



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Ingate SIParator in an Avaya SIP Telephony Environment – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Ingate SIParator 4.4.1 converged network appliance to successfully interoperate with Avaya SIP Enablement Services in an Avaya SIP Telephony environment. The Ingate SIParator provided SIP-aware Network Address Translation as well as SIP proxy functions during the compliance testing.

Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

Session Initiation Protocol (SIP) based communications cannot traverse Network Address Translation (NAT) devices nor firewalls that do not offer the SIP application layer gateway support. The Ingate SIParator is a converged network appliance that can connect to an existing firewall to seamlessly enable the traversal of real-time SIP-based communications. The Ingate SIParator provided SIP-aware Network Address Translation as well as SIP proxy functions during the compliance testing. The integration with the Avaya SIP Telephony environment includes Avaya Communication Manager 3.1.1, Avaya SIP Enablement Services 3.1, and Avaya 4600 Series SIP and H.323 Telephones.

The SIParator can be connected to an existing firewall in three different ways, and only the standalone configuration was utilized in the compliance testing¹. In the standalone configuration shown in **Figure 1**, the SIParator at Site A is connected to the internal private network on its private interface, and to the external public network on its public interface. All SIP traffic between Site A and Site B are routed via the SIParator, with NAT enabled at Site A. For simplicity of the compliance testing, NAT was not enabled at Site B.

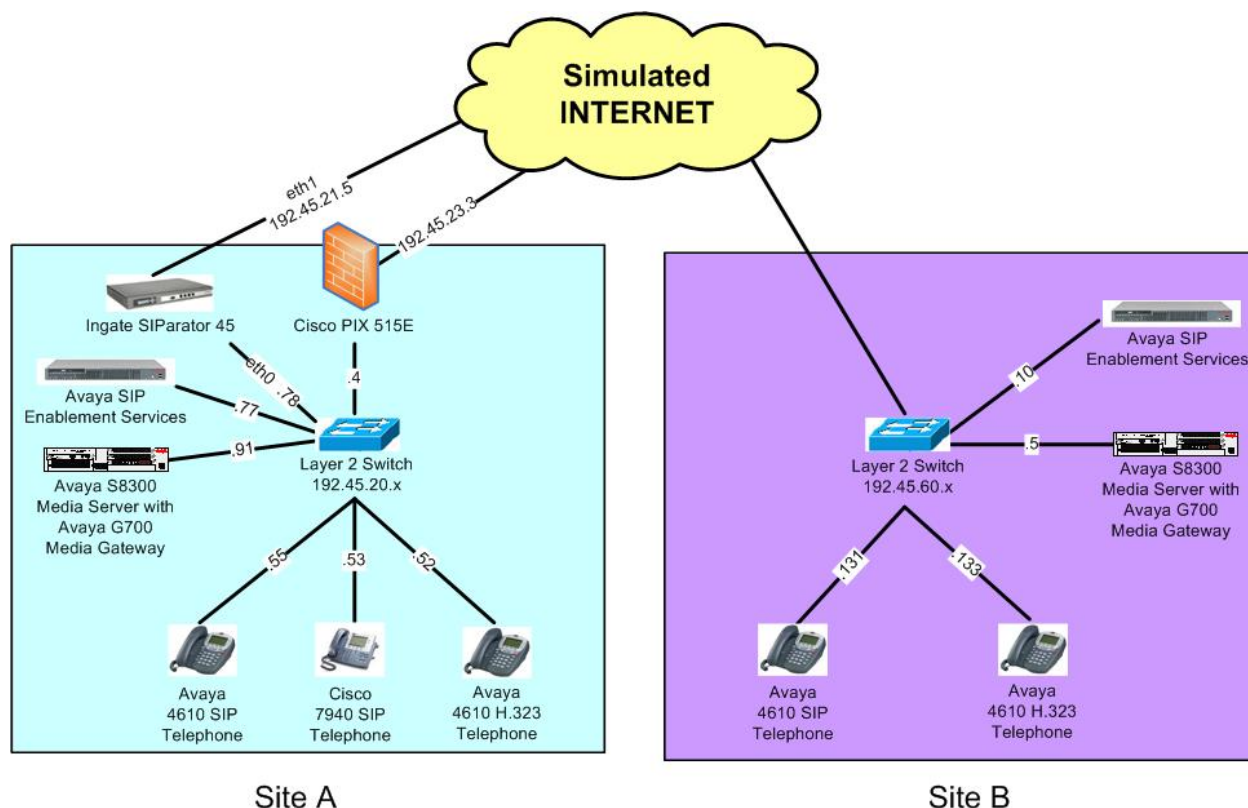


Figure 1: Standalone Ingate SIParator in an Avaya SIP IP Telephony Environment

¹ Refer to the Ingate SIParator documentation in **Section 9** for descriptions of the other connectivity methods.

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8300 Media Servers with G700 Media Gateways	Communication Manager 3.1.1, load 628.7
Avaya SIP Enablement Services	3.1, load 18
Avaya 4610SW IP Telephones (SIP)	2.2.2
Avaya 4612 & 4624 IP Telephones (H.323)	1.8.3
Cisco 7940 SIP Telephone	P0S3-07-4-00
Cisco PIX 515E	IOS 7.1(2)
Ingate SIParator 45	4.4.1

3. Configure Avaya SIP Enablement Services

The detailed administration of the Avaya SIP infrastructure is not the focus of these Application Notes and will not be described. For administration of the Avaya SIP infrastructure, refer to the appropriate documentation listed in **Section 9**.

