

**Environment: Ingate Firewall 4.6.2**  
**ITSP used : Firstreach, Mynetfone, Engin, Faktortel.**  
**Local PBX used: Quadrom32x**

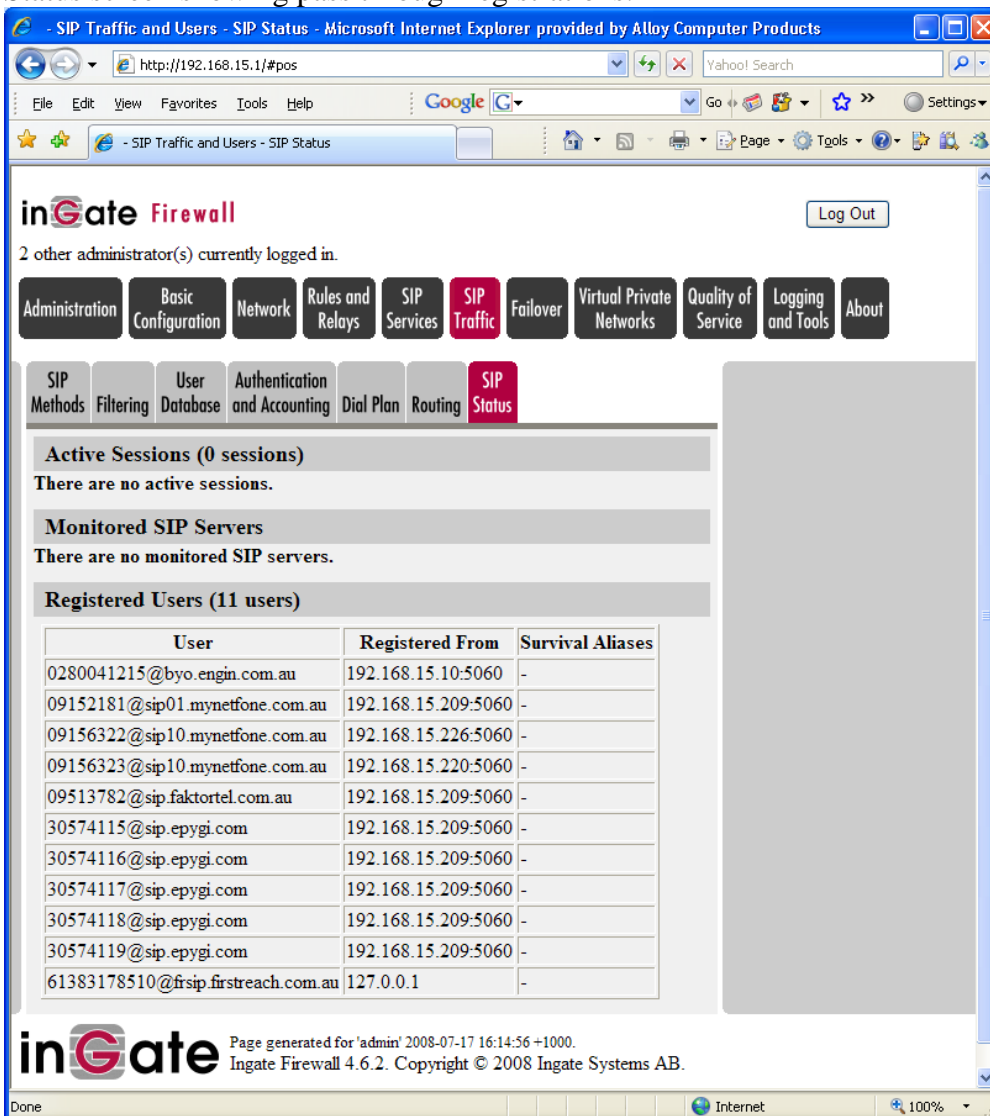
**Ingate Firewall Eth1 : on Public Internet Address.**  
**Ingate Firewall Eth0 : on Private IP address Range.**  
**Ingate Firewall Rules : Single Rule “Forward all LAN traffic to WAN (via NAT)”**

**Section 1.** SIP Passthrough.

With the SIP Module enabled and no optional Licenses the Ingate Firewall will dynamically handle any pass through registrations with SIP Servers, ie ITSP accounts.

It will perform all NAT traversal of outbound calls to the SIP server, and allow inbound calls from registered accounts.

