

JUNIPER NETWORKS MOBILE SECURITY SOLUTION

Market-Leading Security Products Providers Can Use to Mitigate the Deployment Risks of IP-Based Services

Challenge

Network security focused on securing the transport layer is inadequate for next-generation all-IP networks, which require a multilayer security matrix that also protects the control/signaling layers and the service/application layer, integrated policy enforcement, and secure-access technology for all layers.

Solution

Providing an innovative, market-leading mobile security solution that mitigates the risks associated with deploying IP-based services, Juniper's security devices are scalable, reliable, and backed by years of experience shaping the routing and security architectures of the world's top service provider networks.

Benefits

- Highly effective network security through multilayered approach
- Includes network access control, authentication, authorization, transport layer security, firewall, and intrusion detection and prevention
- Provides deployment options for flexibility and a broad range of protocol support

The Challenge

What if you were managing a computer network and not implementing full security protection? Would you feel safe? For years, security was a very obvious element of computer networking but attacks through mobile devices were not that common. However, with increasingly pervasive mobile devices, especially the new generation of smart phones that are becoming more and more like the full-fledged computer, mobile device security cannot be taken for granted anymore. Consequently, the evolution of computer security will repeat itself in the mobile space. The only difference: This time it may be even more complicated than previous network security challenges.

Mobile security is also more challenging than many expect because the concept of network security is changing. Network security today is focused primarily on the transport layer. This approach is inadequate for next-generation all-IP networks, which require a complex, multilayer security matrix that can also protect the control/signaling layers and the service/application layer. In addition, security for all layers must include integrated policy enforcement and secure-access technology using multi-protocol authentication, authorization, and accounting (AAA) services. Failure to implement multilayer security exposes providers to a loss of network integrity, revenue, and potentially corporate reputation.

Mobile network security requires protection from the vast and constantly changing network attacks providers face daily, both externally and internally. External threats are typically widely publicized and include zero-day vulnerabilities, buffer overflows, SQL injections, viruses, worms, and trojans. Internal threats are often overlooked but may well be more common than external threats. Implementing multilayered security helps protect against both external and internal threats.

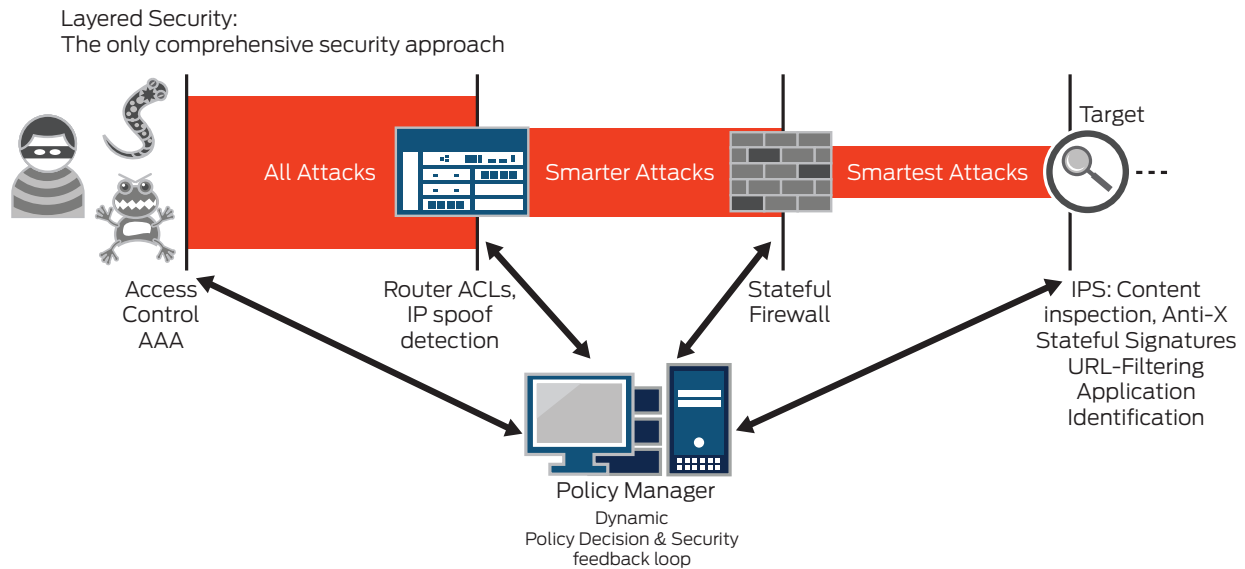


Figure 1: Layered security—the only comprehensive approach

The Juniper Networks Mobile Security Solution

The most comprehensive approach—really the only approach that works—is to protect the entire network with multiple security components applied in layers (see Figure 1).