This section assumes the SIP configuration and connectivity are already in place within each site, and that routing rules are in place in Avaya Communication Manager to route calls across sites. For simplicity, the compliance testing utilized 5-digit routing between Site A and Site B.

Site A has SIP and H.323 telephone users with extensions 77000-78999, and Site B has SIP and H.323 telephone users with extensions 37000-38999. Since all SIP traffic between Site A and Site B is routed via the Ingate SIParator, both sites will need to specify the SIParator as the host contact.

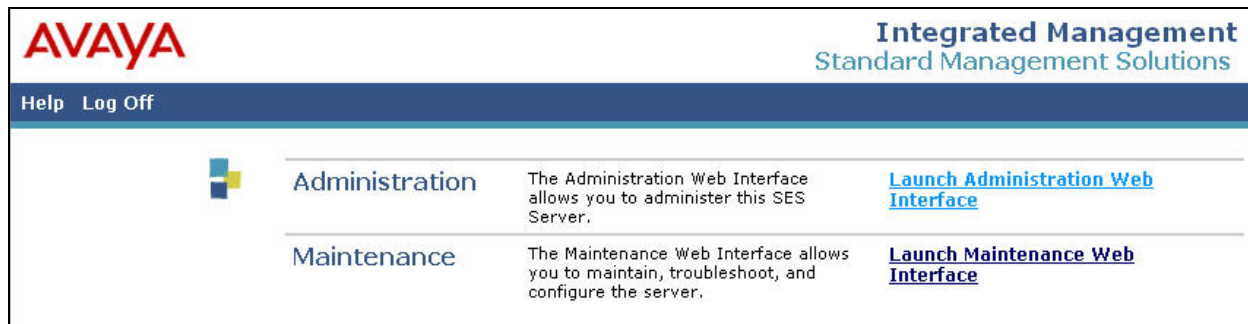
This section provides the procedures for configuring the following at each site:

- Administer host address map
- Administer host contact
- Administer trusted host

3.1. Administer Host Address Map

3.1.1. Host Address Map at Site A

Access the SIP Enablement Services (SES) administration web interface by using the URL “http://<ip-address>/admin” in an Internet browser window, where <ip-address> is the IP address of the SES server at Site A. Note that the IP address for the SES server may vary, and in this case “192.45.20.77” is used. Log in with the appropriate credentials and select the **Launch Administration Web Interface** option.



The **Top** screen is displayed next. Select **Hosts > List** from the left pane.

AVAYA Integrated Management SIP Server Management
 Help Exit Server: 192.45.20.77

Top

Manage Users	Add and delete Users.
Manage Conferencing	Add and delete Conference Extensions.
Manage Media Server Extensions	Add and delete Media Server Extensions.
Manage Emergency Contacts	Add and delete Emergency Contacts.
Manage Hosts	Add and delete Hosts.
Manage Media Servers	Add and delete Media Servers.
Manage Adjunct Systems	Add and delete Adjunct Systems.
Manage Services	Start and stop server processes on this host.
Server Configuration	Edit Properties of the system.
Certificate Management	Manage Web Certificate.
IM Logs	Download IM Logs.
Trace Logger	Manage SIP Trace Logs.
Export Import to ProVision	Export and import data using ProVision on this host.

The **List Hosts** screen is displayed. Click on the **Map** link.

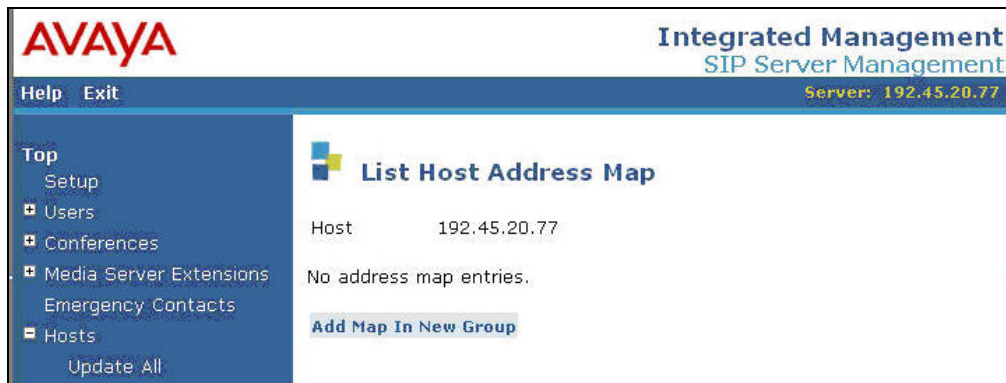
AVAYA Integrated Management SIP Server Management
 Help Exit Server: 192.45.20.77

List Hosts

Status	Commands			Host	Type
up to date	Edit	Map	Go-To	Test-Link	Delete
			192.45.20.77		home/edge

Force All Migrate Home/Edge

In the **List Host Address Map** screen below, click on the **Add Map In New Group** link in the right pane.



