

APPROACHING MULTICLOUD OPERATIONS THROUGH THE LENS OF SD-WAN

Juniper Contrail SD-WAN transforms your branch with unified, automated, and AI-driven management

Challenge

Enterprise branches with insufficient staff require centralized remote management capabilities. Even beyond SD-WAN solutions, enterprise network operations need to simplify and unify orchestration, analytics, and security across the enterprise—cloud, data center, WAN, campus, and branch—while abstracting control and automating workflows.

Solution

Juniper enables the AI-driven enterprise, delivering secure SD-WAN as a service or for on-premises deployment. The Contrail SD-WAN solution spans dynamic hybrid WAN routing, security, and threat protection, providing intelligence and simplicity aligned with business-, user-, and application-oriented policy.

Benefits

- Quick, agile, automated deployment of SD-WAN and SD-branch with zero-touch connectivity ensures easy deployment and centralized orchestration.
- Software-defined and AI-driven control of LAN, Wi-Fi, and security allows you to manage campus and branches consistently and in sync with SD-WAN policy and analytics.
- Dynamic and application-aware routing improves WAN economics and performance.

Business applications, information, processes, and even retail storefronts are moving to the cloud, driving greater business dependency on WAN resources and aligning enterprise operations with business needs. This growing dependence on multicloud infrastructure means that the modern campus and branch, including WAN, LAN, and Wi-Fi, must be secure, agile, and application-aware.

Enter software-defined WAN (SD-WAN), which promises a rich and dynamic application experience for IT departments and end users, empowering this much-needed WAN edge transformation. To meet the growing, dynamic needs of the enterprise, SD-WAN must accommodate existing WAN, campus, and branch requirements with many new capabilities for the automated and rapid deployment of network equipment and services while enhancing application performance with better economics. SD-WAN allows communication service providers (CSPs) to enhance their portfolio with valuable new managed services. It also helps enterprise organizations looking to diversify their branch and multicloud connectivity options simplify and streamline service delivery, protect their customers, reduce costs, and provide monitoring and reporting tools to ensure service-level agreement (SLA) compliance. With SD-WAN, CSPs can expand their services footprint and capture new revenue faster using centralized orchestration in conjunction with distributed end-to-end delivery.

The Challenge

Market dynamics are changing the traditional WAN. As more and more enterprises move to the cloud, they need secure, high-bandwidth connections that are not only cost-aligned to the needs of their applications but can also be deployed quickly and easily to keep up with the accelerating pace and scope of the migration. According to RightScale¹, the typical enterprise customer embarking on this migration accesses five different cloud infrastructures on average, making hybrid WAN a top priority for CIOs. According to Gartner, by 2020, more than 50% of customer premises equipment (CPE) refresh initiatives will be influenced by SD-WAN². Large enterprises will continue to leverage MPLS/VPN and integrate SD-WAN to improve business outcomes. Small to medium-sized businesses may choose that approach or employ a complete SD-WAN overlay approach.

¹ RightScale State of the Cloud Report 2019, <https://info.flexerasoftware.com/PPC-SLO-WP-State-of-the-Cloud-2019>

² http://www.gartner.com/it/content/3478900/3478918/november_8_sdwan_forecast_opportunity_jskorupa.pdf

Any long-term strategy for SD-WAN requires security and integration with existing WANs for the holistic management of branch connectivity and eventually SD-branch services, including unified threat management, LAN, and Wi-Fi. Furthermore, SD-WAN and SD-branch should also simplify service assurance and reliability engineering through AI-driven visibility, analytics, and automation. Finally, SD-WAN and SDN must scale to serve the needs of campus performance, campus architectures, and high availability.

Unfortunately, not all solutions do this, nor do they equally improve stability, security, and operational speed. Not all solutions offer flexible architectures that integrate with today's WAN. And not all solutions drive greater simplicity and reduce overall costs. A successful evolution to SD-WAN demands an agile network service delivery platform.

