White Paper

SRX SERIES AS GI/SGI FIREWALL FOR MOBILE NETWORK INFRASTRUCTURE PROTECTION

Table of Contents

List of Figures

Executive Summary

Mobile network operators (MNOs) are faced with two key challenges—keeping the mobile network up and running (ensuring high uptime) and providing subscribers (mobile network users) with a positive customer experience.

By protecting the mobile network infrastructure through comprehensive threat protection, Juniper Networks® SRX Series Services Gateways can enable MNOs to extend a positive customer experience to subscribers.

This document focuses on the Gi/SGi interface of the mobile network infrastructure, which is susceptible to attacks from the Internet or other untrusted external network(s), such as networks of corporate customers, that are connected to the P-GW (for LTE/4G networks) or GGSN (for 3G networks). This document provides a brief overview of four of the most common threat scenarios for the Gi/SGi interface and explains how Juniper Networks SRX Series Services Gateways can help mitigate the described threats in order to preserve the integrity of the systems, applications and data managed by the mobile network operator.

Introduction

Overview of LTE (4G) Mobile Network

The 4G mobile network is an all-IP based network based on the Long Term Evolution (LTE) standard for transmitting traffic. This standard enables significantly faster download speeds than possible with 3G cellular networks, allowing simultaneous use of voice, data and video, such as Internet access gaming and streamlined multimedia services including TV and video streaming.

As the 4G network is an all-IP based network, there are many points within the infrastructure at which IP-based threats can be introduced.

Key Security Considerations

The escalating power of mobile devices, speedier Internet connections and the rising deployment of wireless networks bring a new range of services to mobile device users. However, this enhanced mobility also introduces many security risks.

The Gi/SGi interface is where the GPRS/LTE network connects to the Internet and corporate networks. Because a subscriber's applications can be virtually anything, operators inevitably expose their network at the Gi/SGi to all types of network traffic. Subscribers are then exposed to all of the ills that we have today on the Internet including viruses, worms, trojans, denial-of-service (DoS) attacks, botnets and other malicious network traffic. This paper examines four specific threat scenarios introduced via the Gi/SGi interface.

If these vulnerabilities are not addressed, operators might be forced to reconcile the repercussions of network compromise including loss of customer loyalty and trust, negative publicity and most critically, loss of sensitive data resulting in misuse. Implementing security as part of the mobile network infrastructure is imperative for maintaining a positive subscriber experience, brand reputation, as well as customer loyalty.

Juniper Networks SRX Series Services Gateways—which integrate CGNAT, stateful firewall, IPsec VPN, intrusion prevention system (IPS), application security and QoS—can address common and complex Internet-borne threats, thereby helping mitigate the risks to MNOs from compromise of the Gi/SGi interface.

Top Four Threats to Gi/SGi Interface and How to Mitigate

Although there are quite a few attack types and vectors, and they are unfortunately evolving and multiplying all the time, in this paper we focus on four of the most common threat scenarios that mobile network operators should be aware of regarding the Gi/SGi interface of the network.

Threat # 1: TCP Sweeps

In a TCP sweep-based attack, an attacker can send TCP SYN packets to one or more target mobile devices—possibly a large range of publicly addressable mobile devices on the network. If the devices respond to those packets, the attacker learns that a port in the target devices is open, which makes the port vulnerable to attack. The attacker's motivation is to target the weakest link in the mobile chain, such as radio bandwidth or other vulnerable network elements in the mobile operator's cloud, as well as the devices' batteries. By keeping the radio resources in continuous use by waking up some unsuspecting mobile devices, the attacker effectively clogs up the precious radio spectrum resulting in denial of service (DoS) for legitimate mobile initiated transactions and ends up significantly draining the devices' batteries. In this way, attackers can keep hundreds of subscribers from being able to use their mobile devices. While the point to such attacks might not be immediately obvious, Juniper and its MNO customers have witnessed them firsthand and they seem to originate with notoriety-seeking hackers as well as those with a financial motive for negatively impacting subscriber productivity.

