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 from Layer 3 to Layer 7, these platforms feature a carrier-grade next-generation firewall and advanced security services such as application security, unified threat management (UTM), intrusion prevention system (IPS), and integrated threat intelligence services.

For advanced protection, the SRX Series offers integrated threat intelligence services via Juniper Networks Sky Advanced Threat Prevention (ATP), Juniper's open threat intelligence platform in the cloud. Juniper Sky ATP delivers actionable security intelligence to SRX Series devices to enable advanced protection against Command and Control (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 Junos® Space 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 1.2 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 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), unified threat management (UTM), 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 1.2 Tbps firewall throughput and latency as low as 32 microseconds for stateful firewall. The SRX5800 also supports 1 Tbps IPS and 395 million concurrent sessions. Equipped with the full range of advanced security services, the SRX5800 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 570 IMIX Gbps firewall throughput, 180 million concurrent sessions, and 460 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 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 285 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 (SPC)

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 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.

Juniper offers the IOC2, a second-generation card with superior connectivity options. The IOC2 offers 100GbE as well as 40GbE and high-density 10GbE and 1GbE 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 IOC2 is supported on all three platforms in the SRX5000 line of services gateways.

The third generation of IOCs from Juniper, the IOC3, delivers the highest throughput levels yet, along with superior connectivity options including 100GbE, 40GbE, and high-density 10GbE interfaces. The IOC2 or IOC3 operates with the Express Path optimization capability, delivering higher levels of throughput—up to an industry-leading 2 Tbps on the SRX5800. The IOC3 cards are supported on the SRX5400, SRX5600, and SRX5800.

Routing Engine (RE2) and Enhanced System Control Board (SCB3)

The SRX5K-RE-1800X4 Routing Engine (RE2) is the latest in the family of REs for the SRX5000 line with a multicore processor running at 1800 MHz. It delivers improved performance, scalability, and reliability with 16 GB DRAM and 128 GB solid-state drive (SSD). The SRX5K-SCB3 Enhanced System Control Board (SCB3) enables 240 Gbps per slot throughput with intra as well as interchassis high availability and 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.
Threat intelligence	Integration with Juniper Sky ATP for application of advanced threat detection technologies and feeds for policy enforcement.	Offers policy enforcement based on optimized and up-to-date threat intelligence, which is automatically syndicated across the firewall estate, enabling higher security effectiveness and operational efficiency.
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.
Intrusion prevention system (IPS)	Detects known and unknown exploits and anomalies in network traffic streams.	Adds a critical layer of protection beyond stateful firewall, enabling detection of vulnerabilities in network traffic and highly granular control over IPS policy enforcement.

Feature	Feature Description	Benefits
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.
User identity-based access control enforcement	Secure access to data center resources via the tight integration of standards-based access control capabilities in 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 categories, 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 and Web filtering options are available from Sophos; Web filtering is available from Forcepoint.	Provides best-in-class UTM protection with strong, high-performance content security leveraging intelligence from multiple expert security companies.
IOC2 supporting 2 MICs	The first firewall I/O card in the industry to offer 100GbE connectivity. The card includes a choice of ten 10GbE, twenty 1GbE, two 40GbE, or one 100GbE I/O interfaces. Pairs well with SPC2s for maximized firewall performance in any of the SRX5000 line of Services Gateways.	Increases connectivity efficiency with high throughput I/O interfaces. Reduces the need for link aggregation to the firewall and enables higher firewall throughput.
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 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.
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.
Express Path	An optional optimization capability (formerly Services Offload) for the SRX5000 line that improves throughput and lowers latency by identifying and accelerating traffic flows that do not require deep inspection. Provides support for single, high-bandwidth flows of 40 Gbps and 100 Gbps. Can be configured on a per-policy basis.	Securely delivers extremely high levels of throughput, making it the ideal solution for high-speed, latency-sensitive networks and applications, as well as high-performance compute networks.
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.

*Requires Junos OS 15.1x49-D10 or greater.
**Requires Junos OS 18.2R1-S1 or greater.

