



SRX300 line of firewalls for the branch

Product overview

The [SRX300 line of firewalls](#) combines effective [security](#), [SD-WAN](#), [routing](#), [switching](#), and [WAN](#) interfaces with [next-generation firewalls](#) and advanced threat mitigation capabilities for cost-effective, secure connectivity across distributed enterprise locations. By consolidating fast, highly available switching, routing, security, and NGFW capabilities in a single device, enterprises can remove network complexity, protect and prioritize their resources, and improve user and application experience while lowering the total cost of ownership (TCO).

Product description

Juniper Networks' SRX300 line of firewalls delivers a next-generation firewall (NGFW) and a secure SD-WAN solution that supports the changing needs of enterprise networks. Whether rolling out new services and applications across locations, connecting to the cloud, or trying to achieve operational efficiency, the SRX300 line helps organizations realize their business objectives while providing scalable, easy to manage, secure connectivity, and advanced threat mitigation capabilities. NGFW and content security capabilities make detecting and proactively mitigating threats easier while improving the user and application experience.

The SRX300 line consists of five models:

- **SRX300:** Securing small branch or retail offices, the SRX300 firewall consolidates security, routing, switching, and WAN connectivity in a small desktop device. The SRX300 supports up to 1.9 Gbps firewall and 336 Mbps IPSec VPN in a single, cost-effective networking and security platform.
- **SRX320:** Securely connecting small distributed enterprise branch offices, the SRX320 firewall consolidates security, routing, switching, and WAN connectivity in a small desktop device. The SRX320 supports up to 1.9 Gbps firewall and 336 Mbps IPSec VPN in a single, consolidated, cost-effective networking and security platform.
- **SRX340:** Securely connecting midsize distributed enterprise branch offices, the SRX340 firewall consolidates security, routing, switching, and WAN connectivity in a 1U form factor. The SRX340 supports up to 4.7 Gbps firewall and 733 Mbps IPSec VPN in a single, cost-effective networking and security platform.

— **SRX345:** Best suited for midsize to large distributed enterprise branch offices, the SRX345 firewall consolidates security, routing, switching, and WAN connectivity in a 1U form factor. The SRX345 supports up to 5 Gbps firewall and 977 Mbps IPSec VPN in a single, consolidated, cost-effective networking and security platform.

— **SRX380:** A high performance and secure SD-WAN gateway, the SRX380 offers superior and reliable WAN connectivity while consolidating security, routing, and switching for distributed enterprise offices. The SRX380 features greater port density than other SRX300 models, with 16x1GbE PoE+ and 4x10GbE ports, and includes redundant dual power supplies — all in a 1U form factor. The SRX380 supports up to 20 Gbps firewall and 4.4 Gbps IPSec VPN in a single, consolidated, cost-effective networking and security platform.

SRX300 highlights

The SRX300 line of firewalls consists of secure SD-WAN routers that bring high performance and proven deployment capabilities to enterprises that need to build a worldwide network of thousands of remote sites. WAN or internet connectivity and Wi-Fi module options include:

- Ethernet, T1/E1, ADSL2/2+, and VDSL
- 3G/4G LTE wireless
- 802.11ac Wave 2 Wi-Fi

Comprehensive Security Suite

The SRX300 line offers a comprehensive suite of application security services, threat defenses, and intelligence services. The services include intrusion prevention system (IPS), application security user role-based firewall controls, and cloud-based antivirus, anti-spam, and enhanced web filtering, protecting networks from the latest content-borne threats. Integrated threat intelligence via [Juniper's Seclntel](#) offers adaptive threat protection against Command and Control (C&C)-related botnets and policy enforcement based on GeolP. Customers can also leverage their custom and third-party feeds to protect their networks from advanced malware and other threats. Integrating the [Juniper Networks Advanced Threat Protection solution](#), the SRX300 line detects and enforces automated protection against known malware and zero-day threats with a very high degree of accuracy.

Security Director Cloud

As HPE's simple and seamless management experience, [Security Director Cloud](#) is 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, applications, and infrastructure.

Security Director Cloud enables organizations to secure their architecture with consistent security policies across any environment — on-premises, cloud-based, cloud-delivered, and hybrid — and expands zero trust to all parts of the network, including the edge, data center, applications, and microservices. With Security Director Cloud, organizations have unbroken visibility, policy configuration, administration, and collective threat intelligence all in one place.

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

Juniper Secure Edge

Secure the remote workforce anywhere with the fast, reliable, and secure access they need. [Juniper Secure Edge](#) delivers full-stack Security Service Edge (SSE) capabilities, including FWaaS, SWG, CASB with DLP, ZTNA, and advanced threat protection. It helps organizations protect access to web, SaaS, and on-premises applications and keep users secure wherever they are located.

