Product Assessment

Juniper Networks SRX5000 Line

Firewalls and VPNs in Enterprise Security

July 14, 2009

Andrew Braunberg
Research Director, Enterprise Software and Security

Contents

Current Analysis
Outsmart your competitors

For more information, please call +1 703 404 9200, toll-free +1 877 787 8947,
Europe +33 (0) 1 41 14 83 14. Or visit our Web site: www.currentanalysis.com

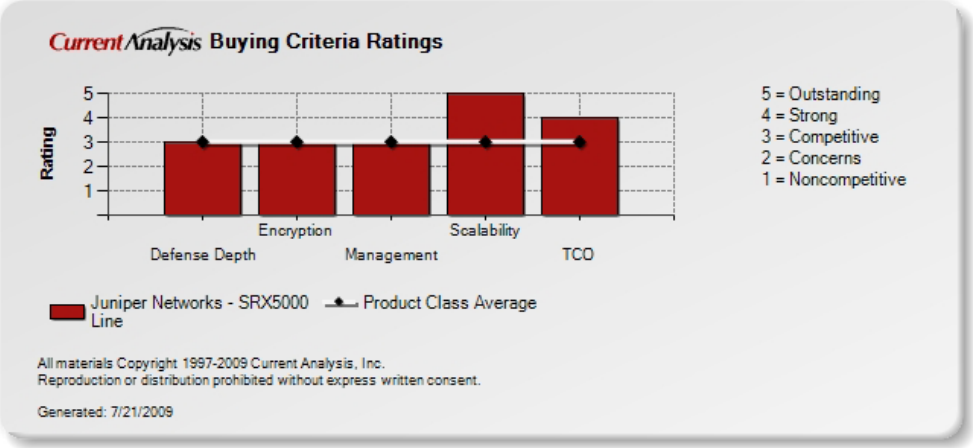
Juniper Networks SRX5000 Line

Analyst:
A. Braunberg

Date Updated:
July 14, 2009
Product Class:
Firewalls and VPNs in Enterprise Security

Summary

Buying Criteria



Current Perspective: Threatening

Juniper's new SRX family of security gateway appliances are threatening because the new products deliver impressive performance improvements to the high end of Juniper's security portfolio. The products leverage Juniper's Dynamic Services Architecture, which allows for flexible and dynamic resource allocation across processor and input/output pools to deliver the appropriate resources to each security service (e.g., firewall, IPS) as needed.

Juniper has been moving to consolidate its entire product portfolio onto its JUNOS operating system for several years now. The shift of security functionality from ScreenOS to JUNOS has been a bit painful, but the release of the SRX gateways is a milestone in that effort. JUNOS is built for performance and the first members of the SRX family (SRX5000 line) of appliances deliver performance in spades.

The foundational strength of the SRX family is Juniper's new Dynamic Services Architecture, which allows a much more intelligent sharing of resources among security services running on the gateway. Supported services include stateful firewall, intrusion prevention system (IPS), distributed denial of service (DDoS/DoS) protection, network address translation (NAT), and dynamic routing. The first products introduced were the SRX5600 and the SRX5800. The SRX5800 delivers up to 120 Gbps firewall throughput and up to 30 Gbps IDP. The SRX5600 provides 60 Gbps firewall and 15 Gbps IDP.

There are several concerns associated with this announcement, however. The product is unmatched as a stand alone firewall but when IPS is added to the mix performance drops significantly and management becomes an issue. Juniper in particular needs to quickly improve Network and Security Manager's ability to manage the IPS features in SRX.

The SRX product family will have a high impact on the threat management markets because of the performance and flexibility that they support. The 5000 series is targeted at large

Product:

Juniper Networks SRX5000 Line

Firewalls and VPNs in Enterprise Security

enterprise and service provider customers and will likely be used predominately as high-performance firewalls and purchased for their throughput capabilities. However, as Juniper continues to introduce additional products to the SRX family, the products will also impact the UTM market as well. For example, the SRX family includes the SRX-branch products – SRX210, SRX240, SRX650 – which include UTM capabilities such as AV, anti-spam, and URL filtering.

Target Markets

Global 2000, ISPs, Global Carriers

Strengths and Weaknesses

Strengths

• The SRX5000 line of security gateways deliver blazing firewall throughput. The SRX5800 boasts 120Gbps through its 16 10Gigabit Ethernet interfaces. The ability to handle that kind of throughput allows users of the SRX boxes to consolidate a lot of legacy security boxes, freeing up considerable rack space and reducing energy requirements.

