



**SIP trunking Configuration Guide  
for Ingate Solutions:  
Virgin Media**

November 15, 2017

## Table of Content

1	Introduction	4
1.1	Purpose.....	4
1.2	Prerequisites.....	4
1.3	Compatibilities and Limitations.....	4
2	Initial configuration	5
2.1	Hardware and network setup.....	5
2.2	Ingate Startup Tool TG.....	6
2.2.1	Initial Setup .....	6
2.2.2	Network Topology.....	8
2.2.3	IP-PBX Configuration.....	9
2.2.4	ITSP Configuration.....	10
2.2.5	Uploading the Configuration.....	12
2.3	Ingate Web Interface.....	13
2.3.1	Applying the Configuration .....	13
3	Continued Configuration via Ingate Web Interface	15
3.1	Network.....	15
3.1.1	Network and Computers.....	15
3.2	DNS Servers .....	16
3.2.1	All Interfaces .....	16
3.3	Basic Configuration.....	18
3.3.1	Access Control.....	18
3.4	Administration.....	19
3.4.1	Date and Time .....	19
3.5	SIP Services .....	21
3.5.1	Basic .....	21
3.5.2	Sessions and Media.....	22
3.6	SIP Traffic.....	26
3.6.1	Filtering .....	26
3.6.2	Dial Plan .....	26
3.7	Routing .....	28
3.8	SIP Trunks .....	29
3.8.1	SIP Trunk 1 .....	29
4	Optional Configuration via Ingate Web Interface	31
4.1	Certificates.....	31
4.2	Access Control .....	32
5	Finalize the configuration	33
6	Where entered configuration ends up	34
6.1	All Interfaces.....	34

Versions: For Ingate Firewall/SIParator version 6.0.2 or later

Revision History:

Revision	Date	Author	Comments
1.0	2017-11-15	Ingate Systems AB: Rolf Lindström	First version of the document
1.1	2017-11-29	Ingate Systems AB: Rolf Lindström	Second version of the document

# 1 Introduction

## 1.1 Purpose

This document describes how to configure an Ingate device to work as a Enterprise Session Border Controller (eSBC) for connecting Virgin Media networks.

## 1.2 Prerequisites

This document describes how to install an Ingate E-SBC of the following series:

- Firewall: All available models with software version 6.0.2 and higher
- Ingate SIParator: All available models with software version 6.0.2 and higher

The operational mode can be set as a SIParator Standalone eSBC, DMZ/LAN or DMZ using the software version 6.0.2 and above, or as Firewall.

1 SIP trunking license and X ccs license (Concurrent Calls SIP Trunk Sessions) will be required.

## 1.3 Compatibilities and Limitations

This E-SBC has been tested and certified with Virgin Media according to Virgin Media's requirements and test procedures of their SIP trunk service. This document will give a description of the configuration between the Ingate E-SBC and the ITSP only.

## 2 Initial configuration

It is recommended to use the [StartupToolTG-1.2.4](#) to automate the deployment of your Ingate E-SBC. The version used for this document is v1.2.4. **Before using the Ingate Startup Tool TG to configure a new Ingate Unit for the first time you must install your licenses into the Ingate unit.** Please read the Startup Tool TG – Getting Started Guide. You find it on our web. [https://www.ingate.com/appnotes/Ingate\\_Startup\\_Tool\\_Getting\\_Started\\_Guide.pdf](https://www.ingate.com/appnotes/Ingate_Startup_Tool_Getting_Started_Guide.pdf)



**Ingate Account Home Page**

**Manage Account**

- [Change contact information or password](#)

**Manage Ingate Appliances**

- [Register a new unit](#)
- [Download upgrades](#)
- [Download IDS/IPS Rulepacks](#)
- [Activate licenses](#)

**View Documentation**

- [Product Manuals](#)
- [Other Documentation](#) (App notes, howtos)
- [Ingate Startup Tool Guide](#)

**Software SIParator/Firewall - For Use on Virtual Machines**

- [Download the Software SIParator/Firewall](#) (7 downloads made)
- [Register the Software SIParator/Firewall after installation](#)
- [Activate licenses for a Software SIParator/Firewall](#)

**Startup Tool**

- [Download new Startup Tool TG \(SUT TG\) \[Recommended\]](#)
- [Download previous Startup Tool \(SUT\) \[No longer recommended\]](#)
- [Ingate Startup Tool Guide](#)

**My Ingate Units**

**DOCUMENTATION**

- How To Guides
- Startup Tool guide
- READ MORE**
- Interoperability
- Ingate Modules and Licenses

### 2.1 Hardware and network setup

After connecting power, connect an Ethernet cable to the port marked **Eth0** of the device. This cable must be connected to your private IP network: the Eth0 port will be used to configure the unit with the Ingate Startup Tool TG (see below).

When you connect the Firewall/SIParator to the external (public IP) network, plug an Ethernet cable into the port marked **Eth1**.

This configuration guide and the Ingate Startup Tool TG assume that **all of the following are connected to the same subnet on the private IP network:**

- Ingate Firewall/SIParator (via port Eth0)
- VoIP Gateway or IP PBX
- Computer running the Ingate Startup Tool TG

If, for some reason, this is not the case (e.g. the VoIP Gateway or IP PBX is on a different subnet from the SIParator), the Startup Tool TG will restrict to Gateways and IP-PBX IP Addresses to the local Subnet of the Ingate. This can be easily changed later on the Ingate Administration GUI. Then you should consult the Ingate Reference Manual (Chapter 6 – Interface: Static Routing) for additional network setup.

## 2.2 Ingate Startup Tool TG

### 2.2.1 Initial Setup

Before you can administer the device, you must configure its IP address and administrative password with the Ingate Startup Tool TG. The tool must run on a PC that is located on the same LAN subnet as the device itself (rather than, for example, a different subnet, across routers, or through a VPN tunnel).

The tool can be downloaded free of charge at [http://www.ingate.com/Startup\\_Tool\\_TG.php](http://www.ingate.com/Startup_Tool_TG.php). Always use the latest version.

Launch the tool.

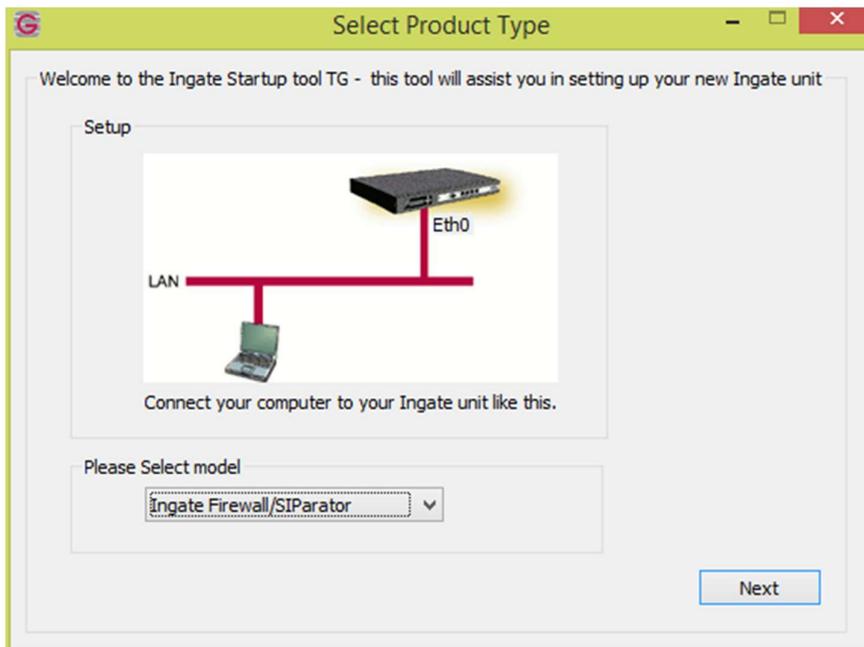
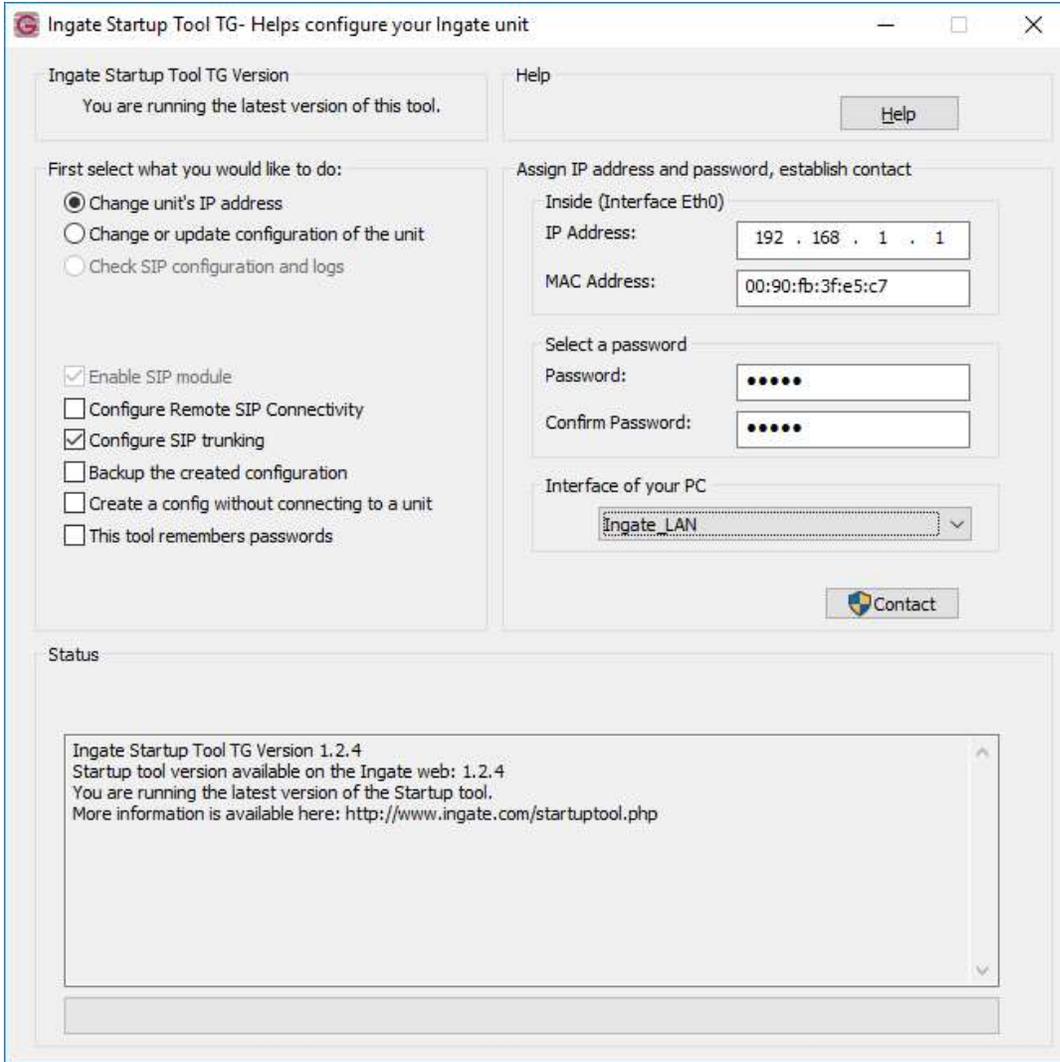


