Configuring a LAN SIParator

Lisa Hallingström

Paul Donald

Bogdan Musat

Adnan Khalid

Per Johnsson

Rickard Nilsson

Table of Contents

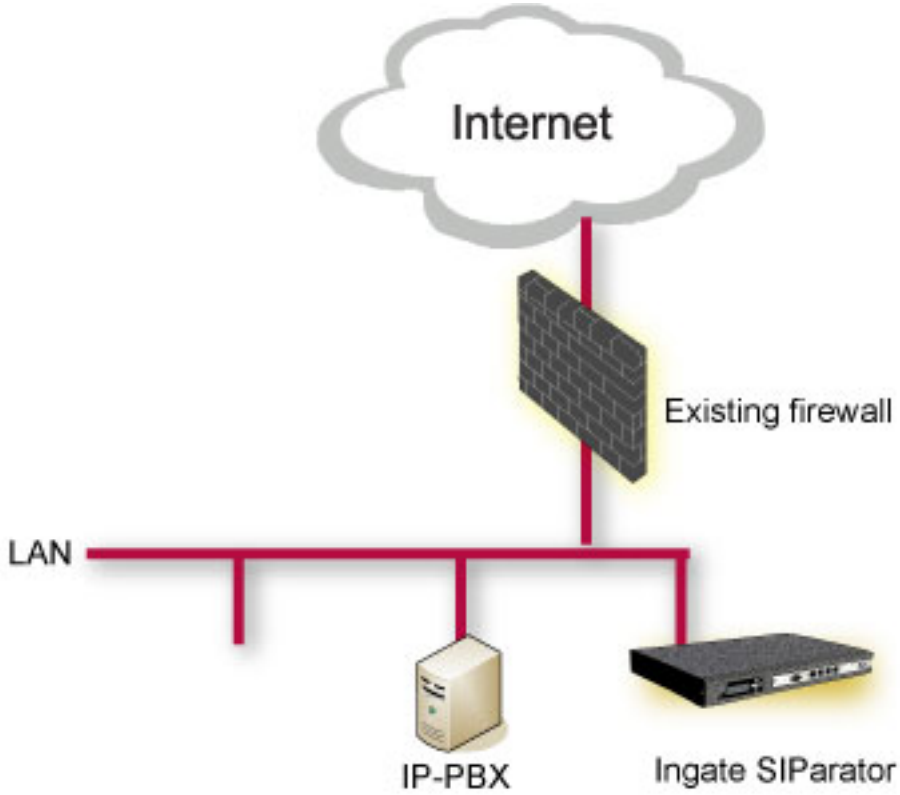
Ingate SIParator version: 4.6.2

Document version: 1.0

LAN SIParator

For various reasons, you might want to use a separate SIP server instead of the built-in server in the SIParator. That SIP server would be located on the inside or maybe on a DMZ.

With the LAN SIParator, you connect the SIParator to a NATed network.



Here are the settings needed for this. It is assumed that the SIParator already has a network configuration. Only the additional SIP settings are listed.

In the instructions below, some settings are marked like this:

> This setting is made by the Startup Tool

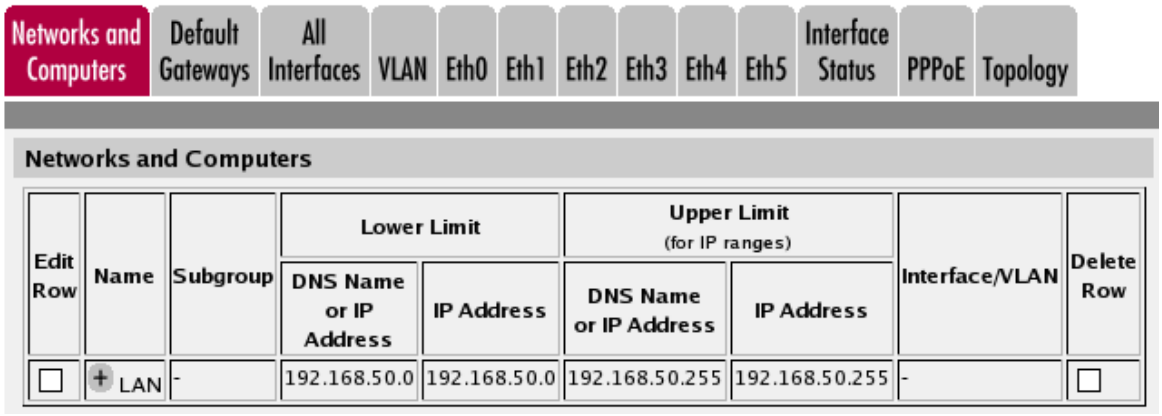
This means that if you started by configuring your SIParator using the Ingate Startup Tool, this setting will already be correct.

