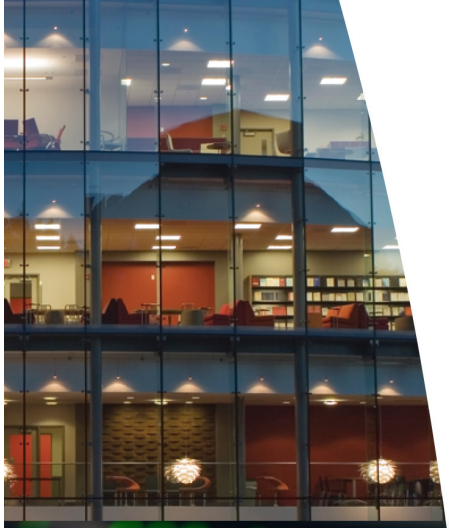

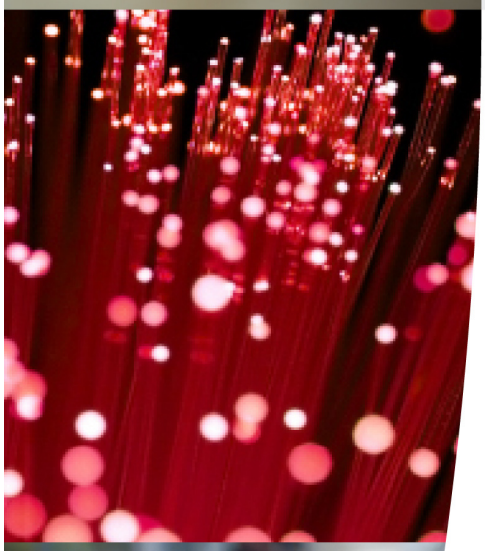

GENBAND

Securing VoIP Networks

GENBAND's multi-layer security architecture and threat mitigation solution

White Paper
February 2011

Executive Summary

The introduction of VoIP solutions for fixed and mobile networks creates opportunities for new services as well as service network delivery. However the adoption of VoIP also brings with it the inherent security vulnerabilities of IP. This paper describes security vulnerabilities and threats that exist in VoIP networks such as Denial of Service (DoS) attacks, theft of service and many others. To mitigate these vulnerabilities GENBAND has implemented a multi-layer security architecture and threat mitigation solution to protect service provider networks.

VoIP based services are accelerating at an increasing rate for both fixed and mobile operators. This growth has created significant new opportunities for consumers, enterprises, network operators and service providers. Yet at the same time, the very open nature of IP networks that has enabled the success and growth of the Internet has also made it vulnerable to a growing number of increasingly sophisticated on-line threats. In fact, the Internet's direct peer-to-peer communication has presented an open invitation to hackers to try to disable services and user endpoints.

Infonetics, a leading communication research company, estimated that in 2010 there were approximately 150 million VoIP subscribers. Additionally, enterprises are migrating to IP-enabled their communication infrastructure and terminating their voice traffic using SIP Trunks with service providers. A large portion of worldwide traffic that was once served by the PSTN is now being served by VoIP service providers at an ever increasing growth rate. Clearly the transition to VoIP and the use of IP networks is nearing a key threshold that will open up significant opportunities for service providers.

While service providers have had to deal with traditional issues such as providing service delivery and managing traffic congestion for the PSTN, today's service provider is confronted by a far broader and increasingly dangerous set of network-based risks. These risks involve attacks directed at the subscriber, the network and the application with the intention of bringing down the network or controlling its resources. The most common and difficult threats include Denial of Service (DoS) attacks, fraud, and theft of service. These attacks can cost businesses millions of dollars of downtime, lost revenue, and productivity. Fortunately there is a security solution that is designed to protect service provider's networks which is standardized and supports VoIP and multimedia services.

The session border controller (SBC) has been defined as the first line of defense for the service provider. While the SBC provides many other functions and capabilities, security is a key requirement and function for protecting service provider networks. GENBAND provides the industry leading SBC with a built-in multi-layer security architecture which protects the service provider's customers, network and application layers for real time services such as VoIP and multi-media.

