SRX4300 FIREWALL DATASHEET

Product Overview

The firewall's role must expand as data centers evolve from traditional architecture to distributed. Rather than being a perimeter technology, firewalls need to be part of a security fabric woven throughout the network. A security fabric ensures that security is maintained at every point of connection.
Juniper Networks SRX4300 next-generation firewall is integral to this new architecture, which empowers organizations to operationalize security across their networks. To secure your network, this 1U, power-efficient firewall delivers built-in Zero Trust, Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) fabric integration, and AI-Predictive Threat Prevention. The SRX4300 supports multiple 100 Gbps interfaces with wire speed MACsec.

Product Description

Juniper Networks® SRX4300 Firewall is a high-performance, next-generation firewall (NGFW) designed to safeguard your enterprise campus, data center edge, and core. It also supports roaming and SD-WAN secure hub firewall use cases. By combining carrier-grade routing with state-of-the-art switching, this platform delivers robust security, effective threat detection, and comprehensive automation and mitigation capabilities.

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

The SRX4300 delivers NGFW features that support the changing needs of cloud-enabled enterprise networks and data centers. Whether rolling out new services within an enterprise campus, connecting to the cloud seamlessly, complying with industry standards, or achieving operational efficiency, the SRX4300 empowers organizations to operationalize Zero Trust principles at scale while realizing their business objectives. The SRX4300 protects critical corporate assets with features such as an intrusion prevention system (IPS), follow-the-user and follow-the-application access policies, and Juniper's AI-Predictive Threat Prevention. Furthermore, the SRX4300 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.

As network architectures become more distributed and decentralized, Juniper Networks SRX Series firewalls ensure seamless integration with other Juniper and third-party networking platforms. At the same time, the NGFWs facilitate architectural transformation, taking organizations from on-premises to hybrid cloud environments seamlessly and cost-effectively. SRX Series firewalls are the first to implement industry-standard Ethernet VPN (EVPN) type 5 and Virtual Extensible LAN (VXLAN) protocols within data center environments, enabling the SRX4300 to act as a secure, fabric-aware leaf in the data center spine-leaf architecture.

The SRX4300 participates in the industry-first Connected Security Distributed Services Architecture, enabling organizations to scale horizontally and elastically, simplifying the operational management of large-scale firewall networks. With this architecture, several SRX4300 platforms can work together as a single large logical firewall to provide security at higher performance and scale.

The SRX4300 is powered by the Junos® operating system (Junos OS), which 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 SRX4300 hardware and software architecture provides cost-effective security in a compact, scalable 1U form factor. Purpose-built to protect network environments, the SRX4300 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 SRX4300 are ideal for data center, enterprise campus, and regional headquarters deployments with IMIX traffic patterns.

Built-in Zero Trust

The SRX4300 features built-in Zero Trust device capabilities to increase trust and streamline operations, including an embedded Trusted Platform Module (TMP) 2.0 and cryptographically signed device ID. The SRX4300 supports RFC-compliant Secure Zero Touch Provisioning (sZTP) to efficiently, expediently, and remotely deploy products in your network. Additionally, the SRX4300 supports MACsec at wire speed, ensuring data integrity and confidentiality.

Connected Security Distributed Services Architecture

The SRX4300 is part of Juniper's Connected Security Distributed Services Architecture, revolutionizing 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 locations. Juniper's solution also provides automated failover and backup nodes for forwarding and inspection components. In addition to redundancy and load balancing, Juniper's Connected Security Distributed Services Architecture simplifies how large-scale data center firewall networks are managed and operated. Regardless of how many firewall engines are added across physical, virtualized, and containerized form factors, they can be managed as one logical unit. This centralized management eliminates the complexity that has been an unintended consequence of a traditional scale-out approach.

Features and Benefits

Business Requirement	Feature/Solution	SRX4300 Advantages
High performance	Hardware-accelerated encryption/decryption	• Offloads CPU-intensive encryption/decryption tasks • Improves performance for SSL and IPsec
High-quality end user experience	Application visibility and control	• 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
Advanced threat protection	NGFW Services: IPS, antivirus, antispam, Web filtering Juniper Advanced Threat Prevention Cloud: sandboxing, Encrypted Traffic Insights, SecIntel threat intelligence feeds	• 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 third-party and custom threat feeds • Detects threats hidden inside encrypted traffic without decrypting
Zero-day protection	Juniper's 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 • 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	• 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
Advanced networking services	Routing, secure wire	• Supports carrier-class advanced routing and quality of service (QoS)
Security embedded into the data center fabric	EVPN-VXLAN (EVPN Type 5 route)	• 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

Business Requirement	Feature/Solution	SRX4300 Advantages
Reliability	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	Juniper Security Director Cloud, on-box GUI	• 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	• 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	• Integrates routing and security capabilities into a single device • Reduces OpEx with Junos OS automation capabilities • Automated integration with other devices running Junos OS, such as Juniper MX, PTX, and ACX routers; EX and QFX switches, and Cloud-Native Contrail Networking (CN2)

