LTE Security for Mobile Service Provider Networks

Juniper Provides a Stable and Secure LTE Network that Differentiates MSPs from the Competition

Table of Contents

Executive Summary

3G services were first offered in 2001, the iPhone launched in 2007, and for more than 10 years, mobile subscribers worldwide have outnumbered fixed-line subscribers. Smartphone adoption continues to grow, with nearly 60% penetration of the mobile phone market. Smartphone adoption will continue to accelerate as more and more service providers are launching LTE.

What does this mean to mobile service providers (MSPs)?

It means that the addressable market continues to grow at an accelerated rate. To maintain their competitive edge, most MSPs are focused on rolling out LTE, scaling up their network, and improving the user experience. However, MSPs need to understand that a secure network is a baseline requirement for a successful LTE deployment. As mobile services become an increasing part of our lives and people use private services such as mobile banking on their smartphones, end customers are expecting these services to be reliable and safe. Any security incident will greatly reduce customer trust, and can even impact customer loyalty towards their MSP of many years. At the same time, MSPs are continuously looking for new revenue streams by entering into new markets such as machine to machine (M2M). Security is an essential foundation as MSPs plan and evolve their networks from 2G/3G to LTE.

To understand the need for security, you must first understand the architectural differences between 2G/3G and LTE. LTE is a flat all-IP network architecture. The function provided by RNC has been distributed between eNodeB, MME and S-GW. Since the eNodeB is highly distributed and exposed and it directly connects to the mobile packet core, LTE security becomes one of the critical items for an MSP's LTE deployment. This white paper will describe LTE security requirements and the corresponding impact to MSPs and their customers.

Introduction

LTE has become a major item on MSP roadmaps across the world. Most MSPs either have launched or are planning to roll out LTE in order to catch up with the high data demand of their subscribers, driven by the proliferation of smartphones and tablets. Since TeliaSonera deployed the first commercial LTE network in December 2009, service providers have been deploying LTE networks at an ever-increasing rate. Although the percentage of LTE subscribers currently is still not significant compared with overall mobile subscriptions, according to Informa[1], LTE subscription growth is robust, especially in APAC and North America. The number of subscribers has increased more than 4 times from 2Q2012 to 2Q2013 (see Figure 1).

Unlike universal mobile telecommunications system (UMTS), LTE utilizes a flat all-IP network architecture. The advantage of this architecture is that it provides lower costs, lower latency, and greater flexibility. However, the nature of flat all-IP networks also creates certain security concerns. The LTE standards body, Third-Generation Partnership Project (3GPP) has recommended various guidelines for LTE security, and MSPs should consider these when they plan for their LTE network deployment. Let's look more closely at the LTE security requirement and see how it is different from the traditional 3G network.

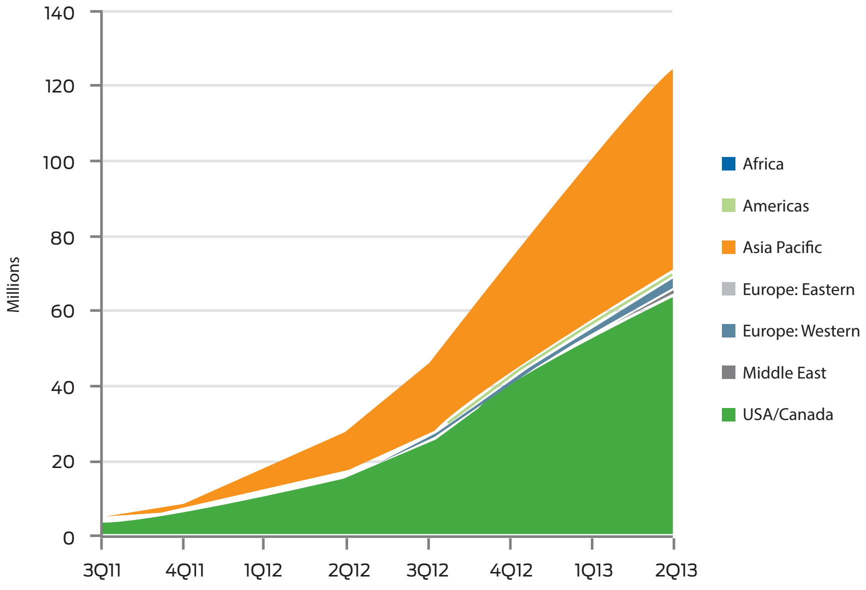

Figure 1: Rise in regional mobile broadband 4GLTE subscriptions

[1] Mobile Broadband Subscriptions, 8-Oct-2013, Informa UK Limited

LTE Security Trends and Requirements

LTE Architecture

From an architecture perspective, the major difference between 2G/3G and LTE is in the access network, or RAN. The LTE access network is a network of base stations (eNodeBs), and the centralized radio network controller (RNC) function in 3G no longer exists, resulting in a flat IP architecture for LTE. This distributes the intelligence to eNodeBs and speeds up connection setup and handover times. With this architecture, LTE can achieve lower latency than 2G or 3G.

