WHITE PAPER

Communications Service Providers
Network Security

Virtual Security Gateways at Network Edge Are Key to Protecting Ultra Broadband Mobile Networks

Combined technologies create a virtualized security gateway with real-time processing even for small packets associated with IP voice applications.

The future of wireless is ultra-broadband packet throughput, with 4G/LTE speeds hitting 25 Mbps to 50 Mbps[1] and 5G technologies targeting even faster speeds. But the IP mobile networks that are serving up this throughput have new security risks for MNOs that can negatively impact their infrastructure, operations, customer services, and data.

Utilizing security gateways (SeGW) in every base station and small cell is the proven way to secure the network against hackers. But legacy gateways don't offer the performance or flexibility to scale for cost-effective deployment at a macrocell or at a small cell. Casa Systems worked with Intel and Intel® Network Builders ecosystem members Advantech and Wind River to build a complete virtual SeGW system with the performance and flexibility for these edge locations—even for demanding IP voice applications that transmit floods of small packets that typically have overwhelmed legacy gateways.

The Critical Issue of Mobile Infrastructure Security

Security in base stations is a critical issue. Letting hackers gain access to the wireless network endangers the infrastructure as well as users' data and personally identifying information (PII). Gaining access to the base station means hackers could hijack the data flows or could crash the base stations to disable service.

According to security researchers,[2] the main cyber security threats and risks to mobile network infrastructure touch on the following areas:

- User identity and privacy
- Base station functions and handovers
- Broadcast or multicast signaling
- Distributed denial of service (DDoS)
- Manipulation of control plane data
- Unauthorized access to the network
- Compromise of eNodeB (eNB) credentials or physical attacks on an eNB
- Protocol attacks on an eNB
- Attacks on the core network

According to the Worldwide Infrastructure Security Report,[3] based on a survey of security professionals worldwide in various industries, 38% of MNO respondents have experienced a security incident on the packet core that led to an outage that impacted customers. Some 70% of those MNOs taking the survey reported DDoS attacks targeting their subscribers or their network.

Table of Contents

Evolving Network Opens New Security Concerns

Several technology trends are making it more important to boost infrastructure security. The network evolution to 4G/LTE networks improved network speeds, but also ushered in an all-IP network with a more open architecture that means any hacker that has access—physical or logical—to an eNB can launch an attack. This contrasts with 3G and previous network generations that were based on closed, circuit-switched telecommunications network technology that is harder for hackers to penetrate.

In addition, traffic from untrusted public Wi-Fi hotspots adds increased exposure to threats that can impact service and compromise security. Network sharing agreements related to co-selling of cloud services can also expose an MNO network if the partner's network has poor security.

Another challenge that stems from faster mobile networks is network densification and the move to heterogeneous networks (HetNets). The increased signal attenuation that is the natural result of faster data throughput speeds means more and different kinds of base stations are required to deliver performance for an increased number of users that are consuming ever more data.

In the 3G era, roughly 200,000 macro base stations were required to cover the U.S. But that number is growing for 4G networks and the rate of growth is expected to take off for 5G networks as throughput speeds continue to increase. Because of the flat nature of LTE networks, having more base stations means there are more places where hackers can gain access to a base station or small cell.

Secured Network Edge Protects Dense, All-IP Network

The solution to these challenges is to add security gateways (SeGW) at the very edge of the network, which secures data as it hits the network, instead of placing the gateways in the core of the network and then backhauling the data to that gateway for processing. Thus, the security gateways protect the network by allowing only authenticated and authorized traffic onto the core network and then by encrypting that traffic using IPsec.

With legacy, fixed-function security gateway appliances, it was costly for MNOs to adopt this edge security architecture. But with network functions virtualization (NFV), security gateway virtual network functions (VNFs) running on industry-standard, high-volume Intel® architecture-based servers can be more easily added to the network edge.

One challenge to this security architecture is large volumes of small IP packets created by mobile voice over IP, voice over LTE, and, in the future, Internet of things (IoT) applications. Depending on vendor and implementation, IP phone applications generate a voice packet every 10 ms to 40 ms with a payload of between 10 bytes and 320 bytes. This results in a data rate from each handset of up to 50 packets per second (for a 20 ms voice sample) many of them in the minimum IP packet length of 64 bytes.

While data payloads are small, the headers require the same amount of processing as any packet. The security gateway control plane must examine this flood of small packets and process each one in real time. This is a challenge for legacy appliance gateways, much less virtualized gateways.

