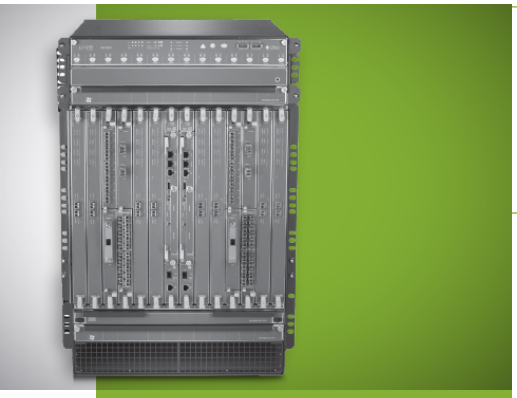

SRX5400, SRX5600, AND SRX5800 SERVICES GATEWAYS

Product Overview

SRX Series Services Gateways are next-generation firewalls based on a revolutionary architecture offering outstanding performance, scalability, availability, and security services integration. Custom designed for flexible processing scalability, I/O scalability, and services integration, the SRX Series Services Gateways exceed the security requirements of data center consolidation and services aggregation. The award-winning SRX Series is powered by Junos OS, the same industry-leading operating system that keeps the world's largest data center networks available, manageable, and secure.

Product Description

The Juniper Networks® SRX5400, SRX5600, and SRX5800 Services Gateways are next-generation firewalls (NGFWs) that deliver outstanding protection, market-leading performance, six nines reliability and availability, scalability, and services integration. These devices are ideally suited for service provider, large enterprise, and public sector networks, including:

- Cloud and hosting provider data centers
- Mobile operator environments
- Managed service providers
- Core service provider infrastructures
- Large enterprise data centers

The SRX5400, SRX5600, and SRX5800 are an integral part of the Juniper Connected Security framework, which is built to protect users, applications, and infrastructure from advanced threats.

Delivering the highest level of protection against exploits, malware, and command and control (C&C) communications, these platforms feature a carrier-grade next-generation firewall and advanced security services such as application security, Content Security, intrusion prevention system (IPS), and integrated threat intelligence services.

For advanced protection, the SRX Series offers integrated threat intelligence services via Juniper Networks Advanced Threat Prevention (ATP), Juniper's open threat intelligence platform in the cloud. Juniper ATP Cloud delivers actionable security intelligence to SRX Series devices to enable advanced protection against C&C-related botnets and Web application threats, as well as allowing policy enforcement based on GeoIP data—all based on Juniper-provided feeds. Customers may also leverage their own custom and third-party feeds for protection from advanced malware and other threats unique to their business environment. This advanced, customer-relevant, and consolidated threat intelligence service is delivered to the SRX Series on-premises from the cloud.

The SRX5400, SRX5600, and SRX5800 are supported by Juniper Networks Security Director, which enables distributed security policy management through an intuitive, centralized interface that enables enforcement across emerging and traditional risk vectors. Using intuitive dashboards and reporting features, administrators gain insight into threats, compromised devices, risky applications, and more.

Based on Juniper's Dynamic Services Architecture, the SRX5000 line provides unrivaled scalability and performance. Each services gateway can support near linear scalability with the addition of Services Processing Cards (SPCs) and I/O cards (IOCs), enabling a fully equipped SRX5800 to support up to 1 Tbps firewall throughput. The SPCs are designed to support a wide range of services, enabling future support of new capabilities without the need for service-specific hardware. Using SPCs on all services ensures that there are no idle resources based on specific services being used—maximizing hardware utilization.

The scalability and flexibility of the SRX5000 line is supported by equally robust interfaces. The SRX5000 line employs a modular approach, where each platform can be equipped with a flexible number of IOCs that offer a wide range of connectivity options, including 1GbE, 10GbE, 40GbE, and 100GbE interfaces. With the IOCs sharing the same interface slot as the SPCs, the gateway can be configured as needed to support the ideal balance of processing and I/O. Hence, each deployment of the SRX Series can be tailored to specific network requirements.

The scalability of both SPCs and IOCs in the SRX5000 line is enabled by the custom-designed switch fabric. Supporting up to 960 Gbps of data transfer, the fabric enables the realization of maximum processing and I/O capability available in any particular configuration. This level of scalability and flexibility enables future expansion and growth of the network infrastructure, providing unrivaled investment protection.

