SECURITY FOR THE NEW MOBILE NETWORK

Layered End-to-End Security Solutions for Mobile Network Operators

Challenge

Unprecedented developments in the mobile device marketplace represent new opportunities—and challenges—for MNOs. As services and content accessible on smart mobile devices become richer, digital data traffic will continue to increase, placing greater strain on network infrastructures constrained by limited bandwidth.

Solution

Juniper Networks end-to-end mobile network security solutions provide protection across networks, devices, and applications. Agile, layered defenses enable mobile operators to consolidate multiple security functions and adapt to evolving threats while monetizing new mobile services.

Benefits

- Comprehensive solutions provide multiple layers of protection for better security and defense in depth.
- Tight integration allows for faster response to threats.
- Scalability drives low TCO even as network infrastructure grows.
- Network-wide automation enables end-to-end security policy enforcement.

Juniper Networks® provides a wide range of security solutions to enable mobile network operators (MNOs) to monetize new services and protect their networks from end to end. Utilizing time-tested standalone networking and/or security products all the way to sophisticated solutions with multiple services and components dynamically interacting in a highly coordinated manner to protect networks from advanced persistent threats, Juniper's customers include 80% of the world's top mobile operators[1].

The Challenge

Smart mobile devices are an indispensable part of consumer and enterprise users' digital lifestyles. As users' dependency on smart mobile devices increases, the volume of non-voice related services that users consume is also expected to increase. By 2015, more than 50% of mobile service revenue is expected to come from non-voice services.[2]

As services and content accessible on smart mobile devices become richer, digital data traffic will continue to increase, placing greater strain on network infrastructures designed originally for voice services and constrained by limited bandwidth. Maintaining network uptime and availability will be a high priority for MNOs seeking to keep customer satisfaction rates high and churn rates low.

The deployment and management of mobile service and content offerings will be further complicated by a myriad of new platforms and devices flooding the market. Each new device on the network represents not only associated deployment, support, and management costs, but increased security risk as well. Each new mobile device increases signaling and data traffic load, exacerbates connection rate issues, and increases the number of potential attack surfaces within the network. Mitigating future advanced, persistent threats, as well as existing issues, requires a comprehensive strategy and a scalable solution.

Applications used on mobile device platforms add a further layer of complexity. The current open-market application development environment and laissez faire purchase model enable vast numbers of developers, unskilled in security and with little understanding of mobile network operation, to create a steady stream of new applications for a variety of mobile devices. The sheer volume of applications available—as well as the variety of locations from which applications can be procured and downloaded—makes rigorous testing of each combination of applications on each mobile device nearly impossible. As more and more applications enter the ecosystem, it is inevitable that some will be inefficient, even harmful, increasing backhaul traffic and generating significant amounts of signaling events that can have unintended, adverse consequences on mobile device battery life, negatively affecting subscriber satisfaction ratings. Rogue applications can prove problematic as they can create vulnerabilities within the network or, worse, be a "wolf in sheep's clothing"—malware exploiting vulnerabilities in the guise of a legitimate application.

The widespread adoption of smart mobile devices as a part of everyday life represents many opportunities for MNOs. But the challenges associated with providing services, securing devices and the information and data on those devices, securing transmissions to and from devices, and protecting the network while generating revenue must also be taken into account.

[1] Wikipedia – List of mobile network operators by subscriber count, as of March 16, 2012 (stat in this paper based on top 20)
[2] The Hindu Business Line newspaper e-edition, July 28, 2011

Juniper Networks Mobile Network Security Solutions

Juniper Networks mobile network security solutions address the needs of MNOs with comprehensive sets of products and services designed to protect the device, network, and applications. Addressing the needs of MNOs, these end-to-end solutions secure the network and protect devices from evolving threats, while enabling cost control measures and revenue generation opportunities. In addition, Juniper mobile network security solutions' components suit the unique needs of the MNO, with carrier-class features for high availability and long, trouble-free service life.

