AudioCodes

WHITE PAPER

Securing Enterprise VoIP Networks with Multi-Service Business Gateways

July 08

AudioCodes

MSBG
AudioCodes
Multi Service
Business Gateway

WHITE PAPER

Executive Summary

The Multi-Service Business Gateway (MSBG) provides small and medium sized businesses (SMB) with an economical way to benefit from converged voice and data services. The MSBG integrates multiple network elements such as WAN access, routing and switching, firewall, VPN, media gateway, session border controller and an IP-PBX application into a single appliance, providing both CAPEX and OPEX savings to users.

As an integrated solution, the MSBG plays a key role in securing enterprise networks. The security framework includes securing the IP network with traditional Firewall and VPN capabilities and advanced VoIP security capabilities, commonly found only in service provider networks.

This paper will detail the MSBG security capabilities which are segmented into four security layers: the network, media, communication session, and application layers.

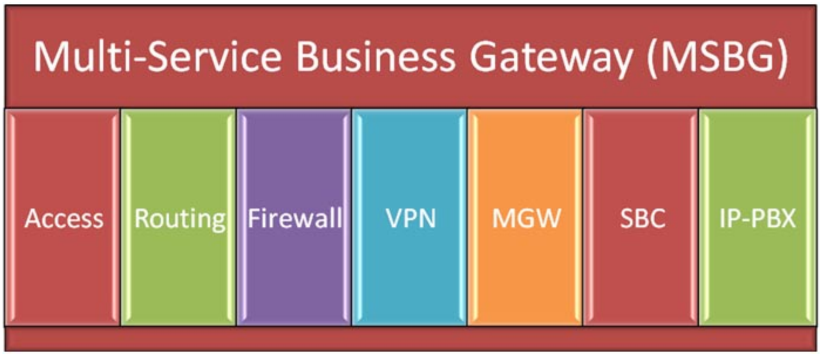
The network security layer framework consists of capabilities such as stateful packet inspection, firewall and IP-VPN. These are basic capabilities that provide the foundation for any security framework. The media security layer protects the enterprise's intellectual property by securing the in and outflow of communication messages, by using security methods such as secure real time protocol and secure SIP. The communication session security layer provides an additional level of defense for securing real-time communication by ensuring that security threats will not hamper normal communication between employees (internally and externally) to the enterprise. The application security layer is built above the previous layers, ensuring that attempts to disrupt normal business operations, such as relying on cheap VoIP calls for telemarketing or spamming enterprise employees, will be as minimal as possible.

Not all MSBGs provide the same level of security. While some provide basic functionality such as firewall and VPN, others provide a comprehensive set of security features, alleviating the need for additional network security components. It is also important to note that MSBGs should be flexible enough, both in terms of their software and hardware, in order to be able to address future threats.

Multi-Service Business Gateway Security Framework

Traditionally the MSBG functionality was implemented using separate and multiple appliances. However, due to advances in technology, MSBGs enable the tight integration of multiple network elements and applications into one box.

Diagram 1 - Main Components of an MSBG



As an integrated device, the MSBG should address multiple security aspects, starting from the IP network infrastructure up until the application level.

We will analyze what requirements are needed from an MSBG device in order to address these multiple security aspects. Today, enterprises face serious security risks both internally and externally. Converged IP data and voice allow for unprecedented economical and efficient ways to conduct business, however new threats should be addressed in order to obtain the real benefits from the technology. Security threats, if not addressed properly, can affect the uptime of networks, cause the loss of valuable data, and even compromise the organization's ability to protect its intellectual property.

Security threats could come from malicious attacks, usually external to the organization, from faulty or rogue devices, incorrect network configurations or even from a failure to enforce a security policy in the organization.