Networks and Computers

The SIParator must know the network structure to be able to function properly. On the **Networks and Computers** page, you define all networks which the SIParator should serve and which are not reached through the default gateway of the *firewall*. All computers that can reach each other without having to go through the firewall connected to the SIParator should be grouped in one network.

You can also define networks and parts of networks for other configuration purposes.

This setting is made by the Startup Tool



Topology

To make the SIParator aware of the network structure, the networks defined above should be listed on the **Topology** page.

Settings in the **Surroundings** table are only required when the SIParator has been made the **DMZ** type.

The SIParator must know what the networks around it look like. On this page, you list all networks which the SIParator should serve and which are not reached through the default gateway of the *firewall*.

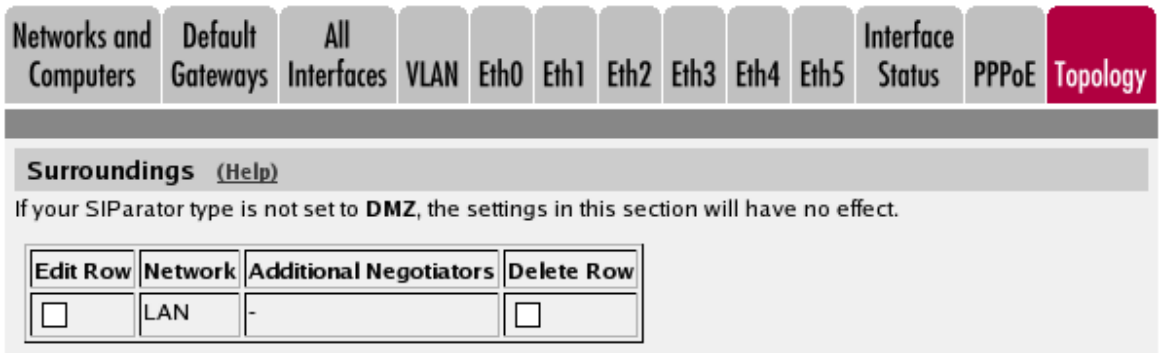
All computers that can reach each other without having to go through the firewall connected to the SIParator should be grouped in one network. When you are finished, there should be one line for each of your firewall's network connections (not counting the default gateway).

One effect of this is that traffic between two users on different networks, or between one of the listed networks and a network not listed here, is NAT:ed.

Another effect is that for connections between two users on the same network, or on networks where neither is listed in Topology, no ports for RTP sessions will be opened, since the SIParator assumes that they are both on the same side of the firewall.

For DMZ and LAN SIParators, at least one network should be listed here. If no networks are listed, the SIParator will not perform NAT for any traffic.

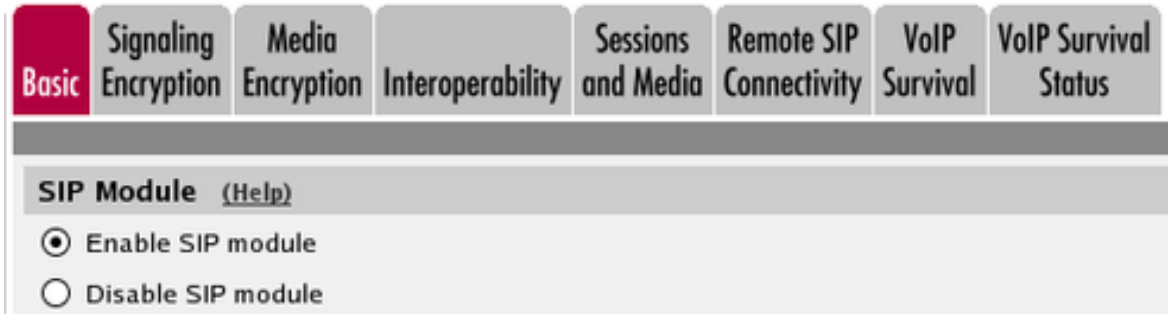
This setting is made by the Startup Tool

