TRIAL EX. 345

Data Sheet

SRX Series Services Gateways for the Branch

SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650

Product Overview

SRX Series Services Gateways for the branch are next-generation security gateways that provide essential capabilities that connect, secure, and manage workforce locations sized from handfuls to hundreds of users. By consolidating fast, highly available switching, routing, security, and next generation firewall capabilities in a single device, enterprises can protect their resources as well as economically deliver new services, safe connectivity, and a satisfying end-user experience. All SRX Series Services Gateways, including products scaled for Enterprise branch, Enterprise edge, and Data Center applications, are powered by Junos OS—the proven operating system that provides unmatched consistency, better performance with services, and superior infrastructure protection at a lower total cost of ownership.

Product Description

The Juniper Networks® SRX Series Services Gateways for the branch combine next generation firewall and unified threat management (UTM) services with routing and switching in a single, high-performance, cost-effective network device.

- SRX Series for the branch runs Juniper Networks Junos® operating system, the proven OS that is used by core Internet routers in all of the top 100 service providers around the world. The rigorously tested carrier-class routing features of IPv4/IPv6, OSPF, BGP, and multicast have been proven in over 15 years of worldwide deployments.
- SRX Series for the branch provides perimeter security, content security, application visibility, tracking and policy enforcement, user role-based control, threat intelligence through integration with Juniper Networks Spotlight Secure*, and network-wide threat visibility and control. Using zones and policies, network administrators can configure and deploy branch SRX Series gateways quickly and securely. Policy-based VPNs support more complex security architectures that require dynamic addressing and split tunneling. The SRX Series also includes wizards for firewall, IPsec VPN, Network Address Translation (NAT), and initial setup to simplify configurations out of the box.
- For content security, SRX Series for the branch offers a complete suite of next generation firewall, unified threat management (UTM) and threat intelligence services consisting of: intrusion prevention system (IPS), application security (AppSecure), user role-based firewall controls, on-box and cloud-based antivirus, antispam, and enhanced Web filtering to protect your network from the latest content-borne threats. Integrated threat intelligence via Spotlight Secure offers adaptive threat protection against command and control (C&C) related botnets and policy enforcement based on GeoIP and attacker fingerprinting technology (the latter for Web application protection)—all of which are based on Juniper provided feeds. Customers may also leverage their own custom and third-party feeds for protection from advanced malware and other threats. The branch SRX Series integrates with other Juniper security products to deliver enterprise-wide unified access control (UAC) and adaptive threat management.
- SRX Series for the branch are secure routers that bring high performance and proven deployment capabilities to enterprises that need to build a worldwide network of thousands of sites. The wide variety of options allow configuration of performance, functionality, and price scaled to support from a handful to thousands of users. Ethernet, serial, T1/E1, DS3/E3, xDSL, Wi-Fi, and 3G/4G LTE wireless are all available options for WAN or Internet connectivity to securely link your sites. Multiple form factors allow you to make cost-effective choices for mission-critical deployments. Managing the network is easy using the proven Junos OS command-line interface (CLI), scripting capabilities, a simple-to-use Web-based GUI, or Juniper Networks Junos® Space Security Director for centralized management.