Features and Benefits

Table 1. Mobile Network Security Solutions' Features and Benefits

Features	Benefit
Layered security approach	Consolidated and tightly integrated security services simplify deployments across Juniper products in optimum locations throughout the network.
Coordinated threat control	Integration of inputs from multiple sensors enables security policy to adapt with greater agility to a dynamically changing environment, to determine and then enforce appropriate network and security policies network-wide, and to be applied in a coordinated manner to the components of an end-to-end solution.
Scalability	Chassis-based platforms are easily scaled to accommodate growing network performance and traffic needs and allow concurrent operation of multiple services without a performance penalty.
Single OS, single release train	A single OS can significantly reduce TCO, allowing security services and functionality to operate consistently across Juniper routers, switches, and security devices in the network, and reducing operational and maintenance effort.
Revenue-focused	Easy to use and deploy solutions which require little user interaction and deliver "Day Zero" protection for users, mobile devices, and sensitive data.
Security infrastructure automation	Policy abstraction and operator workflows enable consistent network-wide security policy to be deployed rapidly and accurately.
Rapid service scaling	Workflows and best practices help operators quickly and easily deploy thousands of devices and security services.

Solution Components

SRX Series Services Gateways

Juniper Networks SRX Series Services Gateways are deployed extensively in MNOs around the world because they are the only security solutions available today with the proven ability to deliver the massive scale, throughput, and performance operators need to handle the traffic generated by the latest generation of smart mobile devices. At the SGi/Gi interface between the mobile packet core and the Internet, Juniper Networks SRX5800 Services Gateway can accommodate up to 20 million sessions. With protection screens and filters running in hardware, and separation between user and control plane, SRX Series Services Gateways are able to protect the largest networks against denial-of-service and distributed denial-of-service (DoS/DDoS) attacks, malicious traffic, reconnaissance sweeps, and rogue applications that saturate signaling networks, drain mobile device batteries, and can deliver malicious payloads. SRX Series Services Gateways are purpose-built, chassis-based systems designed with the carrier-class availability and features operators require for years of trouble-free service life. Supporting Carrier-Grade NAT (CGNAT), large scale VPN, GPRS tunneling protocol (GTP), and Stream Control Transmission Protocol (SCTP), the SRX Series is equally at home on the S8/Gp and S5/Gn interfaces, protecting value-added services, and other critical elements such as interfaces to the GPRS Roaming Exchange (GRX) and Signaling System 7 (SS7) clouds for SIGTRAN.

MX Series 3D Universal Edge Routers

Juniper Networks MX Series 3D Universal Edge Routers are deployed in backbone networks and on SGi/Gi networks of most of the major mobile operators in the world. Powered by Juniper Networks Junos® operating system—the same OS that runs on the SRX Series as well as other lines of Juniper switching, routing, and security products—they provide a consistent, carrier-class operating environment that radically reduces TCO compared to other solutions. The MX Series can also host the Service Delivery Gateway, which consolidates a variety of best-in-class SGi/Gi network services onto a single platform to reduce cost, increase network resiliency, and increase performance. The MX Series is also the foundation for Juniper Networks MobileNext™, the world's first open, secure, and scalable mobile packet core. The solution comprises:

Juniper Networks MobileNext Broadband Gateway: Provides gateway GSN (GGSN) and public data network (PDN)/serving gateway functions in one platform, and delivers scale and performance with uncompromised inline IP services, while enabling service creation with Junos OS for operators to innovate profitable data services.

Juniper Networks MobileNext Control Gateway: Provides Serving GPRS Support Node (SGSN) and mobility management entity (MME) functions for 2G/3G and Long Term Evolution (LTE) mobile packet cores, and delivers control plane functions for mobile networks including user authentication and mobility management to redefine performance for the smart mobile device era.

Juniper Networks MobileNext Policy Manager: Integrates with the industry's leading subscriber management systems, offering choice and flexibility in network and content resource management as well as rapid enablement and monetization of new applications.