For some CSPs, SD-WAN poses a potential threat to existing MPLS and managed services revenue. These CSPs are facing MPLS price pressures due to increased competition in a maturing, commoditized market, from lower cost Ethernet-based services and even basic Internet access. However, CSPs can turn this threat into an opportunity to offer new services while expanding their footprint to reach more customers as they roll out 5G wireless access.

The Juniper Networks Contrail SD-WAN Solution

Juniper® Contrail® SD-WAN delivers a simple, secure multitenant, multisite, and multicloud SD-WAN solution for WAN edges in the campus, branch, and cloud. Cloud-managed Contrail SD-WAN delivers the same solution, but the control and management SDN software is Juniper-managed. Customers

do not need to run or maintain Contrail Service Orchestration; they simply onboard the WAN edge and LAN infrastructure to the Juniper cloud-delivered service via the portal or API.

Contrail SD-WAN combines hybrid WAN connections—MPLS, broadband, legacy interfaces, and wireless 4G/LTE—to connect enterprise sites. It unifies Juniper and third-party security and network functions with zero-touch provisioning (ZTP) on secure CPE devices while supporting virtual CPE-like multicloud endpoints in clouds like AWS and Azure. It also dynamically determines the optimal path for specific application traffic based on policies, while assuring consistent and reliable WAN services that align with business objectives using user- and application-level visibility, analytics, and active/passive quality-of-experience testing.

At the heart of the solution, Juniper Contrail Service Orchestration software designs, creates, and coordinates a secure WAN and LAN service. Customers can select the cloud-managed Contrail SD-WAN service offering from Juniper, a partner-provided offering, or deploy and manage Contrail Service Orchestration themselves on premises or in their own cloud.

The Contrail Service Orchestration platform is highly available, scales easily, and supports multitenancy with role-based access. Multitenancy supports separation of concerns among enterprise teams and personalized experiences. For CSPs, multitenancy is fundamental to building out SD-WAN and enterprise services, increasing competitiveness and enabling real profits.

Contrail SD-WAN supports any WAN network architecture and underlay transport. At campus- and branch-based spoke sites, Contrail SD-WAN uses Juniper Networks NFX Series Network Services Platform, SRX Series Services Gateways, and the vSRX

