Juniper SRX Services Gateway

Performance Testing

June 2017

DR170517D

Miercom.com

www.miercom.com

Contents

Executive Summary

As the opportunity for businesses through the Internet grows, the likelihood for malicious activity equally increases. Businesses, whether on the small or corporate scale, cannot risk downtime caused by external attacks. The most common network protection device is a next generation firewall, but its location in the network can limit its effectiveness. Protection needs to start at the edge of the trusted network, not within it. A secure gateway is the outermost device that could screen incoming traffic before passing through to the network.

Juniper Networks addresses all these needs, and more, with its family of SRX Services Gateways which integrate a unified threat management, a router and a switch into one consolidated device that is an on-premise and cloud-based solution. Policies, encryption, authentication, inspection and application-based proxies ensure all traffic between the internal client and external servers are monitored and filtered efficiently.

Miercom was engaged by Juniper Networks to validate the throughput of their SRX devices and observe the effect of security features on network performance. A total of six SRX products were provided, ranging from small branch office to distributed campus level devices: SRX300, SRX320, SRX340, SRX345, SRX550M and SRX1500. Despite network size, Juniper Networks aimed to strike a balance between security and performance with its design of the Services Gateways. Performance was tested under increasing loads of realistic network traffic, as security features were enabled, to determine how traffic processing would impede the data forwarding rate. The expected result was a minimal impact on data throughput for both stateless and stateful traffic.

Key Findings

- **Competitive performance:** Proven superior performance for firewall and security-enabled operation in real-world customer environment for both IPv4 and IPv6.
- **High-end branch gateway performance:** SRX 300/320/340 Services Gateways outperformed datasheet specifications for firewall throughput of stateless UDP IMIX traffic and IPS enabled throughput of stateful HTTP 44 KB traffic requests.

- **Comprehensive security:** Services gateways include intrusion prevention, antivirus, network address translation, quality of service, application firewall and IPsec capabilities.
- **IPv4/IPv6 support:** Dual-stacking and translation for coexisting standards for business continuity and flexibility for its customers and partners.

Based on the results of our testing, we proudly award the Miercom Performance Verified Certification to the Juniper Networks SRX Services Gateways for superior throughput performance.

Robert Smithers

CEO

Miercom

Products Tested

Juniper Networks SRX Services Gateways delivers a next-generation networking and security solution that supports the changing needs of cloud-enabled enterprise networks. Whether rolling out new services, connecting to the cloud, migrating to the SDWAN or trying to achieve operational efficiency, the SRX services gateways helps organizations realize their business objectives while providing scalable, easy to manage, secure connectivity and advanced threat mitigation capabilities.

The SRX300 Series, SRX550 and SRX1500 services gateways combines security, routing, switching, and WAN interfaces with next-generation firewall and advanced threat mitigation capabilities for cost-effective, secure connectivity across distributed enterprise locations. By consolidating fast, highly available switching, routing, security, and next-generation firewall capabilities in a single device, enterprises can remove network complexity, protect and prioritize their resources, and improve user and application experience while lowering total cost of ownership (TCO).

Based on Junos operating system, SRX products offer comprehensive suite of application security services, threat defenses, and intelligence services. They recognize more than 3,500 Layer 3-7 applications, including Web 2.0 and evasive peer-to-peer (P2P) applications like Skype, torrents, and others. Extension to the application security services, these models integrate advanced security capabilities like intrusion prevention system (IPS), application security user role-based firewall controls, cloud-based antivirus, Web filtering and Sky Advanced Threat Protection (detect and enforces automated protection against known malware and zero-day threats).

SRX300 Series

The SRX300 line of services gateways consists of secure routers that bring high performance and proven deployment capabilities to enterprises that need to build a network of thousands of remote sites. Ethernet, serial, T1/E1, ADSL2/2+, VDSL2, and 3G/4G LTE wireless are all available options for WAN or Internet connectivity to link sites. Multiple form factors with Ethernet switching support on native Gigabit Ethernet ports allow cost-effective choices for mission-critical deployments.

SRX550

This highly flexible platform, all-in-one solution, consolidates security, routing, switching, and WAN connectivity into a single 2U device. As with the SRX300 series, it runs the Junos OS and provides security features for the network's perimeter, content and applications using policies, role-based control and threat intelligence. It is ideal for the large branch office deployments where higher port density and hardware redundancy are the key requirements.

