SRX4600 FIREWALL DATASHEET

Product overview

The SRX4600 is an industry-leading threat protection next-generation firewall that supports the changing needs of enterprise, cloud, and service provider networks. The SRX4600 is best suited for organizations focusing on Zero-Trust architecture and is designed for high performance throughput while preventing exploits, malware, and malicious traffic.
The SRX4600 seamlessly integrates networking and security in a single platform. It 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 Firewall protects mission-critical data center and campus networks for enterprises, service providers, and cloud providers. This Next-Generation Firewall (NGFW) 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. The 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 and 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.

The 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.

The firewall 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, enabling organizations to ensure secure architectures and experiences.

Powering the SRX4600 is Junos®, the industry's leading operating system responsible for keeping 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. The purpose-built firewall protects network environments and provides Internet Mix (IMIX) firewall throughput of up to 400 Gbps, and it 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 with intrusion prevention system (IPS) capabilities and IPsec VPN in the data center, enterprise campus, and regional headquarters deployments with IMIX traffic patterns.

Features and benefits

Table 1. SRX4600 Features and benefits

Business requirement	Feature/Solution	SRX4600 Advantages
High performance	Express Path +	• 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	• 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	• 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	• Predicts and prevents malware at line rate by using AI to identify threats from packet snippets effectively • 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	• Supports carrier-class advanced routing (BGP, OSPF v2/3, IS-IS, RIP v1/2/NG, Multicast ICMP, PIM, BFD, multiple routing instances) 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, IPsec and 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 fans
Easy to manage and scale	On-box GUI, Juniper Security Director Cloud, Security Director, powerful CLI and automation	• 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	• 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
- Port overloading, pool pairing, NAPT, NAT44, NAT66, NAPT, NAP-PT, NAT46, NAT64, Dual Stack Lite

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, SHA-512
- 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, hmac-sha-512
- IPsec Encryption Algorithms: Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, Suite B
- Perfect forward secrecy, anti-reply
- Diffie Hellmann groups from group14 to group24
- 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)
  - 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]

- IPS
- Antivirus
- Antispam
- Category/reputation-based URL filtering
- SSL proxy/inspection
- Protection from botnets (command and control)
- Adaptive enforcement based on GeoIP
- Juniper ATP Cloud, a cloud-based SaaS offering, detects and blocks 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 an advanced security subscription license

Routing protocols

- IPv4, IPv6, static routes, RIP v1/v2
- OSPF/OSPF v3
- BGP with route reflector
- BFD for quick detection
- 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)

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
- gRPC telemetry
- Debug and troubleshooting tools

SRX4600

Hardware specifications

Table 2. SRX4600 Hardware specifications

Specification	SRX4600
Total onboard I/O ports	Up to 24x1GbE/10GbE (SFP+) 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
Meantime between failures (MTBF)	111,626 hours (12.75 years)
FCC classification	Class A
RoHS compliance	RoHS 2
NEBS compliance	Designed for NEBS Level 3
Performance	
Firewall (IMIX) throughput in Gbps[2]	400
Firewall throughput (1518 B) in Gbps[2]	400
IPsec VPN throughput (IMIX) in Gbps[2]	44
IPsec VPN throughput (1400 B) in Gbps[2]	71
Application security performance (TPS##/CPS**) in Gbps[3]	92/41
Next-generation firewall (TPS##/CPS**) in Gbps[4]	90/21
Secure Web Access firewall (CPS**) in Gbps[5]	19
Advanced Threat (CPS**) Gbps[6]	10.5
Connections per second (64B)	570,000
SSL connections per second	16,000
Maximum concurrent sessions (IPv4 or IPv6)	60 million
Route table size (RIB/FIB) (IPv4)	4 million/1.2 million
IPsec VPN tunnels	7,500

[2]There are eight dedicated 1GbE/10GbE ports. The four 40GbE/100GbE ports can use breakout cables to create 4x10GbE (SFP+) ports each, totaling 24x10GbE ports.

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

[4]Next-Generation Data Center firewall performance is measured with Firewall, Application Security, and IPS enabled

[5]Secure Web Access firewall performance is measured with Firewall, Application Security, IPS, SecIntel, and URL Filtering enabled

[6]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

Security Director Cloud

Security Director Cloud is Juniper's simple and seamless management experience delivered in a single UI to connect customers' current deployments with their future architectural rollouts. Management is at the center of the Juniper Connected

Security strategy and helps organizations secure every point of connection on their network to safeguard users, data, and infrastructure.

Organizations can secure their architecture with consistent security policies across any environment—on-premises, cloud-based, cloud-delivered, and hybrid. At the same time, they can expand Zero Trust from the edge all the way into the data center and to the applications and microservices. With Security Director Cloud, organizations have unbroken visibility, policy configuration, administration, and collective threat intelligence all in one place.

Juniper meets customers where they are on their journey, helps them leverage their existing investments, and empowers them to transition to their preferred architecture at a pace that is best for business by automating their transition with Security Director Cloud.

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 the required levels of performance, reliability, and availability. For service-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

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™