Juniper Networks | Engineering Simplicity

White Paper

SECURE SD-WAN

Juniper's Approach to Secure SD-WAN Architecture

EXECUTIVE SUMMARY

Organizations need help understanding the paths available when considering the software-defined wide area networking (SD-WAN) options available to them. Over many years, Juniper Networks has pioneered and supported secure SD-WAN for organizations around the world. As cloud adoption and connectivity requirements have increased, businesses have more choices for connecting their branch and distribution locations, Juniper's innovations have kept pace, delivering capabilities that address these options at every step. With the Juniper Connected Security strategy, customers are assured a "no compromise" security posture with the flexibility and operational ease of addressing diverse application requirements regardless of their WAN connectivity or routing needs. Organizations worldwide, in every vertical, depend on Juniper to support their critical customer and employee needs from branch to cloud.

Introduction

Traditional branch offices are no longer able to provide the security and access flexibility enterprises need to deliver the quality of experience demanded by the business. Organizations require additional capacity and improved application awareness to ensure their users have access from anywhere.

The Challenge

The cloud has transformed how we consume applications and data. In many cases, this has taken the form of Software as a Service (SaaS), further impacting traffic flow and increasing transfers directly from users to the cloud and back. Cloud and SaaS consumption have radically changed how security and network teams secure and improve the quality of user experience across their organizations. For businesses with more than a handful of locations, this has historically been a challenging, operationally burdensome task. Basic SD-WAN only addresses a portion of these challenges, leaving enterprises to solve security separately—a daunting task, given the rapid advances in threat actor efficacy.

The Solution

Juniper developed its Secure SD-WAN branch architecture on top of its award-winning Juniper Networks® SRX Series Services Gateways, adhering to principles in our Connected Security strategy. Under this approach, security and network convergence offers enterprises a new approach that improves efficacy and the ability to see, automate, and protect users and data at every point of connection.

Through a cloud-native management interface, enterprises can employ zero-touch provisioning (ZTP) to automatically configure both security and networking policies, regardless of the branch's physical location. The SRX Series firewalls provide several models to choose from and can accommodate any size branch or performance requirements an organization might have. Using an SRX Series firewall, customers can take advantage of advanced threat prevention, network intrusion prevention system (IPS), and secure Web gateway functions such as URL filtering, antivirus, and data loss prevention (DLP) to provide a holistic offering that includes many other cloud-enabled security capabilities while supporting branch offload or direct-to-SaaS performance.

Benefits

Juniper's uncompromising approach to network security innovations, which provides customers with a best-in-class, automated deployment of SD-WAN and SD-branch with ZTP, ensures ease of deployment and centralized orchestration. Software-defined and AI-driven control of LAN, Wi-Fi, and security provides consistent access to and management control over all sites, including campus, branch, work-from-home, and temporary locations, supported by both secure SD-WAN policy and analytics.

Additionally, Juniper's existing branch SRX Series customers can easily enroll their existing SRX Series firewalls in a secure SD-WAN, avoiding the need to replace their appliances to enjoy the benefits of the technology. Few customer environments are alike. While less flexible competitive solutions require you to purchase additional equipment and lock you in, Juniper's approach maximizes the value of its solutions over their lifetime.

SD-WAN in Transition: From Building a Better WAN to Optimizing Client to Cloud Connectivity

SD-WAN promised to offer more WAN choice and flexibility while providing better visibility and easier management of WAN resources, coupled with a pledge to reduce the cost of maintaining expensive and rigid intranet circuits such as MPLS. Adding multiple links, including inexpensive broadband or direct Internet access to branch sites, delivered:

- More capacity with less expensive bandwidth
- Higher availability through priority-based load balancing
- Greater resilience with active/active WAN architectures

The shift to cloud and the migration to SaaS applications allowed SD-WAN to shine, highlighting its ability to enable and accelerate cloud adoption. Although SD-WAN fully supports traditional hub-and-spoke architectures, it enables alternative topologies that better reflect cloud traffic flows. Traditional WAN topologies routed all branch traffic back to a corporate headquarters (see Figure 1).