SRX1500

The SRX1500 services gateway offer 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.

SRX300

SRX320

SRX340

SRX345

SRX550

SRX1500

	SRX300	SRX320	SRX340	SRX345	SRX550	SRX1500
On-board ports (1GE)	8x1GE	8x1GE	16x1GE	16x1GE	10x1GE	16x1GE
On-board ports (10GE)	NA	NA	NA	NA	NA	4x10GE
On-board MACsec ports	2x1GE	2x1GE	16x1GE	16x1GE	NA	NA
MPIM Slots	NA	2xMPIMs	4xMPIMs	4xMPIMs	2xMPIMs	NA
GPIM Slots	NA	NA	NA	NA	6xGPIMs	NA
Optional POE+ ports	NA	6 (180W)	NA	NA	16 (480W)	NA
Form Factor	Desktop	Desktop	1U	1U	2U	1U
Redundant PSU	No	No	No	Optional	Yes	Yes
Optional SSD Storage	No	No	Yes	Yes	Yes	Built-in
Avg power consumption	15.4W	27W / 212W	122W	122W	85W / 465W	150W
Acoustics	0dB (fanless)	40dBA	45.5dBA	45.5dBA	51.8dBA	66.5dBA

How We Did It

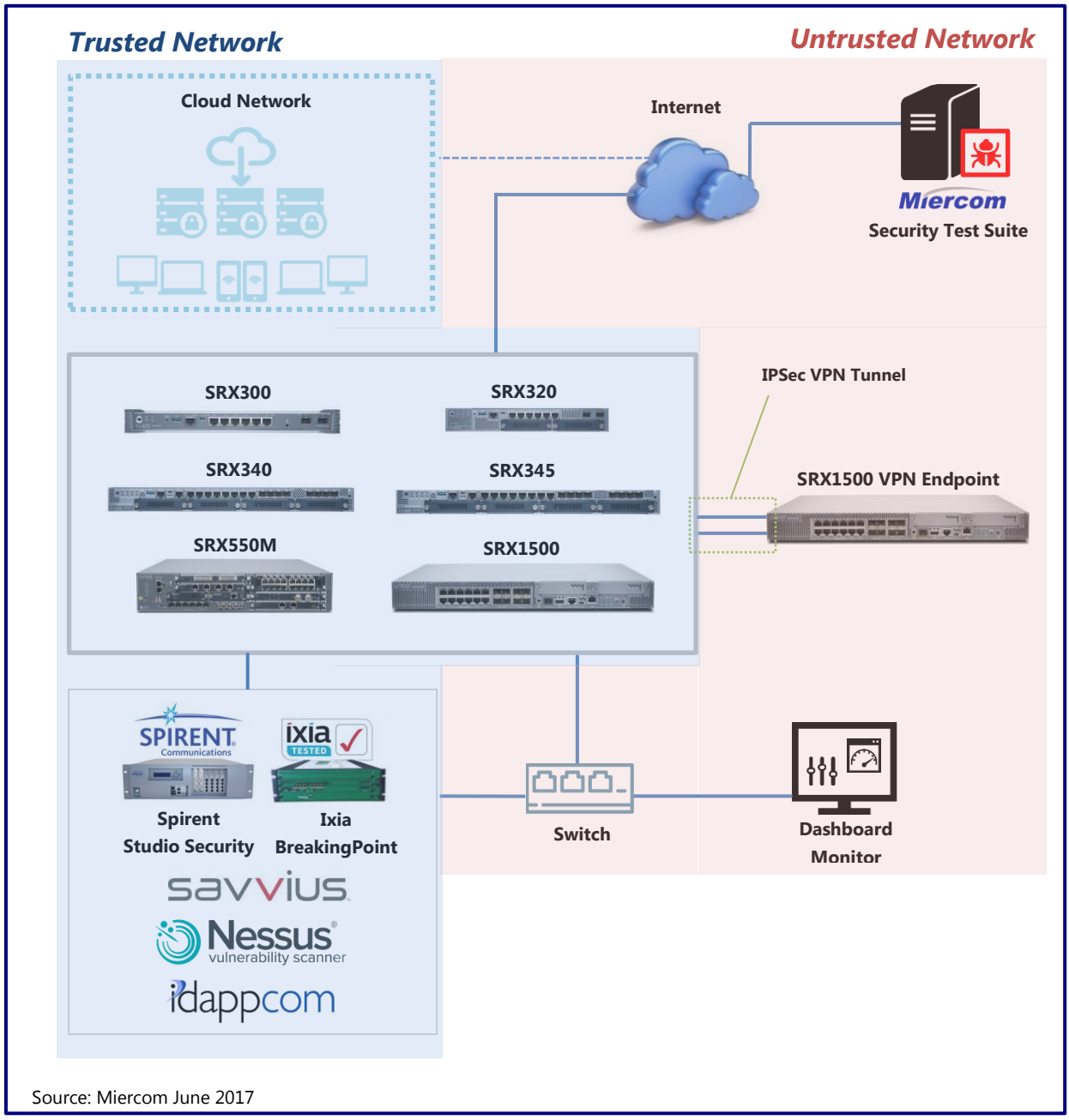
Miercom used hands-on testing designed to simulate real-world threat environments in order to provide a robust, realistic assessment of products' capabilities and their effectiveness. The fundamental aspect of the methodology was to create a framework of tests to validate the throughput performance of each Device Under Test (DUT). Traffic was generated to reflect the network activity of small businesses, branch offices, enterprises and corporations.

