Executive Summary
Results of Testing: Juniper Branch SRX Firewalls

by Joel Snyder / Opus One

prepared for Juniper Networks
June 2012

Table of Contents

Introduction 1
Firewall Feature Set and Role-based Firewall 2
UTM Feature Set: URL Filtering 3
UTM Feature Set: Anti-Malware 3
UTM Feature Set: Intrusion Prevention 4
Virtual Private Networks and Remote Access 5
Wireless Support 5
Management 6

Introduction

In May 2012, Opus One tested Juniper's branch SRX firewall[1] product line running recently-released Junos 12.1 software. The goals of the testing were to evaluate the SRX firewall from a security point of view, and to determine whether the SRX was ready to deploy into enterprise branch offices as a multi-service security device.

Opus One tested the branch SRX firewall, running literally hundreds of tests in 30 broad evaluation areas such as UTM capabilities, next-generation firewall, role-based firewall and IPSec VPNs.

Our tests show that the Juniper branch SRX firewall is fully ready for deployment in most enterprise branch office environments.

Opus One also tested Juniper's Security Threat Response Manager (STRM), a log collection and correlation tool, as an integral part of the SRX firewall. Our tests show that STRM offers valuable additional information, especially in deployments using the built-in IPS. We feel that STRM is a critical component of any mid-sized (or larger) SRX firewall deployment.

Enterprise customers and existing ScreenOS customers will find that the SRX exceeds the capabilities of the ScreenOS platform in areas such as UTM capabilities (especially IPS), clean integration of VPN and routing, IPv6 support, next-generation firewall, and advanced networking. While there are a few limited areas where the SRX and its supporting tools have not reached the sophistication level of older Juniper products, the SRX should be on the short list and test bench of every enterprise customer and existing ScreenOS customers.

Network managers with competitors' branch office firewall products will find that the branch SRX represents a new approach that complements the fusion of networking and security in organizations. Because the SRX UTM firewalls are built on top of the Junos routing platform, network managers don't have to surround the firewall with additional routing and switching devices to build a reliable security boundary. And in the branch environment, the SRX UTM firewalls have enterprise-class switching and routing capabilities, making a one-box-in-the-branch solution possible.

About Juniper SRX

The Juniper SRX firewalls are high-performance security, routing and network solutions for the enterprise. These devices pack high port-density, advanced security with application visibility and control, and flexible connectivity into a single, easily managed platform that supports fast, secure and highly-available operations.

While some of the low-end SRX platforms such as the SRX100/ 110/200 are better suited for the branch environment, many of the SRX devices, particularly the SRX240/550/650, are deployed in mid-enterprises where the SRX is not a branch device but is the enterprise security device.

The SRX firewalls are based on Junos, Juniper's proven operating system which delivers security and advanced protection services. Junos also supports rich routing and switching capabilities; Junos' unique architecture provides reliable service operations and manageability, even under the highest loads.