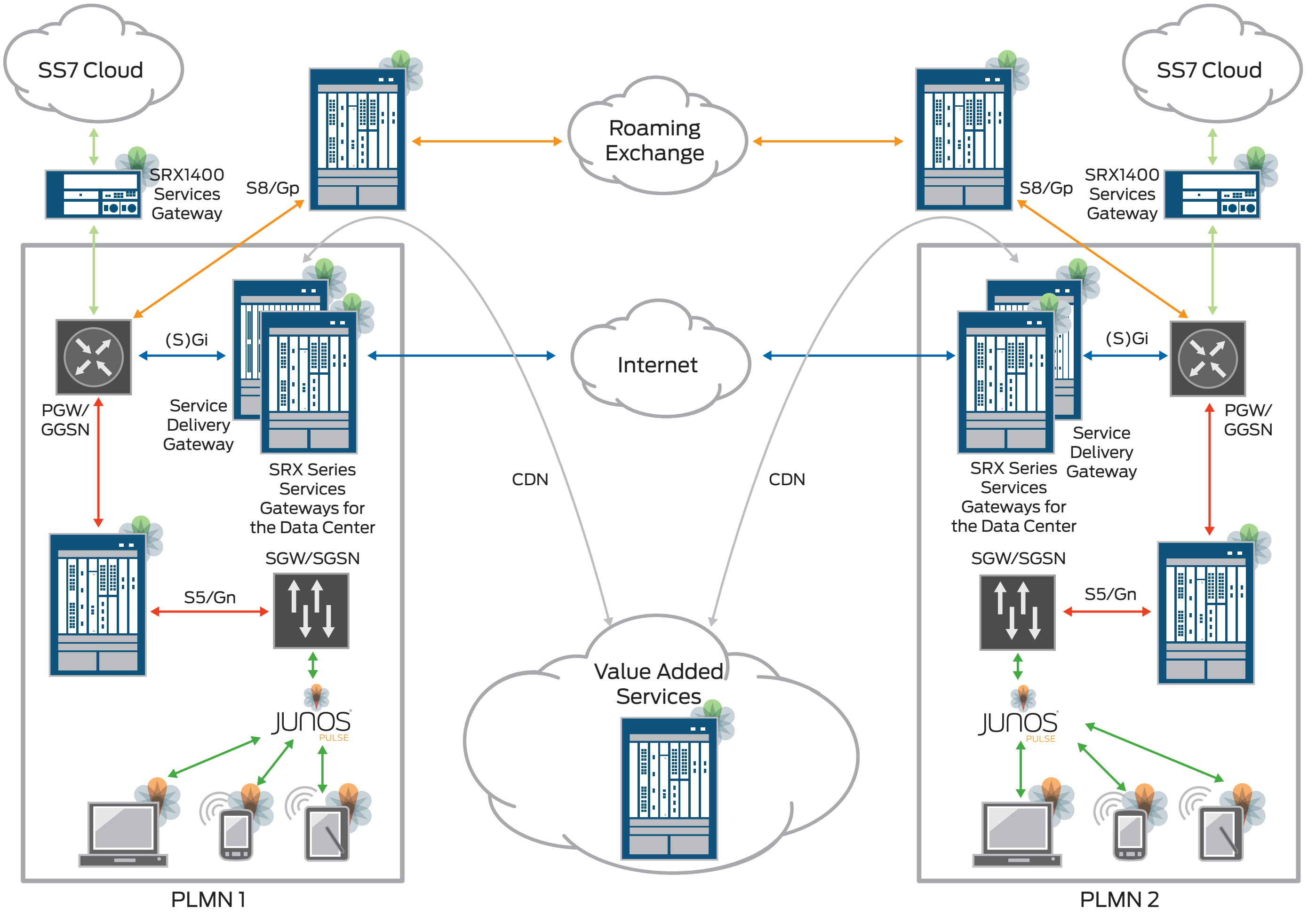

Figure 1: Juniper Networks mobile security solutions

Integrated Security Services

AppSecure

Software applications—particularly video—are generating significant increases in mobile network traffic. They are also becoming the preferred vehicle for delivering malware to subscribers, either by exploiting unpatched vulnerabilities in the application itself or being carried into the network through applications downloaded from the Web. AppSecure and IPS provide necessary visibility into the network, allowing MNOs to manage application types and volume on their networks.

Junos OS Integration

Junos OS is Juniper's unified network operating system, integrating routing, switching, security, and an array of network services. This unique integration between security hardware and software delivers unparalleled performance of security services such as stateful firewall (IPv4, IPv6, GTP, SCTP), IPsec VPN, CGNAT, application-level gateways (ALGs), dynamic routing, quality of service (QoS), stateless firewall (including access control list and DoS/DDoS screens), SSL decryption, and more.

