EMPOWER REMOTE WORKERS WITH TUNNEL-FREE SESSION SMART SD-WAN

Remote work is not only increasingly common, it's grown essential to enterprises during times of crisis

Challenge

Traditionally, VPN solutions are based on IPsec or SSL tunneling. These technologies are complex and difficult to scale, as they are based on a rigid model that makes remote work challenging.

Solution

Session Smart SD-WAN creates a service-centric fabric that enables a "work from anywhere" architecture ideally suited to deliver agility, security, and a quality remote user experience.

Benefits

- Improved user experience and network performance
- Reduced security risks while maintaining compliance
- Rich, fine-grained service and network visibility
- Simplified service-centric and tunnel-free architecture

The COVID-19 pandemic has made companies acutely aware of their shortcomings when it comes to providing flexible, secure, and productive work from home (WFH) environments. This is especially true when it comes to VPNs, which are integral to working from home—or anywhere outside of the office. The demand for highly distributed and secure network solutions that can deliver the quality, reliability, and agility that is needed to support remote workforces, have never been more apparent. Juniper® Session Smart™ SD-WAN delivers a zero trust fabric that provides unparalleled control and access to the critical resources that remote workers need—with routing that seamlessly adapts to application performance and traffic requirements.

The Challenge

Given the increased demand for remote working setups, the availability and security of VPN services are now the focus of enterprise IT departments across the globe. VPNs typically route all traffic through a tunnel to the company network for security reasons. This includes secure public Software as a Service (SaaS) applications (e.g., Microsoft Teams, Salesforce, and Google Suites), standard Internet access, and services hosted on customer premises.

Traditionally, VPN solutions are based on IPsec or SSL tunneling technology. These types of VPNs are complex and difficult to scale, and they do not allow for application control or visibility. As businesses embrace the cloud, the Internet of Things (IoT) expands, users go mobile, and applications require more responsiveness, the rigid routing model provided by these tunneling technologies makes enabling remote work quite challenging. That's why many enterprises are frustrated by high VPN/WAN costs and are seeking to refresh these services. By transforming their networks at the same time, businesses can maximize the investments they're making in the WAN.
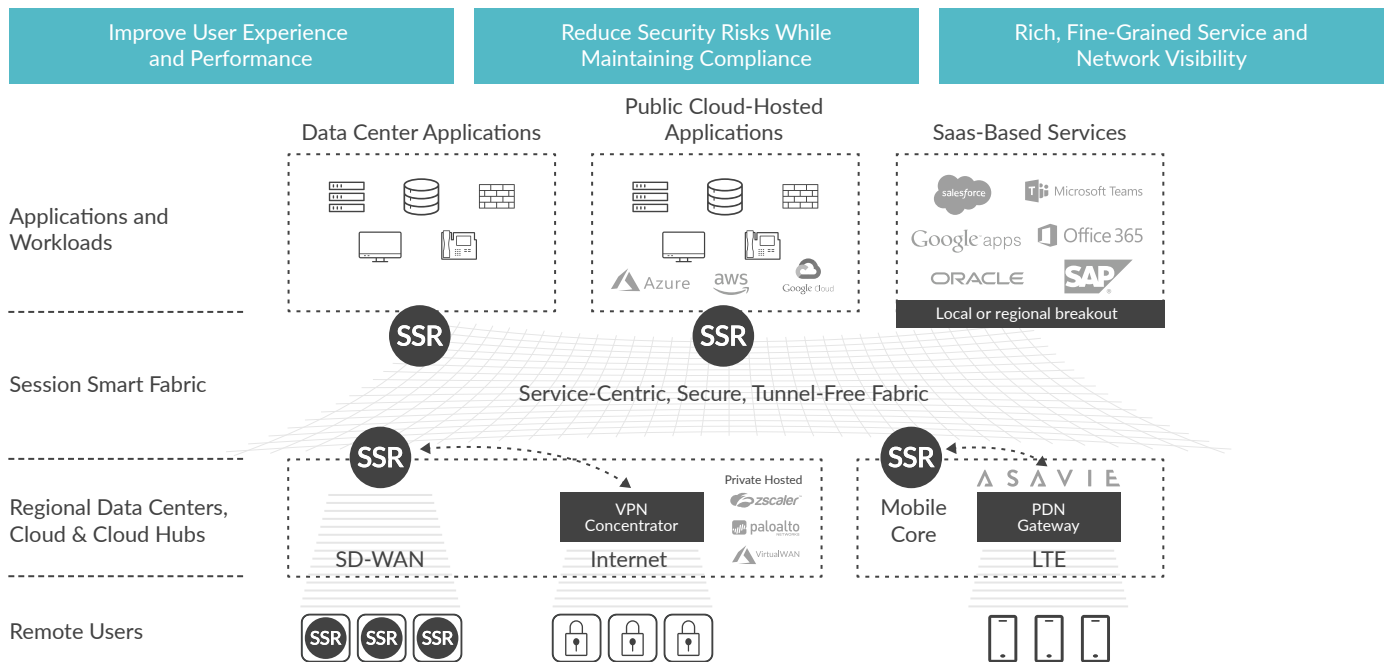
Improve User Experience and Performance	Reduce Security Risks While Maintaining Compliance	Rich, Fine-Grained Service and Network Visibility

