# SRX3400 AND SRX3600 SERVICES GATEWAYS

## Product Overview

Juniper Networks SRX3000 line of services gateways is the next-generation solution for securing the ever-increasing network infrastructure and applications requirements for both enterprise and service providers. Designed from the ground up to provide flexible processing scalability, I/O scalability, and high integration, the SRX3000 line of services gateways can meet the network and security requirements of data center hyper-consolidation, rapid managed services deployments, and aggregation of security solutions. Built on Juniper Networks JUNOS Software, incorporating Juniper's rich routing heritage and service provider reliability with ScreenOS network security heritage, the SRX3000 line offers the high-feature/service integration necessary to secure modern network infrastructure and applications.

## Product Description

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

- Enterprise server farms/data centers
- Service provider data centers
- Aggregation of departmental or segmented security solutions
- Service provider infrastructure security and managed services

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 30 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; network processing performance from 10 to 30 Gbps; and services processing to match specific business needs.

The switch fabric employed in the services gateway 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 enables uninterrupted expansion and growth of the network infrastructure, without the security solution being a barrier.

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 enables market-leading flexibility and scalability. By doubling the number of SPCs supported in half the rack space needed, the SRX3000 line offers not only the underlying architectural innovation but also innovative physical design.

The feature integration on SRX Series Services Gateways is enabled by Juniper Networks JUNOS® Software. By combining the routing heritage of JUNOS Software and the security heritage of ScreenOS®, the SRX Series Services Gateways are equipped with a robust list of features that include firewall, IPsec VPN, intrusion prevention system (IPS), denial of service (DoS), Network Address Translation (NAT), and quality of service (QoS). In addition to the benefit of individual features, incorporating the various features under a single OS greatly optimizes the flow of traffic through the services gateway. With JUNOS Software, the SRX Series enjoys the benefit of a single source OS, single release train, and one architecture traditionally available on Juniper's service provider-class routers and switches.

## SRX3600

The SRX3600 Services Gateway is a market-leading security solution supporting up to 30 Gbps firewall, 10 Gbps firewall and IPS, or 10 Gbps of IPsec VPN along with up to 175,000 new connections per second. Equipped with the full range of security features, the SRX3600 is ideally suited for securing medium to large enterprise data centers, co-located data centers, or securing next-generation enterprise services/applications. It can also be deployed to secure service provider infrastructures as well as for securing next-generation services. The scalability and flexibility of the services gateway makes it ideal for consolidating and growing data center requirements, as well as the rapid service deployment requirements by service and managed service providers. The SRX3600 Services Gateway is managed by Juniper Networks Network and Security Manager; the same management solution used in all Juniper Networks firewall, IDP Series Intrusion Detection and Prevention Appliances, SA Series SSL VPN Appliances, Unified Access Control, and EX Series Ethernet Switches.

## SRX3400

The SRX3400 Services Gateway uses the same SPCs, IOCs and NPCs as the SRX3600 and can support up to 20 Gbps firewall, 6 Gbps firewall and IPS, or 6 Gbps of IPsec VPN, along with up to 175,000 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 or hosting sites. The SRX3400 Services Gateway is also managed by Juniper Networks Network and Security Manager.

## SRX3000 Line Service Processing Cards*

As the "brains" behind the SRX3000 line, SPCs are designed to process all available services on the gateway. 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. All of the processing capabilities of the SPCs are used to support any and all services and capabilities of the gateway. 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.)