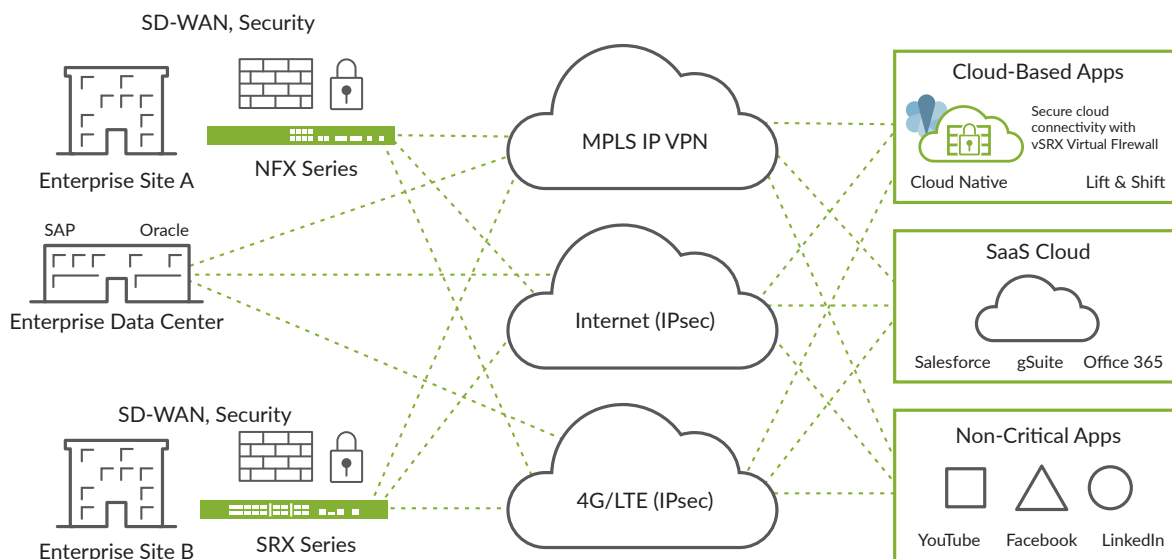


Figure 1: Application routing with SD-WAN

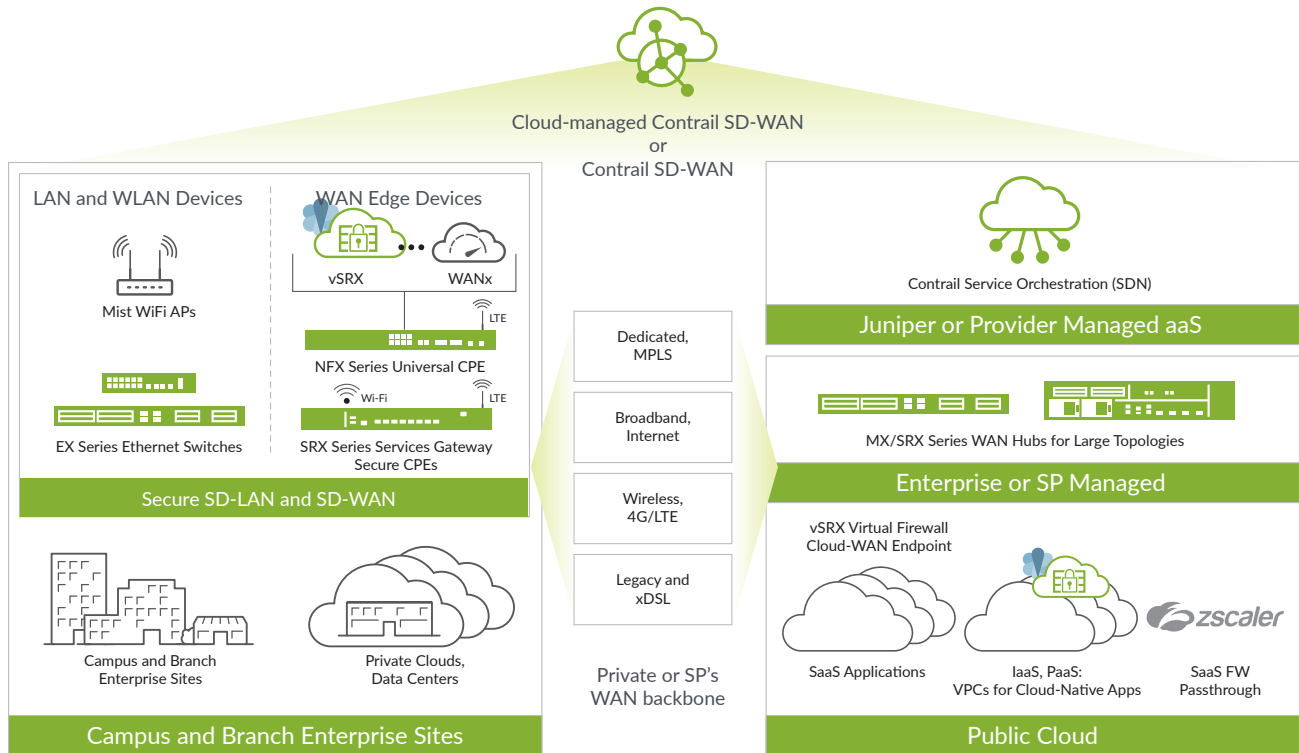


Figure 2: The Juniper Contrail SD-WAN solution.

