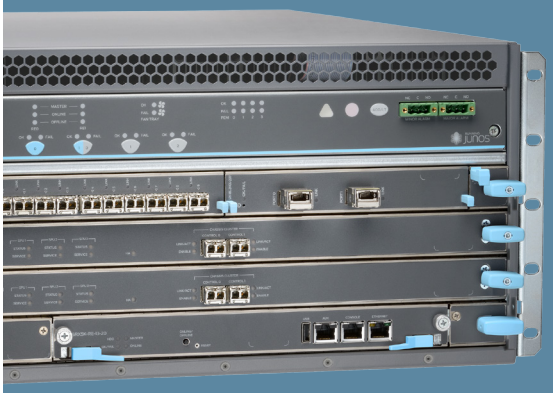


SRX5400, SRX5600, AND SRX5800 SERVICES GATEWAYS

Product Overview

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

Product Description

The Juniper Networks® SRX5400, SRX5600, and SRX5800 Services Gateways are next-generation security platforms based on a revolutionary architecture that provides market-leading performance, scalability, and service 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

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) enabling a fully equipped SRX5800 to support up to 300 Gbps 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 to interfaces, where each platform can be equipped with a flexible number of input/output cards (IOCs) that offer a wide range of connectivity options—from 1GbE to 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. With this flexibility, the SRX5800 can be configured to support more than 400GbE ports, or 220 10GbE, 22 100GbE, or 44 40GbE ports.

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 realization of maximum processing and I/O capability available in any particular configuration. This level of scalability and flexibility facilitates 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. By combining the routing heritage of Junos OS and the security heritage of ScreenOS®, the SRX Series is equipped with a robust list of services that include firewall, intrusion prevention system (IPS), denial of service (DoS), application security, VPN (IPsec), Network Address Translation (NAT), unified threat management (UTM), and quality of service (QoS). In addition to the benefit of individual services, incorporating multiple security and networking services within one OS greatly optimizes the flow of traffic through the platform. Network traffic no longer needs to be routed across multiple data paths/cards or even disparate operating systems within a single gateway.

Junos OS also delivers carrier-class reliability to the already redundant SRX Series. 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 300 Gbps firewall, 100 million concurrent sessions, 100 Gbps IPS, and 450,000 connections per second. Equipped with the full range of security services, SRX5800 is ideally suited for securing large enterprise, hosted or co-located data centers, service provider core and cloud provider infrastructures, and mobile operator environments. The massive performance, scalability, and flexibility of the SRX5800 makes it ideal for densely consolidated processing environments, and the service density make 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 130 Gbps firewall and 60 Gbps IPS. The SRX5600 is ideally suited for securing enterprise data centers as well as aggregation of various security solutions. The capability to support unique security policies per zones and its ability to scale with the growth of the network infrastructure makes 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 IOCII and SPCII and can support up to 65 Gbps firewall and 22 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 capability 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

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, drastically reducing management overhead and complexity. The same SPCs are supported on both SRX5600 and SRX5800 Services Gateways.

Juniper offers the SPCII, a newer SPC with superior performance and scale. The SPCII also features in-service software and in-service hardware upgrades to ensure that security is always on. The SPCII is supported on the SRX5400, SRX5600, and SRX5800 Services Gateways.

Input Output Cards

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 to meet the needs of the most demanding environments.

Juniper offers the IOCII, a newer card with superior connectivity options. The IOCII offers the industry's first 100GbE as well as 40GbE and high-density 10GbE connectivity options. These options reduce the need for link aggregation when connecting high throughput switches to the firewall, as well as enabling increased throughput in the firewall itself. The IOCII is supported on all three platforms in the SRX5000 line of services gateways.