** The Juniper Networks SRX3000 line utilizes common form-factor module (CFM) SPCs, NPCs, and IOCs. All modules are supported on both the SRX3400 and SRX3600, but are not compatible with Juniper Networks SRX5000 line of services gateways. Likewise, all SRX5000 line modules are not compatible with the SRX3000 line.*

## Features and Benefits

### Networking and Security

The SRX Series Services Gateways have been designed from the ground up to offer robust networking and security services.

| FEATURES | FEATURE DESCRIPTION | BENEFIT |
|---|---|---|
| **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. |
| **High availability (HA)** | Has active/passive HA configuration that uses dedicated HA-control interfaces. | Achieve availability and resiliency necessary for critical networks. |
| **Interface flexibility** | Offers flexible I/O options with modular CFM modules based on the Dynamic Services Architecture. | Offers flexible I/O configuration and independent I/O scalability to meet the needs of any particular network requirements. |
| **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 capabilities to tailor unique security and networking policies for various internal, external, and DMZ subgroups. |
| **Robust routing engine** | Has a 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. |
| **Comprehensive threat protection** | Offers highly integrated features on JUNOS Software including multi-gigabit firewall, IPsec VPN, IPS, DoS, and other services. | Offers unmatched integration, ensuring network security against all level of attacks. |

### Traffic Inspection Methods

The SRX Series supports various detection methods to accurately identify the application and traffic flow through the network.

| FEATURES | FEATURE DESCRIPTION | BENEFIT |
|---|---|---|
| **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 DDoS attacks. |
| **IP spoofing detection** | Validate IP addresses by checking allowed addresses inside and outside the network. | Permit only authentic traffic while blocking disguised sources. |
| **DoS detection** | SYN cookie-based protection from SYN flood attacks. | Protect your key network assets from being overwhelmed with SYN floods. |

## IPS Capabilities

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

| FEATURES | FEATURE DESCRIPTION | BENEFIT |
|---|---|---|
| **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 is improved through precise contexts of protocols. |
| **Signatures**[1] | There are more than 6,000 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. |
| **Application awareness/ identification** | Context, protocol information, and signatures are used to identify applications on any TCP or UDP port. | Enable rules and policies based on application traffic rather than ports—protect or police standard applications on non-standard ports. (This also applies for applications that do not have protocol decoders.) |
| **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. |

## Centralized Management

Network and Security Manager—the common management solution for all Juniper Networks firewall, IDP Series, SA Series SSL VPN Appliances, UAC, and EX Series—manages the SRX Series Services Gateways.

| FEATURES | FEATURE DESCRIPTION | BENEFIT |
|---|---|---|
| **Role-based administration** | More than 100 different activities can be assigned as unique permissions for different administrators. | Streamline business operations by logically separating and enforcing roles of various administrators. |
| **Scheduled security update** | SRX Series Services Gateways can be automatically updated with new attack objects/signatures. | Get up-to-the-minute security coverage without manual intervention. |
| **Domains** | Logical separation of devices, policies, reports, and other management activities are permitted. | Conform to business operations by grouping devices based on business practices. |
| **Object locking** | Safe concurrent modification to the management settings is allowed. | Avoid incorrect configuration due to overwritten management settings. |
| **Scheduled database backup** | Automatic backup of NSM database is provided. | Provide configuration redundancy. |
| **Job manager** | View pending and completed jobs. | Simplify update of multiple devices. |

[1]As of August 2009, there are 6,200 signatures with approximately 10 new signatures added every week. Subscription to signature update service is required to receive new signatures.

