supported CPE or EX Series switch out of the box, connect it to the network, and power up. The supported CPE or EX Series switch will call home, download any required software and configuration updates, install them, and begin delivering the provisioned services, reducing operational expenses and demands on IT staff.
Offers flexible deployment options	Supported topologies: <ul style="list-style-type: none"> • Hub-and-spoke, dynamic mesh, and partial mesh topologies are supported, providing flexibility across service provider and enterprise environments. <ul style="list-style-type: none"> - In the hub-and-spoke model, corporate locations or network-based routers or firewalls can be identified as hub gateways, providing network management and control. - In the dynamic mesh topology, each endpoint connects to every other endpoint device based on CPE settings by admins. - In the partial mesh topology, clusters of CPE can be set up for dynamic mesh while gateway/hub mesh enable intra-mesh traffic. Supported architectures: <ul style="list-style-type: none"> • SD-WAN, hybrid WAN, and AWS spoke endpoints are supported for tenants with multiple site types.

Features	Benefits
Supports multiple hub gateway devices	<ul style="list-style-type: none"> On-premises spoke gateways: SRX Series devices can be used as premises-based gateway devices in hub-and-spoke and dynamic mesh topologies, letting enterprises access data center applications directly via the gateway. Cloud- or network-based hub gateways: Specific Juniper Networks MX Series 5G Universal Routing Platforms and SRX Series gateways can be used as multitenant service provider cloud-based hub devices. vSRX Virtual Firewall: The vSRX can be used as an SD-WAN hub, providing greater agility and versatility for supporting platforms that can be used as endpoint devices both on premises and in the cloud.
Supports multiple WAN link types	<p>Contrail Service Orchestration supports five different WAN link types with high bandwidth and low latency:</p> <ul style="list-style-type: none"> MPLS over copper and fiber Ethernet broadband Asymmetric digital subscriber line/ very-high-bit-rate digital subscriber line (ADSL/VDSL) LTE Satellite links with very low latency
Offers native MPLS support	Contrail Service Orchestration natively supports MPLS for integration into IP-VPN network.
Ensures application quality of experience (AppQoE)	<p>Advanced policy-based routing (APBR): Traffic flows can be classified based on application attributes, and filters can be applied based on these attributes to redirect the traffic.</p> <p>AppQoE: Aims to improve the user's application experience by constantly monitoring class-of-service (CoS) parameters and application traffic SLA compliance, ensuring that application data is sent over the best available link.</p>
Features configurable class of service	<p>Traffic type profiles can be created, allowing CSP administrators and tenant administrators to configure CoS parameters that satisfy specific business requirements.</p> <p>Traffic type profiles define a traffic type based on parameters such as priority, buffer, and bandwidth allocations, probe parameters, and DiffServ code point (DSCP) values for the traffic type.</p>
Supports traffic breakouts	<p>Traffic breakouts supported include:</p> <ul style="list-style-type: none"> Policy-based local breakout for all site-, application-, and department-specific traffic Policy-based central breakout for all sites, application and department specific traffic Policy-based central hub breakout for Internet and IP-VPN traffic On-ramp breakout to ZScaler <p>The enterprise IT manager defines which links at the site can be used for local breakout and also enables automatic interface-based source NAT policy for the local breakout links.</p>
Provides comprehensive security	Contrail Service Orchestration is integrated with SRX Series/vSRX for NGFW, UTM, intrusion detection service (IDS), intrusion prevention system (IPS), and antivirus.
Supports threat maps	Threat map support provides the ability to visualize the network's geography to monitor incoming and outgoing traffic, blocked and allowed threat events from IPS, antivirus and antispam engine feeds, and unsuccessful login attempts—all via a simple-to-use GUI.
Enables cloud sites on AWS VPC	Tenant, customer, or client administrators can create and configure a cloud spoke site for an SD-WAN endpoint in an AWS virtual private cloud (VPC).
Integrates Wi-Fi	Contrail Service Orchestration integrates with Mist Cloud to provide Mist access point visibility and monitoring.
Offers high availability and redundancy	<ul style="list-style-type: none"> HA controller: Contrail Service Orchestration can be installed on multiple geographically dispersed servers, creating a fully redundant, highly available environment. Virtual route reflector redundancy: In an SD-WAN solution, virtual route reflectors (VRRs) can be installed on regional servers to support BGP sessions established between hub-and-spoke devices. These VRRs can be configured as high-availability devices. Spoke redundancy: SD-WAN sites can be deployed with two CPE devices (primary and secondary) to protect the site against device and link failures. If the primary device fails, the secondary device takes over traffic processing. Note: The same NFX Series or SRX Series models must be used, and both devices must be running the same version of Juniper Networks Junos® operating system. Multi-hub with traffic failover support: NFX Series and SRX Series platforms can connect with two different hub devices in a hub-and-spoke topology. Traffic automatically switches from the primary hub to the secondary hub if the primary hub, its connection, or all of its overlay tunnels are down. When the primary hub and/or its tunnels become available, traffic is automatically reverted back. Backup link: Any link, other than default links, can be configured as backups so that, if the primary link goes down, the site can use a backup link to route traffic. This includes the LTE link on supported Juniper CPE devices that include an LTE interface and where LTE service is available.
Offers site upgrade support	A GUI utility allows network operators to configure workflows and processes for individual or bulk site upgrades. As some enterprises have thousands of sites, this feature allows service providers to automate and perform bulk updates, greatly reducing the time and effort required to keep customer networks running smoothly and seamlessly.