Features and Benefits

Networking and Security

Juniper Networks SRX5000 line 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 the Dynamic Services Architecture.	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 using dedicated high availability interfaces.	Achieve 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 1, 10, 40, and 100GbE) to meet the port density requirements of demanding network environments.
Network segmentation	Security zones, virtual LANs (VLANs), and virtual routers that 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 routing engine that 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.
AppSecure	Tightly integrated services on Junos OS including multi-gigabit application firewall, IPS, DoS, application traffic control, and other networking and security services.	Unmatched integration ensuring network security against all level of attacks.
Stateful GPRS inspection	Support for GPRS firewall in mobile operator networks.	Enables the SRX5000 line to provide stateful firewall capabilities for protecting key GPRS nodes within mobile operator networks.
User identity-based access control enforcement	Secure access to data center resources via tight integration of standards-based access control capabilities of Juniper Networks Junos Pulse Access Control Service and SRX5000 line.	Enables agent-based and agentless identity security services for enterprise data centers by integrating the SRX5000 line with the standards-based access control capabilities of Junos Pulse Access Control Service. This integration enables administrative flexibility to manage a variety of user access, including corporate, guest, and mobile.
Unified threat management (UTM)	Strong UTM capabilities, including IPS, antivirus, antispam, Web, and content filtering. Available on-box with preinstalled, expanding and adaptive capabilities that are quickly activated for zero-day, easy, and instant protection. Antivirus options are available from Sophos and Kaspersky, Web filtering from Websense, and antispam from Sophos.	Best-in-class UTM protection with strong, high-performance content security leveraging intelligence from multiple expert security companies.
I/O card II	The first firewall I/O card in the industry to offer 100GbE connectivity. The card includes a choice of ten 10GbE, two 40GbE, or one 100GbE I/O interfaces. Pairs well with SPCIIs for maximized firewall performance in any of the SRX5000 line of gateways.	Increases connectivity efficiency with high throughput I/O interfaces. Reduces the need for link aggregation to the firewall and enables higher firewall throughput.
SPC card II	Enables performance and scale with full, backwards compatibility to SRX5000 chassis and cards. Like current SPCs, 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, IKE, and IPsec.	Enables IT administrative time and cost savings with easy, no-touch deployment for IPsec VPN networks.

Traffic Inspection Methods

Juniper Networks SRX Series Services Gateways support various detection methods to accurately identify the application and traffic flow through the network.

Feature	Feature Description	Benefits
Application identification	Identifies applications and tunneled applications independent of protocol and port numbers.	Granular control over application traffic through smart FW policies.
Protocol anomaly detection	Protocol usage against published RFCs is verified to detect any violations or abuse.	Proactively protect network from undiscovered vulnerabilities.
Traffic anomaly detection	Heuristic rules detect unexpected traffic patterns that may suggest reconnaissance or attacks.	Proactively prevent reconnaissance activities or block distributed denial of service (DDoS) attacks.
IP spoofing detection	The validity of allowed addresses inside and outside the network are checked.	Permit only authentic traffic while blocking disguised source.
DoS detection	Protection against SYN flood, IP, ICMP, and application attacks.	Protect your key network assets from being overwhelmed by denial of service attacks.

Unified Threat Management Capabilities

Juniper Networks unified threat management (UTM) assures the highest level of network security with best-in-class protection and high-performance content security leveraging intelligence from multiple expert security companies. Juniper UTM includes AppSecure, IPS, antivirus, antispam, Web filtering, and content filtering.

AppSecure

Juniper Networks AppSecure is a suite of next-generation security capabilities that utilize advanced application identification and classification to deliver greater visibility, enforcement, control and protection over the network.

Feature	Feature Description	Benefits
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	Set prioritization of traffic based on application information and contexts.	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.
AppDoS	Multi-stage detection methods used to identify and mitigate targeted attacks from disrupting critical applications and services.	Identifies attacking botnet traffic against legitimate client traffic to prevent distributed denial of service attacks targeting applications.
Application signatures	More than 900 signatures for identifying applications and nested applications.	Applications are accurately identified and the resulting information can be used for visibility, enforcement, control and protection.
SSL inspection	Inspection of HTTP traffic encrypted in SSL on any TCP/UDP port.	Combined with application identification, provides visibility and protection against threats embedded in SSL encrypted traffic.

