SRX SERIES SERVICES GATEWAYS FOR THE BRANCH

SRX210, SRX240 and SRX650

Product Overview

Juniper Networks SRX Series Services Gateways for the branch provide essential capabilities that connect, secure, and manage work force locations sized from handfuls to hundreds of users. By consolidating fast, highly available switching, routing, security, and applications capabilities in a single device, enterprises can economically deliver new services, safe connectivity, and a satisfying end user experience. All SRX Series Services Gateways, including products scaled for the branch, campus and data center applications, are powered by Juniper Networks JUNOS Software—the proven operating system that provides unmatched consistency, better performance with services, and superior infrastructure protection at a lower total cost of ownership.

Product Description

The Juniper Networks® SRX Series Services Gateways for the branch joins Juniper Networks SRX Series for the high end, EX Series Ethernet Switches, M Series Multiservice Edge Routers, MX Series Ethernet Services Routers, and T Series Core Routers to provide a single Juniper Networks JUNOS® Software-based portfolio of unprecedented scale. With JUNOS, enterprises and service providers can lower deployment and operational costs across their entire distributed workforce.

- SRX Series for the branch runs JUNOS Software, the proven operating system that is used by core Internet routers in all of the top 100 service providers around the world. The rigorously tested carrier class routing features of IPv4/IPv6, OSPF, BGP, and multicast have been proven in over 10 years of worldwide deployments.
- SRX Series Services Gateways for the branch provide perimeter security, content security, access control, and network-wide threat visibility and control. Best-in-class firewall and VPN technologies secure the perimeter with minimal configuration and consistent performance. By using zones and policies, even new network administrators can configure and deploy an SRX Series for the branch quickly and securely. Policy-based VPNs support more complex security architectures that require dynamic addressing and split tunneling. For content security, SRX Series for the branch offers a complete suite of Unified Threat Management (UTM) services consisting of: intrusion prevention system (IPS), antivirus, anti-spam, Web filtering and data loss prevention via content filtering to protect your network from the latest content borne threats. Select models feature Content Security Accelerator for high-performance IPS and antivirus performance. The branch SRX Series integrates with other Juniper security products to deliver enterprise-wide unified access control and adaptive threat management. These capabilities give security professionals powerful tools in the fight against cybercrime and data loss.
- SRX Series for the branch brings high-performance and proven deployment capabilities to enterprises that need to build a worldwide network of thousands of sites. The wide variety of options allows configuration of performance, functionality, and price scaled to support from a handful to thousands of users. Ethernet, serial, T1/E1, xDSL, Metro Ethernet, and third generation (3G) cellular wireless are all available options for WAN or Internet connectivity to securely link your sites. Multiple form factors allow you to make cost-effective choices for mission-critical deployments. Managing the network is easy using the proven JUNOS command-line interface (CLI) and scripting capabilities, or a simple to use Web-based GUI.

Architecture and Key Components

Key Hardware Features of the Branch SRX Series Products

PRODUCT	DESCRIPTION
SRX210 Services Gateway	• 2 10/100/1000 Ethernet and 6 10/100 Ethernet LAN ports, 1 Mini-PIM slot, 1 ExpressCard slot and 2 USB ports • Factory option of 4 dynamic Power over Ethernet (PoE) ports 802.3af • Support for T1/E1, serial, ADSL/2/2+, Ethernet small form-factor pluggable transceiver (SFP), and Gigabit Ethernet interfaces • Content Security Accelerator hardware for faster performance of IPS and ExpressAV • Full UTM; antivirus, anti-spam, Web filtering, intrusion prevention system (with high memory version) • Unified Access Control (UAC) and content filtering • 512 MB DRAM default, optional factory 1 GB DRAM, 1 GB flash default
SRX240 Services Gateway	• 16 10/1000/1000 Ethernet LAN ports, 4 Mini-PIM slots • Factory option of 16 PoE ports; PoE+ 803.3at, backwards compatible with 802.3af • Support for T1/E1, serial, ADSL2/2+, Ethernet SFP, and Gigabit Ethernet interfaces • Content Security Accelerator hardware for faster performance of IPS and ExpressAV • Full UTM; antivirus, anti-spam, Web filtering, intrusion prevention system (with high memory version) • Unified Access Control and content filtering • 512 MB RAM default, optional factory 1 GB DRAM, 1 GB flash default
SRX650 Services Gateway	• 4 fixed ports 10/100/1000 Ethernet LAN ports, 8 Gigabit Ethernet-backplane Physical Interface Module (GPIM) slots • Support for T1, E1, Gigabit Ethernet LAN ports; supports up to 48 ports switching with optional PoE including 802.3at, PoE+, backwards compatible with 802.3af • Content Security Accelerator hardware for faster performance of IPS and ExpressAV • Full UTM; antivirus, anti-spam, Web filtering, and intrusion prevention system • Unified Access Control and content filtering • Modular Services and Routing Engine; future internal failover and hot-swap • 2 GB DRAM default, 2 GB compact flash default, external compact flash slot for additional storage • Optional redundant AC power; standard AC power supply that is PoE-ready; PoE power up to 250 watts redundant, or 500 watts non-redundant.

Network Deployments

The SRX Series Services Gateways for the branch are deployed at remote and branch locations in the network to provide all-in-one secure WAN connectivity, IP telephony, and connection to local PCs and servers via integrated Ethernet switching.

Features and Benefits

Secure Routing

Should you use a router and a firewall to secure your network? By building the branch SRX Series with best in class routing and firewall capabilities in one product, enterprises don't have to make that choice. Why forward traffic if it's not legitimate? SRX Series for the branch checks the traffic to see if it is legitimate, and only forwards it on when it is. This reduces the load on the network, allocates bandwidth for all other mission-critical applications, and secures the network from hacking.

