SRX4100 AND SRX4200 FIREWALLS DATASHEET

Product overview

The SRX4100 and SRX4200 firewalls offer industry-leading threat protection, performance, scalability, high availability, and integrated security services. Designed for high-performance throughput while preventing exploits, malware, and malicious traffic, the SRX4100 and SRX4200 are best suited for enterprise data centers, campuses, and regional headquarters, focusing on adopting a Zero Trust architecture.

The SRX4100 and SRX4200 seamlessly integrate networking and security in a single platform fixed-form-factor firewall. Both firewalls are powered by Junos® operating system (Junos OS) and managed by Security Director Cloud, which helps organizations operationalize Zero Trust and enable architectural transformation through a unified management experience and single-policy framework.

Product description

The Juniper Networks® SRX4100 and SRX4200 are high-performance, next-generation firewalls with hardware acceleration that protect mission-critical data center networks, enterprise campuses, and regional headquarters. The SRX4100 and SRX4200 are an integral part of the Juniper Connected Security framework, which extends security to every point of connection on the network to safeguard users, data, and the infrastructure from advanced threats.

The SRX4100 and SRX4200 integrate networking and security in a single platform to deliver industry-leading intrusion prevention and malware protection with, high-performance throughput, IPSec VPN, and easy policy management to secure the network reliably. Advanced application identification and classification enables greater visibility, enforcement, control, and protection over network traffic, application access, and data. These next-generation firewalls provide detailed analyses of application volume and usage, fine-grained application control policies, and traffic prioritization based on application information and context to reduce complexity across traditional, cloud, and hybrid IT networks.

The SRX4100 and SRX4200 deliver full automation 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.

Both SRX4100 and SRX4200 Firewalls are managed by Juniper Security Director Cloud, a unified management experience that connects the organization's current deployments with future architectural rollouts. Security Director Cloud uses a single policy framework enabling consistent security policies across any environment and expanding Zero Trust to all parts of the network from the edge into the data center. This provides unbroken visibility, policy configuration, administration, and collective threat intelligence all in one place. The SRX4100 and SRX4200 comply with industry standards, delivering scalability, ease of management, secure connectivity, and advanced threat mitigation capabilities that businesses need.

Architecture and key components

The SRX4100 and SRX4200 hardware and software architecture provides cost-effective security performance in a small 1 RU form factor. These firewalls incorporate multiple security services and networking functions on top of the industry-leading Junos OS.

The SRX4100 and SRX4200 recognize more than 4,800 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 1. SRX4100 and SRX4200 features and benefits

Business requirement	Feature/Solution	SRX4100/SRX4200 advantages
High performance	High-performance firewall	• Best suited for enterprise campus and data center edge deployments • Ideal for next-generation firewall deployments at the head office • Scalability and feature capacity meet future needs
High-quality end-user experience	Application visibility and control	• Continuous application updates provided by Juniper Threat Labs • 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 sandboxing, Encrypted Traffic Insights, and SecIntel Threat Intelligence feeds	• Provides IPS capabilities and real-time updates to signatures that effectively protect against exploits, proven most effective in the industry for the past five years confirmed by multiple third-party testing companies • Protects against malware and malicious web traffic • Delivers an open threat intelligence platform that provides a single point for all operational intelligence feeds • Protects against zero-day attacks • Stops rogue and compromised devices from disseminating malware • Restores visibility lost due to encryption without the heavy burden of full TLS/SSL decryption
Zero-day prevention	AI-Predictive Threat Prevention	• Predicts and prevents malware at line rate by using AI to identify threats from packet snippets effectively • Eliminates patient-zero infections • Provides network protection throughout the entire attack lifecycle, preventing reinfection from subsequent attacks, rather than just for the first 24 hours of an attack
Advanced 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 a 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
Embedded security in data center fabric	EVPN-VXLAN Type 5 routes	• Enhances tunnel inspection for VXLAN encapsulated traffic with Layer 4 to Layer 7 security services • Eases operations with Type 5 support through BGP • Does not require decapsulation of EVPN-VXLAN traffic
Highly reliable	Chassis cluster, redundant power supplies	• Provides stateful configuration and session state 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, Juniper Security Director Cloud	• Enables centralized management from Juniper's unified management experience with unbroken visibility, zero-touch provisioning, intelligent firewall policy management and scalability, 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 firewall specifications

Software specifications

Firewall services

- Stateful firewall services
- 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: 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)
  - Multi-Node HA (MNHA)
- IP monitoring with route and interface failover

Application security services[1]

- Application visibility and control
- 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[1]

- 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 threat intelligence
- Juniper ATP Virtual Appliance, a distributed, on-premises advanced threat prevention solution to detect and block zero-day attacks
- AI-Predictive Threat Prevention

[1]Offered as advanced security subscription license.

Routing protocols

- IPv4, IPv6, static routes, RIP v1/v2
- OSPF/OSPF v3
- BGP with route reflector
- EVPN-VXLAN
- 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

- 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

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

Management, automation, logging, and reporting

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

Hardware specifications

Table 2. SRX4100 and SRX4200 hardware specifications

Specifications	SRX4100	SRX4200
Connectivity		
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
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
Environmental and regulatory compliance		
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)

Specifications	SRX4100	SRX4200
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		
Firewall throughput (IMIX) throughput Gbps[2]	25	50
Firewall throughput (1,518 B) Gbps[2]	40	80
IPsec VPN throughput (IMIX) Gbps[2]	13	26
IPsec VPN throughput (1400B)[2]	17.5	35
Application security performance (TPS#/CPS**) in Gbps	35/16	70/32.5
Next-generation firewall (TPS#/CPS**) in Gbps[3]	30/8	60/16
Secure Web Access firewall (CPS**) in Gbps[4]	7	14.5
Advanced Threat (CPS)[5]	3.5	7.5
Connections per second (64B)	275,000	550,000
SSL connections per second	6,000	12,000
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 VPN tunnels	4,075	4,075

[2]Throughput numbers based on UDP packets and RFC2544 test methodology
[3]Next-generation firewall performance was measured with firewall, application security, and IPS enabled
[4]Secure Web Access Firewall performance is measured with Firewall, Application Security, IPS, SecIntel, and URL Filtering enabled
[5]Advanced Threat performance is measured with Firewall, Application Security, IPS, SecIntel, URL Filtering, and Malware Protection enabled
##TPS Method: Throughput performance of average HTTP sessions
**CPS Method: Short-lived sessions

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

Juniper Networks believes that connectivity is not the same as experiencing a great connection. Juniper's AI-Native Networking Platform is built from the ground up to leverage AI to deliver exceptional, highly secure, and sustainable user experiences from the edge to the data center and cloud. Additional information can be found at juniper.net or connect with Juniper on X (formerly Twitter), LinkedIn, 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
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

Juniper Networks | Driven by Experience™