Juniper Networks | Driven by Experience™

SESSION SMART NETWORKING – HOW IT WORKS

The service-centric routing fabric for AI-Driven SD-WAN

White Paper

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This technical white paper provides a detailed explanation of how Juniper® Session Smart™ Networking and Juniper Session Smart Routers work. It details the application-centric architecture and the session-aware data plane. Session Smart Networking offers dramatic benefits over other enterprise WAN solutions in terms of simplicity, agility, security, performance, and cost.

The SSR Series Router is the routing engine for the AI-Driven SD-WAN, which is cited with feature descriptions and resources for more information, but is otherwise beyond the scope of this document.

Introduction

Networks exist to deliver applications and services that businesses need. Most legacy networks include middleboxes to forward packets with policies that the stateless routed network cannot understand. Examples include firewalls, load balancing, deep packet inspection, and tunnels. This approach leads to excessive complexity at too high a cost. It also makes it difficult to run new applications across diverse networks and within cloud environments.

This presents a challenge when supporting video-intensive workloads, for example, or connecting a mobile workforce with its needed services and applications. The sheer complexity exposes the business to increasingly sophisticated cyberattacks and the unacceptably high cost of downtime.

The applications running on your network connect clients to services using the language of sessions. They understand all of the participants, policies, and other resources that may communicate in predetermined ways. Most legacy networks don't operate that way.

Failure to understand the language of sessions is the root cause of much that's nonoptimal in networking today. Session Smart Routers provide session-level intelligence to the network. When deployed as an SD-WAN solution, Session Smart Networking enables a closer working relationship between the network and the applications it needs to support.

Session Smart Routers, which are software based and run on either certified white box (see the Session Smart Routing datasheet) or purpose-built hardware, understand the source user and network segment, destination application, and directionality of flows, along with the requirements of named applications, service topology, and business policies. Session Smart Routers use this information to plot waypoints (IP addresses along the routing path) through the network in real time; this allows them to better support the businesses they serve.

With Session Smart Networking, the network itself becomes an application-centric fabric that is simpler, more agile, and secure for both enterprises and service providers to operate. With Session Smart Networking, Juniper provides a session-aware and high-performance SD-WAN that enables a "zero trust" security model. This results in better performance at a lower cost for any-sized enterprise in any industry.

Secure Vector Routing

Juniper has developed a revolutionary routing standard called Secure Vector Routing (SVR). SVR enables a service-centric fabric with dramatic benefits in terms of simplicity, agility, security, scalability, performance, and cost.

Since networks exist to connect users to applications, network design should start with those applications at the core. SVR enables the network to differentiate the way it delivers applications.

SVR replaces tunnel-based network overlays and inefficient provisioning systems with application-centric control, simple intelligent application-based routing, and in-band (data plane) session-based signaling (Figure 1). SVR is fully compatible and interoperable with existing network protocols and architectures, allowing it to be gradually introduced into an existing IP network without affecting network endpoints or hosts.

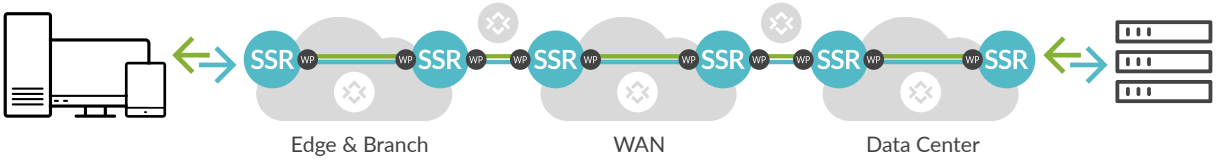

Figure 1. SVR is service-centric with a session-aware data plane.

Application Centricity

The Session Smart Router's control plane is centered on delivering applications and services. Applications are the heart of the SVR design. SVR provides the language for describing the network's services and applications, user groups and devices, and associated policies—everywhere on the network.

Applications are exposed via Representational State Transfer (REST) APIs to deliver a full suite of application and orchestration integration services.

Session-Aware Data Plane

The session-aware data plane makes dynamic forwarding and policy decisions based on SVR's application-centric control plane, the unique attributes and policies of sessions, and real-time network monitoring. SVR-based routers, deployed at network edges, transform a stateless L2 fabric or L3 network data plane into one that is fully session-aware. This is made possible through a combination of three features:

- Session detection and control,
- Waypoint setting (IP addresses of other SSRs in the routing path), and
- Session-based signaling (via metadata).

