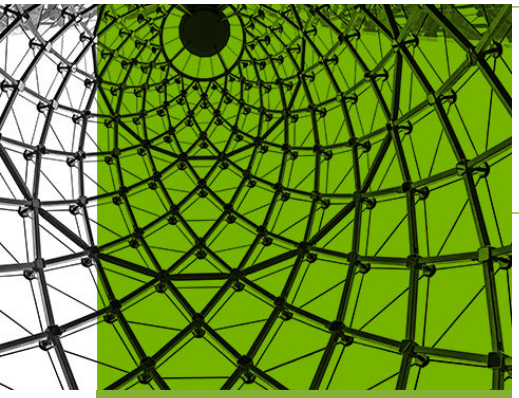

SESSION SMART NETWORKING DATASHEET

Product Overview

The Juniper Session Smart Router (SSR) powers Juniper's AI-driven SD-WAN solution that is designed to provide users with exceptional experiences. Built on an application-aware and zero-trust secure network fabric, the SSR meets the most stringent enterprise performance, security, and availability requirements.

The SSR overcomes inherent inefficiencies of conventional solutions with a tunnel-free architecture that enables improved performance, fast deployments, and cost savings. The solution can run on customer premises equipment (CPE), data center network servers, and in the cloud for flexible deployments.

Product Description

Juniper Networks® SSR Series Routers power Juniper's AI-driven SD-WAN solution. The software-based solution utilizes a unique, tunnel-free routing protocol called Secure Vector Routing. This innovative networking solution improves application performance, rapidly scales to thousands of sites, and secures users and data with inherent, Zero Trust access policies.

The Session Smart™ Router can be managed by either the Juniper Session Smart Conductor or the Juniper Mist™ Cloud. Together, these platforms create a single logical control plane that is highly distributed, and a data plane that is truly session aware. SSR supports a wide range of use cases, including SD-WAN, SD-Branch, multi-cloud, and IoT and can scale from a small branch office to a high-capacity edge router to a hyper-scale, software-defined data center (Figure 1).

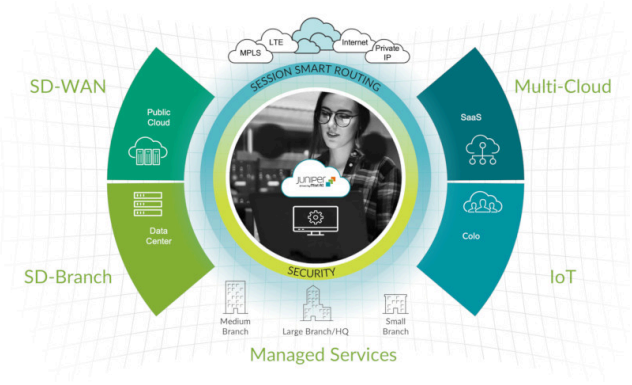

Figure 1: Session Smart Router services, applications, and network domains

Session Smart Router

The Session Smart Router 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.

The Session Smart Router also provides native Zero-Trust security, leveraging hypersegmentation. It also includes several security features:

- Service-centric, tenant-based security architecture: The unique design 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.
- Firewall capabilities: The Session Smart Router provides Layer 3/ Layer 4 network firewall functionality.
- IDS/IPS and URL filtering: Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) and URL filtering capabilities are available through the Advanced Security Pack.
- Security at its core: The advanced design of the Session Smart Router replaces the traditional routing plane with one built for security from the ground up.

