PRODUCT CATEGORY BROCHURE

SECURITY SERVICES GATEWAYS

Integrated Strong Security for Enterprise Data Center and Branch, Service Provider Infrastructure, and Cloud Deployments

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 an integrated and comprehensive, layered approach to securing the network, backed by an industry leader.

Taking a Layered Approach to Securing the Network:

With the number of security attacks on the rise, securing the network has become a critical and challenging task for IT professionals. At Juniper Networks our approach to securing the network is via a comprehensive layered approach comprised of several distinct technologies, including next generation firewalls, virtual security for data centers and clouds, virtual private networks, anti-virus scanning, Web content filtering and anti-spam, intrusion detection/prevention systems and application security. By employing a layered security approach, customers benefit from a system of barriers that is many times tougher than each of the individual components.

Protecting Physical and Virtual Workloads:

The Juniper Networks SRX Series Services Gateways is a purpose-built platform to perform essential networking security functions. Optimized for maximum performance and feature integration, the SRX Series is designed on top of the robust networking and security real-time operating system, the Juniper Networks® Junos® operating system. Unlike general-purpose operating systems, the Junos operating system is not plagued by inefficiencies and vulnerabilities as it has been designed from the ground up to provide superior networking and security capabilities.

The SRX Series provides integrated security and LAN/WAN routing across high-density LAN/WAN interfaces, Juniper Networks integrated security services gateways address the needs of small to medium sized locations, large distributed enterprises, and service providers as well as large and co-located datacenters. These services gateways protect the network from all type of attacks and malware while simultaneously facilitating secure business-to-business communications.

With cloud computing and virtualization adoption on the rise, the evolution of the data center brings a new set of challenges to IT professionals. While the need for physical network security will continue to exist in data centers, organizations will continue to adopt cloud computing in phases, resulting in hybrid environments—essentially, a mix of physical and virtualized data center workloads. This data center model will result in some workloads like those on physical servers being secured by physical firewalls, while others, such as those running on virtual machines (VMs), being at risk, because traditional security methods provide zero visibility into VM traffic. To address this concern, Juniper Networks has integrated Juniper Networks Firefly Host with the Junos OS-based SRX Series platform to extend the protections of the SRX Series products into virtualized environments.

Product Line Highlights:

- AppSecure is a suite of next-generation security capabilities that utilize advanced application identification and classification to deliver greater visibility, enforcement, control, and protection over the network.
- Firefly Host is a purpose built firewall for virtualization that protects traffic to/from virtual machines (east/west traffic). Firefly Host also includes IPS, Virtualization Specific AV, Introspection which allows you to scan the installation properties of a virtual machine (such as the OS, applications and hot fixes), Smart Groups which supports the use of attributes to create dynamic system associations for VMs) and a Compliance Module with pre-defined and custom rules engine alerts on virtual machine and host configuration changes. Firefly Host is tightly integrated into the VMware hypervisor and VMware management framework (VCenter).
- Complete set of next generation firewall and Unified Threat Management (UTM) security features—including stateful firewall, application security, user role-based firewall controls, intrusion prevention, on-box and cloud-based antivirus, antispyware, anti-adware, and antiphishing), antispam, and enhanced Web filtering to protect your network from the latest content-borne threats.
- Integrates with other Juniper security products to deliver enterprise-wide unified access control (UAC) and adaptive threat management
- Centralized, policy-based management minimizes the chance of overlooking security holes by simplifying rollout and network-wide updates.
- Technologies make it easy for administrators to divide the network into secure segments.
- Various high availability (HA) options offer the best redundant capabilities for any given network.
- Rapid-deployment features, including AutoVPN 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 firewall will execute the actions specified in the security policy, which typically involves dropping the packet and logging the action.

Stateful inspection provides more security than other firewall technologies 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 AutoVPN, 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.

SECURITY PLATFORMS
• SRX100
• SRX110
• SRX210
• SRX220
• SRX240
• SRX550
• SRX650
• SRX1400
• SRX3400
• SRX3600
• SRX5400
• SRX5600
• SRX5800

Protection From Application-Level Threats

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 SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650, SRX1400, SRX3000 line and SRX5000 line of services gateways can be deployed for application-level protection. 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 SRX Series Services Gateways perform in-depth analysis of application protocol, context, state and behavior.

Security administrators can deploy Juniper Networks AppSecure capability using deep inspection to block application-level attacks before they infect the network and inflict any damage. AppSecure utilizes advanced, high-performance detection mechanisms integrated with stateful inspection firewall, along with multiple threat inspection engines operating in parallel to accurately detect advanced persistent threats, including those found in nested applications within applications. The services that are enabled by AppSecure include: AppTrack for detailed visibility of application traffic; AppFW for granular policy enforcement of application traffic; AppQoS to prioritize and meter application traffic; and application signatures for identifying applications and nested applications, so that applications are accurately identified and the resulting information can be used for visibility, enforcement, control and protection. AppSecure also works with the SRX Series' integrated intrusion prevention system (IPS) solution to deliver deeper protection.

