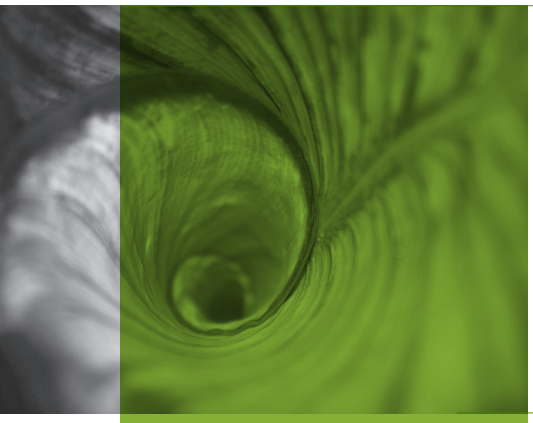

SESSION SMART™ SD-WAN—BUILDING NETWORKS WITH SECURITY AT THEIR CORE

Protect infrastructure, intellectual property, and confidential information with the innovative Session Smart™ Router

Challenge

Despite myriad defense strategies, cyber attacks continue to proliferate. Traditional security techniques aren't enough to protect today's network, and this puts enterprises at risk.

Solution

The Session Smart SD-WAN Solution, powered by the Session Smart Router, provides native Zero Trust Security, leverages hypersegmentation, and integrates multiple middlebox functionalities on a single platform. This simplifies network architecture, protects information assets, and minimizes costs.

Benefits

- *FIPS 140-2 compliant*
- *AES256 encryption and HMAC-SHA256 per packet authentication*
- *Layer 3/Layer 4 DOS/DDOS*
- *Traffic engineering and URL filtering support*
- *ICSA corporate firewall and PCI certification*

Cyber attacks continue to increase in size and frequency. Traditional security techniques aren't enough to protect the network, and this puts intellectual property and confidential information at risk.

The innovative Juniper® Session Smart SD-WAN solution weaves routing and network security together into one platform. With security in its DNA, every aspect of this solution was purpose-built to protect the information, applications, and services that cross the network and ultimately fuel the business.

The Challenge

Despite the proliferation of various techniques to secure, restrict, or segment the network, the number of security breaches, denial-of-service (DoS) events, and other cyber attacks continues to rise. Cybersecurity Ventures predicts that cyber crime costs will reach $10.5 trillion USD annually by 2025[1]. With built-in security that spans the entire network fabric, the Juniper Session Smart SD-WAN solution was specifically designed to reduce the exposure of networked traffic to this growing threat.

The Juniper Session Smart SD-WAN Solution

The Session Smart SD-WAN Solution combines a service-centric control plane, and a session-aware data plane to offer IP routing, feature-rich policy management, improved visibility, and proactive analytics. Unlike solutions that graft security onto an insecure network, our approach embraces the Forrester and NISTS Zero Trust Model. The advanced design of the Session Smart Router replaces the traditional routing plane with one built from the ground up with security principles at its core.

[1]"Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybersecurity Ventures Official Annual Cybercrime Report.

Service-Centric, Tenant-Based Security Architecture

The Juniper Session Smart Router understand sessions—dedicated links between services on the network, and the applications and users that rely on them—to perform vital business operations. The traffic crossing a Session Smart Router is processed, routed, and controlled in a service-centric manner. Services can be made to model a given application, reachable at a given address, set of addresses, or subnets.

Access to these sessions is granted based on tenancy, which groups services together based on shared policies. As sessions are processed through the Session Smart Router, the tenant becomes an important construct for route determination, segmentation, classification, policy, and many other core routing principles.

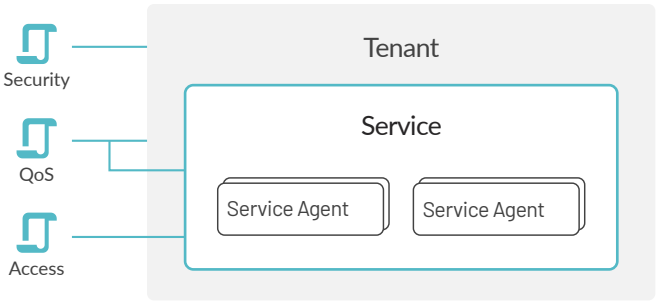

Figure 1: Access to network services is based on Tenancy

With this added layer of intelligence, this solution provides the unique capability to assign security policy, quality-of-service (QoS) parameters, and access control policies on a per service, per tenant basis. This capability makes it possible to have unique encryption and authentication keys, custom traffic engineering parameters, and tight access control at the individual session level. It also offers a flexible way to segment and isolate traffic, enabling administrators to apply different profiles based on the application or service that the session contains.