Figure 1: Session Smart SD-WAN for remote users

The Juniper Session Smart SD-WAN Solution

Never before has networking been so critical to our lives and our livelihoods; indeed, the demand for highly distributed and secure network solutions has never been greater. The service-centric fabric of the Juniper Session Smart SD-WAN solution simplifies the "work from anywhere" architecture that is uniquely able to deliver agility, security, and a quality user experience.

As a key part of the solution, the Juniper Session Smart Router dynamically adapts to application performance needs and routes traffic accordingly. This tunnel-free approach reduces application latency while increasing available bandwidth for video and other network-intensive applications. Native session optimization can be used to improve application speed and reliability, as well as quality, security, and compliance.

Today's highly distributed "work from anywhere" world challenges the legacy perimeter-based security approach, demanding that security be baked into networks. Session Smart SD-WAN delivers a zero trust fabric that provides unparalleled control of access to the critical resources and data that workers need—with the routing that delivers it to the right place at the right time.

The Session Smart Router Advantage

The Juniper Session Smart Router eliminates the need for inefficient VPN tunnels and brings contextual awareness to the network by associating transient sessions with the applications and services they enable. This technology simplifies how enterprises support the needs of a remote workforce by providing centralized management, granular control, individualized flows, and integrated functions—all with infused security and dynamic traffic management. The intelligent features built into the Session Smart SD-WAN solution help enterprises deliver unsurpassed quality, reliability, and scale to the applications and services that help businesses thrive—even under heavy usage from remote workers.
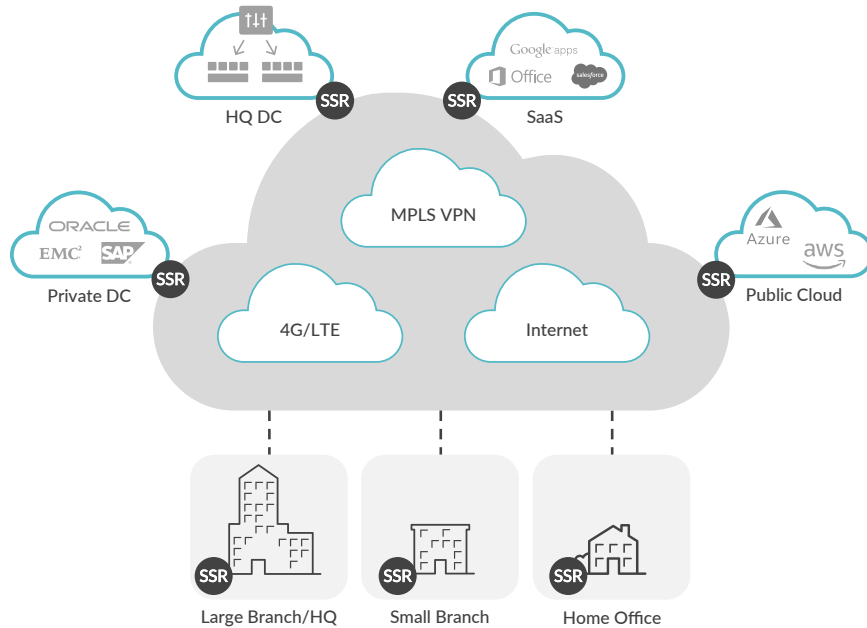
Figure 2: Session Smart SD-WAN, tunnel-free connectivity

Not only does the Session Smart SD-WAN solution eliminate the need for overlays and tunnels, it also centralizes services, tenancy, and policy information. This removes the need for automation tools, minimizes complexity, improves visibility, and maximizes savings. Additionally, this context-aware approach can better support the needs of businesses and help fuel success, especially as unexpected challenges arise and the ability to support remote workers becomes critical.