The tight service integration on the SRX Series is enabled by Juniper Networks Junos® operating system. The SRX Series is equipped with a robust set of services that include stateful firewall, intrusion prevention system (IPS), denial of service (DoS), application security, VPN (IPsec), Network Address Translation (NAT), Content Security, quality of service (QoS), and large-scale multitenancy. In addition to the benefit of individual services, the SRX5000 line provides a low latency solution.

Junos OS also delivers carrier-class reliability with six nines system availability, the first in the industry to achieve independent verification by Telcordia. Furthermore, the SRX Series enjoys the benefit of a single source OS, and single integrated architecture traditionally available on Juniper's carrier-class routers and switches.

SRX5800

The SRX5800 Services Gateway is the market-leading security solution supporting up to 1 Tbps firewall throughput and latency as low as 32 microseconds for the stateful firewall. The SRX5800 also supports 860 Gbps IPS and 338 million concurrent sessions. The SRX5800 is equipped with the full range of advanced security services and is ideally suited for securing large enterprise, hosted, or colocated data centers, service provider core and cloud provider infrastructures, and mobile operator environments. The massive performance, scalability, and flexibility of the SRX5800 make it ideal for densely consolidated processing environments, and the service density makes it ideal for cloud and managed service providers.

SRX5600

The SRX5600 Services Gateway uses the same SPCs and IOCs as the SRX5800 and can support up to 480 IMIX Gbps firewall throughput, 182 million concurrent sessions, and 460 Gbps IPS. The SRX5600 is ideally suited for securing enterprise data centers as well as aggregating various security solutions. The capability to support unique security policies per zone and its ability to scale with the growth of the network infrastructure make the SRX5600 an ideal deployment for consolidation of services in large enterprise, service provider, or mobile operator environments.

SRX5400

The SRX5400 Services Gateway uses the same SPCs and IOCs as the SRX5800 and can support up to 270 Gbps IMIX firewall, 90 million concurrent sessions, and 230 Gbps IPS. The SRX5400 is a small footprint, high-performance gateway ideally suited for securing large enterprise campuses as well as data centers, either for edge or core security deployments. The ability to support unique security policies per zone and a compelling price/performance/footprint ratio make the SRX5400 an optimal solution for edge or data center services in large enterprise, service provider, or mobile operator environments.

Service Processing Cards (SPCs)

As the "brains" behind the SRX5000 line, SPCs are designed to process all available services on the platform. Without the need for dedicated hardware for specific services or capabilities, there are no instances in which a piece of hardware is taxed to the limit while other hardware is sitting idle. SPCs are designed to be pooled together, allowing the SRX5000 line to expand performance and capacities with the introduction of additional SPCs, significantly reducing management overhead and complexity. The high-performance SPC3 cards are supported on the SRX5400, SRX5600, and SRX5800 Services Gateways.

I/O Cards (IOCs)

To provide the most flexible solution, the SRX5000 line employs the same modular architecture for SPCs and IOCs. The SRX5000 line can be equipped with one or several IOCs, supporting the ideal mix of interfaces. With the flexibility to install an IOC or an SPC on any available slot, the SRX5000 line can be equipped to support the perfect blend of interfaces and processing capabilities, meeting the needs of the most demanding environments while ensuring investment protection.

The third generation of IOCs from Juniper, the IOC3, delivers high throughput along with superior connectivity options including 100GbE, 40GbE, and high-density 10GbE interfaces. The IOC3 cards are supported on the SRX5400, SRX5600, and SRX5800.

The fourth generation of IOCs delivers the highest throughput of all available linecards of up to 480 Gbps and offers multiple connectivity options from 10GbE and 40GbE to 100GbE. IOC4 can deliver up to 480 Gbps of hardware-accelerated throughput per linecard.

Routing Engine (RE3) and Enhanced System Control Board (SCB4)

The SRX5K-RE3-128G Routing Engine (RE3) is the latest in the family of REs for the SRX5000 line with a multicore processor running at 2000 MHz. It delivers improved performance, scalability, and reliability with 128 GB DRAM and includes a TPM module. The SRX5K-SCB4 enables 480 Gbps throughput per SCB and can be configured with intra- and interchassis redundancy.

