



Date: 18/02/08
Revision Date (6 months max):

Topic / Issue: **Shoretel SIP Trunking on Ingate**

Written By: Greg.

Public Directory: N/A

Shoretel SIP Trunking on Ingate.

Requirements,

- 1) Any Ingate SIParator or Ingate Firewall model will require a SIP Trunking module installed.
- 2) Some SIP traversal licenses are included with the Ingate base unit at delivery. You need to confirm if the base licensing supports the number of SIP Traversals required. If not additional SIP traversal Licenses can be purchased.

Opertating modes.

Shoretel SIP trunks need to use the B2BUA of the Ingate.

This In effect creates 2 call legs,

- 1) between the shoretel and Ingate
- 2) between the Ingate and the Provider.

Most providers require prior registration to perform SIP Trunking - some Do Not.

This document does not focus on the Shoretel to Ingate setup, this should be provided by your local Shoretel Channel. This document will focus on the Ingate to ITSP side configuration.

Specifics for this example:

Shoretel PBX = 10.0.0.1

Ingate ETH0 (LAN) = 10.0.0.100

Ingate ETH1 (WAN) = 192.168.15.254

Shoretel Side (in brief):

Shoretel PBX is configured with Its Trunk Partner IP address pointing to the Ingate
Shoretel "SIP Trunk Type" – "Use IP Address" = 10.0.0.100

Trunks [New](#) [Copy](#) [Save](#) [Delete](#) [Reset](#) [Help](#)

Edit Trunk * modified

Edit this record [Refresh this page](#)

Site: Headquarters

Trunk Group: SIP Masergy

Name:

Switch:

SIP Trunk Type:

Dynamic

Use IP Address:

Number of Trunks (1 - 120):

Ingate Side :

The Ingate can be configured using two alternative methods:

- (a) the Ingate StartupTool wizard for a complete first time configuration, or
- (b) the traditional configuration via the GUI.

The latter is more suitable if you already have your Ingate configured and operational in your network. Select one of these methods for configuration of the Ingate unit.

Step 1 – Basic Ingate IP Address setup.

1) Download the Ingate Startup Tool.

This tool is available on-line (not on the CD)

Once downloaded you can use this to setup the initial settings on the unit.

On first run select “Configure the unit for the first time”

- a) Enter the MAC address of the unit.
- b) The IP address required to be stored onto it. (ensure your PC has access to this IP Address)
- c) Select password of “admin”

Use the “Contact” button – if it reports as failed, then it wait 60 seconds and try connecting to the settings defined above, but this time use the “update configuration” option with the IP Address you initially selected.

Use the “Establish Contact” button to connect to the unit.

Once connected, use the “Configure Network Topology” Button.

In this case we will not configure the Optional “SIP Trunking” or “Remote SIP Connectivity”

2) Use a serial cable connection in the event that the startup tool fails.

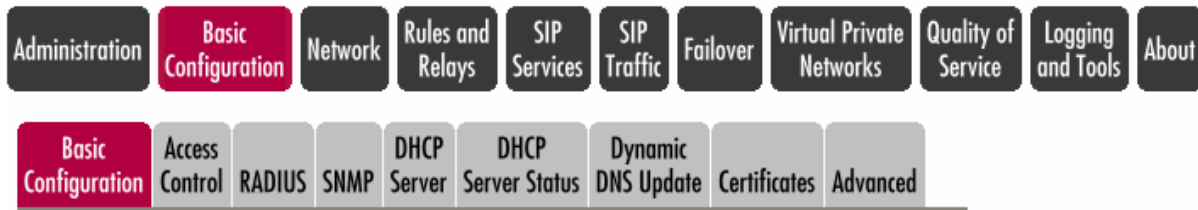
Speed = 19200

Settings = 8 Bits, 1 Stop, No Parity.

Once connected enter username “admin” and password “admin” to login.

On first run it will prompt you on the initial settings.

Step 2 – Basic Configuration.



Sub Menu : **Basic Configuration – DNS Servers**

You **MUST** define DNS servers.