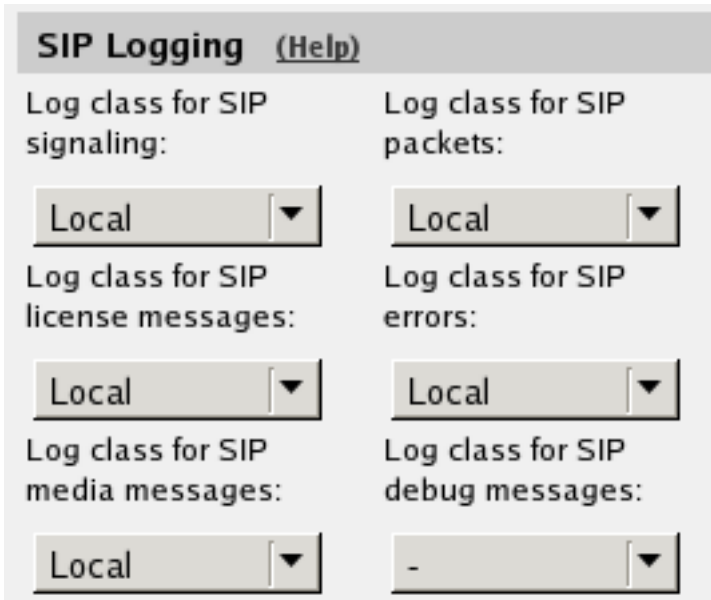


Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool



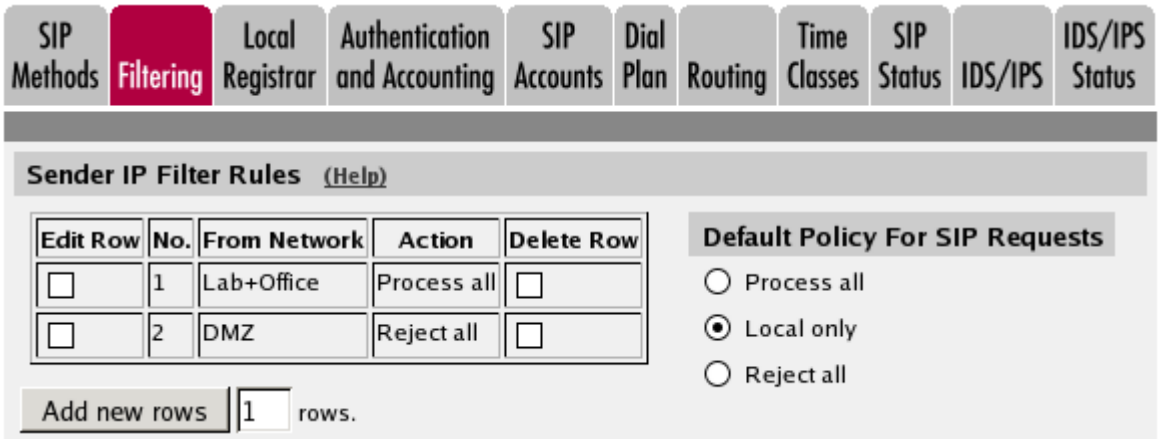


Filtering

To allow SIP traffic through the SIParator, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the SIParator does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.