Figure 3: Session Smart SD-WAN is context-aware

Features and Benefits

Application-Aware Routing

IT departments can improve how their networks perform by providing application-aware routing. For example, the Session Smart Router recognizes applications like Microsoft Office 365, Google Suites, and other SaaS services and directly offloads that traffic to the WAN. Only applications hosted by the enterprise are routed to the data center. Additionally, dynamic session and application awareness provide load balancing and traffic steering based on session policies and the status of the network— features that become critical when hundreds of employees are suddenly working offsite.

FIPS 140-2 Certification

The U.S. government computer security standard, FIPS-140-2, is used to approve cryptographic modules and maintain confidentiality. Session Smart SD-WAN meets this certification and allows enterprises to build a network that is compliant with payment card industry (PCI) and Health Insurance Portability and Accountability Act (HIPAA) requirements. In addition, the Session Smart Router is ICSA Labs Network Firewall Certified and has achieved PCI attestation. Businesses can feel safe knowing that no matter where employees are based, their networks—and their data—are secure.

| ICSA Coporate Network Firewall | ICSA Labs PCI attested | FIPS 140-2 Certified | Future: CSFC/NIAP Cert |

Figure 4: FIPS-140-2 and ICSA Labs Network Firewall Certified

Zero Trust Security

Session Smart SD-WAN allows enterprises to build a network based on zero trust security, ensuring that each flow is encrypted and authenticated based on associated security policies. This enables enterprise leaders to remain confident in the knowledge that even with employees working from home, they can safely offer microsegmented connections or individualized VPNs to different lines of business within a large organization.
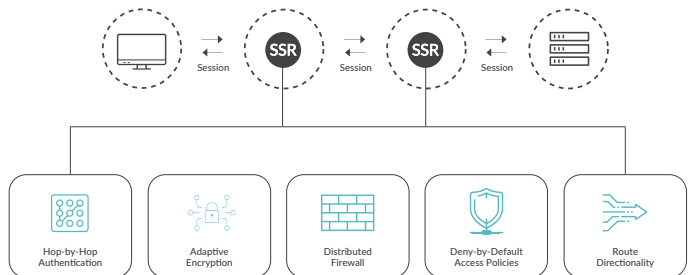

Figure 5: Capabilities of the Session Smart SD-WAN solution

Enhanced Visibility

The Juniper Session Smart Conductor provides centralized orchestration, administration, zero-touch provisioning, monitoring, and analytics for distributed Session Smart Routers. These tools provide a unified view of the entire network and enhanced session statistics, which becomes increasingly important in WFH environments. With them, administrators can generate customized charts based on selected key performance indicators (KPIs) and detailed reports on security and traffic events. This allows enterprises to detect and prevent network attacks, even across a dispersed workforce, while satisfying enterprise compliance requirements.

Session Smart SD-WAN Use Cases
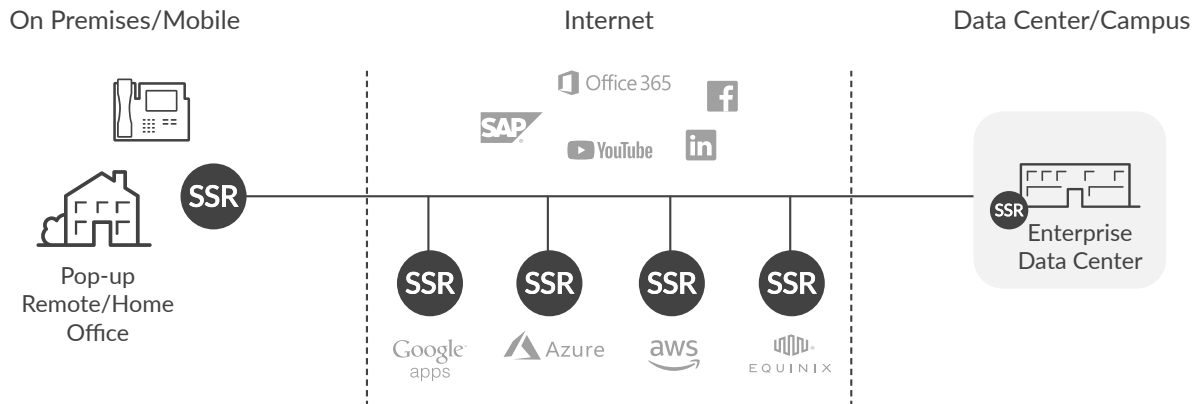
Session Smart SD-WAN at Home