A session-aware data plane creates end-to-end route vectors that are:

- **Deterministic** – Session traffic is steered in segments between waypoints, with enforced flow symmetry, all without tunnel-based overlays.
- **Secure** – Each route vector controls the directionality of the session when it's initiated. Every session is authenticated at each hop. Payload encryption is defined per application and applied per session.
- **Dynamic** – Paths are established dynamically based on application policies and network state. Statically provisioned stateful tunnels are replaced with a model based on session state, where sessions are created on demand and terminated when no longer needed. Link and endpoint session load balancing is native.
- **Hypersegmented** – Hierarchical and secure segmentation is supported end-to-end across network and Network Address Translation (NAT) boundaries.

Session Detection and Control

Session detection and control includes the processes of classifying sessions and their state, along with assuring path symmetry, determining session directionality, and setting waypoint addresses.

Session Classification and State

SVR classifies each Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or other transport session based on the unique source, destination, and application characteristics of the session. Security, quality, routing, and session control policies are applied on a per-session basis to deliver deterministic routing end-to-end. Session state is dynamically established by each router based on service routes, policy, and the observed performance of the connections between each SVR-based router.

Assured Path Symmetry

SVR ensures that bidirectional sessions follow the same path. Traditional routers use a stateless per packet "hot potato" forwarding approach with no notion of session or state. With SVR, all packets associated with a session are routed along the same path, no matter which way they're traveling. This symmetric flow enables packets to be intelligently routed, sessions to be controlled, and traffic to be proactively analyzed. It also prevents unauthorized flows from using a given path.

Session Directionality

Session directionality forms the foundation of SVR's secure routing and segmentation model. It enables an SVR fabric to behave as a Layer3/Layer4 firewall. As every SVR route defines the direction of a session at initiation, each route becomes a secure vector that tightly controls access to the destination or service. In this way, SVR unifies access control and security policies during routing.

Waypoint Setting

SVR defines a location independent and segmented approach to routing and addressing based on waypoints, which are IP addresses configured on each Session Smart Router. Waypoints are used to govern sessions across network paths.

Waypoints are separate and distinct from the IP addresses and named services that identify end-to-end network sessions between devices and applications. Secure vector routes define the path (set of routers) that each session must follow within an SVR topology. Every Session Smart Router can be reached by one or more waypoints, and Bidirectional Forwarding Detection (BFD) is used to test connection and path attributes between the waypoints.

The waypoint-based routing with SVR is inherently segment based, meaning that end-to-end route vectors can be created based on multiple router (or waypoint) hops. Since each SVR router maintains an overall view of the topology and service-based policies, dynamic multisegment paths can be established. Ephemeral session state in each router along the path guarantees symmetric communications (Figure 2).

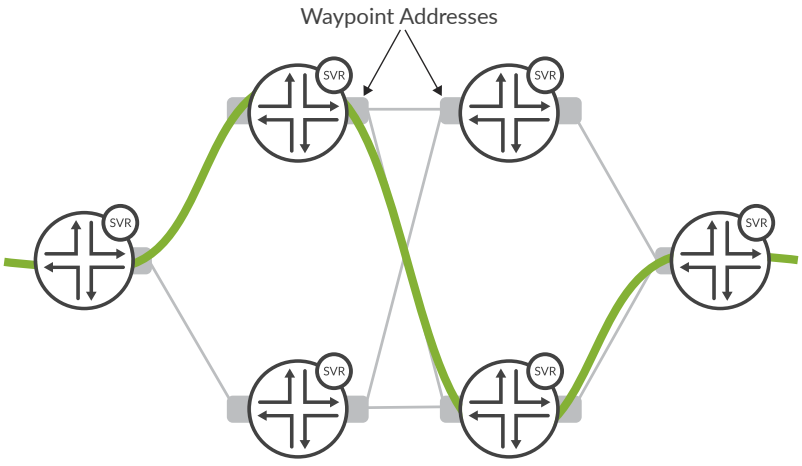

Figure 2. Waypoint addresses govern sessions across network paths.

To establish a symmetric flow, the ingress router performs NAT on the source and destination IP address of every waypoint hop and adds metadata to the first packet of each session (Figure 3). This metadata is used to signal information about a session, including original IP addresses, user, and policy information. The metadata is only included when the SVR router is aware that there is another Session Smart Router downstream. From there, all packets for that session follow the same path.

