Solution Brief

Business applications, information, processes, and even retail storefronts are shifting inexorably to the cloud, driving greater business dependency on WAN resources delivered by service providers. This growing dependence on public and private infrastructure to support today's business needs means that the modern WAN must be secure, scalable, and application-aware.

Enter software-defined WAN (SD-WAN), which promises a rich and dynamic application experience for IT departments and end users—the ideal solution for empowering this much-needed WAN transformation. To meet the growing, dynamic needs of the enterprise, SD-WAN must accommodate existing WAN requirements plus new capabilities such as Zero Touch Provisioning (ZTP) for the automation and rapid deployment of network equipment and services, and the ability to enhance application performance with better economics. For communication service providers (CSPs), SD-WAN provides the ability to deliver a valuable new managed service that enhances their current portfolio. As enterprise organizations look to diversify their WAN connectivity options, SD-WAN simplifies and streamlines service delivery, shrinks time to delivery windows, provides security to ensure the protection of their customers and their business information, reduces costs by automating operations and management, and provides 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 ACG Research\(^1\), the typical enterprise customer, embarking on this migration, accesses six 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-WAN\(^2\). 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.

\(^{1}\) ACG Research, November 2016, Ray Mota at Layer123 SDN Event
\(^{2}\) Source: [http://www.gartner.com/it/content/3478900/3478918/november_8_sdwan_forecast_opportunity_jskorupa.pdf](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. Furthermore, SD-WAN should also simplify service assurance and reliability engineering through visibility, analytics, and automation.

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.

CSPs can leverage SD-WAN to deliver a managed, secure service that meets the growing and dynamic needs of their enterprise customers. SD-WAN can also simplify and streamline the delivery of existing network infrastructure services, such as broadband Internet, carrier Ethernet, and VPN and MPLS services, allowing providers to take advantage of their 4G/LTE network infrastructure as well. The integrated security, GUI-based management, orchestration and reporting tools, redundancy and failover capabilities, and ZTP features provided by SD-WAN help to simplify and streamline the deployment and management of their managed services.

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 network services while expanding their footprint to reach more customers.

For enterprises, offering SD-WAN as a managed service helps achieve better business outcomes by enabling them to forge better, more secure B2B relationships, conduct mergers and acquisitions faster and more efficiently, and provide more cost-effective access to cloud-based applications.

The Juniper Networks Contrail SD-WAN Solution

Juniper Networks’ Contrail® SD-WAN delivers a simple, secure, multitenant, multisite, and multicloud SD-WAN solution, combining hybrid WAN connections—MPLS, broadband, legacy interfaces, and wireless 4G/LTE—to connect sites. Contrail SD-WAN unifies Juniper and third-party security and network functions with 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 service, running just as well on premises as in the cloud. The platform is highly available, scales easily, and supports multitenancy with role-based access. Multitenancy supports separation of concerns among enterprise teams and personalized experience. For CSPs, multitenancy is fundamental to building out SD-WAN as a service and more, increasing competitiveness and enabling real profits.

Figure 1: Application routing with SD-WAN
Contrail SD-WAN supports any WAN network architecture and underlay transport. At branch or spoke sites, Contrail SD-WAN uses Juniper Networks NFX Series Network Services Platform, SRX Series Services Gateways, and the vSRX Virtual Firewall to securely unite the enterprise. In the cloud or atop virtualization platforms, the spoke sites are vSRX firewalls. And powering large-scale WAN architectures, physical SRX Series firewalls, vSRX Virtual Firewalls, or Juniper Networks MX Series Universal Routing Platforms act as routing hubs.

By optionally augmenting Contrail SD-WAN with full-stack carrier-grade Network Functions Virtualization (NFV), powered by Contrail Cloud, CSPs can grow beyond providing managed services for SD-WAN and SD-Branch to realize the complete Juniper Cloud CPE solution—the industry’s most dynamic service creation platform. For CSPs, an evolutionary architecture to deliver comprehensive network services has never been easier.

