SRX1500 FIREWALL DATASHEET

Next-Generation Firewall For The Distributed Enterprise

Product Overview

The SRX1500 is a next-generation firewall and security services gateway offering outstanding protection, performance, scalability, availability, and security service integration. Designed for port density, a high-performance security services architecture, and seamless integration of networking and security in a single platform, the SRX1500 is best suited for client protection in enterprise campus, regional headquarters, or cloud-based security solutions with a focus on application visibility and control, intrusion prevention, and advanced threat protection. The SRX1500 powered by Junos OS is the industry-leading operating system that keeps the world's largest and most mission-critical enterprise networks secure.

Product Description

The Juniper Networks® SRX1500 is a high-performance next-generation firewall and security services gateway that protects mission-critical networks at campuses, and regional headquarters, and large branch offices. The SRX1500 provides best-in-class security, threat detection, and mitigation capabilities, integrating carrier-class routing and feature-rich switching in a single platform.

The SRX1500 delivers a next-generation security solution that supports the changing needs of cloud-enabled enterprise networks. Whether rolling out new services in an enterprise campus, connecting to the cloud, complying with industry standards, or achieving operational efficiency, the SRX1500 helps organizations realize their business objectives while providing scalable, easy-to-manage, secure connectivity and advanced threat detection and mitigation capabilities. The SRX1500 protects critical corporate assets as a next-generation firewall, acts as an enforcement point for cloud-based security solutions, and provides application visibility and control to improve the user and application experience.

Hardware and software architectures on the SRX1500 provides significant performance improvements to a small 1 U form factor. The key to the SRX1500 hardware is the security flow accelerator, a programmable high-speed Layer 4 firewall chip, and a robust x86-based security compute engine for advanced security services like application visibility, intrusion prevention, and threat mitigation capabilities. The SRX1500 software architecture leverages these programmable hardware components and virtualization to deliver high-speed firewall performance, application visibility, and intrusion prevention while lowering the total cost of ownership (TCO).

The SRX1500 is purpose-built to protect 10GbE network environments, consolidating multiple security services and networking functions in a highly available appliance. It supports up to 9.2 Gbps of firewall performance, 3.3 Gbps of intrusion prevention, and 4.5 Gbps of IPsec VPN in enterprise campus, regional headquarters, and large branch deployments.

SRX1500 Highlights

The SRX1500 delivers a full complement of next-generation firewall capabilities that help secure your network with an integrated solution that combines best-in-class application, content, and threat classification with SD-WAN, local switching, and easy policy management. Advanced application identification and classification to enable greater visibility, enforcement, control, and protection over the network as they are tied to users regardless of location or device. It provides a detailed analysis of application volume and usage, fine-grained application control policies to allow or deny traffic based on dynamic application name or group names, and prioritization of traffic based on application information and context to reduce complexity across traditional, cloud, and hybrid IT networks.

Combining perimeter defenses with segmentation to stop lateral threat propagation, the SRX1500 Firewall offers a comprehensive suite of application security services, threat defenses, and intelligence services to protect networks from the latest content-borne threats. Integrated threat intelligence via Juniper Networks Advanced Threat Prevention (ATP) Cloud offers adaptive threat protection against command and control (C&C) solutions that leverage automated protection. This integration helps detect and enforce against known exploits, spyware, malware, and zero-day threats with an extremely high degree of accuracy using advanced AI techniques developed in conjunction with Juniper Threat Labs.

The SRX1500 enables agile SecOps through automation capabilities that support Zero Touch Deployment, Python scripts for orchestration, and event scripting for operational management.

The SRX1500 delivers fully automated SD-WAN to both enterprises and service providers. A Zero-Touch Provisioning (ZTP) capability simplifies branch network connectivity for initial deployment and ongoing management. Due to its high performance and scale, the SRX1500 acts as a VPN hub and terminates VPN/secure overlay connections in the various SD-WAN topologies.

The SRX1500 Firewall runs Juniper Networks Junos® operating system, a proven, carrier-hardened network OS that powers the top 100 service provider networks worldwide. These rigorously tested carrier-class routing features of IPv4/IPv6, OSPF, BGP, and multicast have been proven in over 15 years of worldwide deployments.

Juniper 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—and expand zero trust to all parts of the network 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 our 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 Secure Edge

Juniper Secure Edge secures workforces anywhere with the fast, reliable, and secure access they need. Delivers full-stack SSE capabilities, including FWaaS, SWG, CASB with DLP, ZTNA, and advanced threat protection to protect access to web, SaaS, and on-premises applications and provide users with security that follows them wherever they go. Juniper meets customers where they are and takes them where they want to go by leveraging what they have and extending their zero-trust initiatives to a cloud-delivered architecture without breaking the bank or their ops team.

