SRX4100 AND SRX4200 FIREWALLS DATASHEET

Product Overview

The SRX4100 and SRX4200 Firewalls offer outstanding protection, performance, scalability, availability, and integrated security services. Designed for high-performance security services architectures and seamless integration of networking and security in a single platform, the SRX4100 and SRX4200 are best suited for enterprise data centers, campuses, and regional headquarters, with a focus on application visibility and control, intrusion prevention, advanced threat protection, authentication, confidentiality of information, and integrated cloud-based security. Both devices are powered by Junos OS, the industry-leading operating system that keeps the world's largest mission-critical enterprise networks secure.

Product Description

The Juniper Networks® SRX4100 and SRX4200 Firewalls are high-performance, next-generation firewalls and hardware-accelerated security services gateways that protect mission-critical data center networks, enterprise campuses, and regional headquarters. The SRX4100 and SRX4200 provide best-in-class security and advanced threat mitigation capabilities and integrate carrier-class routing.

The SRX4100 and SRX4200 deliver fully automated SD-WAN to both enterprises and service providers. Their high performance and scale allow the SRX4100 and SRX4200 to act as VPN hubs, terminating VPN/secure overlay connections in various SD-WAN topologies.

The SRX4100 and SRX4200 deliver a next-generation security solution that supports the changing needs of cloud-enabled enterprise networks, helping organizations realize their business objectives whether rolling out new services in an enterprise data center or campus, or connecting to the cloud. The SRX4100 and SRX4200 comply with industry standards, delivering the scalability, ease of management, secure connectivity, and advanced threat mitigation capabilities businesses need.

The SRX4100 and SRX4200 protect critical corporate assets such as next-generation firewalls, act as enforcement points for cloud-based security solutions, and provide application visibility and control to improve the user and application experience.

Architecture and Key Components

The SRX4100 and SRX4200 hardware and software architecture provides cost-effective security performance in a small 1 U form factor. Purpose-built to protect up to 40 Gbps Internet Mix (IMIX) firewall throughput network environments, the SRX4100 and SRX4200 incorporate multiple security services and networking functions on top of the industry-leading Juniper Networks Junos® operating system.

The SRX4100 supports up to 22 Gbps (IMIX) of firewall performance, 9 Gbps of next-generation firewall (application security, intrusion prevention, and logging), and 14.8 Gbps of IPsec VPN in data center, enterprise campus, and regional headquarter deployments with IMIX traffic patterns. The SRX4200 supports up to 44 Gbps of firewall performance, 18 Gbps of next-generation firewall, and up to 29.6 Gbps of IPsec VPN in data center, enterprise campus, and regional headquarter deployments with IMIX traffic patterns.

Table 1. SRX4100 and SRX4200 Statistics[1]

	SRX4100	SRX4200
Firewall throughput	40 Gbps	80 Gbps
Firewall throughput—IMIX	22 Gbps	44 Gbps
Firewall throughput with application security	19.9 Gbps	39.8 Gbps
IPsec VPN throughput-IMIX	14.8 Gbps	29.6 Gbps
Intrusion prevention	13.9 Gbps	27.7 Gbps
NGFW[2] throughput	9 Gbps	18 Gbps
Secure Web Access[3] throughput	6.7 Gbps	13.3 Gbps
Connections per second	250,000	500,000
Maximum session	5 million	10 million

[1]Performance, capacity and features listed are based on systems running Junos OS 21.4R1 and are measured under ideal testing conditions. Actual results may vary based on Junos OS releases and by deployments.

[2]Next-Generation Datacenter Firewall performance is measured with Firewall, Application Security and IPS enabled using 64KB transactions

[3]Secure Web Access Firewall performance is measured with Firewall, Application Security, IPS, SecIntel, and URL Filtering enabled using 64KB transactions

The SRX4100 and SRX4200 recognize more than 4,275 applications and nested applications in plain-text or SSL-encrypted transactions. The firewalls also integrate with Microsoft Active Directory and combine user information with application data to provide network-wide application and user visibility and control.