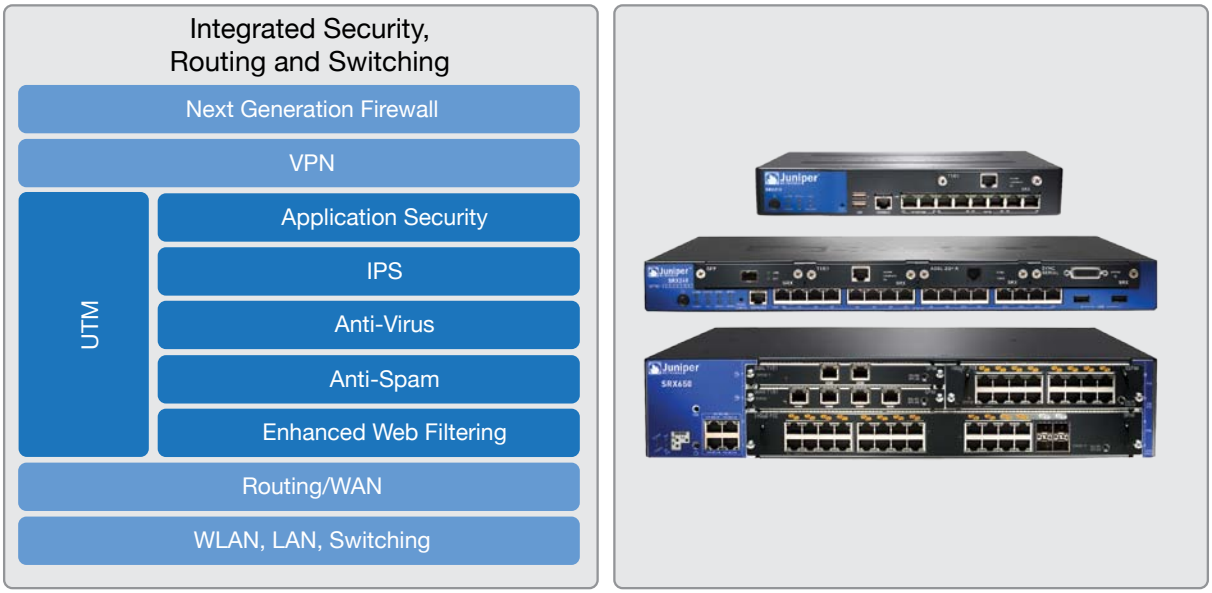

Figure 1. Juniper SRX firewalls are all-in-one device solutions providing consolidated networking and security, including firewall, VPN, and UTM features.

[1] Juniper refers to the SRX product line as "SRX Series Services Gateways." For the purposes of this test, we'll simply call them "SRX firewalls."

Firewall Feature Set and Role-based Firewall

Firewall vendors are busily adding both breadth and depth to their product lines, but any enterprise class firewall must have some basic security and networking features to form a solid foundation. The bar for a "baseline enterprise firewall" has been raised over time so that devices are now expected to go beyond stateful inspection to include:

- Site-to-site VPNs
- Network address translation
- High availability
- QoS/CoS features such as bandwidth management
- Enterprise networking including VLANs and link aggregation
- IPv6 support
- Global management and log aggregation
- Basic dynamic routing
- Role-based (user authentication) rule base

Results of Testing

Criteria	Notes
Create firewall security policies using normal criteria (source and destination IP, port, and protocol)	PASS SRX is a zone-based firewall, giving greater options for policy definition as well.
Create role-based firewall security policies to give different user groups different levels of access	PASS SRX role-based firewalls work in conjunction with Juniper's UAC appliance, extending the 5-tuple to match criteria to include user or group matching.
Validate correct operation of ALGs for VoIP and video, including when NAT is in place	PASS SRX firewall has a large set of media ALGs, including SCCP and MGCP in addition to the SIP and H.323 we tested.
Configure NAT using typical network scenarios	PASS SRX firewall NAT is configured separately from firewall policy, a more flexible approach than used in ScreenOS.
Build site-to-site VPNs using IPSec	PASS SRX firewall supports both IKE v1 an IKE v2. A VPN wizard is able to simplify the process of creating VPNs. More VPN testing appears below.
Configure and test active/passive high availability	PASS SRX firewall kept existing sessions alive and passed traffic when failure of the active node was detected during every test.
Use high availability features to switch outbound routes even when cluster connectivity is normal	PASS SRX firewall Realtime Performance Monitoring and IP Monitoring work together to change routing based on many possible criteria, providing high availability during network and IPS failures.
Configure QoS/CoS to manage bandwidth for different types of traffic	PASS SRX firewall QoS/CoS is configured separately from firewall policy, and may require some duplication of firewall rules and objects to match policies. SRX firewall QoS/CoS is not TCP-aware, so it throttles bandwidth by discarding packets.
Verify support and correct operation for VLANs and link aggregation (multiple Ethernet links)	PASS SRX firewall builds on Junos routing and switching platforms, and is discussed below in "Junos routing and switching."
IPv6 support	PASS SRX firewall IPv6 support is discussed below.
Dynamic routing support	PASS SRX firewall dynamic routing is discussed below in "Junos Routing and Switching."
Evaluate support for global management systems and log aggregation	PASS Juniper STRM log management is discussed in detail below in "Management."

UTM Feature Set: URL Filtering

URL filtering is used to control web browsing by blocking traffic to web sites based on policy criteria. URL filtering can be used to control the types of sites that users can browse (for instance, blocking time-wasting traffic such as games and personal shopping, or work-inappropriate traffic such as hate speech or pornography) and can help protect users against Internet security threats such as malware and phishing attacks.

Results of Testing

Criteria	Notes
Ability to define separate policies for different users, groups, and networks	PASS URL filtering is applied on a per-firewall rule basis, and each rule can invoke a different policy.
Choice among URL filtering engines	PASS SRX firewalls have four different options, including integration with existing enterprise Websense engine (if present). Only one engine can be active at a time.
Inclusion of reputation-based filtering as an option in URL filtering	PASS The Juniper Enhanced engine includes reputation services to increase the effectiveness of anti-malware protection through URL filtering.
Accurately blocks and allows URLs per policy	PASS The Juniper SRX firewall has excellent URL filtering capabilities.
Fully logs both blocked and allowed traffic with category and URL info	PASS SRX, combined with STRM, gives access to logs as well as usage graphs.