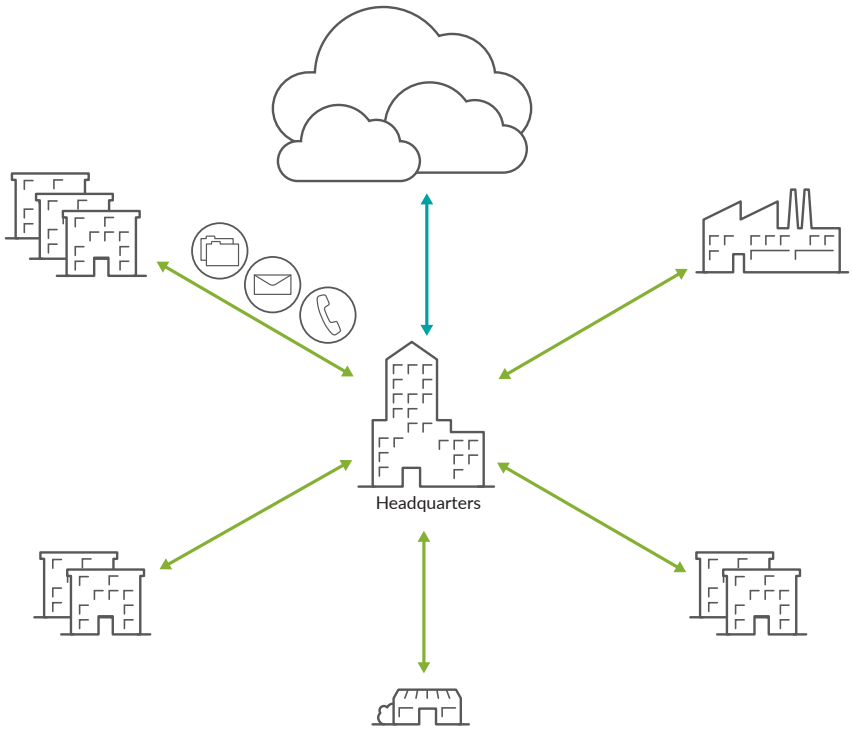

Figure 1: Hub and spoke, backhauling all traffic to headquarters

This made sense at the time, since legacy applications resided in the corporate home data center. Even legacy communication traffic like voice and e-mail was backhauled to headquarters, where it was centrally scrubbed through the corporate perimeter firewall. Conversely, with cloud, more than 90% of traffic is Internet bound. Do any of the following applications sound familiar?

- Communication: Zoom, Microsoft Teams, Skype, Ring Central
- CRM: Salesforce, Oracle
- Office: O365, G Suite
- Collaboration: Slack, Microsoft Teams
- Tasks: Jira, Smartsheets

This list doesn't even include other popular, more prevalent apps and technologies like YouTube, blogs, social, research, and so on. How about general Internet search, or traffic generated by guest Wi-Fi? It's all bound for the Internet.

Backhauling this traffic to headquarters comes at a cost:

- It imposes a 400% bandwidth "tax" by unnecessarily keeping traffic "on the intranet" longer
- It adds 2x round-trip time (RTT) latency, causing poor application experience

As a result, it becomes too costly to duplicate the "HQ stack." SD-WAN, on the other hand, allows local breakout of cloud-bound traffic at the branch (see Figure 2).

