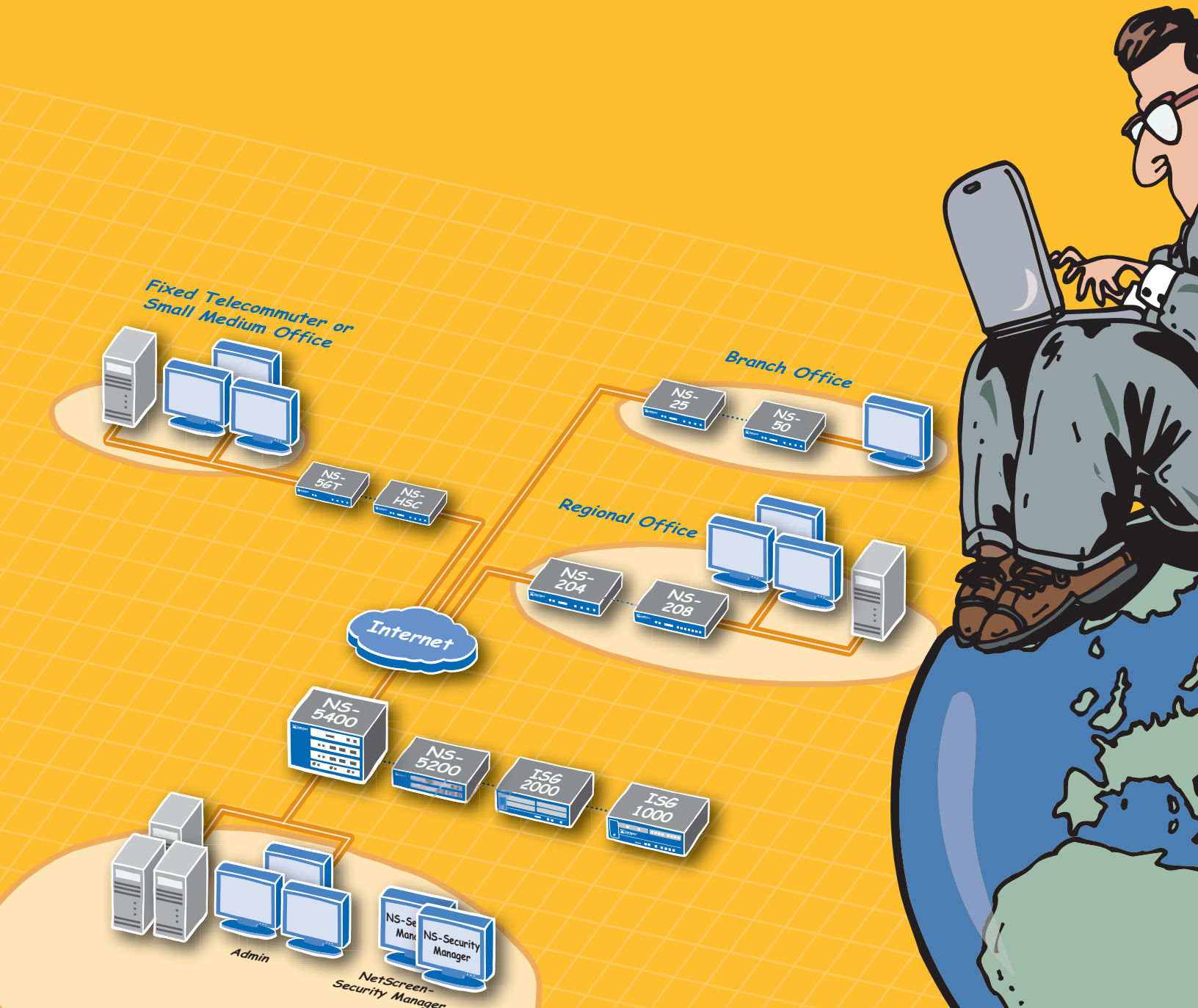
Juniper NETWORKS

Security Solutions Portfolio

Juniper Networks Integrated Firewall/VPN Solutions



Juniper Networks
NetScreen-Hardware Security Client

Juniper Networks
NetScreen-5GT
Wireless

Juniper Networks
NetScreen-5GT and
NetScreen-5GT ADSL

Juniper Networks
NetScreen-50

Juniper Networks
NetScreen-25

Juniper Networks
NetScreen-208

Juniper Networks
NetScreen-204

Juniper Networks
NetScreen-500

Juniper Networks
ISG 1000

Juniper Networks
ISG 2000

Juniper Networks
NetScreen-5200

Juniper Networks
NetScreen-5400

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 security solution backed by an industry leader.

The Juniper Networks integrated security devices are purpose-built to perform essential security functions. Optimized for maximum performance, they are controlled by a security-specific, real-time operating system called ScreenOS. This operating system has been designed from the ground up to perform security functions without the overhead that can create vulnerabilities in other security products that rely on general-purpose operating systems.