Introduction

The rapid growth of VoIP traffic provides new service and network deployment opportunities for service providers. The VoIP architecture offers service providers a quick and flexible way to deliver a seamless user experience wherever and however the service is accessed. These services are interconnected at peering points from which networks exchange VoIP and multi-media traffic. These peering points are also IP borders and create a point from which malicious attacks can be directed at the service provider network.

As shown in Figure 1, traditional firewalls are not sufficient in dealing with real time multimedia sessions and are limited to securing IP traffic for internet applications such as web browsing and file downloads. Session border controller (SBC) is designed to protect VoIP and multimedia sessions by providing a pluggable dynamic policy model that establishes a policy binding for each application and device. The session is monitored and analyzed in real time and corrective action is dynamic. GENBAND S-Series SBC comes with a high performance network processor that provides processing power to prevent any intrusion attack at high call rates.

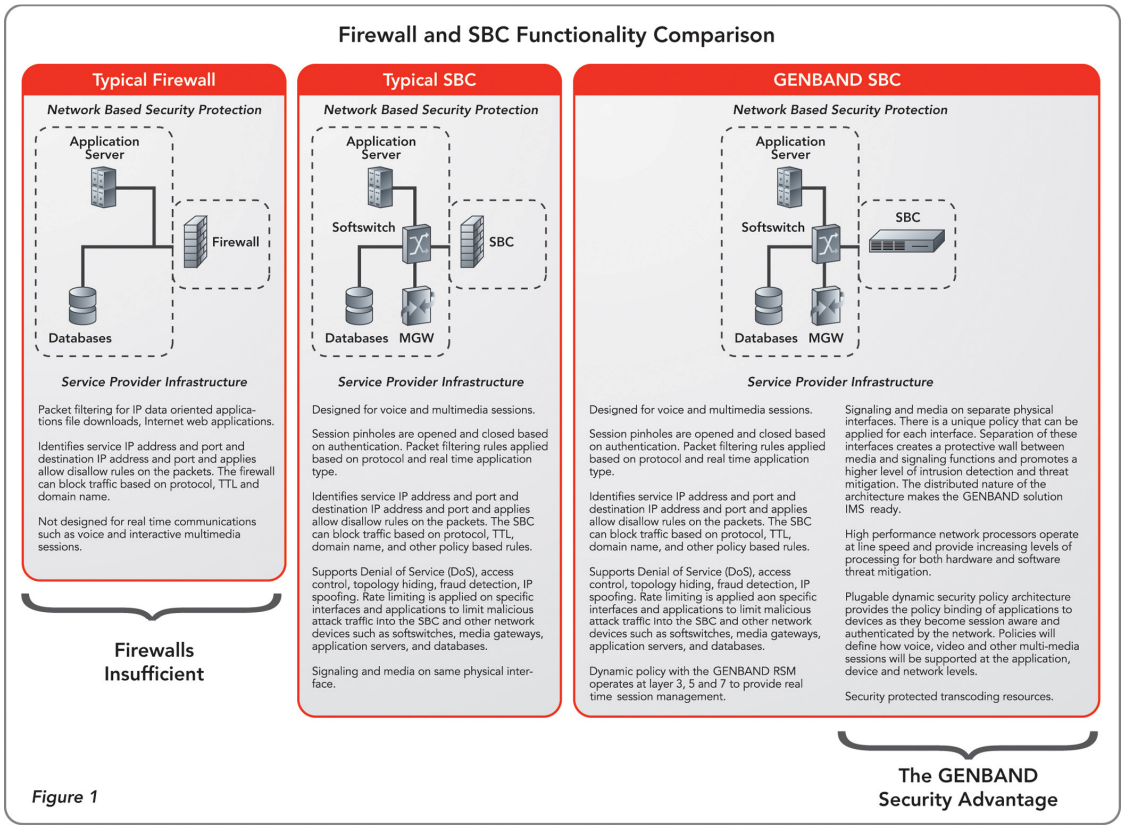

Figure 1

The SBC is positioned at the IP network border and peering point to protect many types of service provider networks. The SBC provides the security function for both fixed and mobile networks including residential and business, federated exchanges, directory and contact centers.