Table 1 details the key features of the Session Smart Router

Category	Features
System and network services	SNAT/DNAT, destination NAPT, shared NAT pool, IPv4/IPv6, DHCP client, DHCP relay, DHCP server, DHCP server extensions, DHCPv6 PD, DNS client, PPPoE, Proxy ARP, NAT traversal, BFD, inline flow performance monitoring, extended firewall pinhole, path MTU discovery, MSS auto adjust, DSCP based service identification for IPsec
Advanced services	Secure Vector Routing (SVR), Multipoint SVR, IPv6 SVR, overlapping IP service segmentation, Ethernet over SVR, application identification
Routing	Service based routing, static routing, BGPv4, BGP route reflector, BGP graceful restart, BGP over SVR, BGP route map, BGP prefix list, OSPFv2, BGP VRF, OSPF VRF, Services and Topology Exchange Protocol (STEP)
Traffic engineering	Traffic scheduling and shaping, flow policing and shaping, packet marking (DiffServ), service rate limiting
Network firewall	Distributed stateful firewall, distributed and automated access control, fine-grained segmentation/tenancy, ICSA network firewall certified, ICMP blackhole
IDS/IPS and URL filtering	Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) and URL filtering capabilities are available through the Advanced Security Pack.
Secure edge connectors	Seamless connections to Juniper Secure Edge or third-party SSE.
Application identification	HTTP/S domain-based identification, O365 identification, DNS based identification, application categorization
Analytics	Session metrics, network metrics, LTE metrics, peer path SLA, MOS score, session analytics, SSL/TLS metrics, session IPFIX records
Session encryption	Session Payload Encryption (AES-256, AES-128), session/route authentication (HMAC-SHA1, HMAC-SHA256, HMAC-SHA-256-128), adaptive encryption, rekeying, FIPS 140-2 validated, enhanced replay attack protection, transport-based encryption
Session management	Path selection, (SLA, MoS, average latency), load balancing using proportional and hunt, session migration, session duplication, session duplication for non-SVR, session duplication for inter-node links, MOS for VoIP, Path of last resort, session optimization, session reliability, service health learning, service route redundancy
Monitoring	Monitoring agent, SNMPv2, Syslog, audit logs
Management and remote access	GUI, CLI, REST, remote access over SVR (LTE), upgrade rollback, Zero Touch provisioning, remote service packet capture, user-defined configuration templates, role-based access control
AAA	Local registry, LDAP
Interface options	Ethernet, LTE support including Dual LTE and Dual SIM, T1
Platforms	Bare metal x86 server, KVM, VMWare ESXi, OpenStack, AWS, Azure, Google Cloud

Session Smart Conductor

The Session Smart Conductor is a centralized management and policy engine that provides orchestration, administration, zero-touch provisioning (ZTP), monitoring, and analytics for distributed Session Smart Routers—while maintaining a network-wide, multi-tenant service, and policy data model. The Session Smart Conductor features multiple, flexible deployment models, from on-premises to private or public cloud.

Juniper Mist WAN Assurance and AI-Native operations

Alternatively, Session Smart Routers can be operated and orchestrated through the Juniper Mist Cloud. Mist AI delivers unprecedented automation using a combination of artificial intelligence, machine learning algorithms, and data sciences techniques to save time, maximize IT productivity, and deliver the best experience to digital users.

Juniper Mist WAN Assurance is built on the Juniper Mist Cloud and delivers full lifecycle management and operations, including AI-Native insights, automated speed tests, dynamic packet capture (dPCAP), anomaly detection, and root cause identification that focuses on end users' experience. For Day-0 and Day-1 operations, WAN Assurance also provides orchestration, administration, and ZTP for Session Smart Routers. See the WAN Assurance Datasheet for more information.

Platform options for the Session Smart Router

SSR100 and SSR1000 Series appliances

The SSR Series of appliances provide the hardware foundation for the Juniper AI-Driven SD-WAN solution:

- The SSR100 line includes small and medium branch platform to support SD-WAN in distributed locations
- The SSR1000 line includes platforms for large branch, and small, medium, large and extra-large data center and campus deployments

Deployment Locations are shown in Table 2, along with links to the relevant datasheets for more information.

Table 2: SSR appliances and suggested locations

Appliance	Suggested Location	Max Throughput (Unencrypted)	Relevant Datasheet
SSR120	Small branch	1.5 Gbps	SSR100 Line of Routers
SSR130	Medium branch	2 Gbps (line rate on ports)	
SSR1200	Large branch or small data center/campus	10 Gbps	SSR1000 Line of Routers
SSR1300	Medium data center/campus	20 Gbps (max. throughput on NIC)	
SSR1400	Large data center/campus	40 Gbps	
SSR1500	Extra-large data center/campus	50 Gbps (max. throughput on NIC)	

The hardware datasheets provide standard specifications such as interface options, number of interfaces, encrypted throughput, and memory and hard drive capacity.

White-box appliances and Juniper NFX Series

The Session Smart Router can run on certified white box platforms. More information on certified white boxes can be found at SSR Certified Hardware Documentation. For Virtual network function (VNF)-based deployments, the Session Smart Router can also run as a VNF using VirtIO and SRIOV network virtualization technologies on the Juniper Networks® NFX150, NFX250, and NFX350 Network Services Platforms.

Public cloud providers

The Session Smart Router can run as an instance on Amazon Web Services (AWS) and Microsoft Azure.

Platform Options for the Session Smart Conductor

The Session Smart Conductor can run on certified white box platforms or on all major public cloud providers, including AWS, Google Cloud, and Azure.

Juniper service and support

Juniper ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net.

About Juniper Networks

Juniper Networks believes that connectivity is not the same as experiencing a great connection. Juniper's AI-Native Networking Platform is built from the ground up to leverage AI to deliver exceptional, highly secure, and sustainable user experiences from the edge to the data center and cloud. Find additional information at www.juniper.net or connect with Juniper on X (formerly Twitter), LinkedIn and Facebook.

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

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240 1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.207.125.700

Juniper Networks | Driven by Experience™