Juniper Networks | Engineering Simplicity

White Paper

SESSION SMART ROUTING—HOW IT WORKS

A service-centric fabric with dramatic benefits in terms of simplicity, agility, security, performance, and cost

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document is intended to provide a thorough understanding of exactly how the Juniper® Session Smart™ Router works. It's written by the founding technology and product team, and is meant for a technical audience. With that said, a quick recap of what we do and why it matters will provide helpful context for the "how" we'll be focusing on later in this white paper.

Introduction

The story begins with the belief that the network exists to deliver applications and services that businesses need. While legacy network vendors are always happy to sell you another box to get there—for firewalls, load balancing, deep packet inspection, and tunnels—the hardware-centric model their business is built on means more complexity, compromise, and cost for you. This middlebox-driven approach makes it hard to run new services and applications across diverse networks and within the hybrid cloud. It makes it a challenge to support video-intensive workloads, or properly connect today's mobile workforce. And the sheer complexity of it all exposes the business to increasingly sophisticated cyber criminals and the unacceptably high cost of downtime.

Fixing the problem ties back to our second founding observation: That the applications and services running on your network should speak the language of sessions, and that for the most part, your network doesn't. This language gap turns out to be the root cause of so much of what's broken in networking today, and at the most basic level, that's what the Juniper Session Smart Router addresses. Our "smart" routers speak the language of sessions, and when they're deployed along the network edge, they enable the network to build a closer working relationship with the applications and services it needs to support.

To do this, we first turn the router into software, and then give it the capabilities it needs to understand source, destination, and directionality of flows, along with the requirements of named applications, service topology, and business policies. Our 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. With Session Smart Routing, Juniper makes orchestration fast and easy, while enabling a "zero trust" security model that's simply not possible in the hardware-centric model. The result? Better performance at a lower cost, for businesses large and small.

Secure Vector Routing

The key to all this is a three-tiered approach that has, at its foundation, a revolutionary routing standard called Secure Vector Routing (SVR). Using that standard, we developed the Session Smart Router that, once deployed across the network, enables a service-centric fabric with dramatic benefits in terms of simplicity, agility, security, scalability, performance, and cost.

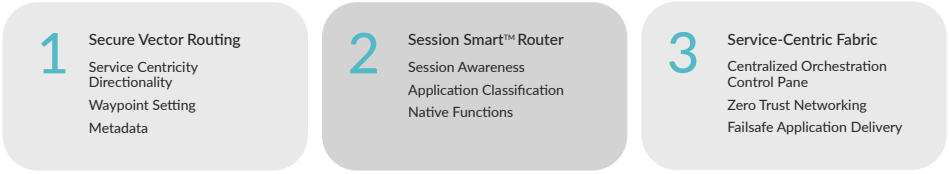

Figure 1: Three-tiered approach to a transformational new routing standard

As we said earlier, networks exist to connect users to services and applications, and network design should start with those services at the core. SVR is a transformational new routing architecture that enables the network to differentiate the way it delivers applications and services. SVR replaces tunnel-based network overlays and inefficient provisioning systems with distributed control, simple intelligent service-based routing, and in-band (data plane) session-based signaling. 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 the network endpoints or hosts.

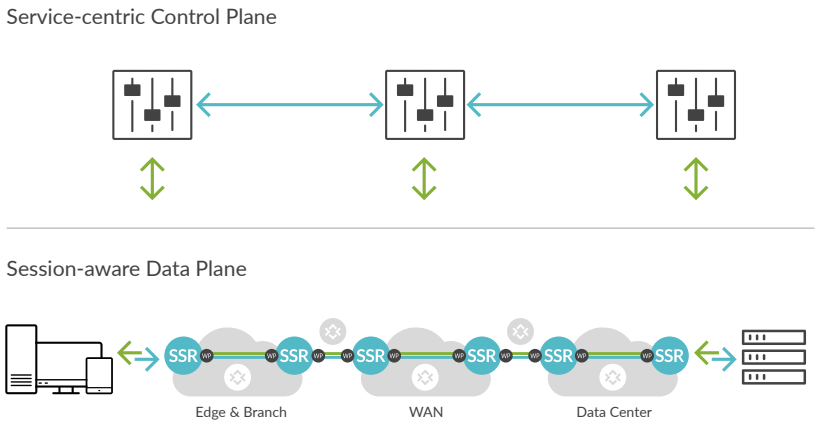

Figure 2: SVR comprises two unique control plane and data plane components, the service-centric control plane and the session-aware data plane.