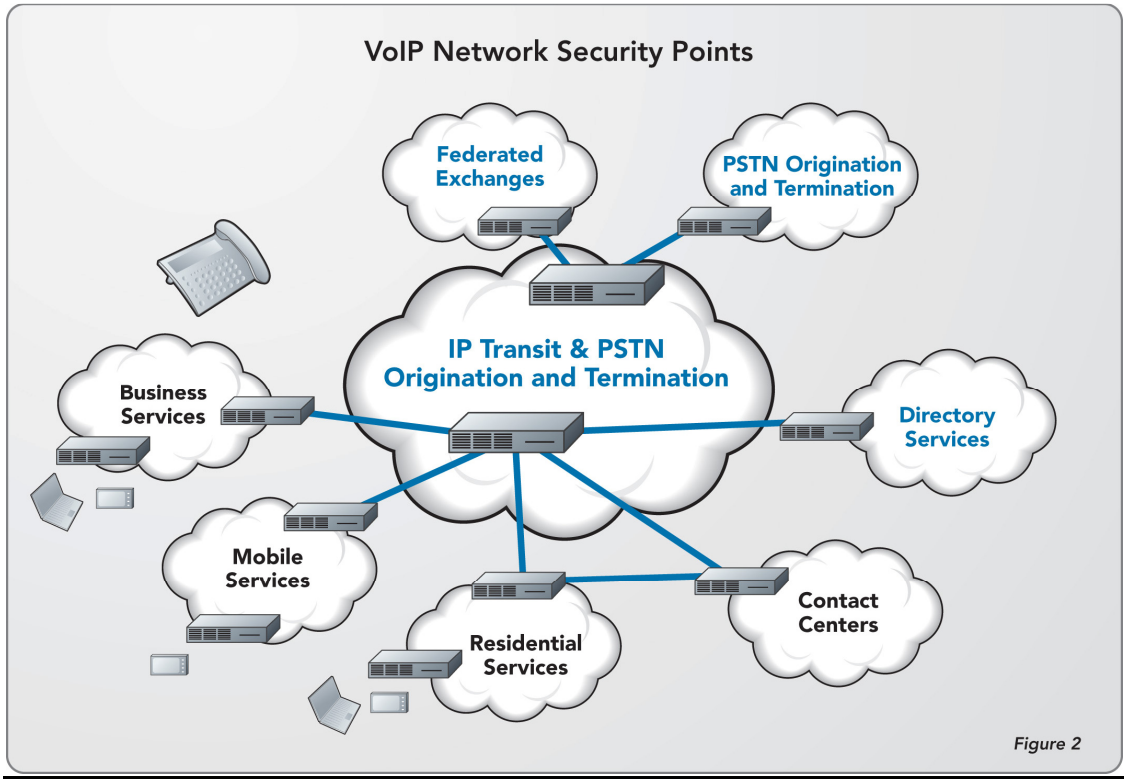

Figure 2

New Threat Environment for Service Providers

The very open nature and flexibility of IP networks also creates opportunities for malicious threats. Denial of service (DoS) and distributed denial of service (DDoS) attacks are becoming common every-day threats for service providers. While attacks on IP based services continue to increase both in volume and cost impact, so does the value of those services to the provider. As usage of real-time VoIP, video and multimedia services grows, they become a more prominent target for intrusion. Loss of VoIP service is more than just loss of revenue; it can also include loss of productivity, brand loyalty and tarnished reputation.

