



SRX5600 AND SRX5800 SERVICES GATEWAYS

Product Overview

Juniper Networks SRX5000 line of services gateways is the next-generation solution for securing the ever increasing network infrastructure and applications requirements for both enterprise and service provider environments. Designed from the ground up to provide flexible processing scalability, I/O scalability, and services integration, the SRX5000 line can meet the network and security requirements of data center hyper-consolidation, rapid managed services deployments, and aggregation of security solutions. Incorporating the routing heritage and service provider reliability of Junos OS with the rich security heritage of ScreenOS. The SRX Series also offers the high feature/service integration necessary to secure modern network infrastructure and applications.

Product Description

The Juniper Networks® SRX5600 and SRX5800 Services Gateways are next-generation security platforms based on a revolutionary new 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
- Securing mobile operator environments
- Managed service providers
- Securing core service provider infrastructure
- Large enterprise data centers
- Aggregation of departmental and segmented security solutions

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 (SPC) enabling a fully equipped SRX5800 to support more than 150 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). 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 400 Gigabit Ethernet ports or 88 10-Gigabit Ethernet 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, Network Address Translation (NAT), 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, single release train, 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 150 Gbps firewall, 26 Gbps IPS and 380,000 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 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 70 Gbps firewall and 12 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.

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.

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 (either Gigabit Ethernet or 10-Gigabit Ethernet). 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.

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.
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 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.

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.

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.
AppFW	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.

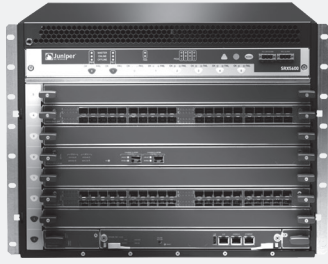
Feature	Feature Description	Benefits
Stateful signature inspection	Signatures are applied only to relevant portions of the network traffic determined by the appropriate protocol context.	Minimize false positives and offer flexible signature development.
Protocol decodes	More than 65 protocol decodes 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 ¹	There are more than 6,700 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.

Centralized Management

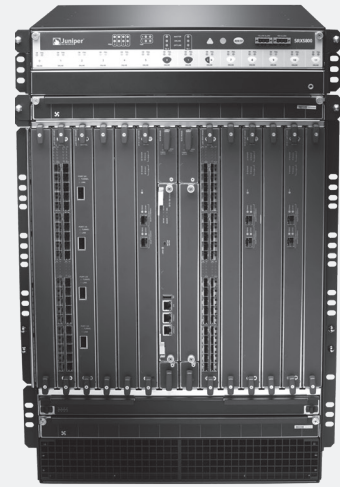
Juniper Networks Junos® Space Security Design delivers scalable and responsive security management that improves the reach, ease, and accuracy of security policy administration. It lets administrators manage all phases of the security policy lifecycle through a single Web-based interface, accessible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

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

¹ As of December 2011, there are 6,700 signatures with approximately 70 new signatures added monthly. Subscription to signature update service is required to receive new signatures.



SRX5600 Services Gateway



SRX5800 Services Gateway

Specifications

	SRX5600	SRX5800
--	---------	---------

Maximum Performance and Capacity²

Tested configuration to achieve performance, capacities and features listed below:
 SRX5600 chassis equipped with four (4) SPCs and two (2) IOCs
 SRX5800 chassis equipped with eight (8) SPCs and four (4) IOCs

	SRX5600	SRX5800
Junos OS version tested	Junos OS 11.4R1	Junos OS 11.4R1
Firewall performance (max)	70 Gbps	150 Gbps
Firewall performance (IMIX)	17.5 Gbps	37.5 Gbps
Firewall packets per second (64 bytes)	7 Mpps	15 Mpps
Maximum AES256+SHA-1 VPN performance	15 Gbps	30 Gbps
Maximum 3DES+SHA-1 VPN performance	16 Gbps	32 Gbps
Maximum IPS performance	12 Gbps	26 Gbps
Maximum AppFW performance	50 Gbps	100 Gbps
Maximum concurrent sessions	9 Million	12.5/20 Million ³
New sessions/second (sustained, tcp, 3way)	380,000	380,000
Maximum security policies	80,000	80,000
Maximum user supported	Unrestricted	Unrestricted

Network Connectivity

	SRX5600	SRX5800
Maximum available slots for IOCs	5	11
LAN interface options	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

	SRX5600	SRX5800
Maximum available slots for SPCs	5	11
SPC options	Dual CPU with 8 GB total memory	Dual CPU with 8 GB total memory

² Performance, capacity and features listed are based on systems running Junos OS 11.4R1 and are measured under ideal testing conditions. Actual results may vary based on Junos OS releases and by deployments.