Features and Benefits

Table 2. SRX4100 and SRX4200 Features and Benefits

Business Requirement	Feature/Solution	SRX4100/SRX4200 Advantages
High performance	Up to 80 Gbps of firewall throughput (up to 40 Gbps of IMIX firewall throughput)	• Best suited for enterprise campus and data center edge deployments • Ideal for secure router deployments at the head office • Addresses future needs for scale and feature capacity
High-quality end-user experience	Application visibility and control	• Detects 3,500+ L3-L7 applications, including Web 2.0 • Controls and prioritizes traffic based on application and use role • Inspects and detects applications inside SSL-encrypted traffic
Advanced threat protection	IPS, antivirus, antispam, enhanced web filtering, Juniper Advanced Threat Prevention Cloud, Encrypted Traffic Insights, Threat Intelligence Feeds, and Juniper ATP Appliance	• Provides real-time updates to IPS signatures and protects against exploits • Implements industry-leading antivirus and URL filtering • Delivers open threat intelligence platform that integrates with third-party feeds • Protects against zero-day attacks • Restores visibility lost due to encryption, without the heavy burden of full TLS/SSL decryption
Professional-grade networking services	Routing, secure wire	• Supports carrier-class advanced routing and quality of service (QoS)
Highly secure	IPsec VPN, Remote Access/SSL VPN	• Provides high-performance IPsec VPN with dedicated crypto engine • Offers diverse VPN options for various network designs, including remote access and dynamic site-to-site communications • Simplifies large VPN deployments with auto VPN • Includes hardware-based crypto acceleration • Secure and flexible remote access SSL VPN with Juniper Secure Connect
Highly reliable	Chassis cluster, redundant power supplies	• Provides stateful configuration and session synchronization • Supports active/active and active/backup deployment scenarios • Offers highly available hardware with redundant power supply unit (PSU) and redundant fans • Delivers dedicated control and fabric link with seamless high availability
Easy to manage and scale	On-box GUI, Junos Space Security Director	• Enables centralized management for auto-provisioning, firewall policy management, Network Address Translation (NAT), and IPsec VPN deployments • Includes simple, easy-to-use on-box GUI for local management
Low TCO	Junos OS	• Integrates routing and security in a single device • Reduces OpEx with Junos OS automation capabilities

SRX4100

SRX4200

SRX4100 and SRX4200 Firewalls Specifications

Software Specifications

Firewall Services

- Stateful and stateless firewall
- Zone-based firewall
- Screens and distributed denial of service (DDoS) protection
- Protection from protocol and traffic anomalies
- Unified Access Control (UAC)

Network Address Translation (NAT)

- Source NAT with Port Address Translation (PAT)
- Bidirectional 1:1 static NAT
- Destination NAT with PAT
- Persistent NAT
- IPv6 address translation

VPN Features

- Tunnels: Site-to-site, hub and spoke, dynamic endpoint, AutoVPN, ADVPN, Group VPN (IPv4/ IPv6/Dual Stack)
- Juniper Secure Connect: Remote access/SSL VPN
- Configuration payload: Yes
- IKE Encryption algorithms: Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, Suite B
- IKE authentication algorithms: MD5, SHA-1, SHA-128, SHA-256, SHA-384
- Authentication: Pre-shared key and public key infrastructure (PKI) (X.509)
- IPsec (Internet Protocol Security): Authentication Header (AH) / Encapsulating Security Payload (ESP) protocol
- IPsec Authentication Algorithms: hmac-md5, hmac-sha-196, hmac-sha-256
- IPsec Encryption Algorithms: Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, Suite B
- Perfect forward secrecy, anti-reply
- Internet Key Exchange: IKEv1, IKEv2
- Monitoring: Standard-based dead peer detection (DPD) support, VPN monitoring
- VPNs GRE, IP-in-IP, and MPLS

High Availability Features

- Virtual Router Redundancy Protocol (VRRP) – IPv4 and IPv6
- Stateful high availability:
  - Dual box clustering
  - Active/passive
  - Active/active
  - Configuration synchronization
  - Firewall session synchronization
  - Device/link detection
  - In-Service Software Upgrade (ISSU)
- IP monitoring with route and interface failover

Application Security Services[3]

- Application visibility and control
- Application-based firewall
- Application QoS
- Advanced/application policy-based routing (APBR)
- Application Quality of Experience (AppQoE)
- Application-based multipath routing
- User-based firewall

Threat Defense and Intelligence Services[3]

- Intrusion prevention system
- Antivirus
- Antispam
- Category/reputation-based URL filtering
- SSL proxy/inspection
- Protection from botnets (command and control)
- Adaptive enforcement based on GeoIP
- Juniper Advanced Threat Prevention, a cloud-based SaaS offering, to detect and block zero-day attacks
- Adaptive Threat Profiling
- Encrypted Traffic Insights
- SecIntel to provide threat intelligence
- Juniper ATP Appliance, a distributed, on-premises advanced threat prevention solution to detect and block zero-day attacks

[3]Offered as advanced security subscription license.

Routing Protocols

- IPv4, IPv6, static routes, RIP v1/v2
- OSPF/OSPF v3
- BGP with route reflector
- IS-IS
- Multicast: Internet Group Management Protocol (IGMP) v1/v2; Protocol Independent Multicast (PIM) sparse mode (SM)/ source-specific multicast (SSM); Session Description Protocol (SDP); Distance Vector Multicast Routing Protocol (DVMRP); Multicast Source Discovery Protocol (MSDP); reverse path forwarding (RPF)
- Encapsulation: VLAN, Point-to-Point Protocol over Ethernet (PPPoE)
- Virtual routers
- Policy-based routing, source-based routing
- Equal-cost multipath (ECMP)

QoS Features

- Support for 802.1p, DiffServ code point (DSCP), EXP
- Classification based on VLAN, data-link connection identifier (DLCI), interface, bundles, or multifield filters
- Marking, policing, and shaping
- Classification and scheduling
- Weighted random early detection (WRED)
- Guaranteed and maximum bandwidth
- Ingress traffic policing
- Virtual channels