Features	Benefits
Enables enterprise-wide policy management	<p>Contrail Service Orchestration secures and simplifies site management with enterprise-wide policy deployment and enforcement.</p> <p>Intent-based firewall policies control transit traffic within a context (source zone to destination zone). Traffic is classified by matching its source and destination zones, source and destination addresses, and the application the traffic carries in its protocol headers with the policy database.</p> <p>Protection can also be enabled against multiple threat types such as spam and malware, and control access to unapproved websites and content by enabling the UTM option and selecting an appropriate UTM profile.</p> <p>These policies can be configured for enterprise site groups or to group LAN segments within a site into departments. Specific policies can be applied to LAN segments that are members of a department. You can also create, view, edit, or delete departments from the Departments GUI.</p>
Supports multitenant	<p>Contrail Service Orchestration can support multiple clients or end customers from one software instance. Users are created as tenants in their own partition, with their own, uniquely personalized experience, without compromising their identity or the security of their data.</p>
Supports object-based role-based access control (RBAC)	<p>The RBAC feature controls which system users can view, read, write, and execute within the Administration and Customer portals. Administrators can provide granular control over GUI objects within each navigation menu, restricting users to the views and/or capabilities specific to their role. Predefined roles are provided, or operators can create their own unique roles. This feature can be used within enterprises to provide hierarchical access to capabilities at different levels, or to allow or restrict access to specific capabilities across departments. Service providers can also use RBAC to offer promotional trials for features that aren't included in the customer's current service offering.</p>
Supports operational company (OpCo)	<p>Service providers must have business entities that manage customers in every region or country in which they operate for regulatory, billing, and operational purposes. The OpCo feature enables global administrators to define a single service across multiple regions while allowing regional administrators to manage their own local customers. In this scenario, global service providers give OpCo administrators access to a centrally deployed Contrail Service Orchestration instance, along with the local resources they need, enabling them to offer SD-WAN services that meet local regulatory requirements.</p>
Provides secure connectivity	<p>Secure Operation, Administration, and Maintenance (OAM) network ensures secure communications between the CPE device and Contrail Service Orchestration controller.</p> <p>Integrated NAT and SSL support ensure that traffic is protected whether flowing across MPLS tunnels, VPNs, or the Internet.</p> <p>IPsec public key infrastructure (PKI) provides enhanced security for data and management.</p> <p>Certification Authority (CA) certificate management simplifies secure connectivity management for the enterprise. Contrail Service Orchestration automates and simplifies CA certificate management by acting as a Simple Certificate Enrollment Protocol (SCEP) server, providing management capabilities through its GUI and back-end API.</p>
Supports device RMA	<p>Device Return Material Authorizations (RMAs) can be managed from the user interface.</p>
Offers VNF integration and service design tools	<p>The Network Service Designer enables service managers and administrators to intuitively define a customized service catalog through a simple wizard.</p> <p>This eliminates error-prone provisioning processes by recommending the most efficient service creation model based on defined VNFs that best meet tenant needs.</p> <p>The intelligent service design portal establishes a workflow that reduces the time required to define and deliver new services to market, increasing productivity and lowering operational expenses.</p> <p>Service chaining is supported for Juniper and third-party VNFs on NFX Series platforms when deployed as universal CPE devices or as endpoints for an SD-WAN or hybrid WAN solution.</p>
Includes performance monitoring	<p>SLA performance monitoring of tenants, sites, and applications is supported, providing network managers and operators with visibility into network performance against defined SLA values over a specified period.</p> <p>SD-WAN events are triggered when SLA requirements for a site are not met and the site switches WAN links.</p> <p>The ability to view the maximum bandwidth and capacity of a WAN link is provided as well.</p> <p>An audit log viewer simplifies the ability to monitor and review the audit log database.</p>
Provides advanced reporting	<p>Reports can be generated that show SLA performance for all or selected sites in a tenant. Report definitions can be created, edited, deleted, and cloned. Report generation can be scheduled, viewed in PDF format, and sent via e-mail. Example reports include:</p> <ul style="list-style-type: none"> SD-WAN Tenant Performance Reports, which provide parameters such as top applications by bandwidth, top sites not meeting SLAs, top sites meeting SLAs with switching, and sites meeting SLAs without link switching, in order to measure SLA performance across all sites in a tenant. SD-WAN Site Performance Reports, which provide parameters such as top 10 applications by bandwidth, link utilization by applications, top profiles not meeting SLAs, and top SLA profiles switching links, in order to measure SLA performance of specific sites in a tenant. Comprehensive audit log reports are also available for system and user/admin operations on the Contrail Service Orchestration portal.
Supports open-standard BGP protocols for routing	<p>Contrail Service Orchestration easily works with existing WAN and service provider routing environments. Its use of open-standard protocols enables it to readily integrate into standard network environments.</p>
Supports open YANG data models and open APIs	<p>Contrail Service Orchestration leverages open, industry-standard APIs to integrate with other systems like BSS/OSS and IT service management (ITSM), or to extend the platform with custom automation to accelerate workflow.</p>