³ To achieve more than 12.5M CP sessions on SRX5800, use software knob available from 10.4 or 11.4 and later.

Specifications (continued)

	SRX5600	SRX5800
Firewall		
Network attack detection	Yes	Yes
DoS and DDoS protection	Yes	Yes
TCP reassembly for fragmented packet protection	Yes	Yes
Brute force attack mitigation	Yes	Yes
SYN cookie protection	Yes	Yes
Zone-based IP spoofing	Yes	Yes
Malformed packet protection	Yes	Yes
IPsec VPN		
Site-to-site tunnels	15,000	15,000
Tunnel interfaces	15,000	15,000
DES (56-bit), 3DES (168-bit), and AES encryption	Yes	Yes
MD5 and SHA-1 authentication	Yes	Yes
Manual key, IKE, PKI (X.509)	Yes	Yes
Perfect forward secrecy (DH groups)	1, 2, 5	1, 2, 5
Prevent replay attack	Yes	Yes
Remote access VPN	Yes	Yes
Redundant VPN gateways	Yes	Yes
Intrusion Prevention System		
Modes of operation: In-line and in-line tap	Yes	Yes
Active/active traffic monitoring	Yes	Yes
Stateful protocol signatures	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
Attack response mechanisms	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
Worm protection	Yes	Yes
Simplified installation through recommended policies	Yes	Yes
Trojan protection	Yes	Yes
Spyware/adware/keylogger protection	Yes	Yes
Other malware protection	Yes	Yes
Application denial of service protection	Yes	Yes
Protection against attack proliferation from infected systems	Yes	Yes
Reconnaissance protection	Yes	Yes
Request and response side attack protection	Yes	Yes
Compound attacks—combines stateful signatures and protocol anomalies	Yes	Yes
Create custom attack signatures	Yes	Yes
Access contexts for customization	500+	500+
Attack editing (port range, other)	Yes	Yes
Stream signatures	Yes	Yes
Protocol thresholds	Yes	Yes
Stateful protocol signatures	Yes	Yes
Approximate number of attacks covered	6,000+	6,000+
Detailed threat descriptions and remediation/patch info	Yes	Yes
Create and enforce appropriate application-usage policies	Yes	Yes
Attacker and target audit trail and reporting	Yes	Yes
Frequency of updates	Daily and emergency	Daily and emergency

Specifications (continued)

	SRX5600	SRX5800
GPRS Security		
GPRS stateful firewall	Yes	Yes
GTP tunnels	1,000,000	1,000,000
Destination Network Address Translation		
Destination NAT with PAT	Yes	Yes
Destination NAT within same subnet as ingress interface IP	Yes	Yes
Destination addresses and port numbers to one single address and a specific port number (M:IP)	Yes	Yes
Destination addresses to one single address (M:1)	Yes	Yes
Destination addresses to another range of addresses (M:M)	Yes	Yes
Source Network Address Translation		
Static Source NAT - IP-shifting DIP	Yes	Yes
Source NAT with PAT - port-translated	Yes	Yes
Source NAT without PAT - fix-port	Yes	Yes
Source NAT - IP address persistency	Yes	Yes
Source pool grouping	Yes	Yes
Source pool utilization alarm	Yes	Yes
Source IP outside of the interface subnet	Yes	Yes
Interface source NAT - interface DIP	Yes	Yes
Oversubscribed NAT pool with fallback to PAT when the address pool is exhausted	Yes	Yes
Symmetric NAT	Yes	Yes
Allocate multiple ranges in NAT pool	Yes	Yes
Proxy ARP for physical port	Yes	Yes
Source NAT with loopback grouping - DIP with loopback grouping	Yes	Yes
User Authentication and Access Control		
Built-in (internal) database	Yes	Yes
RADIUS accounting	Yes	Yes
Web-based authentication	Yes	Yes
Public Key Infrastructure (PKI) Support		
PKI certificate requests (PKCS 7 and PKCS 10)	Yes	Yes
Automated certificate enrollment (SCEP)	Yes	Yes
Certificate authorities supported	Yes	Yes
Self-signed certificates	Yes	Yes
Virtualization		
Maximum number of security zones	2,000	2,000
Maximum number of virtual routers	2,000	2,000
Maximum number of VLANs	4,096	4,096
Logical Systems	32	32
Routing		
BGP instances	128	128
BGP peers	2,000	2,000
BGP routes	1,000,000*	1,000,000*
OSPF instances	400	400
OSPF routes	1,000,000*	1,000,000*
RIP v1/v2 instances	50	50
RIP v2 table size	30,000	30,000
Dynamic routing	Yes	Yes

