Juniper Networks | Engineering Simplicity

TechTarget | Custom Media White Paper

Five Must-Haves for Next-Gen SD-WAN Solutions

EXECUTIVE SUMMARY

Although every business relies on the internet, the truth is that networking was never designed to securely handle today's experience-rich application environments. The original internet host systems were more than happy to share files and information with any and all connected devices, and security protocols were virtually nonexistent.

As a result, the modern internet is fraught with bad actors pouring resources into new ways to gain access to protected information, exfiltrate sensitive data and infect systems with malware or ransomware that can bring an organization to its knees.

This paper looks at the evolution of first-generation software-defined wide-area networks (SD-WANs) and what to consider when evaluating next-generation offerings to address the future of secure networks.

SD-WAN Challenges

SD-WANs have come a long way since their introduction at the beginning of the 21st century. As such, two classes of users now face the need to upgrade. The first is early SD-WAN adopters that have recognized a positive impact but are now suffering the challenges of first-generation products. The second is the many large organizations that still have not made the leap into an SD-WAN environment and continue to rely on more static traditional WAN models.

Over time, these organizations have "Frankensteined" their network security. It is fairly common to use multiple tunnels and virtual private networks (VPNs) and rely on a host of point solutions for each component of security to address each emergent threat. This often leaves IT and the network operations center (NOC) with multiple panes of glass as they try to manage security for LAN, WAN and cloud workloads. And because security is often bolted on as an afterthought to network design, the result is poor application performance and a deprecated user experience. Worse yet, organizations are still experiencing a growing number of breaches and malware attacks that can bring their business—or an entire economy—to a standstill.

Network Routing Must Evolve

Most existing routing protocols and methodologies are based on decades-old technology, and the drawbacks grow more apparent every day. For example:

- Legacy hub-and-spoke designs cannot accommodate new dynamic workflows and the myriad data flows that proliferate, all driven by SaaS and cloud applications.
- Network architects struggle to deliver application-centric service-level agreements (SLAs) that meet user demands.
- Many enterprises must juggle a hodgepodge of special-purpose devices and security products including routers, firewalls, IPS devices, VPN appliances and more—creating another layer of operational and logistical challenges.

It is increasingly clear that legacy SD-WANs have become inefficient and expensive.

It is increasingly clear that legacy SD-WANs have become inefficient and expensive. Although they do help alleviate some manageability problems, they are limited by a lack of service assurance for individual data flows, a lack of visibility into network sessions and application data, and the high overhead that VPN tunneling such as IPsec demands, chewing up valuable bandwidth.

Although routing must change from the ground up, enterprises shudder at the thought of performing a forklift upgrade, discarding everything in place to adopt next-gen SD-WAN benefits.

The Risks of Inaction Are Many

Ever-changing business demands put increasing pressure on IT every day. Challenges include:

- Digital transformation initiatives, which continue to increase the number of users and amount of data on the network
- The growing number of devices being used to access enterprise resources and cloud applications, expanding the organization's attack surface
- The technology skills gap, which puts more pressure on existing teams to do more with less

These increasing demands span every industry, and the hard reality is that if the network cannot keep up, the customer experience suffers—or fails. WANs are no longer about connectivity and sending packets; the WAN determines who is having the right experience, wherever they are and whichever device they are using.

If the network cannot self-heal, or at least self-diagnose, IT and the NOC will be forever delegated to swivel-chair management and finger-pointing when problems—or breaches—occur.

The bottom line is clear: An outmoded legacy WAN can put an organization at a competitive disadvantage.

Next-Gen SD-WAN: What the Enterprise Wants

The path to solving these challenges includes adoption of next-generation SD-WAN solutions, which eliminates much of the legacy point product sprawl and offers the scalability and flexibility that even the largest enterprises demand.

Here are five key factors to consider—and features to demand—when choosing a next-gen SD-WAN:

1. Session-based architecture: This creates a smart routing fabric based on each session's unique needs, providing greater visibility into both user experience and network performance.
2. Zero trust networking: It is time for every enterprise to shift from "trust everyone" to "trust nothing."
3. AIOps: The ability to automate and orchestrate the network helps organizations solve issues before they impact operations or lead to data loss.
4. Tunnel-free networking: This eliminates VPNs and IPsec-based tunnels that chew up resources.
5. Secure access service edge: SASE-based criteria helps ensure the highest levels of performance and security for an increasingly mobile workforce, including centralized, simple security policies and management and role-based access.