Features	Benefits
Provides unified management of centralized and distributed VNFs	VNFs can be placed dynamically, on universal CPE devices at the customer premises or within NFV cloud infrastructures. Regardless of their location, VNFs can be seamlessly interconnected to speed and ease secure network service creation, giving service providers greater flexibility to support their operational and business model requirements. In some cases, users may choose to start small, deploying a service from the cloud and, as demand for the service increases, extending it to the end customer premises. In other cases, operators may choose to deploy one or more services at the customer premises and then add new services in the cloud as customer requirements evolve.
Works with Contrail Provider Cloud and Contrail Networking	Contrail Service Orchestration can be deployed as part of the Juniper Networks Cloud CPE solution with Contrail Provider Cloud and Contrail Networking™, delivering a virtual, cloud-based managed service delivery solution. In this model, service providers can host and manage VNFs in their data centers and leverage service chaining across the network to map VNF-based services to specific customers. This solution can be used with the SRX Series or NFX Series on-premises CPE devices or with other third-party network interface devices (NIDs).
Provides backup and restore capabilities	Contrail Service Orchestration supports complete system backup and restore. Network administrators can schedule daily, weekly, incremental, and full backups. Data can be backed up to external storage systems and systems can easily be restored.

Deployment Modes

Contrail Service Orchestration Software can be deployed at the customer premises, in a customer’s private cloud, or from the Juniper cloud-hosted service.

Cloud-Managed by Juniper Networks

Architecture

Cloud-managed Contrail SD-WAN is based on many secure and highly available Juniper cloud-hosted offerings of Contrail Service Orchestration.

