

SRX4700 FIREWALL DATASHEET



Product Overview

As data centers evolve from traditional architecture to distributed, the firewall's role needs to expand. Rather than being a perimeter technology, firewalls need to be part of a security fabric woven throughout the network. A security fabric will ensure that security is maintained at every point of connection.

[Juniper Networks SRX4700](#) next-generation firewall is integral to this new architecture, and it empowers organizations to operationalize security across their networks. This 1U, power-efficient firewall features built-in zero-trust, Ethernet VPN-Virtual Extensible LAN ([EVPN-VXLAN](#)) fabric integration and AI-Predictive Threat Prevention to secure your network. The SRX4700 firewall delivers the industry's highest throughput, per rack unit, at up to 1.4 Tbps, and supports 400 Gbps interfaces with wire speed MACsec.

Product Description

Juniper Networks® SRX4700 is a high-performance, [next-generation firewall \(NGFW\)](#) designed for [service providers](#), cloud providers, and large enterprises. In addition, enterprises can deploy the SRX4700 as data center core and data center edge firewalls and as a secure [SD-WAN](#) hub. Combining industry-leading security effectiveness and carrier-grade routing with state-of-the-art switching, this platform delivers robust network security, effective threat protection, and comprehensive automation and mitigation capabilities.



NetSec  OPEN

Figure 1: Juniper SRX Firewalls have achieved the highest scores in security effectiveness by Cyber Ratings and NetSecOpen

SRX4700 delivers NGFW features that support the changing needs of cloud-enabled enterprise networks and data centers. Whether rolling out new services on an enterprise campus, connecting to the cloud seamlessly, complying with industry standards, or achieving operational efficiency, the SRX4700 empowers organizations to operationalize zero-trust principles at scale while realizing business objectives. The SRX4700 protects critical corporate assets with features such as intrusion prevention system (IPS), follow-the-user and follow-the-application access policies, and Juniper's AI-Predictive Threat Prevention. Furthermore, SRX4700 works with Juniper's cloud security solutions to secure hybrid-cloud environments with networkwide visibility and control, providing consistently secure on-premises and cloud environments.

For cloud providers, service providers, and enterprises, the hardware acceleration in SRX4700 protects data center core and edge workloads at Layer 7 at wirespeed with industry-leading security efficacy. The SRX4700 adheres to industry-standard EVPN type 5 and VXLAN protocols within these data centers, enabling the SRX4700 to act as a secure, fabric-aware leaf in the spine-leaf architecture and uniquely streamlining security workflows within the data center. And the SRX4700 does all this while delivering the highest firewall performance per rack unit of any data center firewall available today.

Service providers offering 4G and 5G services can take advantage of the proven software in SRX4700 that secures dozens of Tier 1 service providers around the world. Use cases supported with high-performance hardware acceleration include security gateway, Gi / N6 firewall, CGNAT, and roaming firewall. Service providers with power and space constraints can deploy the SRX4700 in both distributed and centralized locations and secure their networks at terabit speeds while consuming only a single rack unit within their data centers.

The SRX4700 participates in [Juniper's Connected Security Distributed Services Architecture](#), enabling organizations to scale both horizontally and elastically, and it

simplifies operational management of large-scale firewall networks. With this architecture, several SRX4700 platforms can work together as a single large logical firewall to provide security at higher performance and scale.

The SRX4700 is powered by [Junos® operating system](#), the OS that underpins and helps secure the world's largest mission-critical enterprise and service provider networks. It is managed by [Juniper Security Director Cloud](#), Juniper's 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.

Architecture and Key Components

The SRX4700 hardware and software architecture provides cost-effective security in a compact, scalable 1U form factor. Purpose built to protect network environments and provide Internet Mix (IMIX) firewall throughput of up to 1.4 Tbps, the SRX4700 incorporates multiple security services and networking functions on top of Junos OS, providing highly customizable threat protection, automation, and integration capabilities. Best-in-class advanced security capabilities on the SRX4700 are offered as 100 Gbps of NGFW, 110 Gbps of IPS, and up to 90 Gbps of IPsec VPN in the data center, enterprise campus, and regional headquarter deployments with IMIX traffic patterns.