Juniper Secure Edge, managed by Security Director Cloud, uses a single policy framework that enables security policies to be created once and applied anywhere, following users, devices, and applications 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 migrates existing security policies from traditional deployments to its cloud-delivered model in clicks, reducing misconfigurations and risk.

Whether securing remote users, campus and branch locations, private cloud, public cloud, or hybrid cloud data centers, HPE 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.

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

Mist AI

WAN Assurance

[Mist WAN Assurance](#) is a cloud service that brings AI-powered automation and service levels to [Juniper SRX Series Firewalls](#), complementing the Juniper Secure SD-WAN solution. Mist WAN Assurance transforms IT operations from reactive troubleshooting to proactive remediation, turning insights into actions and delivering operational simplicity with seamless integration into existing deployments.

- SRX Series firewalls, deployed as secure SD-WAN edge devices, deliver the rich Junos streaming telemetry that provides the insights needed for WAN health metrics and anomaly detection. This data is leveraged within the [Mist Cloud](#) and AI engine, driving simpler operations, reducing mean time to repair (MTTR) and providing greater visibility into end user experiences.
- Insights derived from SRX Series SD-WAN gateway telemetry data allow WAN Assurance to compute unique "User Minutes" that indicate whether users are having a good experience.
- The [Marvis assistant](#) for WAN allows you to ask direct questions like "Why is my Zoom call bad?" and provides complete insights, correlation, and actions.
- Marvis Actions identifies and summarizes issues such as application latency conditions, congested WAN circuits, or negotiation mismatches.

Simplifying Branch Deployments (Secure Connectivity/SD-WAN)

The SRX300 line delivers fully automated SD-WAN to both enterprises and [service providers](#).

- A Zero-Touch Provisioning (ZTP) feature simplifies branch network connectivity for initial deployment and ongoing management.
- SRX300 firewalls offer best-in-class secure connectivity.
- SRX300 firewalls efficiently utilize multiple links and load balance traffic across the enterprise WAN, blending traditional MPLS with other connectivity options such as broadband internet, leased lines, 4G/LTE, and more.
- Policy- and application-based forwarding capabilities enforce business rules created by the enterprise to steer application traffic toward a preferred path.

Table 1. Features and benefits

Business requirement	Feature/solution	SRX300 advantages
High performance	Up to 20 Gbps of routing and firewall performance	<ul style="list-style-type: none">— Best suited for small, medium and large branch office deployments— Addresses future needs for scale and feature capacity
Business continuity	Stateful high availability (HA), IP monitoring	<ul style="list-style-type: none">— Uses stateful HA to synchronize configuration and firewall sessions— Supports multiple WAN interfaces with dial-on-demand backup— Route/link failover based on real-time link performance
SD-WAN	Better end user application and cloud experience and lower operational costs	<ul style="list-style-type: none">— ZTP simplifies remote device provisioning— Advanced Policy-Based Routing (APBR) orchestrates business intent policies across the enterprise WAN— Application quality of experience (AppQoE) measures application SLAs and improves the end user experience— Controls and prioritizes traffic based on application and user role
End user experience	WAN assurance	<ul style="list-style-type: none">— Complements the Juniper Secure SD-WAN solution with AI-powered automation and service levels— Provides visibility and insights into users, applications, WAN links, control, data plane, and CPU for proactive remediation
Highly secure	IPSec VPN, Remote Access/SSL VPN, Media Access Control Security (MACsec)	<ul style="list-style-type: none">— Creates secure, reliable, and fast overlay links over public internet— Employs anti-counterfeit features to protect from unauthorized hardware spares— Includes high performance CPU with built-in hardware to assist IPSec acceleration— Provides TPM-based protection of device secrets such as passwords and certificates— Offers secure and flexible remote access SSL VPN with Juniper Secure Connect

Industry-Certified Junos Operating System

SRX300 firewalls are powered by Juniper's [Junos operating system](#), a proven, carrier-hardened OS that underpins and helps secure the world's largest mission-critical enterprise and top 100 service provider networks.

The rigorously tested, carrier-class, rich routing features, such as [IPv4/IPv6](#), OSPF, BGP, and multicast, have been proven by over 15 years of worldwide deployments.

The SRX300 line also enables agile SecOps through automation capabilities that support Zero Touch Deployment, Python scripts for orchestration, and event scripting for operational management.

