clavister
SolutionSeries

Clavister Small Cell Site Security

Distributed operator environment – Clavister small cell site security solution

SOLUTION AT-A-GLANCE

- Clavister Small Cell Security Gateway offers a comprehensive security solution for small cell sites - a distributed operator environment where operator core network functions combined with security is positioned into a virtualized environment that acts as a distributed operator core network for small cells – a low-powered base station that operates in the licensed spectrum combined with Wi-Fi capabilities.
- Clavister Small Cell Security Gateway acts as a small cell site security anchor point providing firewalling security, internal security through virtual machine separation, IPsec backhaul security designed for small cells, Wi-Fi intelligent mobile offloading, all combined with a full feature-set using a minimal storage and memory footprint.
- Our solution is available for well-known hypervisors and includes support for Intel® Virtualization Technology, Intel® Virtualization Technology for Directed I/O (VT-d) and Intel® AES-NI instruction set.
- New revenue models with value added services can be offered to subscribers with network insight that Clavister Small Cell Security Gateway solution provides.

Executive Summary

When deploying LTE networks, MNOs have struggled with delivering good coverage from macro base stations to indoor environments. Yet it is here where a strong signal is often needed the most, especially in crowded locations, such as shopping malls or sporting venues, where the volume of subscriber traffic puts pressure on weak network coverage. This can lead to slow network and web access, creating a bad user experience.

The solution for MNOs is to install small cells, low-powered base stations that operate in the licensed spectrum combined with Wi-Fi capabilities to enable high transfer speeds. Small cells can easily be deployed indoors and outdoors at street level to provide subscribers with a strong signal and high bandwidth.

The research company Heavy Reading estimates that cellular site numbers will grow by around 50% globally by the end of 2015, to 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.

Small cells also give MNOs an opportunity to introduce a distributed operator environment, in which small cells are collocated and specific network functions shared between operators. A distributed operator environment can place certain core network functions close to small cell sites (such as SGW, PDN) and other services, such as web/video and DNS caching, that benefit subscribers connected to small cell base stations.

The result is an improved subscriber experience and reduced traffic to operators' core networks. Using a virtualized environment like KVM or Xen running on commercial off the shelf (COTS) x86 Intel Architecture®-based platforms greatly reduces cost and deployment time for small cell sites.

However, small cell deployments also introduce new security risks that potentially endanger both end-user data integrity and service quality – especially when those cells are shared across networks.

Clavister's Small Cell Security Gateway architecture provides virtualized domain security that separates and protects the virtual hardware, virtual machines and virtual networks inside the virtual environment in small cell environments.

This solution works together with Clavister's Mobile Backhaul Security, enabling encrypted and authenticated access to each small cell base station to protect subscriber data integrity. It also integrates seamlessly with Clavister's Intelligent Mobile Data Offloading (IMO) solution, which provides intelligent Wi-Fi offloading that supports both seamless authentications with 802.1x EAP-SIM and web portal access to small cells. These solutions can be merged with a wide range of value-added security features such as UTM and application identification to improve the quality of service to subscribers.

Clavister delivers a cost effective, fully functional, carrier-grade security solution, with a minimal memory and storage footprint.

Challenges in a Distributed Operator Environment

As LTE coverage is one of the major challenges for MNOs, small cell base stations which operate in licensed spectrum combined with Wi-Fi network capabilities offer a useful boost to network coverage and performance, especially in densely-populated locations.

Small cells demand the same levels of service quality and subscriber data integrity that MNOs provide for macro base stations that cover wider areas.

Macro base stations typically use MNO-owned network infrastructure for connectivity: however, using wholly-owned infrastructure for small cells would quickly prove expensive for MNOs. Using backhaul owned by a third party, small cells become much more financially viable for MNOs.

However, third-party network infrastructure carries a risk of exposing subscriber integrity: the MNO no longer manages the network connection from the base station to the mobile core.

So the obvious next step for MNOs planning small cell build-outs is to distribute its core network functions closer to the small cell sites, with network functions that are usually found in operators' core networks such as SGW (Serving Gateways) and PDN gateways placed close to small cells. This approach gives the possibility to add services that provide an improved customer experience in the small cell site, such as caching services that minimize the subscriber load time and reduce core network load.