Service Centricity: The Service-Centric Control Plane

Data Model

Services are the heart of the SVR design, and nowhere is that more evident than in its service-centric control plane. At the core of the SVR control plane is a service-based data model, which provides the language for describing the network's services, tenancy, and associated policies. The SVR data model is global and location independent, meaning every router in an SVR fabric shares the same service-based policies and topology, at all times—no matter where it is. The service-centric data model is expressed in YANG and exposed via northbound Representational State Transfer (REST) APIs to deliver a full suite of application and orchestration integration services.

Service and Topology Exchange Protocol (STEP)

SVR defines the industry's first control plane protocol designed specifically for service-based routing and topology: Service and Topology Exchange Protocol (STEP). STEP works to describe connectivity between all routers, exchanging details about each service and its reachability. Traditional routing protocols distribute information that enables routers to select optimal paths between two nodes on a network based on IP addressing. STEP distributes information about services, service state, reachability and policy enabling SVR routers to select the optimal path to a service wherever it may reside, based on service-specific policy and real-time network and service state. Think about the GPS navigation software Waze applied to networks. STEP does not require you to rip out your existing routing protocols, rather it co-exists with your existing underlay allowing you to innovate-in-place.

Session-Aware Data Plane

The session-aware data plane makes dynamic forwarding and policy decisions based on SVR's distributed service-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 the combination of three features: session detection and control, waypoint setting, and session-based signaling (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 service 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 they're no longer needed. Link and endpoint session load balancing is native.
- **Multitenant**—Hierarchical multitenancy and secure segmentation is supported end-to-end across network and Network Address Translation (NAT) boundaries.

Session Detection and Control

Session Classification and State

SVR classifies each Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) 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 zone-based 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 short, Secure Vector Routing (SVR) unifies access control and security policies during routing.

Waypoint Setting

SVR architecture defines a location independent and segmented approach to routing and addressing based on waypoints. Waypoint addresses (or simply “waypoints”) are IP addresses configured on each Session Smart Router, and these 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 services. Secure vector routes define the path (e.g., set of routers) 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 multi-segment paths can be established. Ephemeral session state in each router along the path guarantees symmetric communications.

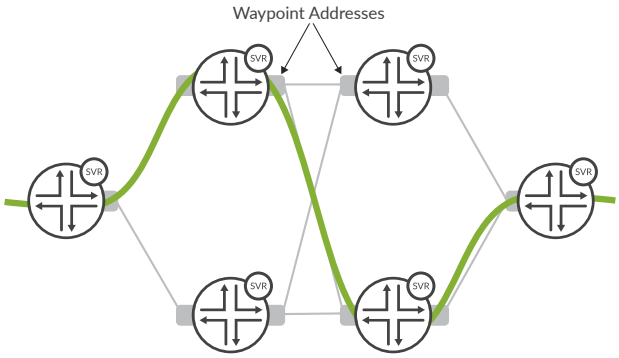

Figure 3: Waypoint addresses govern sessions across network paths

SVR’s waypoint-based routing is location independent and therefore supports mobility. All communications are addressed by two addresses, one for location (e.g., nearest SVR router) and the second for identity (service name or IP address). Destination hosts or workloads are no longer bound by unique fixed IP addresses. This enables global service addressing, allowing one application or service to share the same public IP address across multiple locations, and workload mobility, allowing workloads to maintain their address when in motion.

To establish a symmetric flow, the ingress router adds metadata to the first packet of each session. This metadata is used to signal information about a session, including original IP addresses, tenant, and policy information. The metadata is only included when the SVR router is aware that there is another Session Smart Router downstream and, from there, all packets for that session follow the same path. 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 IP address and port, original destination address and port, the tenant associated with the origin of the request, desired class of service, and other policy and control information. The reverse metadata includes utilization metrics and possible service class modification information.

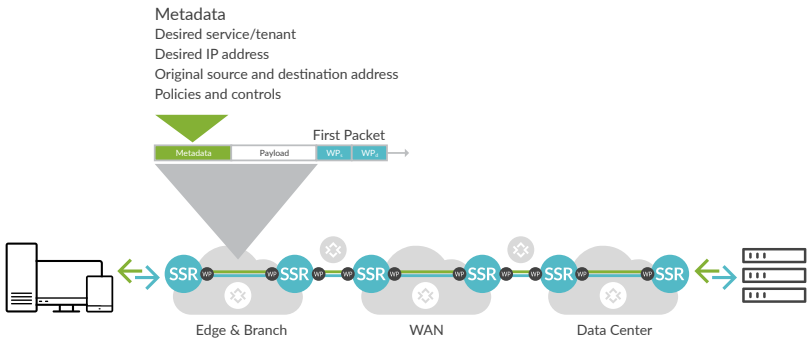

Figure 4: The SSR adds metadata to the first packet of each session to signal information about the session to another SSR.