The **Add Host Address Map** screen is displayed next. This screen is used to specify which calls are to be routed to the other site. For the **Name** field, enter a descriptive name to denote the routing. For the **Pattern** field, enter an appropriate syntax for address mapping. For the compliance testing, a pattern of “`^sip:3[7-8]{1}[0-9]{3}`” is used to match to any extensions in the range of 37000-38999 at Site B. Maintain the check in **Replace URI**, and click **Add**.



The **Continue** screen is displayed next. Click on the **Continue** button.



3.1.2. Host Address Map at Site B

Repeat the same procedures in **Section 3.1.1** to administer the host address map at Site B. In the Internet browser window, use the IP address of the SES server at Site B, in this case “192.45.60.10”. For the host address map, use a pattern of “^sip:7[7-8]{1}[0-9]{3}” to map to extensions in the range of 77000-78999 at Site A, as shown below.



AVAYA Integrated Management SIP Server Management
Server: 192.45.60.10

Help Exit

Top
Setup
Users
Conferences
Media Server Extensions
Emergency Contacts
Hosts
List
Migrate Home/Edge
Media Servers

Add Host Address Map

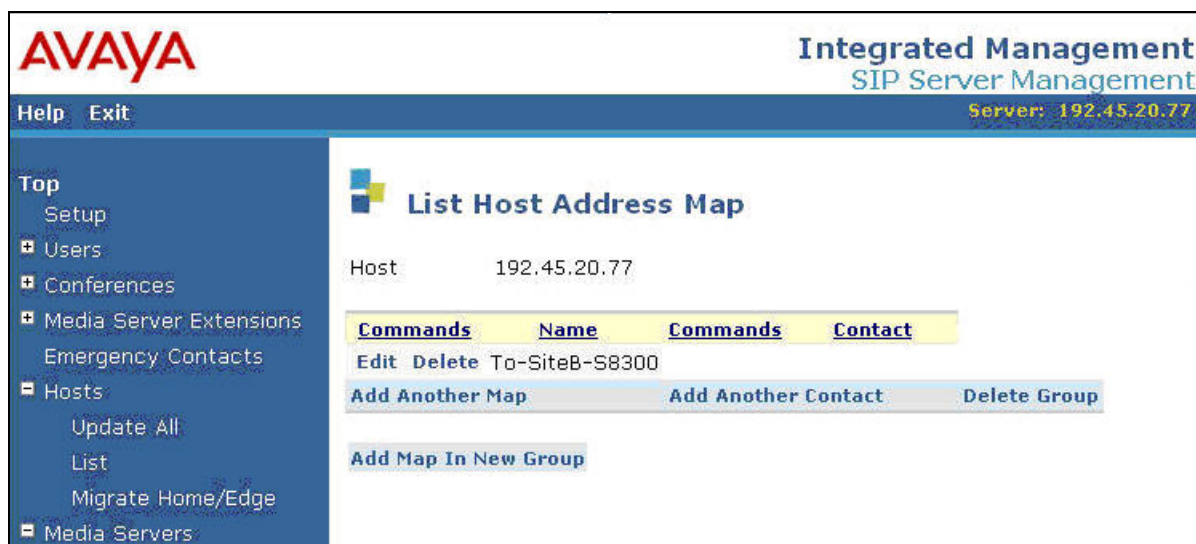
Host: 192.45.60.10
Name*: To-SiteA-S8300
Pattern*: ^sip:7[7-8]{1}[0-9]{3}
Replace URI: ☒
Fields marked * are required.

Add

3.2. Administer Host Contact

3.2.1. Host Contact at Site A

The **List Host Address Map** screen is displayed, and updated with the new address map. Click on **Add Another Contact**.



AVAYA Integrated Management SIP Server Management
Server: 192.45.20.77

Help Exit

Top
Setup
Users
Conferences
Media Server Extensions
Emergency Contacts
Hosts
Update All
List
Migrate Home/Edge
Media Servers

List Host Address Map

Host: 192.45.20.77

Commands	Name	Commands	Contact
Edit Delete	To-SiteB-S8300		

Add Another Map **Add Another Contact** **Delete Group**

Add Map In New Group

All outgoing SIP messages from Site A will be sent to the private network interface of the SIParator. In the **Add Host Contact** screen, enter the contact “sip:\$(user)@192.45.20.78:5060;transport=tcp”. Note the use of the SIParator private network IP address “192.45.20.78” in the contact information, along with port “5060” and transport method of “tcp”. These three values need to match the SIParator dial plan in **Section 4.7**. SES will substitute “\$(user)” with the user portion of the request URI before sending the message to Site B. Click on the **Add** button.



AVAYA Integrated Management
SIP Server Management
Server: 192.45.20.77

Help Exit

Top
Setup
Users
Conferences
Media Server Extensions
Emergency Contacts
Hosts
Update All
List

Add Host Contact

Host 192.45.20.77
Handle To-SiteB-S8300
Contact* sip:\$(user)@192.45.20.78:5060;transport=tcp
Fields marked * are required.

Add

The **Continue** screen is displayed next. Click on the **Continue** button.



