PRODUCT CATEGORY BROCHURE

INTEGRATED FIREWALL/ VPN PLATFORMS

Strong Security for Access Control, User Authentication, and Attack Protection at the Network and Application Level

As threats to the network grow more prevalent and destructive, securing the infrastructure is critical to maintaining a viable business. Attacks come from multiple sources in a variety of forms. Enterprises and service providers need more than just a security device; they require a comprehensive, reliable, and integrated security solution backed by an industry leader.

The Juniper Networks® integrated security devices are purpose-built to perform essential networking security functions. Optimized for maximum performance and feature integration, they are designed on top of robust networking and security real-time operating systems, Juniper Networks Junos® operating system and ScreenOS®. Designed from ground up to provide the superior networking and security capabilities, these operating systems are not plagued by inefficiencies and vulnerabilities of general-purpose operating systems.

With a range of purpose-built, high-performance platforms that deliver integrated security and LAN/WAN routing across high-density LAN/WAN interfaces, Juniper Networks integrated security devices address the needs of small to medium sized locations, large distributed enterprises, and service providers as well as large and co-located datacenters. These integrated devices can protect the network from all manner of attacks and malware while simultaneously facilitating secure business-to-business communications.

Product Line Highlights:

- Complete set of Unified Threat Management (UTM) security features—including stateful firewall, application security, intrusion prevention, antivirus, antispyware, anti-adware, and antiphishing), antispam, and Web filtering—stops worms, spyware, trojans, malware, and other emerging attacks. (**Note**: Not all UTM features are available on all platforms.)
- Centralized, policy-based management minimizes the chance of overlooking security holes by simplifying rollout and network-wide updates.
- Virtualization technologies make it easy for administrators to divide the network into secure segments for additional protection.
- Various high availability (HA) options offer the best redundant capabilties for any given network.
- Rapid-deployment features, including Auto Connect VPN and Dynamic VPN services, help minimize the administrative burden associated with widespread IPsec deployments.

Perimeter Defense Begins with Network-Level Protection

To protect against network-level attacks, Juniper Networks devices use a dynamic packet filtering method known as stateful inspection to unmask malicious traffic. With this method, firewalls collect information on various components in a packet header, including source and destination IP addresses, source and destination port numbers, and packet sequence numbers. When a responding packet arrives, the firewall will compare the information reported in its header with the state of its associated session. If they do not match, the packet is dropped.

Stateful inspection provides more security than other firewall technology such as packet filtering because the traffic is examined under the context of the connection and not as a collection of various packets. By default, the Juniper Networks firewall denies all traffic in all directions. Then, by using centralized, policy-based management, enterprises can create security policies that define the parameters of traffic that is permitted to pass from specified sources to specified destinations.

Secure, reliable WAN connectivity also plays an important role in network-level protection. By deploying robust virtual private networks (VPNs), remote sites can be securely connected to other remote sites and to centralized data and applications using high-bandwidth shared media such as the Internet. Features such as Auto Connect VPN, available on select models, can help ease the administration and management of VPNs, particularly in hub-and-spoke topologies, allowing secure connections to be automatically set up and taken down without manual configuration.

Day-Zero Protection Against Application-Level Attacks

To help block malicious application-level attacks, Juniper Networks seamlessly integrates intrusion prevention across the entire product line. For central enterprise sites, data center environments and service provider networks with high volumes of throughput, the Juniper Networks ISG Series Integrated Security Gateways with IPS, Juniper Networks SRX100, SRX210, SRX220, SRX240, SRX650, SRX3000 line and SRX5000 line of services gateways can be deployed for application-level protection. The ISG Series and SRX Series tightly integrates the same software found on the Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to provide unmatched application-level protection against worms, trojans, spyware, and malware. More than 60 protocols are supported including those used by advanced applications such as VoIP and streaming media.

Unmatched security processing power and network segmentation features protect critical high-speed networks against the penetration and proliferation of existing and emerging application-level threats. With multiple attack detection mechanisms, including stateful signatures and protocol anomaly, the ISG Series and SRX Series performs in-depth analysis of application protocol, context, and state to deliver Zero-day protection from application level attacks

On all other models, security administrators can deploy IPS capability using Deep Inspection to block application-level attacks before they infect the network and inflict any damages. Deep Inspection utilizes two of the eight attack-detection mechanisms available on the standalone IDP Series appliances and integrates them with the stateful inspection firewall.

