

# JUNIPER NETWORKS FMC SECURITY SOLUTION

## Integrated Security for Layered Protection

### Challenge

As service providers converge their fixed and mobile infrastructures, they face a range of new security threats, both internal and external. Their existing security solutions—focused primarily on the transport layer—are not up to the task.

### Solution

Juniper Networks offers multilayered security solutions including access control, router-based security, firewalls and Juniper Networks IDP Series Intrusion Detection and Prevention Appliances. Key products in the Juniper portfolio include Juniper Networks SBR Service Provider Series Steel-Belted Radius Servers, SSG Series Secure Services Gateways, NetScreen 5000 Series Security Systems, ISG1000 and ISG2000 Integrated Security Gateways, as well as Juniper Networks T Series Core Routers, E Series Broadband Services Routers, M Series Multiservice Edge Routers, and MX Series 3D Universal Edge Routers.

### Benefits

The Juniper FMC security portfolio allows service providers to build effective and scalable multilayer network security systems customized to their needs. Juniper security solutions support a wide range of network protocols and architectures.

Fixed Mobile Convergence (FMC), standardized by the European Telecommunications Standards Institute (ETSI) in their TISPAN architecture, promises ubiquitous access to voice, video and data services on any mobile or wireline device. Although FMC enables providers to offer competitive, new revenue-generating services to their customers, it can also introduce network security concerns. As stated in a February 2007 report by McAfee, the number of mobile security incidents reported increased by 500 percent from 2005 to 2006. Also, the same report stated that 83 percent of mobile providers were affected by mobile infections. Half of the service providers surveyed admitted seeing attacks during the preceding three months, an occurrence previously considered highly unusual for mobile providers. This situation can only get worse as networks converge. Service providers must focus carefully on security to ensure the success of their FMC initiatives.

### The Challenge

FMC security is 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 FMC, which requires a complex, multilayer security matrix that can also protect the control and 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.

Securing an FMC network requires protection from the vast and constantly changing network attacks that providers face daily from both inside and outside of the network. 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 to protect against both external and internal threats.

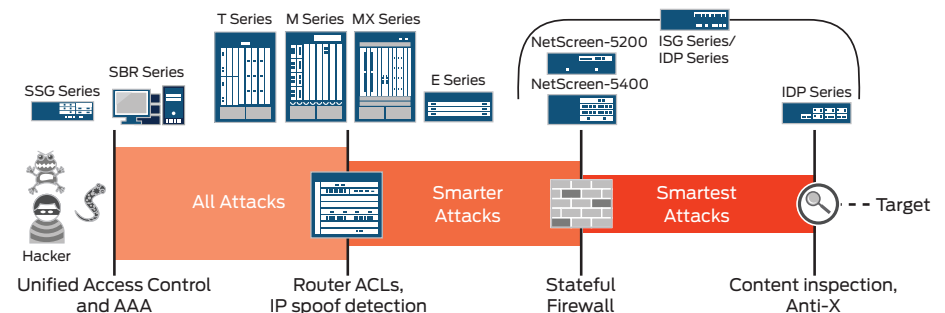


Figure 1: Juniper FMC Security Solution Components

## The Juniper Networks FMC 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 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 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 the L7 or the signaling application layers.

### Unified Access Control and AAA

Juniper Networks Unified Access Control (UAC) and SBR Service Provider Series Steel-Belted Radius Servers provide a secure network access control with powerful user authentication and authorization.

SBR Service Provider Series AAA validates the identity of the user and the UAC solution combines that identity information with device health and location data to deliver granular access control. Only authorized users are accessing the network and applications from devices that adhere to your network security policies.

## Routers

Juniper Networks T Series Core Routers, E Series Broadband Services Routers, M Series Multiservice Edge Routers, and

MX Series Ethernet Services 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 to 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: CALEA (or other government approved), Lawful Intercept (LI) and VLAN mirroring

### Firewall and Intrusion Prevention System (IPS)

Juniper offers a range of products for FMC security, including the NetScreen Series and the ISG Series and IDP Series products.

The ISG Series General Packet Radio Service (GPRS) solutions are GPRS Tunneling Protocol (GTP)-aware and designed for the high-performance security of GPRS (2.5G) and Universal Mobile Telecommunications System (UMTS) (3G)-enabled mobile networks. In addition to countering sophisticated threats, DoS attacks, and malicious users, the ISG2000 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-generation (2G) and third-generation (3G) networks.