Sub Menu : **Access Control**

You **MUST** define who can manage the Ingate for – Interface, Transport and Computers

Sub Menu : **Siparator Type (only for Siparator models)**

You **MUST** define the way the Siparator is connected to your existing firewall.
(see definitions below)

THE DMZ CONFIGURATION

Using this configuration, the SIParator is located on the DMZ of your firewall, and connected to it with only one interface. You need to open the SIP port (normally UDP port 5060) and a range of UDP ports for RTP traffic to and from the SIParator on your firewall. The SIP traffic finds its way to the SIParator using DNS. Internal clients can have the SIParator as an outbound proxy.

THE DMZ/LAN CONFIGURATION

Using this configuration, the SIParator is located on the DMZ of your firewall, and connected to it with one of the interfaces. The other interfaces are connected to your internal networks. The SIParator can handle several networks on its interface even if they are hidden behind routers. Internal users have to configure the SIParator as outbound proxy, or an internal proxy as to use the SIParator as its outbound proxy.

THE STANDALONE CONFIGURATION

Using this configuration, the SIParator is connected to the outside world on one interface and your internal networks on the others. It will run in parallel with your firewall and only handle the SIP traffic. Internal users have to configure the SIParator as outbound proxy, or an internal proxy as to use the SIParator as its outbound proxy.

Step 3 – Network.



Sub Menu : [Networks and Computers](#)

You **MUST** define as a minimum your LAN and the WAN – Typically the WAN can be everything else (be specific with the Interface eth1 for example) Note that local loopback 127.0.0.1 is not listed.

Networks and Computers							
Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
+ LAN	-	10.0.0.0	10.0.0.0	10.0.0.255	10.0.0.255	inside (eth0 untagged)	<input type="checkbox"/>
+ WAN	-	0.0.0.0	0.0.0.0	127.0.0.0	127.0.0.0	outside (eth1 untagged)	<input type="checkbox"/>
	-	127.0.0.2	127.0.0.2	255.255.255.255	255.255.255.255	outside (eth1 untagged)	<input type="checkbox"/>

Sub Menu : [Networks and Computers – Default Gateways](#)

You **MUST** define a default Gateway.

Sub Menu : [Networks and Computers – All Interfaces](#)

Correctly select if the Interface is enabled, and provide logical names for the Interfaces.

You need to define “directly connected Networks”, and associate those networks to Interfaces.

Interface Overview

General				
Physical Device	Interface Name	This Interface Is	Obtain IP Address Dynamically	Speed and Duplex
eth0	inside	On	OFF	Autonegotiation
eth1	outside	On	OFF	Autonegotiation
eth2	Ethernet2	Off	OFF	Autonegotiation

Directly Connected Networks <small>(Help)</small>									
Name	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	Interface	VLAN Id	VLAN Name	Delete
inside	10.0.0.100	10.0.0.100	255.255.255.0	10.0.0.0	10.0.0.255	inside (eth0)		-	<input type="checkbox"/>
outside	192.168.20.254	192.168.20.254	255.255.255.0	192.168.20.0	192.168.20.255	outside (eth1)		-	<input type="checkbox"/>

Add new rows rows.

Sub Menu : [Networks and Computers – NAT \(Firewall only.\)](#)

Correctly define if NAT is required between the interfaces. Do you want to NAT LAN to WAN ?

Sub Menu : [PPPoE \(only if an Interface is used for PPPoE Connection\)](#)

Step 4 – Rules and Relays (Firewall Mode only).

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

Rules Relays DHCP Relay Services Protocols Time Classes

Rules												
Rule No.	Rule State	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete
1	On	LAN	-	WAN_1	-	Ethernet0 -> Ethernet1 (NAT:ed)	icmp/udp/tcp	Allow	24/7	Local	all	<input type="checkbox"/>

Add new rows rows.

Sub Menu : **Rules**

You will probably want to define outbound rules for (non VoIP) traffic.

In the example above all internal LAN traffic is allowed Out to the WAN

Note: Traffic will be processed via NAT (see Network – NAT configuration)

Step 5 – SIP Services.

