Ingate Enhanced Security Module

Voice-over-IP, or VoIP – frequently deployed in SIP trunk solutions -- is quickly being adopted by enterprises worldwide as the communications method of choice. It is cost efficient, as VoIP and especially SIP trunks can save businesses significant communications costs. Even though the VoIP traffic (as other data traffic) is sent over the public Internet, your network and the communication must still be secured against attacks from hackers and eavesdroppers.

Ingate® Systems has the solution.

The Ingate Enhanced Security Module is an add-on software module for all award-winning Ingate Firewall® and Ingate SIParator® products that provides another layer of security for SIP-based applications. It features an Intrusion Detection System/Intrusion Prevention System (IDS/IPS) for SIP, making it possible to detect and protect against Denial of Service (DoS) attacks based on the protocol and to block SIP signaling packets designed to attack SIP devices on the LAN, such as SIP phones.

In addition to IDS/IPS, Ingate Enhanced Security incorporates encryption of both signaling (TLS) and media (SRTP) which makes it almost impossible for eavesdroppers to retrieve the original media stream from the encrypted stream.

The Enhanced Security Software Module works hand-in-hand with Ingate's full SIP proxy technology, which provides an unprecedented level of control over the flow of SIP traffic and the enterprise network. This control offers tremendous advantages with regard to security.

Security of the enterprise network

The IDS/IPS in the Enhanced Security Module enables the Ingate Firewall/SIParator to detect DoS attacks based on the SIP protocol, and to block malicious SIP signaling packets designed to attack certain SIP phones, servers or other devices on the enterprise LAN. This secures the enterprise network as the edge device – the Firewall or the SIParator – handles the attacks while the servers and other SIP devices in the network can still be used.

For DoS attack detection, the administrator specifies what should be regarded as an attack. This offers the administrator flexibility to set the criteria for the number of requests/responses per time frame as environments and functions vary, and must thus be defined individually. The rules may also be written to limit requests/responses from specific IP addresses or domains within a time period, or to block all requests/responses from an IP address or domain if the administrator determines that the attack is being launched from that site.

All logs can be exported for analysis and, based on the findings, the administrator can refine the rules to minimize attacks and intrusions, while also allowing normal communications to continue.

Ingate's Enhanced Security Module can also protect the network against malicious SIP packet attacks: attacks where the SIP packets look correct, but a combination of headers can make a SIP phone or server reboot (or become temporarily unusable). For these intrusion scenarios, Ingate provides rule packs to upload to the Firewall/SIParator. Ingate will provide rule packs for the detection of known attacks as reported by industry watch groups, or by customers. These rule packs may then be installed on the Ingate Firewall/SIParator, so that if there is an attack launched against the customer's network, the Ingate products can detect and block that SIP packets instead of forwarding it to the SIP client, protecting the SIP client from being compromised.

The same rule packs can be applied to monitor outbound traffic to detect if the network has been compromised and the malicious packets are being added to outbound headers. In this case the transmissions will be blocked to avoid delivering the packets to other networks and the administrator will be alerted so that steps can be taken to eliminate the problem.

Encryption of all communications

The Enhanced Security Module also features an advanced encryption system for all SIP communication. It includes TLS (Transport Layer Security), which encrypts the signaling. It also includes support for SRTP (Secure Realtime Transport Protocol). Together, this powerful SRTP-TLS combination protects media from being overheard by unauthorized persons, providing a high level of security for live data with advanced encryption, confidentiality, message authentication, and replay protection. Using TLS and SRTP to encrypt signaling and media traversing the Internet effectively stops eavesdroppers, hackers and spoofers. The integrity of the call is much stronger than ever possible on PSTN.

The Ingate Firewall/SIParator can decrypt the signalling and media and deliver them "in the clear" to devices on the Local Area Network (LAN), or pass the encrypted packets on to the server or phone fully encrypted all the way to the user. This flexibility permits the network administrator to tailor the use of encryption to the needs of the organization and the capabilities of the other SIP equipment in the network.

The integrity of the call is much stronger than ever possible on PSTN.

For more information, visit us at www. ingate.com or write to info@ingate.com.

Ingate 20080414

inGate®

www.ingate.com

Ingate Systems AB · Phone + 46 8 600 77 50 · Ingate Systems Inc · Phone: 1-603-883-6569
info@ingate.com · www.ingate.com