Features and Benefits

Networking and Security

The Juniper Networks SRX5000 line of Services Gateways has been designed from the ground up to offer robust networking and security services.

Feature	Feature Description	Benefits
Purpose-built platform	Built from the ground up on dedicated hardware designed for networking and security services.	Delivers unrivaled performance and flexibility to protect high-speed network environments.
Scalable performance	Offers scalable processing based on Juniper's Dynamic Services Architecture.	Offers a simple and cost-effective solution to leverage new services with appropriate processing.
System and network resiliency	Provides carrier-class hardware design and proven OS.	Offers the reliability needed for any critical high-speed network deployments without service interruption. Utilizes a unique architectural design based on multiple processing cores and a separation of the data and control planes.
High availability (HA)	Active/passive and active/active HA configurations use dedicated HA interfaces.	Achieves availability and resiliency necessary for critical networks.
Interface flexibility	Offers flexible I/O options with modular cards based on the Dynamic Services Architecture.	Offers flexible I/O configuration and independent I/O scalability (options include 1GbE, 10GbE, 40GbE, and 100GbE) to meet the port density requirements of demanding network environments.
Network segmentation	Security zones, virtual LANs (VLANs), and virtual routers allow administrators to deploy security policies to isolate subnetworks and use overlapping IP address ranges.	Features the capability to tailor unique security and networking policies for various internal, external, and demilitarized zone (DMZ) subgroups.
Robust Routing Engine	Dedicated RE provides physical and logical separation to data and control planes.	Enables deployment of consolidated routing and security devices, as well as ensuring the security of routing infrastructure—all via a dedicated management environment.
Advanced threat protection	IPS, antivirus, antispam, enhanced web filtering, Juniper Advanced Threat Prevention Cloud, Encrypted Traffic Insights, Threat Intelligence Feeds, and Juniper ATP Appliance.	• Provides real-time updates to IPS signatures and protects against exploits • Implements industry-leading antivirus and URL filtering • Delivers open threat intelligence platform that integrates with third-party feeds • Protects against zero-day attacks • Stops rogue and compromised devices to disseminate malware • Restores visibility that was lost due to encryption, without the heavy burden of full TLS/SSL decryption
AppTrack	Detailed analysis on application volume/usage throughout the network based on bytes, packets, and sessions.	Provides the ability to track application usage to help identify high-risk applications and analyze traffic patterns for improved network management and control.
AppFirewall	Fine-grained application control policies to allow or deny traffic based on dynamic application name or group names.	Enhances security policy creation and enforcement based on applications and user roles rather than traditional port and protocol analysis.
AppQoS	Leverage Juniper's rich QoS capabilities to prioritize applications based on customers' business and bandwidth needs.	Provides the ability to prioritize traffic as well as limit and shape bandwidth based on application information and contexts for improved application and overall network performance.
Application signatures	Open signature library for identifying applications and nested applications with more than 3000 application signatures.	Accurately identifies applications so that the resulting information can be used for visibility, enforcement, control, and protection.
SSL proxy (forward and reverse)	Performs SSL encryption and decryption between the client and the server.	Combines with application identification to provide visibility and protection against threats embedded in SSL encrypted traffic.
Stateful GTP and SCTP inspection	Support for General Packet Radio Service Tunneling Protocol (GTP) and Stream Control Transmission Protocol (SCTP) firewall in mobile operator networks.	Enables the SRX5000 line to provide stateful firewall capabilities for protecting key GPRS nodes within mobile operator networks.

