INGATE KNOWLEDGE BASE

May 7, 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.

More about Malicious SIP Packet Attacks and Ingate Enhanced Security

The past few weeks we've been focusing on security. This week we'll discuss more about malicious SIP packet attacks, and how Ingate's Enhanced Security software module can help thwart them.

Malicious SIP packet attacks are when the SIP packets look correct, but a combination of headers can make a SIP phone or server reboot (or become temporarily unusable). For this intrusion scenario, Ingate Enhanced Security provides rule packs to upload to the Firewall/SIParator. These rule packs are designed to detect 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 the SIP packets instead of forwarding to the SIP client. This protects 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.

A SIP packet can be redirected, marked/tagged (see Ingate's Quality of Service Module), blocked, rate limited, and of course reported to a reporting agent in the network. In this way, SIP errors of different classifications may be identified and forwarded for analysis. The Ingate Firewall/SIParator can identify packet flows (rather than packet-by-packet analysis), allowing control actions based on accumulated flow information for our IDS/IPS functionality.

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/files/Ingate_QoS_A4_C.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.