Zero Trust Security

Forrester's Zero Trust Model of information security revolves around the "never trust, always verify" principle. With Zero Trust security, there is no automatic trust for any entity—including users, devices, applications, and packets—regardless of what it is and its location on, or relative to, the network. Similarly, The National Institute of Standards and Technology (NIST) SP 800-207 Publication, Zero Trust Architecture (ZTA), defines a ZTA as a network that does not implicitly trust users, assets or resources based solely on their physical or network location. In a world of on-the-go employees and on-demand services, the Zero Trust Model is intended to shrink trust zones, reduce attack surfaces, and restrict lateral movement if a resource is compromised.

With inherent network virtualization and infused security functions, the Session Smart SD-WAN solution can create zero trust security boundaries that compartmentalize different areas of the network. In doing so, businesses can protect sensitive information from unauthorized applications or users, minimize the exposure of vulnerable systems, and prevent the lateral movement of malware throughout the network.

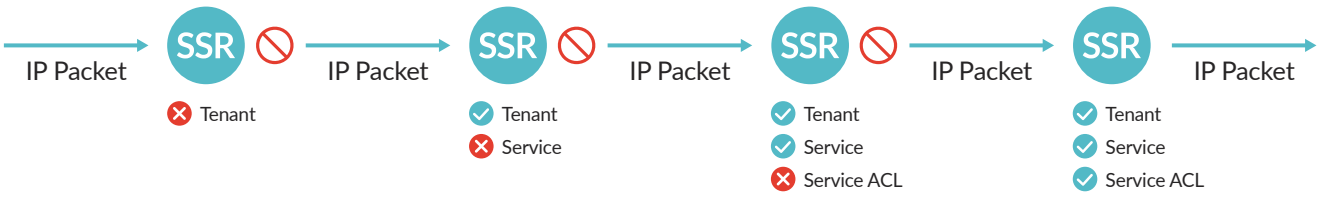

Figure 2: Deny-by-default policy

Unlike a traditional SD-WAN solution, which follows an "allow-by-default" policy, the Session Smart SD-WAN solution follows the principle of "deny-by-default," which uses a series of checkpoints to validate legitimate network traffic.

- When a packet hits a Session Smart Router, the first check is to verify whether the packet belongs to a tenant.
- If the packet does not belong to a tenant, the packet will be dropped.
- When the packet belongs to a tenant, the next check is to verify whether it is destined to a service which the tenant is allowed to access.
- If the destination of the packet does not correspond to any service within the tenant, the packet will be dropped.
- When the destination of the packet belongs to a service, the router examines the context-specific access control list (ACL) to determine whether the source of the packet is allowed access to the service.
- If the source is denied access to the service, the packet will be dropped.
- Once the packet passes the preceding checks, the packet will be forwarded to the next hop toward the destination.

Unless an enterprise explicitly allows a session to cross the network, the Session Smart Router will drop all packets belonging to a session that does not clear the series of checkpoints. While performing the series of checks for every packet, the Session Smart Router maintains the rate of traffic speed to match the line rate.

Next-Generation Firewall Capabilities

The Session Smart Router natively supports network firewall functionality. However, whenever a service requires next-generation firewall (NGFW) treatment, the Session Smart Router can be used along with Juniper SRX to achieve this.

In this model, when a particular service in a branch requires a NGFW treatment, the Session Smart Router in the branch will route the packet to the Session Smart Router in the Data Center or the in the Cloud. The Session Smart Router in the Data Center/Cloud can be service function chained (SFC) with an SRX, which will provide the required NGFW treatment for the service.