As customers login to the Contrail management interface, it is over a management plane that separates network management data from user WAN and LAN data traffic. While management details are provisioned and maintained in Contrail Service Orchestration, user data traffic does not route through or to Juniper. Instead, user data is directed to its destination over the LAN and WAN between source and destination as usual. This

architecture ensures that any loss of management connectivity to the cloud-managed Contrail SD-WAN service does not impact the customer’s network flows or end-user functionality.

Cloud-managed Contrail SD-WAN also provides strong security protections around Juniper’s hosted Contrail Service Orchestration as follows:

- The Contrail Service Orchestration perimeter is secured with network ACLs, managed Distributed Denial of Service (DDoS) protection, and security groups for all public IPs.
- Web application firewalls and https secure user access.
- Strong firewall policies deny access to malicious traffic from public networks.
- Secure firewalls serve as OAM hubs for control plane traffic from devices. Device access is secured through firewalls.
- All data at rest is stored in encrypted form.

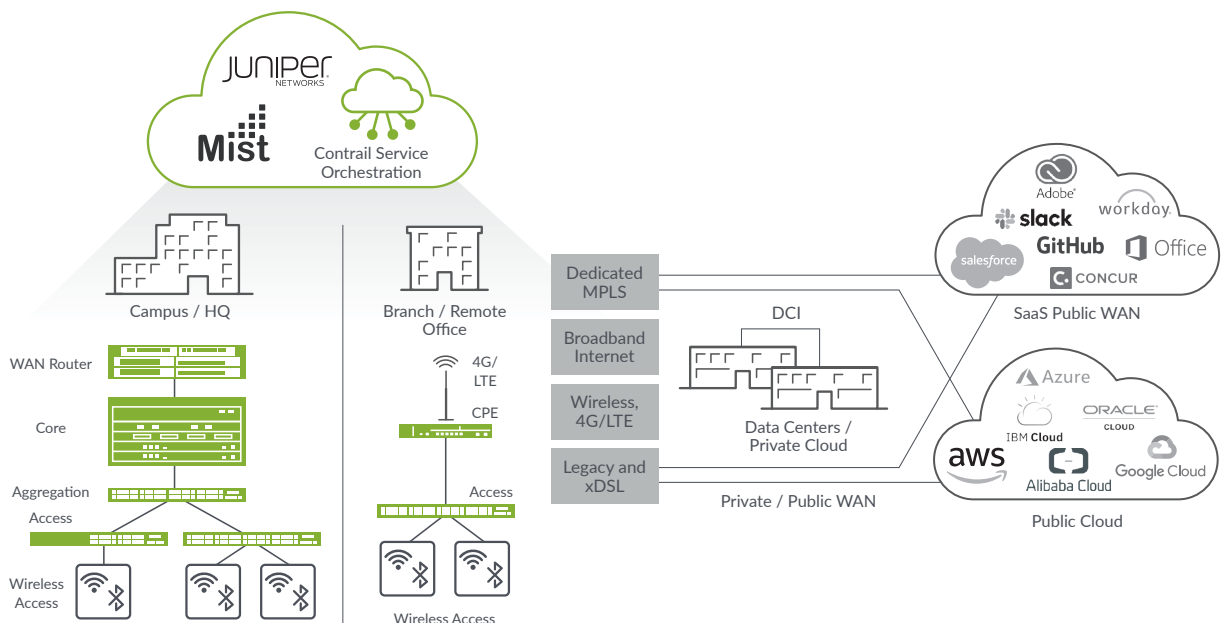


Figure 10: Contrail Service Orchestration manages SD-WAN routing, LAN switching, Mist Wi-Fi, and end-to-end security.

Service Provisioning

Juniper Networks will provide Contrail Service Orchestration customers with the following services:

- Following your successful Contrail Service Orchestration license purchase, Juniper will create a service account and invite the identified contact to join the account. A hyperlink providing access to the service offering, along with the necessary credentials, will be included in this invitation.
- The identified contact can create additional accounts for other users, as needed.

The customer is responsible for:

- Providing and provisioning the CPE devices (SRX Series/NFX Series/EX Series/Mist) and SD-WAN hub devices (SRX Series/MX Series) in accordance with the ordered quantities.
- Providing and managing WAN/LAN connectivity to those devices.
- Monitoring usage and traffic patterns to ensure they are inline with the network capacity connected to those devices.
- Analyzing firewall logs collected by the service and taking appropriate action if a security incident is detected.
- Cooperating with Juniper when planned or emergency maintenance is required.