Putting It All Together—Session-Based First Packet Processing

The first packet of each session serves to establish 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. Let's take a closer look.

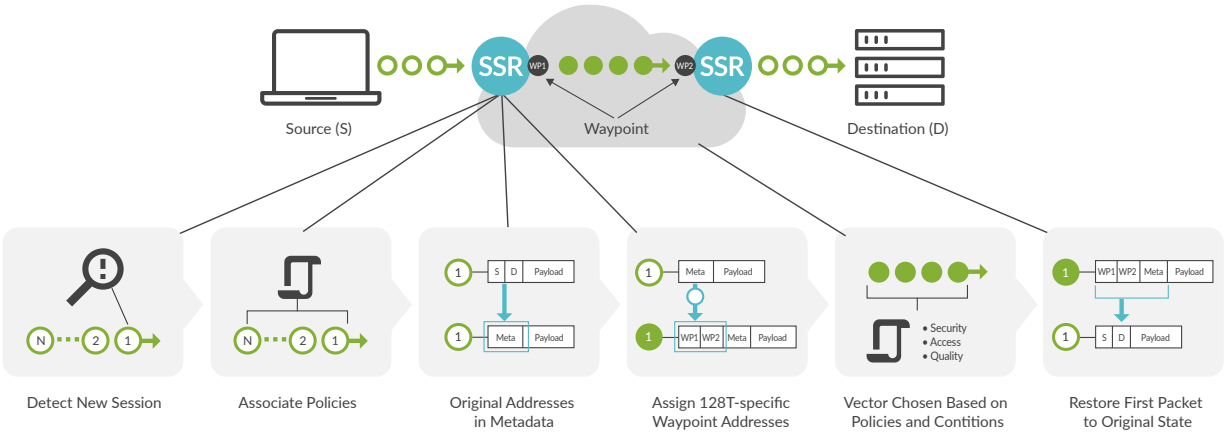

Figure 5: Session-based first packet processing

When the first packet corresponding to a new TCP or UDP 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.
- 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 above processing, 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.

The Session Smart Routing Solution

Juniper Session Smart Routing is comprised of two primary components: The Juniper Session Smart Router and the Juniper Session Smart Conductor. Together, they form a single logical control plane that is highly distributed, and a data plane that is truly session-aware. The Session Smart Routing solution supports a wide 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 Routing solution puts session awareness and state where it belongs, in the router. Why? Sessions are the language of applications and services. Nearly every use of a network involves a stateful exchange of information between endpoints known as a session. Session Smart Routing bridges the gap between networks and the applications they exist to deliver.

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. Secure Vector Routing is the technology that enables the Session Smart Router to do that.

Session Smart Router

The Juniper Session Smart Router is a software-based router built around innovative Session Smart technology and Secure Vector Routing (SVR) capabilities. The Session Smart Router works together with the Session Smart Conductor, enabling enterprises and service providers to build service-centric fabrics that enable new levels of simplicity, agility, security, performance, and savings.

Session Smart Conductor

The Juniper Session Smart Conductor is a centralized management and policy engine that provides orchestration, administration, zero-touch provisioning (ZTP), monitoring, and analytics for the distributed Session Smart Router, while maintaining a network-wide, multitenant service, and policy data model.

100% Software-Based and Cloud Ready

The Session Smart Router and Session Smart Conductor are 100% software-based and can be deployed on general-purpose computing platforms allowing a wide range of deployment models—from remote branch offices to high-capacity network edges to hyperscale data centers and the cloud.

The Session Smart Routing software runs on any commercial off-the-shelf (COTS) platform or white-box 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 intra-cloud routing functions. For deployment in private clouds, the software works with leading cloud management platforms. including OpenStack and VMware vCloud Director.

Application Visibility and Control

Application Classification

The Session Smart Routing solution 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 a range of fast acting methods that can enable early detection, Session Smart Routing allows networks to offer top-of-the-line end-user experiences, protection, and reporting.

Application Visibility

Session Smart Routing 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 the GUI and RESTful APIs, and IPFix-based session detail records are generated on a per-session basis.

Application Control

The 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 tenants. Service-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 Routing, 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.