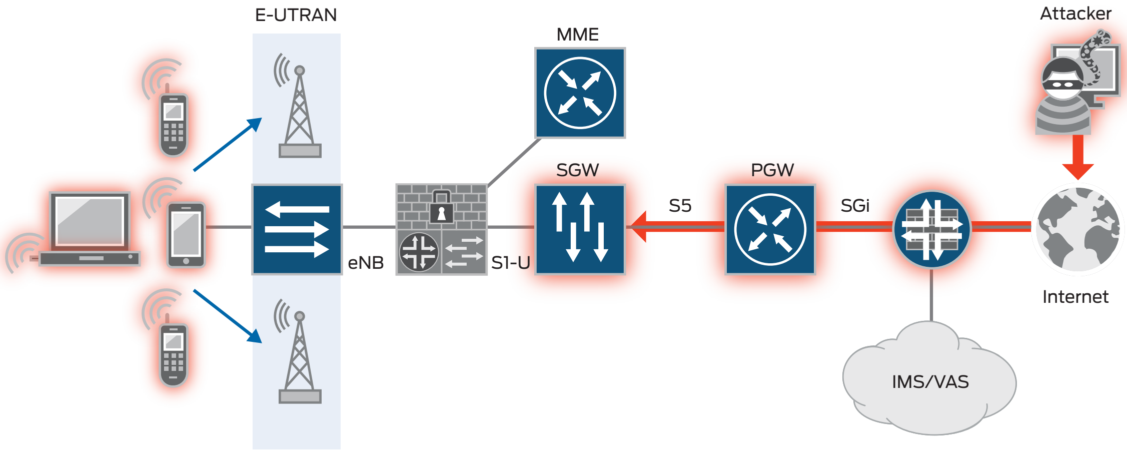


Figure 1. TCP sweeps

Mitigating TCP Sweeps

Juniper Networks SRX Series Services Gateways mitigate risk from TCP sweep attacks through an integrated stateful inspection firewall and IPS engine.

Through its stateful firewall, the SRX Series provides various detection methods and defense mechanisms at the zone and policy levels to combat exploits at all stages of their execution, including screen options at the zone level. A screen is a built-in tunable protection mechanism that performs a variety of security functions, including protection against TCP and UDP sweep attacks, to keep the network safe.

Juniper's built-in IPS adds another layer of security to the firewall by further analyzing the "permitted" traffic, using deep packet inspection (DPI) to identify both suspicious activity as well as active threats. Juniper's library of threat signatures is constantly updated to handle the latest security vulnerabilities. The key purpose of both the firewall and IPS on the Gi/SGi network is to prevent attacks from being launched against the mobile network from hosts out on the Internet. At a high level, IPS works by scrutinizing all of the bits contained within packets to search for both known and unknown attacks. The SRX Series can protect against TCP sweep attacks, whereby it responds to the suspicious activity—in this case, excessive TCP request packets from a single remote host—by either resetting the connection or reprogramming the firewall to block network traffic from the suspected malicious source. As part of the integrated IPS engine within the SRX Series, there is a feature called IP Action where the IPS engine can block any future attacks coming from the malicious source. In this case, it informs the firewall to block future packets/sessions from the malicious source for a finite or infinite amount of time.

Threat # 2: Direct Attacks on Mobile Infrastructure

The mobile infrastructure is subject to certain threats including attacks on the Gi/SGi firewall, IPS or both and bandwidth saturation.

Attack on Firewall and IPS Devices

Firewall and IPS devices are stateful inline devices, by virtue of which they are innately vulnerable to DDoS threats that can overwhelm the state capacity of these systems. Therefore, as devices sitting at the Gi/SGi interface of a mobile network, subject to massive mobile traffic, they must be protected.

