clavister
SolutionSeries

Clavister Mobile Backhaul Security

LTE Backhaul and Small Cell Security

SOLUTION AT-A-GLANCE

- Clavister mobile backhaul security offers an affordable alternative to mobile backhaul security that is built on a software foundation that can be executed directly in a virtualized environment based on VMware or KVM infrastructure.
- Instead of aggregating backhaul security to a central network point in the operator network that is viewed as a static method that limits expansion when base station capacity increases, our solution is available as a software package that can be executed on existing Intel based hardware with the support for Intel® Virtualization Technology including Intel® Virtualization Technology for Directed I/O (VT-d) and AES-NI instruction set.
- Increased encryption performance is just a click away, by allocating more resources to our security solution, capacity can be increased very efficiently from a remote location compared to complementing with more appliance hardware.
- Clavister mobile backhaul security solution supports use-cases based on complete 3GPP LTE NDS feature set.

Executive Summary

Operators have traditionally not had to consider the need for secure backhaul. 2G and 3G services use TDM and ATM backhaul, which have proven to be relatively safe against external attacks. However, since the introduction of 3GPP LTE, end-user traffic is no longer encrypted from the base station to the Radio Network Controller. This means operators need to resolve a potential security issue between the eNodeB (eNB) and the mobile network core, especially when third-party transport links are used.

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 eight 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.

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 gives malicious parties the chance to tamper with small cell sites and exploit the all-IP LTE network environment, to probe for weaknesses from which to gain access to other nodes and to 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.

As a result, eNBs which use third-party backhaul to the mobile core and mobile management entity (MME) need security solutions to protect the unencrypted traffic between the eNB and the operator's core network from being breached. This security is usually based on IPsec protocols for the data traffic, and firewalling at both eNB and on the operator's mobile core.

By adopting a Mobile Backhaul solution from Clavister, operators can secure their subscribers' data, loyalty and revenues by mitigating the risk of network attacks, and enhancing network uptime. This document shows how an effective, standards-based solution to secure LTE backhaul can be deployed.

Challenges for Mobile Network Operators

MNOs are looking for ways of using backhauling technology with the lowest overall cost of deployment and ownership as a mechanism to strengthen ARPU. This leads to a point where earlier, high-cost transport (CS/SDH/ATM) cannot keep up with the bandwidth demands of new and planned base stations. While the data transport cost over IP-based infrastructures is low, both user data and signalling traffic from the eNB to the network core is pure non-encrypted IP traffic, meaning it can be intercepted or altered by an attacker.

To mitigate these risks of attack, and to protect the S1 and X2 interfaces, 3GPP recommends using IPsec to enable authentication and encryption of IP traffic. IPsec is firmly established as a proven, secure technology within enterprise and operator networks. 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.

3GPP recommends using IPsec where an operator decides that that its backhaul is 'untrusted.' But how should MNOs decide if their backhaul network is untrusted, or not? For a backhaul network to be untrusted, it could mean that:

- the backhaul is provided by a third party, or uses an Internet connection
- the backhaul is shared with another operator or provider
- it is built using a Layer 1 technology that falls short of the MNO's definition of 'trusted'

So the issue of whether IPsec is needed or not, is one of the most contentious for network planners as they prepare for wider LTE deployments. Both individual mobile subscribers and corporate users have come to expect high levels of security from mobile networks. To match this expectation, MNOs must evaluate how trusted their backhaul network is in the context of the growing attack surface which results from migrating to LTE architectures.

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 its bandwidth demands. This in turn means using 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.