Juniper Secure Edge, managed by Security Director Cloud, uses a single policy framework that enables security policies to be created once to follow users, devices, and data wherever they go. Customers don't have to start from scratch when adopting cloud-delivered security. With our three-click wizard, customers can easily leverage existing campus edge policies and translate them into an SSE policy. Because it uses a single policy framework regardless of the deployment model, Secure Edge applies existing security policies from traditional deployments to its cloud-delivered model in just a few clicks, reducing misconfigurations and risk.

Whether securing remote users, campus and branch locations, private cloud, public cloud, or hybrid cloud data centers, Juniper provides unified management and unbroken visibility across all architectures. This makes it easy for ops teams to easily and effectively bridge their current investments with their future architectural goals, including SASE. Customers can manage security anywhere and everywhere, on-premises, in the cloud, and from the cloud, with security policies that follow users, devices, and data wherever they go, all from a single UI.

Users have fast, reliable, and secure access to the data and resources they need, ensuring great user experiences. IT security teams gain seamless visibility across the entire network while leveraging their existing investments, helping them transition to a cloud-delivered architecture at their own pace.

Juniper Secure Edge provides consistent security policies that follow the user, device and data without having to copy over or recreate rule sets. It's easy to deploy cloud-delivered application control, intrusion prevention, content and Web filtering, and effective threat prevention without breaking visibility or security enforcement.

Juniper has been consistently validated by multiple third-party tests as the most effective security technology on the market for the past four years, with 100% security efficacy across all use cases.

Features and Benefits

Business Requirement	Feature/Solution	SRX1500 Advantages
High performance	Up to 9 Gbps of firewall performance	• Best suited for enterprise large branch and campus deployments • Addresses future needs for scale and feature capacity
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 user role • Inspects and detects applications inside the SSL-encrypted traffic
Threat protection	IPS, anti-virus, anti-spam, enhanced web filtering, Juniper Advanced Threat Prevention Cloud, Encrypted Traffic Insights, Threat Intelligence Feeds, and Juniper ATP Appliance	• Provides real-time updates to IPS signatures and protects against exploits • Implements industry-leading antivirus and URL filtering • Delivers an open threat intelligence platform that provides a single point for all operational intelligence feeds • Protects against zero-day attacks • 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 effectively identify threats from packet snippets • Eliminates patient-zero infections • Provides protection that lasts for the full attack lifecycle--not merely 24 hours—sso the network is safe from reinfection from subsequent attacks
Professional-grade networking services	Routing, switching, and secure wire	• Supports carrier-class advanced routing, quality of service (QoS), and services • Offers flexible deployment modes (L1/L2/L3)
Highly secure	IPsec VPN, remote access/SSL VPN, secure boot	• Provides high-performance IPsec VPN with dedicated crypto engine • Simplifies large VPN deployments with auto VPN and group VPN • Offers secure and flexible remote access SSL VPN with Juniper Secure Connect • Verifies binaries that execute on the hardware with secure boot
Embed 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
High reliability	Chassis cluster, redundant power supply	• Provides stateful configuration and state synchronization • Supports active/active and active/backup deployment scenarios • Offers highly available hardware with dual PSU, redundant fans
Easy to manage and scale	On-box GUI, Security Director, and Security Director Cloud	• Enables centralized management for auto-provisioning, firewall policy management, Network Address Translation (NAT), and IPsec VPN deployments • Includes simple easy-to-use on-box GUI for local management
Lower TCO	Junos OS	• Integrates routing, switching, and security in a single device • Reduces OpEx with Junos OS automation capabilities

SRX1500

SRX1500 Firewall Specifications

Software Specifications

Firewall Services

- Stateful firewall inspection
- Zone-based firewall
- Screens and distributed denial of service (DDoS) protection
- Protection from protocol and traffic anomalies
- Integration with Pulse Unified Access Control (UAC)
- Integration with Aruba Clear Pass Policy Manager
- User role-based firewall
- SSL Inspection

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

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, SuiteB
- IKE authentication algorithms: MD5, SHA-1, SHA-128, SHA-256, SHA-384