- At the first layer of defense, Juniper Networks® AAA products provide access control to discourage opportunistic attacks from outsiders. Juniper Networks SSG Series Secure Services Gateways offer high-performance security and modular LAN/WAN connectivity.
- Juniper's core and edge routers prevent IP spoofing by implementing access control lists (ACLs) to drop all inbound traffic with suspicious source IPs (or IP ranges).
- Juniper's firewalls with stateful inspection are the next line of defense in this layered security model. They provide IPsec, VPN, and SSL VPN capabilities along with critical protection against denial of service (DoS), distributed denial of service (DDoS), and other types of attacks.
- Juniper Networks IDP Series Intrusion Detection and Prevention Appliances provide important content inspection and antivirus/anti-spam capabilities. Content inspection is designed to stop L7 attacks and is the only way to detect what is really running on L7 or signaling application layers of the network.

Unified Access Control and AAA

Juniper Networks Unified Access Control and Juniper Networks SBR Series Steel-Belted Radius Servers provide secure network access control with powerful user authentication and authorization. SBR Series AAA validates the identity of the user and Unified Access Control combines that identity information with device health and location data to deliver granular access control. Only authorized users can access the network and applications from devices that adhere to your network security policies.

Routers

Juniper Networks T Series Core Routers, and Juniper Networks E Series Broadband Services Routers, M Series Multiservice Edge Routers, and MX Series 3D Universal Edge Routers provide packet handling layer security at a number of levels, as shown in Figure 2.

- **Data plane:** Anti-spoofing, IP fragment filtering, and ACLs drop all inbound traffic with a suspicious source IP address or IP address ranges
- **Network protocols:** BGP Session Security, Secure FTP, and SSH
- **Law enforcement:** Communications Assistance for Law Enforcement Act (CALEA) or other government approved, lawful intercept, and VLAN mirroring, firewall, and IPS

A new unique feature of Juniper's router-based security is session flow protection based on border gateway functionality (BGF). Juniper's BGF can filter and block unwanted flows, rate limit flows based on bandwidth, prioritize flows across the core network, and enable Network Address Translation (NAT)-traversal without tromboning.