Figure 1. Product Type selection Screen

Select the model type of the Ingate unit as Ingate Firewall/SIParator (Figure 1) and click Next.

You will see a configuration page (Figure 2).



**Figure 2. Configure your Ingate unit**

In the group box labelled *First select what you would like to do*, select the radio button labelled **Change unit's IP address**.

In the group box labelled *Inside (Interface Eth0)*, go to the *IP Address* field and enter a static IP address by which the Eth0 interface will address on your private network. Then, go to the *MAC Address* field and enter the address that will be found on a sticker attached to the unit. (Figure 2) shows an example.

In the group box labelled *Select a Password*, enter (and confirm) the password to be used hereafter to authenticate administrators of the device.

In the drop-down list labelled *Interface of your PC*, select the network interface (e.g. **Local Area Connection**) that you wish to use to communicate with the SIParator (Figure 3).



### Figure 3. Selecting the network interface used by the Startup Tool TG

When these values have been entered, the **Contact** button at the bottom right of the form (Figure 2) will become active.

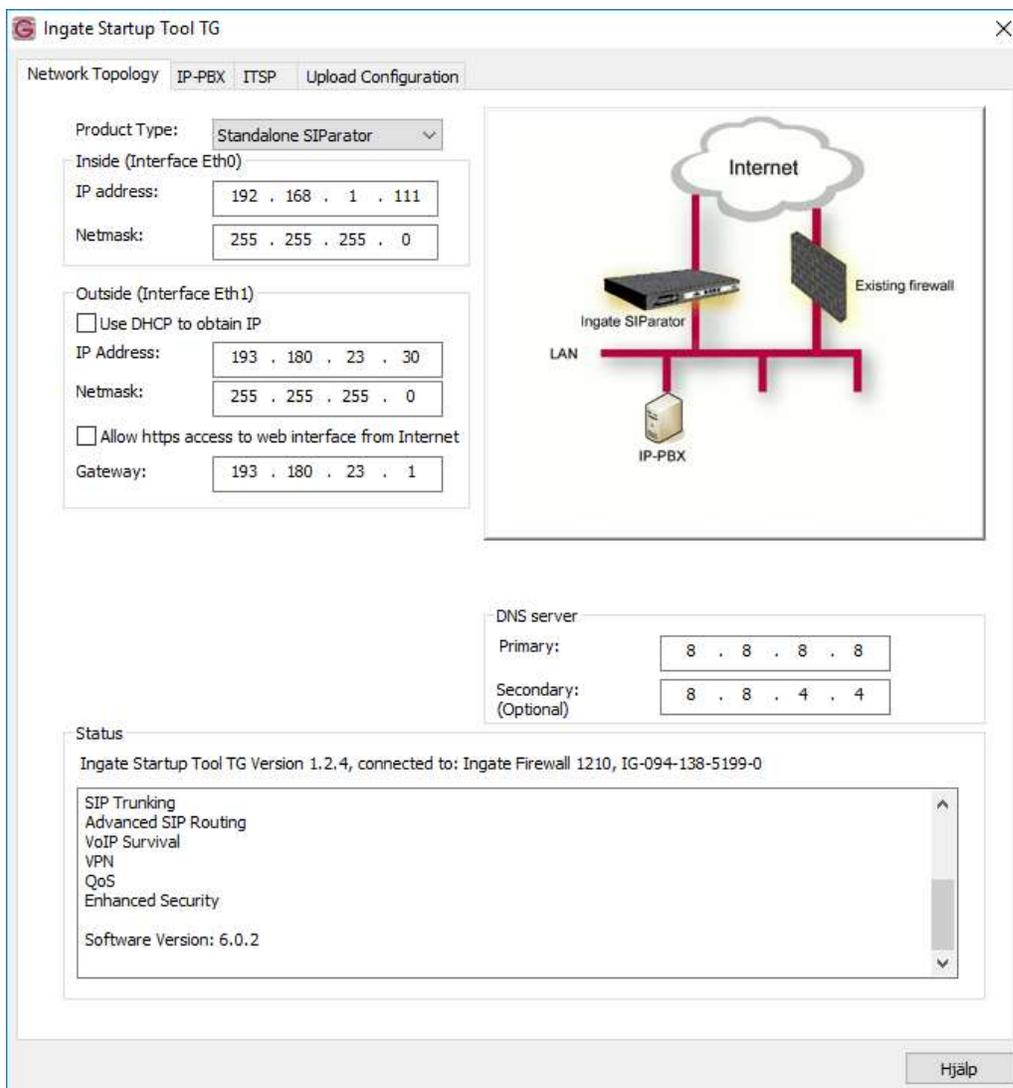
Press the **Contact** button.

The Startup Tool TG will find the Ingate unit on the network, communicate with it and assign its IP address and password.

## 2.2.2 Network Topology

The Ingate SIParator device supports many different configuration modes and functions. Select the Product Type of the Ingate eSBC matching the network topology for your Virgin Media installation, for example as **Standalone SIParator**.

Go to the *Network Topology* tab.



The screenshot shows the 'Ingate Startup Tool TG' application window with the 'Network Topology' tab selected. The interface includes several configuration sections:

- Product Type:** A dropdown menu set to 'Standalone SIParator'.
- Inside (Interface Eth0):** IP address: 192 . 168 . 1 . 111; Netmask: 255 . 255 . 255 . 0.
- Outside (Interface Eth1):**  Use DHCP to obtain IP; IP Address: 193 . 180 . 23 . 30; Netmask: 255 . 255 . 255 . 0;  Allow https access to web interface from Internet; Gateway: 193 . 180 . 23 . 1.
- DNS server:** Primary: 8 . 8 . 8 . 8; Secondary: (Optional) 8 . 8 . 4 . 4.
- Status:** Ingate Startup Tool TG Version 1.2.4, connected to: Ingate Firewall 1210, IG-094-138-5199-0. A list of features is shown: SIP Trunking, Advanced SIP Routing, VoIP Survival, VPN, QoS, Enhanced Security, and Software Version: 6.0.2.

A network diagram on the right shows an 'Internet' cloud connected to an 'Ingate SIParator' device and an 'Existing firewall'. Both are connected to a 'LAN' which includes an 'IP-PBX' device.

At the bottom right of the window is a 'Hjälp' button.

Figure 4. Configuring Network Topology

In the *Product Type* drop down list, select **Standalone SIParator** (Figure 4). After configuring the product type, the controls on the administrative interface will change, according to the type selected.