Table 1. SRX4700 Performance and Capacity

| Feature | |
|---|-------------------|
| Firewall throughput— Internet MIX (IMIX)/1518 B | 1.4 Tbps/1.4 Tbps |
| Firewall throughput with application security | 150 Gbps |
| IPsec VPN throughput (IMIX PowerMode IPsec (PMI)) | 90 Gbps |
| Intrusion prevention system | 110 Gbps |

Features and Benefits

| Business Requirement | Feature/Solution | SRX4700 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 Requires 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"> Updates application continuously and decodes custom applications Controls and prioritizes traffic based on application and user role Inspects and detects applications inside SSL-encrypted traffic, including Web and SaaS |

| Feature | |
|------------------------|------------|
| NGFW throughput | 100 Gbps |
| Connections per second | 600,000 |
| Maximum sessions | 60 million |

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

Built-in Zero Trust

To increase trust and streamline operations, the SRX4700 features several built-in zero trust device capabilities, including an embedded Trusted Platform Module (TMP) 2.0 and cryptographically signed device ID. The SRX4700 supports RFC compliant Secure Zero Touch Provisioning (sZTP) to deploy products in your network efficiently, expediently, and remotely. Additionally, the SRX4700 supports MACsec at wire speed, ensuring data integrity, and confidentiality.

Connected Security Distributed Services Architecture

The SRX4700 is part of [Juniper's Connected Security Distributed Services Architecture](#) which revolutionizes data center security. With Juniper's Connected Security Distributed Services Architecture, firewall performance can scale horizontally by interconnecting traffic forwarding and security services across multiple geographic locations. Juniper's solution also provides automated failover and backup nodes for both forwarding and inspection components. In addition to redundancy and load balancing, Juniper Connected Security Distributed Services Fabric simplifies how large-scale data center firewall networks are managed and operated. Regardless of how many firewall engines across the various form factors (physical, virtual, containerized) are added, they can all be managed as one logical unit. The centralized management eliminates the complexity that has been an unintended consequence of a traditional scale-out approach.

| Business Requirement | Feature/Solution | SRX4700 Advantages |
|---|---|---|
| Advanced threat protection | NGFW Services: IPS, antivirus, antispam, Web filtering Juniper Advanced Threat Prevention Cloud: sandboxing, Encrypted Traffic Insights, SecIntel threat intelligence feed | <ul style="list-style-type: none"> Prevents exploits with 99.9% effectiveness; signatures update in real time Protects against known malware and malicious Web and DNS traffic Sandboxing for unknown malware across multiple OS types, including iOS, Windows, Android, and CentOS Delivers threat intelligence in an open platform to accommodate for third-party and custom threat feeds Detects threats hidden inside encrypted traffic without decrypting |
| Zero-day protection | Juniper's 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 Auto-generates protective signatures that remain active for the full attack lifecycle, keeping the network safe from subsequent attacks |
| Secure data transactions | Juniper Secure Connect: 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 |
| Advanced networking services | Routing, secure wire | <ul style="list-style-type: none"> Supports carrier-class advanced routing and quality of service (QoS) |
| Security embedded into the data center fabric | EVPN-VXLAN (EVPN Type 5 route) | <ul style="list-style-type: none"> Enhances tunnel inspection for VXLAN encapsulated traffic with Layer 4-7 security services Eases operations with Type 5 support through BGP Does not require decapsulation for EVPN-VXLAN traffic |
| Reliability | 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 | Juniper Security Director Cloud, on-box GUI | <ul style="list-style-type: none"> Provides centralized management via Juniper's unified management experience, including zero-touch provisioning (ZTP), unbroken visibility, intelligent rule placement, and simplified policy configuration and automation Supports Network Address Translation (NAT), and automated IPsec VPN deployments via wizards Supports on-box GUI |
| Built-in zero trust capabilities | DevID with TPM 2.0 Module | <ul style="list-style-type: none"> Verifies the device's trust posture easily Provides cryptographically signed device ID that supports RFC-compliant sZTP for hardware and software attestation Mitigates the risks of supply chain attacks |
| Low TCO | Junos OS | <ul style="list-style-type: none"> Integrates routing and security capabilities into a single device Reduces OpEx with Junos OS automation capabilities Automates integration with other devices running Junos OS, such as MX, PTX, and ACX routers, and EX and QFX switches |

*Exploit block rate results tested by CyberRatings' 2023 Enterprise Firewall test report



Figure 2: SRX4700

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)
- Integration with Juniper Mist™ Access Assurance

Carrier-Grade Network Address Translation (CGNAT)

- Carrier-grade Network Address Translation (Large-scale NAT)
- IPv4 and IPv6 address translation NAT44, NAPT44, NAT66, NAPT66, NAT64, NAT46
- Static and dynamic 1-1 translation
- Source NAT with Port Address Translation (PAT)
- Destination NAT with Port Address Translation (PAT)
- Port Block Allocation (PBA)
- Deterministic NAT (DetNAT)
- Port overload