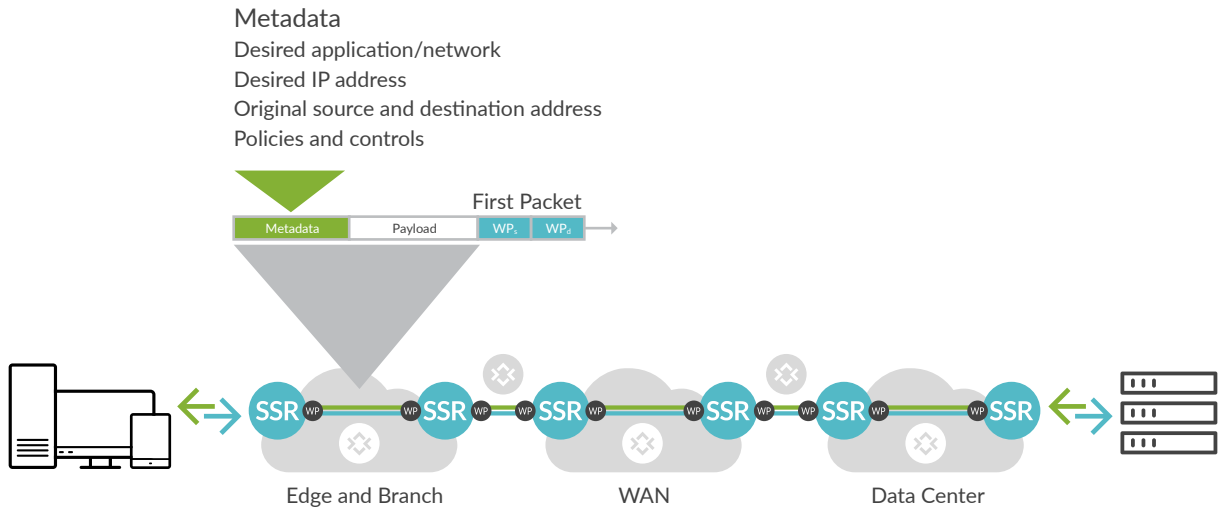

Figure 3. The Session Smart Router adds metadata to the first packet of each session to signal information about the session to another Session Smart Router.

Reverse metadata is included in the first packet on the return path for the same session. The metadata is only included in the initial packets sent between the two SVR routers. The exchange of metadata is always digitally signed to prevent tampering and can be optionally encrypted.

The forward metadata includes information about:

- The original source and destination IP addresses and ports
- The user associated with the request
- The desired class of service
- Other policy and control information

The reverse metadata includes utilization metrics and possible service class modification information.

Session-Based First Packet Processing

The first packet of each session establishes an end-to-end path across the network, defining waypoints based on the SVR routers it crosses along the way. It also initiates a single end-to-end session from ingress to egress router that is transient in nature. The remaining packets that are part of the session are sent along the same path without any form of tunnel overhead (Figure 4).

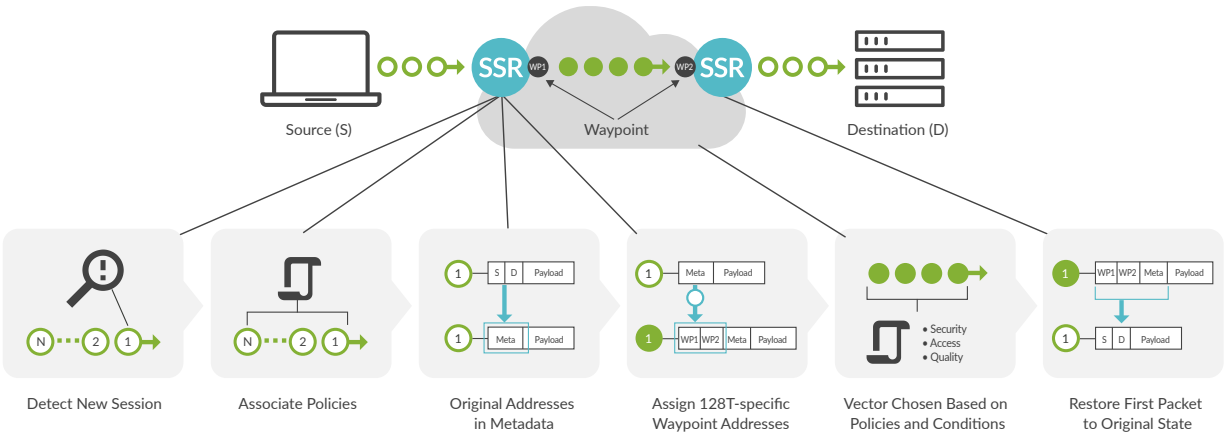

Figure 4. Secure Vector Routing: Session-based, First-Packet Processing

When the first packet corresponding to a new TCP, UDP, or other transport session arrives at a Session Smart Router, it determines the appropriate route corresponding to the session. If a route is found:

- The SVR-based router translates the source address of the packet to its own egress waypoint IP address. The destination address of the packet is translated to the waypoint address of the destination SVR-based router. This is necessary to enforce the return path to be symmetric.
- The SVR router adds metadata to the first packet.
- This metadata includes the original source and the destination addresses of the packet, along with other policy and control parameters. The metadata is then signed and optionally encrypted based on policy.
- The packet is then forwarded to the waypoint address of the next SVR router.
- At the last hop SVR-based router, once authenticated and authorized, the original packet contents are restored and forwarded to the final destination.
- Subsequent packets from the same session are automatically recognized and forwarded in the same way, but without first packet processing.
- Similar to the processing described previously, SVR adds metadata to the first reverse packet and follows the same path as the first forward packet so that complete path symmetry is established.

Metadata may also be used during an active session to communicate service changes or measure link quality. For more information, see the documentation on SSR Metadata.

The Session Smart Networking Solution

Juniper Session Smart Networking powers AI-Driven SD-WAN.

AI-Driven SD-WAN

AI-Driven SD-WAN is a centralized management platform for configuration, deployment, and monitoring of all cloud networking, including AI-driven automation and troubleshooting. Unifying the cloud networking experience in this solution is Mist™ AI, which provides the portal for management and orchestration. The platform is architected using microservices for advanced agility.

For more information on Juniper AI-Driven SD-WAN, see the previous links and the Resources section.

Note: Some organizations that support legacy environments or that may need to adhere to certain governmental guidelines may require an air-gapped on-premises solution. For those cases, the Session Smart Conductor is available.

Session Smart Routers

Session Smart Networking bridges the gap between networks and the applications they exist to deliver. It supports a range of deployment models scaling from a small branch office to a high-capacity edge router to a hyperscale software-defined data center.

The Session Smart Routers put session awareness and state where it belongs, in the router. Sessions are the language of applications and services. Nearly every use of a network involves a stateful exchange of information between endpoints.

Session state is not new to networking. It exists in most standalone network functions such as firewalls and load balancers. Putting session state in the router opens the door to integrating network functions natively into routing. SVR is the technology that enables the Session Smart Router to do that.

The Session Smart Router is a software-based router built around innovative Session Smart technology and SVR capabilities. Session Smart Routers enable enterprises and service providers to build application-centric fabrics that lead to new levels of simplicity, agility, security, performance, and savings.

100% Software-Based and Cloud Ready

Session Smart Routers are 100% software-based and support a range of deployment models—from remote branch offices to high-capacity network edges to hyperscale data centers and the cloud.

The Session Smart Networking software runs on certified partner white boxes or certified customer premises equipment (CPE), whether physical or virtual. It can also be run in virtualized hosted private clouds and in public clouds such as Amazon Web Services (AWS), Azure, or Google Cloud Platform for providing secure cloud on-ramps and other intracloud routing functions. For deployment in private clouds, the software works with leading cloud management platforms.

For installations ranging from small branch offices to large data centers, Juniper provides purpose-built hardware for Session Smart Networking with the SSR100 and SSR1000 Series Routers.

Application Visibility and Control

Application classification, visibility, and control are the key benefits to Session Smart Networking.

Application Classification

Session Smart Networking applies intelligent heuristics to classify thousands of applications from network traffic without decryption. It can identify traffic in all routers—not only at the edges. It can also share previously detected traffic information among other routers for quick detection. With multiple fast acting methods that can enable early detection, Session Smart Networking allows networks to offer top-of-the-line end-user experiences, protection, and reporting.

Application Visibility

Session Smart Networking provides fine-grained, session-based analytics and reporting, delivering maximum visibility into how applications and the network itself are performing. Application and network performance analytics are available via RESTful APIs, and detailed session telemetry is sent to the cloud.

