# SRX550M FIREWALL DATASHEET

## Product Overview

*The SRX550M Firewall combines security, SD-WAN, routing, switching, and WAN interfaces with next-generation firewalls and advanced threat mitigation capabilities for secure, cost-effective connectivity across distributed enterprise locations. By consolidating fast, highly available switching, routing, security, and next-generation firewall 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.*

## Product Description

Juniper Networks® SRX550M Firewall delivers a next-generation firewall (NGFW) and secure SD-WAN solution that supports the changing needs of cloud-enabled enterprise networks. Whether rolling out new services and applications across locations, connecting to the cloud, or trying to achieve operational efficiency, the SRX550M helps organizations realize their business objectives while providing scalable, easy to manage, secure connectivity and advanced threat mitigation capabilities. NGFWs and advanced security make detecting and proactively mitigating threats easier to improve the user and application experience.

## Architecture and Key Components

The SRX550M Firewall is an NGFW that brings performance and flexible deployment capabilities to enterprises, securely building a worldwide network composed of thousands of remote sites. It provides a fully integrated solution with the best-in-class application, content, and threat classification with SD-WAN, local switching, various connectivity modules, and easy policy management to secure your network. Advanced application identification and classification enables 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 names or group names, and prioritization of traffic based on application information and context to reduce complexity across traditional, cloud and hybrid IT networks.

WAN or Internet connectivity:

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

Industry-best, high-performance IPsec VPN solutions provide comprehensive encryption and authentication capabilities to secure intersite communications. Multiple form factors that offer Ethernet switching support on native Gigabit Ethernet ports allow cost-effective choices for mission-critical deployments.

The SRX550M Firewall runs the Junos® operating system, a proven, carrier-hardened network OS that powers the top 100 service provider networks worldwide. The rigorously tested, carrier-class, rich routing features such as IPv4/IPv6, OSPF, BGP, and multicast have been proven in over 15 years of worldwide deployments. The automation and scripting capabilities of Junos OS and Security Director reduce operational complexity and simplify the provisioning of new sites.

The SRX550M combines perimeter defenses with segmentation to stop lateral threat propagation with 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 ATP Cloud offers adaptive threat protection against command and control (C&C)-related botnets and policy enforcement based on GeoIP. The SRX550M integrates with the Juniper Networks Advanced Threat Prevention (ATP) solutions. This integration leverages automated protection to detect and enforce against known exploits, spyware, malware, and zero-day threats with a high degree of accuracy using advanced AI techniques developed with Juniper Threat Labs.

## 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 SRX550M line delivers fully automated SD-WAN to enterprises and service providers.

- A Zero-Touch Provisioning (ZTP) feature simplifies branch network connectivity for initial deployment and ongoing management.
- SRX550M firewalls offer best-in-class secure connectivity.
- The SRX550M firewall efficiently utilizes 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.

## Comprehensive Security Suite

At the perimeter, the SRX550M 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 anti-virus, anti-spam, and enhanced web filtering, protecting networks from the latest content-borne threats. Integrated threat intelligence via Juniper Networks SecIntel offers adaptive threat protection against Command and Control (C&C)-related botnets and policy enforcement based on GeoIP. Customers can also leverage their custom and third-party feeds for protection from advanced malware and other threats.

Integrating the Juniper Advanced Threat Protection solution, the SRX550M detects and enforces automated protection against known malware and zero-day threats with a high degree of accuracy.

## Industry-Certified Junos Operating System

SRX550M Firewalls run the Junos operating system, a proven, carrier-hardened OS that powers the world's top 100 service provider networks.

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

The SRX550M enables agile SecOps through automation capabilities that support Zero Touch Deployment, Python scripts for orchestration, and event scripting for operational management.