We can classify the security threats into four main categories:

1. Network level threats
2. Media threats
3. Communication session threats
4. Application level threats

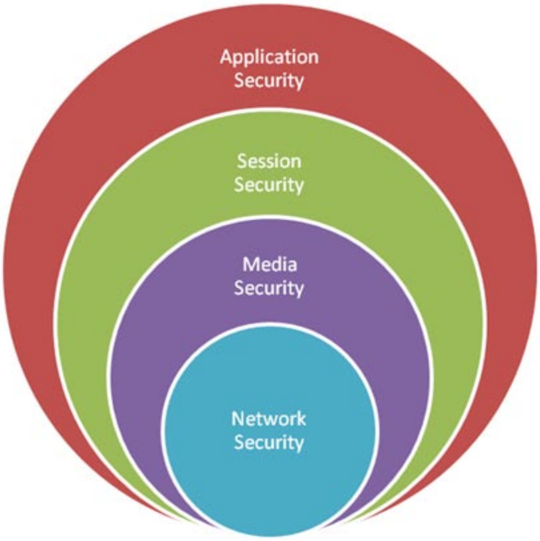


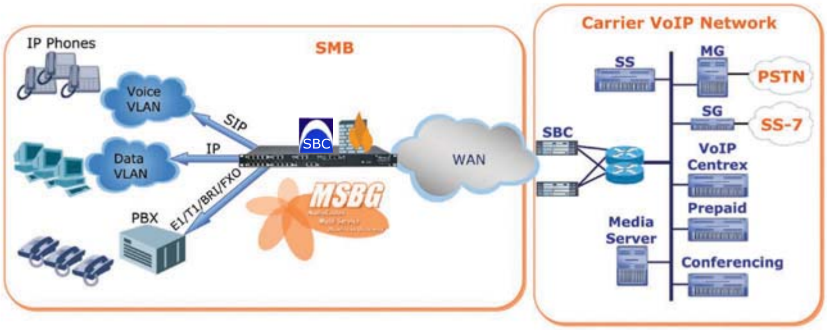
Diagram 2 - The 4 Main Security Categories

1. Addressing network security

Network level threats present the majority of today's threats to enterprise networks. Enterprises have been relying on **Firewalls** for many years in order to protect their networks, especially when accessing the Internet. The Firewall regulates the flow of data between the enterprise and external networks. Incoming and outgoing data is inspected and then either accepted or discarded. It operates according to a set of provisioned "rules" that block unwanted traffic but at the same time allows employees to be able to access and share data, internal and external to the enterprise network, along with maintaining productivity. Firewall rules specify the type of services in external networks that may be accessed from within the Enterprise.

The Firewall rules also specify the services available within the Enterprise network that may be accessed from external networks. The traffic that traverses the firewall is being constantly observed and evaluated against these rules and either accepted or denied.

Diagram 3 - MSBG Deployment in the SMB Network



Additionally, Firewalls serve to mitigate Denial of Service (DoS) attacks. A DoS attack is an attempt to prevent legitimate network users from being able to perform network operations normally, affecting the level of service to these users. Primitive DoS attacks consist of heavy traffic bombardment of certain IP addresses or ports, hoping to "choke" network or compute resources.

More sophisticated attacks try to exploit protocol behavior or implementations (usually software implementations) in order to cause some form of resource starvation, which affects the way service is delivered to users. A DoS attack could also take the form of a distributed DoS attack, where multiple attack sources are coordinated to perform a simultaneous attack. This type of attack presents a more significant threat, because in order to detect it, there is a need to correlate multiple sources of attack.

Firewalls provide a basic but essential level of security. With the rapid adoption of IP technology, new forms of threats have emerged. Though firewalls become continuously more sophisticated, there are threats that Firewalls simply cannot mitigate. We will further review some examples of these threats and their mitigation in this paper.