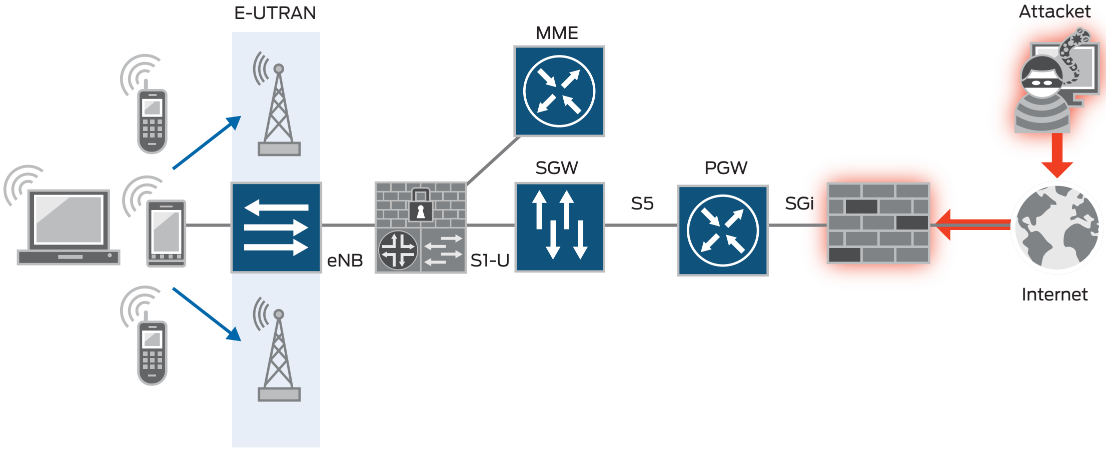


Figure 2. Attack on firewall

Gi/SGi Bandwidth Saturation

Gi/SGi bandwidth is one of the weakest links in the mobile packet edge. By entering through the Internet over the Gi/SGi interface, an attacker can flood the mobile network with excessive network traffic, thereby prohibiting legitimate traffic to pass. This can cause all of the subscribers who are trying to access the Internet on mobile devices to lose network access for some time. In addition, this can completely disable the firewall.

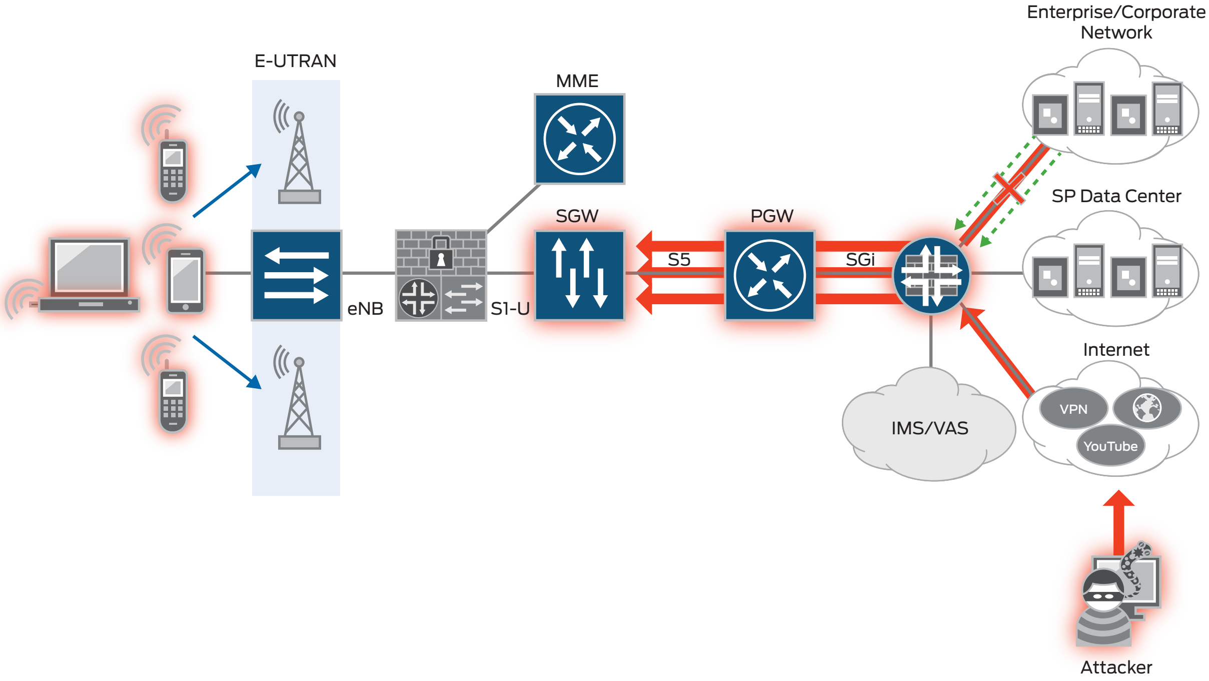


Figure 3. Gi/SGi bandwidth saturation

Mitigating Direct Attacks on Mobile Infrastructure

Protecting Firewall Itself from Attack

Juniper provides best practices for how to protect the SRX Series as the Gi/SGi firewall itself from an attack. The SRX Series Services Gateways, based on Juniper Networks Junos® operating system, are designed in such a way as to allow administrators to harden the control plane from any potential attacks and to ensure availability through configuration of filters and rate limiting of the traffic that reaches the route engine. Additionally, Juniper Networks SRX Series Services Gateways offer screens features that aid in mitigating such attacks to help ensure high-performance traffic flows for a positive customer experience.

