INGATE KNOWLEDGE BASE

March 25, 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.

DEMYSTIFYING DEEP PACKET INSPECTION

Deep packet inspection (or DPI) is a powerful way to protect not just SIP traffic, but also the network. DPI is a form of computer network packet filtering that examines the data (or datagram) and UDP/TCP header part of a packet as it passes through an Ingate SIParator or Firewall.

The Ingate is searching for non-protocol compliance, viruses, spam, intrusions or predefined criteria to decide if the packet can pass or if it needs to be routed to a different destination, or for the purpose of collecting statistical information. This is in contrast to shallow packet inspection (usually called just packet inspection) which only checks the UDP/TCP header portion of a packet.

Shallow packet inspection is the kind of inspection commonly found in most NAT firewall devices.

As Ingate SIParators and Firewalls have Deep Packet Inspection capability, Ingate has the ability to look at Layers 2 through 7 of the OSI model. Since the SIP protocol is an Application Layer (Layer 7) in the OSI Model, Ingate products have a unique ability to:

- Look at the SIP protocol packets, to provide non-protocol compliance rules, routing rules and statistical information, and
- Provide IDS/IPS security features for an effective defense against overflow attacks, denial of service (DoS) attacks, and sophisticated intrusions.This includes headers and SIP protocol structures as well as the actual payload of the message.

DPI will identify and classify the SIP traffic based on a signature database that includes information extracted from the data part of a UDP/TCP packet, providing extremely precise of control of any SIP traffic -- finer than any classification based only on header information only.

Want more information

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

Next week

More About SIP Protocol Security
For more information, visit the Ingate Knowledge Base online at www.ingate.com.