SRX3400 and SRX3600 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

Juniper Networks® SRX3400 Services Gateway and SRX3600 Services Gateway are next-generation security plaforms that deliver outstanding protection, market-leading performance, scalability and service integration in a mid-sized form factor. These devices are ideally suited for medium to large enterprise, public sector and service provider networks, including:

- Enterprise server farms/data centers
- Mobile operator environments
- Aggregation of departmental or segmented security solutions
- Cloud and hosting provider data centers
- Managed services deployments

In terms of security, these platforms feature next-generation firewall services such as application security, Unified Threat Management (UTM) and Intrusion Prevention System (IPS). Integrated threat intelligence via Spotlight Secure offers adaptive threat protection against command and control (C&C) related botnets, and policy enforcement based on GeoIP and attacker fingerprinting technology (the latter for Web application protection)—all of which are based on Juniper provided feeds. Customers may also leverage their own custom and third-party feeds for protection from advanced malware and other threats.

Based on an innovative mid-plane design and Juniper's dynamic services architecture, the SRX3000 line resets the bar in price/performance for enterprise and service provider environments. Each services gateway can support near linear scalability with each additional Services Processing Card (SPC), enabling the SRX3600 to support up to 55 Gbps of 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 in operation—maximizing hardware utilization.

Market leading flexibility and price/performance of the SRX3000 line comes from the modular architecture. Based on Juniper's dynamic services architecture, the gateway can be equipped with a flexible number of I/O cards (IOCs), network processing cards (NPCs) and service processing cards (SPCs)—allowing the system to be configured to support the ideal balance of performance and port density enabling each deployment of the Juniper Networks SRX Series Services Gateways to be tailored to specific network requirements. With this flexibility, the SRX3600 can be configured to support more than 100 Gbps interfaces with choices of Gigabit Ethernet or 10-Gigabit Ethernet ports; firewall performance up to 55 Gbps; and services processing to match specific business needs.

The switch fabric employed in the SRX3000 line enables the scalability of SPCs, NPCs, and IOCs. Supporting up to 320 Gbps of data transfer, the fabric enables the realization of maximum processing and I/O capability available in any particular configuration. This level of scalability and flexibility facilitates future expansion and growth of the network infrastructure, providing unrivaled investment protection.

The flexibility of the SRX3000 line extends beyond the innovation and proven benefit of the dynamic services architecture. Enabling the installation of SPCs on both the front and the back of the SRX3000 line, the mid-plane design delivers market-leading flexibility and scalability. By doubling the number of SPCs supported in half the rack space needed, the SRX3000 line offers not only underlying architectural innovation but also an innovative physical design.

The tight service integration on SRX Series Services Gateways 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 Services Gateways are equipped with a robust list of features that include firewall, intrusion prevention system (IPS), VPN (IPsec), denial of service (DoS), application security, Network Address Translation (NAT), unified threat management (UTM), and quality of service (QoS). In addition, incorporating multiple networking and security services under a single OS greatly optimizes the flow of traffic through the platform. With Junos OS, the SRX Series enjoys the benefit of a single source OS and one architecture that is also available across Juniper's carrier-class routers and switches.

SRX3600

The SRX3600 Services Gateway is a market-leading security solution supporting up to 55 Gbps firewall, 15 Gbps firewall and IPS, or 15 Gbps of IPsec VPN along with up to 270,000 new connections per second. Equipped with the full range of security services, the SRX3600 is ideally suited for securing medium to large enterprise data centers, hosted or co-located data centers, or securing next-generation enterprise services/applications. It can also be deployed to secure cloud provider infrastructures where multi-tenancy is a requirement or to secure mobile operator environments. The scalability and flexibility of the services gateway makes it ideal for consolidating legacy security appliances in densely populated data centers, and the service density makes it ideal for cloud or mobile providers.

SRX3400

The SRX3400 Services Gateway uses the same SPCs, IOCs and NPCs as the SRX3600 and can support up to 30 Gbps firewall, 8 Gbps firewall and IPS, or 8 Gbps of IPsec VPN, along with up to 150,000 new connections per second. The SRX3400 is ideally suited for securing and segmenting enterprise data centers/network infrastructure 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 makes the SRX3400 an ideal deployment for small to midsized server farms, hosting sites, or mobile operators.