Table 1. Features and benefits (continued)

Business requirement	Feature/solution	SRX300 advantages
Threat protection	IPS, antivirus, anti-spam, enhanced web filtering, Juniper Advanced Threat Prevention Cloud, Encrypted Traffic Insights, and Threat Intelligence Feeds	<ul style="list-style-type: none">— Provides real-time updates to IPS signatures and protects against exploits— Protects from zero-day attacks— Implements industry-leading antivirus and URL filtering— Integrates open threat intelligence platform with third-party feeds— Restores visibility that was lost due to encryption without the heavy burden of full TLS/SSL decryption
Application visibility	On-box GUI, Security Director	<ul style="list-style-type: none">— Application updates are provided continually provided by HPE Juniper Networking Threat Labs— Inspects and detects applications inside the SSL-encrypted traffic
Easy to manage and scale	On-box GUI, Security Director	<ul style="list-style-type: none">— Includes centralized management for auto-provisioning, firewall policy management, Network Address Translation (NAT), and IPSec VPN deployments, or simple, easy-to-use on-box GUI for local management
Minimize TCO	Junos OS	<ul style="list-style-type: none">— Integrates routing, switching, and security in a single device— Reduces operation expense with Junos automation capabilities



Figure 1. SRX300 line of firewalls for the branch

SRX300 technical specifications

Software specifications

Routing protocols

- IPv4, IPv6, ISO, Connectionless Network Service (CLNS)
- 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 (PPP), Frame Relay, High-Level Data Link Control (HDLC), serial, Multilink Point-to-Point Protocol (MLPPP), Multilink Frame Relay (MLFR), and 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

Firewall services

- Stateful and stateless firewall
- Zone-based firewall
- Screens and distributed denial of service (DDoS) protection
- Protection from protocol and traffic anomaly
- Integration with Pulse Unified Access Control (UAC)
- Integration with HPE Aruba Networking ClearPass Policy Manager
- User role-based firewall
- SSL Inspection (Forward-proxy)

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, hmac-sha-256
- 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

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)¹
- Bidirectional Forwarding Detection (BFD)
- Two-Way Active Measurement Protocol (TWAMP)
- IEEE 802.3ah Link Fault Management (LFM)
- IEEE 802.1ag Connectivity Fault Management (CFM)

High availability (HA) 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-Band Cluster Upgrade (ICU)
- Dial on-demand backup interfaces
- IP monitoring with route and interface failover

Management, automation, logging, and reporting

- SSH, Telnet, SNMP
- Smart image download
- Juniper CLI and Web UI
- Mist AI
- Simplified management
- WAN Assurance
- Security Director
- Security Director Cloud
- Juniper Secure Edge
- Python
- Junos OS event, commit, and OP script
- Application and bandwidth usage reporting
- Auto installation
- Debug and troubleshooting tools
- Zero-Touch Provisioning with Contrail Service Orchestration

Advanced routing services

- Packet mode
- MPLS (RSVP, LDP)
- Circuit cross-connect (CCC), translational cross-connect (TCC)
- L2/L3 MPLS VPN, pseudowires
- Virtual private LAN service (VPLS), next-generation multicast VPN (NG-MVPN)
- MPLS traffic engineering and MPLS fast reroute

Application security services¹

- Application visibility and control
- Application-based advanced policy-based routing
- Application-based advanced policy-based routing (APBR)
- Application-based link monitoring and switchover with Application quality of experience (AppQoE)

Threat Defense and Intelligence Services¹

- Intrusion prevention
- Antivirus
- Antispam
- Category/reputation-based URL filtering
- Protection from botnets (command and control)
- Adaptive enforcement based on GeolP
- Juniper Advanced Threat Prevention to detect and block zero-day attacks
- Adaptive Threat Profiling
- Encrypted Traffic Insights
- Seclntel to provide threat intelligence

¹ Offered as advanced security services subscription licenses.