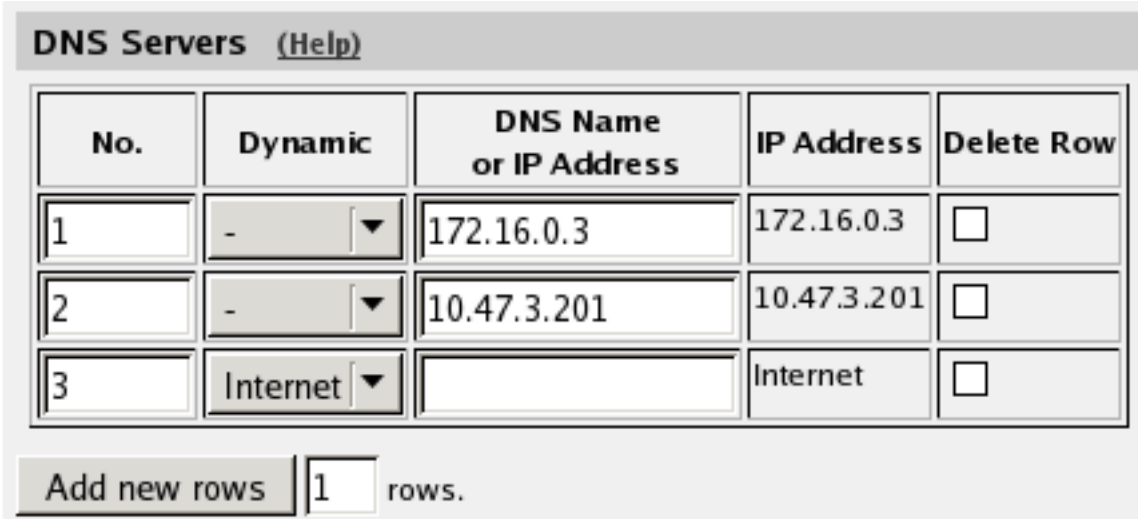
This setting is made by the Startup Tool



Basic Configuration

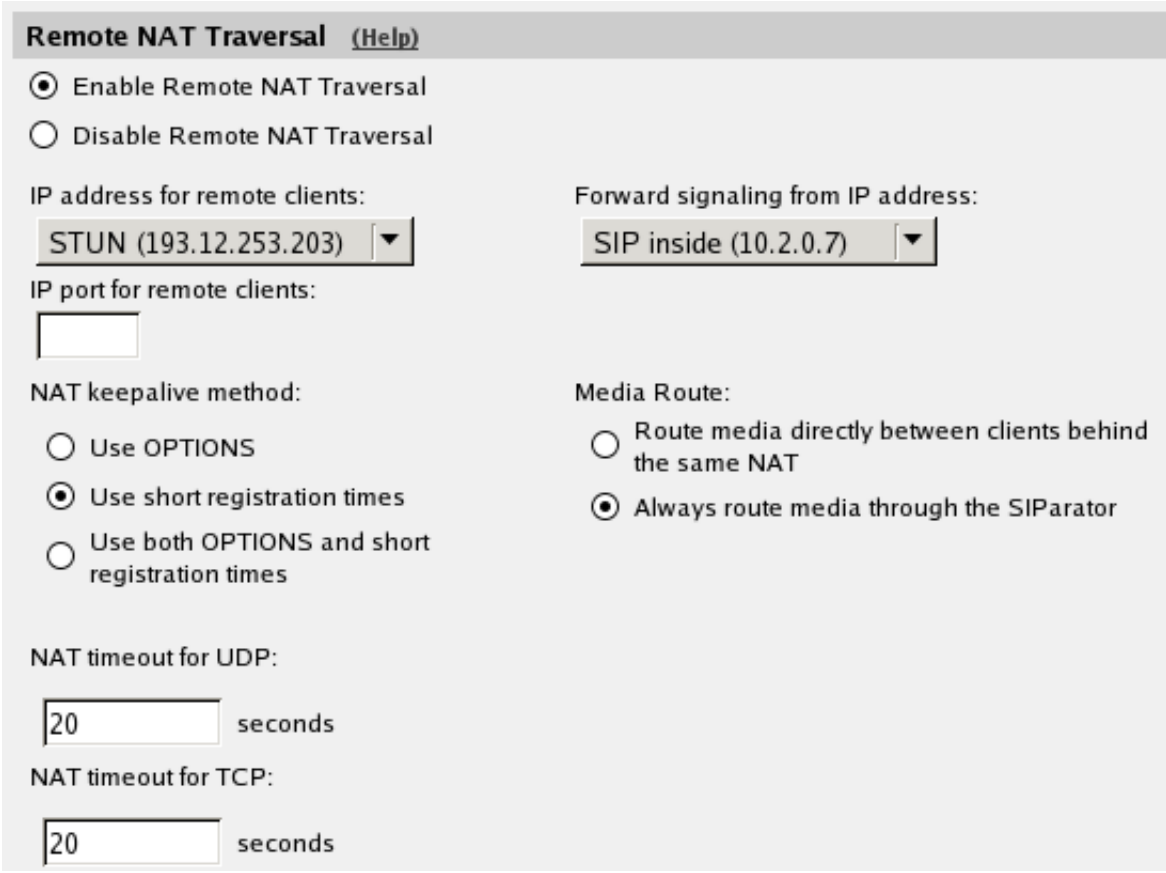
The SIParator must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