SRX3000 Line Service Processing Cards*

As the "brains" behind the SRX3000 line, SPCs are designed to process all available services on the platform. By eliminating the need for dedicated hardware for specific services or capabilities, there are no instances in which any piece of hardware is taxed to the limit while other hardware sits idle. SPCs are designed to be pooled together, allowing the SRX3000 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 the SRX3600 and SRX3400. (Note: A minimum of one NPC and one SPC is required for proper system functionality.)

SRX3000 Line I/O Cards*

In addition to supporting an ideal mix of built-in copper, small form-factor pluggable transceiver (SFP) and high availability (HA) ports, the SRX3000 line allows the greatest I/O port density of any comparable offering in the same class. Each services gateway in the SRX3000 line can be equipped with one or several IOCs, each supporting either 16-gigabit interfaces (16 x 1 copper or fiber Gigabit Ethernet), or 20-gigabit interfaces (2 x 10 Gigabit XFP Ethernet). With the flexibility to provide multiple IOCs, the SRX3000 line can be equipped to support an ideal balance between interfaces and processing capabilities. (Note: A minimum of one NPC and one SPC is required for proper system functionality.)

SRX3000 Line Network Processing Cards*

To ensure maximum processing performance and flexibility, the SRX3000 line utilizes NPCs to distribute inbound and outbound traffic to the appropriate SPCs and IOCs, apply QoS, and enforce DoS/distributed denial of service (DDoS) protections. The SRX3600 can be configured to support one to three NPCs, while the SRX3400 can be configured to support one or two NPCs. Providing additional NPCs to the SRX3000 line allows organizations to tailor the solution to fit their specific performance requirements. (Note: A minimum of one NPC and one SPC is required for proper system functionality.)

In addition, the SRX3000 line also has a new combination NPC/IOC card, NP-IOC. This card expands the gateway's capacity by serving the two functions, network processing and input/output, with just one card in one slot. Like the other cards, this one supports In-service software upgrades; In addition It supports in-service hardware upgrades. It is fully, backward compatible with the current SRX3000 chassis and cards.

**The Juniper Networks SRX3000 line utilizes the same market leading, high-performance dynamic architecture as the SRX5000 line, but in a mid-plane form factor. The SRX3000 line SPCs, IOCs, and NPCs are based on a common form-factor module (CFM) design and are not compatible with the SRX5000 line. Likewise, all SRX5000 line modules are not compatible with the SRX3000 line.*

Features and Benefits

Networking and Security

The SRX3000 line has been designed from the ground up to offer robust networking and security services.

Features	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.	Provides 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 reliability needed for any critical high-speed network deployments. 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 HA-control interfaces.	Achieve availability and resiliency necessary for critical networks.
Interface flexibility	Offers flexible I/O options including on-board ports and modular CFM I/O cards.	Offers flexible I/O configuration and independent I/O scalability to meet the port density requirements of multiple network environments.
Network segmentation	Provides security zones, VLANs, and virtual routers that allow administrators to deploy security policies to isolate guests and regional servers or databases.	Features the capability to tailor unique security and networking policies for various internal, external, and 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.
Threat intelligence	Integration with Spotlight Secure for application of advanced threat detection technologies and feeds for policy enforcement	Policy enforcement based on optimized and up-to-date threat intelligence is automatically syndicated across the firewall estate, enabling higher security effectiveness and operational efficiency.
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.
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	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.	Applications are accurately identified and 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	Combined with application identification, provides 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 critical layer of protection beyond stateful firewall, enabling detection of vulnerabilities in network traffic and highly granular control over IPS policy enforcement
Stateful GPRS and SCTP inspection	Support for GPRS and SCTP firewall in mobile operator networks.	Enables the SRX3000 line to provide stateful firewall capabilities for protecting key GPRS nodes within mobile operator networks.

Features	Feature Description	Benefits
User identity-based access control enforcement	Secure access to data center resources via tight integration of standards-based access control capabilities of Juniper Pulse Access Control Service and the SRX3000 line.	Enables agent-based and agentless identity security services for enterprise data centers by integrating the SRX3000 line with the standards-based access control capabilities of Juniper Pulse Access Control Service. This integration enables administrative flexibility to manage a variety of user access, including corporate, guest, and mobile.
NP-IOC	Like the other cards, this one supports In-service software upgrades; In addition It supports in-service hardware upgrades. It is fully, backward compatible with the current SRX3000 chassis and cards.	Meets business requirements by expanding gateway's capacity and serving latency sensitive applications such as high-speed financial trading
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.