For AI-Driven SD-WAN, considerable additional visibility is supported through Mist AI, which maintains a constant stateful inventory of key assets, users, devices, and applications. Juniper Mist WAN Assurance provides real-time insights into device, WAN link, and application health via Service Level Experiences (SLEs). SLEs provide the basis for Marvis® Virtual Network Assistant to provide streamlined AIOps including prescriptive actions for a self-driving network. Long term visibility is provided via Juniper Mist Premium Analytics.

Application Control

A Session Smart Router applies application-specific routing and policies across the network using a simple contextual data model that is based on named services and groups of users. Application-based policies including access, security, and quality of service (QoS) are all designed to guarantee that applications meet intended service-level agreements (SLAs) with the required degree of network security.

Quality of Service

Within Session Smart Networking, the QoS toolset offers several functions that bring best-in-class quality of experience to end-user applications. The toolset enables differentiated services based on a class model, along with features such as intelligent path selection, fast failover, prioritization, shaping, duplication, and error correction across the network.

Network Functions and Service Chaining

The Session Smart Router integrates multiple middlebox capabilities (security, routing, firewall, VPN, and load balancer) into a single routing platform. This simplifies the overall network architecture and minimizes the costs and deployment time for new network functions.

Network Stateful Firewall

The Session Smart Router natively delivers key stateful network firewall capabilities, including:

- Deny-by-default routing: SVR surpasses traditional network security with a zero trust deny-by-default routing model; this means that no session is permitted without explicit policies to allow it. Directional service routes and access control lists for multiple groups are one and the same.
- NAT: By default, the Session Smart Router will double NAT (NAT both the source and destination IP port) of the packet before sending the packet out of a public interface. Double NAT allows the system to hide information about the source and destination IP port of the flow, keeping the IP port information completely private to the enterprise. The Session Smart Router also supports source and destination NAT (NAT44, NAT46, NAT64) on a per-session basis.
- Encryption and VPN: Per-session encryption and per-packet authentication are supported between all instances of the Session Smart Router. Encryption is performed using AES256, and per-packet authentication is performed using HMAC-SHA256-128. Combined with hypersegmentation, the Session Smart Router delivers scalable multisite VPN.
- Adaptive encryption: While performing encryption of the application traffic, the session-oriented nature of the Session Smart Router can detect whether the traffic is already encrypted using TLS/HTTPS or by IPsec. If the application traffic is already encrypted, the router won't re-encrypt the packet, which eliminates the overhead associated with double encryption.
- PCI-DSS and HIPAA compliance: The Session Smart Router is session-based and provides true zero trust security (ZTS) and a hypersegmented network architecture, allowing organizations to meet PCI-DSS and HIPAA compliance requirements.
- FIPS 140-2 compliance: The SSR is FIPS 140-2 Level 1 certified.
- International Council of Securities Associations (ICSA) Labs: The Session Smart Router is ICSA labs network firewall certified.

Link and Server Load Balancing

Session Smart Networking uses optimized server heuristics and path monitoring to ensure that application traffic loads are optimally balanced across preferred links to desired application servers. Real-time criteria include server loads, maximum session rate, packet loss, latency, and jitter.

SASE Functionality with Secure Service Edge

In addition to natively supporting service functions, the Session Smart Router supports service function chaining with standalone third-party service functions like next-generation firewall, Secure Service Edge (SSE), and WAN optimizer. Both static and dynamic service function chaining capabilities are supported. Session Smart Networking can be deployed as part of a Network Functions Virtualization (NFV) solution either at the edge (virtual CPE) or in the data center.

Benefits of these features include the ability to provide full Secure Access Service Edge (SASE) functionality when pairing Juniper or third-party SSE with AI-Driven SD-WAN.

Interoperability with Existing Routing

The Session Smart Router is fully compatible and interoperable with existing network protocols and architectures. It uses traditional routing protocols such as BGP among many others to effectively communicate with existing routing elements, learn and distribute routes, and forward network traffic.