AVAYA Integrated Management
SIP Server Management
Server: 192.45.20.77

Help Exit

Top
Setup
Users
Conferences
Media Server Extensions
Emergency Contacts
Hosts
Update All

Continue

Host contact sip:\$(user)@192.45.20.78:5060;transport=tcp added for map entry To-SiteB-S8300

Continue

3.2.2. Host Contact at Site B

In the compliance-tested configuration, all outgoing SIP messages from Site B were sent to the public network interface of the SIParator. Had Site B utilized a SIP-aware NAT device, then the outgoing SIP messages would have been sent to the private network interface of the NAT device at Site B.

Repeat the same procedures in **Section 3.2.1** to administer the host contact at Site B. Enter the contact “sip:\$(user)@192.45.21.5:5060; transport=tcp”. Note the use of the SIParator public network IP address “192.45.21.5” in the contact information, along with port “5060” and transport method of “tcp”. SES will substitute “\$(user)” with the user portion of the request URI before sending the message to Site A. Click on the **Update** button.



The screenshot displays the Avaya Integrated Management SIP Server Management web interface. The top header features the Avaya logo on the left and the text 'Integrated Management SIP Server Management' on the right, with a server status indicator 'Server: 192.45.60.10'. A navigation menu on the left includes links for 'Help', 'Exit', 'Top', 'Setup', 'Users', 'Conferences', 'Media Server Extensions', 'Emergency Contacts', 'Hosts', and 'List'. The main content area is titled 'Edit Host Contact' and contains two input fields: 'Host' with the value '192.45.60.10' and 'Contact' with the value 'sip:\$(user)@192.45.21.5:5060;transport=tc'. Below these fields is a note 'Fields marked * are required.' and an 'Update' button.

3.3. Administer Trusted Host

3.3.1. Trusted Host at Site A

Administer SIParator as a trusted host at Site A, so that SIP messages from the SIParator will not be challenged. To configure a trusted host, use the “trustedhost -a x -n y” command in the Linux shell of SES, where “x” is the private network IP address of the SIParator, and “y” is the IP address of the SES at Site A.

```
craft@SES-DevCon1> trustedhost -a 192.45.20.78 -n 192.45.20.77
192.45.20.78 is added to trusted host list.
```

After configuring the trusted host, the user must go back to the SES administration web interface, and click on the **Update** link in the bottom of the left pane for any changes in **Section 3** to take effect.

3.3.2. Trusted Host at Site B

Repeat the same procedures in **Section 3.3.1** to administer SIParator as a trusted host at Site B. Use the public network IP address of the SIParator, and the IP address of the SES at Site B as shown below. Had Site B utilized a SIP-aware NAT device, then the private network interface of the NAT device at Site B would have been administered as the trusted host instead.

Remember to click on the **Update** link in the SES administration web interface.

```
craft@SES-DevCon60> trustedhost -a 192.45.21.5 -n 192.45.60.10
192.45.21.5 is added to trusted host list.
```

4. Configure Ingate SIParator

This section provides the procedures for configuring the Ingate SIParator. The procedures include the following areas:

- Administer IP address
- Verify installed modules
- Administer basic configuration
- Administer network
- Administer basic configuration continued
- Administer SIP services
- Administer SIP traffic
- Apply configuration

4.1. Administer IP Address

Connect a PC to the console serial port of the SIParator. Use a terminal emulator program, set the baud rate to 19,200 bits per second and log in with administrative credentials. The command line interface session will begin with the screen below. Enter “1” as shown, and press enter.

```
Ingate SIParator Administration
1. Basic configuration
2. Save/Load configuration
3. Become a failover team member
4. Leave failover team and become standalone
5. Wipe email logs
6. Set password
q. Exit admin
==>1
```

The screen below is displayed next. For **IP address**, enter the private network IP address for the SIParator. For **Netmask/bits**, enter the net mask for the private network. For **Configure from a single computer**, enter “n” to allow more than one computer to configure the SIParator.

```
Basic unit installation program version 4.4

Press return to keep the default value

Network configuration inside:
Physical device name[eth0]:
IP address [0.0.0.0]: 192.45.20.78
Netmask/bits [255.255.255.0]: 255.255.255.0
Deactivate other interfaces? (y/n) [n]

Computers from which configuration is allowed:

You can select either a single computer or a network.

Configure from a single computer? (y/n) [y]n
```

The screen below is displayed, for specifying further information regarding the computers that can configure the SIParator. For **Network number** and **Netmask/bits**, enter the IP addresses of computers allowed to configure the SIParator. In this case, any computer on the 192.45.20.0/24 subnet will be permitted. For **Password**, enter a new password for the administrative login. Enter “y” to reset the configuration, and an update mode of “3” to remove all previous configurations and apply the current one.

```
Network number [0.0.0.0]: 192.45.20.0
Netmask/bits [255.255.255.0]: 255.255.255.0

Password []:xxx

Other configuration

Do you want to reset the rest of the configuration? (y/n) [n]y
Update mode (1-3) [1]:3
```

The screen below is displayed next. Verify the configuration values, and enter “yes” to complete the configuration.