Test Tools

Source: Miercom June 2017

The test tools featured above are used for real-time traffic generation, traffic monitoring and data capture throughout testing. Miercom uses a unique blend of custom, proprietary attack scripts and globally collected threat samples.

Test Bed Diagram



Source: Miercom June 2017

The DUT was connected to a local network where traffic was generated in real-time by the Ixia BreakingPoint, using different protocols depending on the executed test. Throughput was observed for its maximum rate in bits per second before a single packet was lost. This data was recorded and compared to preliminary results, if available. The processing and memory usage for each test was also recorded, in percent of its maximum capacity. Tests were run first with routing capability only and then successively with security features enabled to determine the effect of security features on throughput performance.

Performance Testing

This section outlines the tests used to measure the gateway throughput. The network and generated traffic reflect real-world conditions for an enterprise environment.

What we tested

For stateless UDP IMIX traffic, the DUTs were tested with the following features enabled:

- Packet mode (routing)
- Firewall (FW)
- Network Address Translation (NAT)
- IPsec
- NAT and IPsec
- NAT, IPsec, Quality of Service (QoS) and Firewall filters

For stateful TCP traffic, the DUTs were tested with the features below:

- Application Firewall (AppFW)
- Application QoS (AppQoS)
- Application Routing (AppRouting)
- Intrusion Prevention System (IPS)
- Unified Threat Management (UTM)

All security features were verified for functionality using proprietary samples proven as malicious with a third-party security device.

UDP Forwarding Rate (IMIX Stateless Traffic)

Description

UDP packets were generated throughout the network to determine the maximum throughput of the DUT by incrementally increasing the load until packets were dropped. IMIX packets, a mixture of different packet size ratio, were used. CPU was recorded for each test. Testing used six modes of the gateway, for IPv4 and IPv6, using a combination of the following features:

Packet mode (routing): Forwarding of packets through network, from the internal client source to external server destination.

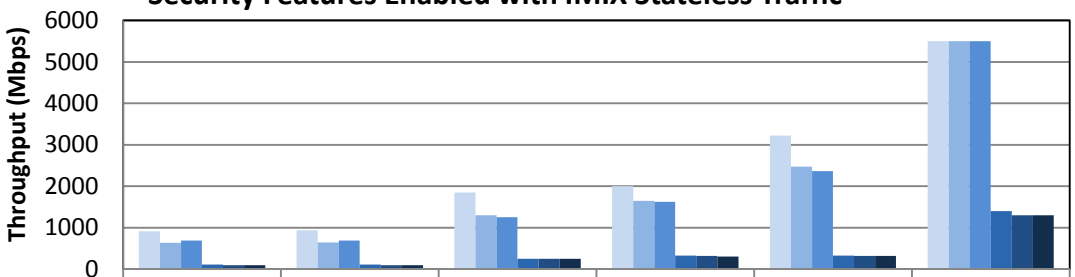
FW: Flow-based traffic was enabled and 100 firewall policies were applied between the trusted and untrusted zones of the network to screen packets for threats.