- Persistent NAT (enables EIM/EIF)
- Twice-NAT44
- DS-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,3DES-CBC, AEC-CBC, AES-GCM, Suite B
- Authentication: Pre-shared key and public key infrastructure (PKI) (X.509)
- 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-replay
- Internet Key Exchange: IKEv1, IKEv2
- Monitoring: Standards-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
 - Configuration synchronization
 - Firewall session synchronization
 - Device/link detection
 - Unified in-service software upgrade (unified ISSU)
- IP monitoring with route and interface failover
- Chassis cluster HA and Multinode HA (MN-HA)

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)

- Intrusion prevention system
- AI-Predictive Threat Prevention
- 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

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)/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)
- EVPN-VXLAN (EVPN Type 5 route)

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
- 8 queues per port

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-MIBs & Traps
- Smart image download
- Juniper CLI, Web UI, NetCONF, XML APIs, RMON
- Juniper Security Director Cloud
- Python
- Junos OS events, commit, and OP scripts
- Application and bandwidth usage reporting
- Debug and troubleshooting tools

Hardware Specifications

Table 3. SRX4700 Hardware Specifications

| Specification | SRX4700 |
|--|--|
| Connectivity | |
| Total onboard I/O ports | 2 x 400 GbE (QSFP56-DD) 10 x 100GbE (QSFP28) 16 x 50 GbE (SFP56) |
| Out-of-Band (OOB) management ports | 1 Gbps (RJ-45) |
| Dedicated high availability (HA) ports | 1 x 1 GbE (SFP) Control 1 x 1 GbE (SFP) Data |
| Console | 1 (RJ-45) |
| USB 3.0 ports (Type A) | 1 |
| Storage | |
| Storage (SSD) | 2x1TB M.2 SSD or 1 x 1TB M.2 SSD + 1 x 2TB M.2 SSD |
| Dimensions and Power | |
| Form factor | 1U |
| Size (W x H x D) | 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) |
| Dimensions and Power | |
| Form factor | 1U |
| Size (W x H x D) | 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 (device and PSU) | Chassis with AC power supplies: 40 lb (18.2 kg) Chassis with DC power supplies: 42 lb (19.1 kg) |
| Redundant PSU | 1+1 |
| Power supply | 2 x 2200 W AC PSU redundant 2 x 2200 W DC PSU redundant |

| Specification | SRX4700 |
|---|---|
| Maximum current consumption | 8.2 A (for 220 V AC power) 16.4 A (for 110 V AC Lowline power) 37.5 A (for 48 V DC power) |
| Environment and Regulatory Compliance | |
| Acoustic noise level | 78 dBA at normal fan speed, 92 dBA at full fan speed |
| Airflow/cooling | Front to back |
| Operating temperature | 32° to 104° F (0° to 40° C at 6000 ft altitude) |
| Operating humidity | 5% to 85% non-condensing |
| Meantime between failures (MTBF) | 133,440 hours (15.23 years) |
| FCC classification | Class A |
| RoHS compliance | RoHS 6 |
| FCC classification | Class A |
| NEBS compliance | Designed for NEBS Level 3 |
| Performance and Scale | |
| Routing/firewall (IMIX packet size) throughput Tbps | 1.4 Tbps |
| Routing/firewall throughput Tbps | 1.4 Tbps |
| IPsec VPN (IMIX packet size) Gbps | 90 Gbps |
| Application security performance in Gbps | 150 Gbps |
| Recommended IPS in Gbps | 110 Gbps |
| Next-generation firewall in Gbps | 100 Gbps |
| Connections per second (CPS) | 600,000 |
| Maximum security policies | 100,000 |
| Maximum concurrent sessions (IPv4 or IPv6) | 60 million |
| Route table size (RIB/FIB) (IPv4 or IPv6) | 4 million/1.2 million |
| IPsec tunnels | 15,000 |
| Number of remote access/SSL VPN (concurrent) users | 7,500 |

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 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

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.

[Statement of Product Direction](#)

The information on this page may contain Juniper's development and plans for future products, features, or enhancements ("SOPD Information"). SOPD Information is subject to change at any time, without notice. Juniper provides no assurances, and assumes no responsibility, that future products, features, or enhancements will be introduced. In no event should any purchase decision be based upon reliance of timeframes or specifics outlined as part of SOPD Information, because Juniper may delay or never introduce the future products, features, or enhancements.

Any SOPD Information within, or referenced or obtained from, this website by any person does not give rise to any reliance claim, or any estoppel, against Juniper in connection with, or arising out of, any representations set forth in the SOPD Information. Juniper is not liable for any loss or damage (howsoever incurred) by any person in connection with, or arising out of, any representations set forth in the SOPD Information.

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