## Features and Benefits

| Business Requirement | Feature/Solution | SRX550M Advantages |
|---|---|---|
| **High performance** | Up to 7 Gbps of routing and firewall performance | • Meets the needs of small, medium, and large branch office deployments<br>• Addresses future needs for scale and feature capacity |
| **Business continuity** | Stateful high availability (HA), IP monitoring | • Uses stateful HA to synchronize configuration and firewall session states<br>• Supports multiple WAN interfaces with dial-on-demand backup<br>• Performs route/link failover based on real-time link performance |
| **SD-WAN** | Better end-user application and cloud experience and lower operational costs | • ZTP simplifies remote device provisioning<br>• Orchestrates business intent policies across the enterprise WAN via centralized or local advanced policy-based routing (APBR)<br>• Measures application service-level agreements (SLAs) and improves end-user experience through application quality of experience (AppQoE)<br>• Continuous application updates provided by Juniper Threat Labs<br>• Inspects and detects applications in SSL-encrypted traffic<br>• Controls and prioritizes traffic based on application and user role |
| **End-user experience** | WAN assurance | • Provides AI-powered automation and service levels that complement the Juniper secure SD-WAN solution<br>• Provides visibility and insights into users, applications, WAN links, controls, and data plane CPU for proactive remediation |
| **High security** | IPsec VPN, Remote Access/SSL VPN, Media Access Control Security (MACsec) | • Creates secure, reliable, and fast overlay link over the public Internet<br>• Employs anti-counterfeit features to defend against unauthorized hardware spares<br>• Includes high-performance CPU with built-in hardware to assist IPsec acceleration<br>• Offers secure and flexible remote access SSL VPN with Juniper Secure Connect |
| **Threat protection** | IPS, anti-virus, anti-spam, enhanced web filtering, Juniper Advanced Threat Prevention Cloud, Encrypted Traffic Insights, and Threat Intelligence Feeds | • Provides real-time updates to IPS signatures and protects against exploits<br>• Implements industry-leading antivirus and URL filtering<br>• Protects against zero-day attacks<br>• Integrates open threat intelligence platform with third-party feeds<br>• Restores visibility lost due to encryption without the heavy burden of full TLS/SSL decryption |
| **Easy management and scale** | On-box GUI, Security Director | • Includes centralized management for autoprovisioning, firewall policy management, Network Address Translation (NAT), and IPsec VPN deployments<br>• Includes simple, easy-to-use on-box GUI for local management |
| **Minimal TCO** | Junos OS | • Integrates routing, switching, and security in a single device<br>• Reduces operational expense with Junos OS automation capabilities |

SRX550M Services Gateway

## SRX550M 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
- Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED)
- Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP)
- Multiple VLAN Registration Protocol (MVRP)
- 802.1X authentication

### Firewall Services

- Stateful firewall inspection
- 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 Aruba Clear Pass 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)
- 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 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
- Junos Space and Security Director
- Python, PyEz, and Ansible modules

- Junos OS event, commit, and OP script
- Application and bandwidth usage reporting
- Auto installation
- Debug and troubleshooting tools
- ZTP 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 Services[1] and Enhanced SD-WAN Services

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

### Enhanced SD-WAN Services

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

### Threat Defense and Intelligence Services[1]

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

[1] Offered as an advanced security services subscription licenses.

## Hardware Specifications

### Network Connectivity

- Fixed I/O: 6 x 10/100/1000 BASE-T + 4 small form-factor pluggable transceivers (SFP transceivers)
- I/O slots: 2 x SRX Series Mini-PIM, 6 x Gigabit-Backplane Physical Interface Module (GPIM) or multiple GPIM and XPIM combinations
- Services and Routing Engine slots: No
- WAN/LAN interface options: See ordering information
- Maximum number of PoE ports (PoE optional on some SRX Series models): Up to 40 ports of 802.3af/at with a maximum of 247 W
- USB: 2

### Flash and Memory

- Memory (DRAM): 4 GB
- Memory slots: 2 DIMM
- Flash memory: 8 GB, CF internal
- USB port for external storage: Yes