Feature	Feature Description	Benefits
IOC3	The third-generation I/O card offers very high levels of firewall throughput and low latency. The card includes two board choices: six 40GbE interfaces and 24 10GbE interfaces, or two 100GbE interfaces and four 10GbE interfaces. The IOC3 pairs well with existing SPC2/SPC3 for maximum firewall performance in any of the SRX5000 line of Services Gateways.	Provides vastly superior, top-of-the-line connectivity efficiency and record-breaking high throughput I/O interfaces. Reduces the need for link aggregation to the firewall and enables very high firewall throughput of up to 2 Tbps with Express Path enabled.
IOC4	The fourth-generation I/O card is being offered in two flavors. The first delivers 40x10GbE interfaces while the second, depending on the chosen optics, delivers 48x10GbE, 12x40GbE, or 4x100GbE interfaces.	Provides the fastest throughput per slot and, in combination with Express Path, can deliver up to 480 Gbps of throughput per I/O card.
SPC3 card	Enables performance and scale with backwards compatibility to the SPC2 service cards. These cards support in-service software and in-service hardware upgrades.	Delivers always-on security resiliency to meet your growing network performance needs.
AutoVPN	One-time hub configuration for site-to-site VPN for all spokes, even newly added ones. Configuration options include: routing, interfaces, Internet Key Exchange (IKE), and IPsec.	Enables IT administrative time and cost savings with easy, zero-touch deployment for IPsec VPN networks.
Remote access/SSL VPN	Secure and flexible remote access SSL VPN with Juniper Secure Connect.	Extends secure access to corporate resources from anywhere.
Multitenancy	Offers logical, large-scale segmentation and separation of security functions and features.	Enables separate, logical instances to be deployed with dedicated security policies, zones, and other features and functions. Removes the need to deploy several physical or virtual firewalls.

IPS Capabilities

Juniper Networks IPS capabilities offer several unique features that assure the highest level of network security.

Feature	Feature Description	Benefits
Stateful signature inspection	Signatures are applied only to relevant portions of the network traffic determined by the appropriate protocol context.	This minimizes false positives and offers flexible signature development.
Protocol decodes	This feature enables highly accurate detection and helps reduce false positives.	Accuracy of signatures is improved through precise contexts of protocols.
Signatures	There are more than 8500 signatures for identifying anomalies, attacks, spyware, and applications.	Attacks are accurately identified and attempts to exploit a known vulnerability are detected.
Traffic normalization	Reassembly, normalization, and protocol decoding are provided.	Overcome attempts to bypass other IPS detections by using obfuscation methods.
Zero-day protection	Protocol anomaly detection and same-day coverage for newly found vulnerabilities are provided.	Your network is already protected against any new exploits.
Recommended policy	Group of attack signatures are identified by Juniper Networks Security Team as critical for the typical enterprise to protect against.	Installation and maintenance are simplified while ensuring the highest network security.
Active/active traffic monitoring	IPS monitoring on active/active SRX5000 line chassis clusters is provided.	Includes support for active/active IPS monitoring, including advanced features such as in-service software upgrade.
Packet capture	IPS policy supports packet capture logging per rule.	Conduct further analysis of surrounding traffic and determine further steps to protect target.

Content Security Capabilities

The Content Security services offered on the SRX5000 line of Services Gateways include industry-leading antivirus, antispam, content filtering, and additional content security services.

Feature	Feature Description	Benefits
Antivirus	Antivirus includes reputation enhanced, cloud-based antivirus capabilities that detect and block spyware, adware, viruses, keyloggers, and other malware over POP3 HTTP, SMTP, IMAP, and FTP protocols. This service is provided in cooperation with Sophos Labs, a dedicated security company.	Sophisticated protection from respected antivirus experts against malware attacks that can lead to data breaches and lost productivity.
Antispam	Multilayered spam protection, up-to-date phishing URL detection, standards-based S/MIME, Open PGP and TLS encryption, MIME type, and extension blockers are provided in cooperation with Sophos Labs, a dedicated security company.	Protection against advanced persistent threats perpetrated through social networking attacks and the latest phishing scams with sophisticated e-mail filtering and content blockers.
Enhanced Web filtering	Enhanced Web filtering includes extensive category granulation (95+ categories) and a real-time threat score delivered with Forcepoint, an expert Web security provider.	Protection against lost productivity and the impact of malicious URLs as well as helping to maintain network bandwidth for business essential traffic.
Content filtering	Effective content filtering is based on MIME type, file extension, and protocol commands.	Protection against lost productivity and the impact of extraneous or malicious content on the network to help maintain bandwidth for business essential traffic.

Advanced Threat Prevention

Advanced threat prevention (ATP) solutions that defend against sophisticated malware, persistent threats, and ransomware are available for the SRX5000 line. Two versions are available: Juniper ATP Cloud, a SaaS-based service, and the Juniper ATP Appliance, an on-premises solution.