Service Availability

- The cloud-managed offering is backed by highly available cloud infrastructure with a 99.9% uptime goal.
- The service provides 24x7 availability monitoring with automated failure detection, along with rapid escalation procedures and alert notifications.
- Juniper advertises scheduled maintenance windows 48 hours in advance and ensures zero downtime for patch updates.
- By operating in headless mode, Contrail Service Orchestration does not receive incoming customer traffic, ensuring it is not impacted when the service is unreachable.
- When Contrail Service Orchestration is unreachable, portal access, configuration and diagnostic tools, device management, monitoring, and reporting services are temporarily unavailable.

Service Reliability

- Contrail Service Orchestration is hosted in data centers designed for physical redundancy and resiliency, providing uninterrupted performance following a power outage or natural disaster.
- On-demand scaling of resources is provided, transparent to the customer.
- Management continuity is provided with controller redundancy and regular backups.

Compliance

- Contrail Service Orchestration is backed by PCI-compliant cloud infrastructure.
- The service is supported by Juniper with proactive monitoring, regular vulnerability scans, and penetration tests performed by reputable third-party providers.

Account Protection and Privacy

- User accounts are password protected with secure access.
- Granular user, role-based access controls and policy framework control access to all resources.
- Customer data traffic does not enter the system.
- System logs are monitored for authentication failures, with instant alert notification for configuration-related security breaches.

Account Termination

If a license is allowed to expire, it will result in the termination of the user account and permanent loss of access to the service, as well as the deletion of all equipment configuration and data. Deleted data cannot be recovered.

Legal Terms

Use of the cloud-managed Contrail SD-WAN service offering is subject to Juniper Networks general terms and conditions of purchase. Details can be found at www.juniper.net/assets/us/en/local/pdf/flyer/9040065-en.pdf

Juniper Networks privacy policy can be found at www.juniper.net/us/en/privacy-policy/

Juniper Networks end-user license agreement can be found at <https://support.juniper.net/support/eula/>

You will also be required to accept the terms of use the first time you log in to the Contrail Service Orchestration web portal.

On-Premises Deployment Specifications

System recommendations and operating environment depend on intended use.

Recommended Operating Environment

- **Network:** 1GbE or 10GbE interface card (one or more)
- **OS:** Linux OS (Ubuntu 14.04.5 LTS)
- **Storage:** Greater than 1 TB Serial Advanced Technology Attachment (SATA), Serial Attached SCSI (SAS), or solid-state drive (SSD)
- **Servers:** Quanta (QuantaPlex T41S-U), Supermicro (SYS-2028TPHC1TR-OTO-4), or Dell (R420) (Intel E5-2670v3 or better) using 2.4 GHz 64-bit dual x86 processor

Table 1 shows the server requirements per configuration. Detailed configurations of virtual machines and memory allocations to the Contrail Service Orchestration functions can be found in the Contrail Service Orchestration deployment guide.

Table 1: Server Requirements per Configuration

Configuration	Number of Servers	vCPUs per Server	Memory per Server (GB RAM)
Small deployment	1	24	96
Medium deployment	3	92	338
Large deployment	7	184	688

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services.

Ordering Information

Contrail Service Orchestration provides 1, 3, and 5 year term-based subscription licenses.

For on-premises deployments using a virtual appliance/software product, you would not buy any hardware license from Juniper, but instead, procure the hardware and additional required support for this hardware from an additional third-party vendor. For additional information on supported hypervisor(s), VM requirements, and recommended hardware configuration, please refer to the technical documentation for this product on our [website](#) under the Support section.

Juniper Networks products are sold directly as well as through Juniper partners and resellers.

For more information on the Juniper Software Advantage business model, please visit www.juniper.net/us/en/products-services/sdn/contrail/. For information on how to buy, please visit www.juniper.net/us/en/how-to-buy.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.0.207.125.700



Copyright 2019 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.