SECURITY PLATFORMS

- SRX100
- SRX210
- SRX220
- SRX240
- SRX650
- SRX3400
- SRX3600
- SRX5600
- SRX5800
- SSG5/SSG5 Wireless
- SSG20/SSG20 Wireless
- SSG140
- SSG320M/350M
- SSG520M/550M
- ISG1000
- ISG2000
- NetScreen-5200
- NetScreen-5400

Integrated Antivirus Protects Remote Locations

For remote offices or smaller locations without full-time IT staff, integration and simplicity are an absolute must in any security solution. Juniper Networks currently provides integrated file-based antivirus protection from Kaspersky Lab on the Juniper Networks SSG Series Secure Services Gateways and the SRX Series Services Gateways for the branch. These products combine firewall and VPN capabilities with an antivirus scanning engine that includes antiphishing, antispyware, anti-adware to provide a comprehensive security solution in a single device.

These integrated appliances scan for viruses imbedded in both email and Web traffic by scrutinizing IMAP, SMTP, FTP, POP3, IM and HTTP protocols. They provide the most advanced protection from today's fast-spreading worms, viruses, trojans, spyware, and other malware from damaging the network. With its ability to uncompress files using common protocols, the engine scans deep inside attachments to detect threats hidden in multiple levels of compression.

Controlling Access to Known Malware and Phishing Websites

Employees who access inappropriate websites from the corporate network risk bringing malicious software into the organization. Worse, their errors in judgment could also expose the company to litigation for not having adequate controls in place. Juniper Networks integrated security devices are the ideal solution to help organizations devise and enforce responsible Web usage policies.

Two approaches are available: external and integrated Web filtering. External Web filtering, available on all Juniper Networks firewall and VPN devices, redirects traffic from the device to a dedicated Websense Web filtering server for enforcement of the organization's policies. Integrated Web filtering, available on the Juniper Networks SRX Series Services Gateways for the branch and SSG Series, enables enterprises to build their own Web access policies by selectively blocking access to sites listed in a continuously updated database. Maintained by Websense, a Juniper Networks security alliance partner, the database lists more than 20+ million URLs organized into more than 54 categories of potentially problematic content.

Customers can rapidly deploy integrated or external Web filtering using default configurations based on the Websense database. Web filtering profiles can be customized by using black lists or white lists, plus a number of predefined and user-defined categories.

Blocking Inbound Spam and Phishing Attacks

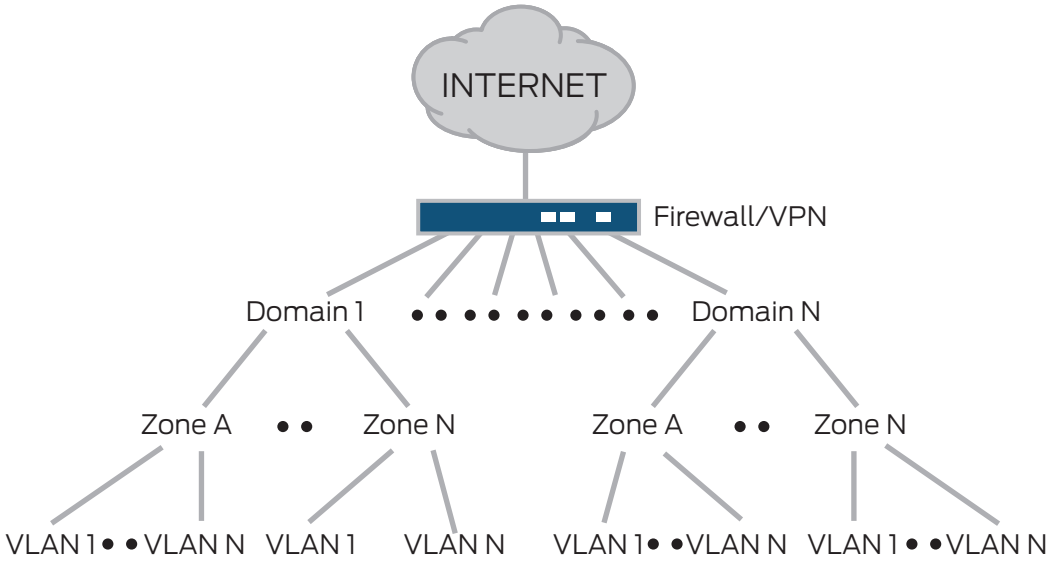
Juniper Networks has teamed up with Sophos to leverage their market-leading antispam solution and reputation service for Juniper's small-to-medium office platforms to help limit unwanted emails and the potential attacks they carry. Installed on the Juniper Networks firewall/VPN gateway, the antispam engine filters incoming email from known spam and phishing users, acting as a first line of defense. When a known malicious email arrives, it is blocked and/or flagged so that the email server can take appropriate action. Integrated antispam is available on the entire SSG Series family and the SRX Series Services Gateways for the branch.