You have now entered the following configuration

Network configuration inside:

Physical device name: eth0

IP address: 192.45.20.78

Netmask: 255.255.255.0

Deactivate other interfaces: no

Computer allowed to configure from:

Network Number: 192.45.20.0

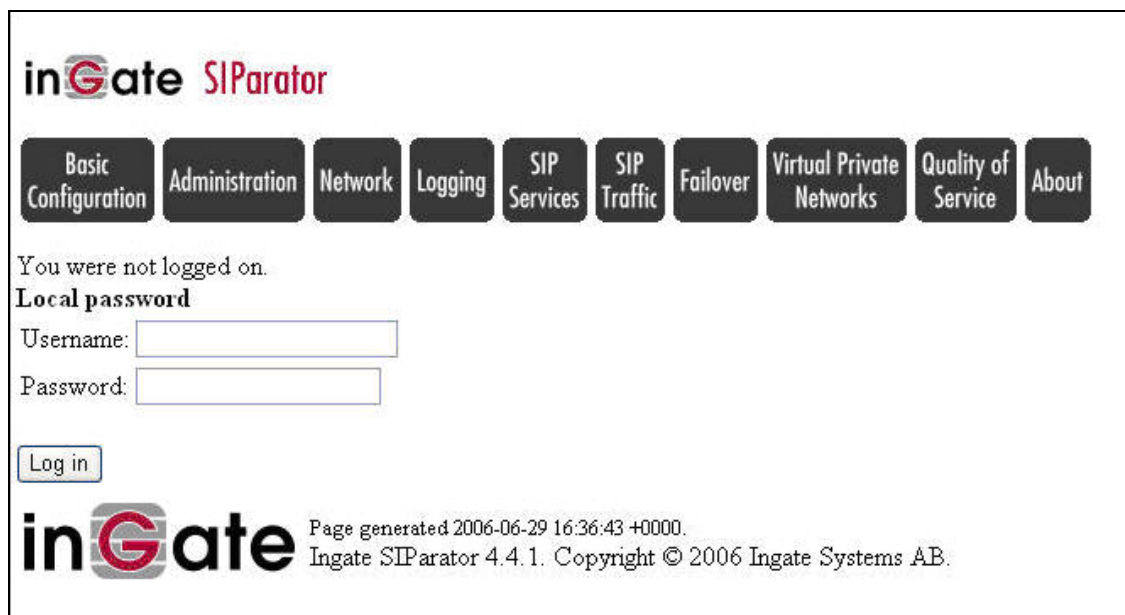
Password: xxx

The rest of the configuration is kept.

Is this configuration correct (yes/no/abort)? **yes**

4.2. Verify Installed Modules

Open an Internet browser window from a PC that meets the network configuration criteria (i.e., configuration of the IP addresses of computers allowed to configure the SIParator) defined in **Section 4.1**. Enter the private network IP address of the SIParator administered in **Section 4.1**, to display the screen below. Enter the administrative user name and password, and click **Log in**.



The screenshot displays the inGate SIParator web interface. At the top, the logo "inGate SIParator" is visible. Below the logo is a horizontal menu with buttons for "Basic Configuration", "Administration", "Network", "Logging", "SIP Services", "SIP Traffic", "Failover", "Virtual Private Networks", "Quality of Service", and "About". The "Basic Configuration" button is highlighted. Below the menu, a message states "You were not logged on." followed by the heading "Local password". There are two input fields: "Username:" and "Password:". Below these fields is a "Log in" button. At the bottom of the page, the "inGate" logo is displayed next to the text "Page generated 2006-06-29 16:36:43 +0000. Ingate SIParator 4.4.1. Copyright © 2006 Ingate Systems AB."

Upon logging in, select **About** from the main menu to display the information below. Verify that the appropriate optional modules are installed. Consult with SIParator personnel to determine the appropriate set of optional modules required for the customer configuration. The compliance testing included scenarios that utilized the **Advanced SIP Routing** and **QoS** optional modules.

inGate SIParator Log out

1 other administrator(s) currently logged in.

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

Ingate SIParator 45
Serial number: IG-425-524-2024-4
Version: 4.4.1
Installed patches:
Installed modules:

- Advanced SIP Routing
- Remote SIP Connectivity (NAT Traversal)
- VoIP Survival
- VPN (IPsec and PPTP)
- QoS

Installed licenses:

- 10 SIP User Registration Licenses
- 5 SIP Traversal Licenses
- 0 SIP Advanced Routing Seat Licenses

[More about Ingate SIParator](#)

inGate Page generated for 'admin' 2006-06-29 16:35:27 +0000.
Ingate SIParator 4.4.1. Copyright © 2006 Ingate Systems AB.

4.3. Administer Basic Configuration

Select **Basic Configuration** from the main menu, followed by **SIParator Type** to display the screen below. In the **Change SIParator type to** drop down box, select “Standalone”. Click **Change type** upon any change to the default value.

inGate SIParator Log out

1 other administrator(s) currently logged in.

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

Basic Configuration Access Control RADIUS SNMP Dynamic DNS Update Certificates Advanced **SIParator Type**

Type of SIParator [\(Help\)](#)

The SIParator can be connected to your network in three different ways, depending on your needs.

Current SIParator type: Standalone Change SIParator type to: Standalone Change type

4.4. Administer Network

Select **Network** from the main menu, followed by **Eth0** to verify the eth0 private network interface settings. In the **General** section, verify the **On** radio button is selected. In the **Directly Connected Networks** section, verify the values are properly populated based on the information entered via the console serial port connection from **Section 4.1**.