In 3G UMTS networks, signaling and user data are encrypted from the mobile device to the RNC. Due to the intelligent, centralized RAN design of UMTS, RNCs are typically installed in the regional data center. Therefore, we have traditionally had few concerns about the UMTS RAN security. However, in LTE, eNodeB to EPC security is optional, which means all traffic is transported as “clear text,” providing an opportunity to inspect subscriber traffic and to easily inject network-impacting traffic.

SCTP Threat

Due to the reliable and in-sequence characteristics of Stream Control Transmission Protocol, SCTP is widely used for various interfaces in LTE, including S1-MME and X2-AP. SCTP has “watch dog” characteristics, which means that it is able to recognize when a packet is dropped or when links go down. This makes SCTP very suitable for delivery of high quality services LTE networks. However, several security attacks have been identified and documented in IETF RFC5062, including: Address Camping or Stealing, Association Hijacking, Bomb Attack, and Association Redirection.

Let’s use Association Hijacking of small cells as an example. With association hijacking an attacker assumes control of the session created by another endpoint. For instance, an eNodeB must be connected to an EPC MME (mobility management entity), and that connection is established over an SCTP association between the eNodeB and the MME. If an attacker is able to receive packets directed to this eNodeB and send packets with the source address of this eNodeB, the attacker can perform a full 4-way handshake using the IP addresses and port numbers from the received packet. The MME will consider this a restart of the SCTP association. In this case, the SCTP association has been hijacked, making it possible for this “evil” eNodeB (attacker’s eNodeB) to attack the MME. Similarly, if the attacker is able to receive packets being sent to the MME and send packets with the source address of the hijacked MME, it can attack all eNodeB(s) associated with this MME. One of the most effective attacks that can be mounted is to tell the other eNodeBs to disable their radio transmitters over the X2-AP interface.

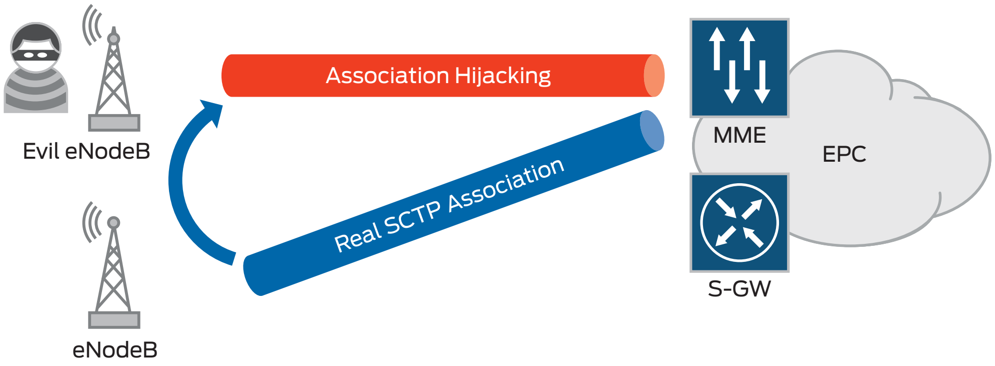

Figure 2: Association Hijacking

People might say that attackers can launch such an attack only if they are able to attach their tools/equipment to the access network. The way this argument goes, if the access network is located in a physically secured environment, the attackers have no way to perform such an attack. This concept is not entirely true. In fact, these kinds of attacks can happen in several ways:

- **Compromised physical security**—Acquiring the location of cell sites is always a challenge for MSPs, especially in city and urban areas. Due to prioritizing radio engineering over security for cell site locations, it is impossible to guarantee the physical security of the eNodeB, even when the eNodeB is installed according to the defined physical security guidelines. When physical security is not 100%, the attacker is able to insert the “evil” eNodeB into the RAN.
- **Internal attacker**—Negatively motivated employees can also present a threat to security. These attackers have official authority to manage and change the network, and the impact of their attacks depends on their role within the organization and the security policy of the company. It might jeopardize the privacy of customer traffic, or it might involve a signaling storm that collapses the whole network.