Virtual Firewall to securely unite the enterprise. In the cloud or atop virtualization platforms, the spoke sites are vSRX virtual firewalls. And powering large-scale WAN topology architectures, physical SRX Series firewalls, vSRX virtual firewalls, or Juniper Networks MX Series 5G Universal Routing Platforms act as routing hubs.

The Contrail SD-WAN solution doesn't stop at the WAN since Contrail Service Orchestration SDN unifies security and management inside the campus and branch as well for LAN and Wi-Fi. It fully orchestrates Juniper Networks EX Series Ethernet Switches to enable SD-LAN services for users, IoT devices, and wireless access points. The Contrail management interface also integrates with wireless LAN products from Mist Systems, interfacing with the Mist Cloud to pull operational visibility into Wi-Fi activity across Mist Access Points, mapping them to enterprise sites and providing the ability to search for wireless endpoints. From the Contrail interface, administrators can cross-launch into the right context of the Mist Cloud interface, where they'll also have visibility into branch switches and WAN analytics. For compact locations needing a CPE all-in-one device connecting WAN, LAN, and WLAN, Juniper offers LAN and Wi-Fi mini cards for the branch SRX Series firewalls.

This evolutionary architecture makes delivering comprehensive enterprise network services easier than ever.

Features and Benefits

Design for Simplicity

Consistently managing branch connectivity is difficult enough without IT staff on hand. Adding security and application-based policies can make WAN configurations even more complex. The Contrail SD-WAN solution was designed with simplicity in mind to provide:

- A more user-friendly Web console experience that guides and automates common workflows
- A broad range of connectivity options, including broadband Internet, MPLS, VPNs, 4G/LTE, and a wide array of legacy WAN interfaces
- Simple branch LAN topologies with Virtual Chassis support
- Larger campus LAN topologies with support for Virtual Chassis technology and ESI LAG
- Wi-Fi integration
- ZTP of WAN and LAN devices and cloud-based endpoints
- Integrated security
- Service design, creation, and operation tools
- Situational awareness and analytics
- Holistic reliability
- Open APIs to simplify third-party component and system integration
- Interoperable "brownfield" WAN networking integration

Upon delivery of enterprise network devices, operators benefit from zero-touch activation of SD-WAN, security, and SD-LAN network functions. For cloud endpoints on AWS specifically, Contrail Service Orchestration automates the endpoint life cycle of the vSRX Virtual Firewall with the help of generated AWS CloudFormation templates. Adding, modifying, or deleting a service like a LAN segment is managed for the entire site as a single entity rather than configuring individual boxes. Security is automatically applied and consistently enforced across all WAN edges and LAN ports, ensuring that sites are safe, while IPsec encryption is applied to all paths traversing the Internet.

Ubiquitous Security

Threats are growing daily. As SD-WAN traffic shifts inexorably towards the Internet, having a security plan for your deployment is critical.

The Contrail SD-WAN solution leverages SRX Series high-performance next-generation firewall (NGFW) software and the vSRX Virtual Firewall to deliver a consistent level of secure SD-WAN in both physical and virtual form factors. The vSRX Virtual Firewall is also included on the universal CPE (uCPE) NFX Series platforms.

Contrail SD-WAN uses deep packet inspection to identify data, determine the optimal route for enterprise applications, and apply security policies to both inbound and outbound traffic while application-based firewall rules offer baseline protection. Additional security layers with unified threat management (UTM), intrusion detection service (IDS), intrusion prevention system (IPS), and antivirus add consistently managed corporate security policies through the enterprise. Juniper Sky™ Advanced Threat Prevention uses real-time information from the cloud to provide anti-malware protection and defend against sophisticated cybercrimes.

The LAN management solution leverages EX Series switches, which support robust first-hop and network access security features to prevent threats at the access layer and also prevent lateral threat propagation.

Integration of the SD-WAN path with the ZScaler Software as a Service (SaaS) firewall and UTM solution offers even more choice for meeting your security needs.