The screenshot shows the inGate SIParator web interface. The top navigation bar includes buttons for Basic Configuration, Administration, Network (selected), Logging, SIP Services, SIP Traffic, Failover, Virtual Private Networks, Quality of Service, and About. Below this is a sub-navigation bar with buttons for Networks and Computers, Default Gateways, All Interfaces, VLAN, Eth0 (selected), Eth1, Eth2, Eth3, Interface Status, PPPoE, and Surroundings. The main content area is divided into two sections: General and Obtain IP Address Dynamically. The General section shows the Physical device as eth0, and the interface is set to On. The Obtain IP Address Dynamically section has radio buttons for OFF (selected), DHCP client ON, and PPPoE client ON. Below these sections is the Directly Connected Networks table, which contains one row for the eth0 interface with the following values: Name: eth0, DNS name or IP address: 192.45.20.78, IP address: 192.45.20.78, Netmask / bits: 255.255.255.0, Network Address: 192.45.20.0, Broadcast Address: 192.45.20.255, VLAN Id: (empty), and VLAN Name: -. At the bottom, there is an 'Add new rows' button and a text field showing '1 rows'.

Name	DNS name or IP address	IP address	Netmask / bits	Network Address	Broadcast Address	VLAN Id	VLAN Name
eth0	192.45.20.78	192.45.20.78	255.255.255.0	192.45.20.0	192.45.20.255		-

Next, select the **Eth1** tab to configure the eth1 public network interface. In the **General** section, select the **On** radio button. In the **Directly Connected Networks** section, click on **Add new rows** and enter the public network information shown below. Note that the actual values for the **Name**, **DNS name or IP address**, and **Netmask / bits** fields may vary, and that the field values in grey are automatically populated based on information entered. Maintain the default values in all remaining fields.

The screenshot shows the inGate SIParator web interface with the Eth1 tab selected. The General section shows the Physical device as eth1, and the interface is set to On. The Obtain IP Address Dynamically section has radio buttons for OFF (selected), DHCP client ON, and PPPoE client ON. Below these sections is the Directly Connected Networks table, which contains one row for the eth1 interface with the following values: Name: Outside_interface, DNS name or IP address: 192.45.21.5, IP address: 192.45.21.5, Netmask / bits: 255.255.255.0, Network Address: 192.45.21.0, Broadcast Address: 192.45.21.255, VLAN Id: (empty), and VLAN Name: -. At the bottom, there is an 'Add new rows' button and a text field showing '1 rows'.

Name	DNS name or IP address	IP address	Netmask / bits	Network Address	Broadcast Address	VLAN Id	VLAN Name
Outside_interface	192.45.21.5	192.45.21.5	255.255.255.0	192.45.21.0	192.45.21.255		-

Select the **Default Gateways** tab to configure the public network default gateway. Click on **Add new rows**. Enter the gateway IP address for the public network interface, and select “Ethernet1 (eth1)” from the drop down box.

The screenshot shows the inGate SIParator web interface. The top navigation bar includes tabs for Basic Configuration, Administration, Network (selected), Logging, SIP Services, SIP Traffic, Failover, Virtual Private Networks, Quality of Service, and About. Below this, a sub-navigation bar shows Networks and Computers, Default Gateways (selected), All Interfaces, VLAN, Eth0, Eth1, Eth2, Eth3, Interface Status, PPPoE, and Surroundings. The main content area is titled "Default Gateways (Help)". It contains a table with the following data:

DNS name or IP address	IP address	Interface	Delete Row
192.45.21.1	192.45.21.1	Ethernet1 (eth1)	<input type="checkbox"/>

Below the table, there is a button "Add new rows" and a text input "1" followed by "rows".

Select the **Networks and Computers** tab to define the range of IP addresses on each network. Click on **Add new rows** and add a row for each network interface as shown below. Note that the actual values for the **Name** and **DNS name or IP address** fields may vary. The eth0 interface connects to the private network, with IP addresses in the 192.45.20.0/24 subnet. The eth1 interface connects to the public network, with any IP addresses denoted by “0.0.0.0”.

The screenshot shows the inGate SIParator web interface. The top navigation bar is the same as the previous screenshot. The sub-navigation bar shows Networks and Computers (selected), Default Gateways, All Interfaces, VLAN, Eth0, Eth1, Eth2, Eth3, Interface Status, PPPoE, and Surroundings. The main content area is titled "Networks and Computers". It contains a table with the following data:

Name	Subgroup	Lower limit		Upper limit (for IP ranges)		Interface
		DNS name or IP address	IP address	DNS name or IP address	IP address	
Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	Ethernet1 (e
LAN	-	192.45.20.0	192.45.20.0	192.45.20.255	192.45.20.255	Ethernet0 (e

Below the table, there is a button "Add new rows" and a text input "1" followed by "groups with" and another text input "1" followed by "rows per group".

4.5. Administer Basic Configuration Continued

Select **Basic Configuration** from the main menu, followed by **Certificates** to create an X.509 certificate for authentication use. Click on **Add new rows**. Enter a descriptive **Name** for the certificate, and click on **Create New**.