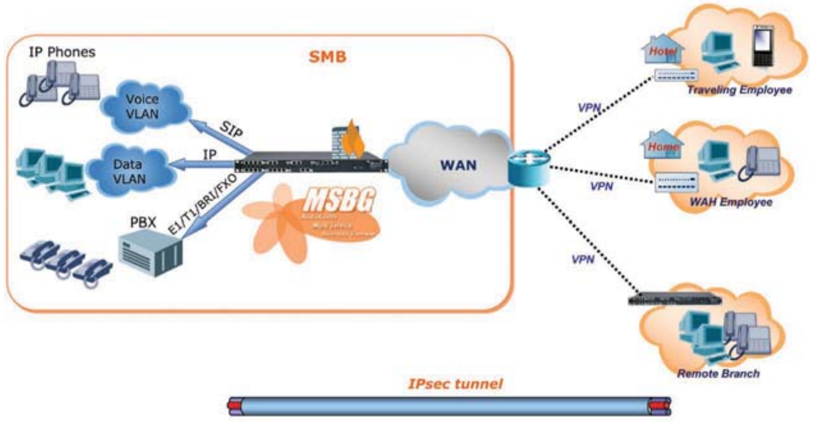
Apart from firewalls which are a fundamental element in any IP security solution, an additional component for network level security is the Virtual Private Network.

Virtual Private Networks (VPNs) are commonly used by enterprises for two main purposes: allowing users external to the organization (employees who travel, employees working from home, etc.) to access the organization's internal network resources and allowing inter branch connectivity, all of this while preserving the highest level of security. VPNs could be viewed as a virtual extension of the organization LAN into employees homes and remote locations. VPN technology relies on tunneling protocols like the IPSec protocol (and others) in order to secure the traffic flowing to and from the enterprise.

The IPSec protocol provides an efficient way to transport IP traffic from one point to another, while providing a confidentiality mechanism (blocking, snooping and exposure of the data flow), sender authentication (blocking identity spoofing and impersonation), and message integrity (preventing manipulation of data flow). This essentially means that VPNs allow organizations to maintain secure communications over external, non-secure networks.

The diagram below depicts how VPN is used in order to connect remote employees and remote branches to the enterprise network.

Diagram 4 - MSBG Providing VPN Service to Remote Locations



2. Addressing Media Security

VPN is an efficient way to connect different network "clouds" in a secure fashion. There are however many cases, in which a secured connection needs to be established between the enterprise network and an external user or service. A good example for this is secure web browsing, when the user is required to send sensitive information such as a credit card number or any other personal information over the internet. Another example is secured VoIP.

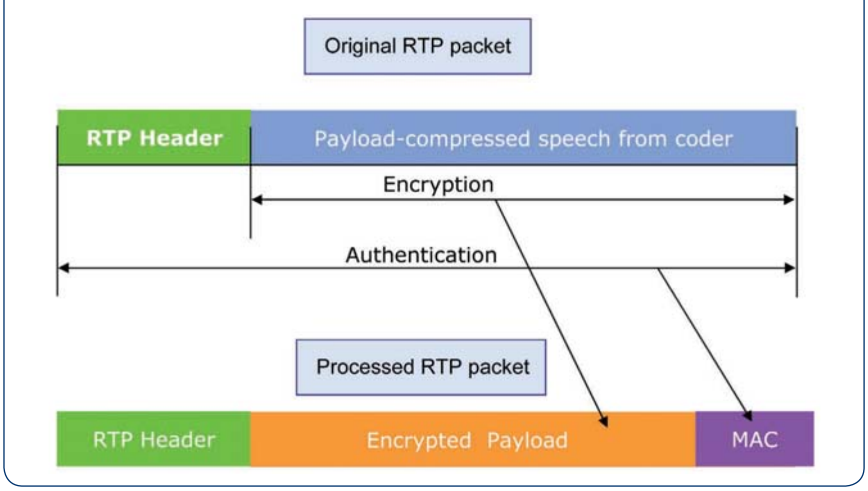
The standard protocol for VoIP media is Real-time Transport Protocol (RTP). RTP is used to carry real-time data such as voice or video over IP networks. Secure Real-time Transport Protocol (SRTP) is an enhancement to the RTP protocol that defines a new profile, intended to provide confidentiality, authentication and message integrity. SRTP also provides replay protection, the prevention of an attacker sending multiple copies of an intercepted message without the real sender's knowledge.

An RTP packet consists of a header and a payload. The header contains information such as the payload type, sequence number, timestamp, etc. The payload contains a compressed voice generated by a voice coder. The payload size depends on the coder in use and on the framing. As discussed above, the main purpose of securing a link is to keep data confidential and to verify data integrity and authenticity. For confidentiality, the packet payload is encrypted at the sender's side and decrypted at the receiver's side using the same encryption key.