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.	Minimize false positives and offer flexible signature development.
Protocol decodes	More than 65 protocol decodes are supported along with more than 500 contexts to enforce proper usage of protocols.	Accuracy of signatures are improved through precise contexts of protocols.
Signatures	There are more than 8,500 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.	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 UTM Capabilities

The UTM services offered on the SRX5000 line of 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.
Integrated Web filtering	Enhanced Web filtering includes extensive category granulation (90+ categories) and a real-time threat score delivered with Websense, 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 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.

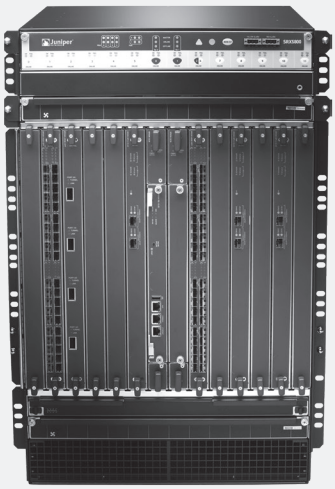
Centralized Management

Juniper Networks Junos Space Security Director delivers scalable and responsive security management that improves the reach, ease, and accuracy of security policy administration. It lets administrators manage all phases of the security policy lifecycle through a single Web-based interface, accessible via standard browsers. Junos Space Security Director centralizes application identification, firewall, IPS, NAT, and VPN security management for intuitive and quick policy administration.

Junos Space Security Director runs on the Junos Space Network Management Platform for highly extensible, network-wide management functionality, including ongoing access to Juniper and third-party Junos Space ecosystem innovations.

SRX5400
Services Gateway

SRX5600
Services Gateway



SRX5800
Services Gateway

Note: We are updating the branding on the SRX5000 line of products. The SRX5400 will ship with a carbon grey interface and current Juniper logo, however current line cards ordered will ship in the blue style faceplates at FRS. We are actively migrating all line cards over to carbon gray in mid 2014.

Specifications

	SRX5400	SRX5600	SRX5800
Maximum Performance and Capacity[1]			
Junos OS version tested	Junos OS 12.1X46	Junos OS 12.1X46	Junos OS 12.1X46
Firewall performance (max)	65 Gbps	130 Gbps	300 Gbps
Firewall performance (IMIX)	30 Gbps	65 Gbps	130 Gbps
Firewall packets per second (64 bytes)	9.8 Mpps	20 Mpps	50 Mpps
Maximum AES256+SHA-1 VPN performance	43 Gbps	75 Gbps	150 Gbps
Maximum 3DES+SHA-1 VPN performance	43 Gbps	75 Gbps	150 Gbps
Maximum IPS performance	22 Gbps	50 Gbps	100 Gbps
Maximum AppFW performance	50 Gbps	80 Gbps	160 Gbps
Maximum concurrent sessions	28 Million	100 Million	100 Million
New sessions/second (sustained, tcp, 3way)	450,000	450,000	450,000
Maximum security policies	80,000	80,000	80,000
Maximum user supported	Unrestricted	Unrestricted	Unrestricted
Network Connectivity			
Maximum available slots for IOCs	2	5	11
LAN interface options	10 x 10-Gigabit Ethernet IOCII 2 x 40-Gigabit Ethernet IOCII 1 x 100-Gigabit Ethernet IOCII	40 x 1-Gigabit Ethernet SFP 4 x 10-Gigabit Ethernet XFP (SR or LR) 16 x 1-Gigabit Ethernet Flex IOC 4 x 10-Gigabit Ethernet XFP Flex IOC	40 x 1- Gigabit Ethernet SFP 4 x 10-Gigabit Ethernet XFP (SR or LR) 16 x 1-Gigabit Ethernet Flex IOC 4 x 10-Gigabit Ethernet XFP Flex IOC
Processing Scalability			
Maximum available slots for SPCs	2	5	11
SPC options	SPCII: Quad CPU with 128 GB memory	SPC: Dual CPU with 8 GB memory SPCII: Quad CPU with 128 GB memory	SPC: Dual CPU with 8 GB memory SPCII: Quad CPU with 128 GB memory
Firewall			
Network attack detection	Yes	Yes	Yes
DoS and 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
DES (56-bit), 3DES (168-bit), and AES encryption	Yes	Yes	Yes
MD5 and SHA-1 authentication	Yes	Yes	Yes
Manual key, IKE, PKI (X.509)	Yes	Yes	Yes
Perfect forward secrecy (DH groups)	1, 2, 5	1, 2, 5	1, 2, 5
Prevent replay attack	Yes	Yes	Yes
Remote access VPN	Yes	Yes	Yes
IPv4 and IPv6	Yes	Yes	Yes
Redundant VPN gateways	Yes	Yes	Yes