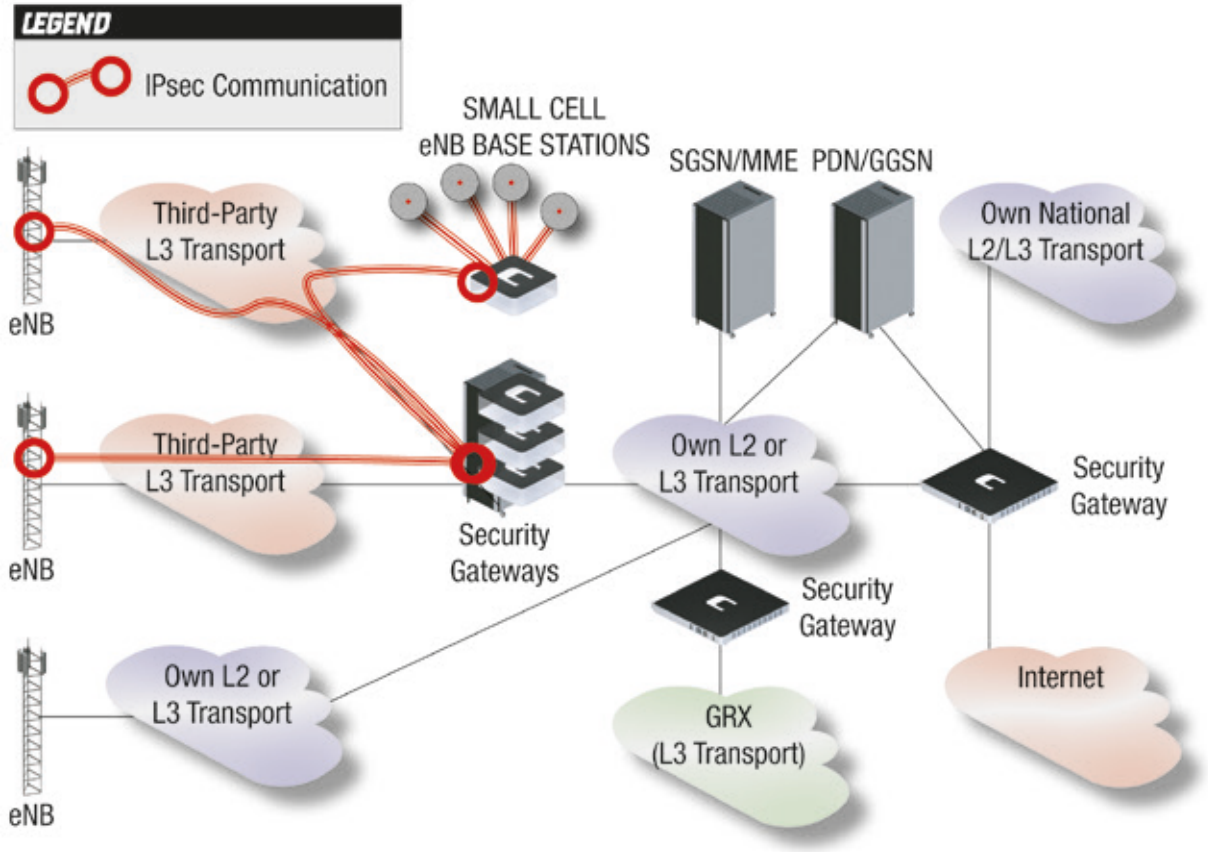
Clavister Mobile Backhaul Security Solution

Instead of having to aggregate the traffic to a central network point or having to complement existing solutions with additional hardware, Clavister's approach enables the solution to be executed directly on COTS x86 platforms embedded in hypervisors such as KVM or VMware. This ensures deployments can be done rapidly, and reduces the complexity of managing the solution. This gives operators a highly flexible solution that can scale from low bandwidth up to very high bandwidth on conventional x86 hardware, giving a future-proofed software foundation.

The solution offers a complete feature-set covering IPSec functionality, including:

- Policy control
- Compliance logging
- Bandwidth management
- Value added services
- Application control bandwidth limitation/guarantee or complete block
- CAPEX/OPEX is lowered with our solution COTS hardware is used instead of purpose build appliances. Existing COTS hardware can be used for the solution
- Supports CMPv2

Clavister's mobile backhaul solution delivers IPSec connectivity in a secure and scalable way. This addresses the many-to-one IPSec tunnel issue, and enables deployment of multiple IPSec tunnels. To lower delays and jitter, Clavister utilizes hardware acceleration, if this is present in the COTS: this improves bandwidth utilization and 'round trip' times for data traffic.



Solution Benefits

In addition to improving the user experience with secure, encrypted data transfers in controlled LTE NDS backhaul ecosystems, operators can be assured – and assure their customers – that Clavister solutions are not shaped by external government or political influences, adding a critical element of trust. The features and trustworthiness of the solution also enables MNOs to add over-the-top revenue streams by introducing value-added new services. Benefits include:

- Utilizes COTS hardware – more cost efficient in comparison to appliance hardware and centralized solutions.
- De-centralized solution – does not require massive centralized multi-gigabit backbone bandwidth
- Virtualized multifunctional security software features
- Supports use-cases based on complete feature set
  - LTE SEG S1 as profiled in 3GPP 33.310
  - IPsec ESP (RFC 4303) as profiled in 3GPP 33.210
  - IKE v2 (RFC 4306) as profiled in 3GPP 33.210
  - User plane protection as profiled in 3GPP 33.401,11,12
  - Public Key Signature X.509v3 3GPP 33.310
  - NEBS Compliant
  - Supports CMPv2

Conclusion

With the introduction of 3GPP LTE, operators need to resolve potential security issues in order to protect their subscribers' data and the network core against the risks of

interception and attack. One of the key risks to be mitigated is via the S1 LTE radio access interface, between the eNodeB and the mobile network.

Using a scalable, flexible security platform that offers advanced IPSec capability and supports other advanced security applications, MNOs can protect their infrastructure against these risks, and easily manage the security deployment. This boosts trust, helps to increase operational efficiency, and protects revenues.

Where to Buy Clavister

For more information about where to buy Clavister products, visit www.clavister.com/partners. Additional resources and customer testimonials can be found at www.clavister.com/support/resources.

About Clavister
Clavister (NASDAQ: CLAV) is a leading security provider for fixed, mobile and virtual network environments. Its award-winning solutions give enterprises, cloud service providers and telecoms operators the highest levels of protection against threats, with unmatched reliability. Clavister's performance in the security sector was recognized with the Product Quality Leadership Award from Frost & Sullivan. The company was founded in Sweden in 1997, with its solutions available globally through its network of channel partners. To learn more, visit www.clavister.com.

Where to Buy
www.clavister.com/partners

Contact
www.clavister.com/contact

clavister®
WE ARE NETWORK SECURITY

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