To set the operational mode to Standalone SIParator is just as example, set it alternatively as a Firewall, DMZ/LAN or DMZ depending on your network requirements.

The internal network interface details, listed in the group box labelled *Inside (Interface Eth0)*, should be consistent with your earlier assignment. These represent the device's interface to your private IP network.

Details of the device's interface to the public IP network can be configured with the controls in the group box labelled *Outside (Interface Eth1)*.

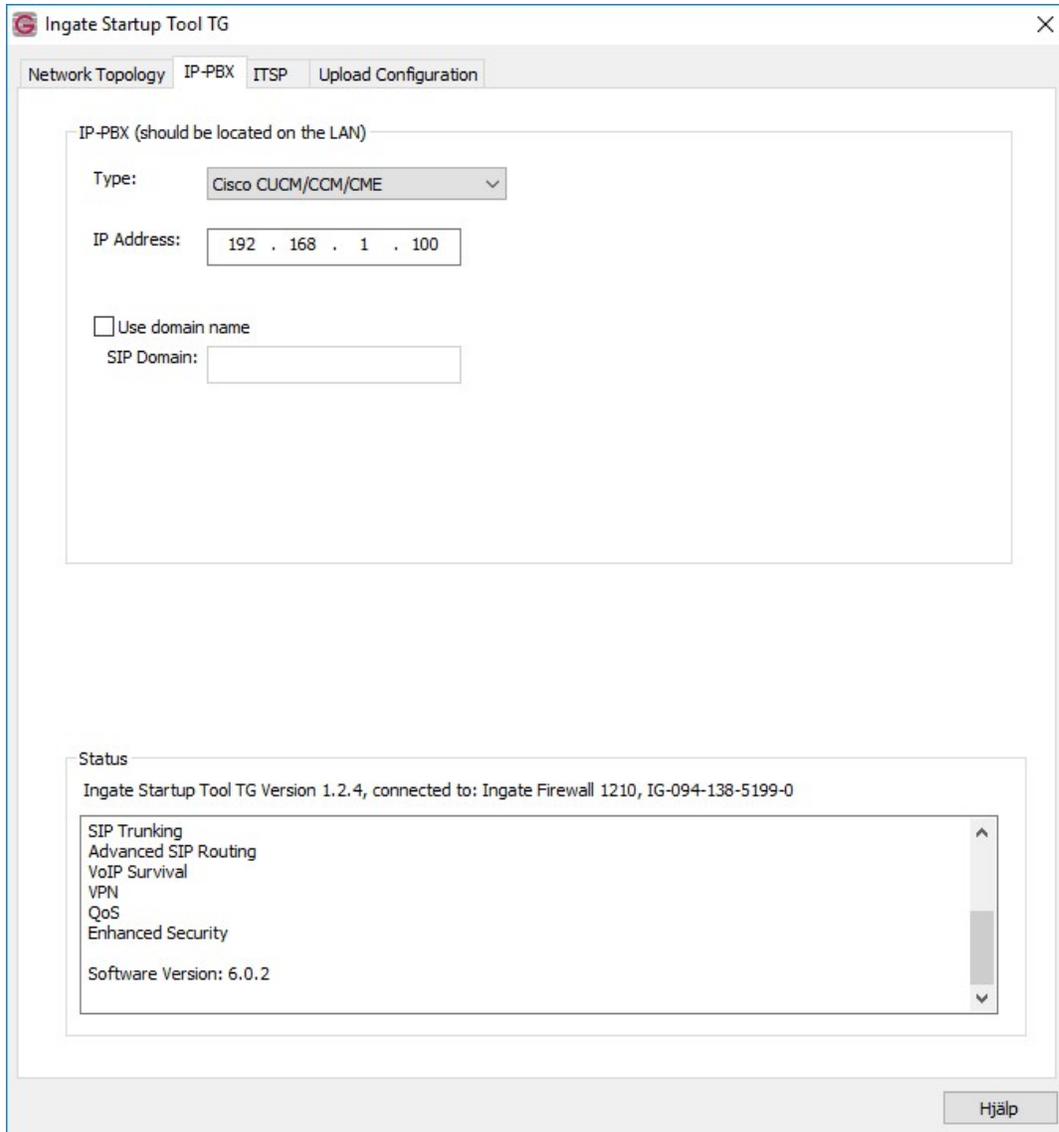
Once you have entered the internal and external interface details, go to the *Gateway* control and enter the address of the router that acts as a firewall gateway for your network.

Finally, enter the DNS server IP addresses. If Virgin has provisioned you with any special DNS servers, those can be supplied here.

### 2.2.3 IP-PBX Configuration

In the Ingate Startup Tool TG, navigate to the *IP-PBX* tab (Figure 5).

This configuration is related to the eSBC's connection, via its internal interface, to the VoIP gateway or IP PBX



**Figure 5. Configuring the IP PBX or VoIP Gateway details**

In the *Type* drop-down list, select an entry that matches your IP PBX or VoIP Gateway. In this example **Cisco CUCM/CCM/CCE** is chosen. If you cannot find a matching item, select **Generic IP-PBX**.

In the *IP Address* field, enter the address of the IP PBX or gateway on your network.

## 2.2.4 ITSP Configuration

In the Ingate Startup Tool TG, navigate to the *ITSP* tab. ITSP stands for Internet Telephony Service Provider.

This configuration is related to the eSBC's connection, via its external interface, to Virgin Media.

**Figure 6. Configuring the external SIP interface details**

In the *Name* drop-down list, select **Virgin**.

The IP addresses in this document are just examples, use what Virgin may provision you with, those DNS names/IP addresses should be used.

In the *Provider address* group box, Use the IP or domain name you got from Virgin media. The Provider address will be used in the Request-URI and To header field for outgoing SIP requests.

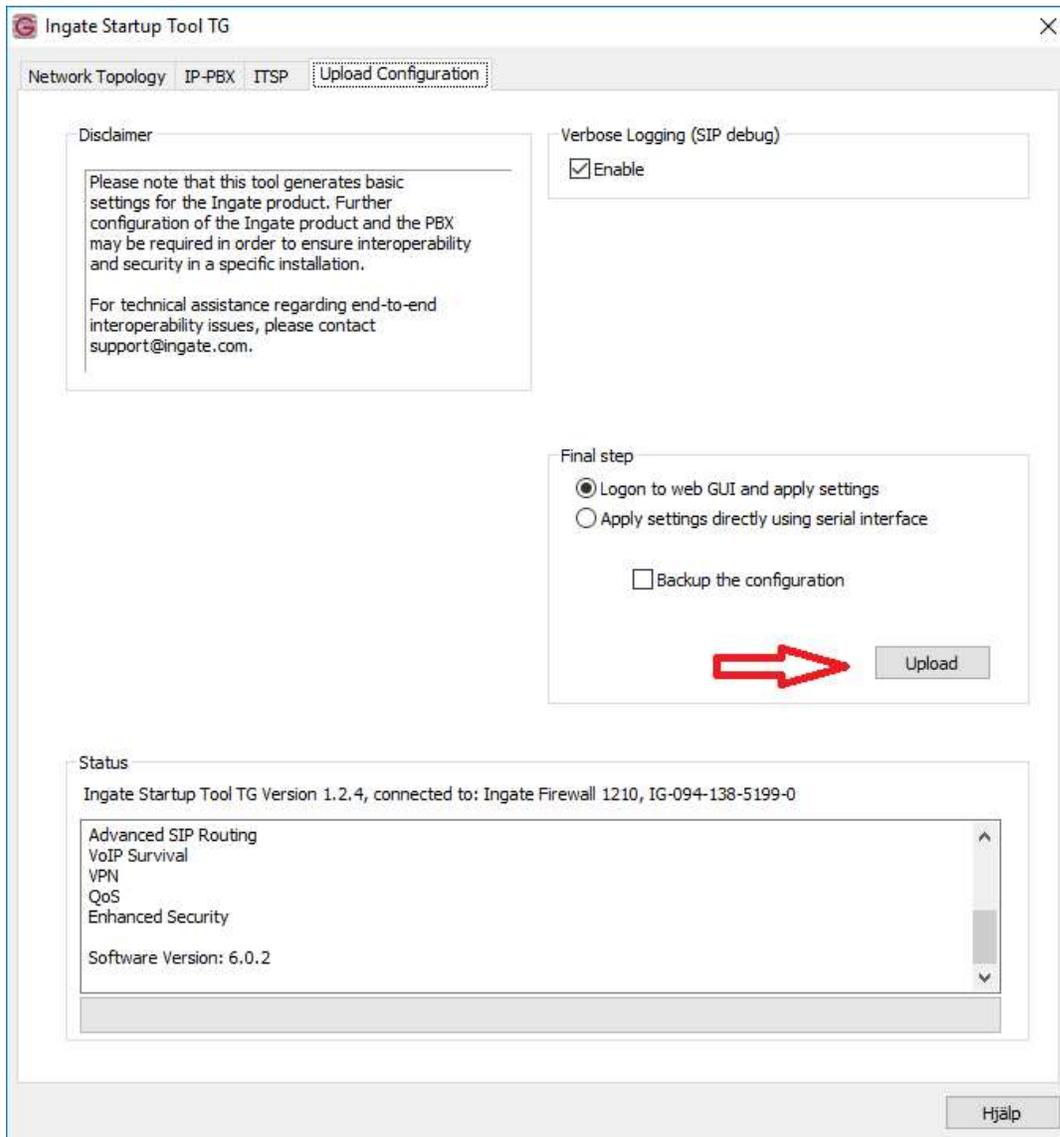
In the *DID*, *PBX* and *Account authentication* fields, fill in values for your numbering plan. The information entered here may be further configured at the SIP Trunk page, (see chapter [3.8.1 SIP Trunk 1](#)).