Figure 6. Session Smart SD-WAN at home

Customer Benefits

User Experience	Security and Compliance	Visibility
• Simple connection to appliance	• FIPS 140-2	• Per session auditing
• Low latency and high throughput	• Inside-out connectivity	• Tenant and service performance
• Zero-touch provisioning	• Microsegmented access	• Fully distributed analytics

In this use case, one Session Smart Router is deployed at home, and another is deployed in the data center or the cloud. Applications are then intelligently routed based on their destination. For example, while SaaS applications will be offloaded directly to the WAN, enterprise applications requiring advanced unified threat management (UTM) treatment can be routed to the enterprise data center.
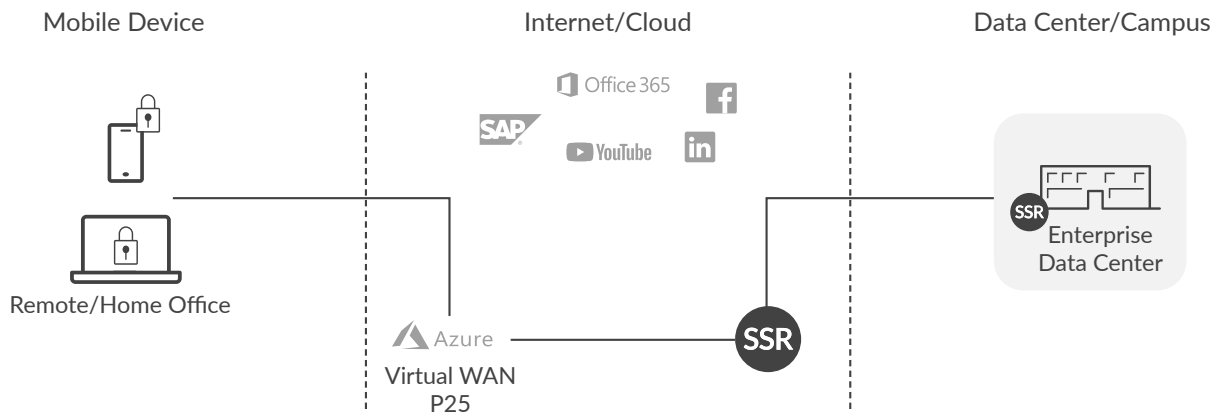
Session Smart SD-WAN in the Cloud

Figure 7: Session Smart SD-WAN in the cloud

Customer Benefits

User Experience	Security and Compliance	Visibility
• VPN client experience (portal/login)	• FIPS 140-2	• Per session auditing
• Cloud-based scaling	• Inside-out connectivity	• Tenant and service performance
• Seamless connectivity	• Microsegmented access	• Fully distributed analytics

In this use case, a remote employee connects to the cloud VPN gateway using standard technology, which then hands over traffic to the Session Smart Router to intelligently route packets to the right destination. The Session Smart Router can differentiate between RFC1918 networks, which are routed to the company network, and all other traffic, including cloud services, which are either routed directly to the services or through a UTM solution.

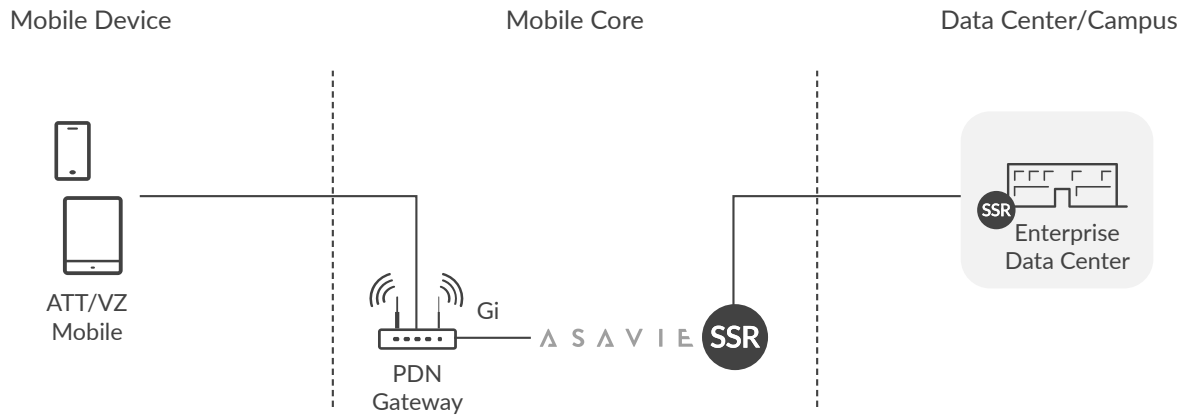## Session Smart SD-WAN in the Data Center with Private LTE Access