With a range of platforms that vary in performance and interface density, Juniper Networks integrated security devices address the needs of small to medium businesses, large distributed enterprises and service providers. These integrated devices provide network and application-level protection, virtual private networking (VPN) capabilities, and denial of service (DoS) mitigation functions.

Product highlights:

- Deep Inspection firewall extends stateful inspection to detect application level attacks and stop them at the network perimeter
- Integrated Intrusion Prevention for unmatched application-level protection against worms, Trojans, Spyware and malware in the enterprise, carrier and data center environments
- Centralized, policy-based management minimizes the chance of overlooking security holes by simplifying roll-out and network-wide updates
- Virtualization technologies make it easy for administrators to divide the network into secure segments for additional protection
- Built-in high availability features allow pairs of devices to be deployed together to eliminate single points of failure
- Rapid Deployment features help minimize repetitive tasks and administrative burden associated with wide spread deployments

Perimeter defense begins with stateful inspection

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 it opens smaller "holes" through which traffic can pass. 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.

Deep Inspection and Integrated Intrusion Prevention deliver application-level protection

The Juniper Networks Deep Inspection firewall builds on the strength of stateful inspection and integrates intrusion prevention technology which provides application-level attack protection at the network perimeter. The Deep Inspection firewall applies a deeper level of application understanding to the traffic across ten commonly used protocols to make access control decisions based on the intent of that traffic. If the packet contents are inappropriate for the application it seeks, the packet can be dropped. Deployed at the perimeter, a Deep Inspection firewall can block application-level attacks before they infect the network and inflict any damages.

For enterprise central site and data center environments with high volumes of throughput, the Juniper Networks Integrated Security Gateway (ISG) Series with IDP can be deployed for application-level protection. The ISG Series with IDP tightly integrates the same software found on the Juniper Networks IDP platforms into ScreenOS to provide unmatched application-level protection against worms, Trojans, Spyware and malware. The ISG Series supports over 60 protocols including those used by advanced applications such as VoIP and streaming media.

Unmatched security processing power and network segmentation features allow the ISG Series to 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 with IDP performs in-depth analysis of application protocol, context and state to deliver Zero Day network and application-level attack protection.

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 network-based antivirus protection on the NetScreen-5GT Series and NetScreen-HSC. The products combine firewall and VPN capabilities with an antivirus engine to provide a comprehensive security solution in a single device.

These integrated appliances scan for viruses imbedded in both e-mail and web traffic by scrutinizing IMAP, SMTP, FTP, POP3 and HTTP protocols. They provide the most advanced protection from today's fast-spreading network viruses such as MSblast, Sobig, and Code Red. With its ability to uncompress files using common protocols, the engine scans deep inside attachments to detect viruses hidden in multiple levels of compression.

Web filtering prevents inappropriate web usage

Employees who access inappropriate web sites 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/VPN devices, redirects traffic from the device to a dedicated SurfControl or Websense web filtering server for enforcement of the organization's policies. Integrated web filtering, available on the NetScreen-HSC, -5GT Series, -25 and -50, enables enterprises to build their own web access policies by selectively blocking access to sites listed on a continuously updated database. Maintained by SurfControl, a Juniper Networks security alliance partner, the database lists more than six million URLs organized into more than 40 categories of potentially problematic content.

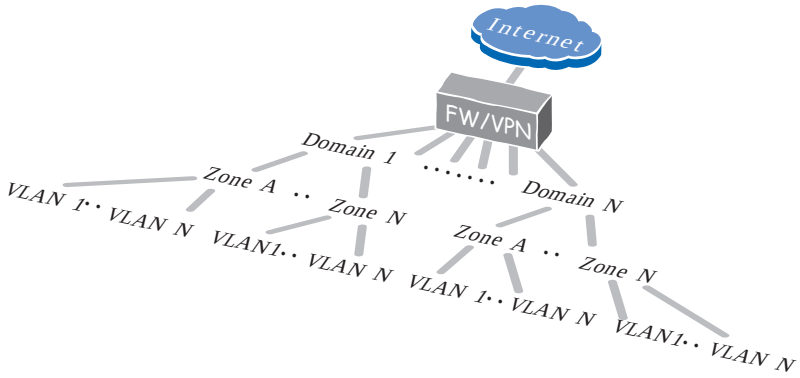
Customers can rapidly deploy integrated or external Web filtering using default configurations based on the SurfControl database. Web filtering profiles can be customized by using black lists, white lists, plus a number of pre-defined and user-defined categories.

Virtualization boosts security by dividing network into multiple network segments

Virtualization technologies in the Juniper Networks integrated firewall/VPN 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 go on to 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 NetScreen-500 and above, 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 the NetScreen-200 and above, 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.