The main purpose of a secure router is to provide firewall protection and apply policies. The firewall (zone) functionality inspects traffic flows and state to ensure that originating and returning information in a session is expected and permitted for a particular zone. The security policy determines if the session can originate in one zone and traverse to another zone. This architectural choice receives packets from a wide variety of clients and servers and keeps track of every session, of every application, and of every user. It allows the enterprise to make sure that only legitimate traffic is on its network and that traffic is flowing in the expected direction.

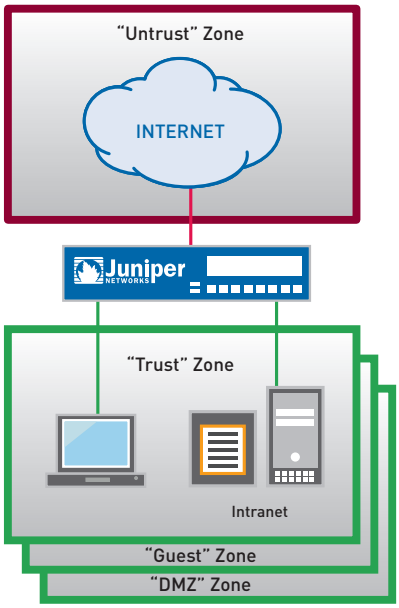

Figure 1: Firewalls, zones and policies

To ease the configuration of a firewall, SRX Series for the branch uses two features—"zones" and "policies." While these can be user defined, the default shipping configuration contains, at a minimum, a trust and an untrust zone. The trust zone is used for configuration and attaching the LAN to the branch SRX Series. The untrust zone is used for the WAN or Internet interface. To simplify installation and make configuration easier, a default policy is in place that allows traffic originating from the trust

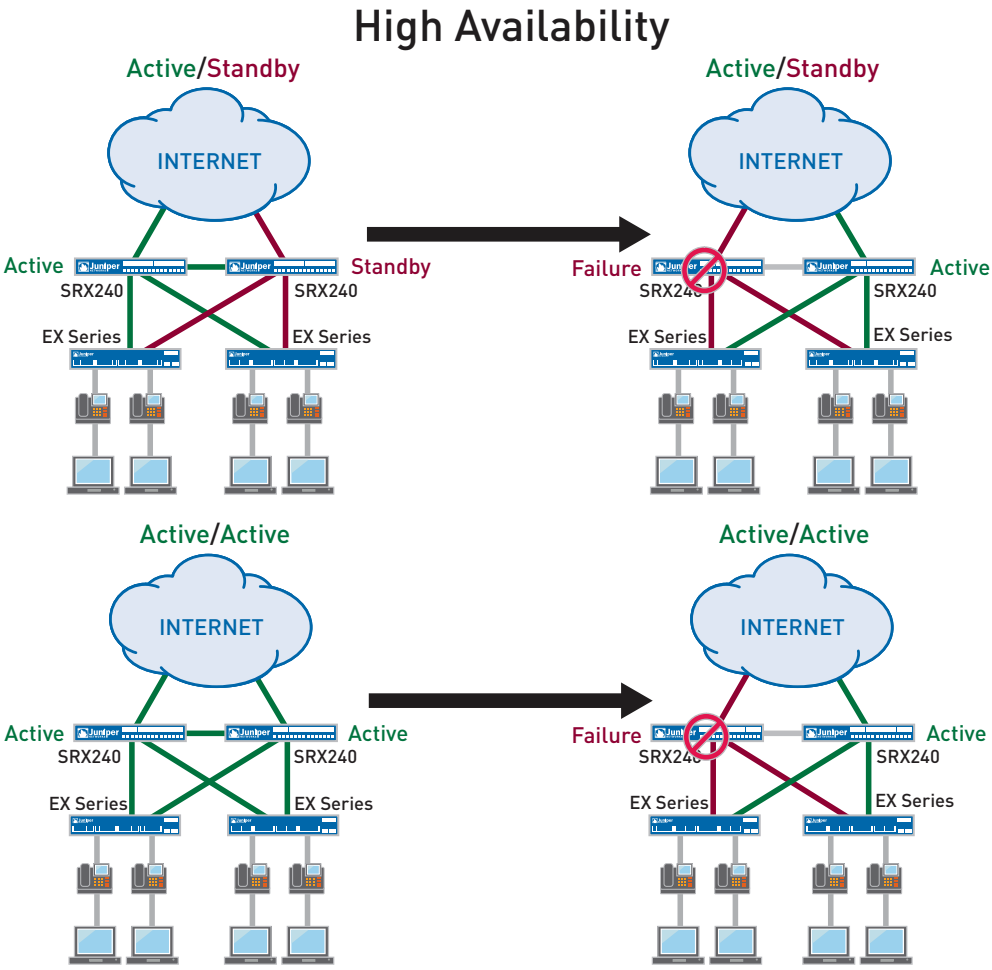

Figure 2: High availability

zone to flow to the untrust zone. This policy blocks ALL traffic originating from the untrust zone to the trust zone. A traditional router forwards all traffic without regard to a firewall (session awareness) or policy (origination and destination of a session).

By using the Web interface or CLI, enterprises can create a series of security policies that will control the traffic from within and in between zones by defining policies. At the broadest level, all types of traffic can be allowed from any source in security zones to any destination in all other zones without any scheduling restrictions. At the narrowest level, policies can be created that allow only one kind of traffic between a specified host in one zone and another specified host in another zone during a scheduled time period.

High Availability

JUNOS Services Redundancy Protocol (JSRP) is a core feature of the SRX Series for the branch. JSRP enables a pair of security systems to be easily integrated into a high availability network architecture, with redundant physical connections between the systems and the adjacent network switches. With link redundancy, Juniper Networks can address many common causes of system failures, such as a physical port going bad or a cable getting disconnected, to ensure that a connection is available, without having to fail over the entire system. This is consistent with a typical active/standby nature of routing resiliency protocols.