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 UTM Capabilities

The UTM 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 Sky ATP, 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 (C&C, 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.
HTTP, HTTPs, e-mail	Web- and e-mail-based threats are analyzed, including encrypted sessions.	Users are protected 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 Junos Space Security Director and JSA SIEM	Juniper Networks Secure Analytics portfolio (JSA Series) security information and event management (SIEM) can consume and correlate threat events. Juniper Sky ATP is also fully integrated with Junos Space 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 Sky ATP can be found at www.juniper.net/us/en/products-services/security/sky-advanced-threat-prevention/. Additional information about the Juniper ATP Appliance can be found at www.juniper.net/us/en/products-services/security/advanced-threat-prevention-appliance/.

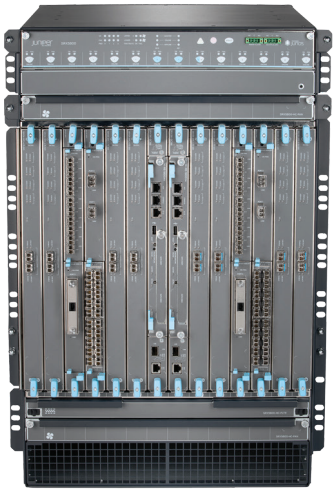
Centralized Management

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 life cycle 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.

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

Specifications

	SRX5400	SRX5600	SRX5800
Maximum Performance and Capacity[1]			
Junos OS version tested	Junos OS 18.2	Junos OS 18.2	Junos OS 18.2
Firewall performance, IMIX	285 Gbps	570 Gbps	1.2 Tbps
Firewall performance	65 Gbps	130 Gbps	320 Gbps
Latency (stateful firewall)	~32µsec	~32µsec	~32µsec
AES256+SHA-1 IMIX VPN performance	60 Gbps	120 Gbps	260 Gbps
Maximum IPS performance	230 Gbps	460 Gbps	1000 Gbps
Maximum concurrent sessions	90 Million	180 Million	395 Million
New sessions/second (sustained, tcp, 3way)	1.75 million	3.5 Million	7.5 Million
Maximum user supported	Unrestricted	Unrestricted	Unrestricted
Network Connectivity			
Maximum available slots for IOCs	2	5	11
IOC3 options (SRX5K-MPC3-100G10G; SRX5K-MPC3-40G10G)	2x100GbE CFP2 and 4x10GbE SFP+ or 6x40GbE QSFP+ and 24x10GbE SFP+		
IOC2 options (SRX5K-MPC)	Supports 2 pluggable MIC modules per card. MICs can be mixed from the following models: 20 x 1GbE SFP (SRX-MIC-20GE-SFP) 10 x 10GbE SFP+ (SRX-MIC-10XG-SFPP) 2 x 40GbE QSFP (SRX-MIC-2X40G-QSFP) 1 x 100GbE CFP (SRX-MIC-1X100G-CFP)		
Processing Scalability			
Maximum available slots for SPCs	2	5	8
Services Process Card (SPC) options	SPC3: Quad 14 core Intel CPU complexes	SPC3: Quad 14 core Intel CPU complexes	SPC3: Quad 14 core Intel CPU complexes

[1] Performance, capacity and features listed are based on systems running Junos OS 18.2R1 and are measured under ideal testing conditions. Actual results may vary based on Junos OS releases and by deployments.

	SRX5400	SRX5600	SRX5800
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
DES (56-bit), 3DES (168-bit), and AES encryption	Yes	Yes	Yes
MD5, SHA-1, and SHA-2 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
IPv4 and IPv6	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

* Session capacity differs based on UTM/AppSecure/IPS features enabled.

	SRX5400	SRX5600	SRX5800
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
Approximate number of attacks covered	15,000+	15,000+	15,000+
Detailed threat descriptions and remediation/patch information	Yes	Yes	Yes
Appropriate application-usage policies created and enforced	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
UTM*			
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
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

* Session capacity differs based on UTM/AppSecure/IPS features enabled.