ROUTER-BASED SECURITY

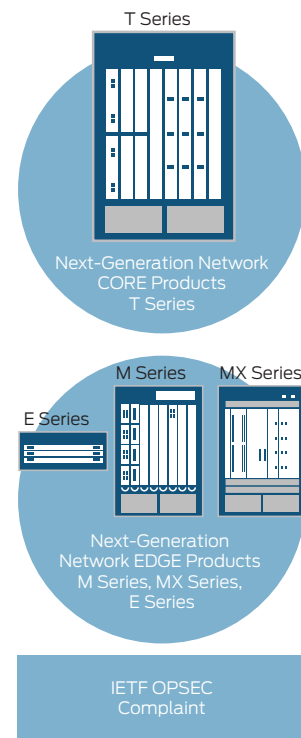
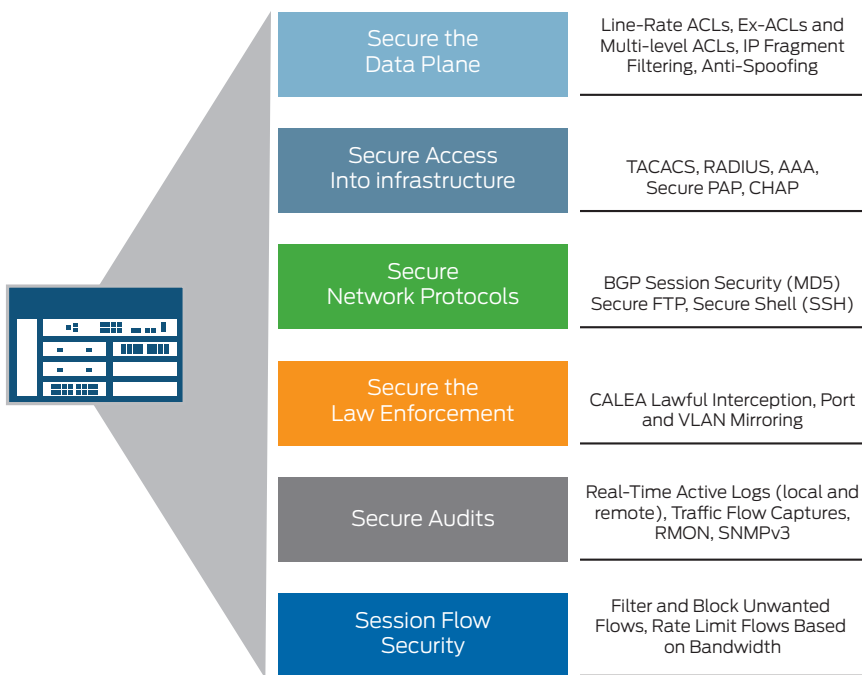


Figure 2: Router-based security

Firewall Security

Effective mobile security requires both stateless and stateful firewalls. Stateless firewalls determine whether a packet is permitted into the network by analyzing basic information in the packet headers. Stateful inspection firewalls monitor and control the flow of traffic between networks by tracking the state of sessions and dropping packets that are not part of authorized sessions. Firewalls must be able to scale to handle the volume of traffic flow so that the network's performance is not negatively impacted. Additional security includes VPN using IPsec for authenticating and encrypting IP packets, SSL, and Transport Layer Security (TLS).

Application/Service Layer

Juniper's security solutions detect unusual or suspicious behavior on the application layer using customizable signatures based on stateful protocol inspection, attack patterns, and behavioral learning. This capability is vital for service providers who want to protect their networks against the most malicious attacks. Juniper protects more than 60 protocols against penetration and proliferation of worms and other malware including trojans, spyware, keyloggers, and adware.

JUNIPER NETWORKS SUPPORT FOR SCTP

Stream Control Transmission Protocol (SCTP) is a reliable message-oriented (not byte-stream) multi-streaming transport protocol operating over IP. SCTP was intended initially for Internet telephony, but now has developed into a robust, general purpose transport protocol. Among other things, SCTP offers network level fault tolerance through its support of multihoming at either or both ends of an association, and it offers congestion avoidance behavior and resistance to flooding and masquerade attacks.

SCTP is essentially the foundation for the transport of telephony SS7 (Signaling System 7) protocols over IP. This trend of conveying SS7 signaling over SCTP/IP is fully backed by leading standard organizations and is expanding to other applications/signaling over SCTP (for example, Media Gateway Control Protocol (MEGACO)). Juniper Networks ISG Series Integrated Security Gateways feature the industry's first SCTP firewall solution. The Juniper solution:

- Checks SCTP syntax
- Performs stateful inspection to deny malicious SCTP messages (hijack and redirection, for example)
- Limits the SCTP traffic rate to counter bombing attacks
- Allows users to configure screening certain types of SCTP messages to reconcile compatibility problems
- Performs address translation to hide the topology
- Logs SCTP traffic for recording irregular activities
- Blocks dynamic capability of removing/adding IPs to already existing SCTP association
- Includes NAT/Naming Authority Pointer (NAPTR) functionality that is necessary to replace "private" IP addresses in the IP and the SCTP header with public IP addresses/port numbers

Security in the data center is extremely important, as it is the heart of information processing for most organizations. It is imperative that data center services are always available and that they are secure. The ideal goal in the data center is to group together services that are alike and trusted to talk to one another without a security barrier. An example of this approach is the tiered application architecture consisting of a Web server, application server, and database server. For a typical deployment, all of the similar types of servers for a specific application deployment are grouped in the same network segment.