When SRX Series Services Gateways for the branch are configured as an active/active pair, traffic and configuration will be mirrored automatically to provide active firewall and VPN session maintenance in case of a failure. The branch SRX Series will now synchronize both configuration and runtime information. As a result, during failover, synchronization of the following information is shared: connection/session state and flow information, IPsec security associations, Network Address Translation (NAT) traffic, address book information, configuration changes, and more. In contrast to the typical router active/standby resiliency protocols such as Virtual Router Redundancy Protocol (VRRP), all dynamic flow and session information is lost and must be reestablished in the event of a failover. Some or all applications sessions will have to restart depending on the convergence time of the links or nodes. By maintaining state, not only is the session preserved, but security is intact. In an unstable network, this active/active configuration also mitigates link flapping affecting session performance.

Session-Based Forwarding Without the Performance Hit

In order to optimize the throughput and latency of the combined router and firewall, JUNOS Software implements session-based forwarding, an innovation that combines the session state information of a traditional firewall and the next-hop forwarding of a classic router into a single operation. With JUNOS Software, a session that is permitted by the forwarding policy is added to the forwarding table along with a pointer to the next-hop route. Established sessions have a single table lookup to verify that the session has been permitted and to find the next hop. This efficient algorithm improves throughput and lowers latency for session traffic when compared with a classic router that performs multiple table lookups to verify session information and then to find a next-hop route.

Figure 3 shows the session-based forwarding algorithm. When a new session is established, the session-based architecture within JUNOS verifies that the session is allowed by the forwarding policies. If the session is allowed, JUNOS will look up the next-hop route in the routing table. It then inserts the session and the next-hop route into the session and forwarding table and forwards the packet. Subsequent packets for the established session require a single table lookup in the session and forwarding table, and are forwarded to the egress interface.

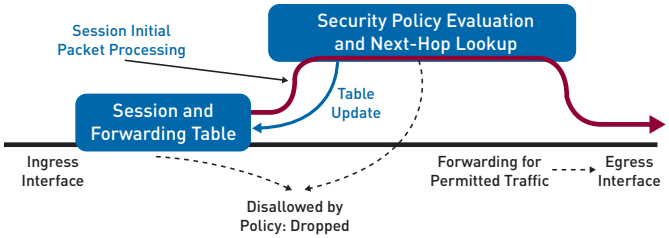

Figure 3: Session-based forwarding algorithm

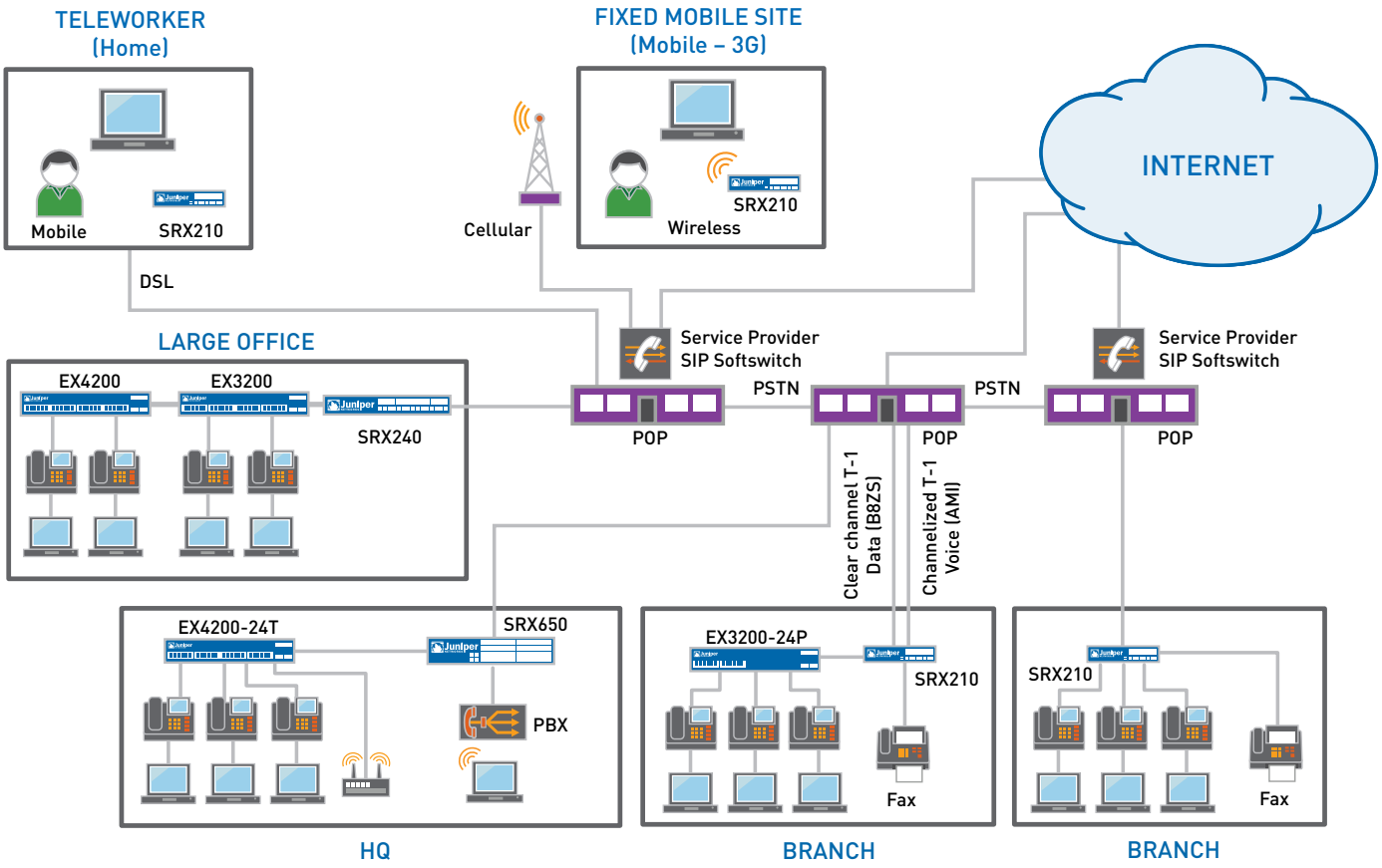

Figure 4: The distributed enterprise

Specifications

Protocols

- IPv4, IPv6, ISO Connectionless Network Service (CLNS)