Application-Centric Fabric in SD-WAN

Enterprises and service providers deploy the Session Smart Router to create end-to-end application-centric fabrics seamlessly across any network infrastructure. These application-centric fabrics offer a single networking solution for multiple SD-WAN use cases including:

- Virtual edge routing, network as a service (NaaS), and WAN refresh
- Multicloud fabric and data center interconnect (DCI)
- Security in the form of zero trust networking at the branch and edge

Application-centric fabrics stretch to anywhere the Session Smart Router is deployed, whether it's at the branch, in the data center, within a collocation facility, or in the public cloud. SVR forms the network routing engine for application-centric fabrics, which are completely tunnel-free. In addition, they are natively service-aware, segmented to any degree necessary, and maintain a vast knowledge of service availability, topology, and policies.

The application-centric fabric is built from the ground up on the principles of zero trust networking. This means that network security is no longer painted onto the perimeter of the network but is rather baked into the network fabric itself. These application-centric fabrics are centrally managed and orchestrated with a single pane-of-glass (Mist AI) that enables AI-Driven SD-WAN (Figure 5) with full network visibility, strong analytics, automated policy provisioning, and zero touch deployments. Juniper application-centric fabrics are open and programmable through RESTful APIs.

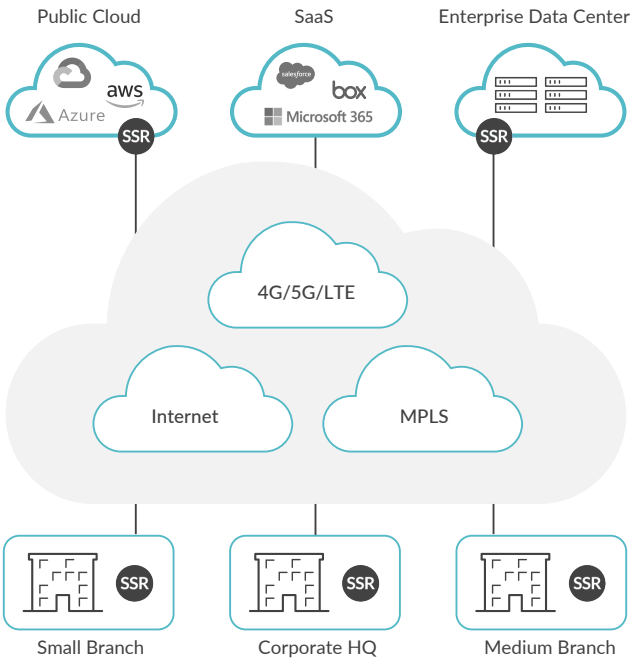

Figure 5. Juniper Session Smart Networking, a Service-Centric Fabric with AI-Driven SD-WAN

In addition to the application visibility and control discussed previously, enterprises and service providers can achieve the following benefits with the service-centric fabrics in AI-Driven SD-WAN:

- **Simplicity** – No tunnels, no overlays, no more hardware-centric networking
- **Agility** – Faster deployment, improved application resiliency, and better responsiveness
- **Security** – Zero trust model with deny-by-default routing plus authentication, encryption, and segmentation
- **Performance** – Less overhead, more scalability, and dynamic optimization
- **Savings** – Reduced bandwidth, connectivity costs, third-party point tools, CapEx, and OpEx

Multipath Routing and Failsafe Application Deliver

Multiple paths often exist between peers within large enterprise and service provider networks. These multiple paths can be used to reroute traffic in case of failures or link performance degradation. In AI-Driven SD-WAN, multiple paths or hybrid networks are deployed to dynamically offload traffic from expensive MPLS links to lower-cost broadband or LTE links, while maintaining strict SLAs.

The Session Smart Router provides application and policy-based multipath routing, intelligent path monitoring, and lossless application delivery capabilities. These capabilities combine to ensure that application traffic is optimized across multiple paths, while forming a failsafe delivery model that ensures application traffic is delivered despite failures.

Application and Policy-Based Multipath Routing – The Session Smart Router sends application traffic along the most optimal paths based on application-specific SLA policies and observed network performance (across MPLS and low-cost broadband or LTE connections).

Intelligent Path Monitoring – Link and path performance is monitored in real time using enhanced Bidirectional Forwarding Detection (BFD) and inline Flow Performance Monitoring (FPM) to determine jitter, latency, and loss for each path. The Session Smart Router also measures packet loss, jitter, and latency by coloring the data packets. If there is active data flow between Session Smart Routers, additional bytes are inserted in the data packet, on a periodic basis, to measure path SLA. Using BFD and FPM together provides more detailed metrics for optimizing different traffic types, such as voice and video.

