

INGATE KNOWLEDGE BASE

January 15, 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 info@ingate.com.

To be removed from the email distribution, send a quick note to sofia@ingate.com.

Digging deeper: how Ingate resolves nat issues

In this issue of the Knowledge Base we'll dig deeper into exactly what problems NAT causes and how Ingate resolves these issues.

As we described in the previous issue, Network Address Translation or NAT is a means of expanding the number of available IP addresses that can be used under the IPv4 addressing scheme. With NAT certain publicly routable IP addresses are provided to a company that has an Internet connection. Other, specific numbers are used by the company for internal communications only, and are not publicly routable, nor are they visible to anyone outside the Local Area Network of that company.

Firewalls do not apply NAT to the Application Layer. As SIP is an Application Layer protocol, the IPv4 addresses and domain resolution are not translated for Application Layer routing. SIP traffic cannot traverse these traditional enterprise firewalls and NAT devices, and as a result, the firewall/NAT device incorrectly routes all SIP traffic, which includes Voice over IP.

When a SIP phone call attempts to traverse a typical firewall, although the TCP/IP addressing is correct, the IP addresses within the SIP protocol information header are not corrected. As a result, when a far-end WAN device receives a SIP request the SIP addresses are the private IP addresses of the SIP device behind the typical firewall. These private IP addresses are not routable back to the original source.

Ingate fixes these issues. Ingate SIParators/Firewalls contain a SIP Proxy, SIP B2BUA, SIP Media Relay, and a SIP Registrar – features not found on traditional firewalls -- that allow the traversal of the IP addresses within the SIP protocol. The Ingate Firewall or SIParator uses these tools to replace the private addresses with publicly routable addresses so that the calls can be connected, and then assigns the correct internal IP address to the call so that it can be delivered to the proper recipient on the inside of the network.

The Ingate will allow the network traversal of VoIP (and SIP trunking) calls to various carriers/service providers from the IP-PBX. It controls both incoming and outgoing SIP communications and routes it to the intended users and devices. The advantage of the Ingate Firewall is that it will allow all voice traffic as well as data traffic to traverse the enterprise firewall/NAT/ALG.

Want more information

Follow the link to find out more

http://www.ingate.com/files/Ingate_Remote_SIP_Connectivity_A4_C.pdf

http://www.ingate.com/files/Solving_Firewall-NAT_Traversal.pdf

Next week

The Problems of Port Forwarding