NAT: Source IP address mapping was enabled to pass trusted LAN data to the public untrusted LAN.

IPsec: An IPv4 Virtual Private Network (VPN) tunnel was created between a secondary SRX1500 gateway and the DUT. Four separate LANs were created to pass traffic through the IPsec tunnel; two in the trusted zone and two in the untrusted zone. This tunnel was used to authenticate and encrypt packets from each zone. Packets were encapsulated as IPv4 for the IPv6 addresses. AES256 encryption and SHA2 authentication algorithms were used.

QoS: Multi-field classifiers were used to mark and classify the LAN traffic into different queues over the IPSec tunnel interfaces.

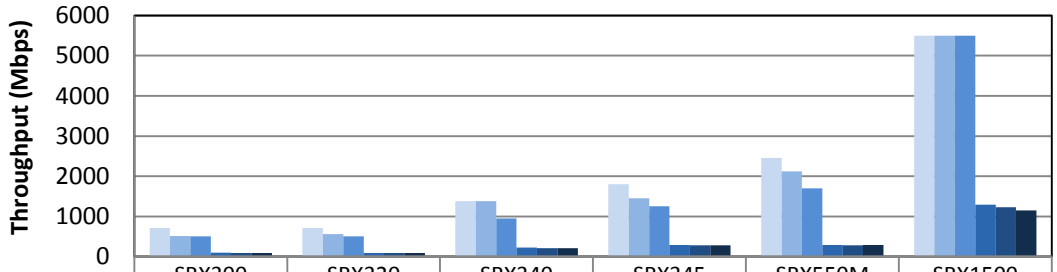
Juniper SRX Services Gateway
IPv4 Throughput (Mbps)
Security Features Enabled with IMIX Stateless Traffic



	SRX300	SRX320	SRX340	SRX345	SRX550M	SRX1500
Packet Mode	912	940	1850	2000	3220	5500
FW	632	640	1300	1650	2471	5500
NAT	690	690	1250	1620	2364	5500
IPsec	110	110	250	326	330	1400
NAT + IPsec	98	98	250	320	320	1300
NAT + IPsec + QoS + FW Filters	94	98	250	300	320	1300

Source: Miercom June 2017

Juniper SRX Services Gateway
IPv6 Throughput (Mbps)
Security Features Enabled with IMIX Stateless Traffic



	SRX300	SRX320	SRX340	SRX345	SRX550M	SRX1500
Packet Mode	712	712	1376	1800	2452	5500
FW	512	560	1376	1450	2120	5500
NAT	500	500	950	1250	1700	5500
IPsec	94	88	226	290	290	1290
NAT + IPsec	88	88	210	276	280	1230
NAT + IPsec + QoS + FW Filters	88	88	210	276	286	1150

Source: Miercom June 2017

TCP Forwarding Rate (HTTP 44KB Stateful Traffic)

Description

TCP packets were generated throughout the network to determine the maximum throughput of the DUT by incrementally increasing the load until packets were dropped. An HTTP 44 KB GET request was sent from the client side to download a binary JPG file from the public untrusted side. CPU was recorded for each test.

Testing used four modes of the gateway, for IPv4 and IPv6, using a combination of the following features:

AppFW: Monitors and controls application service; the HTTP GET request was allowed to pass between the trusted and untrusted networks.

AppQoS: Based on a characterization rule-set, Layer-7 packets can trigger the prioritization of application forwarding for the best efficiency; this was set to the highest priority.

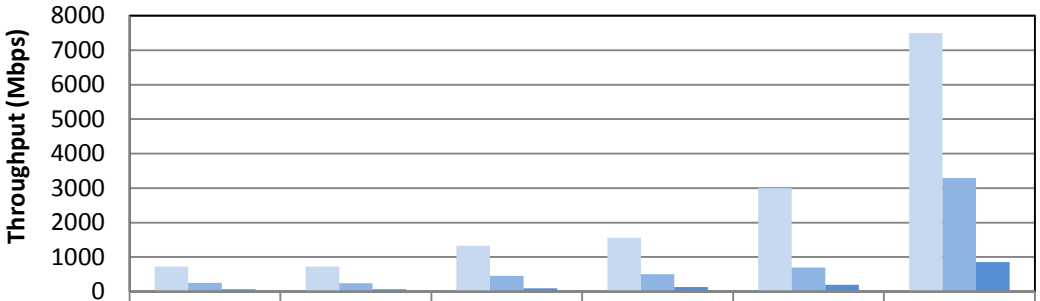
AppRouting: Outgoing WAN interface selection based on the Layer-7 application information; allowed applications were HTTP requests routed to the default gateway address.