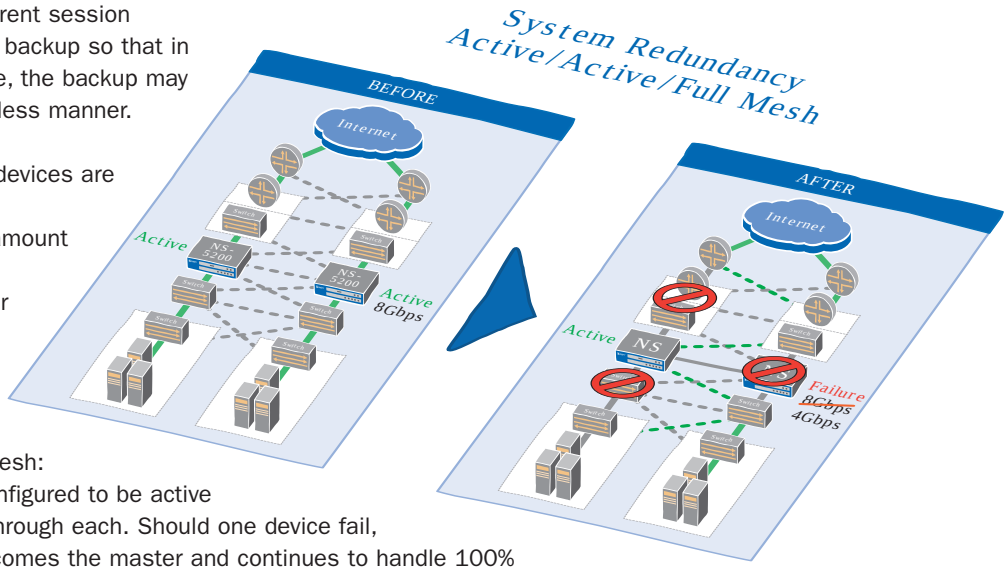
Comprehensive high availability solutions ensure uptime

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). Firewalls and VPNs can be synchronized between high availability pairs to provide sub-second failover to a backup device. Configuration options include:

- Active/Passive: Master device shares all network, configuration settings and the current session information with the backup so that in the event of a failure, the backup may take over in a seamless manner.

- Active/Active: Both devices are active, sharing an approximate equal amount of the load. If one fails, the other unit takes over to maintain traffic flow and security.

- Active/Active/Full Mesh: 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% of the traffic. The redundant physical paths provide maximum resiliency and uptime.



Full-mesh high availability configurations maintain service despite device failures

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 or 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 any changes to the network: firewall, VPN, and 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 multi-layer 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 address assignment, as well as dynamic address assignment through DHCP or PPPoE, enabling Juniper Networks solutions to operate in any network environment.

NetScreen-Security Manager provides centralized, policy-based control

Juniper Networks NetScreen-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.

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

The intuitive user interface of NetScreen-Security Manager streamlines configuring devices, creating security policies, and setting up VPNs. It is easy to delegate administrative roles so that everyone who has a role to play has access to the information and controls they need, while comprehensive logging tracks who performs each action. Dramatic reductions in operating costs are common because NetScreen-Security Manager promotes organizational efficiency like no other product on the market.

For low-cost rapid deployment, drop-ship devices – not administrators

To avoid the high costs of sending administrators to configure systems at remote sites, Juniper Networks integrated security devices can be drop-shipped to remote locations where non-technical users can install them. With the NetScreen-Security Manager Rapid Deployment functionality, network administrators do not need to preconfigure the devices or handle them in any way.

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

Service and support when and where it's needed

Juniper Networks Professional Services consultants and the experts of authorized Juniper Networks partners are recognized throughout the industry as knowledgeable networking specialists. They are uniquely qualified to assist in assessing network vulnerabilities and planning ways to address them.

The Customer Support Center provides responsive assistance and software upgrades, security updates, and online knowledge tools to ensure maximum reliability of Juniper Networks products. Professional instructors of Juniper Networks Educational Services help customers keep pace with rapidly evolving technologies by sharing the company's expertise on operating stable, secure networks.

Juniper Networks delivers secure and assured security solutions

Juniper Networks integrated firewall/IPSec VPN security devices are purpose-built solutions that deliver secure and assured networking by protecting against network and application level attacks while maximizing performance. Designed to satisfy demanding service provider and enterprise environments alike, Juniper's integrated security devices deliver predictable performance for a highly reliable, available and secure network. Juniper Networks integrated firewall/VPN security devices provide the best foundation to secure today's networks.

To purchase Juniper Networks integrated security systems, please contact a Juniper Networks sales representative or authorized reseller.

Juniper Your Net™

www.juniper.net

Juniper NETWORKS

CORPORATE HEADQUARTERS AND SALES HEADQUARTERS FOR NORTH AND SOUTH AMERICA
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

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501

150024-002 Sept2005