UTM Feature Set: Anti-Malware

Enterprise best practices call for anti-malware software to be running on every desktop. However, network managers frequently deploy anti-malware on edge devices such as UTM firewalls to provide an additional layer of protection. Edge anti-malware helps protect branch users if their desktop anti-malware falls behind in updates or is shut off entirely.

Results of Testing

Criteria	Notes
Ability to define separate policies for different networks and traffic types	PASS Anti-malware scanning is applied on a per-firewall rule basis, letting you turn scanning on and off for different subnets and user groups. Configuration options appropriate for this type of device and network location are available.
Choice among anti-malware engines	PASS SRX firewall has three different options, including an in-the-cloud option, an on-device engine, and a performance-optimized engine.
Accurately blocks traffic in critical protocols (HTTP and FTP)	PASS SRX firewall blocked malware found in HTTP and FTP traffic.
Accurately blocks traffic in secondary protocols (SMTP, POP3 and IMAP4)	PASS SRX firewall blocked malware in SMTP and POP3 traffic, but not in IMAP4 traffic.
Blocks application traffic on non-standard ports (such as HTTP on port 1234)	FAIL SRX firewalls do not identify selected protocols running on non-standard ports or encrypted traffic.
Logs all blocked malware	PASS SRX firewalls contain a number of alerting mechanisms to log malware, including syslog and Juniper's STRM.

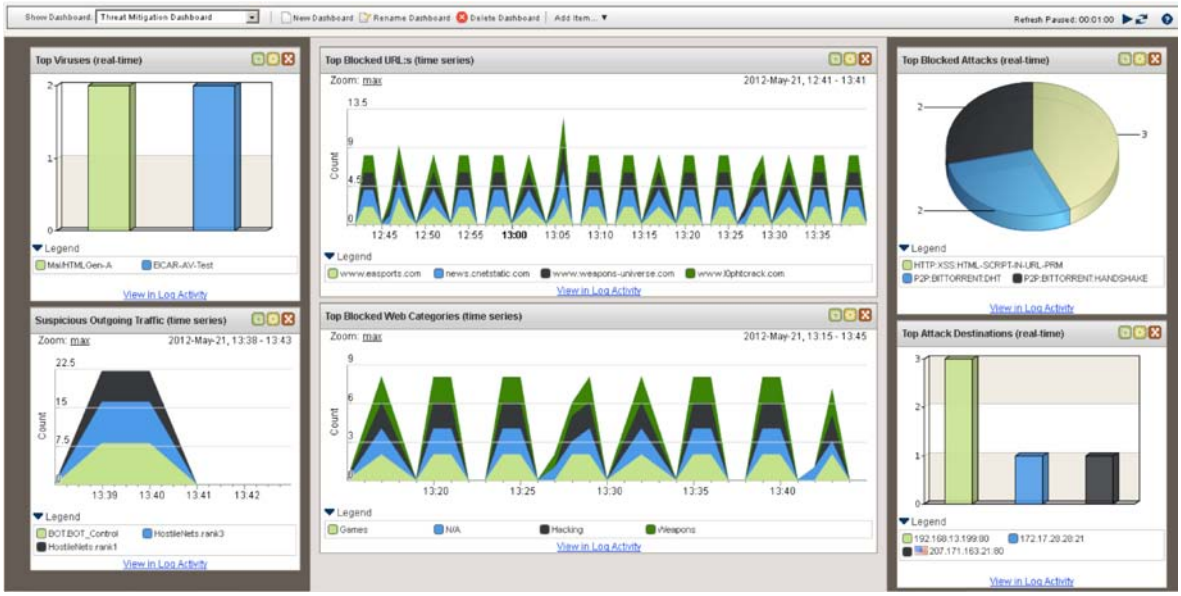

Figure 2. Juniper's STRM reporting console logs blocked viruses and malware, correlating user identity with other log information.

UTM Feature Set: Intrusion Prevention

Intrusion prevention technology in edge firewalls helps to move the protections provided by the firewall towards the application layer. With an attack surface closed off by the firewall at the transport layer and below, the application layer remains a huge target with what seems like an unlimited number of vulnerabilities to be exploited. Adding intrusion prevention technology between the enterprise and the Internet helps to reduce overall risk by blocking thousands of known attacks. As security researchers at Microsoft have shown, more than 80% of infected Windows systems are from malware more than six months old. While zero-day threats remain an issue, 180-day threats are a bigger operational problem for network managers.