The numbering of DID and PBX lines in this document are just examples, use what Virgin may provision you with, those numbers should be used.

## 2.2.5 Uploading the Configuration

When you have completed the previous configuration steps, use the StartUp Tool TG to load the data into the Ingate SIParator. The tool can also be used to create a backup configuration file for later use.

In the tool, navigate to the *Upload Configuration* tab (Figure 7).



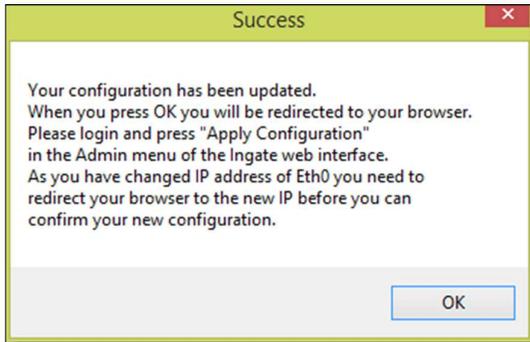
**Figure 7. Uploading configuration data to the SIParator**

In the *Final step* controls, ensure that the radio button labelled *Logon to web GUI and apply settings* is selected.

Click the **Upload** button.

The configuration data will be copied from the Startup Tool TG to the Firewall/SIParator.

When the data has been uploaded, a dialog box will appear (Figure 8).



**Figure 8. Confirmation of configuration data upload**

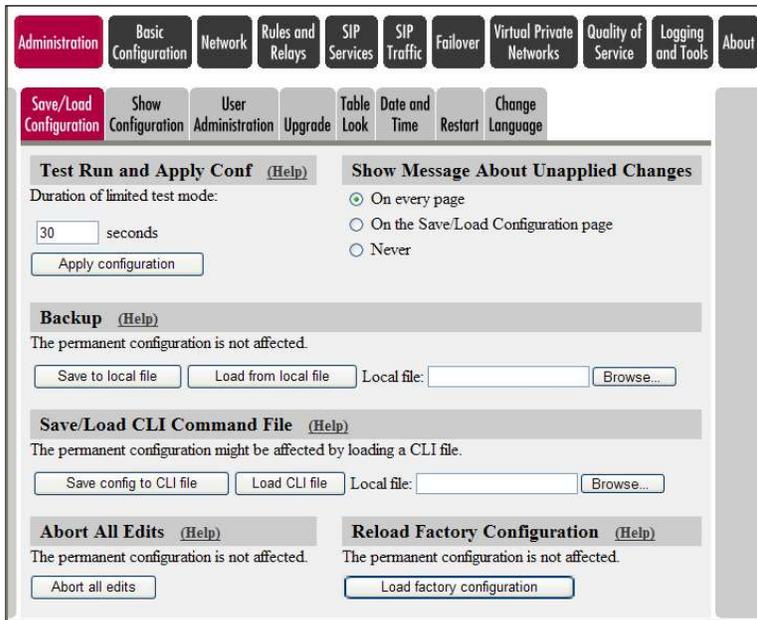
Click on **OK**. The default web browser will launch and navigate you to the SIParator’s web interface.

## 2.3 Ingate Web Interface

### 2.3.1 Applying the Configuration

Although the configuration data has been uploaded to the eSBC, it must still be explicitly applied before the eSBC’s behaviour will change.

Log into the web interface with the administrative password that you selected earlier (in Figure 2).



**Figure 9. Applying the uploaded configuration**

Under **Administration > Save/Load Configuration**, click the **Apply configuration** button.

A window will appear (Figure 10) requesting further input.



**Figure 10. Saving the configuration**

Click the button labelled **Save configuration**.

This completes the process of transferring and applying the configuration data to the SIParator device.

Further configuration settings must now be applied through the web interface.

## 3 Continued Configuration via Ingate Web Interface

### 3.1 Network

First, the eSBC must be configured to be aware of the network in which it operates.

#### 3.1.1 Network and Computers

Here, you specify an alias for the groups of IPs relevant to this ITSP, in addition to the eSBCs settings.

Perform the following steps:

1. Click on **Network** -> **Network and Computers**, see example below, how it looks after been filled in.
2. Fill in **IP Address (Lower Limit)** for the first of the Virgin ISTP Servers for **Network and Computers** with **Name** Virgin.
3. Add a new row for **Network and Computers** with **Name** Virgin\_b or what you want to call the second server.
4. Fill in **IP Address (Lower Limit)** for the second of the Virgin ISTP Servers for **Network and Computers** with **Name** Virgin\_b.
5. Add a new row for **Network and Computers** with **Name** **Safe** and add both Virgin servers and LAN.
6. Click on **Save** to save the configuration to the preliminary configuration.

See example result in figure below:

The screenshot shows the Ingate Firewall web interface. The main navigation bar includes 'Administration', 'Basic Configuration', 'Network', 'Rules and Relays', 'SIP Services', 'SIP Traffic', 'SIP Trunks', 'Failover', 'Virtual Private Networks', 'Quality of Service', 'Logging and Tools', and 'About'. The 'Networks and Computers' section is selected, showing a table with the following data:

Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
Generic IP-PBX	-	192.168.1.100	192.168.1.100			-	<input type="checkbox"/>
LAN	-	192.168.1.0	192.168.1.0	192.168.1.255	192.168.1.255	inside (eth0 untagged)	<input type="checkbox"/>
Safe	LAN					-	<input type="checkbox"/>
	Virgin_A					-	<input type="checkbox"/>
	Virgin_B					-	<input type="checkbox"/>
Virgin_A	-	81.97.95.188	81.97.95.188			outside (eth1 untagged)	<input type="checkbox"/>
	-	sipstestA1.ipmultimedia	81.97.95.188			outside (eth1 untagged)	<input type="checkbox"/>
Virgin_B	-	82.14.171.242	82.14.171.242			outside (eth1 untagged)	<input type="checkbox"/>
	-	sipstestB1.ipmultimedia	82.14.171.242			outside (eth1 untagged)	<input type="checkbox"/>
WAN	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)	<input type="checkbox"/>

Below the table, there are controls for 'Add new rows', 'groups with', and 'rows per group'. At the bottom, there are buttons for 'Save', 'Undo', and 'Look up all IP addresses again'.

Page generated for 'admin' 2017-11-22 10:14:40 +0100.  
Ingate SIParator Firewall 6.0.2. Copyright © 2017 Ingate Systems AB.

## 3.2 DNS Servers

Here, you specify your DNS server.

Click on **Basic Configuration** -> **Basic Configuration**

See example result in figure below:

The screenshot shows the InGate Firewall configuration interface. At the top, it says "inGate Firewall Configured by Ingate SUT TG" with a "Log Out" button. Below this is a navigation menu with buttons for Administration, Basic Configuration (selected), Network, Rules and Relays, SIP Services, SIP Traffic, SIP Trunks, Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Under the Basic Configuration menu, there are sub-menus: Basic Configuration (selected), Access Control, RADIUS, SNMP, DHCP Options, DHCP Server, DHCP Server Status, Router Advertisement, Dynamic DNS Update, Certificates, TLS, Advanced, and SIParator Type. The main configuration area is divided into several sections: General, Version of Ingate SIParator/Firewall, Policy For Ping To the firewall, and DNS Servers (Help). The DNS Servers section contains a table with columns for No., Dynamic, DNS Name or IP Address, IP Address, and Delete Row. There are two rows in the table: Row 1 with No. 1, Dynamic set to "-", DNS Name or IP Address 8.8.8.8, IP Address 8.8.8.8, and a delete checkbox; Row 2 with No. 2, Dynamic set to "-", DNS Name or IP Address 8.8.4.4, IP Address 8.8.4.4, and a delete checkbox. Below the table, there is a button "Add new rows" followed by a text input "1" and the text "rows.". The DNS Lookup Preference section is below, with a dropdown menu set to "Auto" and buttons for "Save", "Undo", and "Look up all IP addresses again".

**General**

Name of this firewall: Configured by Inga

Default domain: .