	SRX5400	SRX5600	SRX5800
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 virtual firewalls with data plane traffic segregation (logical systems/tenants)	2,000	2,000	2,000
Maximum security zones	2,000	2,000	2,000
Maximum virtual firewalls with data plane and administrative separation (logical systems)	32	32	32
Additional off-platform virtual firewall option with Juniper Networks vSRX Virtual Firewall (VM based)	Unlimited	Unlimited	Unlimited
Maximum number of VLANs	4,096	4,096	4,096
Routing			
BGP instances	1,000	1,000	1,000
BGP peers	2,000	2,000	2,000
BGP routes	1 Million[3]	1 Million[3]	1 Million[3]
OSPF instances	400	400	400
OSPF routes	1 Million[3]	1 Million[3]	1 Million[3]
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	Yes	Yes	Yes
IPv6			
Firewall/stateless filters	Yes	Yes	Yes
Dual stack IPv4/IPv6 firewall	Yes	Yes	Yes

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

	SRX5400	SRX5600	SRX5800
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)[4]	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[5]	No	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

[4] Please consult the technical publication documents and release notes for a list of compatible ISSU features.
[5] To enable dual control links on the SRX5000 line, two SRX5K-RE-1800X4 modules must be installed on each cluster member.

	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
Third-Generation Partnership Project (3GPP) TS 20.060 Compliance[6]			
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
Certifications			
Safety certifications	Yes	Yes	Yes
Electromagnetic Compatibility (EMC) certifications	Yes	Yes	Yes
RoHS2 Compliant (European Directive 2011/65/EU)	Yes	Yes	Yes
Designed for NEBS Level 3	Yes	Yes	Yes
NIST FIPS-140-2 Level 2	Yes, Junos OS 12.3X48-D30	Yes, Junos OS 12.3X48-D30	Yes, Junos OS 12.3X48-D30
Common Criteria NDPP+TFFW EP + VPN EP	Yes, Junos OS 15.1X49-D60	Yes, Junos OS 15.1X49-D60	Yes, Junos OS 15.1X49-D60
USGv6	Yes (with Junos OS 12.1X48)	Yes, Junos OS 12.3X48)	Yes, Junos OS 12.3X48)
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)
Operating temperature – short term[7]	23° to 131° F (-5° to 55° C)	23° to 131° F (-5° to 55° C)	23° to 131° F (-5° to 55° C)
Humidity – long term	5% to 85% noncondensing	5% to 85% noncondensing	5% to 85% noncondensing
Humidity – short term[7]	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

[6] 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

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

Warranty

For warranty information, please visit www.juniper.net/support/warranty/.