Feature	Feature Description	Benefits
Advanced malware detection and remediation	Malware analysis and sandboxing are based on machine learning and behavioral analysis.	Protects enterprise users from a spectrum of malicious attacks, including advanced malware that exploits "zero-day" vulnerabilities.
Comprehensive threat feeds (C2, GeoIP, custom)	Curated, actionable threat intelligence feeds are delivered in near real time to SRX Series devices.	Proactively blocks malware communication channels and protects from botnets, phishing, and other attacks.
Encrypted Traffic Insights	SRX Series firewalls collect relevant TLS/SSL connection data, including certificates used, cipher suites negotiated, and connection behavior. This information is processed by Juniper ATP Cloud, which uses network behavioral analysis and machine learning to determine whether the connection is benign or malicious. Policies configured on SRX Series firewalls can be used to block encrypted traffic identified as malicious.	Restores visibility that was lost due to encryption without the heavy burden of full TLS/SSL decryption.
HTTP, HTTPs, e-mail	Web- and e-mail-based threats are analyzed, including encrypted sessions.	Protects users from all major threat vectors, including e-mail. Provides flexible message handling options for e-mail. The Juniper ATP Appliance includes support for cloud-based e-mail services such as Office 365 and Google Mail, and detects threats in SMB traffic.
Integration with Security Director and JSA	Juniper Networks Secure Analytics portfolio (JSA Series) security information and event management (SIEM) can consume and correlate threat events. Juniper ATP Cloud is also fully integrated with Security Director for provisioning and monitoring. The Juniper ATP Appliance includes a built-in management console and is not integrated with Security Director.	Single pane-of-glass management with Security Director and JSA Series integration delivers a simplified policy application and monitoring experience.

More information about Juniper Advanced Threat Prevention products can be found at https://www.juniper.net/us/en/products/security/advanced-threat-prevention.html.

Centralized Management

Juniper Networks® Security Director is the central manager for all SRX Series Services Gateways. It provides security policy management for all physical, logical, and virtual firewalls through an innovative, intuitive, and centralized web-based interface that offers enforcement across emerging and traditional threat vectors. It provides detailed visibility into application performance, reduces risk while enabling users to diagnose, and it resolves problems quickly. More information about Juniper Networks Security Director can be found at https://www.juniper.net/us/en/products/security/security-director-network-security-management.html.

SRX5400 Services Gateway | SRX5600 Services Gateway | SRX5800 Services Gateway

Specifications

Note: Performance, capacity, and features are measured under ideal lab testing conditions. Actual results may vary based on Junos OS release and by deployment.

	SRX5400	SRX5600	SRX5800
Maximum Performance and Capacity[1]			
Junos OS version tested	Junos OS 21.2	Junos OS 21.2	Junos OS 21.2
Firewall Performance, IMIX	480 Gbps per IOC4	480 Gbps per IOC4	480 Gbps per IOC4
Maximum performance per chassis	960 Gbps	1440 Tbps	3.36 Tbps
Next-Generation Firewall Performance	100 Gbps	210 Gbps	400 Gbps
Latency (stateful firewall)	~11µsec	~11µsec	~11µsec
IPsec VPN AES-256-GCM (IMIX)	140 Gbps	280 Gbps	530 Gbps
Maximum IPS performance	230 Gbps	460 Gbps	860 Gbps
Maximum concurrent sessions	91 Million	182 Million	338 Million
New sessions/second (sustained, tcp, 3way, firewall NAT)	1.7/1 million	3.4/2 Million	6.3/4 Million
Maximum users supported	Unrestricted	Unrestricted	Unrestricted
Network Connectivity			
IOC4 options (SRX5K-IOC4-MRAT; SRX5K-IOC4-10G)	40x10GbE SFP+ or 12xQSFP+/QSFP28 multirate		
IOC3 options (SRX5K-MPC3-100G10G; SRX5K-MPC3-40G10G)	2x100GbE CFP2 and 4x10GbE SFP+ or 6x40GbE QSFP+ and 24x10GbE SFP+		
Firewall			
Network attack detection	Yes	Yes	Yes
DoS and distributed denial of service (DDoS) protection	Yes	Yes	Yes
TCP reassembly for fragmented packet protection	Yes	Yes	Yes
Brute force attack mitigation	Yes	Yes	Yes
SYN cookie protection	Yes	Yes	Yes
Zone-based IP spoofing	Yes	Yes	Yes
Malformed packet protection	Yes	Yes	Yes
IPsec VPN			
Site-to-site tunnels	15,000	15,000	15,000
Tunnel interfaces	15,000	15,000	15,000
Number of remote access / SSL VPN (concurrent) users	25,000	40,000	50,000
Tunnels	Site-to-Site, Hub and Spoke, Dynamic Endpoint, AutoVPN, ADVPN, Group VPN (IPv4 / IPv6 / Dual Stack)		
Internet Key Exchange	IKEv1, IKEv2		
Configuration Payload	Yes	Yes	Yes
IKE Authentication Algorithms	MD5, SHA1, SHA-256, SHA-384, SHA-512		