**Version of Ingate SIParator/Firewall**

Check for new versions of Ingate SIParator/Firewall:  Yes  No

Date of last successful version check: Not available

Software version in use: 6.0.2

**Policy For Ping To the firewall**

- Never reply to ping
- Only reply to ping to the same interface
- Reply to ping to all IP addresses

**DNS Servers (Help)**

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	8.8.8.8	8.8.8.8	<input type="checkbox"/>
2	-	8.8.4.4	8.8.4.4	<input type="checkbox"/>

Add new rows 1 rows.

**DNS Lookup Preference (Help)**

Auto

Save Undo Look up all IP addresses again

### 3.2.1 All Interfaces

Add additional routing information for added off-networks subnets for access.

Perform the following steps:

1. Click on **Network** -> **All Interfaces**, see example below, how it looks after been filled in.
2. Create one new row for your **Static Routing** by clicking on: **Add new rows** and fill in 1 as number of rows to add.
3. Fill in **Network Address, Netmask / bits, Router IP Address** and **Interface**.
4. Click on **Save** to save the configuration to the preliminary configuration.

See example result in figure below:

**inGate Firewall** Configured by Ingate SUT TG Log Out

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

Networks and Computers Default Gateways **All Interfaces** NAT VLAN Eth0 Eth1 Eth2 Eth3 Interface Status PPPoE Tunnels Topology

### Interface Overview

**General**

Physical Device	Interface Name	Active	Speed and Duplex
eth0	inside	Yes	Autonegotiation
eth1	outside	Yes	Autonegotiation
eth2	Ethernet2	No	Autonegotiation
eth3	Ethernet3	No	Autonegotiation

**Directly Connected Networks** [\(Help\)](#)

Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	Interface or Tunnel	VLAN Id	VLAN Name	Delete Row
inside	Static	192.168.1.111	192.168.1.111	255.255.255.0	192.168.1.0	192.168.1.255	inside (eth0)		-	<input type="checkbox"/>
outside	Static	193.180.23.30	193.180.23.30	255.255.255.0	193.180.23.0	193.180.23.255	outside (eth1)		-	<input type="checkbox"/>

Add new rows  rows.

**Alias** [\(Help\)](#)

Name	DNS Name or IP Address	IP Address	Interface	Delete Row
------	------------------------	------------	-----------	------------

Add new rows  rows.

**Proxy ARP** [\(Help\)](#)

Get Network From	Proxy ARPed Network			Interface	VLAN Id	VLAN Name	Delete Row
	DNS Name or Network Address	Network Address	Netmask / Bits				

Add new rows  rows.

**Static Routing** [\(Help\)](#)

Routed Network			Router			Interface or Tunnel	Delete Row
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address		
default	default		- ▾	193.180.23.1	193.180.23.1	outside (eth1) ▾	<input type="checkbox"/>

Add new rows  rows.

---

**Unreachable** [\(Help\)](#)

Unreachable Network			Delete Row
DNS Name or Network Address	Network Address	Netmask / Bits	

Add new rows  rows.

Save Undo Look up all IP addresses again

Page generated for 'admin' 2017-11-22 10:21:06 -0100.

### 3.3 Basic Configuration

Add more networks for access control if wanted.

#### 3.3.1 Access Control

Here, you specify any additional off-networks subnets for access.

Perform the following steps:

1. Click on **Basic Configuration** -> **Access Control**, see example below, how it looks after been filled in.
2. Create one new row for your **Configuration Computers** by clicking on: **Add new rows** and fill in 1 as number of rows to add.
3. Fill in **Network Address**, **Netmask / bits** and **Configuration Transport**.
4. Click on **Save** to save the configuration to the preliminary configuration.

See example result in figure below:



**Configuration Allowed Via Interface** [\(Help\)](#)

Interface or Tunnel	Allowed	Delete Row
inside (eth0)	Yes	<input type="checkbox"/>

Add new rows  rows.

**Configuration Transport** [\(Help\)](#)

Protocol	IP Address	Port	Cert	TLS	Delete Row
HTTP	inside (192.168.1.111)	80	-	-	<input type="checkbox"/>

Add new rows  rows.

**User Authentication For Web Interface Access** [\(Help\)](#)

Local users  
 RADIUS database  
 Local users or RADIUS database

**Web Interface Access Settings** [\(Help\)](#)

Login timeout:  seconds

**Configuration Computers** [\(Help\)](#)

No.	DNS Name or Network Address	Network Address	Netmask / Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	Log Class	Delete Row
1	192.168.1.0	192.168.1.0	255.255.255.0	192.168.1.0 - 192.168.1.255	-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Local	<input type="checkbox"/>

Add new rows  rows.

Page generated for 'admin' 2017-11-22 10:36:04 +0100.  
 Ingate SIPParator/Firewall 6.0.2. Copyright © 2017 Ingate Systems AB.

### 3.4 Administration

Set Clock and NTP.

#### 3.4.1 Date and Time

Perform the following steps:

1. Click on **Administration** -> **Date and Time**, see example below, how it looks after been filled in.
2. Select Time Zone in **Change Time Zone**.
3. Select **Yes** for **Synchronize time with NTP**.
4. Fill in DNS Name or IP Address for NTP Server To Use.
5. Click on Save to save the configuration to the preliminary configuration.

See example result in figure below:

**inGate Firewall** Configured by Ingate SUT TG Log Out

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

Save/Load Configuration Show Configuration User Administration Upgrade Table Look **Date and Time** Restart Change Language

### Change Time Zone (Help)

St Helena (Atlantic) St Johns (America) St Kitts (America) St Lucia (America) St Thomas (America) St Vincent (America) Stanley (Atlantic) Stockholm (Europe)

Active time zone: **Stockholm (Europe)**

### Change Date and Time Manually (Help)

Date:   
Time:

### Change Date and Time With NTP (Help)

Synchronize time with NTP:  Yes  No

### NTP Servers To Use If NTP Is Enabled

Dynamic	DNS Name or IP Address	IP Address	Delete Row
- ▾	<input type="text" value="0.se.pool.ntp.org"/>	192.36.143.130	<input type="checkbox"/>

rows.

Page generated for 'admin' 2017-11-22 10:40:20 +0100.  
Ingate SIParator Firewall 6.0.2. Copyright © 2017 Ingate Systems AB.

## 3.5 SIP Services

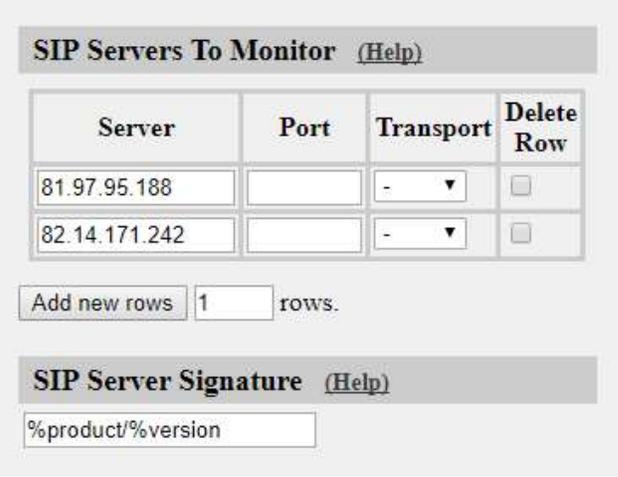
### 3.5.1 Basic

The eSBC at its core is a Firewall. To increase security, you can choose whether the eSBC will only accept SIP signalling from a configured range of addresses. Addresses outside of the permitted ranges will not succeed in making a connection to the eSBCs SIP port.

Perform the following steps:

1. Click on **SIP Services -> Basic**
2. Under **SIP Signalling Access Control**: Select the Network group **safe**.
3. You shall monitor your ITSPs SIP servers to ensure they are up. This is used by the eSBC when SIP signalling should be passed on to the ITSP SBC server. This is useful when a domain resolves to several individual hosts, or there are multiple IPs for the ITSP; the eSBC will know immediately if one of them is down, which accelerates call connection.

The IP addresses that Virgin may provision you with may differ from this document. In which case, those DNS names/IP addresses should be used.



The screenshot shows a web interface for configuring SIP servers. It features a table with columns for Server, Port, Transport, and Delete Row. Below the table is a button for adding new rows and a field for the number of rows to add. Below that is a section for SIP Server Signature with a text input field.

Server	Port	Transport	Delete Row
81.97.95.188		-	<input type="checkbox"/>
82.14.171.242		-	<input type="checkbox"/>

Add new rows  rows.

**SIP Server Signature** [\(Help\)](#)

Perform the following steps:

4. Create new rows for your **SIP Servers to Monitor** by clicking on: **Add new rows** and fill in 2 as number of rows to add.
5. Fill in **Server**, **Port** and **Transport** for respective Server.
6. Click on **Save** to save the configuration to the preliminary configuration.