### Dimensions and Power

- Dimensions (W x H x D): 17.5 x 3.5 x 18.2 in (44.4 x 8.8 x 46.2 cm)
- Weight (device and power supply): 21.96 lb (9.96 kg) (no interface modules, 1 power supply)
- Rack-mountable: Yes, 2 U
- Power supply (AC): 100-240 VAC, single 645 W or dual 645 W
- Maximum PoE power: 247 W redundant, or 494 W non-redundant
- Average power consumption: 85 W
- Input frequency: 50-60 Hz
- Maximum current consumption: 7.5 A @ 100 VAC with single PSU with PoE, 10.5 A @ 100 VAC with dual PSU with PoE
- Maximum inrush current: 45 A for half-cycle
- Average heat dissipation: 238 BTU/hr
- Maximum heat dissipation: 1449 BTU/hr
- Redundant power supply (hot swappable): Yes (up to a maximum capacity of a single PSU)
- Acoustic noise level (per ISO 7779 Standard): 51.8 dB

### Environmental, Compliance, and Safety Certification

- Operational temperature: 32° to 104° F (0° to 40° C)
- Nonoperational temperature: 4° to 158° F, (-20° to 70° C)
- Humidity (operating): 10% to 90% non-condensing

- Humidity (nonoperating): 5% to 95% non-condensing
- Mean time between failures (Telcordia model): 9.6 years with redundant power
- FCC classification: Class A
- RoHS compliance: Yes

## Performance and Scale

- Firewall performance (1518 Byte)2: 7 Gbps
- Firewall performance (IMIX)2: 2 Gbps
- Firewall + routing pps (64 Byte)2: 700 Kpps
- Firewall performance (HTTP)3: 2 Gbps
- IPsec VPN throughput (large packets): 1.0 Gbps
- IPsec VPN tunnels: 2000
- Application firewall4: 2.0 Gbps
- Intrusion prevention system (IPS)3: 800 Mbps
- Connections per second: 27,000
- Maximum concurrent sessions: 375,000
- Maximum security policies: 8000
- Maximum users supported: Unrestricted
- Route table size (RIB/FIB) (IPv4 or IPv6): 1.5 million/750,000
- NAT rules: 6144
- MAC table size: 15,000
- Number of remote access/SSL VPN (concurrent) users: 500
- GRE tunnels: 1500
- Maximum number of security zones: 96
- Maximum number of virtual routers: 128
- Maximum number of VLANs: 3967
- AppID sessions: 65,000
- IPS sessions: 64,000
- URL filtering (URLF) sessions: 64,000

[2]Throughput numbers based on UDP packets and RFC2544 test methodology [3]Throughput numbers based on HTTP traffic with 44 KB transaction size

## Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For 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.

| Product Number | Description |
|---|---|
| **SRX550M Base System** | |
| SRX550-645AP-M | SRX550M Firewall with 4 GB DRAM and 8 GB CF, 2 U height, 6 GPIM slots, 2 Mini-PIM slots, 6 10/100/1000BASE-T ports, 4GbE SFP ports, dual PS slots, and fans; ships with one 645 W AC power supply with 247 W PoE power (power cord and rack-mount kit included) |
| SRX550-645DP-M | SRX550M Firewall with 4 GB DRAM and 8 GB CF, 2 U height, 6 GPIM slots, 2 Mini-PIM slots, 6 10/100/1000BASE-T ports, 4GbE SFP ports, dual PS slots, and fans; ships with one 645 W DC power supply with 247 W PoE power (no power cord or rack-mount kit included) |
| **SRX550M Power Supplies and Accessories** | |
| SRX600-PWR-645AC-POE | Spare 645 W AC PoE power supply unit for SRX550M systems; one is included in SRX550M base system (SRX550M-645AC) |
| SRX600-PWR-645DC-POE | 645 W DC source power supply for SRX550M provides 397 W system power @ 12 V and 248 W PoE power @ 50 VDC; works with 43-56 VDC input; no power cord |
| SRX550-CHAS-M | SRX550M Firewall, 2 U height, 6 GPIM slots, 2 Mini-PIM slots, 6 10/100/1000BASE-T ports, 4 GbE SFP ports, dual PS slots, and fans (power supply not included) |
| **SRX550M Software Licenses** | |
| SRX550-IDP | One-year subscription for intrusion detection and prevention (IDP) updates on SRX550M |
| SRX550-S2-AS | One-year subscription for Juniper-Sophos antispam updates on SRX550M |
| SRX550-W-EWF | One-year subscription for Juniper Web filtering updates on SRX550M |
| SRX550-S-SMB4-CS | One-year security subscription for enterprise; includes Sophos antivirus, enhanced Web filtering, Sophos antispam, AppSecure, and IDP on SRX550M |
| SRX550-ATP-1 | One-year subscription for Advanced Threat Prevention Cloud for SRX550M |
| SRX550-S-AV-3 | Three-year subscription for Juniper-Sophos antivirus updates on SRX550M |
| SRX550-IDP-3 | Three-year subscription for IDP updates on SRX550M |
| SRX550-S2-AS-3 | Three-year subscription for Juniper-Sophos antispam updates on SRX550M |
| SRX550-W-EWF-3 | Three-year subscription for Juniper Web filtering updates on SRX550M |
| SRX550-S-SMB4-CS-3 | Three-year subscription for enterprise-includes Sophos antivirus, enhanced Web filtering, Sophos antispam, AppSecure, and IDP on SRX550M |
| SRX550-ATP-3 | Three-year subscription for Advanced Threat Prevention Cloud for SRX550M |
| SRX550-IDP-5 | Five-year license for IDP updates on SRX550M |
| SRX550-W-EWF-5 | Five-year subscription for Juniper Web filtering updates on SRX550M |
| SRX550-S-SMB4-CS-5 | Five year security subscription for enterprise; includes Sophos antivirus, enhanced Web filtering, Sophos antispam, AppSecure, and IDP on SRX550M |
| SRX550-APPSEC-A-1 | One-year subscription for Application Security and IPS updates for SRX550M |
| SRX550-APPSEC-A-3 | Three-year subscription for Application Security and IPS updates for SRX550M |
| SRX550-APPSEC-A-5 | Five-year subscription for Application Security and IPS updates for SRX550M |
| SRX550-ATP-5 | Five-year subscription for Advanced Threat Prevention Cloud for SRX550 |