To solve this challenge with a virtualized solution, Casa Systems teamed up with Intel and Intel Network Builders members Advantech and Wind River to develop a complete virtual gateway system that can be deployed by MNOs without additional integration.

Maximizing the performance of the solution for small-packet applications, scalability, and flexibility meant starting with a foundation of Advantech's dual-Intel® Xeon® CPU-based 1RU servers with Wind River's Titanium Edge providing the NFV infrastructure. This complete NFV server provides the processing power for the Casa Axyom* Ultra-Broadband Software Framework, which delivers the security gateway functionality. Figure 1 is a system architecture diagram of the solution.

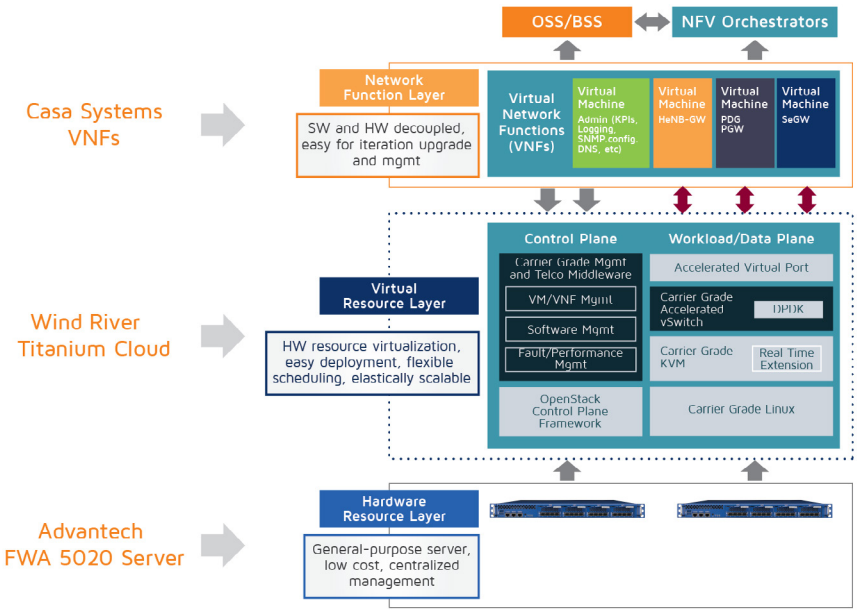

Figure 1. Virtual security gateway system architecture

The components of the solution include:

Casa Systems' Axyom* Ultra-Broadband Security Gateway

The solution is built around the SeGW component of Casa Systems' Axyom* Ultra-Broadband Software Framework. The Axyom framework is a virtualized multi-access solution that combines a carrier-grade NFV infrastructure with a suite of access and core functions such as the SeGW, evolved packet data gateway (ePDG), and others. Axyom is designed to deliver access functions for 3G/4G and trusted/untrusted Wi-Fi access.

The SeGW provides a scalable in-line security solution that has the capacity for millions of IPSec tunnels on a 1RU server. With independent scalability of subscriber sessions, encrypted throughput, and call event processing, the SeGW can be rapidly reconfigured to accommodate new bandwidth, signaling, and session throughputs. The SeGW is deployed in front of the evolved packet core (EPC) to protect the core network by encrypting, authenticating, and authorizing all data packets that pass through. The gateway has a capacity of up to 40 Gbps of full duplex throughput even with high volumes of small packets.

Intel Xeon Processors E5-2600 v4

The servers in the solution utilize Intel Xeon processors E5-2600 v4, Intel's processor platform for Internet of things and networking applications. Manufactured on Intel's 14 nm process technology, the devices feature increased memory bandwidth for fast data transfers for compute-intensive applications. Intel Xeon processors E5-2600 v4 have been developed for security applications with an enhanced security capability via improved data encryption that improves protection from attacks on data moving through the network.

The CPUs also have Intel® Resource Director Technology, which delivers more cache space to applications needing that space for improved NFV performance.