### Features and Benefits

#### Design for Simplicity

Consistently managing branch connectivity is difficult enough. Adding SD-WAN with application-based policies makes WAN configurations even more complex. The Contrail SD-WAN solution has been designed with simplicity in mind, optimized for Day 1 deployment to provide:

- A more user-friendly Web console experience
- A broad range of connectivity options, including broadband Internet, MPLS, VPNs, 4G/LTE, and legacy interfaces
- Integrated security
- Service design, creation, and operation tools
- Situational awareness and analytics
- Holistic reliability
- Open APIs to simplify third-party component and system integration
- Brownfield networking integration

Upon delivery of a CPE device, tenants benefit from zero-touch activation of SD-WAN, security, and optionally other network functions. For cloud endpoints on AWS and Azure, Contrail Service Orchestration automates endpoint life cycle of the vSRX Virtual Firewall. Security is automatically applied and consistently enforced across all WAN edges, 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 the SRX300 line of Services Gateways, 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. 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 (Juniper Sky ATP) uses real-time information from the cloud to provide anti-malware protection and defend against sophisticated cybercrimes.

**Seamless Integration**

When SD-WAN is added to a WAN environment where MPLS, security, and WAN optimization 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 tenant 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 virtual network functions (VNFs) may be folded in, including WAN optimization and WLAN control. With Contrail SD-WAN, VNFs are delivered upon the universal CPE NFX Series platforms. For CSPs deploying the full cloud CPE solution, VNFs run at the best location for satisfying customer requirements—distributed or centralized on the NFV infrastructure.

**High Reliability and 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 QoS models. SD-WAN cost savings are achieved by using lower-cost Internet WAN connections to offload branch-to-Internet traffic and branch-to-branch 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 full mesh of WAN edge infrastructure. Application traffic quality is monitored using Juniper Networks 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. An SD-WAN industry first, Juniper’s NFX Series uCPE devices now support active-active clustering, delivering double the connectivity and double the reliability to your most important sites when paired.

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 Service Orchestration’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 Network Services Platform, 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.
Solution Components

Juniper Contrail Service Orchestration includes an end-user portal for defining policies, managing locations, and visualizing performance behavior. It automates the provisioning and management of CPE devices running SD-WAN and network services.

NFX Series Network Services Platform

The NFX Series 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 the traffic throughput and delivering twice the availability of the branch's WAN.

SRX300 Line of Services Gateways

For use cases not requiring universal CPE platforms, the SRX300 line of Services Gateways is a secure CPE platform for SD-WAN. These physical devices combine SD-WAN, next-generation firewall, and unified threat management (UTM) services with routing and switching in a single, high-performance, cost-effective device.

vSRX Virtual Firewall

The vSRX, a virtualized form of the SRX Series Services Gateways, delivers the same features as its physical counterpart required for secure SD-WAN. The vSRX can run on a branch-based virtualization platform or be fully life cycle-managed in clouds such as Azure and AWS. 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 Universal Routing Platforms.

Professional Services

Juniper offers professional services that help customers and partners evaluate technology choices and develop a plan to integrate them into existing network infrastructures. SD-WAN services cater to all phases of your investigation and implementation journey. Start with JumpStart Services to build a strategic plan; leverage Field Trial Services to gain experience; and utilize Implementation Services to deploy. 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 stems from use cases that are driving the need for agile, on-demand WAN services with improved cost profiles. The benefits from these common scenarios are consistent, but the drivers and situations vary.

Secure Local Breakout and Wireless Reach

WAN requirements vary across enterprises and applications, sometimes driving the need for a breakout at the site. Using Contrail Service Orchestration 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. The NFX Series also supports access for remote and mobile sites that require wireless 4G/LTE connectivity, but 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.

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

Whether creating an evolvable architecture to simplify SD-WAN and SD-Branch growth, seamlessly managing virtual network services 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 addresses these multitenant service provider requirements.

Contrail SD-WAN uses Contrail Service Orchestration to design, secure, automate, and run the entire service life cycle across the NFX Series Network Services Platform, MX Series Universal Routing Platforms, and SRX Series Services Gateways, as well as vSRX Virtual Firewall secure cloud endpoints. This one solution uniquely allows you to chart a course through SD-WAN and SD-Branch, seamlessly integrating full-stack security, monitoring, and third-party network services.

The Contrail SD-WAN solution provides annual and multiyear subscriptions that include Contrail Service Orchestration. They are available in simple bundles of software and hardware platforms; alternatively, Contrail Service Orchestration and other systems may be purchased individually.

Next Steps

To learn more about how Juniper’s SD-WAN 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.