Seamless Integration into Your WAN

When SD-WAN is added to a WAN environment where IP VPN, MPLS, and security already exist, it is critical that the solution integrate seamlessly with the current system while providing a future-proofed path to tomorrow. Contrail SD-WAN's routing easily works with other networks—software-defined or not—based on standard open protocols. All of its API-driven components are open and can be extended via automation or integration to higher-level IT systems or business and operational support systems (BSS/OSS).

The Contrail Service Orchestration platform also administers services in a well-integrated way. Its self-service portal provides access to composed higher-level security and network services, while its administrative portal manages the SD-WAN life cycle and catalogs contributing network functions. Third-party virtualized network functions (VNFs) may be folded in, including WAN optimization. With Contrail SD-WAN, VNFs are delivered on the universal CPE NFX Series platforms.

Reliability and High Performance at Multitenant Scale

Enterprises moving to SD-WAN are more concerned about the reliability of the service compared to service provider IP VPN services with solid SLAs and quality-of-service (QoS) models. SD-WAN cost savings are achieved by using lower-cost Internet WAN connections to offload site-to-Internet traffic and site-to-site with IPsec. Contrail SD-WAN always delivers carrier-grade reliability.

Benefiting the end user and application experience, the solution provides for high availability of the SDN control and management plane as well as the interconnection of the WAN topology of multilinked hub-and-spoke sites or a mesh of WAN edge infrastructure. Application traffic quality is monitored using Juniper Networks Application Quality of Experience (AppQoE) technology, and metrics are collected and analyzed by Contrail Service Orchestration, ensuring that desired reliability levels are met and further optimizing the user experience.

Additionally, Juniper has opened up more architectural reliability and flexibility in the branch and WAN. SRX Series firewalls and NFX Series uCPE devices now support active/active clustering, delivering double the connectivity and reliability to your most important sites when paired—an industry first for SD-WAN.

As service providers look to deliver SD-WAN services, and as enterprises seek assurances that these services can be delivered across all locations, the resulting platform must be agile and capable of scaling cost effectively. While simpler SD-WAN systems offer single tenancy scale and basic reliability, Contrail's foundational microservices architecture ensures cloud-grade reliability and scalability to enable multitenancy and ensure high availability and high performance.

User and Application-Aware Controls and Analytics

Real-time inspection, identification, and policy classification on user and application traffic is foundational to SD-WAN. The NFX Series services platforms, SRX Series firewalls, and vSRX virtual firewalls keep track of every session, every application, and every user. This full Layer 7 inspection not only enables application routing and security policies, it is the basis for the collection of fine-grained metrics fueling administrator and tenant visibility and the analysis for automatic service adjustments and performance optimizations.

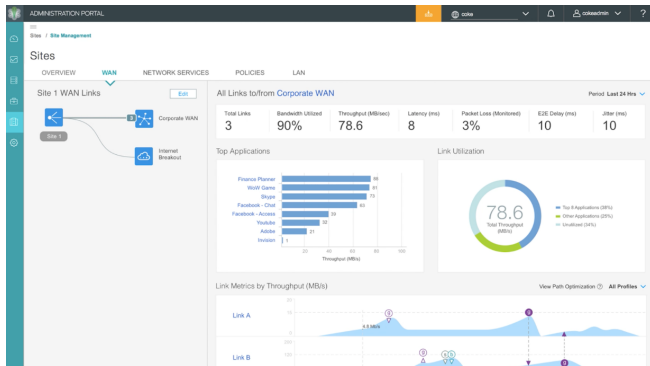


Figure 3: Analytics visualization window

Solution Components

Contrail Service Orchestration

Juniper Contrail Service Orchestration includes a web-based management interface for defining policies, managing locations, and visualizing performance behavior, automating the provisioning and management of devices running SD-WAN, SD-branch, and SD-LAN services.

With the Juniper cloud-managed Contrail SD-WAN solution, customers do not need to run or maintain the Contrail Service Orchestration component of the SD-WAN solution.