* Maximum number of BGP and OSPF routes recommended is 100,000.

Specifications (continued)

	SRX5600	SRX5800
Routing (continued)		
Static routes	Yes	Yes
Source-based routing	Yes	Yes
Policy-based routing	Yes	Yes
Equal cost multipath (ECMP)	Yes	Yes
Reverse path forwarding (RPF)	Yes	Yes
Multicast	Yes	Yes
IPv6		
Firewall/stateless filters	Yes	Yes
Dual stack IPv4/IPv6 firewall	Yes	Yes
RIPng	Yes	Yes
BFD, BGP	Yes	Yes
ICMPv6	Yes	Yes
OSPFv3	Yes	Yes
Class of service	Yes	Yes
Mode of Operation		
Layer 2 (transparent) mode	Yes	Yes
Layer 3 (route and/or NAT) mode	Yes	Yes
IP Address Assignment		
Static	Yes	Yes
Dynamic Host Configuration Protocol (DHCP)	Yes	Yes
Internal DHCP server	Yes	Yes
DHCP relay	Yes	Yes
Traffic Management Quality of Service (QoS)		
Maximum bandwidth	Yes	Yes
RFC2474 IP Diffserv in IPv4	Yes	Yes
Firewall filters for COS	Yes	Yes
Classification	Yes	Yes
Scheduling	Yes	Yes
Shaping	Yes	Yes
Intelligent Drop Mechanisms (WRED)	Yes	Yes
Three level scheduling	Yes	Yes
Weighted round robin for each level of scheduling	Yes	Yes
Priority of routing protocols	Yes	Yes
Traffic management/policing in hardware	Yes	Yes
High Availability (HA)		
Active/passive, active/active	Yes	Yes
In-Service Software Upgrade (ISSU)*	Yes	Yes
Configuration synchronization	Yes	Yes
Session synchronization for firewall and IPsec VPN	Yes	Yes
Session failover for routing change	Yes	Yes
Device failure detection	Yes	Yes
Link and upstream failure detection	Yes	Yes
Dual control links	Yes	Yes
Interface link aggregation/LACP	Yes	Yes
Redundant data and control links**	Yes	Yes

* Please check the technical publication documents and release notes for the list of compatible features for ISSU.

** To enable dual control links on the SRX5000 line, two SRX5K-RE-13-20 modules must be installed on each cluster member.

Specifications (continued)