Table 2. Hardware specifications

Specification	SRX300	SRX320	SRX340	SRX345	SRX380
Connectivity					
Total onboard ports	8x1GbE	8x1GbE	16x1GbE	16x1GbE	20 (16x1GbE, 4x10GbE)
Onboard RJ-45 ports	6x1GbE	6x1GbE	8x1GbE	8x1GbE	16x1GbE
Onboard small form-factor pluggable (SFP) transceiver ports	2x1GbE	2x1GbE	8x1GbE	8x1GbE	4x10GbE SFP+
MACsec-capable ports	2x1GbE	2x1GbE	16x1GbE	16x1GbE	16x1GbE 4x10GbE
Out-of-band (OOB) management ports	0	0	1x1GbE	1x1GbE	1x1GbE
Mini PIM (WAN) slots	0	2	4	4	4
Console (RJ-45 + miniUSB)	1	1	1	1	1
USB 3.0 ports (type A)	1	1	1	1	1
PoE+ ports	N/A	6 ²	0	0	16
Memory and storage					
System memory (RAM)	4 GB	4 GB	4 GB	4 GB	4 GB
Storage	8 GB	8 GB	8 GB	8 GB	100 GB SSD
SSD slots	0	0	1	1	1
Dimensions and power					
Form factor	Desktop	Desktop	1U	1U	1U
Size (WxHxD)	12.63 x 1.37 x 7.52 in. (32.08 x 3.47 x 19.10 cm)	11.81 x 1.73 x 7.52 in. (29.99 x 4.39 x 19.10 cm)	17.36 x 1.72 x 14.57 in. (44.09 x 4.36 x 37.01 cm)	17.36 x 1.72 x 18.7 in. (44.09 x 4.37 x 47.5 cm) / 17.36 x 1.72 x 18.7 in. (44.09 x 4.37 x 52 cm)	17.36 x 1.72 x 18.7 in. (44.09 x 4.37 x 47.5 cm) / 17.36 x 1.72 x 20.47 in. (44.09 x 4.37 x 52 cm)
Weight (device and PSU)	4.38 lb (1.98 kg)	3.28 lb (1.51 kg) ⁴ / 3.4 lb (1.55 kg) ⁵	10.80 lb (4.90 kg) / 11.02 lb (5 kg) ⁶	10.80 lb (4.90 kg) / 11.02 lb (5 kg) ⁶	15 lb (6.8 kg) with 1xPSU / 16.76 lb (7.6 kg) with 2xPSU
Redundant PSU	No	No	No	No	Yes

² SRX320 with PoE+ ports available as a separate SKU: SRX320-POE.³ SRX345 with dual AC PSU model.⁴ SRX320 non PoE model.⁵ SRX320-POE with 6 ports PoE+ model.⁶ SRX345 with DC power supply (operating temperature as per GR-63 Issue 4 2012 test criteria).

Table 2. Hardware specifications (continued)

Specification	SRX300	SRX320	SRX340	SRX345	SRX380
Power supply	AC (external)	AC (external)	AC (internal)	AC (internal) / DC (internal) ⁶	1+1 hot-swappable AC PSU
Rated DC voltage range	N/A	N/A	N/A	-48 to -60 VDC (with -15% and +20% tolerance)	NA
Rated DC operating voltage range	N/A	N/A	N/A	-40.8 VDC to -72 VDC ⁶	N/A
Maximum PoE power	N/A	180W ⁵	N/A	N/A	480W
Average power consumption	24.9W	46W ⁴ /221W ⁵	122W	122W	150W (without PoE) 510W (with PoE)
Average heat dissipation	85 BTU/h	157 BTU/h ⁴ / 755 BTU/h ⁵	420 BTU/h	420 BTU/h	511.5 BTU/hr (without PoE)
Maximum current consumption	0.346A	0.634A ⁴ / 2.755 A ⁵	1.496A	1.496A / 6A @ -48 VDC ⁶	1.79A/7.32A
Acoustic noise level	0 dB (fanless)	37 dBA ⁴ /40 dBA ⁵	45.5 dBA	45.5 dBA	< 50 dBA @ room temperature 27°C
Airflow/cooling	Fanless	Front to back	Front to back	Front to back	Front to back

Environmental, compliance, and safety certification

Operational temperature	-4°F to 140°F (-20°C to 60°C) ⁷	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C) -22°F to 131°F (-30°C to 55°C) for SRX345-DC	32°F to 104°F (0°C to 40°C) with MPIMs 32°F to 122°F (0°C to 50°C) without MPIMs
Nonoperational temperature	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C) -22°F to 158°F (-30°C to 70°C) for SRX345-DC	-4°F to 158°F (-20°C to 70°C) -22°F to 158°F (-30°C to 70°C) for SRX345-DC
Operating humidity	10% to 90% non-condensing	10% to 90% non-condensing			
Nonoperating humidity	5% to 95% non-condensing	5% to 95% non-condensing			
Meantime between failures (MTBF)	44.5 years	32.5 years ⁴ / 26 years ⁵	27 years	27.4 years	28.1 years
FCC classification	Class A	Class A	Class A	Class A	Class A
RoHS compliance	RoHS 2	RoHS 2	RoHS 2	RoHS 2	RoHS 2
FIPS 140-2	Level 2 (Junos 19.2R1)	Level 2 (Junos 19.2R1)	Level 2 (Junos 19.2R1)	Level 2 (Junos 20.2R1)	Level 2 (Junos 20.2R1)
Common Criteria certification	NDPP, VPNEP, FWEP, IPSEP (based on Junos 19.2R1)	NDPP, VPNEP, FWEP, IPSEP (based on Junos 19.2R1)	NDPP, VPNEP, FWEP, IPSEP (based on Junos 19.2R1)	NDPP, VPNEP, FWEP, IPSEP (based on Junos 20.4R1)	NDPP, VPNEP, FWEP, IPSEP (based on Junos 20.4R1)

⁵ SRX320-POE with 6 ports PoE+ model.⁶ SRX345 with DC power supply (operating temperature as per GR-63 Issue 4 2012 test criteria).⁷ As per GR63 Issue 4 (2012) test criteria.