Another Intel technology that is critical to this security gateway solution is Intel® QuickAssist Technology, an encryption and compression hardware acceleration co-processor. The addition of Intel QuickAssist Technology in this product lets the gateway boost its encryption performance without consuming CPU cycles. This technology is used on the Advantech PCIE-3021, a PCI Express* card specifically designed with dual Intel® Communications Chipsets 8955 featuring Intel® QuickAssist Technology and optimized for the FWA-5020.[4]

Additional Axyom Security Gateway Specifications

- 3GPP systems aspect/security: 3GPP TS 33.320, 3GPP TS 33.310, 3GPP TS 33.210 and 3GPP TS 33.402
- Scalable IKEv2 and IPSec SA rekeying
- Firewall and advanced access controls, DDOS protection, IPSec /MOBIKE security associations
- X.509 certificate authentication for IoT embedded SIM applications
- IETF RFC 7383 support for fragmentation before encryption for IKE
- IETF RFC 4303 support for fragmentation before encryption for IPSec ESP

Additional Intel Xeon Processor E5 2600 v4 Specifications

- Core architecture advancements, up to 2400 MHz DDR4 memory speed and high I/O bandwidth combine for higher performance for a broad range of compute applications
- Intel® Transactional Synchronization Extensions (Intel® TSX) boost performance for multi-threaded workloads that are currently slowed by memory locking
- Integrated I/O include up to 80 PCIe* Gen3 lanes, up to 10 SATA Gen3 ports, and up to 14 USB ports to fulfill the design needs

Advantech FWA-5020

The server specified for the gateway product is the Advantech FWA-5020, a 1U rackmount server optimized for networking applications that features either one or two Intel Xeon processors E5-2600 v4 (the two-processor model was specified for the gateway). The servers can be configured with 12-to-22 core CPUs thanks to an advanced thermal system design that supports processor wattage of up to 145W.

The system architecture of the FWA-5020 puts an emphasis on compute performance, data plane throughput, and encryption throughput. Some of the optimizations include larger on-chip cache memories and Intel® QuickPath Interconnect, running at up to 9.6 GT/s for reduced cross-socket memory I/O latencies and increased throughput.

Figure 2. Advantech FWA-5020 configured as a Casa Systems Security Gateway

Memory support for each socket includes four DDR4 channels with speeds up to 2400 MHz for up to 512 GB of error correcting code (ECC) memory. To provide failover capability, the server features advanced reliability, availability, and serviceability (RAS) modes such as mirroring and sparing to increase platform reliability.

The enhanced system architecture with two PCIe* Gen 3 x8 slots per CPU for density-optimized network mezzanine cards (NMC) and one PCIe Gen 3 x16 slot per CPU for the Advantech PCIE-3021 card, with dual Intel Communications Chipsets 8955 featuring Intel QuickAssist Technology, provides Casa with an efficient platform for packet and crypto throughput in a reduced 1RU footprint. The balanced PCI Express design on each of the processor sockets, supporting network IO and security offload at the same time and with equal throughput, lays the foundation for high application performance.

For management, the server has two built in 1000Base-T ports, two USB ports, and a console port with advanced LAN bypass and two 10 GbE SFP+ ports. These built-in options can be augmented by the four front-loaded NMC slots that provide the ability to add additional modules.

Typical IT servers for enterprise and data center applications have lower throughput needs and as such are not architected with such high levels of performance in mind. A typical SeGW configuration offers up to 16 front accessible 10 GbE ports with quad DH8955 crypto acceleration.

Additional FWA-5020 Specifications

- Carrier Grade lights out management
- Remote firmware upgrade capability
- Hardware-based BIOS redundancy
- Front and rear hot swappable field replaceable units (FRUs)
- 2 x 2.5" SATA HDDs/SSDs
- IPMI 2.0 compliant remote management
- Two Advantech PCIE-3021 cards with dual Intel Communications Chipsets 8955 featuring Intel QuickAssist Technology supported (SKU dependent)
- Four NMC bays supporting 1 GbE, 10 GbE, and 40 GbE interfaces
- Two management Ethernet ports, a console port, two USB 3.0 ports

Wind River Titanium Edge

The NFV platform for the product is based on Wind River Titanium Cloud,* a fully integrated virtualization software platform with carrier-grade reliability and deployment-ready features. Specifically, the product integrates Titanium Edge, a version of the software that scales down to as few as two nodes. Like all Titanium Cloud software, Titanium Edge has built-in carrier-grade reliability features and verified compatibility with third-party VNFs from companies in the Wind River Titanium Cloud ecosystem.

The foundation of Titanium Edge is open source software including a hardened Linux* operating system and integrated OpenStack* for cloud computing functionality with Wind River additions that boost reliability and manageability in a carrier network. The software makes use of Ceph* for remote or local storage access or clustering.