The screenshot shows the inGate SIParator web interface. At the top, there's a header with the logo and a 'Log out' button. Below the header, a navigation bar contains buttons for 'Basic Configuration', 'Administration', 'Network', 'Logging', 'SIP Services', 'SIP Traffic', 'Failover', 'Virtual Private Networks', 'Quality of Service', and 'About'. A secondary navigation bar includes 'Basic Configuration', 'Access Control', 'RADIUS', 'SNMP', 'Dynamic DNS Update', 'Certificates' (which is highlighted), 'Advanced', and 'SIParator Type'. The main content area is titled 'Private Certificates (Help)'. It features a table with columns: 'Name', 'Certificate', 'Information', and 'Delete Row'. The 'Name' column contains 'HTTP_Cert'. The 'Certificate' column has buttons for 'Create New', 'Import', and 'View/Download'. The 'Delete Row' column has a checkbox. Below the table, there's a button 'Add new rows' followed by a text input '1' and the word 'rows'.

The screen below is displayed next. For **Common Name**, enter the IP address of the public network interface. Maintain the default value in the remaining fields. Select **Create a self-signed X.509 certificate** or **Create an X.509 certificate request** based on customer corporate policy. For the compliance testing, a self-assigned certificate was created.

The screenshot shows the 'Create Certificate or Certificate Request' form. It includes instructions: 'Fill in the certificate data for "RADIUS" below, then create either a certificate or a certificate request. After generating a certificate request, and having it signed by a signing authority, the certificate must be imported to the firewall.' The form has several input fields: 'Expire in (days):' with a value of 365, 'Country code (C):', 'Organization (O):', 'Common Name (CN):' with a value of 192.45.21.5, 'State/province (ST):', 'Organizational Unit (OU):', 'Email address', and 'Locality/town (L):'. There are also fields for 'Serial number:' (with a value of 0) and 'Challenge password:' (with a confirmation field). At the bottom, there are three buttons: 'Create a self-signed X.509 certificate', 'Create an X.509 certificate request', and 'Abort'. A note at the bottom left states: 'Fields marked with "*" are mandatory.'

Select the **Access Control** tab. In the **Configuration via HTTPS** section on the right, select the public network interface for **Direct the web browser to this address**, and select the newly created certificate for **Certificate to use**. Maintain the default values in all remaining fields.

The screenshot shows the inGate SIParator web interface. At the top, there's a header with the logo and a "Log out" button. Below the header, it says "1 other administrator(s) currently logged in." There are two rows of navigation tabs. The first row includes "Basic Configuration", "Administration", "Network", "Logging", "SIP Services", "SIP Traffic", "Failover", "Virtual Private Networks", "Quality of Service", and "About". The second row includes "Basic Configuration", "Access Control" (which is highlighted in red), "RADIUS", "SNMP", "Dynamic DNS Update", "Certificates", "Advanced", and "SIParator Type". The main content area is titled "Configuration Transport (Help)". It has two columns: "Configuration via HTTP" and "Configuration via HTTPS". Under "Configuration via HTTP", there's a dropdown menu for "Direct the web browser to this address:" showing "eth0 (192.45.20.78)", a "Port:" field with "80", and a "Certificate to use:" dropdown showing "HTTP_Cert". Under "Configuration via HTTPS", there's a dropdown menu for "Direct the web browser to this address:" showing "Outside_interface (192.45.21.5)", a "Port:" field with "443", and a "Certificate to use:" dropdown showing "HTTP_Cert".

4.6. Administer SIP Services

Select **SIP Services** from the main menu, followed by **Basic** to display the screen below. In the **SIP Module** section, select the **On** radio button. In the **SIP Logging** section, select "Local" as the log class for all four fields to enable logging to the local computer.

The screenshot shows the inGate SIParator web interface. At the top, there's a header with the logo and a "Log out" button. Below the header, it says "1 other administrator(s) currently logged in." There are two rows of navigation tabs. The first row includes "Basic Configuration", "Administration", "Network", "Logging", "SIP Services" (which is highlighted in red), "SIP Traffic", "Failover", "Virtual Private Networks", "Quality of Service", and "About". The second row includes "Basic" (highlighted in red), "Signaling Encryption", "Media Encryption", "Interoperability", "Sessions and Media", "Remote SIP Connectivity", "VoIP Survival", and "VoIP Survival Status". The main content area is titled "SIP Services (Help)". It has two columns: "SIP Module" and "SIP Logging". Under "SIP Module", there's a "SIP module:" section with "On" and "Off" radio buttons, and an "Additional SIP Signaling Ports (Help)" section with a table. The table has columns "Port", "Transport", and "Delete Row". Below the table is an "Add new rows" button and a field for "1 rows". Under "SIP Logging", there are four dropdown menus for "Log class for SIP signaling:", "Log class for SIP packets:", "Log class for SIP errors:", and "Log class for SIP debug messages:", all of which are set to "Local".

4.7. Administer SIP Traffic

Select **SIP Traffic** from the main menu, followed by **Filtering** to display the screen below. In the **Proxy Rules** section, select the **Process all** radio button to enable processing for all SIP requests. In the **Content Types** section, select **Add new rows** and enter the information shown below. For **Content type**, enter “*/*” to denote all content types. For the **Allow** drop down box, select “On” to allow processing of all SIP content types. Maintain the default values for the remaining fields.

Proxy Rules (Help)

No.	From network	Action	Delete Row
<input type="button" value="Add new rows"/> 1 rows.			