Results of Testing

Criteria	Notes
Ability to define separate policies for different networks and traffic types	PASS IPS is enabled on a per-rule basis within the firewall, and the IPS policy also can apply specific signatures and signature groups on a per system or subnet basis.
Accurately blocks attacks when directed against clients	PASS SRX firewall blocked over 98% of attacks against clients.
Accurately blocks attacks when directed against servers	PASS SRX firewall blocked over 87% of attacks against servers even though server protections not commonly used in the branch.
Policy management is straightforward and fast	PASS IPS policy management will improve when Juniper Security Design is available and integrated with STRM, but existing CLI-based tools are sufficient for branch policy management.
Logs attacks (when configured), and provides context and central correlation features	PASS SRX firewall combined with Juniper STRM gives sufficient information to identify and research attacks.
Protects against DoS/DDoS attacks	PASS SRX firewall "Screens" tested to block flood attacks.

Virtual Private Networks and Remote Access

Virtual private network (VPN) technology has been considered a "must-have" in firewalls for over a decade. Linking secure communications and access controls makes VPNs and firewalls a logical combination. In the enterprise environment, where each network element represents a support liability and potential failure point, combining VPN, remote access and a UTM firewall in a single system makes even more sense.

Results of Testing

Criteria	Notes
Test for full support of IPSec-based site-to-site VPN tunnels	PASS SRX firewalls support both IKE v1 and IKE v2.
Validate easy design and deployment of VPNs using simplified on-device configuration	PASS SRX wizards support both site-to-site and remote access VPN definition.
Test for dynamic routing support over VPN tunnels	PASS SRX firewalls include support for OSPFv2/v3 (tested), as well as RIP/RIPng, reduced-traffic RIP, BGP/MBGP, IS-IS, multicast routing, and Bidirectional Forwarding Detection (BFD, RFC 5880).
Validate asymmetric routing over VPN tunnels does not interrupt traffic	PASS Asymmetric routing over VPN tunnels is a common problem during routing table convergence in some products, but not with the SRX.
Configure policy-based and route-based IPSec site-to-site VPNs	PASS Most SRX firewall users will choose route-based IPSec VPNs for their management simplicity and flexibility.
Build remote-access VPNs for end-user network connection to branch offices	PASS Both traditional IPSec remote access clients and Juniper's own Windows Pulse client are supported. Users without the Pulse client will automatically download it simply by browsing to the SRX firewall and logging in.
Validate support for central design and deployment of VPNs	Not Tested: Juniper Security Design is Juniper's central management solution for SRX firewalls with full centralized VPN configuration capability, but was not tested.

Wireless Support

Wireless LANs are a key enabling technology for mobility, yet many enterprises have handicapped themselves by avoiding Wi-Fi because of security concerns. Securing Wi-Fi and integrating it with firewall policy enforcement can help break down administrative objections and barriers to adoption.

Results of Testing

Criteria	Notes
Full management of access points	PASS SRX completely manages the APs it is responsible for, including collection of log data.
Creation of secure and unencrypted wireless SSIDs on the same radios	PASS AX411 supports up to 16 SSIDs per radio per access point, although we only tested two. Juniper calls these "Virtual APs."
Segregate traffic by SSID to different VLANs apply per-SSID access policies	PASS Traffic from each SSID is tagged with a VLAN, letting the SRX apply security policies based on SSID.
UTM protections can be applied to wireless traffic before it is sent to the rest of the network	PASS Traffic from the access point can be VLAN-trunked back to the SRX firewall to keep it off the network until after risk mitigation tools such as anti-malware, intrusion prevention and URL filtering.
Enterprise-class wireless security can be applied to the wireless channel	PASS We tested WPA Enterprise, but the access point also supports older encryption protocols and MAC authentication.
Allows physical separation of the AP from the firewall	PASS The AX411 is connected via Ethernet to the SRX firewalls and can be PoE powered by the SRX.

Management

Well-designed and easy-to-use security device management is a critical part of any large deployment. In a branch office environment, where there may be hundreds or thousands of devices, effective management tools are needed to ease the tasks of updating security policies, VPN configurations, software images, and device settings. Regulatory regimes for many industries—and best practices overall—require tight control over firewall configurations and the ability to audit changes and compliance with policy. Reporting is also an important part of firewall deployments, with help desk troubleshooters, IPS managers, and security auditors all dependent on good log management and log analysis tools to support them in their daily tasks.

Results of Testing

Criteria	Notes
Has on-box web-based GUI	PASS SRX firewall GUI runs in most browsers, but some reporting is done in Flash.
Has on-box CLI	PASS CLI is based on Junos syntax, so will be very familiar to network managers with other Juniper network devices.
Has central management system	PASS Junos Space combined with Security Design can be used for central management[2].
Has on-box reporting and monitoring tools	PASS J-Web includes both logging and simple reporting tools to speed debugging and problem resolution.
Has centralized reporting and monitoring tools	PASS Juniper's STRM is a SEIM and log manager with extensive correlation and reporting capabilities.

[2] N.B. Junos Space and Security Design were not tested as part of this test plan.