*Available on SRX550 and higher devices

Architecture and Key Components

Key Hardware Features of the Branch SRX Series Products

Product	Description
SRX100 Services Gateway	· Eight 10/100 Ethernet LAN ports and 1 USB port (support for 3G USB) · Full UTM[1]: antivirus[1], antispam[1], enhanced Web filtering[1], and content filtering · Intrusion prevention system[1], AppSecure[1] · 2 GB DRAM, 2 GB flash default
SRX110 Services Gateway	· VDSL/ADSL2+ and Ethernet WAN interfaces · Eight 10/100 Ethernet LAN ports and two USB port (support for 3G USB) · Full UTM[1]: antivirus[1], antispam[1], enhanced Web filtering[1], intrusion prevention system[1], AppSecure[1] · Unified Access Control (UAC) and content filtering · 2 GB DRAM, 2 GB CF default
SRX210 Services Gateway	· Two 10/100/1000 Ethernet and 6 10/100 Ethernet LAN ports, 1 Mini-PIM slot, and 2 USB ports (support for 3G USB) · Factory option of 4 dynamic Power over Ethernet (PoE) ports 802.3af · Support for T1/E1, serial, ADSL2/2+, VDSL, G.SHDSL, and Ethernet small form-factor pluggable transceiver (SFP) · Content Security Accelerator hardware for faster performance of IPS and ExpressAV (with high memory version) · Full UTM[1]: antivirus1, antispam[1], enhanced Web filtering[1], and content filtering · Intrusion prevention system[1], User role-based firewall, and AppSecure[1] · 2 GB DRAM, 2 GB flash default
SRX220 Services Gateway	· Eight 10/100/1000 Ethernet LAN ports, 2 Mini-PIM slots · Factory option of 8 PoE ports; PoE+ 802.3at, backwards compatible with 802.3af · Support for T1/E1, serial, ADSL2/2+, VDSL, G.SHDSL, and Ethernet SFP · Content Security Accelerator hardware for faster performance of IPS and ExpressAV · Full UTM[1]: antivirus[1], antispam[1], enhanced Web filtering[1], and content filtering · Intrusion prevention system[1], User role-based firewall and AppSecure[1] · 2 GB DRAM, 2 GB CF default
SRX240 Services Gateway	· 16 10/100/1000 Ethernet LAN ports, 4 Mini-PIM slots · Factory option of 16 PoE ports; PoE+ 802.3at, backwards compatible with 802.3af · Support for T1/E1, serial, ADSL2/2+, VDSL, G.SHDSL, and Ethernet SFP · Content Security Accelerator hardware for faster performance of IPS and ExpressAV · Full UTM[1]: antivirus1, antispam[1], enhanced Web filtering[1], and content filtering · Intrusion prevention system[1], AppSecure[1]
SRX550 Services Gateway	· Ten fixed Ethernet ports (6 10/100/1000 copper, 4 SFP), 2 Mini-PIM slots, 6 GPIM slots or multiple GPIM and XPIM combinations · Support for T1/E1, serial, ADSL2/2+, VDSL, G.SHDSL, DS3/E3, Gigabit Ethernet ports; supports up to 52 Ethernet ports including SFP; 40 switch ports with optional PoE including 802.3at, PoE+, backwards compatible with 802.3af (or 50 non-PoE 10/100/1000 copper ports) · Content Security Accelerator hardware for faster performance of IPS and ExpressAV · Full UTM[1]: antivirus1, antispam[1], enhanced Web filtering[1], and content filtering · Intrusion prevention system[1], User role-based firewall, and AppSecure[1] · Threat intelligence for protection from command and control (C&C) botnets, Web application threats, and advanced malware, and policy enforcement based on GeoIP data · 2 GB DRAM default, 2 GB compact flash default (SRX550) · 4 GB DRAM default, 8 GB compact flash default (SRX550 High Memory) · Optional redundant AC power; standard AC power supply that is PoE-ready; PoE power up to 250 watts single power supply or 500 watts dual power supply
SRX650 Services Gateway	· Four fixed ports 10/100/1000 Ethernet LAN ports, 8 GPIM slots or multiple GPIM and XPIM combinations · Support for T1, E1, DS3/E3, Ethernet ports; supports up to 52 Ethernet ports including SFP; 48 switch ports with optional PoE including 802.3at, PoE+, backwards compatible with 802.3af (or 52 non-PoE 10/100/1000 copper ports) · Content Security Accelerator hardware for faster performance of IPS and ExpressAV · Full UTM[1]: antivirus[1], antispam[1], enhanced Web filtering[1], and content filtering · Intrusion prevention system[1], User role-based firewall, and AppSecure[1] · Threat intelligence for protection from command and control (C&C) botnets, Web application threats, and advanced malware, and policy enforcement based on GeoIP data · Modular Services and Routing Engine, future internal failover and hot-swap · 2 GB DRAM default, 2 GB compact flash default, external compact flash slot for additional storage · Optional redundant AC power; standard AC power supply that is PoE-ready; PoE power up to 250 watts single power supply or 500 watts dual power supply

Network Deployments

The SRX Series Services Gateways for the branch are deployed at remote, branch and Enterprise edge locations in the network to provide all-in-one secure WAN connectivity, and connection to local PCs and servers via integrated Ethernet switching.

