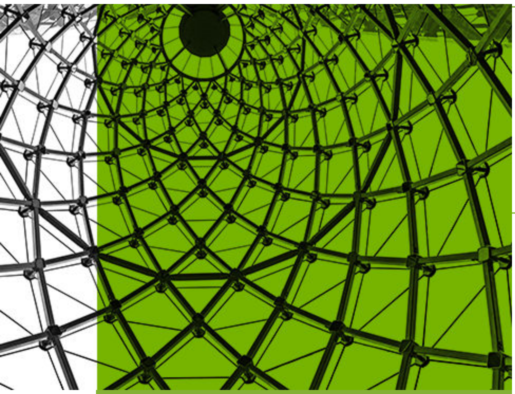
SESSION SMART NETWORKING DATASHEET



Product overview

The [Juniper Session Smart Router (SSR)] powers Juniper's [AI-native 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

The Juniper Networks® Session Smart™ Router (SSR) Series powers Juniper's AI-native 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 Juniper SSR can be managed by either the Juniper Session Smart Conductor or the Mist™ platform. Together, these platforms create a single logical control plane that is highly distributed, and a data plane that is truly session aware. The SSR supports a wide range of use cases, including SD-WAN, SD-Branch, multicloud, 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).

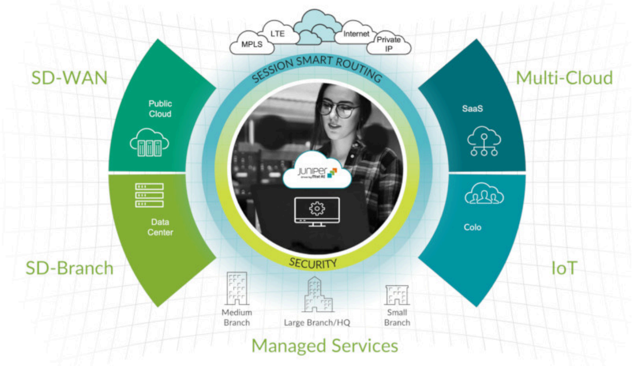


Figure 1: Session Smart Router services, applications, and network domains

Session Smart Router

The SSR combines a service-centric control plane and a session-aware data plane to offer IP routing, a robust policy management engine, improved visibility, and proactive analytics. This architecture, built on a unique tunnel-free foundation, is designed to provide a more efficient and agile service fabric for modern networks.

The SSR also provides native Zero Trust security that leverages hypersegmentation. It includes several key security features:

- **Service-centric, tenant-based security architecture**: The unique design enables the SSR to understand sessions and perform vital business operations, securing connectivity based on user, application, and location.
- **Zero Trust security**: The SSR follows the principle of "deny-by-default," which uses a series of checkpoints to validate legitimate network traffic, assuming no user or device can be trusted by default.
- **Integrated next-generation firewall (NGFW)** : The SSR provides Layer 3/Layer 4 network firewall functionality, integrated directly into the routing fabric.

- **Integrated security**: The solution includes built-in next-generation firewall features such as IDS/IPS, URL filtering, and antivirus, providing robust and consistent protection across the entire branch network.
- **Security at its core**: The advanced design of the SSR replaces the traditional routing plane with one built for security from the ground up, providing a unified security posture without relying on separate, bolted-on appliances.
- **AI-native management**: When paired with Juniper® WAN Assurance, the SSR's security is managed by Marvis® AI, which provides a single, centralized platform for policy orchestration, real-time threat intelligence, and AI-native troubleshooting.

Table 1 details the key features of the SSR.

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 SSRs while maintaining a network-wide, multitenant service, and policy data model. The Session Smart Conductor features multiple, flexible deployment models, from on-premises to private or public cloud.

Juniper WAN Assurance and AI-native operations

Alternatively, SSRs can be operated and orchestrated through the Mist cloud. Marvis AI delivers unprecedented automation using a combination of AI, machine learning algorithms, and data science techniques to save time, maximize IT productivity, and deliver the best experience to digital users.

Juniper WAN Assurance is built on the Mist cloud and delivers full life cycle 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 SSRs. See the WAN Assurance Datasheet for more information.

Platform options for the Session Smart Router

SSR100, SSR400, and SSR1000 Series appliances

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

- The SSR100 line includes small and medium branch platform to support SD-WAN in distributed locations
- The SSR400 line includes small and medium branch platforms to support SD-WAN in distributed locations as well, but also includes integrated Wi-Fi, switching, and 5G
- 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)	
SSR400	Small branch		SSR400 line of routers
SSR440	Medium branch		
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.

Branch in a Box

The SSR400 line of routers offers a “Branch in a box” solution by consolidating multiple branch functions—including Wi-Fi, switching, SD-WAN, and security—into a single, unified, and easy-to-manage platform. This approach simplifies operations by eliminating the need to deploy and manage a complex array of separate devices from various vendors. Our solution significantly reduces a branch's physical footprint and lowers its total cost of ownership.

White box appliances and Juniper NFX Series

The SSR 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 SSR 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 SSR 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.

Advanced Security Pack

Juniper SSR’s Advanced Security Pack (Figure 2) integrates further security functionality into the routing fabric:

- URL filtering prevents access to and from specific sites and meets special business requirements.
- An Intrusion Detection and Prevention System (IDS/IPS) protects against advanced malicious attacks.

Session Smart Routing Security

- Deny by default/ Zero Trust model
- Adaptive encryption
- Route directionality, policy enforcement
- Layer 3/Layer 4 DOS/DDOS.
- FIPS 140-3 certified
- Fine-grained segmentation
- Centralized policy management

SSR SECURITY
SSR
ADVANCED SECURITY PACK

Advanced Security Pack

- IPS/IDS
- URL filtering
- Anti-virus
- Advanced Threat Prevention
- SSL proxy
- Security Assurance dashboard

Secure Edge Connectors to connect to any SSE

- Juniper Secure Edge
- ZScaler
- Any third-party SSE

Figure 2: Foundational SSR router security and the Advanced Security Pack

These features eliminate the need for additional security appliances at the branch, providing this enhanced functionality within the Mist ecosystem of wired, wireless, and SD-WAN. If more cloud-integrated security is needed, customers can add Juniper Secure Edge to the environment.

Meeting you where you are

When it comes to your network security, we want to meet you where you are. The Advanced Security Pack can thus be installed standalone or alongside a Juniper Networks® SRX Series Firewall at your branch or data center.

The Advanced Security Pack can also be used to help you with your SASE Journey, giving you protection in the branch or data center before easily offloading that traffic to an SSE such as Juniper Secure Edge.

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 is leading the convergence of AI and networking. Juniper's Mist™ AI-native networking platform is purpose-built to run AI workloads and simplify IT operations assuring exceptional secure user and application experiences—from the edge, to the data center, to the cloud. Additional information can be found at www.juniper.net, X, 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

Driven by Experience™