INGATE KNOWLEDGE BASE

September 24, 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.

NAT Traversal: Why It's Critical for Service Providers

Last week we discussed how SIP trunking is becoming more of a focus for service providers. In this week's Knowledge Base we'll continue that discussion, addressing one of the key issues many service providers are facing when deploying SIP trunks: NAT, or Network Address Translation, traversal.

When connecting enterprises to SIP trunks directly *via* the Internet, carriers must resolve issues created by the enterprise firewall and traverse the NAT to connect to the customer's Local Area Network (LAN) while also maintaining security. Since carriers deploy SIP trunks on a mass scale, the need to offer customers a guaranteed solution that works seamlessly, and is secure, is all the more critical.

Traditional firewalls are designed to block unwanted, or unrecognized, traffic. When a traditional firewall sees SIP communication – voice, in the case of SIP trunking -- the firewall will not recognize that traffic and, as a result, block it. In addition, NAT breaks SIP. SIP is an application layer protocol at layer 7 of the OSI model, whereas NAT is created at the transport or layer 4 of the OSI model. Since the two are in no way connected, NAT will always frustrate the introduction of SIP into a network.

When using SIP, it is necessary to employ an enterprise border element like the Ingate SIParator, that can provide the necessary functionality to resolve these problems. A benefit of the Ingate is that it will not only allow the SIP traffic through but will do so in a way that protects the network (the Ingate Firewall) or just the SIP traffic itself (the SIParator). Either way, Ingate technology is the safest way to enable a SIP trunk installation.

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 links to find out more

- What is Nat?
- No 5 - Digging Deeper
- What is SIP Trunking.pdf

Please visit the Ingate SIP Trunking Community to read more about Ingate and our commitment to bringing SIP Trunking to enterprise networks.

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