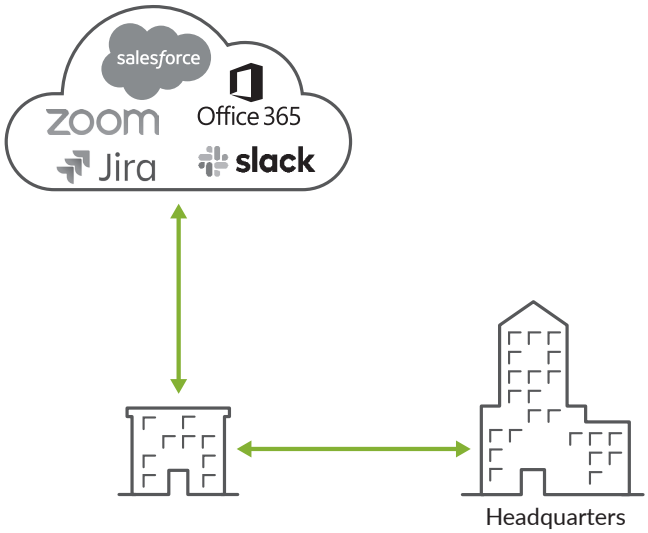

Figure 2: Breakout at the branch

While internal applications hosted in a private data center still exist, they consume a smaller percentage of the bandwidth required for all traffic destined for the WAN link from the branch. These applications, such as point of sale (POS)/inventory systems, healthcare data, and financial software, may be dependent on specific industries.

In discussions with customers around the globe, the opportunity to rethink branch connectivity strategies is not limited to WAN connection methods; it also includes other aspects of branch management. Large enterprises will continue to leverage MPLS/VPN and integrate SD-WAN to improve business outcomes, while small to medium-sized businesses may choose that approach or employ a complete SD-WAN overlay.

At the same time, the need to scale both secure work-from-home and temporary site initiatives drives a requirement for scale and flexibility that is redefining connectivity for everyone. Gartner introduced a new term in 2019, Secure Access Service Edge (SASE), which represents enterprise needs that began to emerge over the last couple of years. While enterprise decisions will be driven by requirements and currently available technologies, SASE will certainly

be top of mind for most SD-WAN considerations moving forward. Leveraging a cloud breakout with cloud security combines the best security and application experiences to accommodate branch-to-cloud needs in the most compelling and effective way.

Unfortunately, not all solutions are equally capable. While they all provide some level of connectivity between sites, offerings differ in their ability to provide stability, security, and operational ease. Few offer flexible architectures that integrate security, provide multiple WAN connectivity options, and deliver the ability to manage holistically non-WAN connectivity.

The Juniper Secure SD-WAN Solution

The Juniper Secure SD-WAN solution offers two administrative modalities: on-premises and cloud-based. The solutions are identical, although the control and management-plane software in the cloud-based version are Juniper-managed. With cloud-based Secure SD-WAN, organizations do not need to run or maintain a separate service orchestration console; they merely onboard the WAN edge and LAN infrastructure to the Juniper cloud-delivered service via the browser portal or API.

Juniper Secure SD-WAN supports any WAN network architecture and underlay transport. At spoke sites, Juniper Networks NFX Series Network Services Platform (purpose-built network function virtualization [NFV] appliances), SRX Series firewalls, or the Juniper Networks vSRX Virtual Firewall can all be used to unite the enterprise securely. In the cloud or on top of virtualization platforms, connectivity is provided by vSRX virtual firewalls. At the same time, large-scale WAN topology architectures can use the physical SRX Series firewalls, with vSRX virtual firewalls acting as routing hubs at major sites. This deployment freedom gives enterprises the ability to meet their secure branch needs, regardless of location, technology, or business requirements, which is the essence of enabling a threat-aware network.

