

SRX4600 FIREWALL DATASHEET



Product Overview

The [SRX4600](#) Firewall is an industry-leading threat protection [next-generation firewall](#) that supports the changing needs of enterprise, cloud, and [service provider networks](#). Designed for high-performance throughput while preventing exploits, malware, and malicious traffic, the SRX 4600 is best suited for organizations with a focus on zero trust architecture. The SRX4600 seamlessly integrates networking and security in a single platform and is 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® SRX4600 next-generation firewall protects mission-critical data center and campus networks for enterprises, service providers, and cloud providers. It is an integral part of the Juniper® Connected Security framework, which extends security to every point on the network to safeguard users, data, and infrastructure from advanced threats. SRX4600 Firewall integrates networking and security in a single platform to deliver industry-leading intrusion prevention and malware protection with high performance throughput, IPSEC VPN, high scalability, 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. The firewall provides a detailed analysis of application volume and usage, fine-grained application control policies to allow or deny traffic based on dynamic application names or group names. Traffic is prioritized based on application information and context to reduce complexity across traditional, cloud, and hybrid IT networks.

SRX4600 also delivers fully automated SD-WAN to both enterprises and service providers. Due to its high performance and scale, the SRX4600 acts as a VPN hub and terminates VPN/secure overlay connections in various SD-WAN topologies.



It is 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 SRX4600 is powered by Junos® operating system, the industry- leading OS that keeps the world's largest mission-critical enterprise and service provider networks secure.

Architecture and Key Components

The SRX4600 hardware and software architecture provides cost-effective security in a small 1 RU form factor. Purpose built to protect network environments and provide Internet Mix (IMIX) firewall throughput of up to 400 Gbps, the SRX4600 incorporates multiple security services and networking functions on top of Junos OS. Best-in-class security and advanced threat mitigation capabilities on the SRX4600 are offered as 33 Gbps of next-generation firewall, 45.4 Gbps of intrusion prevention system (IPS), and up to 44 Gbps of IPsec VPN in the data center, enterprise campus, and regional headquarters deployments with IMIX traffic patterns.

Table 1. SRX4600 Statistics¹

| Performance | SRX4600 |
|--|-------------------|
| Firewall throughput—IMIX/1518 B | 400 Gbps/400 Gbps |
| Firewall throughput with application security | 45.7 Gbps |
| IPsec VPN throughput—IMIX/1400 B | 47.4/75.3 Gbps |
| Intrusion prevention system | 26 Gbps |
| Next-Generation Data Center Firewall ² throughput | 23.7 Gbps |
| Secure Web Access Firewall ³ throughput | 21.4 Gbps |
| Connections per second | 600,000 |
| Maximum session | 60 million |

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

² Next-Generation Data Center 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.

Features and Benefits

Table 2. SRX4600 Features and Benefits

| Business Requirement | Feature/Solution | SRX4600 Advantages |
|--|--|--|
| High performance | Express Path + | <ul style="list-style-type: none"> Provides automatic offload of all eligible flows for line-rate forwarding without additional configuration Delivers full inspection services to all flows regardless of size Demands no trade offs between performance and security Meets requirements for enterprise campus and data center edge deployments Addresses diverse needs and scales for service provider deployments |
| High-quality, end-user experience | Application visibility and control | <ul style="list-style-type: none"> Continuous application updates provided by Juniper Threat Labs Controls and prioritizes traffic based on application and use role Inspects and detects applications inside the SSL-encrypted traffic |
| Advanced threat protection | IPS, antivirus, antispam, enhanced web filtering, Juniper Advanced Threat Prevention Cloud sandboxing, Encrypted Traffic Insights, SecIntel, and Threat Intelligence Feeds | <ul style="list-style-type: none"> Provides IPS capabilities and real-time updates to signatures that effectively protect against exploits, proven most effective in the industry 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 | <ul style="list-style-type: none"> Predicts and prevents malware at line rate by using AI to effectively identify threats from packet snippets Eliminates patient-zero infections Provides protection that lasts for the full attack lifecycle—not merely 24 hours—so the network is safe from reinfection from subsequent attacks |
| Professional-grade networking services | Routing, secure wire | <ul style="list-style-type: none"> Supports carrier-class advanced routing and quality of service (QoS) |
| Highly secure | IPsec VPN, Remote access/SSL VPN | <ul style="list-style-type: none"> 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 |
| Embedded security in data center fabric | EVPN-VXLAN Type 5 routes | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> 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 fans |
| Easy to manage and scale | On-box GUI, Juniper Security Director Cloud | <ul style="list-style-type: none"> Enables centralized management from Juniper's unified management experience with unbroken visibility, zero-touch provisioning, intelligent firewall policy management and scalability. Supports Network Address Translation (NAT), and IPsec VPN deployments Includes simple, easy-to-use on-box GUI for local management |
| Low TCO | Junos OS | <ul style="list-style-type: none"> Integrates routing and security in a single device Reduces OpEx with Junos OS automation capabilities |

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
- Port Block Allocation method for carrier-grade NAT
- Deterministic NAT

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:
 - HA clustering
 - Active/active
 - Active/passive
 - Dual MACsec-enabled HA control ports (10GbE)
 - Dual MACsec-enabled HA fabric ports (10GbE)
 - Configuration synchronization
 - Firewall session synchronization
 - Device/link detection
 - Unified in-service software upgrade (unified ISSU)
- IP monitoring with route and interface failover