The first step in securing server access is the deployment of a stateful firewall. This will limit connectivity between servers to the required minimum number of services, ensuring that unwanted access to servers will not occur. This mitigates the possibility of a host making unauthorized connections to a server, but scaling this type of security configuration can be difficult.

Limiting the way servers are connected to one other is a great start in securing connectivity between applications. The next step is to secure what is inside these connections by employing intrusion prevention system (IPS) techniques. IPS allows a device to look inside network connections to determine if they contain a malicious attack. This is extremely important in locations such as the data center, where an attack can lead to anything from a service outage to the actual loss of data. Because of these risks, deploying IPS is of critical importance.

The two limitations of IPS are scale and deployment location. First, it is difficult to scale an IPS deployment to the needs of a data center using conventional IPS appliances. This is not always a matter of IPS device capacity; it can also be driven by the ability to deploy the IPS device. For example, it may not be practical to deploy IPS units in front of all of the various application sets. The IPS also may not scale to large enough performance numbers to deploy it at the data center core.

To add to this challenge, a typical IPS device can only process a specific amount of traffic. So when an IPS is deployed, it is not possible to specify which traffic it chooses to process or not, and the IPS device is limited by the same performance scaling challenges as mentioned in the previous section. The ideal answer would be deploying an IPS device that could selectively process traffic to reduce the overall throughput necessary to do the job.

Juniper Networks SRX5600 and SRX5800 Services Gateways are engineered from the ground up to offer robust data center networking and security services featuring intelligent IPS technology. Powered by the proven Juniper Networks Junos® operating system and dynamic services architecture, the SRX5000 line also provides unrivaled performance and scalability to ensure uninterrupted network infrastructure expansion and growth without sacrificing security.

IPS Security and Juniper Networks IDP Series

Juniper Networks IDP Series Intrusion Detection and Prevention Appliances lend additional support to the role of firewalls by monitoring and analyzing network traffic for signs of attacks at the application and service layer. The IDP Series can drop traffic that is deemed to be from a malicious user. The IDP Series is designed to detect the presence of attacks within permitted traffic flow to the network by using stateful signatures that scan for attacks based on known patterns. These signatures must be easily customizable in order to meet various provider requirements and specific concerns. In today's environment of constantly evolving threats, mobile providers require solutions that can protect against both unknown and known patterns. Many of the most significant threats involve zero-day attacks, or unknown pattern attacks that leverage vulnerabilities for which there is no signature or software patch.

IDP Series not only prevents networks against attacks, it provides information on rogue servers, as well as types and versions of applications and operating systems that may have unknowingly been added to the network. Application signatures, available on the IDP Series, go a step further and enable accurate intrusion detection of specific applications such as peer-to-peer or instant messaging. Armed with the knowledge of specific applications running in the network, administrators can more easily enforce security policies and maintain compliance with corporate application use policy. IPS devices also provide Differentiated Services (DiffServ) markings to allow the routers to enforce bandwidth limitations on nonessential applications. Not only can administrators control the access of specific applications,

they can ensure that business-critical applications receive a predictable quality of service (QoS).

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 ISG Series with IDP and the SRX5000 line can be deployed for application-level protection. The ISG Series and SRX Series tightly integrate the same software found on the IDP Series 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 the SRX5000 line perform 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 the Deep Inspection firewall to block application-level attacks. 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. Deployed in perimeter locations such as the branch office, a Deep Inspection firewall can block application-level attacks

before they infect the network and inflict any damage.

Juniper offers a range of products for mobile security, including ISG Series and ISG Series with IDP products. The ISG General Packet Radio Service (GPRS) solutions are GPRS Tunneling Protocol (GTP)-aware and designed for the high-performance security of GPRS (enhanced second-generation) and universal mobile telecommunications system (UMTS) third-generation-enabled mobile networks. In addition to countering sophisticated threats, DoS attacks, and malicious users, Juniper Networks ISG2000 Integrated Security Gateway can limit messages, throttle bandwidth-hungry applications that consume uplink/downlink traffic, and perform Third-Generation Partnership Project (3GPP) R6 IE removal to help retain interoperability in roaming between second- and third-generation networks.