See example result in figure below:

Administration Basic Configuration Network Rules and Relays **SIP Services** SIP Traffic SIP Trunks 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

**SIP Module** (Help)

Enable SIP module  
 Disable SIP module

**SIP Signaling Access Control** (Help)

Specify the networks and computers from which the firewall accepts SIP Signaling.

Safe 

**SIP Signaling Ports** (Help)

Active	Port	Transport	Intercept	Comment	Delete Row
Yes	5060	UDP and TCP	Yes	Standard SIP port	<input type="checkbox"/>
No	5061	TLS	Yes	Standard TLS port	<input type="checkbox"/>

Add new rows  rows.

**SIP Media Port Range** (Help)

Ports:  -

**Public IP Address for NATed firewall** (Help)

This setting is not supported for the Standalone configuration.

DNS Name or IP Address

IP Address

**SIP Logging** (Help)

Log class for SIP signaling:

Log class for SIP packets:

Log class for SIP license messages:

Log class for SIP errors:

Log class for SIP media messages:

Log class for SIP debug messages:

Log class for SIP IDS/IPS:

Hide sensitive data:  Yes  No

**SIP Servers To Monitor** (Help)

Server	Port	Transport	Delete Row
81.97.95.188	<input type="text"/>	-	<input type="checkbox"/>
82.14.171.242	<input type="text"/>	-	<input type="checkbox"/>

Add new rows  rows.

**SIP Server Signature** (Help)

### 3.5.2 Sessions and Media

Perform the following steps:

1. Click on **SIP Services** -> **Sessions and Media**
2. In **Limitation of RTP Codecs**
  - a. This is set to **Allow all Codecs** for greatest flexibility. This section is used to lock CODECs permitted via the eSBC down.
  - b. Some ITSPs only allow specific CODECs. In such cases, choose Limit Codecs as Configured and add or remove rows as necessary to match the ITSPs requirements. A Row of Type: "Audio", Name: "pcma", Allowed: "Yes", Add: "No" will suffice. This is normally not done for Virgin.
  - c. Ingate version (6.0.2) Virgin media prefer to use G711A –law as the first codec to be offered. For example 0, 8, 101 (A- law, u-law , telephone events).
3. If you change codec configuration: Click on **Save** to save the configuration to the preliminary configuration. See example result in figures below:

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

---

### Session Configuration

Session timer:  seconds  
 Allowed amount of concurrent sessions (leave blank for no limit):   
 Timeout for SIP over TCP/TLS:  seconds (max 100)  
Change session timer to 3600, default value is 14400

---

### Media Proxy [\(Help\)](#)

Enable Media Proxy  
 Disable Media Proxy

---

### Media Configuration [\(Help\)](#)

Limitation of sender of media streams:  
 Lock IP address and port to first sender  
 Only allow receiving IP address, but multiple ports  
 Allow multiple sender IP addresses and ports

Allowed number of senders:

Allowed amount of media streams per SIP session:

Support forked media streams:  
 Yes  No

Timeout for one-way media streams:  seconds

Tear down media streams at RTP/RTCP timeouts:  
 Yes  No

Timeout for RTP streams:  seconds

Timeout for RTCP streams:  seconds

---

### Always Relay Media [\(Help\)](#)

Always relay media:  Yes  No

---

### Reuse Port Numbers When Changing Media [\(Help\)](#)

Reuse port numbers when changing media (e.g. T.38 FAX):  
 Don't reuse port numbers  
 Reuse port numbers

### Reuse Port Numbers Within Same Session [\(Help\)](#)

Reuse port numbers within same session:

- Don't reuse port numbers
- Reuse port numbers
- Reuse port numbers even when IP has changed

### Detect codec changes [\(Help\)](#)

Detect codec changes in mid call answers in the B2BUA:

- Detect only changes to the first payload type listed
- Detect changes to all payload types (except dynamic)
- Do not detect changes to payload types in mid call answers

### Third Party Call Control Codecs [\(Help\)](#)

No.	Name	Payload Type	Rate	Channels	Parameters	Delete Row
1	PCMU					<input type="checkbox"/>
2	G729				annexb=yes	<input type="checkbox"/>
3	telephone-event	96	8000		0-15	<input type="checkbox"/>

Add new rows  rows.

### Limitation of RTP Codecs [\(Help\)](#)

- Allow all codecs
- Limit codecs as configured

### Strip SDP Lines [\(Help\)](#)

Reg Expr Case Delete Row

Add new rows  rows.

### Local Ringback [\(Help\)](#)

#### Local Ringback Played at Call Transfer

- Never play local ringback
- Play local ringback when transferer hangs up
- Play local ringback when new target rings
- Play local ringback when new target rings or makes progress

**Music on Hold Redirection** [\(Help\)](#)

- Redirect calls on hold to Music on Hold server
- Leave calls on hold as they are

**Resolve domain names in the SDP** [\(Help\)](#)

- Resolve domain names in the SDP
- Don't resolve domain names in the SDP

Default timeout for Invite, Default value = 180, you shall change this value to 200.

**Requests** [\(Help\)](#)

Default timeout for INVITE requests:  seconds

Maximum timeout for INVITE requests:  seconds

SIP blacklist interval:  seconds

B2BUA request pending timeout:  seconds

Base retransmission timeout for SIP requests:  seconds

Maximum amount of retransmissions for INVITE requests:

Maximum amount of retransmissions for non-INVITE requests:

Limit Max-Forwards:

Maximum SIP packet size:  bytes

Page generated for 'admin' 2017-11-22 10:57:28 +0100.  
 Ingate SIParator/Firewall 6.0.2. Copyright © 2017 Ingate Systems AB.

Note: RTP media from your ITSP may come from a different address than the ITSPs SIP servers – this is normal. The Ingate eSBC manages this automatically.

### 3.6 SIP Traffic

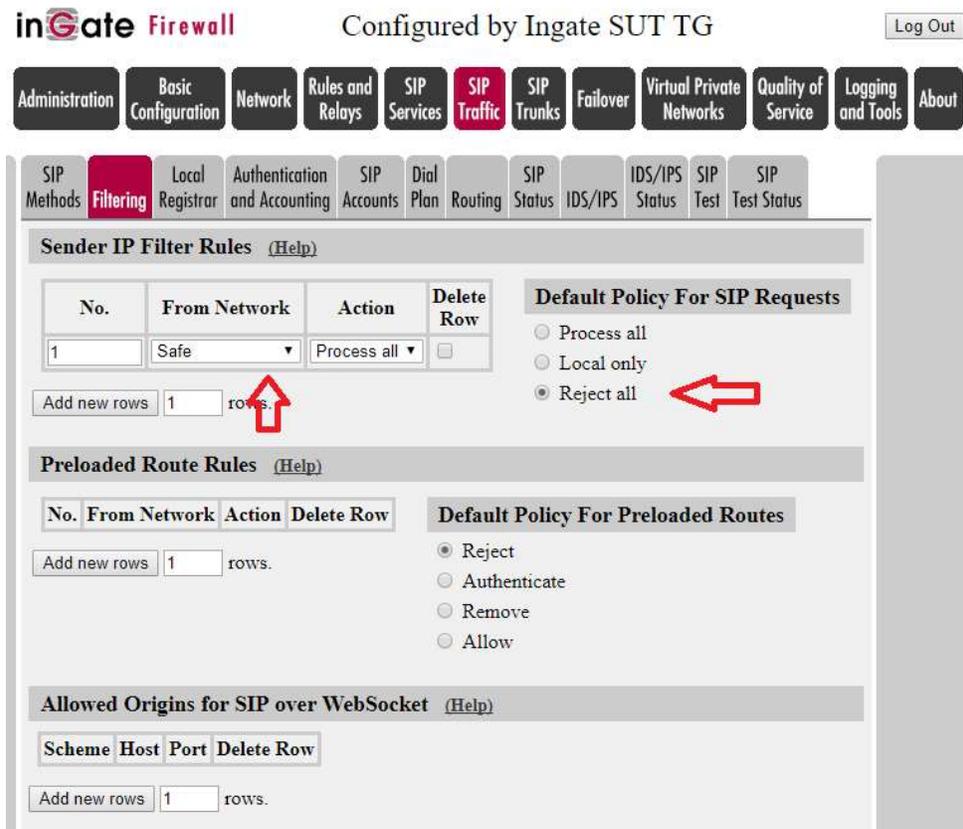
Filtering determines what to do with SIP signalling from configured addresses when it arrives at the eSBC. By default, the eSBC is configured to “Process all”.

Filtering also handles internal processing of SIP OPTIONS packets, which serve as a ping method, used by PBXs and ITSPs to determine if a remote endpoint is alive.

#### 3.6.1 Filtering

Perform the following steps:

1. Click on **SIP Services -> Filtering**
2. Under **Default Policy For SIP Requests** choose “**Reject all**”.
3. Fill in other settings according to your requirements.
4. Click on **Save** to save the configuration to the preliminary configuration.