Protecting Against Gi/SGi Bandwidth Saturation

To protect against Gi/SGi bandwidth saturation threats, the SRX Series utilizes bandwidth policing. It can shape traffic according to traffic class on all inbound traffic to the Gi/SGi interface as a means to prevent DoS attacks. By ensuring that each class of traffic is limited in bandwidth, the SRX Series ensures that each traffic type always has the necessary resources, which, in turn, guarantees a minimal level of quality of service (QoS) at all times—and also prevents service abuse and fraud.

Furthermore, the security administrator can opt to prioritize IPsec traffic meant for corporate networks over that of other traffic. This ensures that attacks to the Internet cannot disrupt corporate intranet services. Administrators can also use the multiple interfaces of the SRX Series to assign traffic of a particular class to a dedicated interface.

Threat # 3: Botnet Attacks

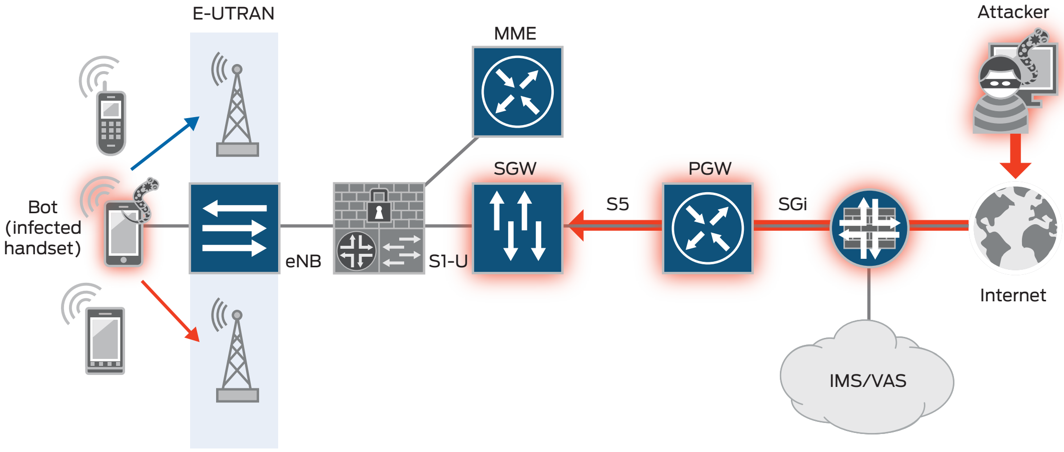
Botnet attacks, which traditionally targeted PCs, are increasingly targeting mobile devices as the latter are becoming more popular and more connected, and the complexity and the number of vulnerabilities in these platforms is increasing.

An attacker might launch a mobile device botnet by taking over full control of multiple devices' data connections. The attacker could do so by fingerprinting each of the devices and injecting exploit code customized to these devices by exploiting a known vulnerability in the mobile network operator's network.