Status screen showing pass through registrations.



The screenshot shows the Ingate Firewall web interface in Microsoft Internet Explorer. The page title is "SIP Traffic and Users - SIP Status". The navigation menu includes: Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (selected), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. The "SIP Status" sub-menu is active, showing "Active Sessions (0 sessions)", "Monitored SIP Servers", and "Registered Users (11 users)".

User	Registered From	Survival Aliases
0280041215@byo.engin.com.au	192.168.15.10:5060	-
09152181@sip01.mynetfone.com.au	192.168.15.209:5060	-
09156322@sip10.mynetfone.com.au	192.168.15.226:5060	-
09156323@sip10.mynetfone.com.au	192.168.15.220:5060	-
09513782@sip.faktortel.com.au	192.168.15.209:5060	-
30574115@sip.epygi.com	192.168.15.209:5060	-
30574116@sip.epygi.com	192.168.15.209:5060	-
30574117@sip.epygi.com	192.168.15.209:5060	-
30574118@sip.epygi.com	192.168.15.209:5060	-
30574119@sip.epygi.com	192.168.15.209:5060	-
61383178510@frsip.firstreach.com.au	127.0.0.1	-

Page generated for 'admin' 2008-07-17 16:14:56 +1000.  
Ingate Firewall 4.6.2. Copyright © 2008 Ingate Systems AB.

## Section 2. SIP Back to Back UA. (2 Call Legs)

In this mode the local LAN PBX makes a call to the Ingate, the Ingate makes a second call to the ITSP, and joins the 2 sides. It is used with PBX systems that don't normally work with the ITSP correctly on their own.

This mode requires the SIP Trunking Module.

- a. Create a Local SIP User entry with the account details of the ITSP.  
Account type = XF/Register  
From should be your WAN interface or Specific WAN IP.

The screenshot shows the InGate Firewall web interface in Microsoft Internet Explorer. The browser address bar shows `http://192.168.15.1/#pos`. The page title is "- SIP Traffic and Users - User Database". The interface includes a navigation menu with buttons for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this is a sub-menu with buttons for SIP Methods, Filtering, User Database (highlighted), Authentication and Accounting, Dial Plan, Routing, and SIP Status. The main content area is divided into two sections: "Local SIP Domains" and "Local SIP User Database". The "Local SIP User Database" section contains a table with the following data:

Username	Domain	Authentication Name	Password	Account Type	Register From	Delete
61383178510	frsip.firstreach.cor	61383178510	Change Password	XF/Register	WAN_IP	<input type="checkbox"/>

At the bottom of the page, there are "Save" and "Undo" buttons. The footer text reads: "inGate Page generated for 'admin' 2008-07-17 16:22:20 +1000. Ingate Firewall 4.6.2. Copyright © 2008 Ingate Systems AB."

Once Created it should show as registered on the SIP Status Screen.

SIP Methods Filtering User Database Authentication and Accounting Dial Plan Routing **SIP Status**

**Active Sessions (0 sessions)**  
There are no active sessions.

**Monitored SIP Servers**  
There are no monitored SIP servers.

**Registered Users (11 users)**

User	Registered From	Survival Aliases
0280041215@byo.engin.com.au	192.168.15.10:5060	-
09152181@sip01.mynetfone.com.au	192.168.15.209:5060	-
09156322@sip10.mynetfone.com.au	192.168.15.226:5060	-
09156323@sip10.mynetfone.com.au	192.168.15.220:5060	-
09513782@sip.faktortel.com.au	192.168.15.209:5060	-
30574115@sip.epygi.com	192.168.15.209:5060	-
30574116@sip.epygi.com	192.168.15.209:5060	-
30574117@sip.epygi.com	192.168.15.209:5060	-
30574118@sip.epygi.com	192.168.15.209:5060	-
30574119@sip.epygi.com	192.168.15.209:5060	-
61383178510@frsip.firstreach.com.au	127.0.0.1	-

**inGate** Page generated for 'admin' 2008-07-17 16:25:14 +1000.  
Ingate Firewall 4.6.2. Copyright © 2008 Ingate Systems AB.

Internet 100%

b. You need to create a dialplan that will trigger the second call leg via the ITSP registration for outbound calls.

In this case we use :

- A Matching From Header to define any Invite from the LAN side
- A Forward to destination of the ITSP Account configured previously
- Then combine these 2 in the Dialplan for outbound calls.