Attackers have three primary objectives when seeking to compromise a network: disruption of service, theft of service, and violation of privacy. Attackers have become very sophisticated in their methodology by creating access through open network ports and launching multi-level attacks at the network. Common examples include:

- Attackers can disable a trusted host and assume its identity - a threat know as IP spoofing or session hijacking
- Attackers can take advantage of weak authentication to gain access to the network exposing it to 3rd party applications
- Man-in-the-middle attacks where the attacker intercepts messages between a client and server and tricks the original entities into thinking they are connecting with each other
- Application level theft
- Infrastructure disclosure
- DoS and Distributed DoS Attacks - Flooding of the network device or infrastructure elements. Attacks include:
    - ICMP Floods
    - TCP Syn Floods

- Ping of Death Floods
- Registration Message Floods
- SIP Invite, Response Message Floods
- ARP Response Floods
- Unintended attacks due to network misconfigurations
- Malformed messages and buffer overflow

Traditional Methods are Inadequate

Traditional methods such as using a static firewall are not equipped to support real time communications requirements such as VoIP or multimedia services. These traditional security systems simply do not provide an acceptable level of protection against the robust attacks and unauthorized access attempts that are common in today's real-time, peer-to-peer communications environment. This situation creates a multi-fold problem. First firewalls that block unsolicited traffic across IP boundaries will not work with dynamically assigned port ranges. Secondly policy management changes that affect RTP and RTCP pin hole configurations will be too great for a traditional firewall. And finally, inbound calls do not have visibility to the private address of the phone they are attempting to reach. As a result, the phone will not even ring, and work-arounds that attempt to address this problem risk compromising network integrity.

GENBAND's SBC Security Framework

The session border controller is in a unique position to defend the service provider's infrastructure from attack and overload, since it provides the first point of communication and defense at the edge of the network. GENBAND's security framework identifies the requirements that a session border controller must satisfy to protect the SBC itself; to protect the service infrastructure (ie SIP servers, application servers, softswitches, media servers or media gateways); and to protect user/subscriber, enterprise and applications. The SBC provides the following key security functions: DoS, DDoS and overload protection, access control, topology hiding, service partitioning and theft protection, monitoring alarming and reporting analytics.