• Juniper is finally making good on its promise to port all of its products over to the JUNOS operating system. The SRX family is part of the new wave of security products from Juniper that leverages the mature and respected JUNOS OS.

• The SRX5000 line leverages Juniper's new Dynamic Services Architecture. This new architecture provides a processing pool that is sharable across security services along with a terabit backplane. This capability allows the SRX products to more efficiently distribute processing loads across service processing cards (SPCs) in the devices while maintaining industry leading performnace.

• The SRX5000 line supports numerous security services. These are: stateful firewall, intrusion prevention system (IPS), distributed denial of service (DDoS/DoS) protection, network address translation (NAT), and dynamic routing. Traffic inspection methods include: protocol anomaly detection; traffic anomaly detection; IP spoofing detection; and DoS detection.

Weaknesses

• When additional services, such as IPS, are also run then throughput drops considerably (30Gbps) compared to performance in firewall only mode. That is not to say that 30Gbps IPS performance is not impressive, but it does point out that even Juniper's innovative Dynamic Services Architecture is going to take a hit when performing deep packet inspection.

• The SRX boxes are very high end enterprise firewalls. The breadth of UTM functionality in the boxes at this point is still fairly limited, however. The products do not support gateway Anti-X capabilities or content filtering.

• Integration between the SRX family and Juniper's Network and Security Manager (NSM) management appliance is not fully realized. For example, NSM does not recognize security alerts from SRX boxes. This limits the flexibility of managing the gateways through NSM, particularly when running IPS.

Product:

Juniper Networks SRX5000 Line

Firewalls and VPNs in Enterprise Security

Point and Counterpoint

Point: The SRX family of products lacks defense in depth.

Counterpoint: The SRX5000 series of products currently support stateful firewall, intrusion prevention system (IPS), distributed denial of service (DDoS/DoS) protection, network address translation (NAT), and dynamic routing. Additional security services will be added over time.

Point: The SRX family of products lacks fully integrated IPS management through Network and Security Manager (NSM).

Counterpoint: NSM is designed to provide comprehensive management of Juniper products. NSM supports Juniper Networks J-series services routers, EX-series Ethernet switches, Secure Access SSL VPN and firewall/VPN and Intrusion Detection and Prevention appliances, and the newly announced Unified Access Control (UAC) solution. The product is rapidly maturing with 5 product updates between January 2007 and December 2008.

Point: Juniper is a pure infrastructure vendor, offering only firewall, VPN, and IDS functionality, and it does not have the breadth of product necessary to support a complete security infrastructure for the enterprise computing environment. Many of Juniper's key competitors offer complete security solutions that reach all the way down to the desktop level. Juniper cannot achieve this level of integration due to its exclusive focus on network hardware.

Counterpoint: Since Juniper is focusing solely on security technologies, it can deliver a much more focused and higher-performance solution at a better cost than competitors can. The SRX products are a prime example of the benefits of this strategy. Juniper also works with key partners, including Symantec, Websense, and Kaspersky to augment its security capabilities.

Point: The SRX family of products lacks SSL VPN capabilities.

Counterpoint: Juniper supports impressive IPSec VPN functionality through the SRX family. The SRX5800 delivers up to 30 Gbps AES or 3DES performance and up to 100,000 concurrent VPN tunnels. The SRX5600 delivers up to 15Gbps AES or 3DES performance and up to 40,000 concurrent VPN tunnels.

Buying/Selecting Criteria

Depth of Defense: COMPETITIVE

• Supported services include stateful firewall, intrusion prevention system (IPS), distributed denial of service (DDoS/DoS) protection, network address translation (NAT), and dynamic routing. Traffic inspection methods include: protocol anomaly detection; traffic anomaly detection; IP spoofing detection; and DoS detection.

• The SRX5000 gateways do not support anti-virus scanning or content filtering.

Product:

Juniper Networks SRX5000 Line

Firewalls and VPNs in Enterprise Security

• The SRX gateways support important IPS capabilities including: stateful signature inspection; protocol decoding; signature matching; traffic normalization; application identification; and zero-day protection.

• There is a 100-MB policy size limit for IDP attack signatures. Because the IDP policy templates supported are dynamic, that is they can be updated with additional attack signatures, they must be monitored so that they do not grow beyond the 100-MB policy size limit.

Encryption: COMPETITIVE

• SRX gateways support DES, 3DES, and AES encryption. The SRX5800 delivers up to 30 Gbps AES or 3DES performance and up to 100,000 concurrent VPN tunnels. The SRX5600 delivers up to 15Gbps AES or 3DES performance and up to 40,000 concurrent VPN tunnels.