#### 3.6.2 Dial Plan

The dial plan is automatically configured when using SUT TG. Make any necessary changes here in order to ensure your dial plan is suitable to permit SIP traffic between your WAN and LAN segments. Global format +44 is Virgin media preferred dial plan although Virgin Media can support Dial plan format of, National, Global, and E164 format.

Perform the following steps:

1. Click on **SIP Traffic -> Dial Plan**
2. Fill in the dial plan according to your wishes.
3. Click on **Save** to save the configuration to the preliminary configuration.

See example result in figure below:

**inGate Firewall** Configured by Ingate SUT TG Log Out

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

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts **Dial Plan** Routing SIP Status IDS/IPS Status SIP Test SIP Test Status

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

On  Off  Fallback

999 112 18000 911 

**Matching From Header** (Help)

Name	Use This ...		... Or This	Transport	Network	Delete Row
	Username	Domain	Reg Expr			
Generic IP-PBX	*	*		Any	Generic IP-PBX	<input type="checkbox"/>
Virgin_optionsA	*	*		Any	Virgin_A	<input type="checkbox"/>
Virgin_optionsB	*	*		Any	Virgin_B	<input type="checkbox"/>
WAN	*	*		Any	WAN	<input type="checkbox"/>

Add new rows  rows.

**Matching Request-URI** (Help)

Name	Use This ...				... Or This	Delete Row
	Prefix	Head	Tail	Min. Tail	Domain	
Options_In			nothing		193.180.23.30	<input type="checkbox"/>
Outbound	0		0.9		*	<input type="checkbox"/>
Outbound_world	00		0.9		*	<input type="checkbox"/>

Add new rows  rows.

**Forward To** (Help)

Name	No.	Use This ...		... Or This		... Or This	... Or This	Use Alias IP	Delete Row
		Account	Replacement Domain	Port	Transport	Reg Expr	Trunk		
Generic (regall)	1	-			-		SIP Trunk 1: Virgin_A,Generic IP-PBX	<input type="checkbox"/>	

**Forward To** (Help)

Name	No.	Use This ...		... Or This		... Or This	... Or This	Use Alias IP	Delete Row
		Account	Replacement Domain	Port	Transport	Reg Expr	Trunk		
Generic (regall)	1	-			-		SIP Trunk 1: Virgin_A,Generic IP-PBX	<input type="checkbox"/>	

Add new rows  groups with  rows per group.

**Dial Plan** (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
					Forward	ENUM				
1	Generic IP-PBX	Outbound_world	Forward	Generic (regall)	+		-	-		<input type="checkbox"/>
2	Generic IP-PBX	Outbound	Forward	Generic (regall)	+44		-	-		<input type="checkbox"/>
3	Generic IP-PBX	-	Forward	Generic (regall)			-	-		<input type="checkbox"/>
4	Virgin_optionsA	Outbound	Forward	Generic (regall)			-	-		<input type="checkbox"/>
5	Virgin_optionsB	Outbound	Forward	Generic (regall)			-	-		<input type="checkbox"/>
6	Virgin_optionsA	Options_In	Allow	-			-	-		<input type="checkbox"/>
7	Virgin_optionsB	Options_In	Allow	-			-	-		<input type="checkbox"/>
8	WAN	-	Reject	-			-	-		<input type="checkbox"/>

Add new rows  rows.

### 3.7 Routing

Sip Traffic -> Routing

To spread the workload over 2 or more SIP server at Virgin fill in DNS Override For SIP Request as shown in the figure below. **This will not work in Firmware version 6.0.2 without a patch delivered by**

**Ingate systems AB**, send Ingate a mail [support@ingate.com](mailto:support@ingate.com) and tell them that you need Round Robin patch for Virgin Media.

From Firmware 6.0.3 the patch is not needed, this fix is inbuilt in firmware 6.0.3. Name of the patch is.

“patch-6-0-2-dnsrr”

Perform the following steps:

1. Click on **SIP Traffic -> Routing**
2. Fill in the IP address you got from Virgin media.
3. Click on **Save** to save the configuration to the preliminary configuration.

See example result in figure below:

The screenshot shows the InGate Firewall configuration interface. The top navigation bar includes 'Administration', 'Basic Configuration', 'Network', 'Rules and Relays', 'SIP Services', 'SIP Traffic' (highlighted), 'SIP Trunks', 'Failover', 'Virtual Private Networks', 'Quality of Service', 'Logging and Tools', and 'About'. Below this, a secondary navigation bar shows 'SIP Methods', 'Filtering', 'Local Registrar', 'Authentication and Accounting', 'SIP Accounts', 'Dial Plan', 'Routing' (highlighted), 'SIP Status', 'IDS/IPS', 'IDS/IPS Status', 'SIP Test', and 'SIP Test Status'. The main content area is titled 'DNS Override for SIP Requests (Help)'. It features a table with columns: 'Domain', 'DNS Name or IP Address', 'IP Address', 'Port', 'Transport', 'Priority', 'Weight', 'Auth', 'Modify RURI', and 'Delete Row'. A 'Random' domain is listed with two entries: one with DNS Name '81.97.95.188' and IP '81.97.95.188', and another with DNS Name '82.14.171.242' and IP '82.14.171.242'. Both entries have 'Port' empty, 'Transport' set to 'UDP', 'Priority' and 'Weight' set to '1', 'Auth' set to 'No', and 'Modify RURI' set to 'Yes'. Red arrows point to the 'Domain', 'Priority', 'Weight', and 'Modify RURI' columns. Below the table, there are input fields for 'Add new rows' (set to 1) and 'groups with' (set to 1) rows per group.

## 3.8 SIP Trunks

The SIP Trunk page is automatically configured when using SUT TG. Make any necessary changes here in order to ensure your eSBCs settings match those required by your ITSP, in this case, Virgin.

### 3.8.1 SIP Trunk 1

Perform the following steps:

1. Click on **SIP Trunks** -> **SIP Trunk 1**
2. Chose in **Restrict to calls from** Servers according to your wish, in this example to ITSP *Virgin* as defined in [Network and Computers](#).
3. It is possible to change the settings for the **From Header Domain** according to the ITSPs requirements, e.g. the ITSPs IP Address, or something else Virgin requires. SUT TG has configured this according what was filled in as *Provider Domain* at ITSP settings and set **as entered**.
4. Fill in rest of parameters according to your requirements. More information about how to fill in the SIP Trunk page is found in [How To Guide: SIP Trunking Configuration Using the SIP Trunk Page](#).

For example: add 01723 for outgoing call, in *PBX Lines, Outgoing calls, Display Name*. This will set the SIP Display Name 01723204908 when calling from PBX line 204908.

5. Click on **Save** to save the configuration to the preliminary configuration.

See example result in figure below:

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

View trunk: SIP Trunk 1: Virgin:Generic IP-PBX ▼ Goto SIP Trunk page

**SIP Trunk 1** [\(Help\)](#)

- Enable SIP Trunk
- Disable SIP Trunk

**SIP Trunking Service** [\(Help\)](#)

- Use parameters from other SIP trunk
- Define SIP trunk parameters

Service name:  (Unique descriptive name)

Service Provider Domain:  (FQDN or IP address)

Restrict to calls from: WAN ▼ ('-' = No restriction)

Outbound Proxy:  (FQDN or IP address)

Use alias IP address: - ▼ (Forces this source address from our side)

Outbound Gateway: - ▼ ('-' = Use Default Gateway)

Signaling Transport: - ▼ ('-' = Automatic)

Port number:

From header domain: Provider domain ▼

Host name in Request-URI of incoming calls:  (Trunk ID - Domain name)

Remote Trunk Group Parameters (RFC 4904):

Used as: - ▼ ('-' = Don't use IGP)

Local Trunk Group Parameters (RFC 4904):

Used as: - ▼ ('-' = Don't use IGP)



Preserve Max-Forwards: No ▼

Relay media: Yes ▼

Exactly one Via header: No ▼

'gin' registration (RFC 6140): No ▼

Hide Record-Route: No ▼

Show only one To tag: No ▼

SIP 3xx redirection to provider domain: No ▼

SIP 3xx redirection to caller domain: No ▼

Route incoming based on: Request-URI ▼

Service Provider domain is trusted: No ▼ (For P-Asserted-Identity)

Use P-Preferred-Identity: No ▼ (Instead of P-Asserted-Identity)

Forward outgoing REFER: No ▼

Max simultaneous calls:  (Call Admission Control)

Max simultaneous calls per Trunk Line:

**Main Trunk Line** [\(Help\)](#)

No.	Reg	Outgoing Calls			Authentication		Incoming Calls	
		Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to
1	No ▼		+441183374120	+441183374120@81.97.9	Auth Name Virgin	Change Password	('')	\$1