IPS Capabilities

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

Features	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	Enables most accurate detection and helps reduce false positives.	Accuracy of signatures is 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 at exploiting 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 SRX3000 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.

Additional UTM Capabilities

The UTM services offered on Juniper Networks SRX3000 includes industry-leading antivirus, antispam, content filtering, and additional content security services.

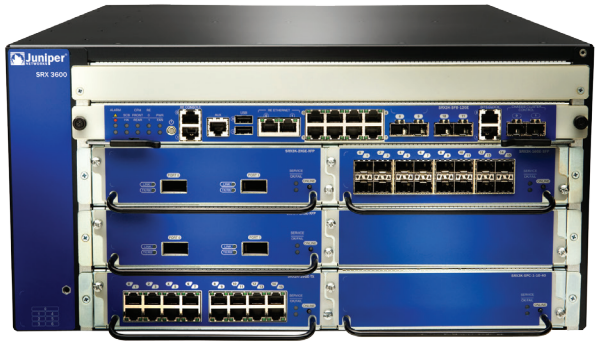
Features	Feature Description	Benefits
Antivirus	Antivirus includes reputation enhanced, cloud-based antivirus capabilities that detect and block spyware, adware, viruses, keyloggers, and other malware over POP3 HTTP, SMTP, IMAP, and FTP protocols. This service is provided in cooperation with Sophos Labs, 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, and 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 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.

SRX3400
Services Gateway



SRX3600
Services Gateway

Specifications

	SRX3400	SRX3600
Maximum Performance and Capacity[1]		
Junos OS version tested	Junos OS 12.1X47	Junos OS 12.1X47
Firewall performance (max)	30 Gbps	55 Gbps
Firewall performance (IMIX)	10 Gbps	20 Gbps
Maximum AES256+SHA-1 VPN performance	8 Gbps	15 Gbps
Maximum 3DES+SHA-1 VPN performance	8 Gbps	15 Gbps
Maximum IPS performance (NSS 4.2.1)	8 Gbps	15 Gbps
Maximum concurrent sessions	2.25/3 million[2]	2.25/6 million[2]
New sessions/second, (sustained, TCP, three-way)	150,000	150,000/270,000[2]
Maximum user supported	Unrestricted	Unrestricted
Latency	Sub-10 µs	Sub-10 µs
Network Connectivity		
Fixed I/O	8 10/100/1000 + 4 SFP	8 10/100/1000 + 4 SFP
LAN interface options	16 x 1 10/100/1000 copper 16 x 1-Gigabit Ethernet SFP 2 x 10-Gigabit Ethernet XFP	16 x 1 10/100/1000 copper 16 x 1-Gigabit Ethernet SFP 2 x 10-Gigabit Ethernet XFP
Maximum available slots for IOCs	Four (front slots)	Six (front slots)
Processing Scalability		
Maximum available slots for SPCs[3]	Up to four SPCs supported per chassis[4] (any slot)	Up to seven SPCs supported per chassis (any slot)
Maximum available slots for NPCs[3]	Up to two NPCs supported per chassis[4] (three rear slots)	Up to three NPCs supported per chassis (three rear-right slots)

[1] Performance, capacity, and features listed are based upon systems running Junos OS12.1.X44 and are measured under ideal testing conditions. Actual results may vary based on Junos OS releases and by deployment. For a complete list of supported Junos OS versions for the SRX Series Services Gateways, please visit the Juniper Customer Support Center (www.juniper.net/customers/support/).

[2] Additional Extreme License required for 3 million and 6 million sessions.

[3] Each SRX3000 line of Services Gateways employ multiple common form-factor module (CFM) expansion slots on the front and rear of the chassis to allow custom configurations of I/O and processing capacities based on customer requirements. SPCs and NPCs are supported on all available CFM slots. However, for proper system functionality and allowing for I/O expansion, the SRX3400 supports a maximum of up to four SPCs and two NPCs per chassis, and the SRX3600 supports a maximum of up to seven SPCs and three NPCs per chassis. Please refer to the respective hardware guides for more information on SPCs and NPCs as well as for guidelines on placements.

[4] Refer to user guide for guidelines when using DC power supplies.

