Data Sheet

Casa Systems Axyom™ Ultra-Broadband Edge Security Gateway (SeGW)

Axyom™ Ultra-Broadband Edge Platform

The shift to all-IP and LTE networks introduces new security risks to mobile networks arising from an inherently more open architecture in which anyone with physical or logical access to an eNode-B can launch an attack. The densification of mobile networks and inclusion of unlicensed access to address increasing bandwidth demands further compounds security risks. Securing both subscriber data as well as signaling messages and core network elements is paramount. Service providers need to strengthen end-to-end network security at endpoints, in the transport network and in the applications themselves.

A majority of service providers have experienced DDoS attacks against their services or their customers, as well as infrastructure outages and bandwidth saturation. 2015 was a high water mark for the number and magnitude of DDoS attacks, with 25% of service providers reporting peak attack sizes over 100Gbps[1]. A variety of risk detection and mitigation solutions have been deployed as a result of this rising tide of attacks. They range from call center reports to firewall logs to network analysis tools. Particularly effective are in-line security solutions, which not only can detect, but also mitigate attacks.

Casa Systems' Security Gateway (SeGW) provides a simple, scalable in-line security solution that also yields high throughput. Capable of supporting millions of IPSec tunnels on a 1RU platform, the solution also scales control plane and data plane functions independently, allowing rapid adaptation to changes in bandwidth, signaling and session requirements. Deployed in front of the EPC, the SeGW protects the core by allowing only encrypted, authenticated, authorized traffic to pass through. Up to 40Gbps of full duplex encrypted traffic is achievable, even for large numbers of small packets (e.g, sensor based M2M or voice applications).

Casa's SeGW runs on Casa's Axyom Ultra-Broadband Edge Platform, which is a carrier-grade software architecture that provides the highest level of performance and control while assuring security, regardless of whether access is provided over a trusted or untrusted network. Fully redundant, Casa's solution enables service providers to provision a single instance of transport security to manage multiple concurrent services such as 3G+LTE or a WAG+ePDG to enable VoWiFi on community hotspots. The common security framework results in higher performance, simplified management and reduced transport costs.

Highlights

- **Transport security applications for Fixed/Mobile Broadband, Enterprise IOT, or Wi-Fi traffic – all with one SeGW instance**
- **Stand-alone security service or deploy with other Casa Systems products to secure RAN sharing, macro-RAN transport, small cells, MVNO/MVNE VoWiFi / IMS calling, inter-provider IMS / VoLTE roaming, Enterprise IoT, PBX replacement / SIP trunking**
- **1M tunnels per RU; high availability /inter VNF redundancy**
- **Industry-leading throughput for small packet sizes (e.g., M2M and voice)**
- **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**

casa systems

The SeGW is deployable in tandem with 3G + LTE small cell aggregation services, or as a stand-alone security solution for:

- Securing RAN backhaul from small cells, macro-RAN environments and /or fronthaul from Remote Radio Heads to the baseband pool, reducing transport costs and further securing leased fiber transport facilities from third parties or independently managed business units
- Enabling secure, high availability enterprise IoT applications, for remote monitoring and telemetry applications including vending machines, video surveillance, connected cars, and remote meter reading
- Securing transport for Wi-Fi calling for enhanced indoor coverage and increased service reach in unmanaged public hotspots
- Protecting against DDoS attacks to provide clean pipes for RAN sharing arrangements
- Protecting VoIP applications from DDoS attacks and mobile malware from BYoD in enterprise environments, enabling adoption of PBX replacement solutions
- Securing emerging applications from the 3.5Ghz Citizen's Broadband Radio spectrum. For example, in neutral host environments service providers will need to securely transport and authenticate the traffic from any enterprise visited roaming network as originating from an inherently untrusted data source.

The list of applications for Casa's SeGW continues to grow as we discover emerging security needs with our customers. For all these needs, Casa's SeGW delivers best-in-class number of tunnels per RU, tunnel setup rates, IPSec throughput and performance per watt, enabling cost-effective security of subscriber data and service provider networks.

[1]*Worldwide Infrastructure Security Report, Arbor Networks, January 2016*

Feature	Benefit
Density: **1M IPSec tunnels per RU**	Cost-effective security to address the growing number of connections
Performance: **40Gbps full duplex encrypted throughput**	High throughput of encrypted traffic, including for large numbers of small packets which occur with sensor-based M2M or voice applications
Robust Features: **Full range of firewall and filtering, DDOS, and IPSec features**	Protection of the network core and of user privacy – without impacting performance
Any Access: **Secure 3G / 4G or Fixed/Mobile Broadband, Enterprise IOT, or Wi-Fi traffic with one SeGW instance**	Lower TCO and improved agility with ability to scale up or down for changes in traffic with a single solution
Multi-purpose: **Deploy Casa's SeGW alone or in conjunction with other Axyom products**	Flexibility to deploy Casa's SeGW with other network functions including small cell gateways, ePDG, WAG, and EPC creates a multi-purpose alternative for service providers who want more choice at lower cost
Deployment Flexibility: **The SeGW can be deployed as an appliance or as part of a cloud system, at the metro or enterprise edge or in a centralized cloud**	Ability to deploy the SeGW where and how it makes the most sense in the network gives providers a solution for a growing array of security use cases.