Table 2. Hardware specifications (continued)

Specification	SRX300	SRX320	SRX340	SRX345	SRX380
Performance and scale					
Routing with packet mode (64 B packet size) in Kpps ⁸	300	300	550	750	1700
Routing with packet mode (IMIX packet size) in Mbps ⁸	800	800	1,600	2,300	5000
Routing with packet mode (1,518 B packet size in Mbps ⁸)	1,500	1,500	3,000	5,500	10,000
Stateful firewall (64 B packet size) in Kpps ⁸	200	200	350	550	1700
Stateful firewall (IMIX packet size) in Mbps ⁸	600	600	1,100	1,500	6,500
Stateful firewall (1,518 B packet size) in Mbps ⁸	1,900	1,900	4,700	5,000	20,000
IPSec VPN (IMIX packet size) in Mbps ⁸	116	116	239	325	1400
IPSec VPN (1,400 B packet size) in Mbps ⁸	336	336	733	977	4,400
Application visibility and control in Mbps ⁹	500	500	1,000	1,700	6,000
Recommended IPS in Mbps ⁹	200	200	400	600	2,000
Next-generation firewall in Mbps ¹¹	226	226	420	430	2,500
Secure Web Access firewall in Mbps ¹²	171	171	280	295	1,800
Route table size (RIB/FIB) (IPv4 or IPv6)	256k/256k	256k/256k	1 million/600k ¹⁰	1 million/600k ¹⁰	1 million/600k ¹⁰
Maximum concurrent sessions (IPv4 or IPv6)	64,000	64,000	256,000	375,000	380,000
Maximum security policies	1,000	1,000	2,000	4,000	4,000
Connections per second	5,000	5,000	10,000	15,000	50,000

⁸ Throughput numbers based on UDP packets and RFC2544 test methodology.⁹ Throughput numbers based on HTTP traffic with 44 KB transaction size.¹⁰ Route scaling numbers are with enhanced route-scale features turned on.¹¹ Next-Generation firewall performance is measured with Firewall, Application Security and IPS enabled using 64KB transactions¹² Secure Web Access firewall performance is measured with Firewall, Application Security, IPS, SecIntel, and URL Filtering enabled using 64KB transactions

Table 2. Hardware specifications (continued)

Specification	SRX300	SRX320	SRX340	SRX345	SRX380
NAT rules	1,000	1,000	2,000	2,000	3,000
MAC table size	15,000	15,000	15,000	15,000	16,000
IPSec VPN tunnels	256	256	1,024	2,048	2,048
Number of remote access/SSL VPN (concurrent) users	25	50	150	250	500
GRE tunnels	256	256	512	1,024	2,048
Maximum number of security zones	16	16	64	64	128
Maximum number of virtual routers	32	32	64	128	128
Maximum number of VLANs	1,000	1,000	2,000	3,000	3,000
AppID sessions	16,000	16,000	64,000	64,000	64,000
IPS sessions	16,000	16,000	64,000	64,000	64,000
URLF sessions	16,000	16,000	64,000	64,000	64,000

WAN and Wi-Fi Interface Support Matrix

1 port T1/E1 MPIM (SRX-MP-1T1E1-R)	No	Yes	Yes	Yes	Yes
1 port VDSL2 Annex A/M MPIM (SRX-MP-1VDSL2-R)	No	Yes	Yes	Yes	Yes
4G / LTE MPIM (SRX-MP-LTE-AA and SRX-MP-LTE-AE)	No	Yes	Yes	Yes	Yes
802.11ac Wave 2 Wi-Fi MPIM	No	Yes	Yes	Yes	Yes

⁸ Throughput numbers based on UDP packets and RFC2544 test methodology.

⁹ Throughput numbers based on HTTP traffic with 44 KB transaction size.

¹⁰ Route scaling numbers are with enhanced route-scale features turned on.

