INGATE KNOWLEDGE BASE

ingate

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.

SIP Security III: Routing Rules and Policies

The Deep Packet Inspection capability of Ingate SIParators and Firewalls offer the ability to apply Routing and Dial Plan rules to all incoming SIP traffic. As the Ingate product has the ability to look at Layer 2 through Layer 7 of the OSI model, Routing and Dial Plan rules can combine the use of several layers at once. Combining such things as the TCP/IP (Transport Layer) with the SIP protocol (Application Layer) ensures that only predefined SIP traffic is processed.

Routing Rules
The Ingate Dial Plan has three main attributes:

1. Match From Header, where the Ingate can match on the From Header SIP URI, (the person making the call). In addition the Ingate can separate the Transport whether UDP, TCP or TLS, and further we can specify which IP address or range of IP addresses at the Network layer from which we can accept calls.

2. Matching Request URI. The Request URI Header is a routable header of any SIP Request. The Ingate can Match & Remove a Prefix, Match any specific Alpha/ Numeric characters or even range of characters. This also includes Domain matching.

3. Forward To. The Forward To section defines where to 'actually' send the call – perhaps to a predefined account, with Registration and/or Header Replacement requirements/behavior; or to an IP address or Domain. It can also change the call request to a different Transport and port if required, and even dynamically assign the use of our B2BUA if needed.

The actual Ingate Dial Plan, then, combines these three attributes to provide the ultimate in flexibility and security in defining A) accepting where the call is coming from and B) where the call is going. If the SIP traffic is not predefined it will be denied.

This also gives the ability to have multiple different IP-PBX vendors and multiple different ITSP accounts. N+1 ITSPs to N+1 IP-PBXs. There is no limit to the customization of call routing in the Ingate.

Policies
Policies related to SIP have to do with allowing or disallowing SIP traffic based on SIP Methods, SIP Mime Content, SIP Domains and other higher-level rules. A SIP Method policy can be implemented to ensure incoming SIP packets are matched on the particular SIP Method and Traffic to specified domains. If required, Authentication can be applied for processing the packet. Further policies can be applied to filter MIME Content types, to ensure the type of SIP Traffic is allowed. Filtering based on specific Header information is also possible.

Ingate also has other Routing Rules and Policies that can be applied to allow for SIP Domain forwarding, Static SIP URI forwarding, SIP Registrar Authentication, and more.

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

Next week
SIP Security IV: IDS/IPS and the Ingate Enhanced Security Software Module
For more information, visit the Ingate Knowledge Base online at www.ingate.com.

Ingate Systems Inc.   I   Ph: +1-603-883-6569   I   info@ingate.com   I   www.ingate.com