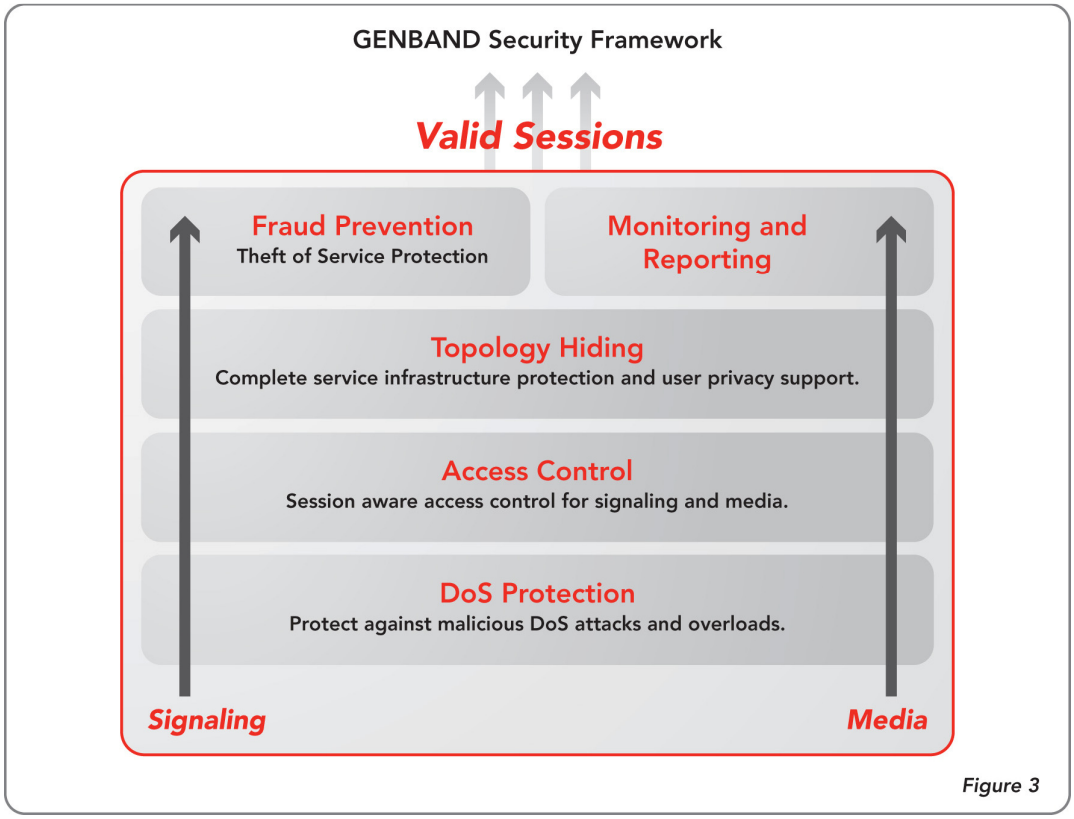

Figure 3

GENBAND's Security Solution

GENBAND's session-based security approach provides a complete protection framework incorporating self-aware security features. Advanced features integrated within this architecture can include early rouge detection (ERD), late rouge detection (LRD), customer authentication and authorization, protocol and media validations, signaling rate throttling, topology hiding and intrusion prevention. All traffic is scanned at wire speeds and examined for patterns across packet boundaries to discern legitimate sessions and to identify and shut down security attacks. Illegitimate session attempts can thus be filtered out before they disrupt network traffic.

SBC Denial of Service (DoS) Protection: The SBC incorporates automatic protection against malicious and non-malicious attacks and overload conditions. Designed specifically for DoS protection for Service Provider infrastructures, this approach provides deep packet classification for signaling and media streams at Layer 2 through Layer 7. Transaction rate limiting is used to ensure that SIP devices on the secure side are not flooded with valid SIP requests from authorized and unauthorized sources. The SBC is self-protected at Layer 3 and Layer 4 against signaling floods. Early rogue and late rogue detection methods protect against fragmented and malformed messages.

Access Control and Confidentiality: Session-aware access control for signaling and media using static and dynamic permit/deny ACL's at layer 3 and 5 has been implemented. Protocol validation though the use of protocol syntax checking, formatting, and proper sequencing of IP protocols filters out in-valid or potentially security intrusions. Protocol validation can be used to prevent IP fragmentation attacks, SYN resource starvation attacks and ICMP floods. Digest authentication using a challenge response method requiring a shared secret is based on the MD5 authentication algorithm. GENBAND

software/hardware platforms are adapted to support industry-standard encryption methods such as TLS, IPSec and SRTP to provide confidentiality and security.

Topology Hiding: Infrastructure topology hiding is provided at all protocol layers for confidentiality and attack prevention security. Topology hiding within signaling packets is provided to ensure the service provider's VoIP infrastructure is not advertised.

Service Partitioning and Theft of Service Prevention: The security framework supports a wide range of fraud prevention, including session-based authentication, authorization, and contract enforcement for signaling and media and service theft protection. Within this framework, every session passes through authentication (customer identification) and authorization (within customer-defined service subscription) before a session is admitted to the network.

Authentication is managed through an operator-controlled process, in which customers are identified by defining an IP address or a range of IP addresses that a legitimate customer might use for session origination or termination. Signaling in the system is processed in virtual partitions to ensure that every user is given fair access to network resources. This insures that user traffic is kept totally separate and eliminates the need for dedicated SBCs for each customer.

Service Infrastructure DoS Protection: The GENBAND S-Series SBC provides protection against malicious and non-malicious attacks and overload conditions that are directed at the infrastructure. Signaling and media overload control; deep packet inspection and call rate throttling are used to prevent DoS attacks from reaching service infrastructure such as SIP servers, application servers, softswitches, media servers or media gateways.