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

Product Number	Description
Base/Bundle	
SRX5400E-B1-AC*	SRX5400 configuration 1 includes chassis, standard midplane, SRX5K-RE-1800X4, SRX5K-SCBE, 2xAC HC PEM, HC fan tray, SRX5K-SPC-4-15-320, SRX5K-MPC, and SRX-MIC-10XG-SFPP.
SRX5400E-B1-DC*	SRX5400 configuration 1 includes chassis, standard midplane, SRX5K-RE-1800X4, SRX5K-SCBE, 2xDC HC PEM, HC fan tray, SRX5K-SPC-4-15-320, SRX5K-MPC, and SRX-MIC-10XG-SFPP.
SRX5400E-B2-AC*	SRX5400 configuration 2 includes chassis, standard midplane, SRX5K-RE-1800X4, SRX5K-SCBE, 2xAC HC PEM, HC fan tray, 2xSRX5K-SPC-4-15-320, SRX5K-MPC, and SRX-MIC-10XG-SFPP.
SRX5400E-B2-DC*	SRX5400 configuration 2 includes chassis, standard midplane, SRX5K-RE-1800X4, SRX5K-SCBE, 2xDC HC PEM, HC fan tray, 2xSRX5K-SPC-4-15-320, SRX5K-MPC, and SRX-MIC-10XG-SFPP.
SRX5400E-B5-AC*	SRX5400E cluster bundle includes 2xSRX5400E-B1-AC (SCB2, RE2, 1xSPC2, 1xIOC2, 1x10GbE MIC, 2xAC PEMs), 4xSRX5600-PWR-2520-AC-S (extra redundant AC PEMS), and 2xSRX5400-APPSEC-1 (1 year).
SRX5400E-B5-DC*	SRX5400E cluster bundle includes 2xSRX5400E-B1-DC (SCB2, RE2, 1xSPC2, 1xIOC2, 1x10GbE MIC, 2xDC PEMs), 4xSRX5600-PWR-2400-DC-S (extra redundant DC PEMS), and 2xSRX5400-APPSEC-1 (1 year).
SRX5400X-B1**	SRX5400 configuration includes chassis, enhanced midplane, SRX5K-RE-1800X4, SRX5K-SCB3, 2xHC PEM, HC fan tray, SRX5K-SPC-4-15-320, SRX5K-MPC, SRX-MIC-10XG-SFPP.
SRX5400X-B2**	SRX5400 configuration includes chassis, enhanced midplane, SRX5K-RE-1800X4, SRX5K-SCB3, 2xHC PEM, HC fan tray, SRX5K-SPC-4-15-320, SRX5K-MPC3-40G10G.
SRX5400X-B3**	SRX5400 configuration includes chassis, enhanced midplane, SRX5K-RE-1800X4, SRX5K-SCB3, 2xHC PEM, HC fan tray, SRX5K-SPC-4-15-320, SRX5K-MPC3-100G10G.
SRX5400X-B5-AC	SRX5400X cluster bundle includes 2xSRX5400X-B1 (SCB3, RE2, 1xSPC2, 1xIOC2, 1x10GbE MIC, 2xAC PEMs), 4xSRX5600-PWR-2520-AC-S (extra redundant AC PEMS), and 2xSRX5400-APPSEC-1 (1 year).
SRX5400X-B5-DC	SRX5400X cluster bundle includes 2xSRX5400X-B1 (SCB3, RE2, 1xSPC2, 1xIOC2, 1x10GbE MIC, 2xDC PEMs), 4xSRX5600-PWR-2400-DC-S (extra redundant DC PEMS), and 2xSRX5400-APPSEC-1 (1 year).
SRX5400X-B6-AC	SRX5400X cluster bundle includes 2xSRX5400X-B1 (SCB3, RE2, 1xSPC2, 1xIOC2, 1x10GbE MIC, 2xAC PEMs), 4xSRX5600-PWR-2520-AC-S (extra redundant AC PEMS), and 2xSRX5400-APPSEC-1 (1 year).
SRX5400X-B6-DC	SRX5400X cluster bundle includes 2xSRX5400X-B1 (SCB3, RE2, 1xSPC2, 1xIOC2, 1x10GbE MIC, 2xDC PEMs), 4xSRX5600-PWR-2400-DC-S (extra redundant DC PEMS), and 2xSRX5400-APPSEC-1 (1 year).
SRX5400X-B7-AC	SRX5400X cluster bundle includes 2xSRX5400X-B1 (SCB3, RE2, 2xSPC2, 1xIOC2, 1x10GbE MIC, 2xAC PEMs), 4xSRX5600-PWR-2520-AC-S (extra redundant AC PEMS), and 2xSRX5400-APPSEC-1 (1 year).
SRX5400X-B7-DC	SRX5400X cluster bundle includes 2xSRX5400X-B1 (SCB3, RE2, 2xSPC2, 1xIOC2, 1x10GbE MIC, 2xDC PEMs), 4xSRX5600-PWR-2400-DC-S (extra redundant DC PEMS), and 2xSRX5400-APPSEC-1 (1 year).
SRX5600E-BASE-AC*	SRX5600 chassis includes standard midplane, SRX5K-RE-1800X4, SRX5K-SCBE, 2xAC HC PEM, HC fan tray.
SRX5600E-BASE-DC*	SRX5600 chassis includes standard midplane, SRX5K-RE-1800X4, SRX5K-SCBE, 2xDC HC PEM, HC fan tray.
SRX5600X-BASE**	SRX5600 configuration includes chassis, enhanced midplane, SRX5K-RE-1800X4, SRX5K-SCB3, 2xHC PEM, HC fan tray.
SRX5800E-BASE-AC*	SRX5800 chassis includes standard midplane, SRX5K-RE-1800X4, 2xSRX5K-SCBE, 2xAC HC PEM, 2xHC fan tray.
SRX5800E-BASE-DC*	SRX5800 chassis includes standard midplane, SRX5K-RE-1800X4, 2xSRX5K-SCBE, 2xDC HC PEM, 2xHC fan tray.
SRX5800X-BASE**	SRX5800 configuration includes chassis, enhanced midplane, SRX5K-RE-1800X4, 2xSRX5K-SCB3, 2xHC PEM, 2xHC fan tray.