• SRX gateways can be deployed as a router, running BGP, RIP, or OSPF, or as an L2 device in "transparent mode." The gateways can maintain a maximum of 8 million concurrent connections.

• SRX gateways do not support SSL VPN. Additionally, Juniper does not provide a VPN client for use with the IPSec VPN functionality.

Management: COMPETITIVE

• Juniper is moving toward a standardized management system for its products. The SRX services gateways are managed by Network and Security Manager (NSM), which is the same management solution used in Juniper's firewall, IDP, Secure Sockets Layer (SSL), Unified Access Control (UAC), and EX-series products. NSM was formerly known as the NetScreen Security Manager. Third party testing of the SRX family demonstrates that management of the full range of security services available on the SRX through NSM is still a work in progress.

• The SRX appliances also leverage the JUNOS operating system. Juniper has been working for years to port its security services over to the mature and scalable JUNOS OS. (Its security products have traditionally run the NetScreen ScreenOS.) Juniper released JUNOS 9.0 in the spring of 2008. Juniper has long criticized Cisco for maintaining too many operating systems and any progress Juniper makes in OS consolidation is welcome.

• In SRX5800 devices, IDP is not officially supported in an active/active chassis cluster configuration. Administrators must disable the IDP configuration when the devices are configured in an active/active chassis cluster.

Scalability: OUTSTANDING

• The SRX5800 delivers up to 120 Gbps firewall throughput and up to 30 Gbps IDP performance. The SRX5600 provides 60 Gbps firewall and 15 Gbps IDP. These are significant improvements over the performance available in Juniper's current NetScreen 5400 and 5200 products.

• The SRX appliances leverage Juniper's new Dynamic Services Architecture. This new architecture provides a processing pool that is sharable across security services on a terabit

Product:

Juniper Networks SRX5000 Line

Firewalls and VPNs in Enterprise Security

backplane. This capability allows the SRX products to more efficiently distribute processing loads across service processing cards (SPCs) in the devices. Supported services include stateful firewall, intrusion prevention system (IPS), distributed denial of service (DDoS/DoS) protection, network address translation (NAT), and dynamic routing.

• Input/output cards (IOCs) can also be mixed as needed and all of the slots can be used for either service processing card or for I/O cards. Each Input/output card supports 40 Gigabit interfaces (4 x 10 Gigabit Ethernet or 40 x 1 Gigabit Ethernet). There is also a newly announced FlexIOC that offers greater modularity in terms of mixing and matching GigE with 10GigE connectivity through 16xGigE and 4x10GigE modules. This architecture provides users with extreme flexibility in tailoring the device to specific network requirements.

• The SRX5800 supports a total of 11 Service Processing Cards (SPC), or IO Cards (IOC). The SRX5600 supports a total of 5 SPC or IOC cards. The SPCs are available with dual CPUs and 8 GB of total memory.

Total Cost of Ownership: STRONG

• One of Juniper's chief selling points for the SRX gateway family is the reduced TCO associated with migration to these boxes. This is realized both through significant space savings when consolidating services onto the SRX as well as considerable power savings.

• Juniper also claims savings by standardizing services onto the JUNOS operating system. All SRX services are delivered on the same version of the same operating system. This in turn, simplifies the use of a common management system, Network and Security Management (NSM) across Juniper security, routing and switching products.

• The base chassis price for the SRX5800 is $68,000. The SRX5600 is a bit less, $65,000. SPC and IOC cards run $100,000. The recently announced FlexIOC offers additional I/O flexibility in terms of mixing copper and fiber GigE with 10 GigE ports and is offered in 16xGigE or 4x10GigE modules. The FlexIOC runs $40,000 while the 16xGigE modules run $15,000 and 4x10GigE modules run $25,000.