Small Cells Trend

Small cells are low power wireless access points, and they operate in a licensed spectrum that has a range of 10 to 500 meters. The low power and limited coverage of small cells enable service providers to use the same amount of spectrum to serve a smaller number of subscribers. By doing so, per subscriber bandwidth capacity becomes higher compared to macro cell deployments. LTE small cells are one of the key techniques that MSPs use to meet the high traffic demand usage from their customers.

Some MSPs may think that their mobile backhaul is already secure as they are using their own mobile backhaul network. This is somewhat true when macro cells are deployed, if the MSP has a very secure physical environment for their eNodeB cell sites and collocated network elements. Theoretically, no unwanted network nodes can connect to their IP network to attack their network or sniff their subscribers' traffic. However, this will no longer be true when small cells are deployed. The deployment of LTE small cells could introduce the following security risks:

- Traditional macro cells are deployed in cell towers or the roof of a building in order to provide higher geographical coverage. Typically, the equipment in a macro cell site is located in a physically secured environment like a proper container or locked room. The small coverage nature of LTE small cells makes the physical security challenging. The deployment of LTE small cells is very similar to Wi-Fi access points, which can be placed on the ceiling of an office, in a shopping mall, coffee shop, stadium, etc. Therefore, a hacker could easily sniff traffic by tapping the S1 or X2 interface. Attackers are also able to mount man-in-the-middle attacks, disrupt traffic, or even disconnect/turn off radio transceivers on adjacent nodes via the X2 interface.
- Because the traffic from eNodeB to EPC uses clear text, the confidentiality of subscribers is broken if encryption technology is not implemented between eNodeB and EPC.
- Rogue eNodeB poses yet another threat. With the distributed small cell architecture, the rogue eNodeB(s) can easily connect to the backhaul to reach EPC, which could cause unforeseen damage and outage to the LTE network.

Signaling Storm

Third-Party Applications on Smart Devices

In early 2012, a large LTE mobile carrier experienced a 4.5-hour outage that impacted 2.5 million subscribers[2]. According to the company, this outage was triggered by a free voice application running on Android OS smartphones, generating a signaling storm. This incident is a clear example of how open operating systems in smartphones can be both innovation enablers and a security threat. Anyone can convert their innovative idea into a mobile app and push it to the market. On the other hand, since these applications are not managed by MSPs, third-party applications on smart devices can potentially increase the signaling load for the network. In the worst-case scenario, a "network unfriendly" signaling storm could be triggered by a smart device application.

M2M and MTC

Machine to machine (M2M) and machine type communication (MTC) represent a profound and transformative market opportunity, providing service providers and Mobile Virtual Network Operators (MVNOs) the promise of a new market segment. One common characteristic of MTC services is the large number of devices participating in these services. For instance, one smart meter enterprise customer could bring a million devices to a service provider's network. Unlike LTE subscriber behavior, M2M traffic places more demand on signaling than throughput. Although the bandwidth utilized by these devices might be very small, they could generate a huge signaling load if the device population performs one or more activities at the same time. The power company could distribute a million smart power meters to its customers, and these smart devices could potentially report their usage all at the same second. In addition, the volume and nature of M2M and MTC signaling traffic cannot be easily predicted, especially in the initial phase of a service launch.

LTE Security Gateway Solution

To address the potential security vulnerabilities described above, there are three key areas that require security when implementing LTE Networks:

1. Traffic encryption between eNodeB(s) and EPC
2. Authentication of network elements to avoid a rogue or evil eNodeB connecting to the network,
3. Management and control of traffic delivered to avoid network downtime from signaling storms

In addition, the LTE security gateway sitting between the eNodeB(s) and EPC offering these protections should have the following capabilities:

4. High availability to prevent the loss of all active subscriber sessions during node failover (e.g., loss of power).
5. Extensive and proven Interoperability testing (IOT) history with various vendors' eNodeBs to account for varying qualities and capabilities of eNodeB IPsec implementations
6. SCTP firewall functionality to protect the mobile packet core from potential signaling storms.