On top of this foundation, Titanium Edge features real-time Kernel-Based Virtual Machine (KVM)* to create the NFV environment. Wind River has enhanced this KVM with reduced interrupt and timing latency for real-time performance. An accelerated virtual switch (vSwitch) is also integrated, which leverages the open source Data Plane Development Kit (DPDK) and virtual NICs for accelerated packet processing. With the DPDK integration, the vSwitch can process more packets for an increased virtual machine density per CPU core.

Additional Titanium Edge Features

- High reliability with fast, secure virtual machine failover
- Installation and Commissioning Simplicity
- Carrier-grade security including encrypted authentication, authorization, and accounting (AAA) database, network-level authentication, data protection via encryption
- Supports OpenStack* Enhanced Platform Awareness

Security Gateway Performance

The Casa Security Gateway built using the Intel Xeon processor-powered Advantech FWA-5020 with Wind River NFVI has been tested in lab and real-world applications and has delivered the following performance.[5]

- 1 million concurrent IPsec tunnels or 2 million IPSEC Security Associations
- 5,000 tunnels per second
- Dead peer detection (DPD) time of 120 seconds for 1M peers for fast detection and status of nearby gateways
- 100 Gbps IPSec throughput for 128 byte packets and 110 Gbps for 256 byte packets
- 2,000 tunnels per watt

This SeGW provides the high-performance edge solution required for MNO networks that need to provision millions of IPSec tunnels for millions of mobile devices. The performance of the gateway is ideal for the transient nature of mobile networks where devices attach and detach from the network frequently. The architecture of the Casa gateway features independent control plane and data plane functions so that MNOs can adapt each separately in response to different bandwidth, signaling, and session requirements.

Conclusion

Securing ultra-broadband mobile networks with security gateways at the network edge is an imperative for all MNOs who have adopted all-IP 4G/LTE networks. With the performance, throughput, and scalability provided by the Casa Systems gateway powered by Intel, Advantech, and Wind River, this is now a cost effective and viable option for MNOs or for equipment manufacturers who want to integrate this functionality into their networking systems.

About Casa Systems, Inc.

Casa Systems, Inc. provides fixed, mobile and Wi-Fi network solutions for ultra-broadband services. As the original supplier of commercially deployed CCAP systems that deliver voice, video, and data over a single port, Casa continues a tradition of bringing leading edge solutions to hundreds of service providers around the world. For more information, please visit http://www.casa-systems.com.

About Intel

Intel (NASDAQ: INTC) is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world's computing devices. As a leader in corporate responsibility and sustainability, Intel also manufactures the world's first commercially available "conflict-free" microprocessors.[6] Additional information about Intel is available at newsroom.intel.com and blogs.intel.com and about Intel's conflict-free efforts at conflictfree.intel.com.

About Advantech

Advantech Networks & Communications Group provides the industry's broadest range of communications infrastructure platforms, scaling from one to hundreds of Intel cores, consolidating workloads onto a single platform architecture and code base. Its technology leadership stems from x86 design expertise combined with high-performance switching, hardware acceleration and innovative offload techniques. For more information, please visit http://www.advantech.com/nc.

About Wind River

A global leader in delivering software for intelligent connected systems, Wind River offers a comprehensive, end-to-end portfolio of solutions ideally suited to address the emerging needs of IoT, from the secure and managed intelligent devices at the edge, to the gateway, into the critical network infrastructure, and up into the cloud. Wind River technology is found in nearly 2 billion devices and is backed by world-class professional services and award-winning

[1] http://www.4g.co.uk/how-fast-is-4g/

[2] International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.2, March 2015 (PDF download)

[3] https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf

[4] Advantech FWA-5020 Datasheet; http://www.advantech.fr/products/1-2jkcw8/fwa-5020/mod_4119f5b7-524e-461a-b36a-610882dcd405

[5] Tests performed by Casa Systems. Configurations: Tests used the Advantech FWA-5020 with two Intel Xeon E5-2600 v4 processors and dual Intel QuickAssist DH8955 adapters.

[6] "Conflict-free" refers to products, suppliers, supply chains, smelters, and refiners that, based on our due diligence, do not contain or source tantalum, tin, tungsten or gold (referred to as "conflict minerals" by the U.S. Securities and Exchange Commission) that directly or indirectly finance or benefit armed groups in the Democratic Republic of the Congo or adjoining countries.