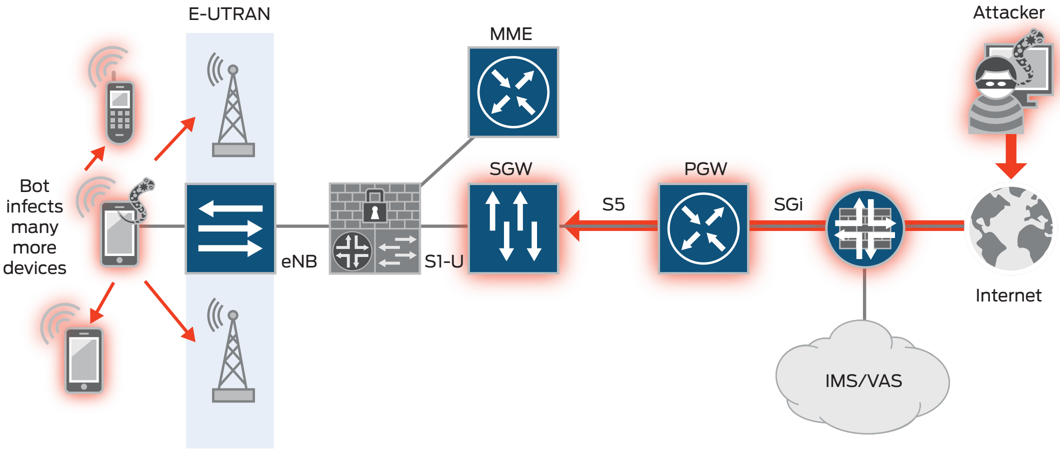
Mobile device botnets can then subsequently be used for launching distributed denial-of-service (DDoS) attacks on the mobile network itself, distressing many customers who cannot connect to the network. Alternatively, a spammer could use the botnet to distribute SMS messages from the compromised mobile devices. A botnet could either be fed a list of phone numbers or just randomly try to send messages to every possible phone number in an area code. In the absence of a firewall or spam-blocking software for SMS messages, mobile device SMS spam botnets could be potentially very profitable to spammers. SMS spam messages could also be used to further spread the botnet through Web links or as part of an attack on the mobile network itself. Furthermore, a botnet could send a lot of bogus content to mobile base station towers in a specific region and subsequently degrade the level of service to these towers.

One example of an Android-specific trojan with botnet-type attributes is Geinimi, a trojan that originated in China in late 2010. Geinimi can compromise a significant amount of data from a user's Android mobile device, sending the data to remote servers controlled by a cyber criminal. Once installed on the device, it could allow the remote server's owner to control the mobile device.

Step 1: Attacker launches malware against a target mobile device on the network via the Gi/SGi interface.



Step 2: Infected mobile device ("bot") infects other devices on the network.



Step 3: Bots collectively launch DoS attack on mobile network, preventing other users from connecting to it.

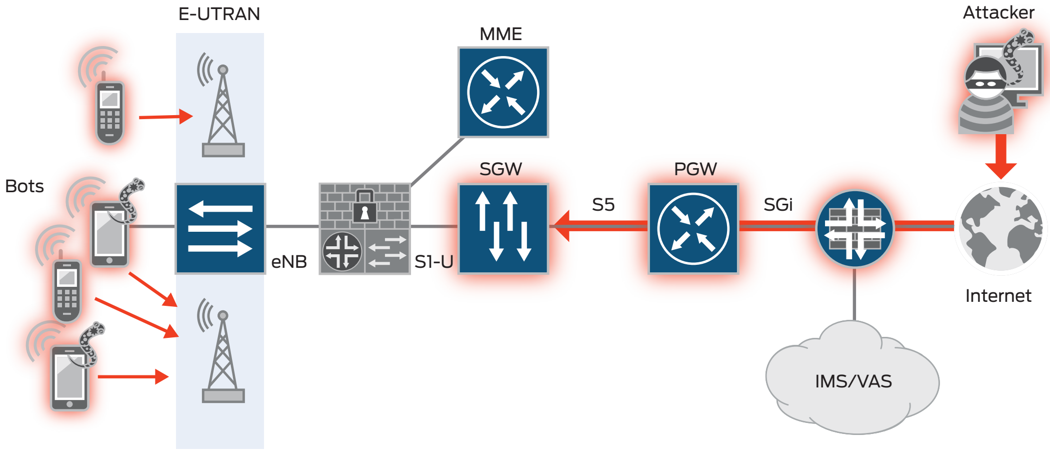


Figure 4. Botnet attack

Mitigating Botnet Attacks

Juniper Networks SRX Series Services Gateways protect against botnet attacks through AppDoS.

The AppDoS service employs multi-stage detection methods used to identify and mitigate targeted attacks from disrupting critical applications and services, and to identify attacking botnet traffic against legitimate client traffic to prevent DDoS attacks that target applications.

In particular, the AppDoS service allows the SRX Series Services Gateways to search for attack patterns. AppDoS searches for DoS and DDoS patterns against a server, the application context (such as the URL) and connection rates from individual clients. Combining and triangulating the information from these three items can stop advanced botnet attacks.