NFX Series Network Services Platform

The NFX Series Network Services Platform includes powerful on-premises devices for SD-WAN and SD-branch that consolidate notorious cable-chained branch appliances, replacing them with VNFs running on a universal CPE to deliver security driven by an embedded vSRX Virtual Firewall. Two NFX Series devices at a single branch site can be paired in an active/active arrangement, doubling traffic throughput and delivering twice the availability of the branch's WAN. NFX Series devices also support a variety of mini physical interface cards for LAN MACsec and PoE+ ports, various WAN ports, and WAN wireless LTE connectivity.

SRX Series Services Gateways

For use cases not requiring universal CPE platforms, SRX Series Services Gateways—up to and including the high-end SRX4000 line—can act as secure CPE platforms for intrinsically secure SD-WAN. These physical devices combine SD-WAN, NGFW, and UTM services with routing and switching in a single, high-performance, cost-effective device. Two SRX Series firewalls at a single branch site can be paired in an active/active arrangement, doubling traffic throughput and delivering twice the availability of the branch's WAN. Branch SRX Series devices also support a variety of mini physical interface cards for Wi-Fi, LAN MACsec and PoE+ ports, various WAN ports, and WAN wireless LTE connectivity.

vSRX Virtual Firewall

The vSRX Virtual Firewall delivers the same features as its physical SRX Series counterparts, providing the comprehensive security required by SD-WAN in a virtualized form factor. The vSRX can run on a branch-based virtualization platform or public cloud Infrastructure as a Service (IaaS); on AWS, it can be fully life-cycle managed with automation. Performance is optimized to maximize throughput in a virtualized environment by leveraging single-root I/O virtualization (SR-IOV) and a Data Plane Development Kit (DPDK).

SD-WAN Gateways and Hubs

To scale large SD-WAN topologies, gateways may reside in the network to aggregate iBGP routes over IPsec and generic routing encapsulation (GRE) tunnels. The SD-WAN gateway is supported on the vSRX Virtual Firewall, SRX1500 and SRX4000 Services Gateways, and MX Series 5G Universal Routing Platforms.

With Contrail SD-WAN, ZScaler and Internet breakout can happen from these hubs as well as the spoke sites.

EX Series Ethernet Switches

The EX Series Ethernet Switches with Virtual Chassis technology combine reliability of modular systems with the economics and flexibility of stackable switches, delivering a high-performance, scalable solution for campus, remote and branch office environments. In a Virtual Chassis configuration, multiple EX Series switches can be interconnected to operate as a single, logical device, dramatically simplifying management and support. In an open, standards-based ESI LAG configuration, switches are managed individually and easily via Contrail Service Orchestration. With multi-gig port speeds and up to 95 W Power over Ethernet (PoE++) support, enterprises can deploy an evolvable EX Series-based wired network infrastructure that can address a future that includes IoT and Wi-Fi 6.

Mist Cloud and Wi-Fi Access Points

The Mist platform can be fully operated and managed through a programmable cloud that includes microservices and an inline AI engine to deliver superior scalability, agility, resiliency, and insights. Mist offers a range of Wi-Fi access points and a variety of cloud-based services, such as asset tracking, location capabilities using virtual Bluetooth Low Energy (vBLE), wired and wireless assurance, and the Marvis AI-Driven Virtual Network Assistant. Contrail Service Orchestration's web portal provides visibility into Mist Access Points by enterprise site and context-aware pass-through to the Mist portal.

Professional Services

Juniper offers advisory, implementation, and testing services that help customers and partners evaluate technology choices and develop a plan to integrate them into existing network infrastructures. Schedule a consultation with Juniper

Professional Services to build a strategic plan and tailor a solution for your business. Leveraging the deep experience of Juniper's industry-leading service and support experts will minimize risk, speed time to deployment, and deliver the desired business outcome.