Routing and Multicast

- Static routes
- RIPv2
- OSPF
- BGP
- BGP Router Reflector[1]
- IS-IS
- Multicast ((Internet Group Management Protocol (IGMPv3), PIM, Session Description Protocol (SDP), Distance Vector Multicast Routing Protocol (DVMRP), source-specific))[7]
- MPLS[4]

IP Address Management

- Static
- Dynamic Host Configuration Protocol (DHCP) (client and server)
- DHCP relay

Encapsulations

- Ethernet (MAC and tagged)
- Point-to-Point Protocol (PPP) (synchronous)
  - Multilink Point-to-Point Protocol (MLPPP)
- Frame Relay
  - Multilink Frame Relay (MLFR) (FRF.15, FRF.16)
- High-Level Data Link Control (HDLC)
- Serial (RS-232, RS-449, X.21, V.35, EIA-530)
- 802.1q VLAN support
- Point-to-Point Protocol over Ethernet (PPPoE)

Traffic Management

- Marking, policing, and shaping
- Class-based queuing with prioritization
- Weighted random early detection (WRED)
- Queuing based on VLAN, data-link connection identifier (DLCI), interface, bundles, or filters

Security

- Firewall, zones, screens, policies
- Stateful firewall, ACL filters
- Denial of service (DoS) and distributed denial of service (DDoS) protections (anomaly-based)
- Prevent replay attack; Anti-Replay
- Unified Access Control
- UTM (SRX650 and high memory versions of SRX210 and SRX240 only)
  - Antivirus, anti-spam, Web filtering, IPS[2]
  - Content Security Accelerator in SRX210 high memory, SRX240 high memory, and SRX650[2]
  - ExpressAV option in SRX210 high memory, SRX240 high memory, and SRX650[2]
  - Dynamic remote access
  - Content filtering

VPN

- Tunnels (generic routing encapsulation, IP-in-IP, IPsec)
- IPsec, Data Encryption Standard (DES) (56-bit), triple Data Encryption Standard (3DES) (168-bit), Advanced Encryption Standard (AES) (256-bit) encryption
- Message Digest 5 (MD5) and SHA-1 authentication
- Access Manager: Dynamic VPN Client. Browser based remote access feature requiring a license.

Voice Transport

- FRF.12
- Link fragmentation and interleaving (LFI)
- Compressed Real-Time Transport Protocol (CRTP)

High Availability

- VRRP
- Stateful failover and dual box clustering via JSRP[3]
- SRX650:
  - Redundant power (optional)
  - Future GPIM hot swap (online insertion and removal, OIR)
  - Future internal failover and SRE hot swap (OIR)
- Backup link via 3G wireless or other WAN

Specifications (continued)

IPv6[4]

- OSPFv3
- IPv6 Multicast Listener Discovery (MLD)
- BGP
- Quality of service (QoS)

SLA and Measurement

- Real-time performance monitoring (RPM)
- Top talkers (sessions, packets, bandwidth usage)
- J-Flow flow monitoring and accounting services

Logging and Monitoring

- Syslog
- Traceroute

Administration

- Juniper Networks Network and Security Manager support
- Juniper Networks STRM Series Security Threat Response Managers support
- Juniper Networks Advanced Insight Solutions support
- External administrator database (RADIUS, LDAP, SecureID)
- Auto configuration
- Configuration rollback
- Rescue configuration with button
- Commit confirm for changes
- Auto record for diagnostics
- Software upgrades
- J-Web

Product Comparison

	SRX210	SRX240	SRX650
Maximum Performance and Capacity			
JUNOS Software version tested	JUNOS 9.5	JUNOS 9.5	JUNOS 9.5
Firewall performance (large packets)	750 Mbps	1.5 Gbps	7 Gbps
Firewall performance (IMIX)	250 Mbps	500 Mbps	2.5 Gbps
Firewall + routing PPS (64 Byte)	80 Kpps	200 Kpps	900 Kpps
AES256+SHA-1/3DES+SHA-1 VPN performance	75 Mbps	250 Mbps	1.5 Gbps
IPsec VPN Tunnels	256	1,000	3,000
IPS (intrusion prevention system)	80 Mbps	250 Mbps	900 Mbps
Antivirus	30 Mbps	85 Mbps	350 Mbps
Connections per second	2,000	9,000	30,000
Maximum concurrent sessions DRAM options	32 K / 64 K[5] 512 MB / 1 GB DRAM	64 K / 128 K[5] 512 MB / 1 GB DRAM	512 K[6] 2 GB DRAM
Maximum security policies	512	4096	8192
Maximum users supported	Unrestricted	Unrestricted	Unrestricted
Network Connectivity			
Fixed I/O	2 x 10/100/1000BASE-T + 6 x 10/100	16 x 10/100/1000BASE-T	4 x 10/100/1000BASE-T
I/O slots	1 x SRX Mini-PIM	4 x SRX Mini-PIM	8 x GPIM
Services and Routing Engine slots	N/A	N/A	2[3]
ExpressCard slot (3G WAN)	Yes	No	No
WAN/LAN interface options	See ordering information	See ordering information	See ordering information
Optional maximum number of PoE ports	Up to 4 ports of 802.3af with maximum 50 W	Up to 16 ports of 802.3af/at with maximum 150 W	Up to 48 ports of 802.3af/at with maximum 247 W
USB	2	2	2 per SRE
Routing			
BGP instances	10	20	64
BGP peers	8	32	256
BGP routes	8 K / 16 K[5]	32 K / 64 K[5]	1 M[6]
OSPF instances	10	20	64
OSPF routes	8 K / 16 K[5]	32 K / 64 K[5]	1 M[6]
RIP v1 / v2 instances	10	20	64
RIP v2 routes	8 K / 16 K[5]	32 K / 64 K[5]	1 M[6]
Static routes	8 K / 16 K[5]	32 K / 64 K[5]	1 M[6]