Lossless Application Delivery – Sessions and bandwidth are optimized along the desired path or multiple paths. Key capabilities are:

- **Multipath Session Migration** – Instantly migrate existing sessions from primary to secondary paths in the event of network brownout conditions or failures.
- **Multipath Session Redundancy** – Mitigate quality problems due to excessive packet loss and duplicate packets, and send in separate redundant streams on multiple links.

Zero Trust Network Security

Zero trust security (ZTS), meaning no packets are above suspicion, is key to the Session Smart Networking approach. Juniper service-centric fabrics shift from legacy perimeter-based security to a zero trust model with the following components:

- **Zero Trust Routing Fabric:** The session-oriented approach assumes no user, traffic source, or connected network—regardless of what it is and its location on, or relative to, the corporate network—is to be trusted. The Session Smart Router is deployed to create zero trust and service-centric fabrics where routes become directional firewall rules using a deny-all routing model. No application, device, or user may initiate a session on the zero-trust fabric that is not explicitly allowed based on business policies. All routes and sessions are authenticated, and all session traffic is dynamically encrypted end-to-end.
- **Application-Centric Hypersegmentation:** Offers segmentation of user groups and devices, and fine-grained per-service access policies with a global network data model. Hypersegmentation is free of any dependency on overlay networks. It does this over the existing network infrastructure, irrespective of public/private network boundaries, broadcast domains, and administrative boundaries.
- **Native Session Stateful Security Functions:** Branch and data center security architectures are simplified with the Session Smart Router. It natively supports session L2-L7 stateful firewall functions, including NAT, encryption, VPN, and traffic filtering. A Juniper Session Smart Router's Advanced Security Pack provides intrusion detection and prevention systems (IDS/IPS) and URL filtering capabilities.
- **Security Policy Automation and Scale:** The solution centrally manages application-centric and user knowledge-based security policies that are expressed in the language of business, resulting in automated and simplified network security policy management. This reduces security OpEx and overall risks due to user error, since security policy management is simple and scalable across thousands of sites.
- **Secure Edge Functionality:** The Juniper Secure Edge protects web, SaaS, and on-premises applications and—along with AI-Driven SD-WAN—is part of Juniper's best-in-class SASE functionality. SSE connectors provide simple integration with cloud-based security, including Secure Edge, zScaler, and others.

Conclusion

Today's networks needs to deliver applications and services that the business needs, when and where it needs them. To do this requires applications, routers, and services that can "speak the language of sessions," which most networks are unable to do.

Speaking the language of sessions means understanding how to support only valid sessions on the network. Not being able to do this turns out to be the root cause of many of the quality difficulties in networking today, and this is what Juniper Session Smart Networking addresses. The Session Smart Router's data plane is truly session aware.

Because the Session Smart Router is 100% software-based and cloud-ready, it has the capabilities to understand source, destination, and directionality of flows, along with the requirements of named applications, service topology, and business policies. Routers use this information to plot waypoints through the network in real time, to better support the businesses they serve, turning the network itself into a service-centric fabric that is simpler, more agile, and secure for both enterprises and service providers to operate.

Session Smart Routers are deployed along the network edge, enabling the network to build a closer working relationship with the applications and services it exists to support. Session Smart Networking is a key facet of AI-Driven SD-WAN, providing a "zero trust" security model that's tunnel-free and doesn't require IPsec or TLS. This results in much better performance at a lower cost for enterprises and service providers, and businesses of all sizes.

Resources

Web Pages

- Session Smart Router
- Secure Vector Routing
- AI-Driven SD-WAN
- Mist WAN Assurance
- Mist AI and Cloud
- SD-WAN Elevate Community

Technology Explainer Videos

- Session Smart Technology Overview (SVR)
- Simplified: AI-Driven SD-WAN with Session Smart

Documentation

- Session Smart Networking Platform: What is It and How Does it Work?

Solution Briefs

- AI-Driven SD-WAN: Building Networks with Security at their Core
- Building a Secure AI-Driven SD-Branch

White Papers

- AI-Driven SD-WAN Secures Today's Cloud Era Networks
- Client-to-Cloud Assurance with an AI-driven Enterprise
- Enabling SASE with AI-Driven SD-WAN

Analyst Reports

- Tunnel-Based Versus Tunnel-Free SD-WAN (ACG Research)

Datasheets

- Session Smart Router
- SSR100 Line of Routers
- SSR1000 Line of Routers
- Advanced Security Pack

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

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 | Driven by Experience™