For verifying authentication of messages, SRTP relies on a hash algorithm that produces a unique sequence of bytes (called MAC) that are being appended to the packet end. This scheme enables the receiver to verify the integrity of the payload as well as fields in the header, such as the packet sequence number, to combat replay attacks.

The figure below demonstrates the security operation on an RTP packet at the sender's side:

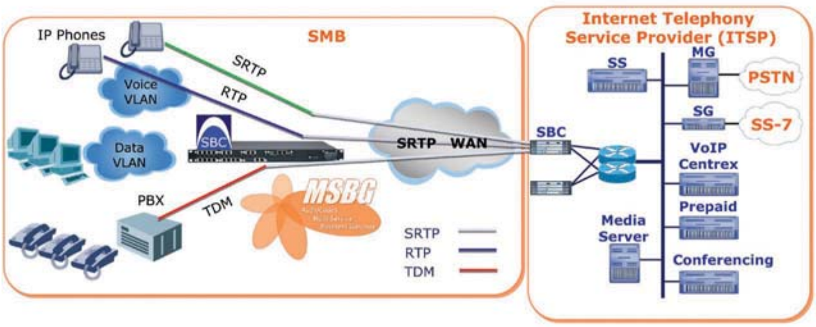
Diagram 5 - RTP to SRTP Conversion



In order to enable secure real time communication using SRTP, the MSBG should be able to support multiple call scenarios.

1. A call from a SRTP enabled enterprise IP-Phone to an external service provider network supporting SRTP
2. A call from a IP-Phone not supporting SRTP to an external service provider network supporting SRTP
3. A call from a legacy PBX extension (TDM) to en external service provider network supporting SRTP
4. A call from an extension supporting SRTP (TDM or IP) to an extension not supporting SRTP (TDM or IP) within the enterprise
5. A call from an extension supporting SRTP (TDM or IP) in one enterprise branch to an extension not supporting SRTP (TDM or IP) in another enterprise branch

Diagram 6 - SRTP Scenarios in an Enterprise Network



The scenarios above imply that the MSBG should be able to receive standard RTP from one side and convert it to SRTP on the other side (and vice versa). The MSBG should also be able to allow transparent flow of SRTP between endpoints that support it natively. A further interesting point is the secure communication for legacy TDM equipment (PBX or analog phones). The Media Gateway component in the MSBG should be able to convert the TDM voice into SRTP packets allowing secure communication for legacy equipment.

3. Addressing Session Level Security

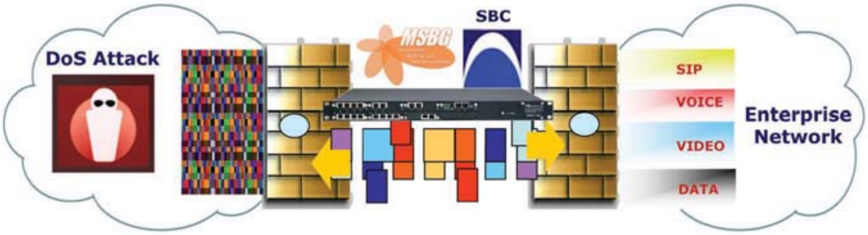
In addition to supporting network level and media security, the MSBG supports some unique features for the protection of real-time communications. These features are available in service provider stand-alone Session Border Controllers (SBCs).

The SBC element within the MSBG is designed for enhancing the level of protection delivered to voice, video and instant messaging users. In most cases, SBCs are used for protecting real-time communications flowing in and out of the enterprise boundary. This could involve remote workers using the enterprise PBX from home or abroad to dial remote branches, connected to the PBX at headquarters or an enterprise connected to an Internet Telephony Service Provider (ITSP) in a way most commonly known as “SIP trunks”. There are also incidences in which the SBC is involved in delivering enhanced security and control of network resources for the intra enterprise communication. The SBC performs “Topology Hiding” when routing SIP signaling across enterprise boundaries.