	SRX5400	SRX5600	SRX5800
IKE Encryption Algorithms	Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, SuiteB		
Authentication	Pre-shared key and public key infrastructure (PKI X.509)		
IPsec (Internet Protocol Security)	Authentication Header (AH) / Encapsulating Security Payload (ESP) protocol		
Perfect forward secrecy	Yes		
IPsec Authentication Algorithms	hmac-md5, hmac-sha-196, hmac-sha-256, hmac-sha-384, hmac-sha-512		
IPsec Encryption Algorithms	Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, SuiteB		
Monitoring	Standard-based Dead peer detection (DPD), VPN monitoring		
Prevent replay attack	Yes	Yes	Yes
VPNs (GRE, IP-in-IP, MPLS)	Yes	Yes	Yes
Redundant VPN gateways	Yes	Yes	Yes
Intrusion Prevention System (IPS)			
Signature-based and customizable (via templates)	Yes	Yes	Yes
Active/active traffic monitoring	Yes	Yes	Yes
Stateful protocol signatures	Yes	Yes	Yes
Attack detection mechanisms	Stateful signatures, protocol anomaly detection (zero-day coverage), application identification	Stateful signatures, protocol anomaly detection (zero-day coverage), application identification	Stateful signatures, protocol anomaly detection (zero-day coverage), application identification
Attack response mechanisms	Drop connection, close connection, session packet log, session summary, e-mail	Drop connection, close connection, session packet log, session summary, e-mail	Drop connection, close connection, session packet log, session summary, e-mail
Attack notification mechanisms	Structured system logging	Structured system logging	Structured system logging
Worm protection	Yes	Yes	Yes
Simplified installation through recommended policies	Yes	Yes	Yes
Trojan protection	Yes	Yes	Yes
Spyware/adware/keylogger protection	Yes	Yes	Yes
Advanced malware protection	Yes	Yes	Yes
Protection against attack proliferation from infected systems	Yes	Yes	Yes
Reconnaissance protection	Yes	Yes	Yes
Request and response side attack protection	Yes	Yes	Yes
Compound attacks—combines stateful signatures and protocol anomalies	Yes	Yes	Yes
Custom attack signatures creation	Yes	Yes	Yes
Contexts accessible for customization	600+	600+	600+
Attack editing (port range, other)	Yes	Yes	Yes
Stream signatures	Yes	Yes	Yes
Protocol thresholds	Yes	Yes	Yes
Stateful protocol signatures	Yes	Yes	Yes
Frequency of updates	Daily and emergency	Daily and emergency	Daily and emergency
Content Security			
Antivirus	Yes	Yes	Yes
Content filtering	Yes	Yes	Yes
Enhanced Web filtering	Yes	Yes	Yes
Redirect Web filtering	Yes	Yes	Yes
Antispam	Yes	Yes	Yes
AppSecure			
AppTrack (application visibility and tracking)	Yes	Yes	Yes
AppFirewall (policy enforcement by application name)	Yes	Yes	Yes
AppQoS (network traffic prioritization by application name)	Yes	Yes	Yes
User-based application policy enforcement	Yes	Yes	Yes
GPRS Security			
GPRS stateful firewall	Yes	Yes	Yes

