INGATE KNOWLEDGE BASE

March 17, 2009

Ingate Knowledge Base - a vast resource for information about all things SIP – including security, VoIP, SIP trunking etc. - just for the reseller community. *Drill down for more info!*

To sign up a friend, have them email sofia@ingate.com.

To be removed from the email distribution, send a quick note to sofia@ingate.com.

SIP SECURITY

Like any application over Voice-over-IP and all similar applications should be implemented in a way that ensures the continued security and integrity of the enterprise network. With the proper protections in place, SIP applications are very secure. In fact, VoIP calls can be more secure than those made on the PSTN. That's just an example of how, with the right measures, any SIP application can be secure enough for enterprise use.

The SIP protocol resides in the Application Layer; it is written in clear text within the datagram of a UDP or TCP transport. Because it is in clear text, it is readily readable to any malicious efforts to compromise your VoIP or data traffic. Sensitive IP address information, port address information, contact addresses, usernames, SIP compliance capabilities, media stream attributes and more are all contained in the SIP protocol.

In addition, the VoIP media stream is also unencrypted. Common media streams such as G711, G723, and G729 are open for malevolent efforts to record conversations over the Internet.

Given that SIP is a relatively new protocol for VoIP deployment, there have been very few malicious SIP attacks to date. But as popularity grows and SIP becomes more widespread, the possibility for these kinds of events increases.

But since the SIP protocol has been developed by the IETF it has built in capabilities to ensure that the security and control of the enterprise network is maintained, and that measures can be taken to protect the integrity of all Internet-based communications, even for the most sensitive conversations.

The IP-PBX should be deemed a "Mission Critical" server. The IP-PBX is the controller for all of the VoIP phones and SIP applications. Any service outage or degradation would result in the loss of communication and ultimately the loss of business revenue. The IP-PBX must be protected from the Internet and foreign or unknown networks just as any other mission-critical server on the network.

That means that the PBX should never be assigned a publicly routable IP address. The Network Address Translation to the private address space provides a layer of security that must be maintained for the IP-PBX.

Measures such as deep packet inspection, encryption and support for TLS and SRTP, authentication, intrusion detection and prevention (IDS/IPS) functionality, DoS attack detection and even SIP (and SIPconnect) compliance are all necessary ways to protect not just the SIP traffic, but also the network.

Ingate employs all of these and more, including filtering capabilities to ensure that only authorized users are permitted access. With an E-SBC in place, like the SIParator from Ingate Systems, SIP communications can be successfully and securely introduced to the network and the enterprise remains in full control of their network.

All of these security "must-have's" will be detailed in future Knowledge Bases.

Want more information

Follow the link to find out more http://www.ingate.com/appnotes/Ingate_Security_Best_Practices.pdf

Next week

Demystifying Deep Packet Inspection

For more information, visit the Ingate Knowledge Base online at www.ingate.com.