Application Security Services (offered as advanced security subscription license)

- 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 (offered as advanced security subscription license)

- IPS
- Antivirus
- Antispam
- Category/reputation-based URL filtering
- SSL proxy/inspection
- Protection from botnets (command and control)
- Adaptive enforcement based on GeoIP
- Juniper ATP, 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

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)/dense mode (DM)/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)



SRX4600

Hardware Specifications

Table 3. SRX4600 Hardware Specifications

| Specification | SRX4600 |
|--|--|
| Total onboard I/O ports | Up to 24x1GbE/10GbE (SFP+) ^a 4x40GbE/100GbE (QSFP28) |
| Out-of-Band (OOB) management ports | RJ-45 (1 Gbps) |
| Dedicated high availability (HA) ports | 2x1GbE/10GbE (SFP+) Control 2x1GbE/10GbE (SFP+) Data |
| Console | RJ-45 (RS232) |
| USB 2.0 ports (Type A) | 1 |
| Memory and Storage | |
| System memory (RAM) | 256 GB |
| Secondary storage (SSD) | 2x 1 TB M.2 SSD |
| Dimensions and Power | |
| Form factor | 1 U |
| Size (WxHxD) | 17.4 x 1.7 x 26.5 in (44.19 x 4.32 x 67.31 cm) With AC PEMs: 17.4 x 1.7 x 27.29 in (44.19 x 4.32 x 69.32 cm) With DC PEMs: 17.4 x 1.7 x 29.20 in (44.19 x 4.32 x 74.17 cm) |
| Weight (system and 2 power entry modules) | With AC PEMs: 38 lb (17.24 kg) Shipping weight: 45.47 lb (20.62 kg) With DC PEMs: 40 lb (18.14 kg) Shipping weight: 47.47 lb (21.53 kg) |
| Redundant PSU | 1+1 |
| Power supply | 2x 1600 W AC-DC PSU redundant 2x 1100 W DC-DC PSU redundant |
| Average power consumption | 650 W |
| Average heat dissipation | 2218 BTU/hour |
| Maximum current consumption | 12 A (for 110 V AC power) 6 A (for 220 V AC power) 24 A (for -48 V DC power) |
| Precision Time Protocol Timing Ports | |
| Time of day – RS-232 (EIA-23) | 1xRJ-45 |
| BITS clock | 1xRJ-48 |
| 10-MHz timing connector (GNSS) | 1xInput (COAX) 1xOutput (COAX) |
| Pulse per second connection (1-PPS) | 1xInput (COAX) 1xOutput (COAX) |
| Environmental and Regulatory Compliance | |
| Acoustic noise level | 69 dBA at normal fan speed, 87 dBA at full fan speed |
| Airflow/cooling | Front to back |
| Operating temperature | 32° to 104° F (0° to 40° C) |
| Operating humidity | 5% to 90% non-condensing |
| Mean time between failures (MTBF) | 111,626 hours (12.75 years) |
| FCC classification | Class A |
| RoHS compliance | RoHS 2 |
| NEBS compliance | Designed for NEBS Level 3 |

QoS Features

- Support for 802.1p, DiffServ code point (DSCP)
- Classification based on interface, bundles, or multifield filters
- Marking, policing, and shaping
- Classification and scheduling
- Weighted random early detection (WRED)
- Guaranteed and maximum bandwidth

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)

Management, Automation, Logging, and Reporting

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

| Specification | SRX4600 |
|--|-----------------------|
| Performance | |
| Routing/firewall (64 B packet size) throughput Gbps ⁴ | 104 Gbps |
| Routing/firewall (IMIX packet size) throughput Gbps ⁴ | 400 Gbps |
| Routing/firewall throughput Gbps ⁴ | 400 Gbps |
| IPsec VPN (IMIX packet size) Gbps ⁴ | 44.4 Gbps |
| IPsec VPN (1400 B packet size) Gbps ⁴ | 69.6 Gbps |
| Application security performance in Gbps ⁵ | 75.5 Gbps |
| Recommended IPS in Gbps ⁶ | 45.5 Gbps |
| Next-generation firewall in Gbps ⁶ | 33 Gbps |
| Secure Web Access firewall in Gbps ⁷ | 22.6 Gbps |
| Connections per second (CPS) | 600,000 |
| Maximum security policies | 80,000 |
| Maximum concurrent sessions (IPv4 or IPv6) | 60 million |
| Route table size (RIB/FIB) (IPv4 or IPv6 ⁸) | 4 million/1.2 million |
| IPsec tunnels | 7500 |
| Number of remote access/SSL VPN (concurrent) users | 7500 |

⁴There are eight dedicated 1GbE/10GbE ports. The four 40GbE/100GbE ports can use breakout cables to create 4x10GbE (SFP+) ports each, resulting in a total of 24x 10GbE ports.

⁵Throughput numbers based on UDP packets and RFC2544 test methodology.

⁶Next-Generation Data Center firewall performance is measured with Firewall, Application Security, and IPS enabled using 64KB transactions.

⁷Secure Web Access firewall performance is measured with Firewall, Application Security, IPS, Secintel, and URL Filtering enabled using 64KB transactions.

⁸IPv6 FIB scale is with 32-bit mask.

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For services specific information specific to SRX Series Firewalls, please read the Firewall Conversion Service or the SRX Series QuickStart Service datasheets. 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