Product Comparison (continued)

	SRX210	SRX240	SRX650
Routing (continued)			
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
MPLS[4]			
Layer 2 VPN (VPLS)	Yes	Yes	Yes
Layer 3 VPN	Yes	Yes	Yes
LDP	Yes	Yes	Yes
RSVP	Yes	Yes	Yes
Circuit Cross-connect (CCC)	Yes	Yes	Yes
Translational Cross-connect (TCC)	Yes	Yes	Yes
Multicast[7]			
IGMP (v1, v2, v3)	Yes	Yes	Yes
PIM SM	Yes	Yes	Yes
PIM source-specific multicast (SSM)	Yes	Yes	Yes
Multicast inside IPsec tunnel	Yes	Yes	Yes
IPsec VPN			
Concurrent VPN tunnels	256	1000	3000
Tunnel interfaces	64	128	512
DES (56-bit), 3DES (168-bit) and AES (256-bit)	Yes	Yes	Yes
MD-5 and SHA-1 authentication	Yes	Yes	Yes
Manual key, Internet Key Exchange (IKE), public key infrastructure (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
Dynamic remote access VPN	Yes	Yes	No
IPsec NAT traversal	Yes	Yes	Yes
Redundant VPN gateways	Yes	Yes	Yes
User Authentication and Access Control			
Third-party user authentication	RADIUS, RSA SecureID, LDAP	RADIUS, RSA SecureID, LDAP	RADIUS, RSA SecureID, LDAP
RADIUS accounting	Yes	Yes	Yes
XAUTH VPN, Web-based, 802.X authentication	Yes	Yes	Yes
PKI certificate requests (PKCS 7 and PKCS 10)	Yes	Yes	Yes
Certificate Authorities supported	VeriSign, Entrust, Microsoft, RSA Keon, iPLanet, (Netscape), Baltimore, DoD PKI	VeriSign, Entrust, Microsoft, RSA Keon, iPLanet, (Netscape), Baltimore, DoD PKI	VeriSign, Entrust, Microsoft, RSA Keon, iPLanet, (Netscape), Baltimore, DoD PKI
Virtualization			
Maximum number of security zones	12	32	128
Maximum number of virtual routers	10	20	60
Maximum number of VLANs	64	512	4096
Encapsulations			
PPP/MLPPP	Yes	Yes	Yes
MLPPP maximum physical interfaces	1	4	12
Frame Relay	Yes	Yes	Yes
MLFR (FRF .15, FRF .16)	Yes	Yes	Yes
MLFR maximum physical interfaces	1	4	12
HDLC	Yes	Yes	Yes

Product Comparison (continued)

	SRX210	SRX240	SRX650
Address Translation			
Source NAT with Port Address Translation (PAT)	Yes	Yes	Yes
Static NAT	Yes	Yes	Yes
Destination NAT with PAT	Yes	Yes	Yes
IP Address Assignment			
Static	Yes	Yes	Yes
DHCP, PPPoE client	Yes	Yes	Yes
Internal DHCP server	Yes	Yes	Yes
DHCP relay	Yes	Yes	Yes
L2 Switching			
VLAN 802.1Q	Yes	Yes	Yes
Link Aggregation 802.3ad/LACP	Yes	Yes	Yes
Jumbo Frame (9216 Byte)	Yes	Yes	Yes
Spanning Tree Protocol (STP) 802.1D, RSTP 802.1w, MSTP 802.1s	Yes	Yes	Yes
Authentication 802.1x Port based and multiple supplicant	Yes	Yes	Yes
Traffic Management Quality of Service (QoS)			
Guaranteed bandwidth	Yes	Yes	Yes
Maximum bandwidth	Yes	Yes	Yes
Ingress traffic policing	Yes	Yes	Yes
Priority-bandwidth utilization	Yes	Yes	Yes
DiffServ marking	Yes	Yes	Yes
High Availability			
Active/active—L3 mode	Yes	Yes[3]	Yes[3]
Active/passive—L3 mode	Yes	Yes[3]	Yes[3]
Configuration synchronization	Yes	Yes[3]	Yes[3]
VRRP	Yes	Yes	Yes
Session synchronization for firewall and VPN	Yes	Yes[3]	Yes[3]
Session failover for routing change	Yes	Yes[3]	Yes[3]
Device failure detection	Yes	Yes[3]	Yes[3]
Link failure detection	Yes	Yes[3]	Yes[3]
Firewall			
Network attack detection	Yes	Yes	Yes
DoS and DDos protection	Yes	Yes	Yes
TCP reassembly for fragmented packet protection	Yes	Yes	Yes
Brute force attack mitigation	Yes	Yes	Yes
SYN cookie protection	Yes	Yes	Yes
Zone-based IP spoofing	Yes	Yes	Yes
Malformed packet protection	Yes	Yes	Yes
Unified Threat Management[2]			
Intrusion Prevention System (IPS)	Yes	Yes	Yes
Protocol anomaly detection	Yes	Yes	Yes
Stateful protocol signatures	Yes	Yes	Yes
Intrusion prevention system (IPS) attack pattern obfuscation	Yes	Yes	Yes
Customer signatures creation	Yes	Yes	Yes
Frequency of updates	Daily and emergency	Daily and emergency	Daily and emergency

Product Comparison (continued)