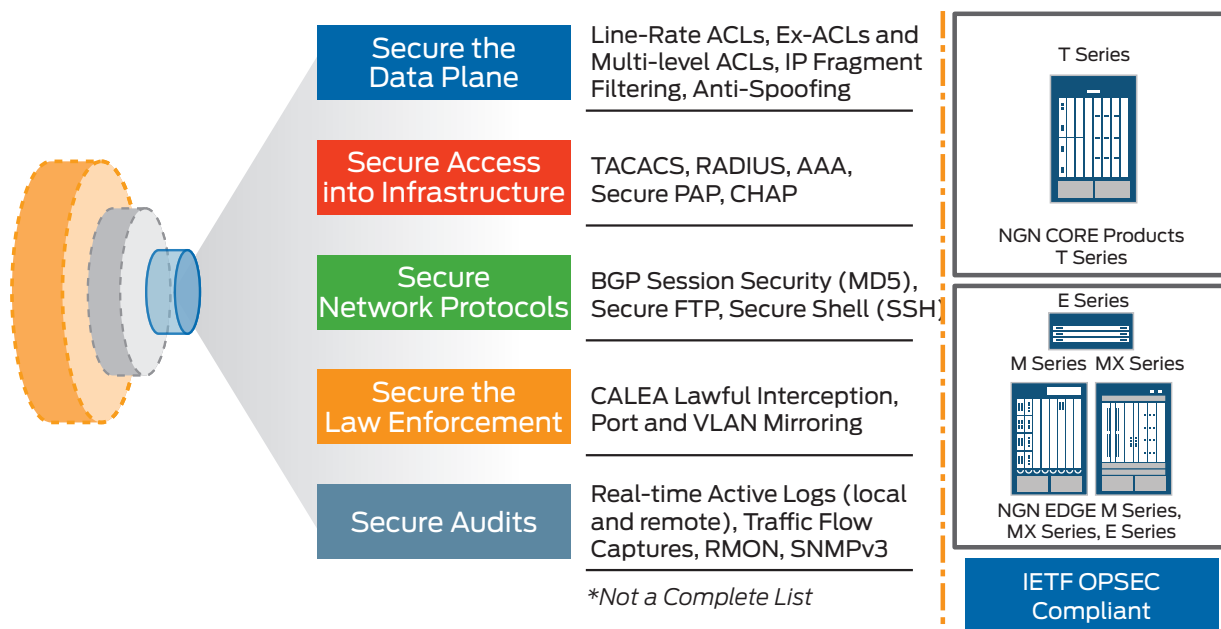


Figure 2: Packet Handling Layer Security Model

## Firewall Security

Effective FMC 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.

The IDP Series lends 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. These systems are 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 need to be easily customizable in order to fit into different 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.

## Features and Benefits

- Highly effective network security through multilayered approach that includes:
  - Network access control
  - Packet handling layer
  - Firewall
  - Intrusion detection and prevention
- Flexible deployment options:
  - Standalone firewall, standalone IPS, and firewall/IPS combination products
  - Security features across Juniper core and edge router families
  - SBR Service Provider 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

### JUNIPER 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 supporting of multi-homing at either or both ends of an association, and 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, Diameter and the Media Gateway Control Protocol, MEGACO).

ISG Series gateways product line features the industry's first SCTP firewall solution. The Juniper solution checks the SCTP syntax and also performs a full SCTP stateful inspection.

## Solution Components

### Juniper Networks SBR Service Provider Series Steel-Belted Radius Servers

The SBR Service Provider Series of high-performance RADIUS servers is a core component of FMC 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 Secure Services Gateways

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

### Juniper Networks NetScreen 5000 Series Security Systems

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 FMC service provider networks and network data centers.

### Juniper Networks ISG Series Integrated Security Gateways

ISG1000 and ISG2000 with IDP Series appliances provide 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 Routers

Juniper routers provide packet handling layer security to ensure a robust layer of defense against suspicious traffic attempting to enter and traverse FMC networks. These reliable and scalable routing platforms incorporate Juniper Networks Junos® operating system, Juniper's trusted network operating system that has proved itself in high-performance networking environments.

## Summary—Juniper Provides Multilayered Security for FMC Networks

Juniper Networks provides innovative and market-leading security products that service providers can use to mitigate the risks associated with deploying IP-based services. The SBR Service Provider Series provides vital network access control functionality to intercept hackers trying to gain unauthorized access to service provider FMC networks.

Juniper 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, standalone IDP Series systems, and combination firewall and IDP Series products. According to a recent Network World study, Juniper Networks ISG2000 Integrated Security Gateway with IPS is the top-rated security appliance, scoring first among all evaluated devices in the categories of management; intrusion prevention, availability and routing. Juniper's IPS 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 quality of service (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 40 largest service provider networks.

## Next Steps

To learn more about Juniper FMC security solutions, please visit [www.juniper.net](http://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](http://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](http://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.