[1] Unified Threat Management—antivirus, antispam, Web filtering, AppSecure, and IPS require a subscription license option to use the feature. UTM is not supported on the low memory version. Please see the ordering section for options. Content Filtering and UAC are part of the base software with no additional license.

Features and Benefits

Next Generation Firewall

SRX Series Services Gateways deliver next generation firewall protection with application awareness and extensive user role-based control options plus best-of-breed UTM to protect and control your business assets. Next generation firewalls are able to perform full packet inspection and can apply security policies based on layer 7 informat on. This means you can create security policies based on the application running across your network, the user who is receiving or sending network traffic or the content that is traveling across your network to protect your environment against threats, manage how your network bandwidth is allocated, and control who has access to what.

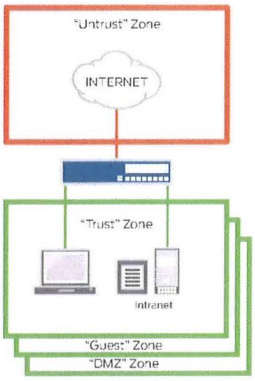

Figure 1: Firewalls, zones, and policies

AppSecure

AppSecure is a suite of application security capabilities for Juniper Networks SRX Series services Gateways that identifies applications for greater visibility, enforcement, control, and protection of the network.

Intrusion Prevention

The intrusion prevention system (IPS) understands application behaviors and weaknesses to prevent application-borne security threats that are difficult to detect and stop.

Unified Threat Management (UTM)

SRX Series can include comprehensive content security against malware, viruses, phishing attacks, intrusions, spam and other threats with unified threat management (UTM). Get a best-of-breed solution with anti-virus, anti-spam, web filtering and content filtering at a great value by easily adding these services to your SRX Series Services Gateway. Cloud-based and on-box solutions are both available.

User Firewall

Juniper offers a range of user role-based firewall control solut ons that support dynamic security policies. User role-based firewal capabilities are integrated with the SRX Series Services Gateways for standard next generation firewall controls. More extensive, scalable, granular access controls for creating dynamic policies are available through the integration of SRX with a Juniper Unif ed Access Control solution.

Adaptive Threat Intelligence

To address the evolving threat landscape that has made it imperative to integrate external threat intelligence into the firewall for thwarting advanced malware and other threats, some SRX Series Services Gateways include threat intelligence via integration with Spotlight Secure. The Spotlight Secure threat intelligence platform aggregates threat feeds from multiple sources to deliver open, consolidated, actionable intelligence to SRX Series Services Gateways across the organization for policy enforcement. These sources include Juniper threat feeds, third party threat feeds and threat detection technologies that the customer can deploy.

Administrators are able to define enforcement policies from all feeds via a single, centralized management point, Junos Space Security Director.

Secure Routing

Many organizations use both a router and a firewall/VPN at their network edge to fulfill their networking and security needs. For many organizations, the SRX Series for the branch can fulfill both roles with one solution. Juniper built best-in-class routing, switching and firewall capabilities into one product.

SRX Series for the branch checks the traffic to see if it is legitimate and permissible, and only forwards it on when it is. This reduces the load on the network, allocates bandwidth for all other mission-critical applications, and secures the network from malicious users.

The main purpose of a secure router is to provide firewall protection and apply policies. The firewall (zone) functionality inspects traffic flows and state to ensure that originating and returning information in a session is expected and permitted for a particular zone. The security policy determines if the session can originate in one zone and traverse to another zone. Due to the architecture, SRX Series receives packets from a wide variety of clients and servers and keeps track of every session, of every application, and of every user. This allows the enterprise to make sure that only legitimate traffic is on its network and that traffic is flowing in the expected direction.

High Availability

Junos Services Redundancy Protocol (JSRP) is a core feature of the SRX Series for the branch. JSRP enables a pair of SRX Series systems to be easily integrated into a high availability network architecture, with redundant physical connections between the systems and the adjacent network switches. With link redundancy, Juniper Networks can address many common causes of system failures, such as a physical port going bad or a cable getting disconnected, to ensure that a connection is available without having to fail over the entire system. This is consistent with a typical active/standby nature of routing resiliency protocols.

