



GENBAND's S2 Security Gateway allows mobile operators to offer secure, scalable fixed mobile convergence solutions, including femtocells and FMC/WiFi/WLAN solutions, advancing high quality voice and multimedia services to residential and business subscribers at their homes or places of work. For the mobile operator, femtocells and FMC pose significant security threats since these services typically use the public Internet for communication into the mobile core network. Use of the Internet for backhauling voice and multimedia traffic exposes the operator's core network to numerous types of IP-based attacks and exploitations, and user privacy is also at risk of being compromised. The S2 Security Gateway ensures that femtocell/FMC communications can travel securely over untrusted networks like the Internet, into the mobile core network.

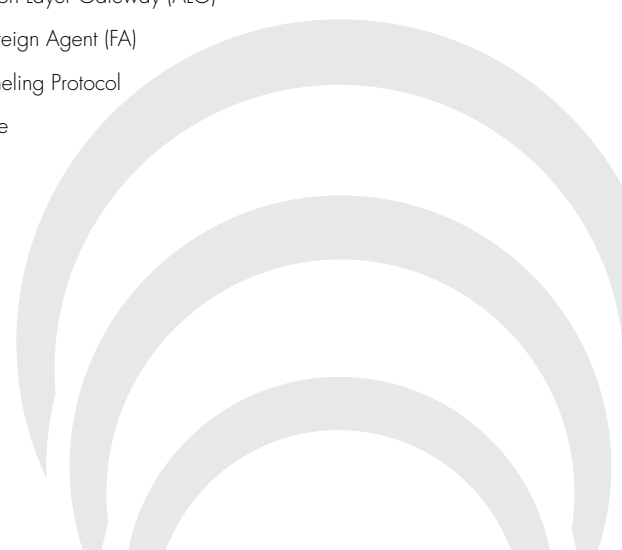


The S2 protects the mobile operator's network and ensures user privacy by leveraging state-of-the-art security technologies. Based on a carrier-class Advanced Telecom Computing Architecture (ATCA), the S2 uses purpose-built Security Gateway modules that reside in GENBAND's 2-slot Integrated Border Gateway chassis. The S2 offers full high-availability (HA) with sub-second failover and supports hot-swappable components, with in-service platform upgrades. Highly scalable in a small form factor, it can reach up to 200,000 IPSec tunnels and 500 tunnels per second setup. In femtocell/FMC networks, the S2 platform provides security, user authentication, mobile-IP connectivity management, secured tunnel management, policy enforcement, and accounting. It monitors each femtocell/FMC connection for IP intrusion and attacks, and filters and firewalls mobile control protocols. The S2 manages mobile traffic flows from the femtocell/FMC access point into the mobile core network. Voice traffic is forwarded to the Mobile Switching Center (MSC) or Call Session Control Function (CSCF) where call treatment takes place, and multimedia traffic is forwarded to the Packet Data Serving Node (PDSN) in a CDMA network or to the Gateway GPRS Support Node (GGSN) in a GSM/UMTS network.

The S2 Security Gateway enables choice and flexibility for femtocell/FMC deployment models that best fit the operator's business and technical requirements. Open standards compliance with IETF, IMS, and 3GPP/3GPP2 allows flexible options for deploying femtocell/FMC services - operators can start with a traditional MSC service model and migrate to architectures such as IMS and LTE. In GSM/UMTS networks, the S2 is a Tunnel Termination Gateway (TTG), and in CDMA networks the S2 functions as the Packet Data Interworking Function (PDIF). The S2 Security Gateway also addresses the technical gaps not addressed by the GGSN or the Packet Data Serving Node (PDSN).

BENEFITS OF THE S2 SECURITY GATEWAY

- Supports 2G, 3G and IMS/LTE deployment models across GSM/UMTS and CDMA networks
- Splits and grooms voice and data traffic
- Firewall and filtering
- DoS detection and protection
- IP access routing
- IPSec IKEv1 and IKEv2
- Up to 200,000 IPSec tunnels per gateway
- Up to 500 IPSec tunnels per second per gateway
- Dead peer detection (DPD)
- 3GPP and 3GPP2 I-WLAN standards compliant
- SIP Application Layer Gateway (ALG)
- Mobile-IP Foreign Agent (FA)
- Generic Tunneling Protocol
- AAA Interface





