Data Sheet

Casa Systems Axyom™ Security Gateway

The open architecture of all-IP core networks inherently means that service providers face security risks since anyone with physical or logical access to the network 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. In 2017, 87% of service providers reported that they had experienced DDoS attacks[1]. A variety of risk detection and mitigation solutions have been deployed as a result of this rising tide of attacks. These 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) is a virtualized solution running on x86 servers to provide 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 IoT or voice applications).

Casa's Axyom SeGW Virtual Network Function (VNF) is based upon Casa's Axyom Software 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. Casa's fully redundant solution enables service providers to provision a single instance of transport security to manage transport links between the service provider's core netowrk and small cells, macrocells, carrier Wi-Fi access points and peer networks. The common security framework results in higher performance, simplified management and reduced transport costs.

Highlights

- Virtualized 3GPP SeGW solution
- Secure transport links to small cells, macrocells, Wi-Fi access points and peer networks
- Transport security applications for Fixed / Mobile Broadband, Enterprise IoT, or Wi-Fi traffic - all with one SeGW virtual instance
- Standalone solution or integrated with other Casa solutions, such as Casa's virtualized Small Cell Solution (HeNB Gateway, HNB Gateway, SeGW) or Casa's WAG
- 1M tunnels per RU; high availability /inter VNF redundancy
- Industry-leading throughput for small packet sizes (e.g., IoT 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 Axyom SeGW is deployable in tandem with other Casa virtual functions or as a standalone virtutalized 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.
- Growing small cell deployments need secure, scalable transport between the small cells and the service provider core network. As mobile traffic continues to grow at high rates, small cell densification is needed. Unfortunately, the small cell locations and transport links cannot be secured. Thus, the use of a SeGW for small cell deployment is essential.
- Enabling secure, high availability enterprise IoT applications, for remote monitoring and telemetry applications including vending machines, video surveillance, connected cars, and remote meter reading
- Protecting all core networks against DDoS attacks.
- Securing emerging applications from the 3.5GHz Citizen's Broadband Radio spectrum (CBRS). The transport network between CBRS small cells and the core network must be secured. Also 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.
- Implementing a virtualized security function as an integrated element within other Casa virtual solutions, such as Casa's Small Cell Core or Wireless Access Gateways (WAG).

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]*NetScout Arbor's 13th Annual Worldwide Infrastructure Security Report, 2018*

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 Small Cell 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: Axyom SeGW VNF can be deployed on bare metal, as a virtual machine or in a container. The Axyom SeGW is location independent and can be deployed at the enterprise edge or in a centralized data center	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.