[1] Performance, capacity and features listed are based on systems running Junos OS 12.1X44 and are measured under ideal testing conditions. Actual results may vary based on Junos OS releases and by deployments.

Specifications (continued)

	SRX5400	SRX5600	SRX5800
Intrusion Prevention System			
Modes of operation: In-line and in-line tap	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, email	Drop connection, close connection, session packet log, session summary, email	Drop connection, close connection, session packet log, session summary, email
Attack notification mechanisms	Structured syslog	Structured syslog	Structured syslog
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
Other malware protection	Yes	Yes	Yes
Application denial of service 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
Create custom attack signatures	Yes	Yes	Yes
Access contexts for customization	500+	500+	500+
Attack editing (port range, other)	Yes	Yes	Yes
Stream signatures	Yes	Yes	Yes
Protocol thresholds	Yes	Yes	Yes
Stateful protocol signatures	Yes	Yes	Yes
Approximate number of attacks covered	8,000+	8,000+	8,000+
Detailed threat descriptions and remediation/patch info	Yes	Yes	Yes
Create and enforce appropriate application-usage policies	Yes	Yes	Yes
Attacker and target audit trail and reporting	Yes	Yes	Yes
Frequency of updates	Daily and emergency	Daily and emergency	Daily and emergency
GPRS Security			
GPRS stateful firewall	Yes	Yes	Yes
GTP tunnels	1,000,000	1,000,000	1,000,000
Destination Network Address Translation			
Destination NAT with 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

Specifications (continued)

	SRX5400	SRX5600	SRX5800
Source Network Address Translation			
Static Source NAT - IP-shifting 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 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 and PKCS 10)	Yes	Yes	Yes
Automated certificate enrollment (SCEP)	Yes	Yes	Yes
Certificate authorities supported	Yes	Yes	Yes
Self-signed certificates	Yes	Yes	Yes
Virtualization			
Maximum number of security zones	2,000	2,000	2,000
Maximum number of virtual routers	2,000	2,000	2,000
Maximum number of VLANs	4,096	4,096	4,096
Logical Systems	32	32	32
Routing			
BGP instances	1,000	1,000	1,000
BGP peers	2,000	2,000	2,000
BGP routes	1,000,000[2]	1,000,000[2]	1,000,000[2]
OSPF instances	400	400	400
OSPF routes	1,000,000[2]	1,000,000[2]	1,000,000[2]
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
Reverse path forwarding (RPF)	Yes	Yes	Yes
Multicast	No	Yes	Yes

[2] Maximum number of BGP and OSPF routes recommended is 100,000.

Specifications (continued)

	SRX5400	SRX5600	SRX5800
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	Yes	Yes	Yes
Mode of Operation			
Layer 2 (transparent) mode	No	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
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
In-Service Software Upgrade (ISSU)[3]	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	No	Yes	Yes
Interface link aggregation/LACP	Yes	Yes	Yes
Redundant data and control links[4]	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

[3] Please check the technical publication documents and release notes for the list of compatible features for ISSU.
[4] To enable dual control links on the SRX5000 line, two SRX5K-RE-13-20 modules must be installed on each cluster member.