Topology hiding is used for hiding the internal network topology of the enterprise network (such as IP addresses of IP-PBX and other network elements) providing an additional level of security and privacy. Topology hiding is accomplished by processing SIP Invite messages as a SIP User Agent Server (UAS) on one interface while acting as a SIP User Agent Client (UAC) on another one. This is also known as B2BUA (Back-to-back user agent) method of operation.

The SBC examines the payload of a control session to determine the private address of a contacting device, and then coordinates with the firewall to establish a session-based “pinhole” for that media flow. Once the session is complete (usually because the call has ended), the pinhole is closed and any traffic destined for this pinhole would be discarded. Using this approach, all traffic is scanned at wire speeds and examined for patterns across packet boundaries to discern legitimate sessions while identifying and shutting down security attacks. Illegitimate session attempts can therefore be filtered out prior to disrupting network traffic. Furthermore, before establishing a session, the SBC employs a set of operations to decide whether to allow the session to commence or deny it.

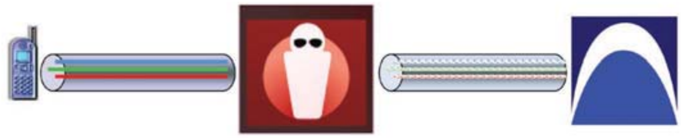
Diagram 7 - The Pinhole Concept



The SBC performs user authentication and authorization with or without the assistance of the IP-PBX. For example, the SBC can be configured to accept new sessions (calls) from a specific network address or subnet. It can be configured to allow calls coming to and from a specific domain, in which case the SBC would perform a DNS query to decide whether to allow the call.

The SBC can also be configured to use certificates in order to authenticate users who are trying to place calls. The SBC protects SIP traffic transferred over the TCP protocol using encryption enabled by the Transport Layer Security (TLS) protocol and associated X.509 certificates. Using the TLS protocol, the SBC authenticates user agents and mutually authenticates trusted peers based on installed TLS certificates. These certificates are used to prevent man-in-the-middle attacks, eliminating the possibility of a 3rd party impersonating another party in a secure communication session establishment.

Diagram 8 - Man in the Middle Attack



Threat	Counter Measure
Man in the Middle A device intercepts and masquerades as client/server by presenting fraudulent credentials. From this position the intermediary device can eavesdrop, or actively manipulate information	• Mutual Authentication • Authentication based on shared secrets • Certificate based Authentication

In addition, authentication can also be facilitated by using the IP-PBX. For example, the SBC could proxy user requests to the IP-PBX for performing what is commonly known as a SIP challenge process. In this case users send an encrypted password which is being checked against the user password database in the IP-PBX.

The SBC will only allow the session to commence after the challenge process has been terminated successfully. Moreover, the SBC will perform signaling rate throttling, in order not to put the IP-PBX under heavy load, thereby affecting normal service to other users. The SBC performs another important task known as protocol validation. Communication messages (SIP, RTP, etc) that do not conform to the standard implementation or to a predefined policy will be dropped by the SBC. This is a way to protect against DoS attacks that make use of malformed messages and requests, in order to exploit software bugs or put a heavy load on call processing elements such as the IP-PBX.

The SBC should be able to protect itself from heavy loads and is therefore required to be able to work at wire-speed. In this case, unlike routers or switches that are allowed to drop traffic (usually according to some QoS policy) under heavy loads, the SBC should not drop legitimate user traffic. In other words, the SBC should be intelligent enough to recognize attack traffic or ineligible traffic (i.e. a legitimate user that is trying to place multiple calls while he is allowed to make one simultaneous call), and discard it before it flows into the enterprise network and affects the normal level of service. In order to achieve this, the SBC must keep state information and have user awareness. This kind of operation is fundamentally different to that of a normal firewall. In fact it can be viewed as a firewall working at "OSI layer 7" or the application layer.