Virtualization Boosts Security by Dividing the Network into Multiple Network Segments

Virtualization technologies in the Juniper Networks integrated firewall/VPN, and secure router security solutions enable users to segment their network into many separate compartments, all controlled through a single appliance. Administrators can simply segment traffic bound for different destinations, or they can further divide the network into distinct, secure segments with their own firewalls and separate security policies.

The firewall/VPN devices support the following virtualization technologies:

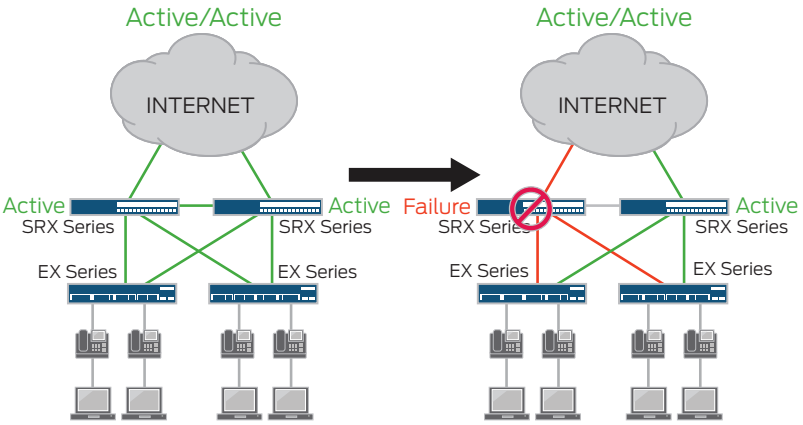
- **Security Zones:** Supported on every product, security zones represent virtual sections of the network, segmented into logical areas. Security zones can be assigned to a physical interface or, on the larger devices, to a virtual system. When assigned to a virtual system, multiple zones can share a single physical interface which lowers ownership costs by effectively increasing interface densities.
- **Virtual Systems (VSYS):** Available on the ISG Series and Juniper Networks NetScreen Series Security Systems, virtual systems are an additional level of partitioning that creates multiple independent virtual environments, each with its own set of users, firewalls, VPNs, security policies, and management interfaces. By providing administrators with the ability to quickly segment networks into multiple secure environments managed through a single device, VSYS enables network operators to build multi-customer solutions with fewer physical firewalls and reduced administrative attention. This reduces both capital and operational expenses.
- **Virtual Routers (VR):** Supported on all products, virtual routers enable administrators to partition a single device so it functions like multiple physical routers. Each VR can support its own domains, ensuring that no routing information is exchanged with domains established on other VRs. This enables a single device to support multiple customer environments, lowering total cost of ownership.
- **Virtual LANs (VLAN):** Supported on all platforms, VLANs are a logical – not physical – division of a subnetwork that enables administrators to identify and segment traffic at a very granular level. Security policies can specify how traffic is routed from each VLAN to a security zone, virtual system or physical interface. This makes it easy for administrators to identify and organize traffic from multiple departments and define what resources each can access.



Networks are segmented into hierarchies of secure compartments using virtual technology.