Specifications (continued)

	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
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)	3,180 watts (AC standard capacity) 4,100 watts (AC high capacity)	5,100 watts (AC standard capacity) 8,200 watts (AC high capacity)
Certifications			
Safety certifications	Yes	Yes	Yes
Electromagnetic Compatibility (EMC) certifications	Yes	Yes	Yes
Designed for NEBS Level 3	Yes	Yes	Yes
NIST FIPS-140-2 Level 2	No	Yes (with Junos OS 10.4R4)	Yes (with Junos OS 10.4R4)
ISO Common Criteria NDPP+TFFW EP	No	Yes (with Junos OS 12.1x44)	Yes (with Junos OS 12.1x44)
ICSA Network Firewall	No	Yes	Yes
ICSA IPsec	No	Yes	Yes
USGv6	No	Yes (with Junos OS 11.4R1)	Yes (with Junos OS 11.4R1)
3GPP TS 20.060 Compliance[5]			
R6: 3GPP TS 29.060 version 6.21.0	Yes	Yes	Yes
R7: 3GPP TS 29.060 version 7.3.0	Yes	Yes	Yes
R8: 3GPP TS 29.060 version 8.3.0	Yes	Yes	Yes
Environmental			
Operating temperature – long term	41º to 104º F (5º to 40º C)	41º to 104º F (5º to 40º C)	41º to 104º F (5º to 40º C)
Operating temperature – short term[6]	23º to 131º F (-5º to 55º C)	23º to 131º F (-5º to 55º C)	23º to 131º F (-5º to 55º C)
Humidity – long term	5% to 85% noncondensing	5% to 85% noncondensing	5% to 85% noncondensing
Humidity – short term[6]	5% to 93% noncondensing but not to exceed 0.026kg water/kg of dry air	5% to 93% noncondensing but not to exceed 0.026kg water/kg of dry air	5% to 93% noncondensing but not to exceed 0.026kg water/kg of dry air

[5] SRX5000 line of gateways operating with Junos OS release 10.0 and later are compliant with the R6, R7, and R8 releases of 3GPP TS 20.060 with the following exceptions (not supported on the SRX5000 line):
- Section 7.5A Multimedia Broadcast and Multicast Services (MBMS) messages
- Section 7.5B Mobile Station (MS) info change messages
- Section 7.3.12 Initiate secondary PDP context from GGSN

[6] Short term is not greater than 96 consecutive hours, and not greater than 15 days in 1 year

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 **www.juniper.net/us/en/products-services**.

Ordering Information

Model Number	Description
Base/Bundle	
SRX5400BB-AC	SRX5400 base bundle includes Chassis, Routing Engine (RE), SCB, two AC HC power supplies, SRX5K-SPC-4-15-320, SRX5K-MPC, and SRX-MIC-10XG-SFPP
SRX5400BB-DC	SRX5400 base bundle includes Chassis, RE, SCB, two DC HC power supplies, SRX5K-SPC-4-15-320, SRX5K-MPC, and SRX-MIC-10XG-SFPP
SRX5400B2-AC	SRX5400 bundle 2 includes Chassis, RE, SCB, two AC HC power supplies, two SRX5K-SPC-4-15-320, SRX5K-MPC, and SRX-MIC-10XG-SFPP
SRX5400B2-DC	SRX5400 bundle 2 includes Chassis, RE, SCB, two DC HC power Supplies, two SRX5K-SPC-4-15-320, SRX5K-MPC, and SRX-MIC-10XG-SFPP
SRX5600BASE-HC-AC	AC SRX5600 chassis, includes RE, SCB, 2 AC high capacity power supplies
SRX5600BASE-HC-DC	DC SRX5600 chassis, includes RE, SCB, 2 DC high capacity power supplies
SRX5800BASE-HC-AC	AC SRX5800 chassis, includes RE, 2xSCB, 2 AC high capacity power supplies
SRX5800BASE-HC-DC	DC SRX5800 chassis, includes RE, 2xSCB, 2x high capacity DC power supplies