Fortunately, organizations can realize all of these capabilities and more with Juniper's Session Smart™ SD-WAN.

The Session Smart™ Difference

Why Session Smart™? Ensuring the best possible user experience on the network is critical to any business's success. A Session Smart™ network is the only one capable of providing the advanced combination of intelligence, visibility and simplicity necessary to meet the stringent network performance and security requirements for today and tomorrow. Session Smart™ networks are user-based and convey context, offering fine-grained control over security and performance SLAs.

Completely based on a zero trust model to ensure the highest levels of security, Session Smart™ networks utilize Secure Vector Routing (SVR), an innovation that delivers what administrators have come to expect from an IPsec tunnel but without packet overhead and other drawbacks. So, while reducing network congestion and improving bandwidth, it also offers administrators better visibility into every traffic flow and allows monitoring of end-to-end quality for every connection. Security and performance are further enhanced by adaptive encryption, a smarter way to ensure security while boosting user experience. After all, since 90% of all traffic is already encrypted, why encrypt twice?

Because these innovations ensure high-quality user experiences and meet global compliance standards, customers looking for an SD-WAN solution that meets SASE criteria should look no further. (SASE is a modern cybersecurity architecture focused on bringing security services closer to users and granting them the appropriate level of access based on their risk level at that moment.)

Session Smart™ SD-WAN is entirely software-based and works in conjunction with what customers already have in place, so the enterprise can enjoy a nondisruptive transition without the need for a forklift upgrade. A session- and software-based approach also helps reduce complexity at the edge by halting the proliferation of middleboxes such as load balancers, routers, DDoS protection and more. Instead, these capabilities are collapsed into a single Session Smart™ Router and run as part of the SD-WAN on any industry-standard hardware platform, helping to guarantee performance whether it is deployed on a virtual machine or white box server, or in the cloud running on Azure or Amazon Web Services.

In many cases, a Session Smart™ Router at the edge—with Layer 3 and 4 firewalling capability and zero trust baked in—is more than sufficient from a security standpoint, reducing the need for costly and potentially performance-zapping next-gen firewall boxes at every branch.

Session Smart™ SD-WAN delivers the following:

- A 50% improvement in bandwidth utilization on average
- Ability to massively scale, to 10,000-plus sites
- Layer 3 and 4 firewall functionality, including packet filtering, IDP/IPS, DoS protection, DPI, URL filtering and more
- A zero trust, deny-by-default model
- Ability to constantly monitor pathways for the best available routes to ensure an optimal user experience
- Ability to detect and understand the users and applications on the network and intelligently route sessions in accordance to easily configurable performance and security SLAs
- Elimination of the tromboning or hairpin effect caused by sending all traffic to the data center, which can throttle performance and degrade the user experience

IPsec and VPNs cannot scale indefinitely and often fail as demand grows. Session Smart™ SD-WAN is a cost-effective, simple approach to scale networks and security for even the largest enterprises, with a tunnel-free architecture that is not limited in size or scope across LAN, WAN, cloud and IoT.

Customizable service levels allow IT teams to instantly understand the WAN's impact on the end-user experience.

Experience Is the New Uptime

With the introduction of Session Smart™ SD-WAN into a growing and comprehensive portfolio, including recent acquisitions of 128 Technology, Apstra and Netrounds, Juniper's vision for a complete, end-to-end and client-to-cloud vision is a reality. The strategy is clear: Experience is the new uptime.

The rich telemetry data that is gathered at the user and application level by the Session Smart™ Router is fed to Mist WAN Assurance and Marvis, an AI-based virtual network assistant. This gives IT teams insights and the ability to deliver proactive problem resolution. Customizable service levels allow IT teams to instantly understand the WAN's impact on the end-user experience. And ultimately, the Mist AI and Marvis correlate across wireless, wired and WAN network segments to drive a single, uninterrupted and optimized experience throughout the enterprise, for both users and operators.

Next Steps

The Juniper Session Smart™ Router fuels an advanced, service-centric networking solution that takes software-defined routing to a new level. Ideal for today's digital businesses, the Session Smart™ Router enables agile, secure, resilient WAN connectivity with breakthrough economics and simplicity. To learn more, visit: https://www.juniper.net

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

This content was commissioned by Juniper Networks and produced by TechTarget Inc.