[2] Android Signaling Storm Rises in Japan (www.lightreading.com/blog/mobile-operating-systems/android-signaling-storm-rises-in-japan/240005553)

IPsec Protection and Network Authentication

One of the main functions of an LTE security gateway is to set up an IPsec tunnel with the eNodeB to encrypt all traffic between the eNodeBs and the EPC. During the IPsec tunnel setup process, the two endpoints will quickly establish, via the Internet Key Exchange (IKE) control plane, that they need to authenticate each other with X.509 certificates. The eNodeB validates the certificate of the security gateway (single-sided authentication) to confirm that it is connecting to the correct network. Typically, however, the security gateway will also validate the certificate of the eNodeB, thus validating the eNodeB's identity. Authentication of both the security gateway and the eNodeB is called mutual authentication. After a negotiated time period, the security gateway and eNodeB rekey, which means that they change their keys for both the IKE_SA as well as the IPsec_SAs (bearer plane). Periodic and regular rekeying makes it much harder for an attacker to derive the keys used to encrypt the traffic.

After the eNodeB has been authenticated, the eNodeB and LTE security gateway will be treated as trusted peers. S1-MME, S1-U and X2-AP, and X2-U messages can be passed through the tunnel. Rogue eNodeBs can be filtered out, as they will not be able to pass the authentication process. Also, with data being encrypted with Encapsulation Security Payload (ESP) protocol, attackers/hackers will not be able to understand the content, even if they are able to sniff the traffic anywhere between eNodeBs and LTE security gateways. The MSP's network will be protected even when small cells are rolled out.

SCTP Firewall

SCTP firewalling performs stateful inspection of SCTP traffic based on security policy. It can deny malicious messages (hijack, redirection, etc.), and SCTP rate limiting can avoid signaling storms triggered by user equipment malware and unexpected M2M traffic.

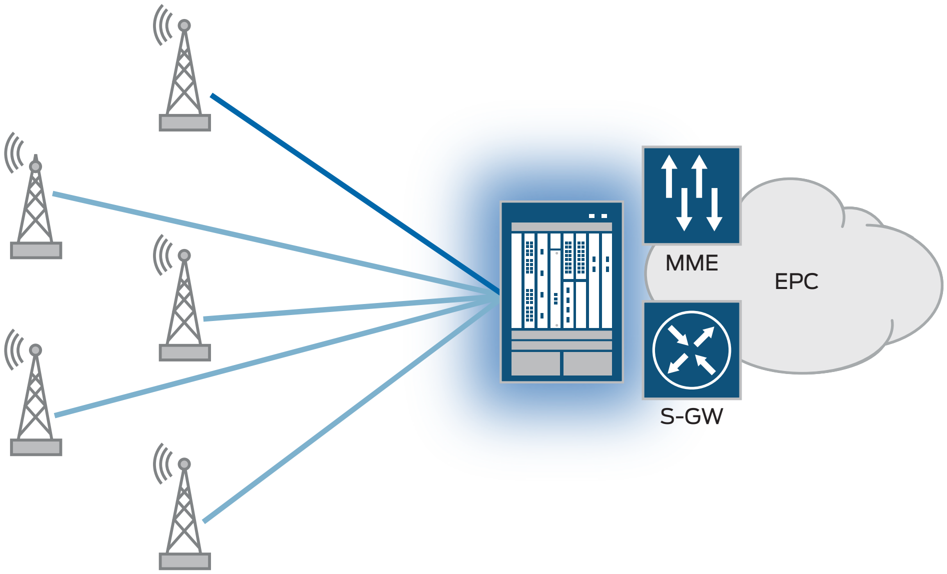

Figure 3: Global or per IP rate limiting

Rate-Limiting per Association

Though ideally each EPC element (MME, serving gateway, etc.) would have its own overload protection mechanism, these are not in practice designed as self-protecting security elements. An SCTP firewall is needed to protect the packet core. For instance, for each SCTP association, an SCTP firewall can be configured to drop SCTP packets delivered beyond that association's packet per second limit. When attacker/malware user equipment sends a traffic flood to exhaust an MME's resources, or an inadvertent DoS attack is launched by well-intentioned subscribers or devices, the SCTP firewall on the LTE security gateway can reduce the packets per second (pps) first as in Figure 3, and perform further inspection later. The same could be applied to an M2M application if you have an LTE small cell serving a particular M2M customer. We recommend using an LTE security gateway with SCTP firewall capability as an element that can be inserted unilaterally to avoid a signaling storm accidentally attacking the EPC.

Cookie Inspection: During a 4-way handshake procedure, a cookie is cached for each association. If attackers attack servers with COOKIE-ECHO messages, it could be a real cookie attack or a random cookie attack. In either case, the SCTP firewall must be able to isolate and stop this attack traffic while allowing "good" traffic to pass.