Virtualization of MNO core network functions and security using x86 Intel Architecture®-based platforms is the only financially viable option for MNOs when building distributed operator environments for small cells. However, a distributed operator environment using virtualized architecture, and combined with third-party network access for small cells gives rise to several challenges:

- Virtualized networking security – MNOs today secure their core networks with network zones using numerous security gateways and encryption security points to protect the traffic from eNodeBs. A distributed operator environment bears the same network zone and security requirements with dissimilar policies per core virtualized network function. A distributed operator network runs within the same server hardware
- MNOs need to guarantee that subscriber traffic from small cells is protected to the distributed operator environment when third-party network access is used by small cell base stations
- Virtual machines in the distributed operator environment have to preserve the lowest storage and memory footprint to preserve capital expenditure
- Security solutions in the distributed environment must support flexibility and allow MNOs to add new services as required

What's needed is a security solution within the distributed operator environment that supports virtualized network security zones, and can act as an encryption anchor point to provide integrity and service quality for subscriber traffic from small cells. In addition to a full security feature set, the solution should have a small footprint, as storage capacity is limited in a distributed operator environment.

Clavister Small Cell Site Security Gateway Solution

The virtualized security solution that Clavister offers for small cell site in a distributed operator environment, where small cell base stations are conjoined with operator core network functions such as SGW and PDN using virtualized architecture, surpasses the challenges associated with distributed deployment. Clavister's Small Cell Security Gateway delivers security by enabling:

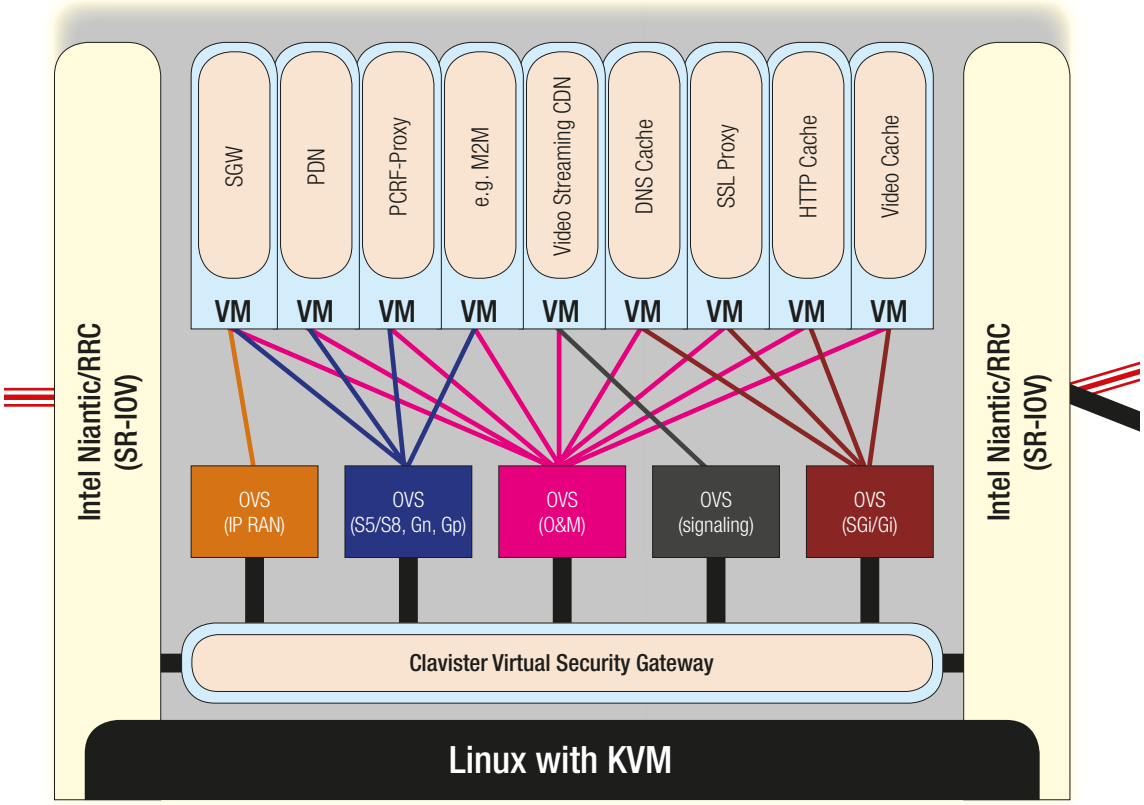

Fig. 1 – Small cell site virtual environment. Virtual machines are segregated with Clavister Virtual Security Gateway using Open vSwitch (OVS) bridges. Clavister Virtual Security Gateway acts as an IPsec termination point from small cells and provides authenticated and encrypted operator core connectivity to the virtual environment.

