



# Ingate SIParators™

Your company is communications intensive and you want access to the best in real time person-to-person IP communications. But your attempts at using Voice over IP or presence and instant messaging have failed because your firewall blocks SIP-based traffic. The Ingate SIParator™ is a product that seamlessly works with your existing firewall, allowing employees to utilize SIP-based applications.

## Internet, the LAN and Firewalls

Every business has a Local Area Network (LAN) with Internet access. To maintain privacy and security on the LAN, it is protected and separated from the public Internet by a firewall. Current firewalls are designed to allow communication from computers on the LAN, behind the firewall, to servers on the Internet and to allow sharing of one single public IP address. Today, there are more efficient methods of Internet communications, including presence, instant messaging (IM), conferencing and VoIP. However, these applications require that SIP capabilities be added to the existing firewall.

The Ingate SIParator™ is the only product of its kind and allows you to add SIP transparency to your network. The SIParator™ is designed to support a full range of capacity requirements and is compatible with all commercially available firewalls.

The Ingate SIParator™ performs all SIP proxy and registrar functions. The registrar holds the private IP addresses of the users inside your network, allowing the SIParator™ to relay SIP signalling. Once the session has been initiated, the agreed UDP or TCP ports are opened and the SIParator™ relays the media streams. This functionality enables SIP communications also to and from NATed networks.

Ingate® offers SIParators™ for small, medium and large enterprises. The SIParator™ can be configured as a part of the DMZ or in a standalone mode. In both cases, the benefits of SIP-based communications can be added to the network simply and easily.

## SIP transparency

Existing commercially available firewalls prevent delivery of realtime SIP-based communications. Some existing firewalls will allow SIP messages through port 5060, but media stream is not supported. Using Ingate's SIP technology, this problem is solved. The Ingate SIP proxy negotiates between the two end points and dynamically opens the media ports in the SIParator™ necessary to allow the traffic to flow. Enterprises that want the time and cost saving benefits of interoperable, universal realtime communications without replacing their existing firewall can purchase a one-box solution: the Ingate SIParator™.

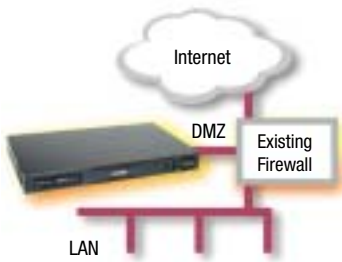
All Ingate SIParators™ are cost-effective and scalable, designed to meet the needs of today's dynamic enterprises. For more information, please visit our website at [www.ingate.com](http://www.ingate.com)



**inGate®**

[www.titan-tech.net](http://www.titan-tech.net)

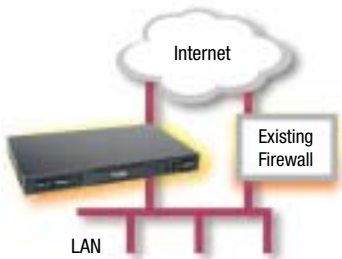
Configuration 1: DMZ



Configuration 2: DMZ/LAN



Configuration 3: Parallel



### Configuration 1: DMZ

The Ingate SIPParator™ connects to the existing firewall through the DMZ interface. All traffic will pass through the existing firewall. The configuration requires that a static range of UDP and TCP ports are opened between the Internet and the SIPParator™ and between the SIPParator™ and the LAN. SIP clients on the LAN need to have the SIPParator™ defined as their outgoing proxy or be referred to it via DNS. The firewall continues to control security, but SIP traffic is routed to the LAN only via the SIPParator™.

### Configuration 2: DMZ/LAN

The Ingate SIPParator™ connects to the DMZ of the existing firewall and to the LAN. This means that SIP traffic and media streams only have to pass through the existing firewall once (or not at all for calls inside the office). A static range of UDP and TCP ports need to be opened in the firewall between the Internet and the SIPParator™. SIP clients on the LAN need to have the SIPParator™ defined as their outgoing proxy or be referred to it via DNS.

### Configuration 3: Standalone

The Ingate SIPParator™ connects to both the LAN and the Internet, operating entirely in parallel with the existing firewall. The SIPParator™ will only handle SIP signalling and media streams; everything else will pass through the existing firewall. This setup has no requirements for the existing firewall and requires no configuration changes. SIP clients on the LAN need to have the SIPParator™ defined as their outgoing proxy or be referred to it via DNS.

## Technical Specifications Ingate SIPParators™

Feature	Ingate SIPParator 20	Ingate SIPParator 40	Ingate SIPParator 80	Ingate SIPParator 88
Processor	VIA C3,533	Celeron 566	Athlon XP 1800+	Athlon MP 1800+
Operating System	Linux 2.4	Linux 2.4	Linux 2.4	Linux 2.4
Interfaces (10/100 Mbit/s)	2	2	2	2
Interfaces (1 Gbit/s)	No	No	Yes	Yes
Redundant Power Supply	No	No	No	Yes
Dimensions WxDxH – mm	220x254x44	482.6x254x44	482.6x460x177	482.6x460x177
Dimensions WxDxH – inch	8.66"x10"x1.75"	19"x10"x1.75"	19"x18"x7"	19"x18"x7"
Certifications	CE, FCC, UL	CE, FCC, UL	CE, FCC, UL	CE, FCC, UL
<b>Management</b>				
Automatic check for new release	Yes	Yes	Yes	Yes
Web GUI	Yes	Yes	Yes	Yes
DHCP client	Yes	Yes	Yes	Yes
SNMP	Yes	Yes	Yes	Yes
Internal log to HD	No	Yes	Yes	Yes
Syslog	Yes	Yes	Yes	Yes
E-mail events	Yes	Yes	Yes	Yes
Free software upgrades	Yes	Yes	Yes	Yes
<b>SIP Functionality</b>				
SIP Proxy	Yes	Yes	Yes	Yes
SIP Registrar	Yes	Yes	Yes	Yes
SIP traffic out&in without extra proxy	Yes	Yes	Yes	Yes
SIP traffic to private IP addresses (NAT/PAT)	Yes	Yes	Yes	Yes
TLS encryption	Yes	Yes	Yes	Yes
SIP connection set up (SIP+RTP)	0.15 s	0.15 s	<0.15 s	<0.15 s
RTP-data delay (10mbps/100mbps network)	0.19/0.08 ms	0.19/0.08 ms	0.19/0.08 ms	0.19/0.08 ms
Number of concurrent RTP sessions	50	180	400	800
Registered SIP users included	10	50	50	50
Max recommended registered SIP users	400	1000	4000	8000

**inGate**®

www.titan-tech.net