INGATE KNOWLEDGE BASE

May 18, 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.

The introduction of SIP to a network brings the challenge of protecting the network from an untrusted network, and the opportunity to manage the routing of calls to a degree not possible with traditional telephony. This instalment of our continuing Knowledge Base will review some of the things that can be configured with an Ingate Enterprise Session Border Controller to address both the challenges and opportunities.

How Ingate Differs from Other SIP Solutions

Many vendors tout their expertise in enabling SIP capabilities – making SIP communications possible – for enterprises. However, these solutions lack the security measures that are absolutely necessary for the business environment.

The bottom line is this: mission-critical voice **must not** be compromised. And SIP applications **cannot** serve as an “open door” for malicious attacks on the network.

Ingate as compared to a SIP phones & IP-PBXs
SIP phones and IP-PBXs may be stateful to the SIP protocol, providing a level of SIP integration and conformance. They also make it possible to make SIP calls by generating and receiving any SIP requests and generate responses.

· **Why Ingate:** Ingate SIParators/Firewalls have the added DPI intelligence to provide non-protocol compliance rules, routing rules and statistical information and to provide IDS/IPS security features for an effective against defense against overflow attacks, denial of service (DoS) attacks, SPAM over Internet Telephony (SPIT) and sophisticated intrusions. SIP phones and IP-PBXs are just clients looking for service, and not necessarily security conscious and able to redirect or deny SIP traffic based on defined rules.

Traditional IP-PBXs
Many IP-PBXs lack the capacity to sit right on the Internet. Others, such as those from Mitel, Nortel and Avaya, can have a public IP address assigned. However, none have any built-in security. A firewall is required to protect from malicious Internet activity.

Why Ingate: For SIP communications each of these IP-PBX vendors require the use of an Ingate or SIP-aware firewall resolve NAT traversal issues. With an Ingate, not only is NAT traversal solved, but Ingate’s strict security measures are also in place to protect both SIP applications (VoIP, etc.) as well as the network itself.

WANT MORE INFORMATION

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

NEXT WEEK

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

**We would like to hear from you.
Let us know of any topics you’d like to see addressed in future issues of the Knowledge Base series by writing to sofia@ingate.com or steve@ingate.com.**