Junos Pulse Mobile Security Suite and Junos Pulse

Juniper Networks Junos® Pulse Mobile Security Suite is a comprehensive mobile security software solution that protects and manages smartphones, tablet devices, and other smart mobile devices running most major mobile operating systems. The Junos Pulse Mobile Security Suite delivers mobile security, protecting identity, personal information, and corporate data for the enterprise and consumer. This complete mobile security and device management solution delivers antivirus, anti-spam, endpoint firewall, loss and theft protection, parental controls, device monitoring, and application control. It enables MNOs to offer tailored, premium mobile security and management services to enterprise customers and consumer subscribers with the benefits of increasing average revenue per user (ARPU), enhancing subscriber retention, providing competitive differentiation, and increasing user satisfaction. Junos Pulse Mobile Security Suite may be deployed as a secure, hosted Software-as-a-Service offering, easing customer and subscriber deployment, enabling fast, seamless scalability, and the ability to deploy—and monetize—new mobile security services quickly and simply.

Juniper Networks Junos Pulse serves as the user interface for Pulse Mobile Security Suite on a smart mobile device. Junos Pulse is also an endpoint software platform which provides dynamic, secure mobile remote access and connectivity (via Juniper's award-winning SSL VPN), network access control (NAC), and security through a simple and elegant user experience. Junos Pulse eases role-based, secure, remote connectivity, and network and application access from smartphones, tablets, and other smart mobile devices, over an array of mobile platforms and operating systems. It does this by leveraging the industry-leading Juniper

Networks MAG Series Junos Pulse Gateways or Juniper Networks SA Series SSL VPN Virtual Appliances. When deployed in concert with Junos Pulse Secure Access Service and either MAG Series gateways (customer premises equipment) or SA Series Virtual Appliances, Junos Pulse enables MNOs to deliver the third pillar of securing mobility—connectivity—to their enterprise customers and end consumers as a managed service, and to enable secure, mobile remote access to networks, private and public clouds, and applications, while protecting vulnerable data in transit. Junos Pulse, Junos Pulse Mobile Security Suite, and Juniper's award-winning physical and virtual SSL VPN offerings enable MNOs to connect, protect, and manage their enterprise and consumer customers' mobile life.

Application-Aware Firewall Policies

Juniper Networks MAG Series Junos Pulse Gateways, with the Junos Pulse Access Control Service and the UAC/SRX license, enable application-aware firewall policies with the Juniper Networks SRX Series Services Gateways. This capability provides a cost-effective solution to secure specific applications by user role within the network—in a data center, for example—by allowing the MAG Series gateways to provide its list of roles to the SRX Series firewall. The end user gains a seamless experience through the integrated Windows domain single sign-on (SSO) functionality.

Junos Space Security Design

Junos Space Security Design delivers scalable and responsive security management that improves the reach, ease, and accuracy of security policy administration. It lets network security administrators more quickly and intuitively manage all phases of the security policy lifecycle through a single Web interface. Security Design runs on the Juniper Networks Junos Space platform for highly extensible, network-wide management functionality, including ongoing access to Juniper and third-party Junos Space ecosystem innovations.

STRM Series Threat Detection and Management

Juniper Networks STRM Series Security Threat Response Managers combine, analyze, and manage an incomparable set of surveillance data—network behavior, security events, vulnerability profiles, and threat information—to empower companies to efficiently manage business operations on their networks from a single console. The integrated approach of the STRM Series, used in conjunction with unparalleled data collection, analysis, correlation, and auditing capabilities, enables organizations to quickly and easily implement a corporate-wide security management program delivering security best practices that include log, threat, and compliance management.

Summary—Mobile Network Security for the MNO

Opportunities in the consumer and enterprise smart mobile device market are numerous and are expected to increase. As these devices continue to proliferate and become a ubiquitous part of the digital lifestyle, MNOs will be well positioned to take advantage of every opportunity to capitalize on these trends. Juniper Networks mobile network security solutions enable MNOs to leverage these opportunities with a layered, end-to-end approach that delivers comprehensive protection, scalability, and opportunities for managed security service offerings.

Next Steps

For more information about Juniper Networks mobile network security solutions, please contact your Juniper Networks representative.

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.

3510386-002-EN Mar 2012

Printed on recycled paper