INGATE KNOWLEDGE BASE

APRIL 21, 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.

IDS/IPS and the Ingate Enhanced Security Software Module

As we talked about earlier, Ingate SIParators and Firewalls have Deep Packet Inspection capability, which gives Ingate the ability to look at Layer 2 through Layer 7 of the OSI model.

Deep packet inspection combines the functionality of Ingate's intrusion detection system (IDS) and intrusion prevention system (IPS) features with our traditional stateful SIP Session Border Controller functionality in the Firewall/SIParator. This combination makes it possible to detect certain attacks that neither the IDS/IPS nor the stateful firewall can catch on their own. DPI can be effective against buffer overflow attacks, denial of service (DoS) attacks, sophisticated intrusions, and a small percentage of worms that fit within a single packet.

The IDS/IPS in Ingate's Enhanced Security software module enables the Ingate Firewall/SIParator to detect DoS attacks based on SIP, 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 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.

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.

Want more information

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

Next week

More about Malicious SIP Packet Attacks and Ingate Enhanced Security
For more information, visit the Ingate Knowledge Base online at www.ingate.com.