- Authentication: Pre-shared key and public key infrastructure (PKI) (X.509)
- IPsec (Internet Protocol Security): Authentication Header (AH)/ Encapsulating Security Payload (ESP) protocol
- IPsec Authentication Algorithms: hmac-md5, hmac-sha-196
- IPsec Encryption Algorithms: Prime, DES-CBC, 3DES-CBC, AEC-CBC, AES-GCM, SuiteB
- 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)
- 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

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

Threat Defense and Intelligence Services[1]

- Intrusion prevention
- Antivirus
- Antispam
- Category/reputation-based URL filtering
- 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
- Juniper ATP Appliance, a distributed, on-premises advanced threat prevention solution to detect and block zero-day attacks
- Adaptive Threat Profiling
- Encrypted Traffic Insights
- SecIntel to provide threat intelligence
- 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
- 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), 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
- Hierarchical shaping and policing

Switching Features

- ASIC-based Layer 2 forwarding
- MAC address learning
- VLAN addressing and integrated routing and bridging (IRB) support
- Link aggregation and LACP
- LLDP and LLDP-MED
- STP, RSTP, MSTP
- MVRP
- 802.1X authentication

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)
- Bidirectional Forwarding Detection (BFD)
- Two-Way Active Measurement Protocol (TWAMP)
- IEEE 802.3ah Link Fault Management (LFM)
- IEEE 802.1ag Connectivity Fault Management (CFM)

Advanced Routing Services

- Packet mode
- 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 reroute

Management, Automation, Logging, and Reporting

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

Hardware Specifications

Specification	SRX1500
Connectivity	
Total onboard ports	16x1GbE and 4x10GbE
Onboard RJ-45 ports	12x1GbE
Onboard small form-factor pluggable (SFP) transceiver ports	4x1GbE
Onboard SFP+ ports	4x10GbE
Out-of-Band (OOB) management ports	1x1GbE
Dedicated high availability (HA) ports	1x1GbE (SFP)
PIM slots	2
Console (RJ-45 + miniUSB)	1
USB 2.0 ports (type A)	1
Memory and Storage	
System memory (RAM)	16 GB
Primary boot storage (mSATA)	16 GB
Secondary storage (SSD)	100 GB
Dimensions and Power	
Form factor	1 U
Size (WxHxD)	17.28 x 1.75 x 18.2 in (43.9 x 4.44 x 46.22 cm)
Weight (device and PSU)	16.1 lb (7.30 kg)
Redundant PSU	1+1
Power supply	AC/DC (external)
Average power consumption	150 W
Average heat dissipation	512 BTU / hour
Maximum current consumption	2.5A (for AC PSU); 6.2A (for DC PSU)
Maximum inrush current	50A by 1 AC cycle
Acoustic noise level	66.5dBA
Airflow/cooling	Front to back
Operating temperature	32° to 104° F (0° to 40° C)
Nonoperating temperature	4° to 158° F (-20° to 70° C)
Operating humidity	10% to 90% non-condensing
Nonoperating humidity	5% to 95% non-condensing
Meantime between failures (MTBF)	9.78 years (85,787 hours)
FCC classification	Class A
RoHS compliance	RoHS 2
FIPS 140-2	Level 2 (Junos 19.2)
Performance and Scale	
Routing/firewall (IMIX packet size) Gbps[2]	4.8
Routing/firewall (1,518 B packet size) Gbps[2]	9.2
IPsec VPN (IMIX packet size) Gbps[2]	1.3
IPsec VPN (1400 B packet size) in Gbps[2]	4.5
Application visibility and control in Gbps[3]	7.9
Recommended IPS in Gbps[3]	3.3
Next-generation firewall in Gbps[4]	2.1
Secure Web Access firewall in Gbps[5]	1.6
Route table size (RIB/FIB) (IPv4)	2 million / 1 million
Maximum concurrent sessions (IPv4 or IPv6)	2,000,000
Maximum security policies	16,000
Connections per second	90,000
NAT rules	8,000
Media access control (MAC) table size	64,000 (standalone mode)
IPsec VPN tunnels	2,000
Number of remote access/SSL VPN (concurrent) users	2,000
GRE tunnels	2,048
Maximum security zones	512
Maximum virtual router	512
Maximum VLANs	3,900

[2]Performance numbers based on UDP packets and RFC2544 test methodology.

[3]Performance numbers based on HTTP traffic with 44 KB transaction size.

[4]Next-Generation firewall performance is measured with Firewall, Application Security and IPS enabled using 64KB transactions

[5]Secure Web Access firewall performance is measured with Firewall, Application Security, IPS, SecIntel, and URL Filtering enabled using 64KB transactions

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 for your network. 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.

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™