## Simple, Flexible Deployment

| FEATURES | FEATURE DESCRIPTION | BENEFITS |
|---|---|---|
| **Centralized policy management** | • Delivers centralized policy management when deployed with NSM and SA Series SSL VPN Appliances.<br>• Create common configuration templates that can be shared between SA Series SSL VPN (remote access control) and UAC (LAN access control) deployments using NSM.<br>• NSM also delivers a single management server that can configure many key components within a UAC deployment. | • Delivers consistent remote and local access control policy implementation and enforcement across a distributed network.<br>• Makes possible and simplifies enterprise-wide deployment of uniform network access control. |
| **Open, standards-based solution** | • Leverages industry-standards like 802.1X, RADIUS, IPsec, and innovative open standards, such as TNC to deliver a standards-based access control solution.<br>• Leverages existing 802.1X-enabled switches and access points. | • Delivers standards-based, vendor-agnostic access control and seamless support for heterogeneous networking environments.<br>• Facilitates quick, simple, and flexible access control deployments without requiring forklift upgrades, saving time and cost.<br>• No single vendor lock-in. |
| **Phased access control deployment** | • Innovative design allows organizations to start controlling access virtually anywhere on their network.<br>• Audit mode enables organizations to track user and device policy compliance without enforcing policies. | • Saves access control deployment time and cost.<br>• Enables users to become familiar with policies and necessary compliance and allows organizations to phase in policy compliance enforcement. |
| **Windows Statement of Health (SOH) and embedded NAP agent support** | • Through the TNC SOH standard, allows organizations to leverage their pre-installed Microsoft Windows Vista and XP (SP3) clients with UAC for access control.<br>• Allows the use of the Windows Security Center (WSC) SOH in access control decisions.<br>• Can pass the SOH to a Microsoft NPS server for external enforcement and validation of the SOH and transmit the information back to the IC Series UAC Appliance for use in access control decisions. | • Streamlines client deployment.<br>• Simplifies access control rollout and deployment. |
| **Dynamic authentication policy (leveraging existing AAA investments)** | • Leverages an organization's existing investment in directories, PKI, and strong authentication.<br>• Supports 802.1X, RADIUS, LDAP, Microsoft Active Directory, RSA ACE/Server, Network Information Service (NIS), certificate servers (digital certificates/PKI), local login/password, Netegrity SiteMinder (Computer Associates), RSA Cleartrust, Oblix (Oracle), and RADIUS Proxy. | • Establishes a dynamic authentication policy for each user session.<br>• RADIUS Proxy enables support for deployments where certain authentications are supported by a backend RADIUS server. |
| **Automatic realm decisions based on authentication protocols** | IC Series UAC Appliance can be configured to make a realm selection based on the authentication protocol in the request. | Improves and eases the administrative experience by offering a simple way to solve a complex challenge without requiring complicated authentication schemes or configuration issues. |
| **Role-based UAC Agent download** | Agent downloads can be based on role and dynamically delivered in the appropriate manner (agent-based or agent-less). | Enables agent-less or agent-based access to be dynamically linked to a user and/or device identity, instead of forcing an upfront selection. |


## Specifications

| | SRX3400 | SRX3600 |
|---|---|---|
| **Maximum Performance and Capacity[2]** | | |
| Tested configuration to achieve performance, capacities and features listed below:<br>SRX3400 chassis equipped with four (4) SPCs, one (1) IOC, two (2) NCPs, and AC power supplies<br>SRX3600 chassis equipped with seven (7) SPCs, two (2) IOCs, three (3) NPCs, and AC power supplies | | |
| JUNOS Software version tested | JUNOS 9.6 | JUNOS 9.6 |
| Firewall performance (max) | 10 / 20 Gbps | 10 / 20 / 30 Gbps |
| Firewall performance (IMIX) | 8 Gbps | 18 Gbps |
| Firewall packets per second (64 bytes) | 3 Mpps | 6 Mpps |
| Maximum AES256+SHA-1 VPN performance | 6 Gbps | 10 Gbps |
| Maximum 3DES+SHA-1 VPN performance | 6 Gbps | 10 Gbps |
| Maximum IPS performance (NSS 4.2.1) | 6 Gbps | 10 Gbps |
| Maximum concurrent sessions | 1 million | 2 million |
| New sessions/second, (sustained, TCP, three-way) | 175,000 | 175,000 |
| Maximum security policies | 40,000 | 40,000 |
| Maximum user supported | Unrestricted | Unrestricted |
| **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<br>16 x 1 Gigabit Ethernet SFP<br>2 x 10-Gigabit Ethernet XFP | 16 x 1 10/100/1000 copper<br>16 x 1 Gigabit Ethernet SFP<br>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) |

[2]Performance, capacity, and features listed are based upon systems running JUNOS 9.6 and are measured under ideal testing conditions. SRX3400 DC-powered systems achieve lower performance levels as fewer cards can be supported. Actual results may vary based on JUNOS releases and by deployment. For a complete list of supported JUNOS versions for the SRX Series Services Gateways, please visit the Juniper Customer Support Center (www.juniper.net/customers/support/).