	SRX5400	SRX5600	SRX5800
Destination Network Address Translation			
Destination NAT with Port Address Translation (PAT)	Yes	Yes	Yes
Destination NAT within same subnet as ingress interface IP	Yes	Yes	Yes
Destination addresses and port numbers to one single address and a specific port number (M:1P)	Yes	Yes	Yes
Destination addresses to one single address (M:1)	Yes	Yes	Yes
Destination addresses to another range of addresses (M:M)	Yes	Yes	Yes
Source Network Address Translation			
Static Source NAT—IP-shifting Dynamic Internet Protocol (DIP)	Yes	Yes	Yes
Source NAT with PAT—port translated	Yes	Yes	Yes
Source NAT without PAT—fix port	Yes	Yes	Yes
Source NAT—IP address persistency	Yes	Yes	Yes
Source pool grouping	Yes	Yes	Yes
Source pool utilization alarm	Yes	Yes	Yes
Source IP outside of the interface subnet	Yes	Yes	Yes
Interface source NAT—interface DIP	Yes	Yes	Yes
Oversubscribed NAT pool with fallback to PAT when the address pool is exhausted	Yes	Yes	Yes
Symmetric NAT	Yes	Yes	Yes
Allocate multiple ranges in NAT pool	Yes	Yes	Yes
Proxy Address Resolution Protocol (ARP) for physical port	Yes	Yes	Yes
Source NAT with loopback grouping—DIP with loopback grouping	Yes	Yes	Yes
User Authentication and Access Control			
Built-in (internal) database	Yes	Yes	Yes
RADIUS accounting	Yes	Yes	Yes
Web-based authentication	Yes	Yes	Yes
Public Key Infrastructure (PKI) Support			
PKI certificate requests (PKCS 7, PKCS 10, and CMPv2)	Yes	Yes	Yes
Automated certificate enrollment (SCEP)	Yes	Yes	Yes
Certificate authorities supported	Yes	Yes	Yes
Self-signed certificates	Yes	Yes	Yes
Virtualization			
Maximum custom routing instances with data plane separation	2000	2000	2000
Maximum security zones	2000	2000	2000
Maximum virtual firewalls with data plane and administrative separation (logical/tenant systems)	500	500	500
Additional off-platform virtual firewall option with Juniper Networks vSRX Virtual Firewall (VM based)	Unlimited	Unlimited	Unlimited
Maximum number of VLANs	4096	4096	4096
Routing			
BGP instances	1000	1000	1000
BGP peers	2000	2000	2000
BGP routes	1 Million	1 Million	1 Million
OSPF instances	400	400	400
OSPF routes	1 Million	1 Million	1 Million
RIP v1/v2 instances	50	50	50
RIP v2 table size	30,000	30,000	30,000
Dynamic routing	Yes	Yes	Yes
Static routes	Yes	Yes	Yes
Source-based routing	Yes	Yes	Yes
Policy-based routing	Yes	Yes	Yes
Equal cost multipath (ECMP)	Yes	Yes	Yes