IPS: Advanced attacks are detectable using the enterprise-grade, stringent intrusion detection; all possible methods are used to stop threats. This policy protects the server, web services, mail services, internal services and DNS against malicious activity to provide full protection. A "recommended" policy is identified and indexed by the Juniper Security Center.

UTM: Antivirus scanning with less processing-intensive, in-cloud solution; its database is stored and maintained on external Sophos servers, eliminating downloading of databases to the Juniper SRX. It is HTTP-based and supports FTP, SMTP, POP3 and IMAP. The Sophos AV, web-filtering and anti-spam was enabled.

Results

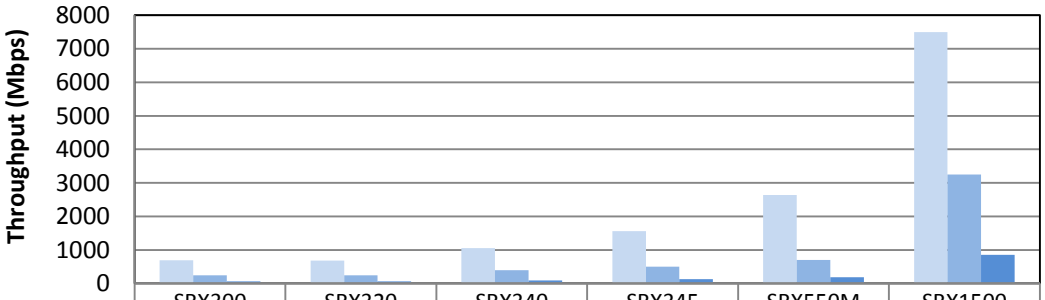
Juniper SRX Services Gateway
IPv4 Throughput (Mbps)
Security Features Enabled with Stateful Traffic



	SRX300	SRX320	SRX340	SRX345	SRX550M	SRX1500
AppFW + AppQoS + AppRouting	720	720	1325	1560	3000	7500
AppFW + AppQoS + AppRouting + IPS	250	240	450	500	700	3300
AppFW + AppQoS + AppRouting + IPS + UTM	60	60	90	130	190	850

Source: Miercom June 2017

Juniper SRX Services Gateway
IPv6 Throughput (Mbps)
Security Features Enabled with Stateful Traffic



	SRX300	SRX320	SRX340	SRX345	SRX550M	SRX1500
AppFW + AppQoS + AppRouting	690	680	1050	1560	2640	7500
AppFW + AppQoS + AppRouting + IPS	240	240	400	500	700	3250
AppFW + AppQoS + AppRouting + IPS + UTM	60	60	90	130	190	850

Source: Miercom June 2017

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed. Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

About Discovered Exploits

Miercom is under no obligation to provide notification or samples to any vendor with vulnerabilities discovered during testing. Active participation is afforded to each vendor before, during and after testing to work with Miercom to rectify any weak areas of security or performance. Unless there is active participation or an Ongoing Customer Care plan in state, all exploit samples are proprietary and kept confidential. Samples and specific vulnerabilities are not publicly published for the safety of the vendor, its products and product users.

About Miercom Annual Industry Assessment

Our Industry Assessment consists of comparative observations of products on the market which is published with results and recommendations. Every vendor is afforded the opportunity to represent themselves in the review. If a vendor does not actively participate, Miercom may elect to acquire the product(s) for testing. Industry Assessments are updated regularly to best reflect the current averages and comparative measurements. Any product tested by Miercom is eligible to be submitted into its industry's assessment.

Customer Use and Evaluation

We encourage customers to do their own product trials, as tests are based on the average environment and do not reflect every possible deployment scenario. We offer consulting services and engineering assistance for any customer who wishes to perform an on-site evaluation.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This is a private, confidential report and should only be apprehended and viewed under a mutual non-disclosure agreement between the featured vendor and the individual or party requesting pertinent data. If this report is acquired, it must be through a private and secure source. You are not permitted at any time to disclose this report and content therein. If you are interested in sharing this document, please contact the private source or Miercom.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.