The screenshot shows the Asterisk SIP Traffic and Users web interface in Microsoft Internet Explorer. The browser address bar shows 'http://192.168.15.1/#pos'. The interface has a navigation menu with tabs for SIP Methods, Filtering, User Database, Authentication and Accounting, **Dial Plan**, Routing, and SIP Status. The 'Dial Plan' tab is active.

Under the 'Dial Plan' tab, there are three main sections:

- Use Dial Plan (Help)**: Includes radio buttons for 'On', 'Off', and 'Fallback'. The 'Emergency Number' is set to '911'.
- Matching From Header (Help)**: A table for defining matching criteria.
 

Name	Use This ...		... Or This	Transport	Network	Delete
	Username	Domain	Reg Expr			
QuadroM32x	*	*		Any	LAN	<input type="checkbox"/>
- Forward To (Help)**: A table for defining forwarding destinations.
 

Name	Subno.	Use This ...	... Or This			... Or This	Delete
		Account	Replacement URI	Port	Transport	Reg Expr	
Firstreach_WAN	1	61383178510@frsip.firstreach.com.au			-		<input type="checkbox"/>
- Dial Plan (Help)**: A table for defining dial plan rules.
 

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete
					Forward	ENUM				
1	QuadroM3	-	Forward	Firstreach_WAN			-	-		<input type="checkbox"/>

- c. Now calls from the ITSP need to be forwarded back to the LAN side PBX. On the Routing TAB, add an entry to match inbound calls from the ITSP, and send them direct back to a Valid SIP URL for the LAN PBX. Ie [00@192.168.15.208](mailto:00@192.168.15.208) Ext 00 on the PBX.

**inGate Firewall** Log Out

2 other administrator(s) currently logged in.

Administration Basic Configuration Network Rules and Relays SIP Services **SIP Traffic** Failover Virtual Private Networks Quality of Service Logging and Tools About

- Changes have been made to the preliminary configuration, but have not been applied.

SIP Methods Filtering User Database Authentication and Accounting Dial Plan **Routing** SIP Status

### DNS Override For SIP Requests (Help)

Domain	Relay To						Delete
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	
Add new rows <input type="text" value="1"/> groups with <input type="text" value="1"/> rows per group.							

### SIP Routing Order (Help)

No.	Routing Function
<input type="text" value="1"/>	Local Registrar
<input type="text" value="2"/>	DNS Override
<input type="text" value="3"/>	Dial Plan

Add new rows  rows.

### Class 3xx Message Processing (Help)

Forward all  
 Follow redirects

### User Routing (Help)

User	Alias	Restrict Incoming Callers	Forward		Send To Voice Mail	Time Class	Comment	Delete
			Action	To				
61383178510@frsip.firstreach.com.au		Off	Forward	00@192.168.15.2	-	-		<input type="checkbox"/>
Add new rows <input type="text" value="1"/> rows.								