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

Basic Signaling Encryption Media Encryption Interoperability Sessions and Media Remote SIP Connectivity VoIP Survival VoIP Survival Status

Sub Menu : **Basic**

You **MUST** enabled the SIP Module.

Step 6 – SIP Traffic.

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

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

Sub Menu : **Filtering**

You **MUST** ensure that the **Default Policy for SIP Requests = Process All**

Sub Menu : **User Database**

If your carrier requires active registration for SIP Trunking then define the carrier settings here.

Local SIP User Database (Help)

Username	Domain	Authentication Name	Password	Account Type	Register From	Delete
09152181	sip01.mynetfone.d	09152181	Change Password	B2BUAWM/Register	WAN_1	<input type="checkbox"/>

Add new rows 1 rows.

Account Type should be **B2BUAWM/Register**

Register from should be **WAN**

Sub Menu : **Dial Plan**

The Use Dial Plan setting must be ON

Use Dial Plan (Help) **Emergency Number** (Help)

On Off Fallback

Emergency Number: 911

Matching From Header (Help)

Name	Use This Or This	Transport	Network	Delete
	Username	Domain	Reg Expr			
Shoretel	*	localhost		Any	LAN	<input type="checkbox"/>

Add new rows 1 rows.

The From Header :

This is the key to matching outbound calls from shoretel to the carrier.

The from Header Domain can match how the shoretel would normally format its from addresses.

In the example above the invites from header would look like.

“from: 1234@localhost”

or..

In its simplest mode, the domain could be “*” as long as the network is defined as “LAN”

(Caution: doing this is **not** very specific, and can create overlapping rules if not careful)

Matching Request-URI (Help)

Name	Use This Or This	Delete
	Prefix	Head	Tail	Min. Tail	Reg Expr	
Inbound calls			any character		192.168.15.254	<input type="checkbox"/>

Add new rows 1 rows.

The Matching Request-URI should be used to match the inbound calls from the Carrier (ITSP)

This may be an IP address or a host Name (Carrier and setup dependant)

Note: Matching Request-URI and Matching From Headers simply provide specific matches to SIP Invites. The Ingate needs to match new Invites to either inbound or outbound traffic directions. It is possible to use any combination in either of these 2 sections. Ie both in and out traffic defined by request-URI or From Header, or as above one in each.

Forward To [\(Help\)](#)

Name	Subno.	Use This Or This			... Or This	Delete
		Account	Replacement URI	Port	Transport	Reg Expr	
+ Shoretel in	1	-	10.0.0.1		-		<input type="checkbox"/>
+ Shoretel out	1	09152181@sip01.mynetfone.com.au			-		<input type="checkbox"/>

Add new rows groups with rows per group.

The Forward To This is used in the dial plan for destination mapping of SIP calls. For Carrier Services that allow both sending and receiving of calls you will need 2 entries – one for either direction. The “Shoretel in” forwards calls to the LAN IP address (Replacement URI) of the Shoretel server. The “Shoretel out” forwards the calls via a registered SIP Trunk account.

Dial Plan [\(Help\)](#)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete
					Forward	ENUM				
1	-	Inbound calls	Forward	Shoretel in			-	24/7		<input type="checkbox"/>
2	Shoretel	-	Forward	Shoretel out			-	-		<input type="checkbox"/>

Add new rows rows.

The Dial Plan This is used in glue the matching rules and the forwarding rules together and active them. Matches exist in both directions, and 2 Dial Plan rules are created with forwarding addresses.

Sub Menu : [Routing](#)

On Shoretel systems you **MUST enable “Local REFER Handling”**
Tick the “Always handle REFER locally” option box.

Sub Menu : [SIP Status](#)

Confirm that your Carrier SIP registration is OK.