X2 Adjacency Firewalling: The X2 interface between two eNodeBs enables low latency handover. X2 adjacency firewalling in an SCTP firewall only allows for the eNodeBs within geographic proximity of each other to communicate using the X2 interface. Rogue eNodeBs can thus be blocked from attacking MSP eNodeBs, and superfluous signaling traffic caused by misconfiguration can be removed.

High Availability (HA)

Stateful failover is extremely important in an LTE security gateway to provide non-stop operation of the LTE network. As shown in Figure 4, stateful failover means that the state of the IPsec IKE_SA control plane tunnel and the pair of IPsec_ SA unidirectional tunnels for bearer traffic are kept up when the system fails over from the primary to the backup. If an LTE security gateway does not support stateful failover, then the eNodeB will try to reestablish the IPsec tunnel with the security gateway. This process could take 5 seconds or even 30 seconds depending upon the dead peer detection interval of the keepalive between the eNodeB to security gateway, and even after the detection of a dead peer occurs, additional time will elapse due to the need to validate certificates against a certificate authority during the setup of the new IPsec tunnel.

While this IPsec tunnel is reestablished, there is no connectivity between the eNodeB and MME or eNodeB and serving gateway (S–GW) meaning all traffic between the user equipment and the EPC is dropped. Once this happens, the user equipment has to re-signal for new bearers. While the exact amount of time this will take depends on the number of user devices, it will take 10-15 seconds for all user equipment to realize that they no longer have valid bearers and that they must signal to request new ones. Any applications in progress, including video streaming (once buffers are exhausted), e-mail downloads, webpage downloads, gaming app updates/synchronization will all stop in their tracks. For these reasons, stateful failover HA is a mandatory requirement of any LTE security gateway solution.

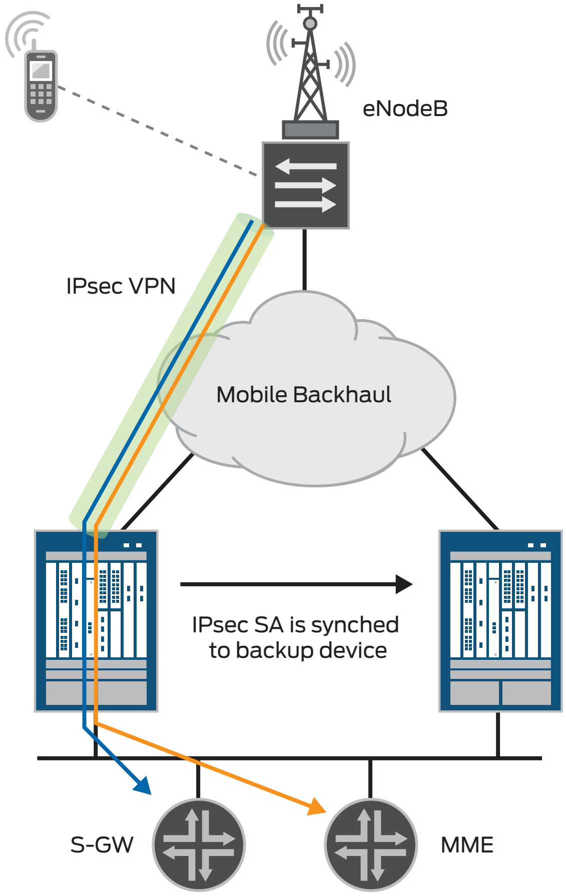

Figure4: High Availability LTE security gateway

In-Service Software Upgrade (ISSU) and In-Service Hardware Upgrade (ISHU)

Software upgrades and capacity expansion are unavoidable with any system, and the LTE security gateway is no exception. Without ISSU, the impact discussed above for non-stateful failover will occur whenever the administrator wants to perform scheduled software upgrades or updates. This will reduce customer quality of experience due to network downtime and erode brand loyalty. Supporting unified ISSU is essential, as it provides 24x7 uninterrupted protection to the MSP's infrastructure and customers.