SRX Series Services Gateways

- **Scalable performance:** Dynamic Services Architecture allows the SRX Series to leverage new services with appropriate processing capabilities without sacrificing overall system performance.
- **System and network resiliency:** Carrier-class reliability based on features ranging from redundant hardware and components to Juniper's proven Junos OS.
- **Interface flexibility:** Highly flexible I/O configuration and independent I/O scalability meet the needs of virtually any network environment.
- **Network segmentation:** Security zone, virtual LANs (VLANs), and virtual routers allow administrators to tailor security and networking policies for various internal, external, and demilitarized zone (DMZ) subgroups.
- **Robust routing engine:** Carrier-class routing engine provides physical and logical separation of data and control planes to allow deployment of consolidated routing and security devices, and ensures the security of routing infrastructures.
- **Comprehensive threat protection:** Integrated security features and services include a multi-gigabit firewall, intrusion detection and protection, DoS, NAT, and QoS.

The security in the SRX Series Services Gateways takes advantage of Juniper Networks technologies, leveraging the firewall capabilities in the ScreenOS® software and the IPS technology of the IDP Series. This is integrated into Junos OS running on service processing cards (SPCs). The firewall capabilities and policy creation are similar to the configuration on ScreenOS; policies are created between zones and then the specific hosts and applications are specified. This creates a policy that the administrator can configure to permit, deny, or reject the traffic.

When a traditional stateful firewall is not enough, it is also possible to inspect the traffic as it goes through the firewall by flagging a security policy for IPS inspection. Once the session is established, the IDP Series engine inspects the traffic and the IDP Series policy is consulted to check against the traffic. The IDP Series matches against the familiar source IP, destination IP, and application, and it also checks against a set of attacks. If the traffic matches one of these attacks, the attack is stopped.

SRX Series Services Gateways leverage over 10 years of experience from all of Juniper's various products. In particular, the SRX Series has been designed using a similar architecture as that employed in the MX Series 3D Universal Edge Routers. The difference between the MX Series and the SRX Series is that the SRX Series needs to be able to implement secure traffic services. To do so, Juniper Networks has created the SPC for the SRX Series—a powerful, high-speed, high-density computing card that is modular so that several of them can be added into a chassis. Adding additional cards automatically allows for scalable performance.

The SRX Series has true separation between control and forwarding planes. The control plane allows all of the management and dynamic routing interaction to occur independent of the data plane processing. The data plane is a high-performance switching backplane that allows for line rate transversal of traffic between SPCs and interface cards. This ensures that the chassis can push traffic as fast as it can be processed by the SPCs. The interface cards also are similar to the interfaces used on the MX Series routers. The cards offer line rate performance, avoiding road blocks for getting traffic in and out of the interfaces. The interface capability of the SRX Series is extremely high density for a firewall. It can support up to 10 slots of interfaces mixing and matching 4-port 10-Gigabit Ethernet interface cards and 40-port 1-Gigabit Ethernet interfaces. The remaining slots can be used for service processing cards.

To deal with performance scalability, the SRX Series has been designed with expandable hardware architecture. This allows the end user to start small in terms of the number of security processing cards that are used, and then add additional cards to scale the performance over time. Each new SPC that is added increases the performance in a predictable way, allowing the organization to plan for the hardware it needs as it grows.

Each SPC contains two services processing units (SPUs), with each unit acting as a high-density processor. The first SPC uses one of the SPUs as a central point. The central point processes traffic like each of the other SPUs, but it also is the central authority for determining if a session already exists or not. The central point is used as the central authority for whether or not a session is already created. If traffic enters the SRX Series and the session is not created, the central point sends the traffic to the next available SPU based upon its load balancing algorithm. The SPU performs most of the security services on the SRX Series Services Gateways. This is essentially the heavy lifting on the device. All firewalling, intrusion detection and protection, and session state maintenance is done on the SPU.

This type of performance scalability is what is needed in the data center. It allows the SRX Series to be deployed with confidence that it will be able to handle all of the necessary sessions. An additional SPC can be added to increase performance, reducing the need to perform an expensive forklift upgrade of a low-performance device.