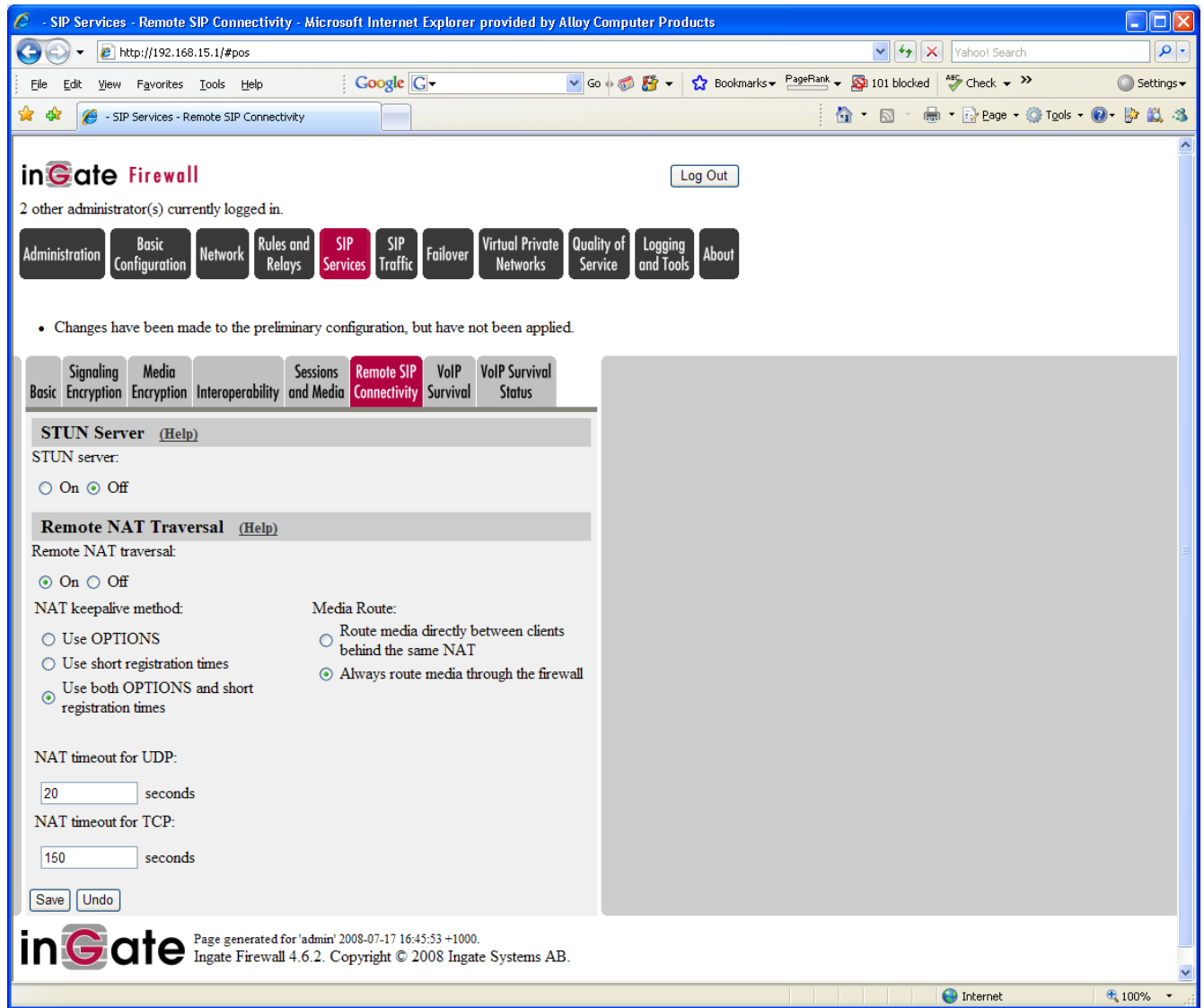
Done Internet

**Section 3.** Registering remote IP Phones to a LAN side PBX. With both Remote and Local Side NAT.

This is where you have multiple remote IP Phones that need to register with a LAN side PBX which is behind NAT. Many PBXs don't support far end NAT traversal very well, the ingate can remap all ports and Payload to ensure this works.

This mode requires the Remote SIP Connectivity Module

- a. Ensure the remote NAT traversal mode is enabled.



- b. Create a DNS Override Rule for SIP requests.  
 This will detect WAN side Invites and Registrations and MAP them to the LAN side PBX.  
 Domain = WAN IP or DNS Name (our remote Phone register to this address)  
 Relay to section = the LAN side IP-PBX (transport and ports can be remapped if required)

The screenshot shows the inGate Firewall web interface. The browser address bar displays `http://192.168.15.1/#pos`. The interface includes a navigation menu with tabs for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (selected), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. A notification states: "Changes have been made to the preliminary configuration, but have not been applied." The "Routing" tab is active, showing the "DNS Override For SIP Requests" section. Below this, there is a table with columns: Domain, DNS Name or IP Address, IP Address, Port, Transport, Priority, Weight, and Delete. A single row is present with the following values: Domain: 203.100.253.51, DNS Name or IP Address: 192.168.15.10, IP Address: 192.168.15.10, Port: 5060, Transport: UDP, Priority: (empty), Weight: (empty), and Delete: (checkbox). Below the table, there are controls for "Add new rows" (set to 1) and "groups with 1 rows per group." Other sections visible include "SIP Routing Order" (with a table for No., Routing Function), "Class 3xx Message Processing" (with radio buttons for Forward all and Follow redirects), "Static Registrations" (with a table for Requests To User, Also Forward To, and Delete), and "Local REFER Handling".

Domain	Relay To						Delete
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	
203.100.253.51	192.168.15.10	192.168.15.10	5060	UDP			<input type="checkbox"/>