IP SECURITY AND ENCRYPTION

- **IPSec Tunnels:** To 200,000 per S2 gateway
- **PSec:** RFC 2401/4301 series – IKE, IKEv2 and manual setup of security associations
- **Encapsulation Security Payload (ESP):** DES, 3DES, AES encryption; integrity algorithms: SHA-1, MD-5
- **Extensible Authentication Protocol (EAP) and EAP-SIM:** RFC 3748; draft-haverinen-pppext-eap-sim-1.6.txt; draftarkko-pppext-eap-aka-1.5.txt
- **Internet Key Exchange (IKE):** Pre-shared secrets and digital signature authentication; RFC 2407; RFC 2408; RFC 2409; RFC 4306; RFC 4307; RFC 3947, negotiation of NAT-T
- **Roaming:** RFC 2486, Network Address Identifier (NAI)
- **Security Gateway:** For securing subscriber and device to remote device; distinct virtual gateways and independent policies per subscriber
- **IPsec Clients:** iQSecure and compatible with SafeNet, SSH, supports XAUTH, MODE-CFG and NAT traversal
- **Digital Certificates:** X.509v3
- **Encryption/Decryption Performance:** Full line rate per interface simultaneously on all ports

FIREWALL SECURITY

- **Firewall Filtering:** Tailored subscriber firewall services at up to line rate per flow; filtering based on IP and transport headers with wildcards and masking, and on application type with stateful packet inspection; permit and deny filters
- **Stateful Packet Inspection:** TCP, UDP, ICMP, and IP
- **Application Layer Gateways:** For FTP, SIP, ICMP and other portagile applications
- **Concurrent Rules and Flows:** over 160,000 stateful flows
- **Per-Flow Mirroring:** Stateful mirroring of traffic flows for use with IDS systems on a per-subscriber per-firewall rule basis
- **Statistical Thresholding:** DOS/ DDOS attack detection
- **DOS and DDOS Attack Prevention:** Protection against common attacks, including SYN flood, LAND attack, SMURF, Ping of Death, and fragmentation attacks
- **Subscriber Session Limits:** Adjustable session limits prevent resource exhaustion and DOS/DDOS attacks
- **Anti-Spoofing:** Protects against subscriber address spoofing
- **Real-Time Logging and Statistics:** Logging of rule hits and violations in real-time; detailed session statistics. Firewall logs are WebTrends compliant
- **Subscriber Identification Rules:** Recognized by source/ destination IP prefix, IP address, next/ previous hop, incoming/outgoing tunnel, Virtual Router, and logical interface; a subscriber may be a site, host, network, or user
- **DiffServ:** Full implementation; RFC 2474, RFC 2475, RFC 2597, RFC 3246 and RFC 3247

- **Per Hop Behaviors (PHBs):** Defined by Weighted Random Early Detection (WRED) queue admission control, drop precedence, queue priority, queue weight, delay bound, service type (UBR and CBR), and Layer 2 priority
- **Service Classes:** Customizable based on Profile Action Sets (of 3 PHBs) allowing for special handling of out-of-profile traffic; several predefined standards-compliant service classes
- **Traffic Policing:** Dual token-bucket policing; two-rate three-color marker (RFC 2698); color aware and color-blind modes; applied to each service class instance; metered against provisioned traffic parameters
- **Class-based Link Sharing:** Prioritized Weighed Fair Queuing (PW/FQ) with WRED; WRED/queue parameters set by service class definitions
- **Traffic Shaping:** Transport-independent traffic shaping on output; enables CBR services
- **IP Explicit Congestion Notification:** RFC 2481; may be enabled or disabled
- **Statistical Thresholding:** SLA monitoring

ROUTING AND ADDRESS MANAGEMENT

- **Dynamic and Static NAT:** One-to-one IP address mapping; enabled per subscriber; RFC 1631, RFC 2663; detailed session statistics; NAPT: Multiple subscribers / hosts mapped to a single shared IP address; detailed session statistics
- **Mode-CFG:** Per Virtual Router Address pools for IPsec Remote Clients
- **Dynamic Address Assignment:** IPCP negotiation; DHCP relay with option 82; RADIUS attributes
- **Up to 682 802.1Q VLANs**

SERVICES AND SYSTEM MANAGEMENT

- **High Availability Stateful Failover of IP Sessions:** Sub-second fail-over with IP session state maintained during failover
- **GenView Management:** Industry-standard CLI; Complete configuration and monitoring; multiple access privilege levels; access via Telnet, Telnet with IPsec, and SSH; management firewalls and ACLs; RADIUS authentication; full audit trail
- **Events and Alarms:** SNMP Monitoring: SNMP v1/v2; relevant MIBs – System, Environmental, IPsec, and Firewall; Multiple Syslog servers, SNMP traps, and Telco alarm panel connections
- **Accounting Data:** Comprehensive real-time traffic statistics collected by subscriber and service (VPN, firewall, QoS, etc.); interface and backbone statistics via standard MIBs; historical service auditing, RADIUS accounting