Features and Benefits

- Highly effective network security through multilayered approach that includes:
 - Network access control
 - Packet handling layer
 - Firewall
 - Intrusion prevention system
- Flexible deployment options:
 - Standalone firewall, standalone IDP Series, and firewall/IDP technology combination products
 - Security features across Juniper core and edge router families
 - SBR Series products tailored for needs of wireline, Code Division Multiple Access (CDMA), and Global System for Mobile Communications (GSM) service providers
- Broad range of protocol support including:
 - Control and signaling layer security (SIP, H.323, MGCP, SIGTRAN, SOAP)
 - Mobile protocols including GPRS Tunneling Protocol (GTP), Generic Routing Encapsulation (GRE), IP-IP encapsulation, Point-to-Point Protocol (PPP)
 - Stream Control Transmission Protocol (SCTP) for SS7 telephony

Solution Components

Juniper Networks SBR Series

The SBR Series of high-performance RADIUS servers is a core component of mobile service provider networks, providing centralized user authentication and access policy management with the performance and reliability to handle any traffic load.

Juniper Networks SSG Series

The SSG Series of purpose-built security products has been designed to satisfy customer networking and security requirements for mobile networks.

Juniper Networks NetScreen-5200 and NetScreen-5400

NetScreen-5200 and NetScreen-5400 integrated firewall/IPsec VPN appliances are purpose-built, dynamic security appliances with industry-leading flexibility and performance capabilities to protect mobile service provider networks and network data centers.

Juniper Networks ISG1000 and ISG2000

ISG1000 and ISG2000 with IDP provides strong access control, secure communications, and network and application-level security while lowering the total cost of ownership for deploying best-in-class firewall, VPN, and intrusion prevention services.

Juniper Networks SRX Series

Based on Junos OS and dynamic services architecture, the SRX5600 and SRX5800 are designed to meet the network and security requirements for data center hyper-consolidation, rapid managed services deployments, and aggregation of security services.

Juniper Networks IDP Series

IDP Series products provide comprehensive and easy-to-use inline protection that prevents network and application-level attacks before they inflict any damage to the network, minimizing the time and costs associated with maintaining a secure network. Using industry-recognized stateful intrusion detection and prevention techniques, the IDP Series provides zero-day protection against worms, trojans, spyware, keyloggers, and other malware from penetrating the network or spreading from already infected network segments.

Juniper Networks Routers

Juniper's routers provide packet handling layer security to ensure a robust layer of defense against suspicious traffic attempting to enter and traverse service provider networks. These reliable and scalable routing platforms incorporate Junos OS, Juniper's trusted network operating system proven in high-performance networking environments.

Summary: Juniper Networks Provides Multilayered Security for Mobile Networks

Juniper provides an innovative, marketing-leading mobile security solution that service providers can use to mitigate the risks associated with deploying IP-based services. SBR Series Steel-Belted Radius Servers provide vital network access control functionality to intercept hackers trying to gain unauthorized access to service provider mobile networks.

Juniper's firewall and VPN devices have been purpose-built to perform essential security functions that safeguard the network against worms, trojans, viruses, and other malware. Juniper offers standalone firewalls enabling up to 120 Gbps firewall throughput (on the fully equipped SRX5800), standalone IDP Series systems with market-leading performance of 10 Gbps of real-world throughput, and combination firewall and IDP products.

According to a Network World study, Juniper Networks ISG2000 with IDP is the top-rated security appliance, scoring first among all evaluated devices in the categories of management, intrusion prevention, availability, and routing. Juniper's IDP technology, integrated into the ISG2000, operates on a policy- and definition-driven basis to identify and stop network and application-level attacks. Juniper routers can process QoS-sensitive multimedia traffic at very high speed, while enacting powerful packet filters to defeat IP-level attacks. Juniper Networks security devices are scalable, reliable, and backed by years of experience shaping the routing and security architectures of the world's top service provider networks.

Next Steps

To learn more about Juniper's Mobile Security Solution, please visit www.juniper.net or contact your local Juniper Networks sales representative.

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.

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

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.