SRX5000 Line Components

Product Number	Description	Compatible Systems
SRX5K-SCBE*	SRX5000 line enhanced Switch Control Board	SRX5400E SRX5600E SRX5800E
SRX5K-SCB3**	SRX5000 line SCB3 Switch Control Board	SRX5400X SRX5600X SRX5800X
SRX5K-RE-1800X4*	SRX5000 line RE, 1.8 GHz quad-core Xeon, 16 GB DRAM, 128 GB SSD	SRX5400E SRX5600E SRX5800E SRX5400X SRX5600X SRX5800X
SRX5K-SPC-4-15-320	SRX5000 line next-generation Services Processing Card (SCP) featuring 20 million sessions	All models
SRX-5K-BLANK	Blank panel for SRX5000 line	All models
SRX5K-MPC3-100G10G**	SRX5000 line IOC3, 2x100GbE and 4x10GbE port	SRX5400E SRX5600E SRX5800E SRX5400X SRX5600X SRX5800X
SRX5K-MPC3-40G10G**	SRX5000 line IOC3, 6x40GbE and 24x10GbE ports	SRX5400E SRX5600E SRX5800E SRX5400X SRX5600X SRX5800X
SRX5K-MPC	MPC for 100GbE, 40GbE, 10GbE, and 1GbE MIC Interfaces	All models; supports 2 MIC modules
SRX-MIC-1X100G-CFP	MIC with 1x100GbE CFP interface MIC module for SRX5K-MPC	All models

*These products require Junos OS 12.1X47-D15 or greater.
**Requires Junos OS 15.1X49-D10 or greater.

Product Number	Description	Compatible Systems
SRX-MIC-2X40G-QSFP	MIC with 2x40GbE QSFP+ interfaces MIC module for SRX5K-MPC	All models
SRX-MIC-10XG-SFPP	MIC with 10x10GbE SFP+ interfaces, MIC module for SRX5K-MPC	All models
SRX-MIC-20GE-SFP	MIC with 20x1GbE SFP interfaces, MIC module for SRX5K-MPC	All models