[1]Exploit block rate results tested by CyberRatings' 2023 Enterprise Firewall test report

Figure 2: SRX4300 firewall

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)
- Persistent NAT (EIM/EIF)
- Port Block Allocation (PBA)
- Deterministic NAT (DetNAT)
- Port overload
- 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)
- 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-replay
- 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
  - BFD monitoring
- Chassis cluster HA and Multinode HA (MNHA)

Application Security Services[2]

- 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[2]

- 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 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

[2]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
- EVPN-VXLAN (EVPN Type 5 route)
- 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

- 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-MIBs, Traps
- Smart image download
- Juniper CLI and Web UI, NetCONF, XML APIs, RMON
- Juniper Security Director Cloud

- Python
- Junos events, commit and OP scripts
- Application and bandwidth usage reporting
- Debug and troubleshooting tools

Hardware Specifications

Table 1. SRX4300 Hardware Specifications

Specifications	SRX4300
Connectivity	
Onboard ports	8 x 1 GbE/2.5 GbE/5 GbE/10 GbE BASE-T
Onboard small form-factor pluggable plus (SFP+) transceiver ports	8 x 1 GbE/10 GbE SFP+ 4 x 1 GbE/10 GbE/25 GbE SFP28 6 x 40 GbE/100 GbE QSFP28
Out-of-Band (OOB) management ports	1 x 1 GbE G (RJ-45)
Dedicated high availability (HA) ports	2 x 1 GbE SFP
Console	1 (RJ-45)
USB 3.0 ports (Type A)	1
Storage	
Storage (SSD)	1 x 120 GB (primary), 1 x 960 GB (secondary + logging disk)
Dimensions and Power	
Form factor	1U
Size (W x H x D)	17.28 x 1.74 x 18.20 in (43.89 x 4.42 x 46.23 cm)
Weight (device and PSU)	Chassis with two AC PSU: 20.2 lb (9.2 kg) Chassis with two DC PSU: 20.5 lb (9.3 kg) Chassis with package: 36.6 lb (16.6 kg)
Redundant PSU	1+1
Power supply	2 x 850W AC PSU redundant 2 x 850 W DC PSU redundant
Average heat dissipation	1 x DC PSU (40V): 1221.5 BTU/h 2 x DC PSU (40V): 1224.9 BTU/h 1 x AC PSU (110V): 1206.2 BTU/h 1 x AC PSU (230V): 1175.5 BTU/h 2 x AC PSU (110V): 1228.4 BTU/h 2 x AC PSU (230V): 1206.2 BTU/h
Maximum current consumption	4.67 A (for 110 V AC PSM) 2.188 A (for 230 V AC PSM) 11.53 A (for -40 V DC Power)
Maximum inrush current	40 A for 1 cycle of AC (AC PSM) 40 A-pk (DC PSM)
Environment and Regulatory Compliance	
Airflow/cooling	Front to back
Operating temperature	32° to 104° F (0° to 40° C at 6000 ft altitude)
Operating humidity	5% to 90% non-condensing
Meantime between failures (MTBF)	Over 100,000 hours (12 years)
FCC classification	Class A
RoHS compliance	RoHS 6
Performance and Scale	
Firewall throughput[3] (IMIX) in Gbps	70
Firewall throughput[3] (1518B) in Gbps	98
IPsec VPN throughput[3] (IMIX) in Gbps	40
IPsec VPN throughput[3] (1400B) in Gbps	94
Application security performance (TPS[##]) in Gbps	85/45
Next-generation firewall (TPS[##])[4] in Gbps	83/24
Secure Web Access Firewall (CPS[**]) in Gbps	21
Advanced Threat (CPS[**])[6] in Gbps	11
Connections per second (64B)	800,000
SSL connections per second	10,000
Maximum concurrent sessions (IPv4 or IPv6)	10 Million
Route table size (RIB/FIB) (IPv4)	2 Million/1.2 Million
IPsec VPN tunnels	4,000

[3]Throughput numbers based on UDP packets and RFC2544 test methodology
[4]Next-generation 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

Juniper Mist WAN Assurance and AI-Native Operations

Alternatively, the SRX4300 firewall can be operated and orchestrated through the Juniper Mist Cloud. Mist AI delivers unprecedented automation using a combination of artificial intelligence, machine learning algorithms, and data science techniques to save time, maximize IT productivity, and deliver the best experience to digital users.

Juniper Mist WAN Assurance is built on the Juniper Mist Cloud and delivers full lifecycle management and operations, including AI-Native insights, automated speed tests, dynamic packet capture (dPCAP), anomaly detection, and root cause identification that focuses on end users' experience. For Day 0 and Day 1 operations, WAN Assurance also provides orchestration, administration, and ZTP for SRX4300. See the WAN Assurance Datasheet for more information.

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 the 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