Product Metrics

Product: Juniper Networks SRX5000 Line

General Information	
Product Functionality	The Juniper Networks SRX 5800 is a next-generation services gateway based on a revolutionary new architecture that provides market-leading scalability and service integration. Equipped with full security and networking capabilities, the SRX services gateway represents the highest performing firewall in the market, with more than 120 Gbps firewall throughput.
Device Specific Information	
Interface Count	Can support up to 440 Gigabit Ethernet ports, or up to 88 10 Gigabit Ethernet ports
Interface Types	40 x 1 Gigabit ethernet form-factor pluggable transceiver (SFP)4 x 10 Gigabit Ethernet XFP (SR or LR)16 x Gigabit ethernet (copper or fiber) FlexIOC4 x 10 Gigabit ethernet XFP (SR or LR) FlexIOC"
Redundant Power Supplies	Yes, AC and DC
NEBS Compliance	Yes
Remote/Out of Band Management	Yes
High Availability Port	Yes - Active/Passive, Active/Active HA configuration using dedicated high availability interfaces
Routing Protocols	BGP, OSPF, RIP v1/v2, dynamic routing, static routes, source-based routing, policy-based routing, ECMP, RPF, ISIS
Product Warranty	1 year for hardware, 90 days for software
802.1Q VLAN Tagging	Yes
Latest Shipping Software	JUNOS 9.5 Software
VPN Specific Information	
Maximum Concurrent Connections	8 Million
3DES Performance	30 Gbps
3DES Accelerated Performance	30 Gbps
Encryption Algorithms	DES, 3DES, AES
Network Integration	SRX5000 series can be deployed as a router, running BGP, RIP, or OSPF, or as an L2 device in "transparent mode"
Industry Certifications	
Tunneling Protocols	IPSec
CAs Supported	MS, RSA, Baltimore
Key Management	IKE, PKI (x.509)
CA Revocation Methods	CRL,OCSP
High Availability Features	Active/passive, active/active; Configuration synchronization; Session synchronization for firewall and IPsec VPN; Session failover for routing change; Device failure detection; Link failure detection
VPN Architecture	Policy-based, route-based
AES Performance	30 Gbps

Continued

Product Metrics *(Continued)*

Product: Juniper Networks SRX5000 Line *(Continued)*

NAT Traversal	Yes
SSL VPN Tunneling Features	N/A
SSL VPN Translation Features	N/A
SSL VPN Browser Support	N/A
VPN Client Information	
Client Name	No client provided
Client Status	No client provided
OS Support	No client provided
Authentication Methods	No client provided
Split Tunnel Support	No client provided
Client Lock-Out	No client provided
Personal Firewall	No client provided
Personal Firewall Configuration	No client provided
Remote Management	No client provided
Client Config Check	No client provided
Client Failover	No client provided
Firewall Features	
Firewall Type	Stateful
Address Translation	Destination, Source, Static (rules based)
High Availability Sessions	Session state sync between chassis for both firewall and IPSec VPN
Load Balancing	Internal to the chassis session based load balancing across an array of N processing blades
Protocol Support	IP RFC 791; ICMP RFC 792; ARP RFC 826; RIP RFC 1058; RIP Version 2 (with authentication) RFC 1723; OSPF RFC 2328; IGMP (multicast) RFC 2236; BGP4 RFC 1771; IPv6 Core RFCs; IPv4 RFC 1812; BOOTP/DHCP Server, Relay, Client; PIM-SM, RIPng
Firewall Architecture	Stateful, multi-blade, multi-processor
Virtual Firewalling	Targetted 2H10
Management Features	
Management Station	Network and Security Manager (NSM)
Management OS Support	2008.1 or later
Management Devices Supported	NSMXpress
Management Client Support	2008.1 or later on Windows 2000, XP, Vista and Linux
Logging Options	STRM
NMS Integration	Yes, integrates with all major network management systems
Policy Based Configuration	Supported

Continued

Product Metrics *(Continued)*

Product: Juniper Networks SRX5000 Line *(Continued)*

Management Security	Yes - HTTPS, SSH, telnet over IPSec
Value Added Features	
Denial of Service Protection	Yes - DDoS/DoS
IDS Intelligence	5500 signatures for identifying anomalies, attacks, spyware, and applications; Stateful Signature Inspection; Protocol decodes; Traffic normalization; Application awareness/ identification on any TCP or UDP port; Zero-day protection
Anti-Virus Scanning	No
Content Filtering	No
Pricing	
Solution Hardware Pricing	"Base chassis - $68,000 Includes chassis, fan trays, power supplies, switch fabric and route engine"
Add-on Hardware	SPC - US$100,000, IOC - US$100,000, FlexIOC - US$40,000.
Software Licenses	IPS Subscription
VPN Client Pricing	N/A
Solution Description & Restrictions	N/A
Support/Maintenance	
Hardware Maintenance Costs	Varies depening on system configuration
Maintenance Include S/W Updates	Varies depening on system configuration
Software ONLY Maintenance Cost	We do not offer SW only support. Minimum service level includes JTAC phone support and web based support tools.