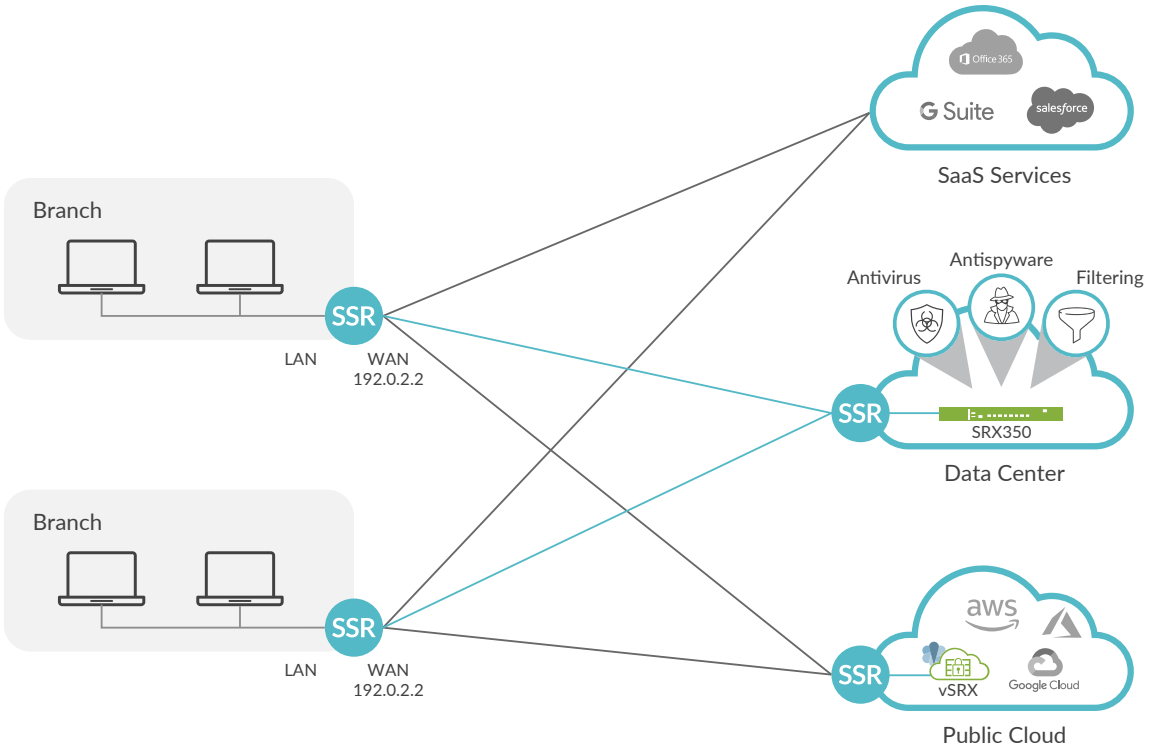

Figure 3: For NGFW treatment, the Session Smart Router can be used with the Juniper SRX.

Features and Benefits

- Service-centric, tenant-based security architecture: enables the Session Smart Router to understand sessions and perform vital business operations.
- Zero trust security: The Session Smart Router follows the principle of "deny-by-default," which uses a series of checkpoints to validate legitimate network traffic.
- Next-generation firewall capabilities: The Session Smart Router provides network firewall functionality and can be service function chained with the Juniper SRX for next-generation firewall capabilities.
- Security at its core: The advanced design of the Session Smart Router replaces the traditional routing plane with one built from the ground up with security principles at its core.

Session Smart Router Next-Generation Firewall Capability Metrics

● Supported ● Planned ● Service Function Chain

	Session Smart Router	NGFW (SRX)
Layer 3/Layer 4 DOS/DDOS	●	●
Layer 3/Layer 4 Intrusion Detection Service (IDS)/Intrusion Prevention System (IPS)	●	●
URL Filtering	●	●
Traffic Engineering	●	●
High Availability	●	●
Context-Aware	●	●
Network Policy Management Tool	●	●
IPv4/IPv6 Support	●	●
NAT44, NAT46, NAT64, and NAT66	●	●
Site-to-Site VPN	●	●
Autodiscovery (AD), Lightweight Directory Access Protocol (LDAP), and Dynamic Host Configuration Protocol (DHCP)7 Support	●	●
Support for Virtualized Environment	●	●

	Session Smart Router	NGFW
Application Fingerprinting with Cert/SNI	●	●
SSL VPN Support	●	●
Basic Support for HTTP/HTTPS Proxy	●	●
Routing Protocols	●	
Service-Centric Network Architecture	●	
Secure Vector Routing	●	
Zero Touch Security and Hypersegmentation	●	
SD-WAN Capabilities	●	
Context-Specific ACL	●	
Cloud-Hosted Security	●	●
Inspect Encrypted Traffic	●	●
Layer 5/Layer 7 Content Filtering	●	●
Layer 5/Layer 7 IDS/IPS	●	●
Network Antivirus and Anti-spyware	●	●

Summary—Zero Trust Security at the Network Core

The Session Smart SD-WAN approach to zero trust security allows the network to be built around the services it's meant to deliver, addressing the cyber threats that target today's hyper-connected environments. With native security controls that replace obsolete perimeter-based solutions, and integrated features that would otherwise require an array of middleboxes, Session Smart SD-WAN helps enterprises protect the assets that are critical to their success.

Next Steps

To find out more about the Juniper Session Smart Routing solution, please contact your Juniper account representative and go to 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