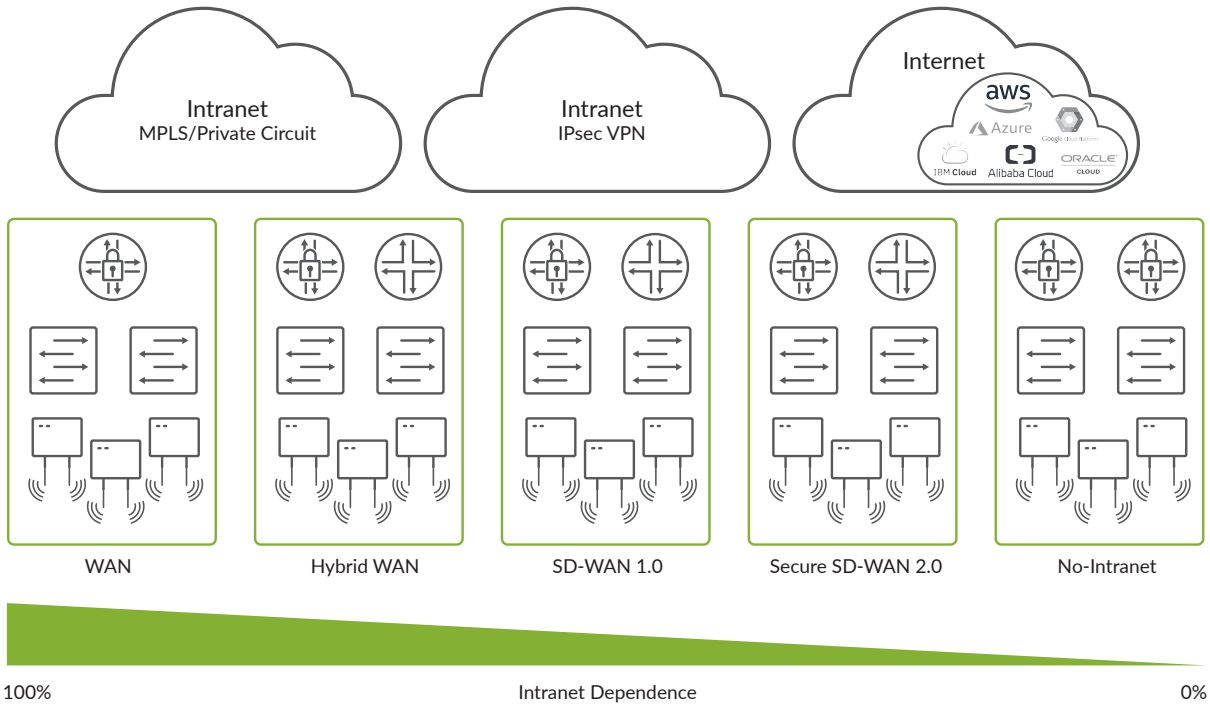

Figure 3: Migration to the cloud

The cloud management interface also integrates with wireless LAN products from Mist Systems, a Juniper company, 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 cloud 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 customer premises equipment (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.

User and Application-Aware Controls and Analytics

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

Looking Ahead, Intranet Dependence Decreases

Figure 3 shows that over time, the need for a private WAN diminishes and, in some cases, disappears. This diminished need is due to an increase in SaaS-first strategies, born in the cloud companies, and an increase in the distributed enterprise.

Security services will also migrate to the cloud, driven by initiatives to lower maintenance, preserve bandwidth, and improve user experience by moving workloads closer to the end user.

Lastly, management and operational simplicity will be critical, taking advantage of simplified operations through machine learning and artificial intelligence.

