clavister ThoughtLeader

LTE Security: Backhaul to the Future

Kimmo Klemola, technical manager at Clavister investigates how operators should approach securing their LTE network backhaul to meet subscriber expectations, without impacting on network performance or their bottom line.

It's hard to hit moving targets, but subscribers to 4G and LTE networks need to be assured that their data has better protection than just being part of a high volume, fast-moving flow of traffic. This is a key issue with LTE architectures – the connection between the cell site and the core network is not inherently secure.

Operators have previously not had to consider the need for secure backhaul. 2G and 3G services use TDM and ATM backhaul, which proved relatively safe against external attacks. What's more, 3rd Generation Partnership Project (3GPP) based 2G and 3G services provide inbuilt encryption from the subscriber's handset to the radio network controller. But in LTE networks, while traffic may be encrypted from the device to the cell site (eNB), the backhaul from the eNB to the IP core is unencrypted, leaving the traffic (and the backhaul network) vulnerable to attack and interception.

This security problem is compounded by the rapid, widespread deployment of microcell base stations that provide extra call and data capacity in public spaces, such as shopping centres and shared office complexes. The analyst Heavy Reading expects that the global number of cellular sites will grow by around 50% by the end of 2015, to approximately 4 million. Many of these new sites will be micro- and small cells, driven by the demand to deliver extra bandwidth to subscribers at lower cost.

Microcell security matters

These small base stations placed in publicly-accessible areas typically only have a minimum of physical security when compared to a conventional base station. This creates the risk of malicious parties tampering with small cell sites to exploit the all-IP LTE network environment, to probe for weaknesses from which to gain access to other nodes, and stage an attack on the mobile core network. These attacks could involve access to end-user data traffic, denial-of-service on the mobile network, and more.

Furthermore, operators are starting to experience pressure to deliver strong security for subscribers' data, because of competitive pressure from rivals and the need to assure both current and future customers that their mobile traffic is fully protected against interception and theft.

As a result, backhaul from the eNB to the mobile core and mobile management entity (MME) needs securing, to protect both unencrypted traffic and the operator's core network. Especially when the backhaul network is provided by a third party, is shared with another operator or provider, or uses an Internet connection – which are all common scenarios for MNOs looking to deploy backhaul with the lowest overall cost of deployment and ownership. While these types of backhaul network deliver lower costs, they also reduce the overall trustworthiness of the network. So how should MNOs protect backhaul infrastructure against security risks, to boost subscriber trust and protect data and revenues?

Tunnel vision

To mitigate the risks of attack on backhaul networks, and to protect the S1 interface between the eNB and mobile core, 3GPP recommends using IPsec to enable authentication and encryption of IP traffic, and firewalling at both eNB and on the operator's mobile core. The 3GPP-recommended model involves IPsec tunnels being initiated at the cell site, carrying both bearer and signalling traffic across the backhaul network and being decrypted in the core network by a security gateway. IPsec is already used in femtocell, IWLAN (TTG) and UMA/GAN deployments, and a majority of infrastructure vendors support the use of IPsec tunnels in their eNB solutions.

However, while IPsec is the standard approach to security recommended by 3GPP, there are common concerns about its deployment, based on factors such as the operator's market position and customer profile; the cost and complexities of deployment; and how IPsec deployment might impact on overall network performance.

MNOs need to be confident that their IPsec deployments are highly scalable, and offer high availability to cater for the expected explosive growth in LTE traffic and bandwidth demands. This in turn means using security solutions that offer true carrier-grade throughput capabilities as well as compliance with latest 3GPP security standards, while being flexible enough to adapt to the operator's needs as they evolve. At the same time, the IPsec solution should be as cost-effective as possible, to minimise impact on budgets.

Scalable security

To address these concerns, the IPsec security solution should run on commercial off-the-shelf platforms embedded in virtualized hypervisors. This avoids the costs and complexity of having to aggregate backhaul traffic to a central network point, or complementing existing solutions with additional hardware, while also enabling rapid deployment and easier management. A virtualized solution also gives excellent scalability to support operators' future needs.

In terms of network performance, the solution should also support both single and multiple IPsec tunnels from the eNBs to the network core, which enables the use of flexible QoS network optimization based on specific criteria such as the tunnel ID or service used – making the security transparent to the subscriber. This also enables the operator to offer dedicated IPsec tunnels to different customer groups – such as public safety users – to segregate different types of sensitive traffic from each other.

Using a flexible security platform that offers advanced IPsec capability and supports other advanced security applications, MNOs can protect their subscribers' data and the network core against the risks of interception and attack, and easily manage the security deployment. This in turn helps them to secure their subscribers' data, loyalty and ongoing revenues.

More From Clavister

For more though leader articles and information about Clavister products, visit **www.clavister.com**.

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com