¹¹ Next-Generation firewall performance is measured with Firewall, Application Security and IPS enabled using 64KB transactions

¹² Secure Web Access firewall performance is measured with Firewall, Application Security, IPS, SecIntel, and URL Filtering enabled using 64KB transactions

Table 3. WAN and Wi-Fi interface module performance data

Interface Module	Description	Performance
4G/LTE	Dual SIM 4G/LTE-A CAT 6	Up to 300 Mbps download and 50 Mbps upload
Wi-Fi MPIM	Dual-band 802.11 a/b/g/n/ac Wave 2 (2x2 MIMO)	Up to 866 Mbps at 5GHz / 300 Mbps at 2.4 GHz

Juniper Mist WAN Assurance and AI Operations

Alternatively, the SRX300 line of firewalls 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 SRX300 firewalls. See the [WAN Assurance data sheet](#) for more information.

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>.

Table 4. Ordering information

Feature	SRXnnn-SYS-JB
Hardware	
Management (CLI, JWEB, SNMP, Telnet, SSH)	Included
Ethernet switching (L2 Forwarding, IRB, LACP, etc.)	Included
L2 Transparent, Secure Wire	Included
Routing (RIP, OSPF, BGP, Virtual router)	Included
Multicast (IGMP, PIM, SSDP, DMVRP)	Included
Packet Mode	Included
Overlay (GRE, IP-IP)	Included
Network Services (J-Flow, DHCP, QOS, BFD)	Included
Stateful Firewall, Screens, ALGs	Included
NAT (static, SNAT, DNAT)	Included
IPSec VPN (Site-to-Site VPN, Auto VPN, Group VPN)	Included
Firewall policy enforcement (UAC, HPE Aruba Networking CPPM)	Included
Remote Access/SSL VPN (concurrent users) ¹³	Optional

¹³ Based on concurrent users; two free licenses included

Table 4. Ordering information (continued)

Feature	SRXnnn-SYS-JB
Chassis Cluster, VRRP, ISSU/ICU	Included
Automation (Junos scripting, auto-installation)	Included
MPLS, LDP, RSVP, L3 VPN, pseudo-wires, VPLS	Included

Table 5. Base system model numbers

Product number	Description
SRX300-SYS-JB	SRX300 Firewalls include hardware (8GbE, 4G RAM, 8G Flash, power adapter, and cable) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS, and switching). RMK not included.
SRX320-SYS-JB	SRX320 Firewalls include hardware (8GbE, 2x MPIM slots, 4G RAM, 8G Flash, power adapter and cable) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching). RMK not included.
SRX320-SYS-JB-P	SRX320 Firewalls includes hardware (8GbE, 6-port PoE+, 2x MPIM slots, 4G RAM, 8G Flash, power adapter and cable) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching). RMK not included.
SRX340-SYS-JB	SRX340 Firewalls include hardware (16GbE, 4x MPIM slots, 4G RAM, 8G Flash, power supply, cable and RMK) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching)
SRX345-SYS-JB	SRX345 Firewalls include hardware (16GbE, 4x MPIM slots, 4G RAM, 8G Flash, power supply, cable and RMK) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching)
SRX345-SYS-JB-2AC	SRX345 Firewalls include hardware (16GbE, 4x MPIM slots, 4G RAM, 8 Flash, dual AC power supply, cable and RMK) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching)
SRX345-SYS-JB-DC	SRX345 Firewalls include hardware (16GbE, 4x MPIM slots, 4G RAM, 8G Flash, single DC power supply, cable and RMK) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching)
SRX380-P-SYS-JB-AC	SRX380 Firewalls include hardware (16GbE PoE+, 4x10GbE, 4x MPIM slots, 4GB RAM, 100GB SSD, single AC power supply, cable and RMK) and Junos Software Base (firewall, NAT, IPSec, routing, MPLS and switching)