Media and Signaling Separation: The separation of signaling and media enhances the overall security solution. Media and signaling separation provided with overload control and media validation work to prevent DoS attacks, including malicious RTP. Deep packet inspection allows filtering and discarding of packets of inappropriate size, and ensures the size of packets does not change during a valid session. The solution also ensures that media packets are arriving at a valid rate and discards packets with known attack signatures. Signaling rate throttling is used to police the amount of transactions per second forwarded to an element in the service providers network preventing DoS attacks such as INVITE flooding. At the signaling stack layer messages field-level semantics, message sequencing and timing will not cause fault in
your internal application server, softswitch, NGN core or IMS network. This protection mechanism ensures that potentially damaging signaling won't be transparently passed on to other network elements

Monitoring and Reporting Analytics: A broad range of monitoring and reporting information is provided to the service provider. Event logs on a call by call basis, reporting and alarming, CDR's, call quality scoring and lawful intercept capability.

Call Admission Control: The call admission control (CAC) capability provides the ability to throttle users and networks (signaling and media) from consuming scarce network resources either from malicious or accidental reasons. As an example RTP streams that exceed negotiated or configured rates are throttled to ensure fairness of allocation of media bandwidth.

A summary of the security threats and how the threats are mitigated by SBC is shown below:

Security Threat Environments

SBC Security Threat and Protection Model Summary

Security Threat	Protection Method
Denial of Service ■ Call Control Message Floods ■ Malformed Requests ■ Distributed Attacks, Authorized and Unauthorized	■ Intrusion Prevention - VoIP Firewall ■ Access Control and Deep Packet Classification ■ Policy Establishment - Dynamic Allow and Deny ■ Rogue Packet Detection ■ Bandwidth Policing and RTP Header Validation
Fraud and Theft of Service ■ Illegitmate Access and Use of Resources will Compromise Service Level Agreements ■ Attacks on Subscriber Identity ■ Man in the Middle Attacks	■ Strong Authentication ■ Per Flow Bandwidth Policing ■ Bandwidth Based Admission Control
Impersonation and IP Spoofing	■ Strong Authentication ■ Correlating IP Address on the Bearer Level with Public and Private Identities

Figure 4

GENBAND's Technical Solution and Architecture

The GENBAND solution is comprised of three key elements:

- A high performance hardware platform capable of deep packet inspection at wire-rates on all physical interfaces on signaling and media traffic. The media processor is capable of encryption at wire-rates.
- Separation of signaling and media in hardware and software.
- An advanced software architecture that addresses security threats at multiple layers in call processing.

The Hardware Platform: Uses the most advanced server CPUs for signaling and network processors for media. This allows for deep-packet inspection and processing at wire-rates for both signaling and media. The platform allows for the protection of service even at extremely high rates of attacks. The processors also support wire-speed encryption on both signaling and media.

Separation of signaling and media: The GENBAND architecture supports separate interfaces for signaling and for media. A DoS attack on either the media interface or signaling interface has no effect on the other. Thus, creating effective attacks on the GENBAND SBC becomes more difficult and, for the SBC, thwarting attacks becomes a simpler. For example, a flood attack on the signaling interface, even at a very high rate, has no effect on RTP media processing through the media interfaces.

Software architecture: Protection against multiple forms of attacks requires a sophisticated approach. Attacks may come from known and unknown devices, individual endpoints or from a large number of endpoints. In all cases, the system ensures that both - the SBC itself and the network servers are protected. DoS and DDoS protection is performed at the lowest layers with co-ordination by higher, policy layers. This delivers high

performance and minimal impact during attacks. Lower layers are also capable of encryption (TLS, IPSec and SRTP) at wire rates.

The highest layer in the architecture includes management functions: attacks are detected and reported to the management layer. Real-time reporting and alarming gives visibility into the service environment. Furthermore, the system allows automatic or operator initiated control. The service can be disabled to offending users or devices that are detected as the source of a DoS attack.

Figure 5 shows the multi-stage ingress call rate limiting and egress call gapping within the SBC. On ingress, the first stage is the blacklist filter. This can be manually configured or invoked by higher layers during specified conditions. The first layer also includes the unknown device rate limiter. All devices that are not properly registered or manually configured are limited to a configurable aggregate rate. This ensures that the system will not succumb to a DDoS attack while allowing un-registered devices to go through the registration process.