Use Cases

The demand for SD-WAN, SD-LAN, and SD-branch stems from use cases that are driving the need for agile, on-demand services with improved cost profiles. The benefits from these common scenarios are consistent, but the drivers and situations vary.

Secure Internet Breakout and Wireless Reach

WAN requirements vary across enterprises and applications, sometimes driving the need for a breakout at the branch site. Using Contrail SD-WAN to map application needs to business criteria, a secure local breakout gives sites the choice of routing traffic securely over a broadband Internet connection or over a dedicated connection with high SLAs. SD-WAN hub sites also support Internet breakout for efficient routing to multicloud infrastructure from choice hub locations such as data center collocation providers. The branch WAN edge devices also support access for remote and mobile sites that require wireless 4G/LTE connectivity, as many sites may benefit from the general simplicity of wireless access.

Cloud-Optimized Network Regional Breakout

To access cloud applications and services, branch offices often leverage MPLS connections back to the corporate location before creating a breakout from the campus location towards the cloud service. In this situation, SD-WAN can be deployed to activate a more optimal network breakout that is regionally based. At this breakout point, traffic can be redirected to the Internet to gain access to the cloud or directed to an MPLS connection to the cloud service for high SLA traffic. With Contrail SD-WAN, throughput and latency are optimized, with the best path to the cloud service within the policy constraints designed by network engineers.

Remote Site Aggregation

Intelligently aggregating multiple broadband links at the remote office provides a secure pipe for moving corporate traffic into the private MPLS WAN through distributed aggregation points at branch or enterprise locations. This helps efficiently manage WAN links, secure corporate traffic, and reduce costs at remote offices. Contrail SD-WAN's intelligent solution sends data over multiple links while prioritizing streams through easy-to-create policies, ensuring efficient handling of available bandwidth with less loss and jitter.

B2B Integrations and Acquisitions and Mergers

The need to establish secure connections between two entities in a B2B relationship, or to integrate two companies following a merger, is a common scenario. Contrail SD-WAN provides an on-demand model for business to connect securely, avoiding the pitfalls of misalignment created by the provisioning times of traditional MPLS connections.

Distributed Enterprise

Large enterprises with hundreds or thousands of sites across the world need a central orchestration system that manages remote and branch offices without the need for technical expertise on site. Contrail SD-WAN provides abstracted control and automated workflows, enabling the entire distributed branch infrastructure to be managed in a unified way.

All-in-One Branch in a Box and Wireless Branch

Enterprises with small sites or kiosks often want the simplicity of integrating security and connectivity for WAN, LAN, and Wi-Fi into a single device, all remotely managed by a central staff with ZTP and SDN policy and control. The branch SRX Series firewalls and their variety of mini physical interface cards meets these requirements. For example, for an all-wireless site, integrated wireless 4G LTE can be used for WAN connections while integrated Wi-Fi can be used for WLAN connections. Juniper wireless 4G LTE cards meet all primary global wireless standards and are fitted with dual SIMs with automatic switchover for reliability.

Summary—Automate and Simplify the WAN with Juniper Contrail SD-WAN

Whether creating an evolvable architecture to simplify SD-WAN growth, seamlessly managing virtual network services such as cloud endpoints and on-premises universal CPE platforms, managing and enforcing multiple levels of security policy across multicloud and enterprise sites, or collecting and analyzing data for situational awareness, efficiency, and management, Contrail SD-WAN delivers a flexible and multifaceted solution.

Contrail SD-WAN uniquely allows you to chart a course through any sized campus and branch SD-WAN to also include SD-LAN, seamlessly integrating full-stack security, monitoring, and third-party network services.

Next Steps

To learn more about how Juniper's SD-WAN and branch solutions can help your company gain a competitive edge, contact your Juniper sales representative or visit <http://juniper.net/sd-wan>.

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

Fax: +1.408.745.2100

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

Fax: +31.0.207.125.701

JUNIPER NETWORKS | Engineering
Simplicity



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.