	SRX210	SRX240	SRX650
Unified Threat Management (continued)[2]			
Antivirus			
Express AV (packet-based AV)	Yes	Yes	Yes
File-based antivirus	Yes	Yes	Yes
Signature database	Yes	Yes	Yes
Protocols scanned	POP3, HTTP, SMTP, IMAP, FTP	POP3, HTTP, SMTP, IMAP, FTP	POP3, HTTP, SMTP, IMAP, FTP
Anti-spyware	Yes	Yes	Yes
Anti-adware	Yes	Yes	Yes
Anti-keylogger	Yes	Yes	Yes
Anti-spam	Yes	Yes	Yes
Integrated Web filtering	Yes	Yes	Yes
Redirect Web filtering	Yes	Yes	Yes
Content filtering	Yes	Yes	Yes
Based on MIME type, file extension, and protocol commands	Yes	Yes	Yes
System Management			
Web UI	Yes	Yes	Yes
Command-line interface	Yes	Yes	Yes
Network and Security Manager	Yes	Yes	Yes
STRM Series	Yes	Yes	Yes
Flash and Memory			
Memory minimum and maximum (DRAM)	512 MB, 1 GB	512 MB, 1 GB	2 GB
Memory slots	Fixed memory	Fixed memory	4 DIMM
Flash memory	1 GB	1 GB	2 GB CF internal on SRE, External slot empty, up to 2 GB CF supported
USB port for external storage	Yes	Yes	Yes
Dimensions and Power			
Dimensions (W x H x D)	11.1 x 1.75 x 7.1 in (28.2 x 4.4 x 18 cm)	17.5 x 1.75 x 16.1 in (44.4 x 4.4 x 40.8 cm)	17.5 x 3.5 x 18.2 in (44.4 x 8.8 x 46.2 cm)
Weight	7 lb (3.2 kg) Non-PoE / 8 lb (3.6 kg) PoE No interface modules	25 lb (11.3 kg) Non-PoE / 26 lb (11.8 kg) PoE No interface modules	24.9 lbs (11.3 kg) No interface modules 1 power supply
Rack mountable	Yes, 1 RU	Yes, 1 RU	Yes, 2 RU
Power supply (AC)	100–240 VAC, 60 W (Non-PoE) / 150 W PoE	100–240 VAC, 150 W Non PoE / 350 W PoE	100–240 VAC, Single 645 W or Dual 645 W
Maximum PoE power	50 W	150 W	247 W redundant, or 494 W non-redundant
Average power consumption	27 W Low Memory (LM), 28 W High Memory (HM), 84 W (PoE)	61 W (LM), 65 W (HM), 179 W (PoE)	122 W
Input frequency	50-60 Hz	50-60 Hz	47-63 Hz
Maximum current consumption	0.41 A @ 100 VAC (LM), 0.44 A @ 100 VAC (HM), 1.13 A @ 100 VAC (PoE)	1.0 A @ 100 VAC for LM 1.1 A @ 100 VAC for HM 3.0 A @ 100 VAC for PoE	5.3 A at 100 VAC with single PSU with PoE 8.3 A at 100 VAC with dual PSU with PoE
Maximum inrush current	80 A for LM/HM, 60 A for PoE	40 A for LM/HM, 45 A for PoE	45 A for 1/2 cycle

Product Comparison (continued)

	SRX210	SRX240	SRX650
Average heat dissipation	92 BTU/hr (SRX210B) 95 BTU/hr (SRX210H), 116 BTU/hr (SRX210H-PoE)	208 BTU/Hr (SRX240B) 222 BTU/Hr (SRX240H) 249 BTU/Hr (SRX240H-PoE)	319 BTU/Hr
Maximum heat dissipation	120 BTU/hr (SRX210B), 126 BTU/hr (SRX210H), 157 BTU/hr (SRX210H-PoE)	344 BTU/Hr (SRX210B) 369 BTU/Hr (SRX210H) 413 BTU/Hr (SRX210H-PoE)	699 BTU/Hr
Power supply (DC)	60 W @ 12 V (LM, HM), 150 W @ 48 V (PoE)	150 W Non-PoE / 350 W PoE	Single 645 W (12 V + PoE) or Dual 645 W
Redundant power supply (hot swappable)	No	No	Yes (up to maximum capacity of single PSU)
Acoustic noise level (Note: Per ISO 7779 Standard)	<50 dB	<60 dB	60.9 dB
Environment			
Operational temperature	32° to 104° F, (0° to 40° C)	32° to 104° F, (0° to 40° C)	32° to 104° F, (0° to 40°C)
Nonoperational temperature	4° to 158° F, (-20° to 70° C)	4° to 158° F, (-20° to 70° C)	4° to 158° F, (-20° to 70° C)
Humidity	10–90% noncondensing	10–90% noncondensing	10–90% noncondensing
Mean time between failures (Telcordia model)	15.2 years (SRX210B) 14.3 years (SRX210H) 10.4 years (SRX210H-PoE)	15.2 years (SRX240B) 14.3 years (SRX240H) 10.4 years (SRX240H-PoE)	9.6 years with redundant power
Certifications and Network Homologation			
USA			
Safety certifications	UL 60950-1	UL 60950-1	UL 60950-1
EMC certifications	FCC class B	FCC class A	FCC class A
Network homologation	TIA-968	TIA-968	TIA-966
Canada			
Safety certifications	CSA 60950-1	CSA 60950-1	CSA 60950-1
EMC certifications	ICES class B	ICES class A	ICES class A
Network homologation	CS-03	CS-03	CS-03
Australia			
Safety certifications	AS / NZS 60950-1	AS / NZS 60950-1	AS / NZS 60950-1
EMC certifications	AS / NZS CISPR22 Class B	AS / NZS CISPR22 Class A	AS / NZS CISPR22 Class A
Network homologation	AS / ACIF S 002, S 016, S 043.1, S043.2	AS / ACIF S 002, S 016, S 043.1, S043.2	AS / ACIF S 016
New Zealand			
Safety certifications	AS / NZS 60950-1	AS / NZS 60950-1	AS / NZS 60950-1
EMC certifications	AS / NZS CISPR22 Class B	AS / NZS CISPR22 Class A	AS / NZS CISPR22 Class A
Network homologation	PTC 217, PTC 273	PTC 217, PTC 273	PTC 217
Japan			
Safety certifications	CB Scheme	CB Scheme	CB Scheme
EMC certifications	VCCI Class B	VCCI Class A	VCCI Class A
Network homologation	Certificate for Technical Conditions	Certificate for Technical Conditions	Certificate for Technical Conditions
European Union			
Safety certifications	EN 60950-1	EN 60950-1	EN 60950-1
EMC certifications	EN 55022 Class B, EN 300386	EN 55022 Class A, EN 300386	EN 55022 Class A, EN 300386
Network homologation	CTR 12 / 13, CTR 21, DoC	CTR 12 / 13, CTR 21, CoC	CTR 12 / 13, DoC