- Network zoning – Virtual machine segregation, with different policies and feature sets enabled for each. Core network functions in the distributed environment will be separated into zones with different policies.
- Clavister backhaul security – Carrier grade backhaul IPsec encryption security from small cell base stations to the distributed operator environment.
- Clavister Intelligent Mobile data offloading – Mobile data offloading solution providing 802.1x EAP-SIM based access for seamless handover to Wi-Fi, including with web portal based access from small cells.
- Full feature set, including
  - Policy control
  - Application based access control
  - UTM-services
  - Anti-virus scanning
  - Bandwidth management
  - User data transfer accounting
  - Compliance logging
- Minimal storage and memory footprint
- Executes in virtualized environments
- Supports Intel® Virtualization Technology including Intel® Virtualization Technology for Directed I/O including SR-IOV technology for carrier class performance
- Supports Intel® Advanced Encryption Standard New Instructions

Clavister Backhaul Security

One of the key LTE security risks that needs to be mitigated is via the S1 LTE radio access interface between small cells and the distributed operator network. Using a scalable, flexible security platform with minimal footprint that offers advanced IPsec capabilities and supports advanced security applications, MNOs can protect infrastructure against risks, and easily manage security deployments.

This boosts trust, helps to increase operational efficiency, and protects revenues.

Clavister Intelligent Mobile Data Offloading

Improvements to the user experience with controlled offloading from small cells supporting Wi-Fi capabilities, and the corresponding traffic decrease in the core mobile network, provides subscribers with a range of advanced service options that go beyond simple connectivity.

Clavister IMO enables MNOs to introduce valuable over-the-top revenue streams. Clavister intelligent mobile data offloading incorporates per-subscriber network slicing, enabled by application based traffic control and high scalability, to ensure that you operators stay in control of their networks.

Benefits

By deploying Clavister's Small Cell Security Gateway solution, MNOs can guarantee subscriber data integrity and service quality with a secure, fully isolated environment within the virtualized small cell site and supreme scalability, with a minimal storage and memory footprint.

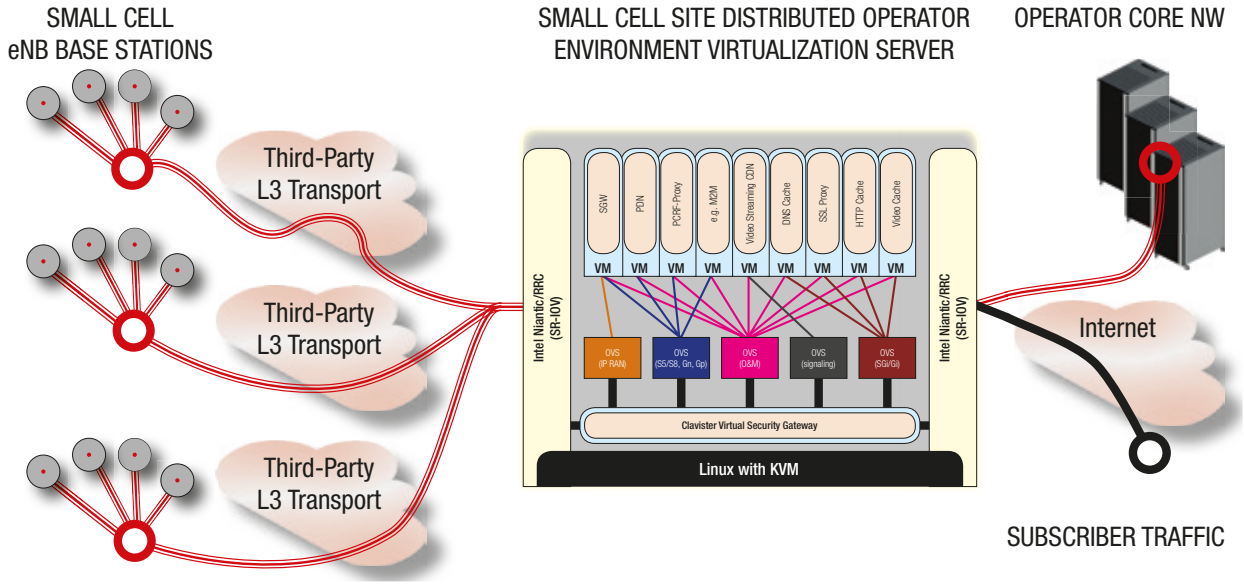

Fig. 2 – Small cell site solution view. Integrated Clavister backhaul security provides encryption and authentication security to small cells, Clavister IMO provides intelligent mobile data offloading capabilities from small cells with Wi-Fi integrated and virtual machine separation.

Conclusion

Small cell deployments are a focus for MNOs, as they are reaching a point where these are considered to be the most efficient way of expanding indoor coverage in the licensed spectrum. Distributed operator environment build-out is closely linked to small cell base station expansion.

This gives MNOs new challenges, to resolve both potential external and internal security aspects in their small cell site deployments in order to protect subscribers' data, at minimal cost.

Using a scalable, flexible, multifunctional security platform with minimal memory and storage footprint that offers security both to the data transport from small cells, and the internal distributed core network, MNOs can protect their infrastructure

against security risks and deliver flexibility to accommodate future expansion. This 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