

SIP and Security

SIP (Session Initiation Protocol) is the new standard for IP-based realtime communication, including telephony, presence, instant messaging, voice and video applications. SIP is a protocol for communication between users, end-point to end-point.

While this new standard allows for many increasingly popular forms of communication there have been problems getting SIP to the private LANs where the users are located. Those problems are solved using products from Ingate Systems or Intertex Data.

Firewalls are required to make the LAN (Local Area Network) private and not a part of the public Internet. They block unwanted access and control data flowing into the network. The shortage of IP-addresses has also led to the need for NATs (Network Address Translators) that allow the use of many private IP-addresses behind a single public IP address. NATs and firewalls (often combined into a single product) both create problems for the SIP protocol. There are two types of problems:

- Normal firewalls will not let the SIP traffic through, since they do not know which ports to open for the voice traffic and at what time. For security reasons a large range of ports cannot be left open at all times
- Behind a NAT, private IP addresses that cannot be accessed from the Internet are used. Thus, an incoming SIP call cannot directly reach a SIP device behind the NAT.

Intertex and Ingate have solved these problems in their SIP capable firewalls and the SIParator™. In these products, a SIP proxy that understands the SIP signalling, controls the firewall and open and close ports in a secure way. This means that the SIP traffic is let through, while the unwanted traffic is still stopped by the firewall. The products also include a SIP registrar, a record-keeper that knows where every SIP device on the private network is. This means that the SIP registrar can direct incoming and outgoing traffic to the correct device, while still hiding the private IP address from the outside.

This method of controlling the firewall and NAT using a proxy and a registrar is superior to other technologies trying to accomplish the same thing, since it both works transparently and preserves security. SIP signalling can even be encrypted using TLS (Transport Layer Security) to hide the signaling and messages sent.

Ingate has developed the Ingate Firewall 1400, a stand-alone firewall for 50-1000 users. Also available is the Ingate SIParator™ 40 which attaches to an existing firewall to SIP enable the network. Intertex Data has focused on the residential and small office market and sells the IX66, a firewall/NAT for up to 30 users that also can be supplied with a built-in ADSL modem.