Transceivers

SRX-SFP-1GE-LH	Small form factor pluggable (SFP) 1000BASE-LH GbE optic module	SRX5K-MPC
SRX-SFP-1GE-LX	SFP 1000BASE-LX GbE optic module	SRX5K-MPC
SRX-SFP-1GE-SX	SFP 1000BASE-SX GbE optic module	SRX5K-MPC
SRX-SFP-1GE-T	SFP 1000BASE-T GbE module (uses Cat 5 cable)	SRX5K-MPC
SRX-SFP-10GE-LR	10GbE SFP+ optical transceiver, LR	SRX5K-MPC SRX5K-MPC3
SRX-SFP-10GE-SR	10GbE SFP+ optical transceiver, SR	SRX5K-MPC SRX5K-MPC3
SRX-CFP-100G-LR4	100GbE LR4 C form-factor pluggable transceiver (CFP) (IEEE 802.3ba) for SRX-MIC-1X100G-CFP	SRX5K-MPC
SRX-CFP-100G-SR10	100GbE SR10 CFP transceiver, MMF, 100M, OM3 for SRX-MIC-1X100G-CFP	SRX5K-MPC
SRX-QSFP-40G-SR4	40GbE SR4 quad small form-factor pluggable plus transceiver (QSFP+) transceiver for SRX-MIC-2X40G-QSFP	SRX5K-MPC SRX5K-MPC3
SRX-SFPP-10G-SR-ET	10GbE SR SFP+ transceiver, 200M ET 0-85	SRX5K-MPC SRX5K-MPC3
SRX-SFPP-10G-LR	10GbE SFP+ optical transceiver, LR	SRX5K-MPC SRX5K-MPC3
SRX-QSFP-40G-LR4	40GbE QSFP+ optical transceiver, LR	SRX5K-MPC SRX5K-MPC3
CFP2-100GBASE-SR10	CFP2 100GbE optical transceiver, SR	SRX5K-MPC3-100G10G
CFP2-100GBASE-LR4	CFP2 100GbE optical transceiver, LR	SRX5K-MPC3-100G10G
JNP-QSFP-40G-LX4	QSFP+ 40GBASE-LX4 40GbE transceiver, 100 m (150 m) with OM3 (OM4) duplex multimode fiber-optic (MMF) fiber	SRX5K-MPC, SRX5K-MPC3-40G10G

AppSecure Subscription

Product Number	Description
SRX5400-APPSEC-1	One year subscription for AppSecure and IPS updates for SRX5400, SRX5400E
SRX5400-APPSEC-3	Three year subscription for AppSecure and IPS updates for SRX5400, SRX5400E
SRX5400-APPSEC-5	Five year subscription for AppSecure and IPS updates for SRX5400, SRX5400E
SRX5600-APPSEC-A-1	One year subscription for AppSecure and IPS updates for SRX5600, SRX5600E
SRX5600-APPSEC-A-3	Three year subscription for AppSecure and IPS updates for SRX5600 , SRX5600E
SRX5600-APPSEC-A-5	Five year subscription for AppSecure and IPS updates for SRX5600, SRX5600E
SRX5800-APPSEC-A-1	One year subscription for AppSecure and IPS updates for SRX5800, SRX5800E
SRX5800-APPSEC-A-3	Three year subscription for AppSecure and IPS updates for SRX5800
SRX5800-APPSEC-A-5	Five year subscription for AppSecure and IPS updates for SRX5800, SRX5800E

IPS Subscription

SRX5K-IDP	One year IPS signature subscription for SRX5000 line
SRX5K-IDP-3	Three year IPS signature subscription for SRX5000 line
SRX5K-IDP-5	Five year IPS signature subscription for SRX5000 line

