Data Sheet

Casa Systems Axyom™ ePDG

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.

Service providers are striving to meet this burgeoning demand with new, differentiated and profitable services. Incorporating cellular as well as trusted and untrusted Wi-Fi with applications, such as Wi-Fi Calling (a.k.a.VoWiFi), into their portfolios opens up new opportunities for service providers.

As the figure on the next page shows, VoWiFi calls are controlled by the IMS core, as a result encrypted IPSec tunnels must be established between the UE and the core network to ensure that the voice bearer and signaling from a untrust Wi-Fi access network is secured prior to traversing the core. The ePDG provides the secure interworking between the untrusted Wi-Fi world and the secure core network.

Casa Systems' ePDG 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 x86 server, the solution also scales control plane and data plane functions independently, allowing rapid adaptation to changes in bandwidth, signaling and session requirements. The ePDG protects the core by allowing only encrypted, authenticated, voice calls to pass through to the PGW. Up to 40 Gbps of full duplex encrypted traffic is achievable, even for large numbers of small packets used for VoWiFi.

Casa's Axyom ePDG Virtual Network Function (VNF) runs on Casa's Axyom Software Platform, which is a carrier-grade software architecture that provides the highest level of performance and control while assuring security over an untrusted Wi-Fi access network.

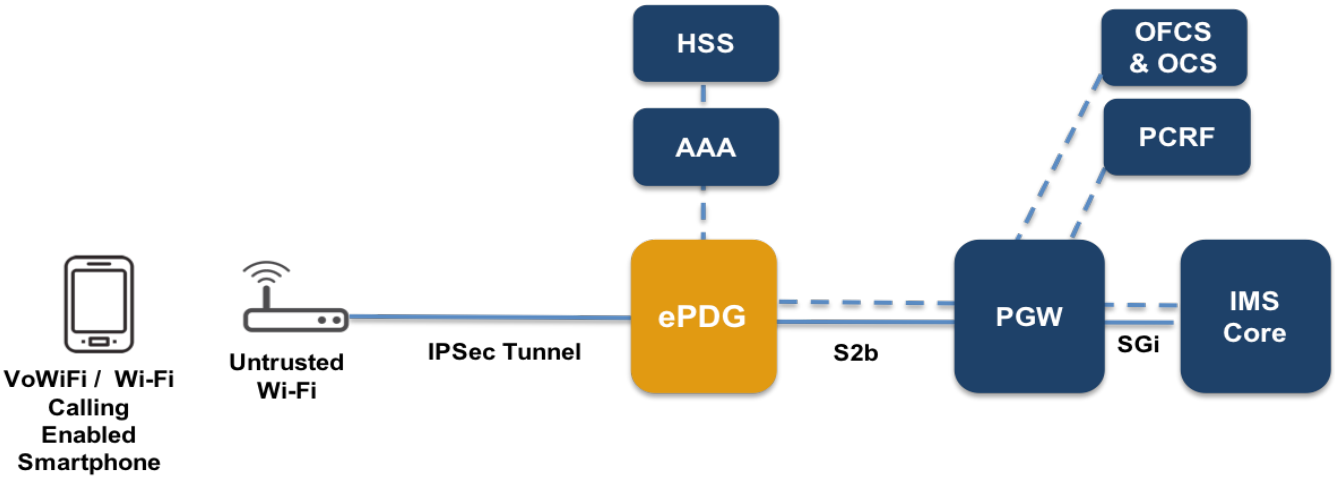
Highlights

- Virtualized 3GPP ePDG solution running on x86 servers
- Leverage existing Wi-Fi access to securely expand voice coverage with Wi-Fi Calling / VoWiFi
- Enhanced customer experience with seamless, secure mobility between VoWiFi and VoLTE
- 1M tunnels per RU; high availability / inter VNF redundancy
- Firewall and advanced access controls, DDOS protection, IPSec / MOBIKE security associations
- Support for UICC / Non-UICC clients EAP-AKA, EAP-TTLS, EAP-MSCHSPv2, X.509 certi icates with OCSP
- Handover: MOBIKE (RFC 4555, TS23.402), VoLTE - VoWiFi
- IETF RFC 4303 support for fragmentation before encryption for IPSec ESP
- The Axyom ePDG can be deployed on bare metal, as a virtual machine or in a container

casa systems

Casa Systems' Axyom ePDG virtualized solution is highly reliable and carrier-grade, with all the features service providers need to extract the benefits from Wi-Fi Calling / VoWiFi, without the risks. Positioned between the untrusted Wi-Fi access network and the mobile core (PGW), Casa's ePDG:

- Authenticates the UE attempting to attach to the core
- Secures the data transmission between the UE and the EPC over an untrusted non-3GPP access
- Acts as a termination node of IPSec tunnels established with the UE
- Applies real-time subscriber, session and application intelligence
- Enables service providers to extend wireless voice service coverage, reduce the load on the macro wireless network, and makes use of existing backhaul infrastructure to reduce the cost of carrying wireless calls
- Enables service providers to offer secure VoWiFi with seamless mobility to VoLTE



Feature	Benefit

Carrier-Grade Security	• Firewall and filtering
	• DOS and DDOS detection, protection and prevention
	• Anti-spoofing
	• Subscriber session limits
	• IKEv2 with certificate based authentication
	• IKE and IPSec SA rekeying
	• Multiple child SA support
	• Diffie-Hellman Groups 1, 2, 5 and 4
	• Dead Peer Detection (DPD)
	• IKE and IPSEC rekeying
	• Supports Encapsulating Security Payload (ESP) tunnel mode
	• Extensible Authentication Protocol (EAP)
	• Supported encryption and authentication algorithms
	  • MAC-MD5-96
	  • HMAC-SHA1-96
	  • AES-128-CSC
	  • AES-192-CSC
	  • DES-CBC
	  • 3DEC-CBC
	  • PRF-AES-128-CBC
	  • AES-128, 192 and 256
	  • Null encryption
	• AAA interface for EAP-AKA authentication
	• Pre-shared keys and certification (X.509)
	• Real-time logging and statistics

High Availability + Redundancy	• 99.999% availability • In-service software upgrades • Geographical redundancy • Automatic failover • Session recovery • Stateful intra-chassis redundancy
Scaling and Performance	• Scales to 1M tunnels per RU • Security, encryption and authentication applied to every packet with no degradation of performance•Independent scaling of CEPS, sessions and throughput
Intelligence Applied	• Real-time integrated subscriber, session and application intelligence which can be applied for both network optimization and for monetization of new services

100 Old River Road | Andover, MA 01810 | Tel: 978.688.6706 | www.casa-systems.com