	SRX5400	SRX5600	SRX5800
Reverse path forwarding (RPF)	Yes	Yes	Yes
Multicast	Yes	Yes	Yes
IPv6			
Firewall/stateless filters	Yes	Yes	Yes
Dual-stack IPv4/IPv6 firewall	Yes	Yes	Yes
RIPng	Yes	Yes	Yes
BFD, BGP	Yes	Yes	Yes
ICMPv6	Yes	Yes	Yes
OSPFv3	Yes	Yes	Yes
Class of service (CoS)	Yes	Yes	Yes
Mode of Operation			
Layer 2 (transparent) mode	Yes	Yes	Yes
Layer 3 (route and/or NAT) mode	Yes	Yes	Yes
IP Address Assignment			
Static	Yes	Yes	Yes
Dynamic Host Configuration Protocol (DHCP)	Yes	Yes	Yes
Internal DHCP server	Yes	Yes	Yes
DHCP relay	Yes	Yes	Yes
Traffic Management Quality of Service (QoS)			
Maximum bandwidth	Yes	Yes	Yes
RFC2474 IP Diffserv in IPv4	Yes	Yes	Yes
Firewall filters for CoS	Yes	Yes	Yes
Classification	Yes	Yes	Yes
Scheduling	Yes	Yes	Yes
Shaping	Yes	Yes	Yes
Intelligent Drop Mechanisms (WRED)	Yes	Yes	Yes
Three-level scheduling	Yes	Yes	Yes
Weighted round robin for each level of scheduling	Yes	Yes	Yes
Priority of routing protocols	Yes	Yes	Yes
Traffic management/policing in hardware	Yes	Yes	Yes
High Availability (HA)			
Active/passive, active/active	Yes	Yes	Yes
Unified in-service software upgrade (unified ISSU)	Yes	Yes	Yes
Configuration synchronization	Yes	Yes	Yes
Session synchronization for firewall and IPsec VPN	Yes	Yes	Yes
Session failover for routing change	Yes	Yes	Yes
Device failure detection	Yes	Yes	Yes
Link and upstream failure detection	Yes	Yes	Yes
Dual control links	Yes	Yes	Yes
Interface link aggregation/Link Aggregation Control Protocol (LACP)	Yes	Yes	Yes
Redundant fabric links	Yes	Yes	Yes
Management			
WebUI (HTTP and HTTPS)	Yes	Yes	Yes
Command line interface (console, telnet, SSH)	Yes	Yes	Yes
Junos Space Security Director	Yes	Yes	Yes

	SRX5400	SRX5600	SRX5800
Administration			
Local administrator database support	Yes	Yes	Yes
External administrator database support	Yes	Yes	Yes
Restricted administrative networks	Yes	Yes	Yes
Root admin, admin, and read-only user levels	Yes	Yes	Yes
Software upgrades	Yes	Yes	Yes
Configuration rollback	Yes	Yes	Yes
Logging/Monitoring			
Structured syslog	Yes	Yes	Yes
SNMP (v2 and v3)	Yes	Yes	Yes
Traceroute	Yes	Yes	Yes
Certifications			
Safety certifications	Yes	Yes	Yes
Electromagnetic Compatibility (EMC) certifications	Yes	Yes	Yes
RoHS2 Compliant (European Directive 2011/65/EU)	Yes	Yes	Yes
NIST FIPS-140-2 Level 2	Yes	Yes	Yes
Common Criteria NDPP+TFFW EP + VPN EP	Yes	Yes	Yes
USGv6	Yes	Yes	Yes
Dimensions and Power			
Dimensions (W x H x D)	17.45 x 8.7 x 24.5 in (44.3 x 22.1 x 62.2 cm)	17.5 x 14 x 23.8 in (44.5 x 35.6 x 60.5 cm)	17.5 x 27.8 x 23.5 in (44.5 x 70.5 x 59.7 cm)
Weight	Fully configured 128 lb (58.1 kg)	Fully Configured: 180 lb (81.7 kg)	Fully Configured: 334 lb (151.6 kg)
Power supply (AC)	100 to 240 VAC	100 to 240 VAC	200 to 240 VAC
Power supply (DC)	-40 to -60 VDC	-40 to -60 VDC	-40 to -60 VDC
Maximum power	4,100 watts (AC high capacity)	4,100 watts (AC high capacity)	8,200 watts (AC high capacity)
Typical Power	1540 watts	2440 watts	5015 watts
Environmental			
Operating temperature – long term	41° to 104° F (5° to 40° C)	41° to 104° F (5° to 40° C)	41° to 104° F (5° to 40° C
Humidity – long term	5% to 85% noncondensing	5% to 85% noncondensing	5% to 85% noncondensing
Humidity – short term	5% to 93% noncondensing but not to exceed 0.026 kg water/kg of dry air	5% to 93% noncondensing but not to exceed 0.026 kg water/kg of dry air	5% to 93% noncondensing but not to exceed 0.026 kg water/kg of dry air

[1] Performance, capacity and features listed are measured under ideal testing conditions. Actual results may vary based on Junos OS releases and by deployments.

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit https://www.juniper.net/us/en/products.html.

Ordering Information

To order Juniper Networks SRX Series Services Gateways, and to access software licensing information, please visit the How to Buy page at https://www.juniper.net/us/en/how-to-buy/form.html.

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

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™