Native 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-All Routing:** SVR surpasses traditional network security with a zero trust deny-all routing model; this means that no session is permitted without explicit policies to allow it. Directional service routes and multitenant access control lists become one in the same.
- **DoS/DDoS:** Denial of service (DOS) and distributed denial of service (DDOS) protection are applied to every session passing through the Session Smart Router, not only at the edge but wherever a Session Smart Router is deployed. The context-specific nature of a Session Smart Router allows it to provide better analytics and logging to track and discover these attacks.

- **Network Address Translation (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 multitenant segmentation, 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 it 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 Session Smart Router is FIPS 140-2 Level 1 certified.
- **ICSA Labs:** The Session Smart Router is ICSA labs network firewall certified.

Link and Server Load Balancing

Session Smart Routing 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.

Service Function Chaining

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 and WAN optimizer. Both static and dynamic service function chaining capabilities are supported. Session Smart Routing can be deployed as part of a Network Functions Virtualization (NFV) solution either at the edge (virtual CPE) or in the data center.

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.

Service-Centric Fabrics

Enterprises and service providers deploy the Session Smart Router together with the Session Smart Conductor to create end-to-end service-centric fabrics seamlessly across any network infrastructure. These service-centric fabrics offer a single networking solution for multiple use cases in a number of areas including:

Strategic Network Capabilities: SD-WAN, Virtual Edge, NaaS and WAN refresh

Multi-cloud Fabric and Data Center Interconnect

Security: Zero Trust Networking, Secure Branch/Edge

Service-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. Secure Vector Routing forms the network Routing Engine (RE) for service-centric fabrics, which are completely tunnel-free. In addition, they are natively service-aware, multitenanted, and maintain a vast knowledge of service availability, topology, and policies.

The Juniper service-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 service-centric fabrics are centrally managed and orchestrated by the Session Smart Conductor with a single pane-of-glass application that enables network visibility, strong analytics, automated policy provisioning, and zero touch deployments. Juniper service-centric fabrics are open and programmable through northbound RESTful APIs.

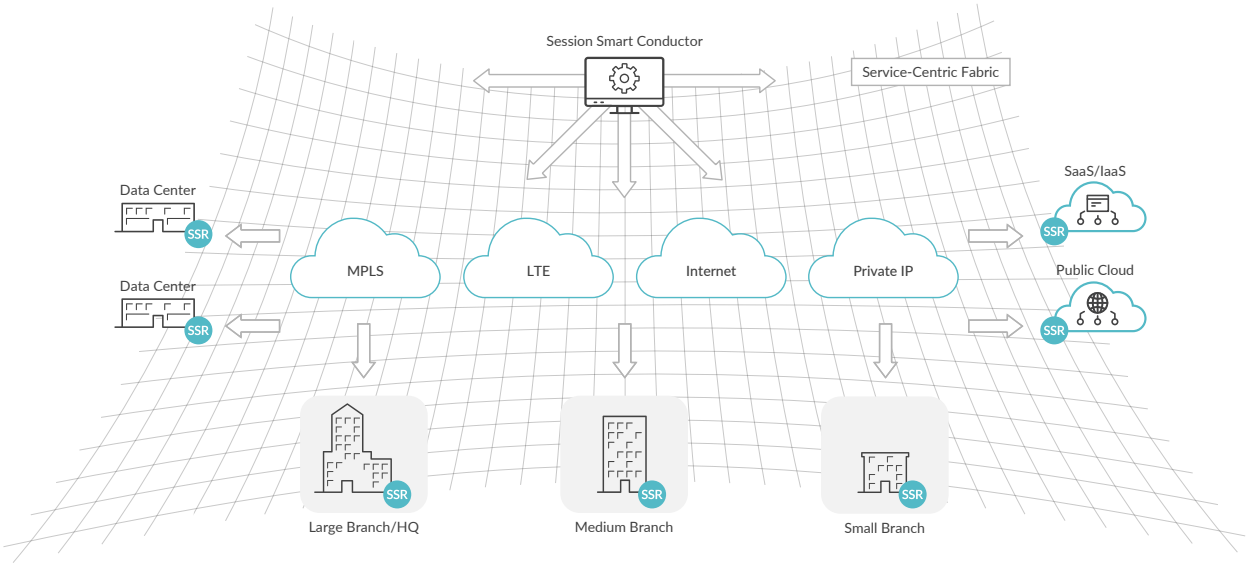

Figure 7: Juniper Session Smart Routing service-centric fabric

Enterprises and service providers can achieve the following benefits with Juniper service-centric fabrics:

- **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-all 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