	SRX5600	SRX5800
Management		
WebUI (HTTP and HTTPS)	Yes	Yes
Command line interface (console)	Yes	Yes
Command line interface (telnet)	Yes	Yes
Command line interface (SSH)	Yes	Yes
Junos Space Security Design	Yes	Yes
Administration		
Local administrator database support	Yes	Yes
External administrator database support	Yes	Yes
Restricted administrative networks	Yes	Yes
Root admin, admin, and read only user levels	Yes	Yes
Software upgrades	Yes	Yes
Configuration rollback	Yes	Yes
Logging/Monitoring		
Structured syslog	Yes	Yes
SNMP (v2)	Yes	Yes
Traceroute	Yes	Yes
Dimensions and Power		
Dimensions (W x H x D)	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: 180 lb / 81.7 kg	Fully Configured: 334 lb / 151.6 kg
Power supply (AC)	100 to 240 VAC	200 to 240 VAC
Power supply (DC)	-40 to -60 VDC	-40 to -60 VDC
Maximum power draw	2,800 watts	5,100 watts
Certifications		
Safety certifications	Yes	Yes
Electromagnetic Compatibility (EMC) certifications	Yes	Yes
NEBS Level 3	Yes	Yes
Security Certifications		
Common Criteria : EAL3	Yes	Yes
3GPP TS 20.060 Compliance*		
R6: 3GPP TS 29.060 version 6.21.0	Yes	Yes
R7: 3GPP TS 29.060 version 7.3.0	Yes	Yes
R8: 3GPP TS 29.060 version 8.3.0	Yes	Yes
Operating temperature	32° to 104° F 0° to 40° C	32° to 104° F 0° to 40° C
Humidity	5% to 90% noncondensing	5% to 90% noncondensing

* 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

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 Systems	
SRX5600BASE-AC	AC SRX5600 chassis, includes RE, SCB, 2 AC power supplies
SRX5600BASE-DC	DC SRX5600 chassis, includes RE, SCB, 2 DC power supplies
SRX5800BASE-AC	AC SRX5800 chassis, includes RE, 2xSCB, 3 AC power supplies
SRX5800BASE-DC	DC SRX5800 chassis, includes RE, 2xSCB, 2 DC power supplies
SRX5800BASE-HC-AC	HC AC SRX5800 chassis, includes RE, 2xSCB, 2x HC AC, 2x HC fan

SRX5000 Line Components

SRX5K-SCB	SCB SRX5000 line Switch Control Board
SRX5K-RE-13-20	SRX5000 line Routing Engine, 1.3 GHz, 2 GB DRAM
SRX5K-SPC-2-10-40	SRX5000 line Service Processing Card
SRX5K-4XGE-XFP	4x10 Gigabit XFP Ethernet I/O Card for the SRX5000 line, no transceivers
SRX5K-40GE-SFP	40x1 Gigabit SFP Ethernet I/O Card for the SRX5000 line, no transceivers
SRX5K-FPC-IOC	SRX5000 line Flex IOC – supports two pluggable port modules
SRX-IOC-16GE-TX	SRX5000 line Flex IOC 16-port 10/100/1000 Ethernet module
SRX-IOC-16GE-SFP	SRX5000 line Flex IOC 16-port SFP Ethernet module, no transceivers
SRX-IOC-4XGE-XFP	SRX5000 line Flex IOC 4x10 Gigabit XFP Ethernet module, no transceivers
SRX5K-IOC-BLANK	Blank Panel for SRX5K-FPC-IOC

Transceivers

SRX-SFP-1GE-LH	Small form factor pluggable 1000BASE-LH Gigabit Ethernet optic module
SRX-SFP-1GE-LX	Small form-factor pluggable 1000BASE-LX Gigabit Ethernet Optic Module
SRX-SFP-1GE-SX	Small form-factor pluggable 1000BASE-SX Gigabit Ethernet Optic Module
SRX-SFP-1GE-T	Small form-factor pluggable 1000BASE-T Gigabit Ethernet Module (uses Cat 5 cable)
SRX-XFP-10GE-SR	10-Gigabit Ethernet pluggable transceiver, short reach multimode
SRX-XFP-10GE-LR	10-Gigabit Ethernet pluggable transceiver, 10 Km, single mode
SRX-XFP-10GE-ER	10-Gigabit Ethernet pluggable transceiver, 40 Km, single mode

AppSecure Subscription

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

SRX5K-SVCS-OFFLOAD-RTU	Services offload license for SRX5000 line; this is not an annual license subscription
------------------------	---

Model Number	Description
Logical Systems License	
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

IPS Subscription

SRX5K-IDP	One year IPS signature subscription
SRX5K-IDP-3	Three year IPS signature subscription
SRX5K-IDP-3-R	Three year IPS signature subscription renewal
SRX5K-IDP-R	One year IPS signature subscription renewal

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 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

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

Copyright 2012 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.