	SRX3400	SRX3600
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	7,500	7,500
Tunnel interfaces	7,500	7,500
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)	1,2,6	1,2,6
Prevent replay attack	Yes	Yes
Remote access VPN	Yes	Yes
IPv4 and IPv6 VPN	Yes	Yes
Redundant VPN gateways	Yes	Yes
Intrusion Prevention System		
Signatures based and customizable (via templates)	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, custom session	Drop connection, close connection, session packet log, session summary, email, custom session
Attack notification mechanisms	Structured system logging	Structured system logging
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	600+	600+
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	15,000+	15,000+
Detailed threat descriptions and remediation/patch info	Yes	Yes

	SRX3400	SRX3600
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
Unified Threat Management		
Antivirus (Sophos AV) throughput	2.5 Gbps	4.5 Gbps
Enhanced Web filter throughput	8 Gbps	14 Gbps
GPRS Security		
GPRS stateful firewall	Yes	Yes
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:1P)	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 loopback grouping	Yes	Yes
User Authentication and Access Control		
Built-in (internal) database	Yes	Yes
RADIUS accounting	Yes	Yes
Web-based authentication	Yes	Yes
UAC enforcement point	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 virtual firewalls with data plane traffic segregation (virtual routers (1,000) and zones (512))	512	512
Maximum virtual firewalls with data plane and administrative separation (logical systems)	32	32
Additional off-platform virtual firewall option with Firefly (VM based)	Unlimited	Unlimited
Maximum number of L3 subinterfaces	16,384[5]	16,384[5]
Maximum number of VLANs	4,096	4,096

	SRX3400	SRX3600
Routing		
BGP instances	1,000	1,000
BGP peers	2,000	2,000
BGP routes	1,000,000[6]	1,000,000[6]
OSPF instances	256	256
OSPF routes	1,000,000[6]	1,000,000[6]
RIP v1/v2 instances	50	50
RIP v2 table size	30,000	30,000
Dynamic routing	Yes	Yes
Static routes	Yes	Yes
Filter-based forwarding (FBF)	Yes	Yes
Equal-cost multipath (ECMP)	Yes	Yes
Reverse path forwarding (RPF)	Yes	Yes
Multicast	Yes	Yes
IPv6		
Firewall/stateless filters	Yes	Yes
VPN	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 QoS		
Maximum bandwidth	Yes	Yes
RFC2474 IP DiffServ in IPv4	Yes	Yes
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

[5] Maximum number of supported L3 subinterfaces in HA configuration is 1,000.
[6] Maximum number of BGP and OSPF routes recommended is 100,000.

	SRX3400	SRX3600
High Availability		
Active/passive, active/active	Yes	Yes
Low impact chassis cluster upgrades	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
Interface link aggregation/LACP	Yes	Yes
Redundant data and control links[7]	Yes	Yes
In-Service Software Upgrade (ISSU)[8]	Yes	Yes
Management		
WebUI (HTTP and HTTPS)	Yes	Yes
Command-line interface (console)	Yes	Yes
Network and Security Manager version 2008.2 or later	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 system log	Yes	Yes
SNMP (v2/v3)	Yes	Yes
Traceroute	Yes	Yes
Dimensions and Power		
Dimensions (W x H x D)	17.5 x 5.25 x 25.5 in (44.5 x 13.3 x 64.8 cm)	17.5 x 8.75 x 25.5 in (44.5 x 22.2 x 64.8 cm)
Weight	Chassis: 32.3 lb (14.7 kg) Fully configured: 75 lb (34.1 kg)	Chassis: 43.6 lb (19.8 kg) Fully configured: 115.7 lb (52.6 Kg)
Power supply (AC)	100 to 240 VAC	100 to 240 VAC
Power supply (DC)	-40 to -72 VDC	-40 to -72 VDC
Maximum power draw	1,100 W (AC power) 1,050 W (DC power)	1,750 W (AC power) 1,850 W (DC power)
Power supply redundancy	1 + 1	2 + 1 / 2 + 2
Certifications		
Safety certifications	Yes	Yes
Electromagnetic compatibility (EMC) certifications	Yes	Yes
Designed for NEBS Level 3	Yes	Yes
NIST FIPS-140-2 Level 2	Yes (with Junos OS 10.4R4)	Yes (with Junos OS 10.4R4)
ISO Common Criteria NDPP+TFFW EP	Yes (with Junos OS 12.1x44)	Yes (with Junos OS 12.1x44)
IPsec	Yes	Yes
USGv6	Yes (with Junos OS 11.4R1)	Yes (with Junos OS 11.4R1)

[7] To enable dual control links on the SRX3000 line, the SRX3K CRM module must be installed on each cluster member.
[8] Please check the technical publication documents and release notes for the list of compatible features for ISSU.