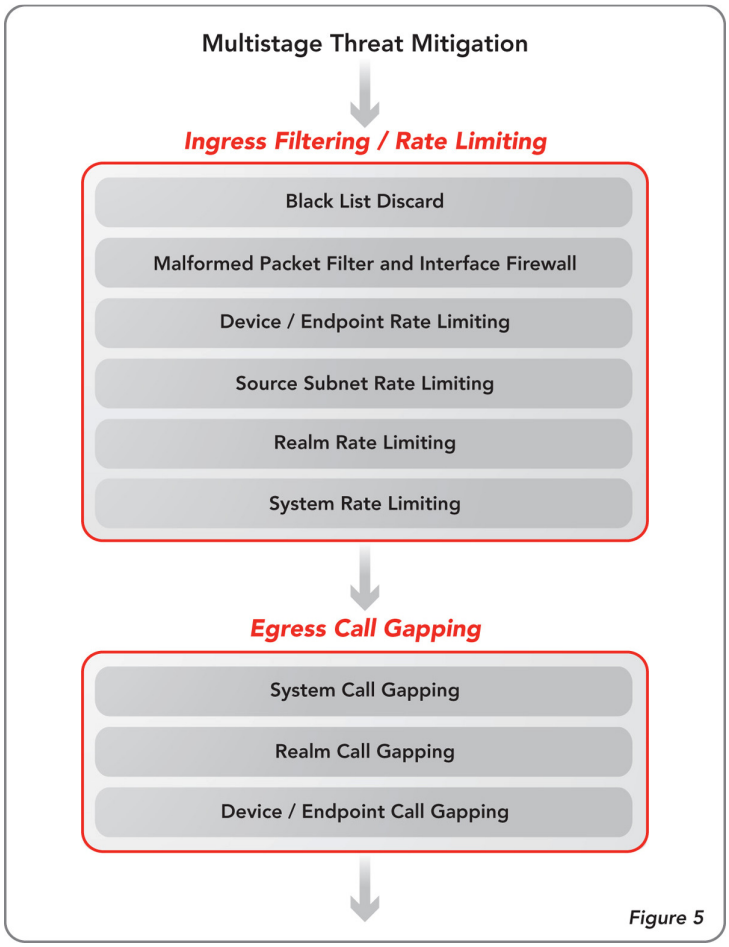

Figure 5

The second and subsequent layers at ingress are for rate limiting at a system/interface, realm and device level for “known” devices. This allows for rate policies to be applied at any desired granularity.

Call-burst processing is supported through a token scheme internal to the system. A realm in the GENBAND SBC is a virtual proxy that supports overlapping IP addresses and represents a unique construct to the GENBAND SBC. Inter-realm traffic with policy

enforcement allows carriers to flexibly manage traffic in complex networks. Egress processing includes call-gapping support, again at system, realm and device granularities. Since ingress traffic in the SBC may route to any egress devices (depending on policy and traffic), egress call-gapping must be independent of ingress rate limiting. This control allows application servers to be protected. Early in the signaling processing pipeline is a parsing and mal-formed packet filter. GENBAND's innovative deep packet inspection technology supports wire rate processing and filtering of mal-formed packets.

GENBAND's unique security architecture also facilitates and protects transcoding resources required for DTMF and voice transcoding. These resources can only be accessed via the SBC and provide another layer of security for media and signaling traffic for the service provider.

CPU Utilization: Due to the advanced software architecture and high performance hardware platform, processing of signaling can be handled even during near-wire-speed DoS or DDoS attacks. Even under extreme conditions such as wire speed attacks, CPU load is under 70%. Memory and I/O utilization are also well under maximum limits. Excess capacity in the platform ensures that no function in the system is ever starved for resources.

In summary GENBAND's security architecture is uniquely designed to address the security challenges that service providers face today. The architecture is designed from a multi-layered approach methodology and prevents intrusions at wire speed and at high session capacity levels.

