

## Mobile Network Security: The Threat of Convergence & IMS

### EXECUTIVE SUMMARY

This report analyzes the mechanisms used to integrate alternative IP-based access into the mobile packet core and tracks the evolution of today's security-focused gateway products into "service anchor nodes" capable of supporting security, mobility, and policy enforcement across network domains.

The focus is on how the move by wireless operators to embrace alternative access networks is driving demand for a new category of convergence gateway equipment as they seek to address unfamiliar security and IP mobility challenges.

Initial security gateway deployments are focused around Unlicensed Mobile Access and wireless local-area network interworking, where there is a need for tunnel-terminating gateways with enhanced security features such as firewalls, denial-of-service protection, and intrusion detection systems. Other requirements, such as fast tunnel setup, massive scalability, and the ability to support large numbers of secure tunnels switching rapidly between active and inactive states, also are driving the need for a new generation of equipment.

Equipment deployed today, however, needs a clear product roadmap. The next phase of development will see IP Multimedia Subsystem (IMS)-capable Packet Data Gateways and Packet Data Interworking Function devices take on a more advanced mobility management role, and, potentially, offload Session Initiation Protocol security tasks from Proxy-Call Session Control Function in IMS architectures.

Equipment suppliers and network operators also are developing the requirements for the next-generation mobile core network being defined in the third-generation System Architecture Evolution (SAE) standards groups. As well as providing a low-latency packet core for the next generation of radio access systems, SAE identifies support for multi-access network services using a variety of access selection techniques and device types, including multi-radio terminals, as a key objective.

Among the highlights of the report:

- Convergence gateways offer security for the multi-access mobile core; later evolutions will enforce QOS, manage mobility, and act as service anchor points across IP networks
- Mobile operators want security architectures that unify the transport, access, and services layers to streamline management and vendor relationships
- Services-layer security players are well positioned to determine mobile security architectures, but uncertainty remains on how to implement security in converged networks
- Major equipment providers will partner with security and IP networking specialists until market requirements and demand are clearer
- Evolved packet data gateways with Mobile IP and Mobike support will be offered in 2007

The majority of vendors use ATCA-based platforms, often with customized backplanes and custom-built processor boards, for convergence gateway products; others use proven edge router or GGSN/PDSN platforms. Vendor product platforms are summarized below (names excised):

**Excerpt: Summary of Security Gateway Products**

Company	Back-ground	Platform	IPsec Blade	Performance	Security Services	AAA Server	Applications
[name excised]	CDMA RAN	Custom 14-slot ATCA chassis	Custom-built on ATCA form factor	Up to 160,000 active sessions	Integrated on each blade	No	PDG/PDIF by mid 2007; may be used as UMA security gateway
[name excised]	Startup	14-slot ATCA chassis	Off-the-shelf ATCA	Up to 500,000 IPsec sessions	Integrated on each blade	Yes, Service Control Node	TTG-mode PDG; UMA security gateway; PDIF by end 2006; PDG in 2007
[name excised]	Routing, security, mobile packet core	Catalyst 7600 Edge Router (13-slot chassis)	Custom-built	Not revealed	Individual firewall, IDP, and DOS blades	Yes, Cisco Access Registrar	UMA security gateway and TTG-PDG in early 2007
[name excised]	Service provider and govt. security	Custom 8-slot, 4U chassis	Custom-built	16 Gbit/s of VPN throughput; 400,000 concurrent IPsec sessions	Integrated on each blade	No	UMA security gateway; may develop TTG-mode PDG
[name excised]	Session border controllers	Currently custom fixed config.; moving to 14-slot ATCA	Currently custom-built; moving to ATCA	20 Gbit/s of VPN throughput; 300,000 concurrent IPsec sessions	Integrated on each blade; SIP security modules	No	UMA security gateway, TTG-PDG, P-CSCF, SBC on common platform by end 2006
[name excised]	Managed security services gateway	Custom chassis	Custom-built	5 Gbit/s of VPN throughput; up to 1 million concurrent media sessions; 150,000 active users	Integrated on each blade; media and control-layer security	No	UMA security gateway, IMS security gateway
[name excised]	Mobile packet core	Custom chassis; new platform by early 2007	Custom-built	Not revealed	Integrated on each blade	No	PDG/PDIF applications planned
[name excised]	Startup	Custom 5-slot ATCA chassis; 14-slot planned	Custom-built on ATCA form factor	16 Gbit/s of VPN throughput, 256,000 concurrent IPsec tunnels	Integrated on each blade	No	Not revealed
[name excised]	Startup	2U fixed config.; 14-slot ATCA planned	Intel server platform	Not revealed	Integrated	Yes	Primarily AAA today; TTG-PDG planned for mid 2006

Source: *Unstrung Insider*

Companies analyzed in this report include: Airvana Inc.; Azaire Networks Inc.; Check Point Software Technologies Ltd. (Nasdaq: CHKP); Cisco Systems Inc. (Nasdaq: CSCO); Clavister AB; Fortinet Inc.; Juniper Networks Inc. (Nasdaq: JNPR); Netrake Corp.; Reef Point Systems Inc.; Starent Networks Corp.; Stoke Inc.; and Tata Systems Inc.

**Mobile Network Security: The Threat of Convergence & IMS**, a 26-page report in PDF format, is available as part of an annual subscription (12 monthly issues) to *Unstrung Insider*, priced at \$1,350. Individual reports are available for \$900.

To subscribe, please visit: [www.unstrung.com/insider](http://www.unstrung.com/insider).

For additional information and details of multi-user licensing options, please contact:

Jeff Claudino  
Director of Sales  
*Insider* Research Services  
619-229-9940  
[claudino@lightreading.com](mailto:claudino@lightreading.com)