Diagram 9 - DoS Attack

Threat	Counter Measure
Denial of Service • Call Control Message Floods (SIP Register) • Malformed Requests • Distributed Attacks (Authenticated and Un-authenticated Sources) • IKE Initialization Floods • IP Packet Floods (SYN, ICMP, Fragments)	• VoIP Firewall ▪ Access Control and Deep Packet Classification ▪ Policy Establishment – Dynamic "Allow" – Dynamic "Deny" ▪ Transaction Rate Limiting • IPSec / TLS-SRTP • Rogue Packet Detection/ Quarantine ▪ BW Policing, RTP Header Validation ▪ RTP traffic from multiple sources ▪ RTP traffic after call is terminated

In summary, the SBC component of the MSBG performs the following in order to provide session level security:

- The SBC compliments the Firewall DoS protection capability by adding necessary application intelligence in order to prevent sophisticated VoIP attacks. The SBC 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 within the enterprise boundaries are not flooded with valid SIP requests from unauthorized sources. The SBC is self-protected against signaling floods.
- Infrastructure topology hiding at all protocol layers for confidentiality and for the prevention of service attacks
- Encryption such as TLS is used to provide user authentication and privacy
- Session aware access control for signaling and media using static and dynamic ACLs based on threshold limits on Layer 3 and Layer 5
- Monitoring and reporting including event logs, access violation logs, management access logs, Call Detail Records (CDRs) with performance monitoring, and raw packet capture ability

4. Addressing Application Level Security

All of us are familiar with email spam. Email spam and other forms of spam on the internet are so common because they remain an economic way for advertisers who have no operating costs (other than a fixed cost for accessing the internet). Secondly, it is still very difficult to hold spam senders accountable.

With the price of VoIP being reduced and service providers offering “fixed price” calling packages, it is no surprise that enterprises are beginning to face additional problems by people who abuse cheap VoIP calling for telemarketing and other types of solicitation, usually in the form of automated messages. This problem could hurt productivity significantly. Most employees when receiving a call, even without a recognized caller ID, will still pick up the phone and be distracted from their work.

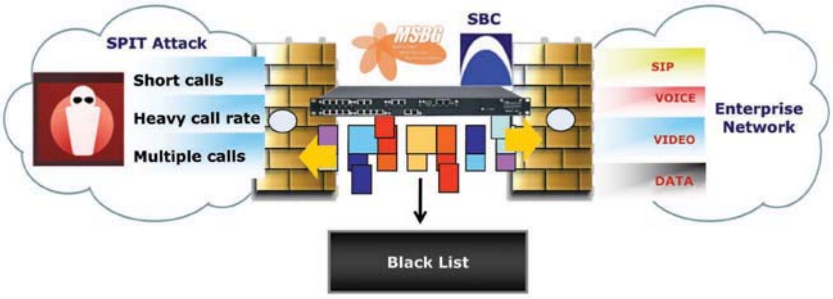
This type of attack or interference with every day life is often referred to as SPIT (Spam over IP Telephony). As with email spam, it is expected that SPIT will become an increasingly difficult problem to handle. As long as the economical drive for spammers exists and methods like free calling over the internet will become more prevalent, enterprises should find a way to protect their networks and in this case their most precious asset, human capital, from this type of attack.

Fortunately, as with email spam, there is a lot that can be done in order to protect VoIP networks from these types of attacks. There are two main options for dealing with SPIT. One is automatic and based on call pattern heuristics in order to distinguish between legitimate calls and suspected SPIT. For example it is expected that SPIT calls should be very short because most people would hang-up immediately after recognizing it as a spam call. A simple but effective way to prevent SPIT would therefore be to detect source phone numbers that generate very short calls. These numbers could then be placed into a dynamic “black list” of numbers suspected as spammers. Another heuristic would be to look at source phone numbers that generate a lot of simultaneous calls or that generate heavy call volumes and tag them as suspected spam.

The other method for detecting SPIT relies on what is commonly known as a Reverse Turing test in order to be able to distinguish between automated calls and human calls. The problem with this method is that it requires the caller to perform some action in order to be authenticated and this could harm quality of experience (QoE) with VoIP calling. Another option which involves detection of voice content in real-time is still not practical using today’s computer resources.

An MSBG should be equipped with an anti-SPIT mechanism. Although it may make sense to use a dedicated box for this purpose with service provider networks, in enterprise networks and especially in the SMB the addition of dedicated boxes for solving SPIT is usually not an acceptable solution.