As stated earlier, all MSPs are faced with the dramatic growth in mobile broadband traffic. With this dynamic traffic growth, hardware capacity expansion could occur yearly or even quarterly. Traditional hardware capacity expansion involves network redesign and reconfiguration, since new interfaces are introduced associated with the new capacity being brought online. This adds complexity to the expansion and operation of the LTE security gateway. The LTE security gateway must be architected so hardware resources can be added and load-balanced independent of the device configuration. Since the load balancing to the system is performed internally, reconfiguring and manually load-balancing tunnels to specific hardware resources in the chassis is not required. Another benefit of this product architecture is that the addition of hardware resources at the security gateway does not require changes on the eNodeB(s). With this in-service hardware upgrade (ISHU), capacity is expanded simply by adding hardware resources to the security gateway. No reconfiguration is necessary, simplifying capacity expansion and reducing time to market.

Interoperability Testing (IOT)

All of the previous requirements for security gateways are meaningless without proven interoperability capabilities. Although LTE security gateway to eNodeB IPsec tunnels should "just work" since both implement the IETF IPsec standards specified in the 3GPP LTE standards, in practice there can be significant interoperability issues. The problem is that eNodeB vendors have different interpretations of the implementation of both IPsec and the Internet Key Exchange Protocol Version 2 (IKEv2) standards, and StrongSwan, the open source client software typically used by eNodeB vendors in their IKEv2 implementations. The problems arise in determining the meaning of information elements in the IKE_SA messages, such as what is the correct response to certain messages from the other end of the IPsec negotiation, and what to do when negotiations fail, leaving much to interpretation.

Since StrongSwan is very flexible, there are multiple ways in which the client implementation can be approached, and this means that client implementations are not always compliant with the RFCs standards. Also, there is a specific set of 3GPP profiles and behaviors in TS 33.210/310 that are typically not followed to the letter, which results in a wide variety of interpretations of the standard. The only way to normalize all of this is to have a "relaxed, but experienced" implementation of IKEv2 on the security gateway that takes into account real-world scenarios with eNodeB implementations and adjusts for them. When considering LTE security gateway solutions, it is important to select a vendor with extensive IOT experience – you do not want to be the customer at which IOT development is performed by the vendor.

Juniper LTE Security

Juniper Networks® SRX Series Services Gateways are high-performance network security solutions for enterprises and service providers that pack high port density, advanced security, and flexible connectivity into easily managed platforms. These versatile and cost-effective solutions support fast, secure, and highly available operations, with unmatched performance to deliver some of the industry's best price-performance ratios and lowest TCOs.

SRX Series Services Gateways—which integrate carrier-grade NAT (CGNAT) implementations, stateful SCTP firewall, IPsec VPN, intrusion prevention system (IPS), application security, and quality of service (QoS)—can address common and complex security threats. Specifically the SRX5600 and SRX5800 gateways are extremely suitable to be the LTE security gateway, as each supports all key requirements, including:

- IPsec protection
- Network authentication
- SCTP firewall
- High availability
- In-service software and hardware upgrade

Conclusion

LTE is a cutting-edge technology that enables high-speed and low-latency mobile broadband and provides significant improvements in user experience over 3G / UMTS. With its innovative flat-IP architecture, however, LTE security requirements are very different from UMTS. An LTE security gateway solution needs to not only authenticate eNodeBs and encrypt traffic with IPsec, but also provide SCTP firewall functions to protect the mobile packet core from signaling storms and man in the middle attacks. In addition, an LTE security gateway must support high availability to prevent the loss of all active subscriber sessions during node failover.

In order to provide a stable and secure network, differentiate from the competition, and capture revenue streams from new market segments such as M2M, MSPs will need to roll out their LTE networks with an LTE security gateway that provides both IPsec and SCTP firewalling functions to protect both the network and customers. SRX Series gateways excel at meeting all of the key requirements of an LTE environment. SRX Series have performed eNodeB interoperability testing with RAN vendors like Ericsson, NSN, and Huawei, and come with strong LTE security gateway live references to ensure interoperability with eNodeBs. MSPs can have full confidence in Juniper's LTE security solution with more than two dozen live deployments around the globe.

References

What do we mean by "Mobile overtakes Fixed"? (**www.itu.int/osg/spu/ni/mobileovertakes**)

Smartphone Penetration Nears 60% of the Mobile Market (**www.marketingcharts.com/wp/interactive/smartphone-penetration-nears-60-of-the-mobile-market-30760**)

Mobile Broadband Subscriptions, 8-Oct-2013, Informa UK Limited

Android Signaling Storm Rises in Japan (**www.lightreading.com/blog/mobile-operating-systems/android-signaling-storm-rises-in-japan/240005553**)

3GPP TS33.401

3GPP TS33.210

3GPP TS33.310

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.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

2000536-001-EN Sept 2015