Comprehensive High Availability Solutions Ensure Uptime

A security system is only as good as its reliability and uptime. Juniper Networks security solutions include reliable, high availability systems based on the NetScreen Redundancy Protocol (NSRP) and Juniper Services Redundancy Protocol (JSRP) to run on Junos operating system-based products. Firewall, VPN, and IPS flows can be synchronized between high availability pairs to provide subsecond failover to a backup device. Configuration options include:



High availability configurations maintain service despite device or link failures

- **Active/Passive:** Master device shares all network, configuration setting, and current session information with the backup so that, in the event of a failure, the backup can take over in a seamless manner. Juniper Networks Network and Security Manager provides centralized, policy-based control.
- **Active/Active:** Both devices are configured to be active, with traffic flowing through each. Should one device fail, the other device becomes the master and continues to handle 100 percent of the traffic. The redundant physical paths provide maximum resiliency and uptime.

Device Integration Made Easy

Networks are never static. Potentially costly and time-consuming changes and additions occur all the time. When the network topology changes, or as new offices, business partners, and customers are added to the network, network interoperability becomes especially important. To simplify network integration and help minimize administrative effort when changes are required, Juniper Networks integrated security solutions can operate in three different modes:

- **Transparent mode** affords the simplest way to add security to the network. In transparent mode, organizations can deploy a Juniper Networks firewall/VPN appliance without making any other changes to the network: firewall, VPN, IPS, and denial-of-service (DoS) mitigation functions work without an IP address, making the device "invisible" to the user.
- **Route mode** enables the security device to actively participate in network routing by supporting both static and dynamic routing protocols, including BGP, OSPF, RIPv1, RIPv2, and ECMP. Route mode enables administrators to quickly deploy multilayer security solutions with a minimum of manual configuration.
- **NAT mode** automatically translates an IP address or a group of IP addresses to a single address to hide an organization's private addresses from public view.

Juniper Networks integrated security devices support both static and dynamic address assignment through DHCP or PPPoE, enabling Juniper Networks solutions to operate in any network environment.

Unbound Scalability

As network requirements continue to evolve, the processing and I/O requirements for various network devices will also evolve. To meet the demands of ever changing scalability requirements, the SRX3000 line and SRX5000 line of services gateways leverage the Dynamic Services Architecture.

Dynamic Services Architecture enables the most flexible I/O and processing configuration by supporting service processing cards and I/O cards on the same slot, allowing the SRX3000 line and SRX5000 line of services gateways to be configured as a processing-intensive solution or an I/O-intensive solution and anywhere in between. The scalability with incremental cards are almost linear with very little overhead. This extensive I/O and processing scalability brought about by Juniper's Dynamic Services Architecture is only available on the SRX3000 line and SRX5000 line of services gateways.

Managing the Network and Security

Unlike solutions that require administrators to use multiple management tools to control a single device, Network and Security Manager enables IT departments to control the device throughout its life cycle with a single, centralized dashboard. It is designed specifically to foster teamwork among device technicians, network administrators, and security personnel.

Network and Security Manager takes a new approach to security management by providing IT departments with an easy-to-use solution that controls all aspects of the firewall/VPN security device, including device configuration, network settings, and security policy.

Juniper Networks STRM Series Security Threat Response Managers provides Security Information and Event Management (SIEM) capabilities with advanced multivendor monitoring and event correlation and sophisticated comprehensive log management. Juniper Networks Advanced Insight Solution(AIS) and Juniper Networks Advanced Insight Manager (AIM) provide in-service diagnostic functionality with flexible automated monitoring and reporting. Third-party network management partners supporting the Juniper products provide additional management solutions for network, fault, performance, and change control. By selecting the appropriate management tool, network administrators can deploy, manage and troubleshoot large network deployments.

For Low-Cost Rapid Deployment, Drop Ship Devices—Not Administrators

To avoid the high cost of sending administrators to configure systems at remote sites, Juniper Networks integrated security devices can be installed by nontechnical users. With the Network and Security Manager Rapid Deployment functionality, network administrators do not need to preconfigure the devices or handle them in any way.

At the remote site, the new device simply needs to be cabled up and loaded with a small configuration file, which a central administrator has either emailed or sent on CD to the remote location. The initial configuration file establishes a secure connection to Network and Security Manager which then pushes the complete configuration files to the new device.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at **www.juniper.net.**

JUNIPER NETWORKS SERVICE AND SUPPORT

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services/.**

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

♻ Printed on recycled paper

1500024-009-EN Aug 2010