Diagram 10 - Preventing SPIT using MSBG



Summary

In this paper we reviewed some of the ways in which MSBGs can be used in order to secure enterprise networks, without the need for additional security elements. The MSBG provides small and medium businesses (SMB) with an economical way to benefit from converged voice and data services without compromising the security framework.

Prior to selecting the correct MSBG for your needs, you need to take into account the security mechanisms that it offers. Security mechanisms in the MSBG span from the basic network level protection up to application aware, a “OSI level 7” protection that not all MSBG devices in the market can offer. Since the MSBG is the cornerstone of the enterprise VoIP network, it is important to work with a vendor with extensive knowledge and experience in delivering enterprise VoIP solutions. It is also important to understand that new threats are constantly emerging, especially since VoIP is becoming so mainstream. When selecting an MSBG device you need to take into account the options for upgrading hardware and software components, in order to address new features and requirements.

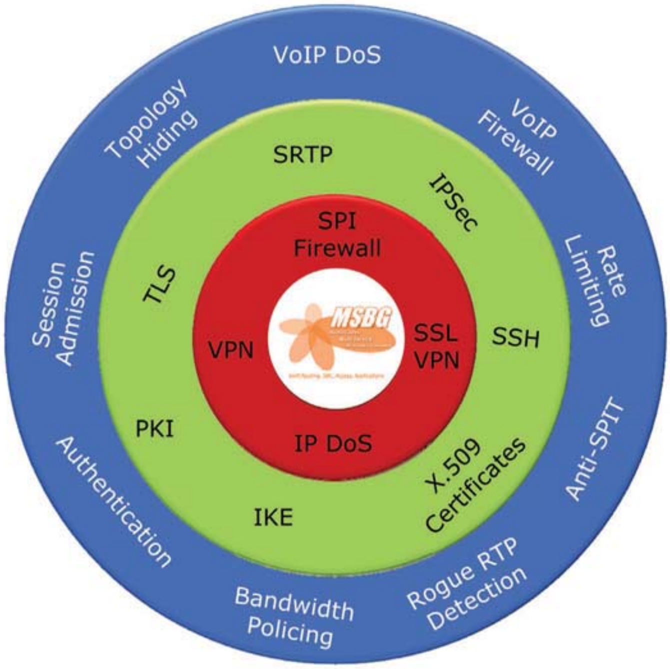


Diagram 11 - MSBG Security Capabilities

About AudioCodes

AudioCodes Ltd. (NasdaqGS: AUDC) provides innovative, reliable and cost-effective Voice over IP (VoIP) technology, Voice Network Products, and Value Added Applications to Service Providers, Enterprises, OEMs, Network Equipment Providers and System Integrators worldwide. AudioCodes provides a diverse range of flexible, comprehensive media gateway, and media processing enabling technologies based on VoIPerfect(tm) – AudioCodes' underlying, best-of-breed, core media architecture. The company is a market leader in VoIP equipment, focused on VoIP Media Gateway, Media Server, Session Border Controllers (SBC), Security Gateways and Value Added Application network products. AudioCodes has deployed tens of millions of media gateway and media server channels globally over the past ten years and is a key player in the emerging best-of-breed, IMS based, VoIP market. The Company is a VoIP technology leader focused on quality and interoperability, with a proven track record in product and network interoperability with industry leaders in the Service Provider and Enterprise space. AudioCodes Voice Network Products feature media gateway and media server platforms for packet-based applications in the converged, wireline, wireless, broadband access, cable, enhanced voice services, video, and Enterprise IP Telephony markets. AudioCodes' headquarters and R&D are located in Israel with an additional R&D facility in the U.S. Other AudioCodes' offices are located in Europe, India, the Far East, and Latin America.

International Headquarters
1 Hayarden Street,
Airport City
Lod 70151, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
27 World's Fair Drive,
Somerset, NJ 08873
Tel:+1-732-469-0880
Fax:+1-732-496-2298

Contact us: www.audiocodes.com/info
Website: www.audiocodes.com

Ref # LTRM-80026 07/08 V.1