SRX5000 Line Components		Compatible Systems
SRX5K-SCB	SCB SRX5000 line Switch Control Board	SRX5400 SRX5600 SRX5800
SRX5K-RE-13-20	SRX5000 line Routing Engine, 1.3 GHz, 2 GB DRAM	SRX5400 SRX5600 SRX5800
SRX5K-SPC-4-15-320	SRX5000 line Next-Generation Service Processing Card (featuring 20 million sessions)	SRX5400 SRX5600 SRX5800
SRX5K-SPC-2-10-40	SRX5000 line Service Processing Card	SRX5600 SRX5800
SRX5K-4XGE-XFP	4x10 Gigabit XFP Ethernet I/O Card for the SRX5000 line, no transceivers	SRX5600 SRX5800
SRX5K-40GE-SFP	40x1 Gigabit SFP Ethernet I/O Card for the SRX5000 line, no transceivers	SRX5600 SRX5800
SRX5K-FPC-IOC	SRX5000 line Flex IOC	SRX5600 SRX5800 Supports 2 Flex IOC modules
SRX-IOC-16GE-TX	SRX5000 line Flex IOC 16-port 10/100/1000 Ethernet module	Flex IOC module for SRX5k-FPC-IOC SRX5600 SRX5800
SRX-IOC-16GE-SFP	SRX5000 line Flex IOC 16-port SFP Ethernet module, no transceivers	Flex IOC module for SRX5k-FPC-IOC SRX5600 SRX5800
SRX-IOC-4XGE-XFP	SRX5000 line Flex IOC 4x10 Gigabit XFP Ethernet module, no transceivers	Flex IOC module for SRX5k-FPC-IOC SRX5600 SRX5800

Model Number	Description	
SRX5000 Line Components (continued)		Compatible Systems
SRX5K-IOC-BLANK	Blank Panel for SRX5K-FPC-IOC	SRX5600 SRX5800
SRX5K-MPC	MPC for 100GbE, 40GbE, 10GbE MIC Interfaces	SRX5400 SRX5600 SRX5800 Supports 2 MIC modules
SRX-MIC-1X100G-CFP	MIC with 1x100GbE CFP Interface MIC module for SRX5k-MPC	SRX5400 SRX5600 SRX5800
SRX-MIC-2X40G-QSFP	MIC with 2x40GbE QSFP+ Interfaces MIC module for SRX5k-MPC	SRX5400 SRX5600 SRX5800
SRX-MIC-10XG-SFPP	MIC with 10x10GbE SFP+ Interfaces MIC module for SRX5k-MPC	SRX5400 SRX5600 SRX5800
Transceivers		
SRX-SFP-1GE-LH	Small form factor pluggable 1000BASE-LH Gigabit Ethernet optic module	SRX5600 SRX5800
SRX-SFP-1GE-LX	Small form-factor pluggable 1000BASE-LX Gigabit Ethernet Optic Module	SRX5600 SRX5800
SRX-SFP-1GE-SX	Small form-factor pluggable 1000BASE-SX Gigabit Ethernet Optic Module	SRX5600 SRX5800
SRX-SFP-1GE-T	Small form-factor pluggable 1000BASE-T Gigabit Ethernet Module (uses Cat 5 cable)	SRX5600 SRX5800
SRX-XFP-10GE-SR	10-Gigabit Ethernet pluggable transceiver, short reach multimode	SRX5600 SRX5800
SRX-XFP-10GE-LR	10-Gigabit Ethernet pluggable transceiver, 10 Km, single mode	SRX5600 SRX5800
SRX-XFP-10GE-ER	10-Gigabit Ethernet pluggable transceiver, 40 Km, single mode	SRX5600 SRX5800
SRX-CFP-100G-LR4	100GbE LR4 CFP transceiver (IEEE 802.3ba) Transceiver for SRX-MIC-1X100G-CFP	SRX5400 SRX5600 SRX5800
SRX-CFP-100G-SR10	100GbE SR10 CFP transceiver, MMF,100M,OM3 Transceiver for SRX-MIC-1X100G-CFP	SRX5400 SRX5600 SRX5800
SRX-QSFP-40G-SR4	40GbE SR4 QSFP+ transceiver Transceiver for SRX-MIC-2X40G-QSFP	SRX5400 SRX5600 SRX5800
SRX-SFPP-10G-SR-ET	10GbE SR SFP+ transceiver, 200M ET 0-85 Transceiver for SRX-MIC-10XG-SFPP	SRX5400 SRX5600 SRX5800