	SRX3400	SRX3600
3GPP TS 20.060 Compliance[9]		
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
Environmental		
Operating temperature (long term)	41º to 104º F (5º to 40º C)	41º to 104º F (5º to 40º C)
Operating temperature (short term[10])	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
Humidity (short term[10])	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

[9] SRX3000 line 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 SRX3000 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

[10] 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 System	
SRX3400BASE-AC	SRX3400 chassis, midplane, fan, routing engine, SFB-12 Gigabit Ethernet, AC PEM* - no power cord - no SPC - no NPC
SRX3400BASE-DC2	SRX3400 chassis, midplane, fan, routing engine, SFB-12 Gigabit Ethernet, DC2 PEM - no SPC - no NPC
SRX3600BASE-AC	SRX3600 chassis, midplane, fan, routing engine, SFB-12 Gigabit Ethernet, 2xAC PEM* - no power cords - no SPC - no NPC
SRX3600BASE-DC2	SRX3600 chassis, midplane, fan, routing engine, SFB-12 Gigabit Ethernet, 2xDC PEM - no SPC - no NPC
SRX3000 Line Components	
SRX3K-SPC-1-10-40	SRX3000 line Services Processing Card with 1 GHz processor and 4 GB memory
SRX1K3K-NP-2XGE-SFPP	SRX3000 line Network Processing and I/O Card
SRX3K-NPC	SRX3000 line Network Processing Card
SRX3K-16GE-TX	16 x 1 10/100/1000 Copper CFM I/O Card for SRX3000 line
SRX3K-16GE-SFP	16 x 1 Gigabit SFP Ethernet I/O Card for SRX3000 line, no transceivers
SRX3K-2XGE-XFP	2 x 10 Gigabit XFP Ethernet I/O Card for SRX3000 line, no transceivers
SRX3K-CRM	Clustering module for the SRX3000 line to enable redundant control links in high-availability clusters

Model Number	Description
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
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
Logical System License	
SRX-3400-LSYS-1	1 incremental Logical Systems License for SRX3400
SRX-3400-LSYS-5	5 incremental Logical Systems License for SRX3400
SRX-3400-LSYS-25	25 incremental Logical Systems License for SRX3400
SRX-3600-LSYS-1	1 incremental Logical Systems License for SRX3600
SRX-3600-LSYS-5	5 incremental Logical Systems License for SRX3600
SRX-3600-LSYS-25	25 incremental Logical Systems License for SRX3600

Model Number	Description
AppSecure Subscription	
SRX3400-APPSEC-A-1	One year subscription for Application Security and IPS updates for SRX3400
SRX3400-APPSEC-A-3	Three year subscription for Application Security and IPS updates for SRX3400
SRX3400-APPSEC-A-5	Five year Subscription for Application Security and IPS updates for SRX3400
SRX3600-APPSEC-A-1	One year subscription for Application Security and IPS updates for SRX3600
SRX3600-APPSEC-A-3	Three year subscription for Application Security and IPS updates for SRX3600
SRX3600-APPSEC-A-5	Five year Subscription for Application Security and IPS updates for SRX3600
Services Offload License	
SRX3K-SVCS-OFFLOAD-RTU	Services offload license for SRX3000 line; this is not an annual license subscription
IPS Subscription	
SRX3K-IDP	One year IPS signature subscription for SRX3000 line
SRX3K-IDP-3	Three year IPS signature subscription for SRX3000 line
SRX3K-IDP-5	Five year IDP signature subscription for SRX 3000 line
IPS Subscription	
SRX3K-IDP	One year IPS signature subscription for SRX3000 line
SRX3K-IDP-3	Three year IPS signature subscription for SRX3000 line
SRX3K-IDP-5	Five year IDP signature subscription for SRX 3000 line
UTM Subscription	
SRX3400-CS-BUN-1	One year subscription for AppSecure, IDP, EWF, AV and Anti-spam service on SRX3400
SRX3400-CS-BUN-3	Three year subscription for AppSecure, IDP, EWF, AV and Anti-spam service on SRX3400
SRX3400-CS-BUN-5	Five year subscription for AppSecure, IDP, EWF, AV and Anti-spam service on SRX3400
SRX3600-CS-BUN-1	One year subscription for AppSecure, IDP, EWF, AV and Anti-spam service on SRX3600
SRX3600-CS-BUN-3	Three year subscription for AppSecure, IDP, EWF, AV and Anti-spam service on SRX3600
SRX3600-CS-BUN-5	Five year subscription for AppSecure, IDP, EWF, AV and Anti-spam service on SRX3600
SRX3400-S-AS-1	One year subscription for Juniper-Sophos Anti-spam service on SRX3400
SRX3400-S-AS-3	Three year subscription for Juniper-Sophos Anti-spam service on SRX3400
SRX3400-S-AS-5	Five year subscription for Juniper-Sophos Anti-spam service on SRX3400
SRX3600-S-AS-1	One year subscription for Juniper-Sophos Anti-spam service on SRX3600
SRX3600-S-AS-3	Three year subscription for Juniper-Sophos Anti-spam service on SRX3600

