SRX1600 FIREWALL DATASHEET

Product Overview

As data centers evolve from traditional architectures 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 ensures that security is maintained at every point of connection. Juniper's Connected Security Distributed Services Architecture, managed by Juniper Security Director Cloud, offers a high-performance, scalable, and easy-to-manage firewall solution to secure today's distributed data centers. Juniper Networks SRX1600 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 SRX1600 delivers next-generation firewall throughput of 21 Gbps per rack unit and supports 25 Gbps interfaces with wire speed MACsec.

Product Description

Juniper Networks® SRX1600 Firewall is a high-performance, next-generation firewall (NGFW) designed to safeguard your enterprise campus edge, data center edge, and branch offices. It also supports roaming, SD-WAN large branch, and SD-WAN secure hub use cases. Combining industry-leading security efficacy 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.

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

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 SRX1600 to act as a secure, fabric-aware leaf in the data center spine-leaf architecture.

The SRX1600 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 SRX1600 platforms can work together as a single large logical firewall to provide security at higher performance and scale.

The SRX1600 is powered by the 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 SRX1600 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 9 Gbps, the SRX1600 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 SRX1600 are offered as 21 Gbps of NGFW, 21 Gbps of IPS, and up to 5.5 Gbps of IPsec VPN in the data center, enterprise campus, and regional headquarters deployments with IMIX traffic patterns.

Built-in Zero Trust

To increase trust and streamline operations, the SRX1600 features several built-in zero trust device capabilities, including an embedded Trusted Platform Module (TMP) 2.0 and cryptographically signed device ID. The SRX1600 supports RFC compliant Secure Zero Touch Provisioning (sZTP) to deploy products in your network efficiently, expediently, and remotely. Additionally, the SRX1600 supports MACsec at wire speed, ensuring data integrity and confidentiality.

Connected Security Distributed Services Architecture

The SRX1600 is part of Juniper's Connected Security Distributed Services Fabric 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. The Juniper solution also provides automated failover and backup nodes for both 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 across the various form factors 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.

Features and Benefits

Business Requirement	Feature/Solution	SRX1600 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[2]; 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	• 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	• 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 • Ensures 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 routes)	• Enhances tunnel inspection for VXLAN encapsulated traffic with Layers 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	• 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

Business Requirement	Feature/Solution	SRX1600 Advantages
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 devices' trust posture easily • Provides cryptographically signed device ID that supports RFC8572-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 • Automates integration with Cloud-Native Contrail Networking (CN2) and other devices running Junos OS, such as Juniper MX, PTX, and ACX routers, and EX and QFX switches

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

Figure 2: SRX1600 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)
- User role-based firewall
- SSL inspection
- 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 and Port Control Protocol (PCP)

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-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)
  - IP monitoring with route and interface failover

  - BFD monitoring
- Chassis cluster HA and Multinode HA (MNHA)

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 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

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
- Hierarchical shaping and policing
- Virtual channels

Switching Features

- ASIC-based Layer 2 forwarding
- MAC address learning
- VLAN addressing and integrated routing and bridging (IRB) support
- Link aggregation and LACP
- Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED)
- STP, RSTP, MSTP
- Multiple VLAN Registration Protocol (MVRP)
- 802.1x authentication
- MACsec

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

Hardware Specifications

Table 3. SRX1600 Hardware Specifications

Specifications	SRX1600
Connectivity	
Onboard ports	16 x 1 GbE 10/100/1000 BASE-T
Onboard small form-factor pluggable plus (SFP+) transceiver ports	4 x 1 GbE/10 GbE SFP+ 2 x 1 GbE/10 GbE/25 GbE SFP28
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
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 power supplies: 15.7 lb (7.1 kg) Chassis with two DC power supplies: 15.9 lb (7.2 kg) Chassis with package for shipping: 32.8 lb (14.9 kg)
Redundant PSU	1+1
Power supply	2 x 450 W AC PSU redundant 2 x 650 W DC PSU redundant
Average heat dissipation	1 x DC PSU (40V): 487.9 BTU/h 2 x DC PSU (40V): 498 BTU/h 1 x AC PSU (110V): 467.5 BTU/h 1 x AC PSU (230V): 445.3 BTU/h 2 x AC PSU (110V): 510 BTU/h 2 x AC PSU (230V): 501.6 BTU/h
Maximum current consumption	2 A (for 110 V AC PSM) 1 A (for 230 V AC PSM) 4.7 A (for -40 V DC PSM)
Maximum inrush current	50 A for 1 cycle of AC (AC PSM) 40 A-pk (DC PSM)
Environment and Regulatory Compliance	
Acoustic noise level	58 dB (max)
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)	9 Gbps
Firewall throughput[3] (1518B)	24 Gbps
IPsec VPN throughput[3] (IMIX)	5.5 Gbps
IPsec VPN throughput[3] (1400B)	18 Gbps
Application security performance (TPS#/CPS**)	21.5 Gbps/5.3 Gbps
Next-generation firewall (TPS#/CPS**)[4]	21 Gbps/2.75 Gbps
Secure Web Access Firewall (CPS**)	2.5 Gbps
Advanced Threat (CPS)[6]	1.3 Gbps
Connections per second (64B)	95,000
SSL connections per second	2,400
Maximum concurrent sessions (IPv4 or IPv6)	2 Million
Route table size (RIB/FIB) (IPv4)	2 Million/1 Million
IPsec VPN tunnels	2,000

[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 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

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

Juniper Networks | Driven by Experience™