Integrated Antivirus Protects Remote Locations

For remote offices or smaller locations with limited IT staff, integration and simplicity are an absolute must in any security solution. Juniper Networks currently provides on-box or cloud-based AV protection on the Juniper Networks SRX Series Services Gateways for the branch. These products combine firewall and VPN capabilities with an antivirus scanning engine that includes antiphishing, antispyware, and 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 to prevent damage to 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 SRX Series for the branch, 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 60 million websites organized in more than 95 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

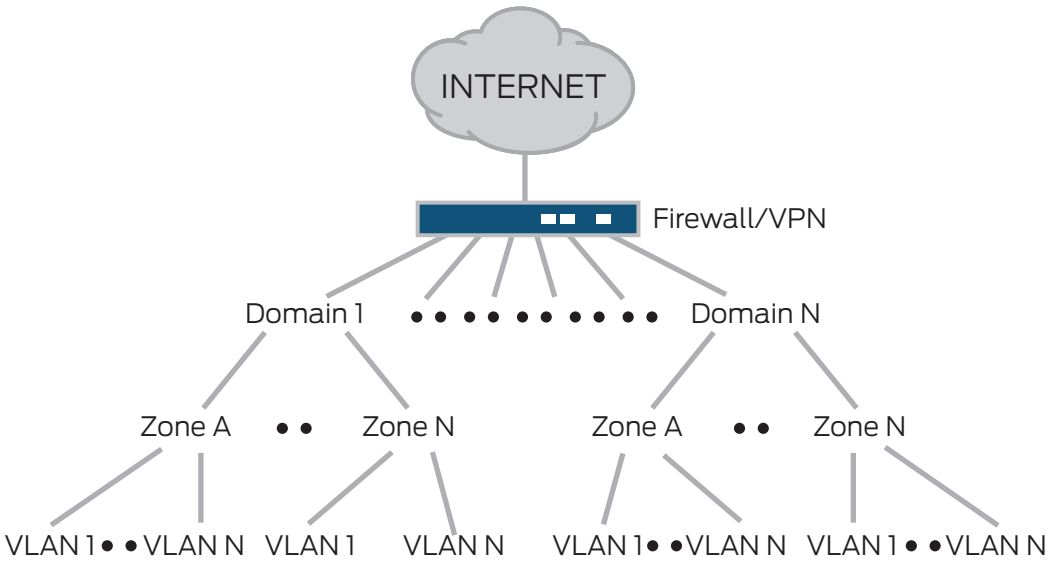
Juniper Networks has teamed up with Sophos to leverage their market-leading antispam solution and reputation service for Juniper's small-to-medium office platforms to help limit unwanted emails and the potential attacks they carry. Installed on the Juniper Networks firewall/VPN gateway, the antispam 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 SRX Series for the branch.

Boosting Security by Dividing the Network into Multiple Network Segments

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 all SRX Series gateways, 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. There is zone policy visibility and integration with Firefly Host.
- **Logical Systems (LSYS):** Available on the SRX1400, SRX3000 line and SRX5000 line of services gateways gateways, logical 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, LSYS 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 SRX Series gateways, 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.



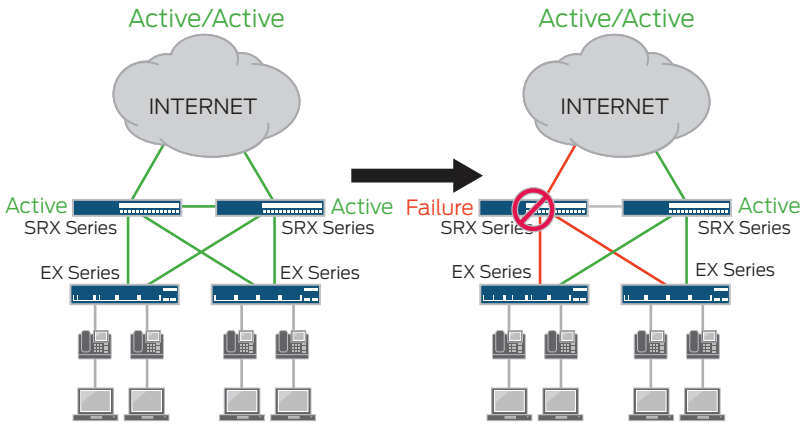
Networks are segmented into hierarchies of secure compartments using virtual technology.

- **Virtual LANs (VLAN):** Supported on all SRX Series gateways, 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.

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 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:

- **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 Junos Space Security Director 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.



High availability configurations maintain service despite device or link failures.

In addition, Juniper Networks SRX1400, SRX3000 line and SRX5000 line of services gateways are the only high-end firewall line in the market to support in-service software upgrades (ISSU) and in-service hardware upgrades (ISHU) for always-on security, offering maximized security 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 SRX1400, SRX3000 line and SRX5000 line of services gateways leverage the Juniper Networks 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 high-end SRX Series Services Gateways to be configured as a processing-intensive solution or an I/O-intensive solution and anywhere in between. The SRX3000 line and SRX5000 line is able to scale performance almost linearly by adding additional network and services processing cards with very little overhead. This extensive I/O and processing scalability brought about by Juniper's Dynamic Services Architecture is only available on the data center class of SRX Series Services Gateways.

Managing the Network and Security

Unlike solutions that require administrators to use multiple management tools to control a single device, Junos Space Security Director enables IT departments to control the device throughout its life cycle with a single, centralized dashboard.

As an application on Junos Space Network Management Platform, Junos Space Security Director provides extensive security scale, granular policy control, and policy breadth across the network. It helps administrators quickly manage all phases of the security policy life cycle for stateful firewall, unified threat management (UTM), intrusion prevention system (IPS), application firewall (AppFW), VPN, and Network Address Translation (NAT) through a centralized web-based interface. Junos Space Security Director reduces management costs and errors with efficient security policy, workflow tools, and a powerful "app" and platform architecture.

Juniper Networks Secure Analytics provides Security Information and Event Management (SIEM) capabilities. By combining, analyzing and managing an unparalleled set of surveillance data—network behavior, security events, vulnerability profiles, and threat information—it helps empower companies to efficiently manage business operations on their networks from a single console. It offers superior log management with distributed log collection and centralized viewing; threats management that deliver real-time surveillance and detection information; and compliance management capabilities—all viewed and managed from one console. Juniper Networks Advanced Insight Solution (AIS) provides 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.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. 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 +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

1500024-013-EN June 2014