Figure 8: Session Smart SD-WAN in the data center with private LTE access

Customer Benefits

User Experience	Security and Compliance	Visibility
• Client-based experience (portal/login)	• FIPS 140-2	• Per session auditing
• Cloud-based scaling	• Inside-out connectivity	• Tenant and service performance
• Seamless connectivity	• Microsegmented access	• Fully distributed analytics

This use case benefits from a partnership with Asavie, which provides end-to-end secure private LTE connections to facilitate work from home connections. The Session Smart SD-WAN is deployed in the LTE core and the enterprise data center, providing network security, network access control, application-aware routing, and compliance.
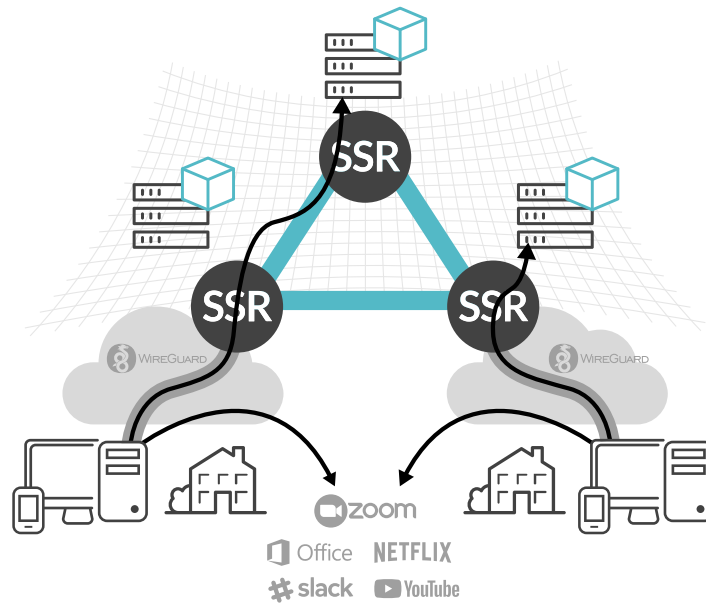
Session Smart SD-WAN with Wireguard

Figure 9: Session Smart SD-WAN with Wireguard

Customer Benefits

User Experience	Security and Compliance	Visibility
• Zero-touch experience (Wi-Fi join)	• FIPS 140-2	• Per session auditing
• Cloud-based scaling	• Inside-out connectivity	• Tenant and service performance
• Zero-touch provisioning	• Microsegmented access	• Fully distributed analytics

In this final deployment scenario, corporate devices designed to work outside the office are set up with a lightweight Wireguard—a free and open-source VPN solution—which peers with one (or many) Session Smart routers in the corporate topology. It selectively and intelligently sends secure sessions to the Session Smart Router peers where services can be accessed, and offloads secure SaaS and consumer services directly to broadband. Wireguard, combined with the Session Smart Router, extends the corporate network access edge to users displaced from the office.

Summary—Session Smart SD-WAN Sets Remote Workers Up for Success

The Juniper Session Smart SD-WAN solution provides centralized control, simplified deployment of context-aware networks, intelligent service routing with in-band signaling, fine-grained microsegmentation, and infused security based on a zero trust model. This mix of features and capabilities goes above and beyond traditional router offerings by solving several underlying network issues that would otherwise inhibit WFH success.

The result is a context-aware network that can easily, dynamically, and securely stretch across boundaries, enabling organizations to build application-friendly infrastructures that are flexible enough to cope with the demands of a dispersed workforce.

Next Steps

To learn how Session Smart SD-WAN can help your organization empower remote workers, please contact your Juniper account manager or visit 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