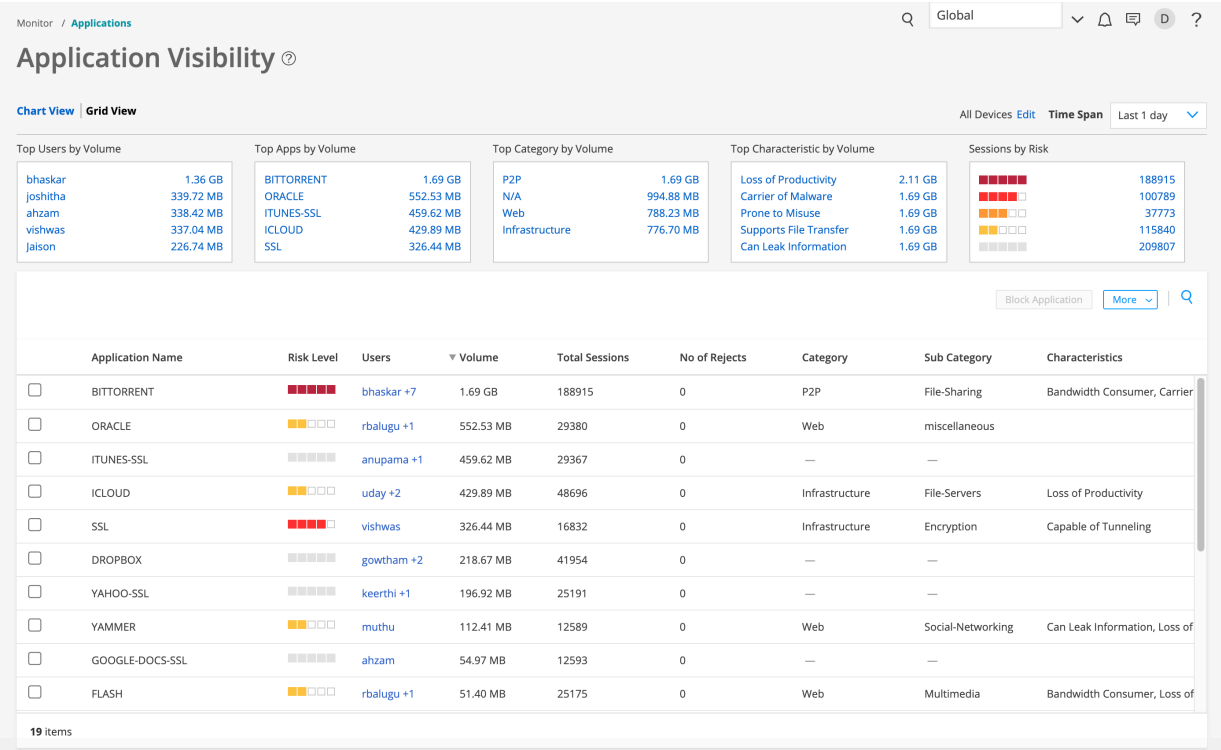

Figure 4: Detailed application visibility

Ubiquitous Security

As SD-WAN traffic shifts inexorably towards direct Internet links, having a security plan for your deployment is critical. The Juniper Secure 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 is also included on the universal CPE (uCPE) NFX Series platforms, delivering the consistency that enterprises require for their diverse vendor and distributed environments—one of the primary challenges Juniper sought to address with Connected Security.

Juniper's Secure SD-WAN uses deep packet inspection (DPI) to identify data, determine the optimal route for enterprise applications, and apply unified security policies to both inbound and outbound traffic—all while application-based firewall rules offer baseline protection. Additional security layers with advanced security services, intrusion detection service (IDS), IPS, and antivirus provide consistent managed security policies. Juniper Advanced Threat Prevention uses real-time information from the cloud to provide anti-malware protection and defend against sophisticated cybercrimes.

Features and Benefits

Historically, enterprises have lacked choices when it came to the WAN. MPLS with a service-level agreement (SLA) was pretty much the de facto choice of the last decade. With secure SD-WAN and SASE options now available, pervasive inspection of traffic and the management of all WAN services is here, freeing enterprises to use alternate services such as DSL and cable to augment or replace their MPLS links at branch sites. The Juniper Secure SD-WAN solution was designed to provide:

- A unified approach to creating SD-WAN and security policies with workflow management in a single UI that guides and automates common workflows to support greater control and policy granularity
- ZTP of WAN and LAN devices and cloud-based endpoints
- User- and application-based policies offering 5000 predefined applications
- A full suite of cloud-delivered advanced security services like advanced threat prevention and URL filtering anti-malware with industry-leading IPS verified by NSS Labs 2019 DCSG Test Report
- Service assurance capabilities, ensuring quality user experience by identifying flows or links that are impacting locations and applications
- A broad range of connectivity options, including broadband Internet, MPLS, VPNs, 4G/LTE, and a wide array of legacy WAN interfaces
- Service design and operation tools, including APIs that simplify third-party component and system integration
- Lower TCO and simplified procurement with Juniper WAN edge devices that combine security and SD-WAN

Upon delivery of enterprise network devices, operators benefit from the ZTP capabilities of SD-WAN, security, and SD-LAN network functions. 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. In addition, IPsec encryption is applied to all paths traversing the Internet; however, Juniper Secure SD-WAN's simplification of connectivity doesn't end there.