1. BGP Route Reflector supported on SRX650. See ordering section for more information.
2. Unified Threat Management- antivirus, antispam, Web filtering and IPS require a subscription license to use the feature. Please see the ordering section for options. Content Filtering and UAC are part of the base software with no additional license.
3. High availability. VRRP supported on all SRX Series products. SRX240 and SRX650 will support high availability features in JUNOS 9.6.
4. Supported in 9.5 in packet mode without services.
5. When UTM is enabled capacities supported are low memory specifications, on high memory system options.
6. When UTM is enabled concurrent sessions supported is 50% 0f value shown.
7. Multicast features in SRX240 and SRX650 are supported as of the 9.6 release

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.**

Ordering Information

The following tables outline part numbers for SRX650, SRX240, and SRX210 base systems and options; associated WAN and LAN modules; and additional accessories.

MODEL NUMBER	DESCRIPTION
SRX650 Base System	
SRX650-BASE-SRE6-645AP	SRX650 Services Gateway with 1 Services Routing Engine (SRE), 4 x 10/100/1000BASE-T ports, 2 GB DRAM, 2 GB CF, fan tray, 645 W AC PoE power supply unit for SRX650. Provides 397 W system power @ 12 V and 247 W POE power @ 50 VDC. Works with 90-250 VAC input. Includes power cord and rack mount kit.
SRX650 Options	
Interface Modules	
SRX-GP-16GE	16-port 10/100/1000BASE-T XGPIM
SRX-GP-16GE-POE	16-port 10/100/1000BASE-T PoE XGPIM
SRX-GP-24GE	24-port 10/100/1000BASE-T XPIM, includes 4 SFP slots
SRX-GP-24GE-POE	24-port 10/100/1000BASE-T PoE XPIM, includes 4 SFP slots
SRX-GP-DUAL-T1-E1	Dual T1/E1 GPIM
SRX-GP-QUAD-T1-E1	QUAD T1/E1 GPIM
Power Supplies and Accessories	
SRX600-PWR-645AC-POE	Spare 645 W AC PoE power supply unit for SRX650 systems. One is included in SRX650 Base System (SRX650-BASE-SRE6-645AP).
SRX600-SRE6H SPARE	Spare SRE6-H for SRX650. One is included in SRX650 Base System (SRX650-BASE-SRE6-645AP).
SRX650-CHAS	SRX650 chassis including fan tray. No system processor (SRE) and no power supply unit.
SRX650-FAN-01	Spare SRX650 fan tray. One is included in SRX650 Chassis Spare (SRX650-CHAS), and included in SRX650 Base System (SRX650-BASE-SRE6-645AP)
SRX650-FILT-01 OPTIONAL	Not included in SRX650 Chassis Spare (SRX650-CHAS), and not included in SRX650 Base System (SRX650-BASE-SRE6-645AP). Optional, as this is not required for normal operations, but recommended for dusty environments.
Additional Software Feature Licenses	
SRX650-K-AV	One year subscription for Juniper-Kaspersky antivirus updates on SRX650
SRX650-IDP	One year subscription for IDP updates on SRX650

MODEL NUMBER	DESCRIPTION
Additional Software Feature Licenses (continued)	
SRX650-S-AS	One year subscription for Juniper-Symantec anti-spam updates on SRX650
SRX650-W-WF	One year subscription for Juniper-Websense Web filtering updates on SRX650
SRX650-SMB-CS	One year security subscription for enterprise - includes antivirus, WF, AS, and IDP on SRX650
SRX650-K-AV-3	Three year subscription for Juniper-Kaspersky antivirus updates on SRX650
SRX650-IDP-3	Three year subscription for IDP updates on SRX650
SRX650-S-AS-3	Three year subscription for Juniper-Symantec anti-spam updates on SRX650
SRX650-W-WF-3	Three year subscription for Juniper-Websense Web filtering updates on SRX650
SRX650-SMB-CS-3	Three year security subscription for enterprise - includes antivirus, WF, AS, and IDP on SRX650
SRX-BGP-ADV-LTU	Advanced BGP on SRX650 (Route Reflector)
SRX240 Base System	
SRX240B	SRX240 Services Gateway with 16 Gigabit Ethernet ports, 4 Mini-PIM slots, and base memory (512 MB RAM, 1 GB Flash)
SRX240H	SRX240 Services Gateway with 16 Gigabit Ethernet ports, 4 Mini-PIM slots, and high memory (1 GB RAM, 1 GB Flash)
SRX240H-POE	SRX240 Services Gateway with 16 Gigabit Ethernet ports, 4 Mini-PIM slots, and high memory (1 GB RAM, 1 GB Flash), with 16 ports PoE (150 W)
SRX240-RMK	SRX240 Rack mount kit for 19 in rack. Holds one unit.
Interface Modules	
SRX-MP-1SERIAL	1-port Sync Serial Mini Physical Interface Module (Mini-PIM) for branch SRX Series
SRX-MP-1ADSL2-A	1-port ADSL2+ Mini-PIM supporting ADSL/ADSL2/ADSL2+ Annex A
SRX-MP-1ADSL2-B	1-port ADSL2+ Mini-PIM supporting ADSL/ADSL2/ADSL2+ Annex B
SRX-MP-1SFP	1-port SFP Mini Physical Interface Module (Mini-PIM) for branch SRX Series
SRX-MP-1T1E1	1-port T1 or E1 Mini Physical Interface Module (Mini-PIM) for branch SRX Series
Additional Software Feature Licenses	
SRX240-K-AV	One year subscription for Juniper-Kaspersky antivirus updates on SRX240
SRX240-IDP	One year subscription for IDP updates on SRX240
SRX240-S-AS	One year subscription for Juniper-Symantec anti-spam updates on SRX240
SRX240-W-WF	One year subscription for Juniper-Websense Web filtering updates on SRX240
SRX240-SMB-CS	One year security subscription for enterprise - includes antivirus, WF, AS, and IDP on SRX240
SRX240-K-AV-3	Three year subscription for Juniper-Kaspersky antivirus updates on SRX240
SRX240-IDP-3	Three year subscription for IDP updates on SRX240
SRX240-S-AS-3	Three year subscription for Juniper-Symantec anti-spam updates on SRX240
SRX240-W-WF-3	Three year subscription for Juniper-Websense Web filtering updates on SRX240
SRX240-SMB-CS-3	Three year security subscription for enterprise - includes antivirus, WF, AS, and IDP on SRX240