**PBX Lines** [\(Help\)](#)

No.	Reg	Outgoing Calls			Authentication		Incoming Calls		Delete Row	
		From PBX Number/User	Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match		Forward to PBX Account
1	No ▼	1183374121	+441183374121	+441183374121	+441183374121@81.97.9	Auth Name Virgin	Change Password	(01183374121)	\$1	<input type="checkbox"/>
2	No ▼	1183374122	+441183374122	+441183374122	+441183374122@81.97.9	Auth Name Virgin	Change Password	(01183374122)	\$1	<input type="checkbox"/>
3	No ▼	1183374123	+441183374123	+441183374123	+441183374123@81.97.9	Auth Name Virgin	Change Password	(01183374123)	\$1	<input type="checkbox"/>
4	No ▼	1183374124	+441183374124	+441183374124	+441183374124@81.97.9	Auth Name Virgin	Change Password	(01183374124)	\$1	<input type="checkbox"/>
5	No ▼	1183374125	+441183374125	+441183374125	+441183374125@81.97.9	Auth Name Virgin	Change Password	(01183374125)	\$1	<input type="checkbox"/>
6	No ▼	1183374126	+441183374126	+441183374126	+441183374126@81.97.9	Auth Name Virgin	Change Password	(01183374126)	\$1	<input type="checkbox"/>
7	No ▼	1183374127	+441183374127	+441183374127	+441183374127@81.97.9	Auth Name Virgin	Change Password	(01183374127)	\$1	<input type="checkbox"/>
8	No ▼	1183374128	+441183374128	+441183374128	+441183374128@81.97.9	Auth Name Virgin	Change Password	(01183374128)	\$1	<input type="checkbox"/>
9	No ▼	anonymous	anonymous	anonymous.invalid?Privac			Change Password			<input type="checkbox"/>

Add new rows | 1 rows.

**SIP Lines** (Help)

No.	Reg	Outgoing Calls				Authentication		Incoming Calls		Delete Row
		From SIP Number/User	Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to SIP Account	
Add new rows <input type="text" value="1"/> rows.										

**Setup for the PBX** (Help)

Use PBX from other SIP trunk  
 Define PBX settings

PBX Name:  (Unique descriptive name)  
 Use alias IP address:  (Forces this source address from our side)

PBX Registration SIP Address	Authentication		PBX IP Address		PBX Domain Name
	User ID	Password	DNS Name or IP Address	IP Address	
<input type="text"/>	<input type="text"/>	<input type="text" value="Change Password"/>	<input type="text" value="192.168.1.100"/>	<input type="text" value="192.168.1.100"/>	<input type="text"/>

(At least one of PBX Registration, IP address or Domain Name is required to locate the PBX)

PBX Network:   
 Signaling transport:  (\* = Automatic)  
 Port number:   
 Match From Number/User in field:   
 Common User Name suffix:   
 To header field:   
 Forward incoming REFER:   
 Remote Trunk Group Parameters usage:  (\* = Don't use TGP)  
 Local Trunk Group Parameters usage:  (\* = Don't use TGP)

Page generated for 'admin' 2017-11-27 10:20:11 +0100.  
 Ingate SIParator Firewall 6.0.2. Copyright © 2017 Ingate Systems AB.

## 4 Optional Configuration via Ingate Web Interface

### 4.1 Certificates

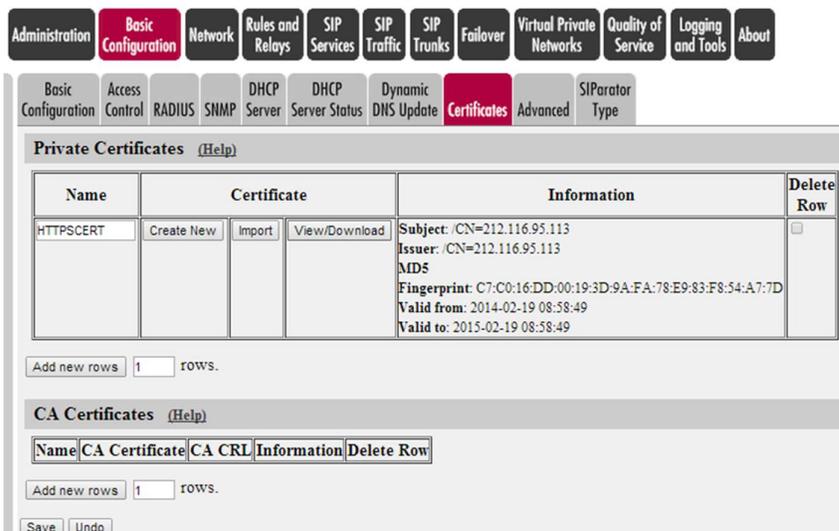
To use HTTPS to access the firewall web interface a certificate is needed.

Perform the following steps:

1. Click on **Basic Configuration** -> **Certificates**
2. Choose a name for the certificate and write it in the **Name** field.
3. Click **Create New**.
4. Fill in desired **Information** for the Certificate.
5. Click on **Save** to save the configuration to the preliminary configuration.

If you already have the certificates you can import them instead of doing above steps.

See example result in figure below:



## 4.2 Access Control

You also need to configure how to access the web interface of the firewall.

Perform the following steps:

1. Click on **Basic Configuration** -> **Access Control**
2. Configuration via HTTP is already on for inside from the startup of the firewall.
3. If you want to be able to configure the firewall from the outside this is done over HTTPS. Select which **IP address** and **Port** the firewall administrator should direct the web browser to.
4. Select the **Certificate to use** you created/imported in the previous chapter.
5. Create new rows for your **Configuration Computers** by clicking on: **Add new rows** and fill in number of rows to add.
6. Fill in **IP Address** and **Netmask/Bits** and chose HTTP or HTTPS for respective Configuration Computer.
7. Click on **Save** to save the configuration to the preliminary configuration.

See example result in figure below:

**Configuration Allowed Via Interface** (Help)

Interface or Tunnel	Allowed	Delete Row
inside (eth0)	Yes	<input type="checkbox"/>

Add new rows  rows.

**Configuration Transport** (Help)

Protocol	IP Address	Port	Cert	TLS	Delete Row
HTTP	inside (192.168.1.111)	80	-	-	<input type="checkbox"/>

Add new rows  rows.

**User Authentication For Web Interface Access** (Help)

- Local users
- RADIUS database
- Local users or RADIUS database

**Web Interface Access Settings** (Help)

Login timeout:  seconds 

**Configuration Computers** (Help)

No.	DNS Name or Network Address	Network Address	Netmask / Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	Log Class	Delete Row
1	192.168.1.0	192.168.1.0	255.255.255.0	192.168.1.0 - 192.168.1.255	-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Local	<input type="checkbox"/>

Add new rows  rows.

Save Undo Look up all IP addresses again

## 5 Finalize the configuration

Finally click on the **Administration** tab and click the **Apply Configuration** button to apply the changes to the Ingate unit. Press **Save configuration** to complete the saving process.

## 6 Where entered configuration ends up

Beside pages already shown in this document, following pages includes configurations that was entered with the SUT TG.

### 6.1 All Interfaces

To get an overview of all interfaces.

Click on **Network** -> **All Interfaces**

See example result in figure below:

**inGate Firewall** Configured by Ingate SUT TG Log Out

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

Networks and Computers Default Gateways **All Interfaces** NAT VLAN Eth0 Eth1 Eth2 Eth3 Interface Status PPPoE Tunnels Topology

#### Interface Overview

**General**

Physical Device	Interface Name	Active	Speed and Duplex
eth0	inside	Yes ▼	Autonegotiation ▼
eth1	outside	Yes ▼	Autonegotiation ▼
eth2	Ethernet2	No ▼	Autonegotiation ▼
eth3	Ethernet3	No ▼	Autonegotiation ▼

**Directly Connected Networks** (Help)

Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	Interface or Tunnel	VLAN Id	VLAN Name	Delete Row
inside	Static ▼	192.168.1.111	192.168.1.111	255.255.255.0	192.168.1.0	192.168.1.255	inside (eth0) ▼		-	<input type="checkbox"/>
outside	Static ▼	193.180.23.30	193.180.23.30	255.255.255.0	193.180.23.0	193.180.23.255	outside (eth1) ▼		-	<input type="checkbox"/>

Add new rows  rows.

**Alias** (Help)

Name	DNS Name or IP Address	IP Address	Interface	Delete Row
------	------------------------	------------	-----------	------------

Add new rows  rows.

**Proxy ARP** (Help)

Get Network From	Proxy ARPed Network			Interface	VLAN Id	VLAN Name	Delete Row
	DNS Name or Network Address	Network Address	Netmask / Bits				

Add new rows  rows.

#### Static Routing

**Static Routing** (Help)

Routed Network			Router			Interface or Tunnel	Delete Row
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address		
default	default		- ▼	193.180.23.1	193.180.23.1	outside (eth1) ▼	<input type="checkbox"/>

Add new rows  rows.

**Unreachable** (Help)

Unreachable Network			Delete Row
DNS Name or Network Address	Network Address	Netmask / Bits	

Add new rows  rows.