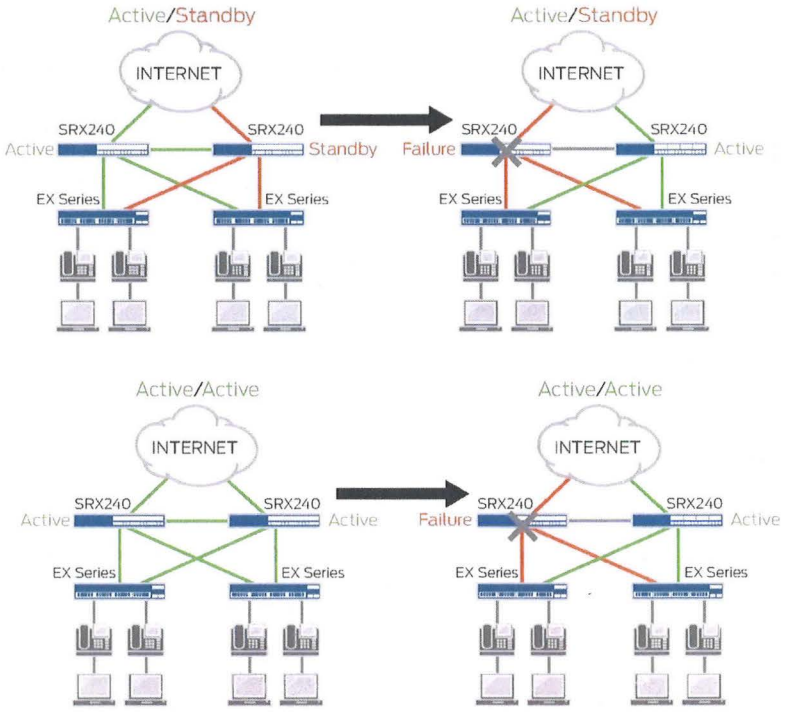

Figure 2: High availability

When SRX Series Services Gateways for the branch are configured as an active/active HA pair, traffic and configuration is mirrored automatically to provide active firewall and VPN session maintenance in case of a failure. The branch SRX Series synchronizes both configuration and runtime information. As a result, during failover, synchronization of the following information is shared: connection/session state and flow information, IPSec security associations, Network Address Translation (NAT) traffic, address book information, configuration changes, and more. In contrast to the typical router active/standby resiliency protocols such as Virtual Router Redundancy Protocol (VRRP), all dynamic flow and session information is lost and must be reestablished in the event of a failover. Some or all network sessions will have to restart depending on the convergence time of the links or nodes. By maintaining state, not only is the session preserved, but security is kept intact. In an unstable network, this active/active configuration also mitigates link flapping affecting session performance.

Session Based Forwarding Without the Performance Hit

In order to optimize the throughput and latency of the combined router and firewall, Junos OS implements session-based forwarding, an innovation that combines the session state information of a traditional firewall and the next-hop forwarding of a classic router into a single operation. With Junos OS, a session that is permitted by the forwarding policy is added to the forwarding table along with a pointer to the next-hop route. Established sessions have a single table lookup to verify that the session has been permitted and to find the next hop. This efficient algorithm improves throughput and lowers latency for session traffic when compared with a classic router that performs multiple table lookups to verify session information and then to find a next-hop route.

Figure 3 shows the session-based forwarding algorithm. When a new session is established, the session-based architecture within Junos OS verifies that the session is allowed by the forwarding policies. If the session is allowed, Junos OS will look up the next-hop route in the routing table. It then inserts the session and the next-hop route into the session and forwarding table and forwards the packet. Subsequent packets for the established session require a single table lookup in the session and forwarding table, and are forwarded to the egress interface.

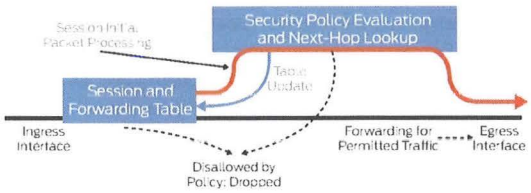

Figure 3: Session-based forwarding algorithm

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.