[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.

## Specifications (continued)

| | 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** | | |
| Tunnel interfaces | 5,000 | 5,000 |
| 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** | | |
| 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 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 |
| 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 |

## Specifications (continued)

| | SRX3400 | SRX3600 |
|---|---|---|
| **Intrusion Prevention System (continued)** | | |
| 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 |
| **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 number of security zones | 256 | 256 |
| Maximum number of virtual routers | 256 | 256 |
| Maximum number of VLANs per interface | 4,096 | 4,096 |
| Maximum number of L3 subinterfaces | 16,384 | 16,384 |

## Specifications (continued)

| | SRX3400 | SRX3600 |
|---|---|---|
| **Routing** | | |
| BGP instances | 128 | 128 |
| BGP peers | 2,000 | 2,000 |
| BGP routes | 1,000,000 | 1,000,000 |
| OSPF instances | 256 | 256 |
| 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 |
| Static routes | Yes | Yes |
| Filter-based forwarding (FBF) | Yes | Yes |
| Equal-cost multipath (ECMP) | Yes | Yes |
| Reverse path forwarding (RPF) | 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 |
| **High Availability** | | |
| Active/passive, active/active | 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 failure detection | Yes | Yes |
| **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 |
| Network and Security Manager version 2008.2 or later | Yes | Yes |

## Specifications (continued)

| | SRX3400 | SRX3600 |
|---|---|---|
| **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<br>(44.5 x 13.3 x 64.8 cm) | 17.5 x 8.75 x 25.5 in<br>(44.5 x 22.2 x 64.8 cm) |
| Weight | Chassis: 32.3 lb (14.7 kg)<br>Fully configured: 75 lb (34.1 kg) | Chassis: 43.6 lb (19.8 kg)<br>Fully configured: 115.7 lb (52.6 Kg) |
| Power supply (AC) | 100 to 240 VAC | 100 to 240 VAC |
| Power supply (DC) | -40 to -60 VDC | -40 to -60 VDC |
| Maximum power draw | 1,200 W (AC power)<br>1,020 W (DC power) | 1,800 W (AC power)<br>1,800 W (DC power) |
| Power supply redundancy | 1 + 1 | 2 + 1 / 2 + 2 |
| **Certifications** | | |
| Safety certifications | Yes | Yes |
| Electromagnetic compatibility (EMC) certifications | Yes | Yes |
| **Operating Environment** | | |
| Operating temperature | 32° to 104° F (0° to 40° C) | 32° to 104° F (0° to 40° C) |
| Humidity | 5% to 90% noncondensing humidity | 5% to 90% noncondensing humidity |

## Performance-Enabling Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains, faster rollouts of new business models and ventures, and greater market reach, while generating higher levels of customer satisfaction. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/products-services.**

| MODEL NUMBER | DESCRIPTION |
|---|---|
| **Base System** | |
| SRX3400BASE-AC | SRX3400 chassis, midplane, fan, routing engine, SFB-12 Gigabit Ethernet, AC PEM[5] - no power cord - no SPC - no NPC |
| SRX3400BASE-DC | SRX3400 chassis, midplane, fan, routing engine, SFB-12 Gigabit Ethernet, DC PEM - no SPC - no NPC |
| SRX3600BASE-AC | SRX3600 chassis, midplane, fan, routing engine, SFB-12 Gigabit Ethernet, 2xAC PEM[5] - no power cords - no SPC - no NPC |
| SRX3600BASE-DC | 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 |
| 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 |
| **Transceivers** | |
| 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 |
| **IPS Subscription** | |
| SRX3K-IDP | One year IPS signature subscription for SRX3000 line |
| SRX3K-IDP-3 | Three year IPS signature subscription for SRX3000 line |

| MODEL NUMBER | DESCRIPTION |
|---|---|
| **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 |

[5] 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, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. 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

**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
Fax: 35.31.8903.601

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



1000267-005-EN Aug 2009

Printed on recycled paper.