Ingate Firewall/SIParator® SIP Security for the Enterprise

Ingate Systems
February, 2013

Ingate Systems |www.ingate.com | info@ingate.com
Ingate Systems Inc Tel: +1 603 883 6569
Ingate Systems AB (publ) Tel: +46 8 600 77 50

Background

Voice over IP (VoIP) is incorporated into a variety of computer networks, both public and private, and used for everyday transactions and communications among carriers, businesses, government agencies and individuals. SIP trunking, remote/mobile workers, and Unified Communications are some of many forms of VoIP applications.

Over these varieties of computer networks, enterprises use IP-PBXs, Unified Communications (UC) applications, computers, mobile smart phones, wireless connectivity, Internet access and VoIP carriers make it easier than ever for workers to conduct business anywhere, anytime. Extending corporate voice, video and UC services to Internet users and VoIP carriers, businesses can implement flexible telecommunication applications and business communication plans, and eliminate costly legacy phone system expenses.

But operating VoIP with IP-PBXs and Unified Communications systems over the Internet and untrusted networks raises a variety of security, interoperability and reliability concerns. Businesses are worried about exposing corporate resources and information to hackers (via the Internet or internally) and eavesdroppers, maintaining acceptable voice and video quality over the Internet and VoIP carriers, and encountering interoperability issues when interfacing with firewalls and public network services.

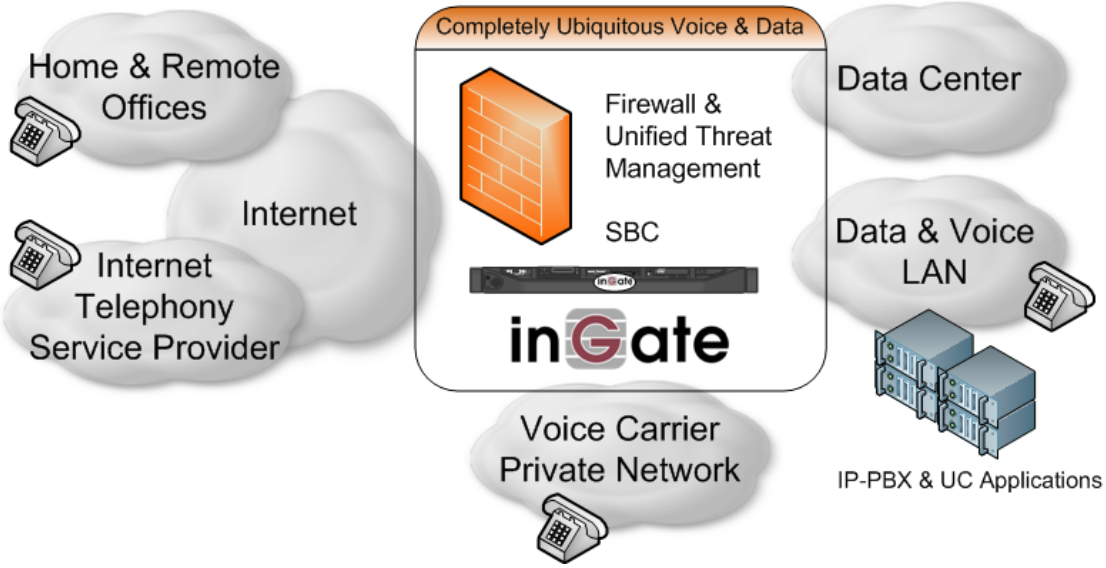
The Ingate SIParator is an Enterprise Session Border Controller (E-SBCs) specifically designed to deliver the strong network security, with easy interoperability and reliable communications, required for VoIP SIP communications - voice, video and multimedia - over the Internet and VoIP carrier networks.

1 Network Security

Network Security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security must also extend into VoIP applications such as SIP trunking, remote/mobile workers, and Unified Communications.

All security solutions start with a security policy. It is in the best interest of every enterprise to protect corporate resources and information from unknown users and malicious activities. Often enterprises create Network Security Zones, a boundary between networks that describes a level of trust, referred to as Trusted Zones and Untrusted Zones. When Networks are part of a Trusted Zone, all traffic is allowed and no authentication is required. But in Untrusted Zones, no traffic is allowed and an administrator defines the services and policies to restrict access.