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

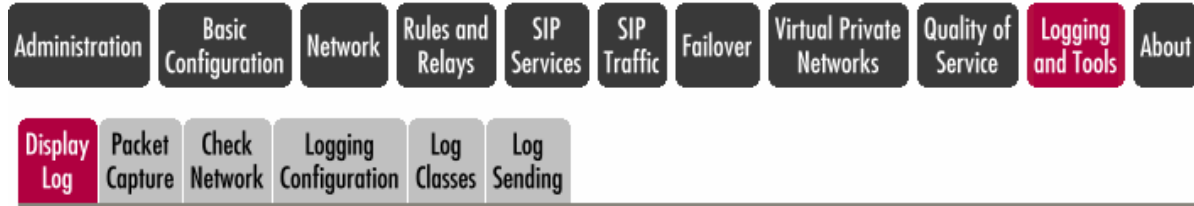
Active Sessions (0 sessions)
There are no active sessions.

Monitored SIP Servers
There are no monitored SIP servers.

Registered Users (1 users)

User	Registered From	Survival Aliases
09152181@sip01.mynetfone.com.au	127.0.0.1	-

Step 7 – logging and Tools.



Sub Menu : **Display Log**

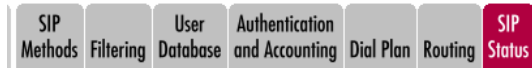
It is likely you will need to use the Display Log function to help in setting up the dial plan correctly. It is easy to define the dial plan if you know what the invite requests look like, to do this send some traffic to the Ingate, and then review the logs.
 To simplify this select the following options (and only these options)
 SIP errors, SIP signaling, SIP packets, SIP license messages, SIP media messages, SIP debug messages
 And enable the option “Show Newest at Top”

Time	Protocol	From			To			Type: Code	Flags	Decision	Reason
		Iface	IP Address	Port	Iface	IP Address	Port				
2008-02-18 16:20:04.482		>>> Info: sipfw: recv from 125.213.160.81:5060 via UDP connection 2: SIP/2.0 200 OK Via: SIP/2.0/UDP 203.100.253.51:5060;branch=z9hG4bK6d1eab01b26a4acbef7cde96abeb689d.0 Via: SIP/2.0/UDP 203.100.253.51:5060;branch=z9hG4bK27e60073dd39ab0bb19ae01b2d73be0c.pL5aII9LrVffkx5leXsRbw__ To: <sip:09152181@sip01.mynetfone.com.au>;tag=6d2aed0-co9037-INS001 From: <sip:09152181@sip01.mynetfone.com.au>;tag=4c04f08a Call-ID: 64f14def-47b9158337e42-272fe967@sigpt-1e741f35 CSeq: 1050157707 REGISTER Expires: 3600 Contact: <sip:6gSulkv9yju8O3thJthB@203.100.253.51:5060> User-Agent: ENS2.5.23 Content-Length: 0									
2008-02-18 16:20:04.482		>>> Info: sipfw: recv from 125.213.160.81:5060: SIP/2.0 200 OK									

Take Note of the “From” formatting.

Step 8 – Troubleshooting.

Example of active call with B2BUA. And the various port mappings in play.



Active Sessions (2 sessions)

Start	Caller	Callee	State	Call-ID / Media Type
16:22:38	<sip:0419521322@125.213.160.81:5060>	<sip:6gSulkv9yju8O3thJThB@192.168.15.10	Established	f1b39e7-47b9161cd764e-37d4bea7@sipgt-1e741f35
	125.213.160.70:15332 ← (192.168.15.10:62928)		UDP Audio	
16:22:38	<sip:0419521322@125.213.160.81:5060>	<sip:6gSulkv9yju8O3thJThB@203.100.253.51:5060>	Established	27b7-49b-08197075541-img-01-mas-0@125.213.168.3
	(125.213.160.70:15332) → 192.168.15.10:62928		UDP Audio	

Monitored SIP Servers

There are no monitored SIP servers.

Registered Users (1 users)

User	Registered From	Survival Aliases
09152181@sip01.mynetfone.com.au	127.0.0.1	-

Other Notes:

Resetting the Password or unknown password.

- 1) Reboot the Firewall.
- 2) When the firewall is booting up, the CONFIG button should be pressed at a certain time. Start pressing the CONFIG button when the Alert LED is lit the first time. You must then keep on pressing it until the LED has been lit and gone out twice.