Centralized Orchestration and Control—The Session Smart Conductor

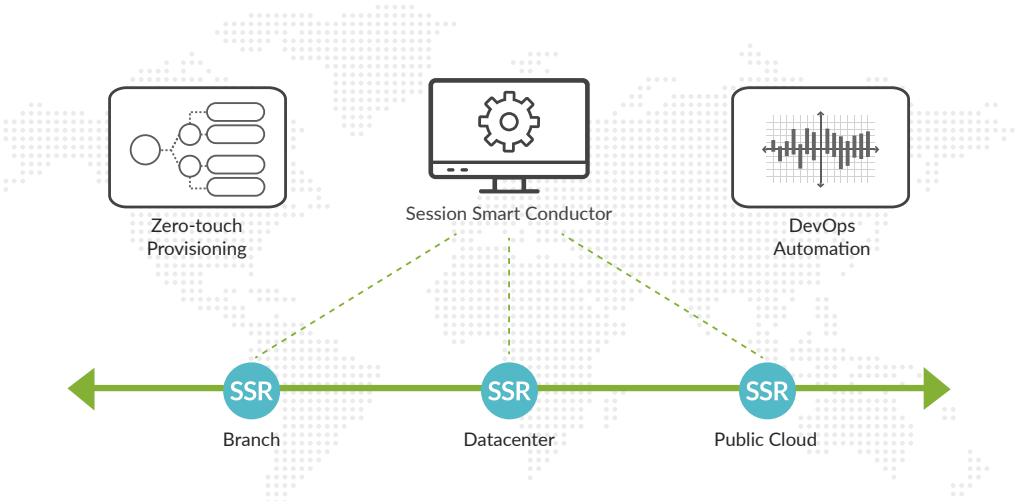

Figure 8: Session Smart Conductor orchestration and control

The Session Smart Conductor is a platform that provides fabric-wide central administration, provisioning, monitoring, analytics, network-wide visibility, and automation with a consistent visual user experience. It is a separate application from the Session Smart Router and operates from any location with secure connectivity to routers in the fabric. From a central point, the Session Smart Conductor provides administrative functions, including zero-touch installation to enable rapid deployment of new instances across a network. It also enables automated network-wide, zero-touch software upgrades and centralized key and entitlement management.

The Session Smart Conductor greatly simplifies wide scale deployment by enabling zero-touch provisioning (ZTP), where non-IT users can quickly add network connectivity to a new branch site. This Juniper platform supports numerous service-aware features to simplify provisioning, including autoconfiguration, back up, versioning, and auditing. From a central point, the Session Smart Conductor ensures consistent policy and service management. For broader service integration, the Session Smart Conductor also supports northbound REST and GraphQL interfaces to third-party operations support systems (OSS) and business support systems (BSS).

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. Multiple paths or hybrid networks are deployed, as in SD-WAN use cases, 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 makes sure 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 (e.g., 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) 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.

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

- Multipath Session Migration—Rapidly 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) is key to the Session Smart Router approach. Originating from Forrester, the zero trust model for security ends the notion that any packet should be considered above suspicion. Juniper's service-centric fabrics shift from legacy perimeter-based security to the 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.

Service-Centric Hypersegmentation: Hypersegmentation offers almost limitless hierarchical tenancy and fine-grained per-service access policies with a global multitenanted data model. Hypersegmentation is free of any dependency on overlay networks. Best of all, 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-L5 stateful firewall functions, including DoS/DDoS protection, NAT, encryption, VPN, and traffic filtering. Where advanced firewall functions are needed, dynamic service chaining of the Juniper SRX is also supported.

Security Policy Automation and Scale: The Session Smart Conductor centrally manages service-centric and tenant-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.

Conclusion

Today's network needs to be able 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. This language gap turns out to be the root cause of much of what's broken in networking today, and it's what the Juniper Session Smart Routing Solution addresses.

The two primary components of Juniper Session Smart Routing are the Session Smart Router and the Session Smart Conductor. Together, they form a single logical control plane that is highly distributed, and a data plane that is truly session-aware.

Because the Session Smart Router is 100% software-based and cloud-ready, it has the capabilities it needs 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.

And because Session Smart Routers speak the language of sessions, they can be deployed along the network edge, enabling the network to build a closer working relationship with the applications and services it exists to support. With the Session Smart Router and its session-aware data plane topology, Juniper makes orchestration fast and easy, while enabling a "zero trust" security model that's simply not possible with a hardware-centric approach. The result? Much better performance at a lower cost for enterprises and service providers, businesses large and small.

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