Threat # 4: IPv6 DDoS Attacks

The increasing sophistication of mobile devices and the applications that run on them is driving mobile network operators toward public addressing solutions, including IPv6 deployment, to improve scalability and to minimize operating expenses. With the inevitable shift from IPv4 to IPv6, which intermittently requires mobile networks to support both address schemes, large amounts of undesirable state are inserted into the mobile network in the form of 6to4 gateways and carrier-grade NAT (CGN) devices. The large amounts of state present in these devices make them highly vulnerable to both deliberate and inadvertent DDoS attacks.

The first IPv6-related DDoS attack probably took place in 2004.[1] The target was the 6to4 gateway of a major EMEA-based network operator. This gateway was being attacked from the IPv4 Internet, and just a relatively small amount of traffic brought it down—disrupting service for all legitimate users of the gateway. As more stateful 6to4 and CGN infrastructure devices are installed in the mobile network, the risk of attacks increases. According to a survey conducted in 2011, certain service providers revealed that they experienced IPv6 DDoS attacks "in the wild" on a production network. This represented a significant milestone in the "war" between attackers and defenders, and it serves as a reminder to mobile operators to ensure that they have sufficient visibility and mitigation capabilities to protect IPv6-enabled properties.[2]

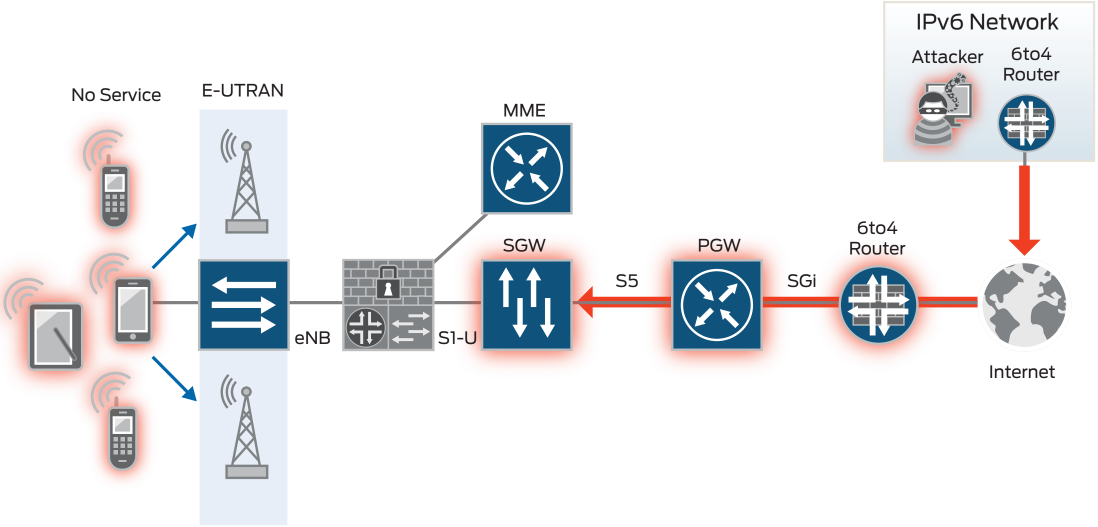


Figure 5. IPv6 DDoS attack

Mitigating IPv6 DDoS Attacks

Juniper Networks SRX Series Services Gateways can mitigate IPv6 DDoS attacks through AppDDoS, a solution that is integrated into the IPS engine to profile the servers that AppDDoS is protecting. AppDDoS can also identify hosts that cross the application thresholds to enforce an action on them. It essentially takes place in the protocol decoding phase of IPS processing, by matching on contexts within the application and then enforcing rate limiting on the application contexts.

Conclusion

If mobile network operators implement firewall, DoS attack prevention, IPS, application protection and QoS as integrated components for uninterrupted connectivity—and implement threat detection, alerting and monitoring as a single holistic solution for protecting the Gi/SGi interface—the operators can reduce risk to their networks and provide a positive customer experience.

[1] "Worldwide Infrastructure Security Report 2010," Arbor Networks

[2] "Worldwide Infrastructure Security Report 2011," Arbor Networks

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**.

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.

2000468-001-EN Apr 2012

♻ Printed on recycled paper