Ordering Information (continued)

MODEL NUMBER	DESCRIPTION
Additional Software Feature Licenses (continued)	
SRX-RAC-5-LTU	Dynamic VPN Client: 5 simultaneous users for SRX210 and SRX240 only
SRX-RAC-10-LTU	Dynamic VPN Client: 10 simultaneous users for SRX210 and SRX240 only
SRX-RAC-25-LTU	Dynamic VPN Client: 25 simultaneous users for SRX210 and SRX240 only
SRX-RAC-50-LTU	Dynamic VPN Client: 50 simultaneous users for SRX240 only
SRX210 Base System	
SRX210B	SRX210 Services Gateway with 2 GbE + 6 Fast Ethernet ports, 1 Mini-PIM slot, 1 ExpressCard slot and base memory (512 MB RAM, 1 GB Flash)
SRX210H	SRX210 Services Gateway with 2 GbE+ 6 Fast Ethernet ports, 1 Mini-PIM slot, 1 ExpressCard slot and high memory (1 GB RAM, 1 GB Flash)
SRX210H-POE	SRX210 Services Gateway with 2 GbE + 6 Fast Ethernet ports, 1 Mini-PIM slot, 1 ExpressCard slot and high memory (1 GB RAM, 1 GB Flash), with 4 ports PoE (50 W)
Interface Modules	
SRX-MP-1SERIAL	1 port Sync Serial Mini Physical Interface Module (Mini-PIM) for branch SRX Series
SRX-MP-1ADSL2-A	1-port ADSL2+ Mini-PIM supporting ADSL/ ADSL2/ADSL2+ Annex A
SRX-MP-1ADSL2-B	1-port ADSL2+ Mini-PIM supporting ADSL/ ADSL2/ADSL2+ Annex B
SRX-MP-1SFP	1-port SFP Mini Physical Interface Module (Mini-PIM) for branch SRX Series
SRX-MP-1T1E1	1-port T1 or E1 Mini Physical Interface Module (Mini-PIM) for branch SRX Series
Additional Hardware	
SRX210-DESK-STAND	SRX210 desk top stand. Holds one unit.
SRX210-RMK	SRX210 Rack mount kit for 19 in rack. Holds one unit.
SRX210-WALL-KIT	SRX210 Wall mount kit. Holds one unit.
SRX210-PWR-60W-*	Spare SRX210 switching power supply, 60 W (non-PoE)
SRX210-PWR-150W-*	Spare SRX210 switching power supply, 150 W (PoE)

*See price list for country-specific power cord model numbers.

MODEL NUMBER	DESCRIPTION
Additional Software Feature Licenses	
SRX210-K-AV	One year subscription for Juniper-Kaspersky antivirus updates on SRX210
SRX210-IDP	One year subscription for IDP updates on SRX210
SRX210-S-AS	One year subscription for Juniper-Symantec anti-spam updates on SRX210
SRX210-W-WF	One year subscription for Juniper-Websense Web filtering updates on SRX210
SRX210-SMB-CS	One year security subscription for enterprise - includes antivirus, WF, AS, and IDP on SRX210
SRX210-K-AV-3	Three year subscription for Juniper-Kaspersky antivirus updates on SRX210
SRX210-IDP-3	Three year subscription for IDP updates on SRX210
SRX210-S-AS-3	Three year subscription for Juniper-Symantec anti-spam updates on SRX210
SRX210-W-WF-3	Three year subscription for Juniper-Websense Web filtering updates on SRX210
SRX210-SMB-CS-3	Three year security subscription for enterprise - includes antivirus, WF, AS, and IDP on SRX210
SRX-RAC-5-LTU	Dynamic VPN Client: 5 simultaneous users for SRX210 and SRX240 only
SRX-RAC-10-LTU	Dynamic VPN Client: 10 simultaneous users for SRX210 and SRX240 only
SRX-RAC-25-LTU	Dynamic VPN Client: 25 simultaneous users for SRX210 and SRX240 only
SRX-RAC-50-LTU	Dynamic VPN Client: 50 simultaneous users for SRX240 only
Small Form Factor Pluggable (SFP) Transceivers	
SRX-SFP-1GE-LH	SFP 1000BASE-LH Optical Transceiver
SRX-SFP-1GE-LX	SFP 1000BASE-LX Optical Transceiver
SRX-SFP-1GE-SX	SFP 1000BASE-SX Optical Transceiver
SRX-SFP-1GE-T	SFP 1000BASE-T Copper Transceiver
SRX-SFP-FE-FX	SFP 100BASE-FX Optical Transceiver

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.

1000281-002-EN June 2009

Printed on recycled paper.