Security Evolution for IMS and Fixed Mobile Networks

As service providers transition to all IP infrastructures such as the IP Multimedia Subsystem architecture, GENBAND's security framework is evolving to meet service provider needs. The IMS architecture promises significant benefits, not the least of which is a common, open industry standard environment across vertical markets that equipment vendors can support and that allows service providers easy interconnection. Previously, enhanced services have been deployed using a collection of point solutions that are vertically integrated. IMS is a unified architecture that supports a wide range of services and is based on SIP as the signaling protocol. The IMS architecture extends both fixed and mobile networks and strengthens overall end-to-end security of these networks. GENBAND's IMS strategy leverages the ETSI-TIPSAN standard, which provides building blocks that support fixed as well as mobile networks. GENBAND has also accounted for the requirements of the cable industry which are defined in the Packet Cable 2.0 standard. GENBAND has moved aggressively to support the 3G IPX standard which plays a key role in delivery of SIP based services such as IM, presence and push to talk between service providers.

GENBAND's pluggable security framework provides the next level of sophistication for dynamically delivering policy at both the application as well as device level. This policy function extends beyond the realm of security to include bandwidth allocation by service type, subscriber authentication filters and many other features. By supporting each of these key reference architectures GENBAND's product solutions fit seamlessly into many network configurations. Within the ETSI-TISPAN reference architecture, in particular, defines disassociated network elements that provide access and interconnect level security. These network elements are defined as P-CSCF, A-BGF, I-BCF and IBGF. From a security perspective they prevent DoS attacks on core IMS elements by dynamically discovering and blocking malicious signaling and media attacks or non-malicious overloads. Figure 6 describes the key security threats and protection methodology for the

IMS/ETSI-TISPAN architectures. The access and interconnect SBC will play a critical role in protecting service provider networks. For further details on GENBAND's IMS solutions please visit our website.

IMS Threats and Protection Schemes

Security Threat	Authentication & Authorization	Encryption	IMS Firewall	Intrusion Prevention	Network Security Management
Unauthorized Use	Addressed by IMS, HSS, AAA, P-CSCF				
Privacy		Addressed by IMS, IPSec, TLS			
Attacks on Infrastructure		Addressed by IMS, IPSec, TLS	Policy Filters Deep Packet Inspection	Deep Packet Inspection	Event Correlation Network Threat
Attacks on End Users	Digest Authentication	Addressed by IMS, IPSec, TLS	Policy Filters Deep Packet Inspection	Media Filtering Content and Application Filtering	

Figure 6

Why GENBAND

The GENBAND SBC architecture provides key advantages for service providers that want to provide VoIP and next generation services.

Carrier-Class Security and Performance
The GENBAND SBC provides carrier-class reliability and security – DoS protection and attack mitigation, intrusion detection, theft of service prevention, monitoring and alarming in addition to other required SBC functions. Other benefits include:

- **Proven platform:** GENBAND's SBC is deployed in over 500 service provider accounts around the world operating under high capacity conditions.
- **Comprehensive Security Architecture:** The SBC provides multi-level protection against all major classes of network security threats including fragmented traffic, malformed requests, DoS attacks, properly formed requests from unauthenticated sources, DDoS attacks and UDP and TCP floods. Real-time dynamic authentication and admission control across control and media sessions. Robust protection schemes, including: deep packet classification, traffic shaping and management, alarms, logging, static/dynamic ACL methods and transaction limiting. Specifically designed to counteract large, line-rate, wire-speed network attacks.

High Availability: GENBAND has proven solutions that meet the most demanding carrier conditions and environments around the world.

IMS Evolution: Future proof service provider networks as they evolve toward IMS, ETSI-TISPAN, and Packet Cable 2.0 architectures.

Conclusion

The open, peer-to-peer nature of the Internet has created exciting new opportunities for consumers, businesses and network operators. Unfortunately, that same openness poses serious risks to subscriber privacy and network security. Current-generation firewalls

provide only fixed-parameter access control and cannot adequately deal with the dynamic, high-volume traffic requirements of carrier-grade networks. GENBAND's S-Series SBC which is based on a standardized hardware configuration, and customized software and system integration, provides leading edge security protection for service providers. By leveraging Moore's law for continued processor performance upgrades GENBAND will lead the way in security under high performance conditions.