INGATE KNOWLEDGE BASE

April 2, 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.

MORE ABOUT SIP PROTOCOL SECURITY: SIP COMPLIANCY

As discussed in last week's Knowledge Base, Ingate SIParators and Firewalls have deep packet inspection (DPI) capability, which gives Ingate the ability to look at Layer 2 through Layer 7 of the OSI model. As the SIP protocol is an application layer (Layer 7) in the OSI model, Ingate products have a unique ability to evaluate the SIP protocol packets and provide non-protocol compliance rules, routing rules and policies. Deep packet inspection also provides an important layer of security.

How else does Ingate ensure security for SIP applications?

Ingate products, which strictly adhere to the SIP protocol, look specifically for SIP compliancy. If there is a failure of SIP protocol compliance, the Ingate will use SIP components such as its full SIP proxy and SIP B2BUA to correct or discard SIP traffic to resolve compliancy issues.

It can also apply policies to correct SIP non-conformances in various applications such as:

removal of VIA headers	SIP method processing rules	MIME content filtering
SIP offer/answer call flow	escaped whitespaces rules	SIP method authentication
URI encoding	session timers	180 response removal
username checks	limitation of media streams	and so much more
UDP packet size	limitation of RTP codecs	

Depending on the nature of the failure to adhere to the protocol, the Ingate can also invoke a denial of service.

Want more information

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

Next week

SIP Security: TLS and SRTP

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