This setting is made by the Startup Tool



Remote SIP Connectivity

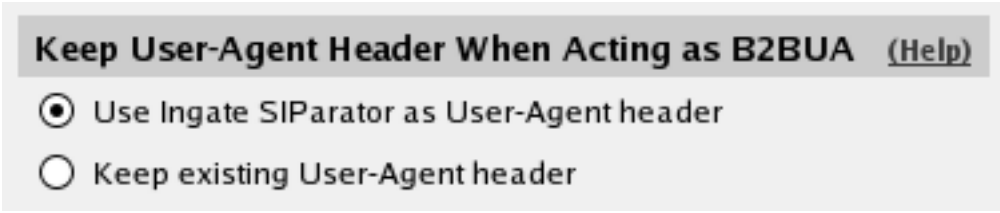
If you have remote SIP clients behind other NAT boxes, you need to activate **Remote NAT Traversal**.



Interoperability

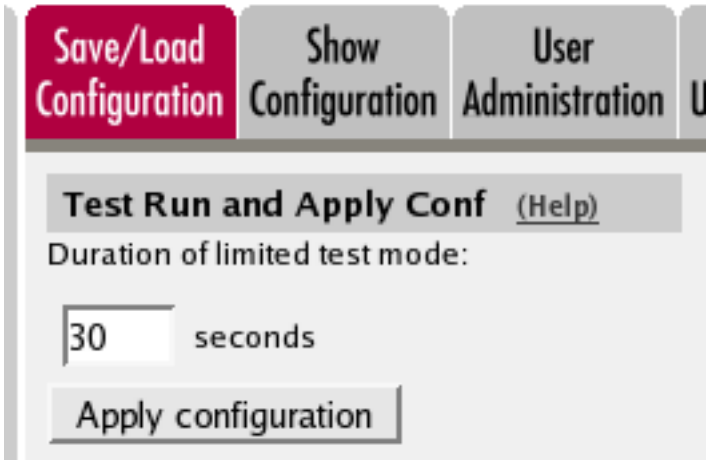
You need to enter the public IP that corresponds to the SIParator under **Public IP address for NATed SIParator**. This will make the SIParator able to rewrite outgoing SIP packets properly.

This setting is made by the Startup Tool

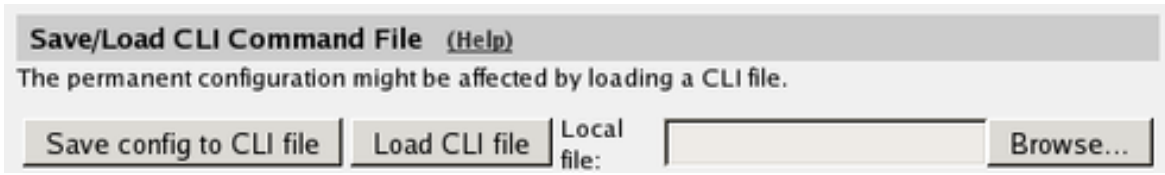


Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



The Firewall

The firewall in front of the LAN SIParator must be configured in this way:

- There must be a static IP address that can be mapped to the SIParator's private IP address. All traffic to this IP address must be forwarded to the SIParator.
- When the firewall forwards traffic to the SIParator, it must not NAT this traffic, i.e. the SIParator needs to see the original sender IP address.
- All outgoing traffic from the SIParator should be allowed through the firewall.
- For outgoing traffic from the SIParator, the firewall needs to use the same IP address as above when performing NAT. If another IP address is used, some SIP signaling will go awry, and Remote SIP Connectivity will not always work properly.
- For outgoing traffic from the SIParator the firewall must not change sender port when performing NAT. If it does change port, Remote SIP Connectivity will not always work properly.