Table 6. Software licenses

Product number	Description
S-SRXnnn-A1-1	SRXnnn Advanced 1 - JSE/SD-WAN, includes SD-WAN features App+ (AppID, AppFW, AppQoS, AppRoute, AppQoE, AppTrack) and IPS; 1-year subscription (example: S-SRX380-A1-1)
S-SRXnnn-A1-3	SRXnnn Advanced 1 - JSE/SD-WAN, includes SD-WAN features App+ (AppID, AppFW, AppQoS, AppRoute, AppQoE, AppTrack) and IPS; 3-year subscription (example: S-SRX380-A1-3)
S-SRXnnn-A1-5	SRXnnn Advanced 1 - JSE/SD-WAN, includes SD-WAN features App+ (AppID, AppFW, AppQoS, AppRoute, AppQoE, AppTrack) and IPS; 5-year subscription (example: S-SRX380-A1-5)
S-SRXnnn-P1-1	SRXnnn Premium 1, includes App+ (AppID, AppFW, AppQoS, AppRoute, AppQoE, AppTrack), IPS and Juniper ATP; 1-year subscription (example: S-SRX380-P1-1)
S-SRXnnn-P1-3	SRXnnn Premium 1, includes App+ (AppID, AppFW, AppQoS, AppRoute, AppQoE, AppTrack), IPS and Juniper ATP; 3-year subscription (example: S-SRX380-P1-3)
S-SRXnnn-P1-5	SRXnnn Premium 1, includes App+ (AppID, AppFW, AppQoS, AppRoute, AppQoE, AppTrack), IPS and Juniper ATP; 5-year subscription (example: S-SRX380-P1-5)
S-SRXnnn-A2-1	SRXnnn Advanced 2, includes App+ (AppID, AppFW, AppQoS, AppRoute, AppQoE, AppTrack), IPS and Content Security (UTM, Cloud AV, URLF and AS); 1-year subscription (example: S-SRX380-A2-1)

Table 6. Software licenses (continued)

Product number	Description
S-SRXnnn-A2-3	SRXnnn Advanced 2, includes App+ (AppID, AppFW, AppQoS, AppRoute, AppQoE, AppTrack), IPS and Content Security (UTM, Cloud AV, URLF and AS); 3-year subscription (example: S-SRX380-A2-3)
S-SRXnnn-A2-5	SRXnnn Advanced 2, includes App+ (AppID, AppFW, AppQoS, AppRoute, AppQoE, AppTrack), IPS and Content Security (UTM, Cloud AV, URLF and AS); 5-year subscription (example: S-SRX380-A2-5)
S-SRXnnn-P2-1 ¹⁴	SRXnnn Premium 2, includes App+ (AppID, AppFW, AppQoS, AppRoute, AppQoE, AppTrack), IPS, Content Security (UTM, Cloud AV, URLF and AS) and Juniper Sky ATP; 1-year subscription (example: S-SRX380-P2-1)
S-SRXnnn-P2-3 ¹⁴	SRXnnn Premium 2, includes App+ (AppID, AppFW, AppQoS, AppRoute, AppQoE, AppTrack), IPS, Content Security (UTM, Cloud AV, URLF and AS) and Juniper Sky ATP; 3-year subscription (example: S-SRX380-P2-3)
S-SRXnnn-P2-5 ¹⁴	SRXnnn Premium 2, includes App+ (AppID, AppFW, AppQoS, AppRoute, AppQoE, AppTrack), IPS, Content Security (UTM, Cloud AV, URLF and AS) and Juniper Sky ATP; 5-year subscription (example: S-SRX380-P2-5)

¹⁴ The S-SRXnnn-P2-1/3/5 year SKUs are only available for the SRX340, SRX345, and SRX380 models.

Table 7. Remote Access/Juniper Secure Connect VPN license

Product number	Description
S-RA3-SRX300-S-1	SW, Remote Access VPN - Juniper, 25 Concurrent Users, Standard, with SW support, 1 Year
S-RA3-SRX320-S-1	SW, Remote Access VPN - Juniper, 50 Concurrent Users, Standard, with SW support, 1 Year
S-RA3-SRX340-S-1	SW, Remote Access VPN - Juniper, 150 Concurrent Users, Standard, with SW support, 1 Year
S-RA3-SRX345-S-1	SW, Remote Access VPN - Juniper, 250 Concurrent Users, Standard, with SW support, 1 Year
S-RA3-SRX380-S-1	SW, Remote Access VPN - Juniper, 500 Concurrent Users, Standard, with SW support, 1 Year
S-RA3-5CCU-S-1	SW, Remote Access VPN - Juniper, 5 Concurrent Users, Standard, with SW support, 1 Year
S-RA3-25CCU-S-1	SW, Remote Access VPN - Juniper, 25 Concurrent Users, Standard, with SW support, 1 Year
S-RA3-50CCU-S-1	SW, Remote Access VPN - Juniper, 50 Concurrent Users, Standard, with SW support, 1 Year
S-RA3-100CCU-S-1	SW, Remote Access VPN - Juniper, 100 Concurrent Users, Standard, with SW support, 1 Year
S-RA3-250CCU-S-1	SW, Remote Access VPN - Juniper, 250 Concurrent Users, Standard, with SW support, 1 Year
S-RA3-500CCU-S-1	SW, Remote Access VPN - Juniper, 500 Concurrent Users, Standard, with SW support, 1 Year
S-RA3-SRX300-S-3	SW, Remote Access VPN - Juniper, 25 Concurrent Users, Standard, with SW support, 3 Year
S-RA3-SRX320-S-3	SW, Remote Access VPN - Juniper, 50 Concurrent Users, Standard, with SW support, 3 Year
S-RA3-SRX340-S-3	SW, Remote Access VPN - Juniper, 150 Concurrent Users, Standard, with SW support, 3 Year
S-RA3-SRX345-S-3	SW, Remote Access VPN - Juniper, 250 Concurrent Users, Standard, with SW support, 3 Year