Network Services

- Dynamic Host Configuration Protocol (DHCP) client/server/ relay
- Domain Name System (DNS) proxy, dynamic DNS (DDNS)
- Juniper real-time performance monitoring (RPM) and IP monitoring
- Juniper flow monitoring (J-Flow)

Advanced Routing Services

- Packet Mode
- MPLS (RSVP, LDP)
- Circuit cross-connect (CCC), translational cross-connect (TCC)
- L2/L2 MPLS VPN, pseudo-wires
- Virtual private LAN service (VPLS), next-generation multicast VPN (NG-MVPN)
- MPLS traffic engineering and MPLS fast re-route

Management, Automation, Logging, and Reporting

- SSH, Telnet, SNMP
- Smart image download
- Juniper CLI and Web UI
- Juniper Networks Junos Space Security Director
- Python
- Junos events, commit and OP scripts
- Application and bandwidth usage reporting
- Debug and troubleshooting tools

Hardware Specifications

Table 3. SRX4100 and SRX4200 Hardware Specifications

Connectivity	SRX4100	SRX4200
Total onboard ports	8x1GbE/10GbE	8x1GbE/10GbE
Onboard small form-factor pluggable plus (SFP+) transceiver ports	8x1GbE/10GbE	8x1GbE/10GbE
Out-of-Band (OOB) management ports	1x1GbE	1x1GbE
Dedicated high availability (HA) ports	2x1GbE/10GbE (SFP/SFP+)	2x1GbE/10GbE (SFP/SFP+)
Console (RJ-45)	1	1
USB 2.0 ports (type A)	2	2
Memory and Storage		
System memory (RAM)	64 GB	64 GB
Secondary storage (SSD)	240 GB with 1+1 RAID	240 GB with 1+1 RAID
Dimensions and Power		
Form factor	1 U	1 U
Size (WxHxD)	17.48 x 1.7 x 25 in (44.39 x 4.31 x 63.5 cm)	17.48 x 1.7 x 25 in (44.39 x 4.31 x 63.5 cm)
Weight (device and PSU)	Chassis with two AC power supplies: 29 lb (13.15 kg) Chassis with two DC power supplies: 28.9 lb (13.06 kg) Chassis with package for shipping: 47.5 lb (21.54 kg)	Chassis with two AC power supplies: 29 lb (13.15 kg) Chassis with two DC power supplies: 28.9 lb (13.06 kg) Chassis with package for shipping: 47.5 lb (21.54 kg)
Redundant PSU	1+1	1+1

Connectivity	SRX4100	SRX4200
Power supply	2x 650 W redundant AC-DC/DC-DC PSU	2x 650 W redundant AC-DC/DC-DC PSU
Average power consumption	200 W	200 W
Average heat dissipation	685 BTU / hour	685 BTU / hour
Maximum current consumption	4A (for 110 V AC power) 2A (for 220 V AC power) 9A (for -48 V DC power)	4A (for 110 V AC power) 2A (for 220 V AC power) 9A (for -48 V DC power)
Maximum inrush current	50 A by 1 AC cycle	50 A by 1 AC cycle
Acoustic noise level	70 dBA	70 dBA
Airflow/cooling	Front to back	Front to back
Operating temperature	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operating humidity	5% to 90% noncondensing	5% to 90% noncondensing
Meantime between failures (MTBF)	221,729 hours (about 25.3 years)	221,729 hours (about 25.3 years)
FCC classification	Class A	Class A
RoHS compliance	RoHS 2	RoHS 2
Performance and Scale		
Routing/firewall (IMIX packet size) throughput Gbps[4]	22.5	44
Routing/firewall (1,518 B packet size) throughput Gbps[4]	40	80
IPsec VPN (IMIX packet size) Gbps[4]	14.8	29.6
Application visibility and control in Gbps[5]	19.9	39.8
Recommended IPS in Gbps[5]	13.9	27.7
Next-generation firewall in Gbps[6]	9	18
Secure Web Access firewall in Gbps[7]	6.7	13.3
Connections per second (CPS)	250,000	500,000
Maximum security policies	60,000	60,000
Maximum concurrent sessions (IPv4 or IPv6)	5 million	10 million
Route table size (RIB/FIB) (IPv4)	2 million/1.2 million	2 million/1.2 million
IPsec tunnels	7500	7500
Number of remote access/SSL VPN (concurrent) users	7500	7500
Multitenancy (LSYS/TSYS)	32/200	32/200

[4]Throughput numbers based on UDP packets and RFC2544 test methodology

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

[6]Next-Generation Datacenter Firewall performance is measured with Firewall, Application Security and IPS enabled using 64KB transactions.

[7]Secure Web Access Firewall performance is measured with Firewall, Application Security, IPS, SecIntel, and URL Filtering enabled using 64KB transactions

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services 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. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit https://www.juniper.net/us/en/products.html.

Ordering Information

To order Juniper Networks SRX Series Firewalls, and to access software licensing information, please visit the How to Buy page at https://www.juniper.net/us/en/how-to-buy/form.html.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240 1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.207.125.700