For cloud endpoints on AWS specifically, Juniper's management automates the endpoint life cycle of the vSRX Virtual Firewall with the help of generated AWS CloudFormation templates, making it possible to run the vSRX as an SD-WAN hub and NGFW.

Seamless Integration into Your WAN

When adding SD-WAN to a WAN environment where IP VPN, MPLS, and security already exist, the solution must integrate seamlessly with the current system while providing a future-proofed path to the future. Juniper Secure SD-WAN possesses robust routing that easily works with other networks—software-defined or not—based on

standard open protocols, which is not always the case with offerings from vendors new to networking. All Juniper Secure SD-WAN's API-driven components are open and can be extended via automation or integration to other orchestration systems already in use.

Contrail® Service Orchestration platform also administers services through a unified approach. 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 included, with components such as WAN optimization. With Juniper Secure SD-WAN, VNFs are delivered on the uCPE NFX Series platforms.

Reliability and High Performance at Multitenant Scale

Enterprises moving to SD-WAN often raise concerns about the reliability and user experience of the service compared to service provider IP VPN services with solid SLAs and quality-of-service (QoS) models. Achieve SD-WAN cost savings by using lower-cost Internet WAN connections to offload both site-to-Internet traffic and site-to-site traffic via IPsec. Juniper Secure SD-WAN delivers resilience and reliability through robust traffic inspection and monitoring, as well as flow analytics to make adjustments based on demand and network policy needs.

Juniper's 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 Application Quality of Experience (AppQoE) technology; metrics are collected and analyzed by Contrail Service Orchestration, ensuring that desired reliability levels are met, further optimizing the user experience.

Connectivity and reliability can both be enhanced with industry-first support for active/active clustering of both SRX Series firewalls and NFX Series uCPE devices. Contrail's foundational microservices architecture ensures cloud-grade reliability and scalability to enable multitenancy and ensure both high availability and high performance.