Ordering Information (continued)

Model Number	Description
AppSecure Subscription	
SRX5400-APPSEC-1	One year subscription for Application Security and IPS updates for SRX5400
SRX5400-APPSEC-3	Three year subscription for Application Security and IPS updates for SRX5400
SRX5400-APPSEC-5	Five year subscription for Application Security and IPS updates for SRX5400
SRX5600-APPSEC-A-1	One year subscription for Application Security and IPS updates for SRX5600
SRX5600-APPSEC-A-3	Three year subscription for Application Security and IPS updates for SRX5600
SRX5800-APPSEC-A-1	One year subscription for Application Security and IPS updates for SRX5800
SRX5800-APPSEC-A-3	Three year subscription for Application Security and IPS updates for SRX5800

Services Offload License		Compatible Systems
SRX5K-SVCS-OFFLOAD-RTU	Services offload license for SRX5000 line; this is not an annual license subscription	SRX5600 SRX5800

Logical Systems License	
SRX-5400-LSYS-1	1 incremental Logical Systems License for SRX5400
SRX-5400-LSYS-5	5 incremental Logical Systems License for SRX5400
SRX-5400-LSYS-25	25 incremental Logical Systems License for SRX5400
SRX-5600-LSYS-1	1 incremental Logical Systems License for SRX5600
SRX-5600-LSYS-5	5 incremental Logical Systems License for SRX5600
SRX-5600-LSYS-25	25 incremental Logical Systems License for SRX5600
SRX-5800-LSYS-1	1 incremental Logical Systems License for SRX5800
SRX-5800-LSYS-5	5 incremental Logical Systems License for SRX5800
SRX-5800-LSYS-25	25 incremental Logical Systems License for SRX5800

Model Number	Description
IPS Subscription	
SRX5K-IDP	One year IPS signature subscription
SRX5K-IDP-3	Three year IPS signature subsciption
Power Cords	
CBL-M-PWR-RA-AU	AC power cord, Australia (SAA/3/15), C19, 15 A/250 V, 2.5 m, Right Angle
CBL-M-PWR-RA-CH	AC power cord, China (GB 2099.1-1996, Angle), C19, 16 A/250 V, 2.5 m, Right Angle
CBL-M-PWR-RA-EU	AC power cord, Cont. Europe (VII), C19, 16 A/250 V, 2.5 m, Right Angle
CBL-M-PWR-RA-IT	AC power cord, Italy (I/3/16), C19, 16 A/250 V, 2.5 m, Right Angle
CBL-M-PWR-RA-JP	AC power cord, Japan (NEMA LOCKING), C19, 20 A/250 V, 2.5 m, Right Angle
CBL-M-PWR-RA-TWLK-US	AC power cord, US (NEMA LOCKING), C19, 20 A/250 V, 2.5 m, Right Angle
CBL-M-PWR-RA-UK	AC power cord, UK (BS89/13), C19, 13 A/250 V, 2.5 m, Right Angle
CBL-M-PWR-RA-US	AC power cord, USA/Canada (N6/20), C19, 20 A/250 V, 2.5 m, Right Angle
CBL-PWR-RA-JP15	AC power cable, JIS 8303 15 A/125 V 2.5 m length for Japan, Right Angle
CBL-PWR-RA-TWLK-US15	AC power cable, NEMA L5-15P (twist lock) 15 A/125 V 2.5 m length for U.S., Canada, and Mexico, Right Angle
CBL-PWR-RA-US15	AC power cable, NEMA 5-15 15 A/125 V, 2.5 m length for North America, parts of South America, parts of Central America, parts of Africa, and parts of Asia, Right Angle

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
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

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at +1-866-298-6428 or authorized reseller.

1000254-014-EN Dec 2013 Printed on recycled paper