| Product Number | Description |
|---|---|
| **Remote Access/Juniper Secure Connect VPN Licenses** | |
| 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, 5 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 |
| **Interface Modules** | |
| SRX-GP-16GE-POE | 16-port 10/100/1000BASE-T PoE XPIM |
| SRX-GP-8SFP | 8-port GbE copper, fiber SFP XPIM |
| SRX-GP-DUAL-T1-E1 | Dual T1/E1 GPIM |
| SRX-GP-QUAD-T1-E1 | Quad T1/E1 GPIM |
| SRX-GP-1DS3-E3 | 1-port clear channel DS3/E3 GPIM single GPIM slot |
| SRX-MP-1T1E1-R | 1 port T1E1, MPIM form factor supported on SRX320, SRX340, SRX345, SRX380, and SRX550M Firewalls; ROHS compliant |
| SRX-MP-1VDSL2-R | 1 port VDSL2 (backward compatible with ADSL/ADSL2+), MPIM form factor supported on SRX320, SRX340, SRX345, SRX380, and SRX550M Firewalls; ROHS compliant |
| SRX-MP-1SERIAL-R | 1 port Synchronous Serial, MPIM form factor supported on SRX320, SRX340, SRX345, SRX380, and SRX550M Firewalls; ROHS compliant |
| SRX-MP-LTE-AA | 4G/LTE MPIM support for 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 Firewalls |
| SRX-MP-LTE-AE | 4G/LTE MPIM support for 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 Firewalls |

| Product Number | Description |
|---|---|
| SRX-MP-WLAN-US | Wireless access point (Wi-Fi) MPIM for SRX320, SRX340, SRX345, SRX380, and SRX550M Firewalls; supported for U.S. regulatory bands only |
| SRX-MP-WLAN-WW | Wireless access point (Wi-Fi) MPIM for SRX320, SRX340, SRX345, SRX380, and SRX550M Firewalls; supported for worldwide regulatory bands (excluding U.S. and Israel) |
| SRX-MP-WLAN-IL | Wireless access point (Wi-Fi) MPIM for SRX320, SRX340, SRX345, SRX380, and SRX550M Firewalls; supported for Israel regulatory bands only |
| SRX-MP-ANT-EXT | Antenna extension cable for WLAN MPIM on SRX Series platforms |

## 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™