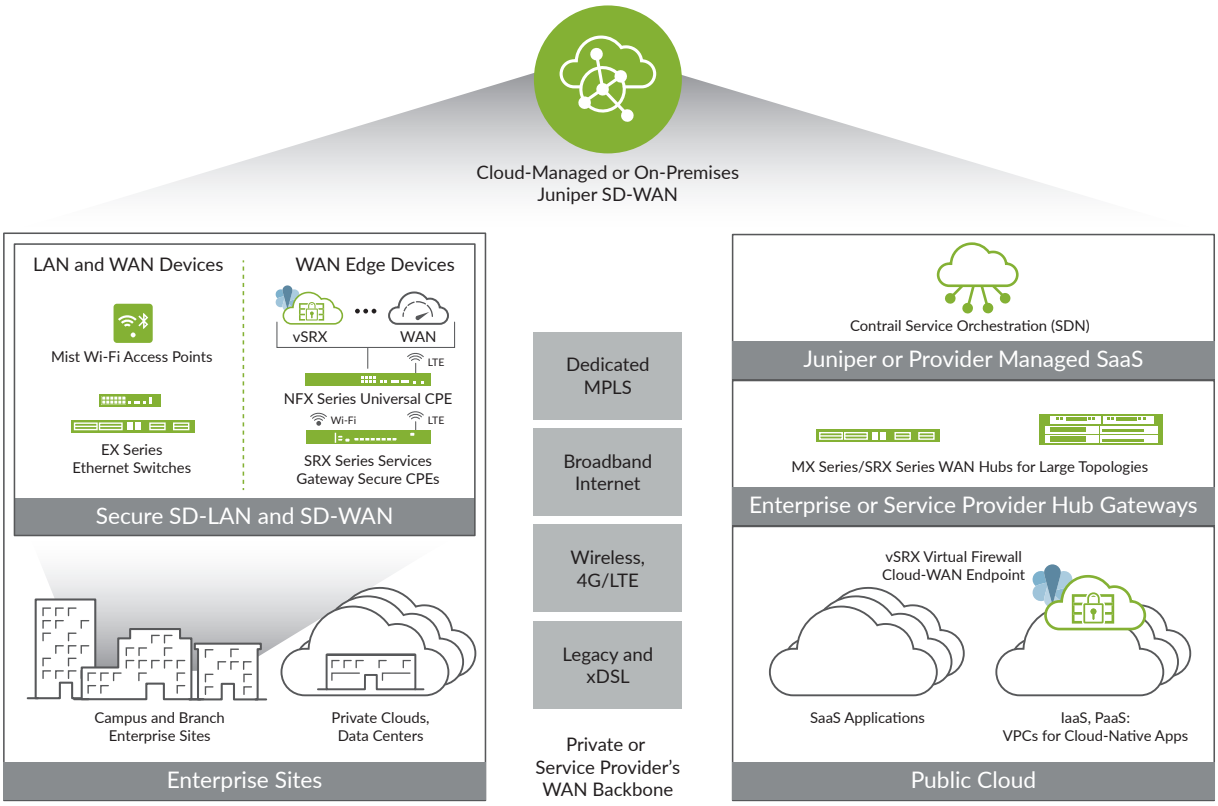

Figure 5: Juniper Secure SD-WAN Solution.

Juniper Secure SD-WAN Solution Components

Contrail Service Orchestration

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

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 WAN edge connection platforms for secure SD-WAN. These physical devices combine SD-WAN and advanced security 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, offering the ability to increase connectivity while delivering twice the availability of the branch's WAN. Branch SRX Series devices support a variety of mini-physical interface cards for Wi-Fi, LAN Media Access Control Security (MACsec) and Power over Ethernet Plus (PoE+) ports, various WAN ports, and WAN wireless LTE connectivity.

NFX Series Network Services Platform

The NFX Series Network Services Platform family 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 uCPE 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 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.

Use Cases

The demand for SD-WAN, SD-LAN, and SD-Branch stems from varying 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, and ultimately every scenario requires uncompromising security.

Secure Internet Breakout and Wireless Reach

WAN requirements vary across enterprises and applications, compelled more often today by SaaS or multicloud requirements that drive the need for hybrid WAN/split tunneling at a WAN edge site. Using Juniper Secure SD-WAN to map application needs to business criteria, a secure local breakout with advanced threat prevention gives sites the choice of routing traffic securely over any type of WAN connection, including mobile connectivity, multiple types of Internet connectivity, and dedicated connections with high SLAs. SD-WAN hub sites also support this Internet breakout capability, allowing for efficient routing from hub locations such as data center collocation providers. With Juniper SD-WAN, throughput and latency are optimized, using the best path to the cloud service within the policy constraints designed by network engineers.

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 requiring onsite technical expertise. Juniper Secure SD-WAN provides abstracted control and automated workflows, enabling the entire distributed branch infrastructure to be managed in a unified way. Juniper Networks' history of operating at service provider scale ensures that enterprises, who increasingly function as service providers themselves, are supported by Juniper's ability to scale to meet any need, simply and reliably.

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 Modules meet these requirements. For example, for an all-wireless site, integrated wireless LTE can be used for WAN connections, while integrated Wi-Fi can be used for WLAN connections. Juniper wireless LTE cards meet all primary global wireless standards and are fitted with dual Subscriber Identity Modules (SIMs) with automatic switchover for reliability.

Professional Services

Juniper offers advisory, implementation, and testing services that help customers and partners evaluate technologies and 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.

Summary

Juniper Secure SD-WAN creates an evolvable architecture that simplifies and secures SD-WAN while offering the ability to handle any amount of growth. It offers seamless management for virtual network services such as cloud endpoints and on-premises uCPE platforms, and it manages and enforces multiple levels of security policy across all points of presence for any organization. Juniper Secure SD-WAN provides IT teams with the tools needed to collect and analyze data for situational awareness, efficiency, and management, enabling them to deliver a flexible and multifaceted solution.

Juniper Secure SD-WAN uniquely enables organizations to manage and secure all of their connectivity needs, seamlessly integrating full-stack security, monitoring, and third-party network services.

To learn more about how Juniper Secure 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