Table 7. Remote Access/Juniper Secure Connect VPN license (continued)

Product number	Description
S-RA3-SRX380-S-3	SW, Remote Access VPN - Juniper, 500 Concurrent Users, Standard, with SW support, 3 Year
S-RA3-5CCU-S-3	SW, Remote Access VPN - Juniper, 5 Concurrent Users, Standard, with SW support, 3 Year
S-RA3-25CCU-S-3	SW, Remote Access VPN - Juniper, 25 Concurrent Users, Standard, with SW support, 3 Year
S-RA3-50CCU-S-3	SW, Remote Access VPN - Juniper, 50 Concurrent Users, Standard, with SW support, 3 Year
S-RA3-100CCU-S-3	SW, Remote Access VPN - Juniper, 100 Concurrent Users, Standard, with SW support, 3 Year
S-RA3-250CCU-S-3	SW, Remote Access VPN - Juniper, 250 Concurrent Users, Standard, with SW support, 3 Year
S-RA3-500CCU-S-3	SW, Remote Access VPN - Juniper, 500 Concurrent Users, Standard, with SW support, 3 Year

Table 8. Interface modules

Product number	Description
SRX-MP-1T1E1-R	1 port T1E1, MPIM form factor supported on SRX320, SRX340, SRX345, SRX380, and SRX550M. ROHS complaint
SRX-MP-1VDSL2-R	1 port VDSL2 (backward compatible with ADSL / ADSL2+), MPIM form factor supported on SRX320, SRX340, SRX345, SRX380, and SRX550M. ROHS complaint
SRX-MP-LTE-AA	4G / LTE MPIM support 1, 3, 5, 7-8, 18-19, 21, 28, 38-41 LTE bands (for Asia and Australia). Supported on SRX320, SRX340, SRX345, SRX380, and SRX550M
SRX-MP-LTE-AE	4G / LTE MPIM support 1-5, 7-8, 12-13, 30, 25-26, 29-30, 41 LTE bands (for Americas and EMEA). Supported on SRX320, SRX340, SRX345, SRX380, and SRX550M
SRX-MP-WLAN-US	Wireless access point (Wi-Fi) MPIM for SRX320, SRX34x, SRX380, and SRX550M. Supported for U.S. regulatory bands only.
SRX-MP-WLAN-WW	Wireless access point (Wi-Fi) MPIM for SRX320, SRX34x, SRX380, and SRX550M. Supported for worldwide regulatory bands (excluding U.S. and Israel).
SRX-MP-WLAN-IL	Wireless access point (Wi-Fi) MPIM for SRX320, SRX34x, SRX380, and SRX550M. Supported for Israel regulatory bands only.
SRX-MP-ANT-EXT	Antenna extension cable for WLAN MPIM on SRX Series platforms

Table 9. Accessories

Product number	Description
SRX300-RMK0	SRX300 rack mount kit with adaptor tray
SRX300-RMK1	SRX300 rack mount kit without adaptor tray
SRX300-WALL-KITO	SRX300 wall mount kit with brackets
SRX320-P-RMK0	SRX320-POE rack mount kit with adaptor tray
SRX320-P-RMK1	SRX320-POE rack mount kit without adaptor tray

Table 9. Accessories (continued)

Product number	Description
SRX320-RMK0	SRX320 rack mount kit with adaptor tray
SRX320-RMK1	SRX320 rack mount kit without adaptor tray
SRX320-WALL-KITO	SRX320 wall mount kit with brackets
SRX34X-RMK	SRX340 and SRX345 rack mount kit
EX-4PST-RMK	SRX380 rack mount kit
JSU-SSD-MLC-100	Juniper Storage Unit, SSD, MLC, 100GB
JPSU-600-AC-AFO	SRX380 600W AC PSU, front-to-back

About Hewlett Packard Enterprise

HPE is a leader in essential enterprise technology, bringing together the power of AI, cloud, and networking to help organizations achieve more. As pioneers of possibility, our innovation and expertise advance the way people live and work. We empower our customers across industries to optimize operational performance, transform data into foresight, and maximize their impact. Unlock your boldest ambitions, with HPE. Discover more at HPE.com.

[Visit HPE.com](https://HPE.com)[Chat now](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a00150823ENW, Rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com