Model Number	Description
SRX3600-S-AS-5	Five year subscription for Juniper-Sophos Anti-spam service on SRX3600
SRX3400-S-AV-1	One year subscription for Juniper-Sophos AV service on SRX3400
SRX3400-S-AV-3	Three year subscription for Juniper-Sophos AV service on SRX3400
SRX3400-S-AV-5	Five year subscription for Juniper-Sophos AV service on SRX3400
SRX3600-S-AV-1	One year subscription for Juniper-Sophos AV service on SRX3600
SRX3600-S-AV-3	Three year subscription for Juniper-Sophos AV service on SRX3600
SRX3600-S-AV-5	Five year subscription for Juniper-Sophos AV service on SRX3600
SRX3400-W-EWF-1	One year subscription for Juniper-Websense Enhanced Web Filtering service on SRX3400
SRX3400-W-EWF-3	Three year subscription for Juniper-Websense Enhanced Web Filtering service on SRX3400
SRX3400-W-EWF-5	Five year subscription for Juniper-Websense Enhanced Web Filtering service on SRX3400
SRX3600-W-EWF-1	One year subscription for Juniper-Websense Enhanced Web Filtering service on SRX3600
SRX3600-W-EWF-3	Three year subscription for Juniper-Websense Enhanced Web Filtering service on SRX3600
SRX3600-W-EWF-5	Five year subscription for Juniper-Websense Enhanced Web Filtering service on SRX3600
Extreme LTU	
SRX3K-EXTREME-LTU	Expanded performance and capacity Extreme License for SRX3000 line
C19 Straight Power Cables	
CBL-PWR-C19S-132-UK	Power cord, AC, Great Britain & Ireland, C19 at 70-80 mm, 13 A/250 V, 2.5 mm, straight
CBL-PWR-C19S-151-US15	Power cord, AC, Japan/US, NEMA 5-15 to C19 at 70-80 mm, 15 A/125 V, 2.5 m, straight
CBL-PWR-C19S-152-AU	Power cord, AC, Australia/New Zealand, C19 at 70-80 mm, 15 A/250 V, 2.5 m, straight
CBL-PWR-C19S-162-CH	Power cord, AC, China, C19, 16 A/250 V, 2.5 m, straight
CBL-PWR-C19S-162-EU	Power cord, AC, Continental Europe, C19, 16 A/250 V, 2.5 m, RA
CBL-PWR-C19S-162-IT	Power cord, AC, Italy, C19 at 70-80 mm, 16 A/250 V, 2.5 m, straight
CBL-PWR-C19S-162-JP	Power cord, AC, Japan, NEMA 6-20 to C19, 16 A/250 V, 2.5 m, straight
CBL-PWR-C19S-162-JPL	Power cord, AC, Japan/US, C19 at 70-80 mm, 16 A/250 V, 2.5 m, straight, locking plug
CBL-PWR-C19S-162-US	Power cord, AC, Japan/US, NEMA 6-20 to C19 at 70-80 mm, 16 A/250 V, 2.5 m, straight
CBL-PWR-C19S-162-USL	Power cord, AC, US, NEMA L6-20 to C19, 16 A/250 V, 2.5 m, straight, locking plug

* AC power cords are not included. One C19-Straight cable with appropriate wall-plug for the final destination of the system is required for each power supply.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
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

1000267-020-EN Mar 2017