The Internet is obviously an Untrusted Zone, as there is no control over network access, users and malicious activity. Firewalls are ubiquitous in today's IP networks, they protect IP data networks, servers and applications against a variety of threats through stateful inspection and filtering, they are used to define the services and polices allowed from the Internet and Untrusted Zones to the enterprise Trusted Zone. To complete the ubiquitous solution, including VoIP, an E-SBC is used define the VoIP services and polices that are allowed. But VoIP is delivered from more networks than just the Internet. VoIP is delivered on foreign networks such as carrier private networks for the use of SIP trunking and hosted applications. Since these networks are outside of the Trusted Zone of the enterprise an E-SBC must be used to provide the security service and policy between the enterprise Trusted Zone and Untrusted Zones.



2 Why is VoIP Security Important?

There is an "End of Geography," IP Protocol is an OPEN network system, no longer is there a need to be physically present to gain access to a device, any IP address can connect with any other IP address. IP protocol and IP addresses are fundamental in a variety of computer networks, both public and private, and used in every day transactions and communications among carriers, businesses, government agencies and individuals.

Businesses are concerned about exposing corporate VoIP resources and VoIP information to hackers (via the Internet or internally, public or private) and eavesdroppers, maintaining acceptable voice and video quality over the Internet and VoIP carriers, and encountering interoperability issues when interfacing with firewalls and public network services. A method to prevent fraudulent VoIP activities is needed between Trusted and Untrusted Networks.

Types of fraudulent VoIP activities include the following; Identify Theft, Toll Fraud, Spoofing, Misuse, SPAM, SPIT, Vishing, Eavesdropping, Data Mining, Reconnaissance, Disruption of Service, Denial of Service, and Fuzzing.

3 Security with an E-SBC

Session Border Controllers uniquely provide all of the controls required for delivering trusted, secured, reliable and high-quality IP interactive communications:

Security: IP PBX and UC server DoS/DDoS attack protection, SBC self-protection

Communications reach maximization: IP PBX and UC – SIP Protocol interoperability, remote NAT traversal
SLA assurance: IP PBX & UC server session admission and overload control, data center disaster recovery, remote site survivability, Call Admission Control, SBC high-availability operation

Data Firewalls with application layer gateways (FW/ALG) are effective in securing data-oriented application infrastructure (PCs, servers) but do not generally have the tools necessary to also manage and control enterprise SIP implementations.

E-SBCs provide detailed access control features to prevent fraud and service theft; IP address and topology hiding to safeguard privacy and confidentiality. Also DoS/DDoS prevention and IP telephony spam protection to ward off malicious attacks; and signaling and media encryption to prevent eavesdropping, hijacking and Theft of Service. Ingate SIParator E-SBCs support Transport Layer Security (TLS) and Secure Real-Time Protocol (SRTP) to ensure privacy and confidentiality without the complexity or overhead of conventional VPN solutions.

The Ingate SIParator can be used as a VoIP security device to address some common SIP attacks such as:

- Intrusion of Services (or Theft of Service)
  - Devices attempting Register with a IP-PBX in an attempt to look like an IP-PBX extension and gain IP-PBX services
  - SPIT (SPAM over Internet Telephony)
- Toll Fraud
  - A form of an Intrusion of Service, where malicious attempts to send INVITEs to an IP-PBX to gain access to PSTN Gateways and SIP Trunking to call the PSTN
- Denial of Service
  - INVITE (or any SIP Request) Flood in an attempt to slow services or disrupt services
  - Or any UDP or TCP traffic directed at a SIP Service on SIP Ports
- Indirect Security Breaches
  - Data Mining, Network Topology

4 Successful Delivery of VoIP

Requirements for the successful delivery of enterprise and contact center VoIP/UC services and applications:

- SBC/FW DoS/DDoS Self-Protection
- VoIP Security for Theft of Service
- IP PBX & UC SIP Protocol Interoperability
- IP PBX/UC Server Session Admission & Overload Control
- Remote Site NAT Traversal
- High Availability VoIP Operations
- Data Center Disaster Recovery
- Remote Site Survivability using SBC/FW
- Call Admission Control