UTM Subscription

SRX5400-CS-BUN-1	One year subscription for AppSecure, IDP, EWF, AV, and antispam service on SRX5400, SRX5400E
SRX5400-CS-BUN-3	Three year subscription for AppSecure, IDP, EWF, AV, and antispam service on SRX5400, SRX5400E
SRX5400-CS-BUN-5	Five year subscription for AppSecure, IDP, EWF, AV, and antispam service on SRX5400, SRX5400E
SRX5400-S-AS-1	One year subscription for Juniper-Sophos antispam service on SRX5400, SRX5400E
SRX5400-S-AS-3	Three year subscription for Juniper-Sophos antispam service on SRX5400, SRX5400E
SRX5400-S-AS-5	Five year subscription for Juniper-Sophos antispam service on SRX5400, SRX5400E
SRX5400-S-AV-1	One year subscription for Juniper-Sophos AV service on SRX5400, SRX5400E
SRX5400-S-AV-3	Three year subscription for Juniper-Sophos AV service on SRX5400, SRX5400E
SRX5400-S-AV-5	Five year subscription for Juniper-Sophos AV service on SRX5400, SRX5400E
SRX5400-W-EWF-1	One year subscription for Juniper-Websense Enhanced Web Filtering service on SRX5400, SRX5400E
SRX5400-W-EWF-3	Three year subscription for Juniper-Websense Enhanced Web Filtering service on SRX5400, SRX5400E
SRX5400-W-EWF-5	Five year subscription for Juniper-Websense Enhanced Web Filtering service on SRX5400, SRX5400E
SRX5600-CS-BUN-1	One year subscription for AppSecure, IDP, EWF, AV, and antispam service on SRX5600, SRX5600E
SRX5600-S-AS-1	One year subscription for Juniper-Sophos antispam service on SRX5600, SRX5600E
SRX5600-S-AV-1	One year subscription for Juniper-Sophos AV service on SRX5600, SRX5600E
SRX5600-W-EWF-1	One year subscription for Juniper-Websense Enhanced Web Filtering service on SRX5600, SRX5600E
SRX5800-CS-BUN-1	One year subscription for AppSecure, IDP, EWF, AV, and antispam service on SRX5800, SRX5800E
SRX5800-S-AS-1	One year subscription for Juniper-Sophos antispam service on SRX5800, SRX5800E
SRX5800-S-AV-1	One year subscription for Juniper-Sophos AV service on SRX5800, SRX5800E
SRX5800-W-EWF-1	One year subscription for Juniper-Websense Enhanced Web Filtering service on SRX5800, SRX5800E

Product Number	Description
Advanced Threat Prevention Subscription	
SRX5400-ATP-1	Juniper Sky ATP, SRX5400, 1 year
SRX5400-ATP-3	Juniper Sky ATP, SRX5400, 3 year
SRX5400-ATP-5	Juniper Sky ATP, SRX5400, 5 year
SRX5600-ATP-1	Juniper Sky ATP, SRX5600, 1 year
SRX5600-ATP-3	Juniper Sky ATP, SRX5600, 3 year
SRX5600-ATP-5	Juniper Sky ATP, SRX5600, 5 year
SRX5800-ATP-1	Juniper Sky ATP, SRX5800, 1 year
SRX5800-ATP-3	Juniper Sky ATP, SRX5800, 3 year
SRX5800-ATP-5	Juniper Sky ATP, SRX5800, 5 year

Express Path (Formerly Service Offload License)*		Compatible Systems*
SRX5K-SVCS-OFFLOAD-RTU	Perpetual License	SRX5400 SRX5600 SRX5800

Logical Systems and Tenant Systems License	
SRX-5400-LSYS-1	1 incremental Logical Systems License for SRX5400, SRX5400E
SRX-5400-LSYS-5	5 incremental Logical Systems Licenses for SRX5400, SRX5400E
SRX-5400-LSYS-25	25 incremental Logical Systems Licenses for SRX5400, SRX5400E
SRX-5600-LSYS-1	1 incremental Logical Systems License for SRX5600
SRX-5600-LSYS-5	5 incremental Logical Systems Licenses for SRX5600, SRX5600E
SRX-5600-LSYS-25	25 incremental Logical Systems Licenses for SRX5600
SRX-5800-LSYS-1	1 incremental Logical Systems License for SRX5800, SRX5800E
SRX-5800-LSYS-5	5 incremental Logical Systems Licenses for SRX5800, SRX5800E
SRX-5800-LSYS-25	25 incremental Logical Systems Licenses for SRX5800, SRX5800E

* In 12.3X48-D10, the Services Offload feature was renamed Express Path and is included without requiring a license for Junos OS X48 releases and beyond. With the X48 release, the Express Path feature is supported on all SRX5000 Services Gateways including the SRX5400. For versions prior to the X48 release, the Services Offload license is still required and supports only SRX5600 and SRX5800 products.

Express Path is available on the SRX5400, SRX5600, and SRX5800 Services Gateways. No separate license required.

Product Number	Description
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 brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

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: +31.0.207.125.700

JUNIPER NETWORKS | Engineering Simplicity

EXPLORE JUNIPER
Get the App.
JUNIPER 1ON1
Available on the App Store
ANDROID APP ON Google Play

Copyright 2019 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos 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.