Default Policy For SIP Requests

☒ Process all
☐ Local only
☐ Reject all

Header Filter Rules (Help)

No.	From Header	To Header	Action	Delete Row
<input type="button" value="Add new rows"/> 1 rows.				

Default Header Filter Policy

☒ Process
☐ Reject

Content Types (Help)

Edit Row	Content type	Allow	Delete Row
<input checked="" type="checkbox"/>	*/*	On	<input type="checkbox"/>
<input type="checkbox"/>	application/SOAP+xml	Off	<input type="checkbox"/>
<input type="checkbox"/>	application/adrl+xml	Off	<input type="checkbox"/>
<input type="checkbox"/>	application/pdf+xml	Off	<input type="checkbox"/>
<input type="checkbox"/>	application/vnd-microsoft-roaming-acls+xml	Off	<input type="checkbox"/>
<input type="checkbox"/>	application/vnd-microsoft-roaming-contacts+xml	Off	<input type="checkbox"/>
<input type="checkbox"/>	application/vnd-microsoft-roaming-provisioning+xml	Off	<input type="checkbox"/>
<input type="checkbox"/>	application/xml	Off	<input type="checkbox"/>
<input type="checkbox"/>	image/jpeg	Off	<input type="checkbox"/>
<input type="checkbox"/>	text/html	Off	<input type="checkbox"/>
<input type="checkbox"/>	text/pdf	Off	<input type="checkbox"/>
<input type="checkbox"/>	text/plain	Off	<input type="checkbox"/>
<input type="checkbox"/>	text/xml	Off	<input type="checkbox"/>
<input type="checkbox"/>	text/xml+msrtc.pdf	Off	<input type="checkbox"/>
<input type="checkbox"/>	text/xml+msrtc.wpending	Off	<input type="checkbox"/>

1 rows.

Select the **Dial Plan** tab to configure routing of SIP calls. Maintain the default values in the **Use Dial Plan**, **Emergency Number**, and **Matching From Header** sections.

The **Matching Request-URI** section is used to define the criteria for matching to the Request-URI in the SIP messages. Click on **Add new rows** to add the matching criteria for the network configuration. For the compliance testing, three criteria were added as shown below. Note that the support for use of IP addresses in the **Domain** field is provided by the Advanced SIP Routing module.

The first criterion matches SIP messages to Site A that have the following characteristics: the user portion of the request URI contains digits that start with “7” (**Head**) followed by any number of digits “0-9” (**Tail**), and the domain portion contains the SIParator public network IP address (**Domain**). The second and third criterion defines the SIP messages to Site B that have the following characteristics: the user portion of the request URI contains digits that start with “37” or “38” followed by any number of digits “0-9”, and the domain portion contains the SIParator private network IP address.

inGate SIParator Log out

1 other administrator(s) currently logged in.

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

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

Use Dial Plan [\(Help\)](#) **Emergency Number** [\(Help\)](#)

☒ On ☐ Off ☐ Fallback

911

Matching From Header [\(Help\)](#)

Name	Use this or this	Transport	Network	Delete R
	Username	Domain	Reg Exp			
Any	*	*		Any	-	<input type="checkbox"/>

[Add new rows](#) 1 rows.

Matching Request-URI [\(Help\)](#)

Name	Use this
	Prefix	Head	Tail	Min. Tail	Domain	
To Site A		7	0..9		192.45.21.5	
To Site B_37		37	0..9		192.45.20.78	
To Site B_38		38	0..9		192.45.20.78	

[Add new rows](#) 1 rows.

The **Forward To** section is used to define the criteria for where to and how the requests should be forwarded. Click on **Add new rows** to add the criteria for the network configuration. For the compliance testing, two criteria were added as shown below. SIP messages to Site A and Site B will have the domain portion of the URI replaced by the IP address of the receiving SES server. The values entered for the **Port** and **Transport** fields will need to match the SES host contact information configured in **Section 3.2**.

The **Dial Plan** section is used to define the actual dial plan, by matching entries in the **Matching Request-URI** section with entries in the **Forward To** section, and selecting an **Action** type. Click on **Add new rows** to add dial plan entries for the network configuration. For the compliance testing, three dial plan entries were added as shown below. The “Forward” **Action** type allows the messages to be sent to the **Forward To** destination.

Forward To (Help)							
Name	Subno.	Use this or this		... or this		De
		Account	Replacement URI	Port	Transport	Reg Exp	
<input type="text" value="To Site A"/>	<input type="text" value="1"/>	- <input type="button" value="v"/>	<input type="text" value="192.45.20.77"/>	<input type="text" value="5060"/>	<input type="text" value="UDP"/>	<input type="text"/>	<input type="checkbox"/>
<input type="text" value="To Site B"/>	<input type="text" value="1"/>	- <input type="button" value="v"/>	<input type="text" value="192.45.60.10"/>	<input type="text" value="5060"/>	<input type="text" value="UDP"/>	<input type="text"/>	<input type="checkbox"/>

groups with rows per group.

Dial Plan (Help)						
No.	From Header	Request-URI	Action	Forward To	Add Prefix	
					Forward	
<input type="text" value="1"/>	<input type="text" value="Any"/>	<input type="text" value="To Site A"/>	<input type="text" value="Forward"/>	<input type="text" value="To Site A"/>	<input type="text"/>	<input type="text"/>
<input type="text" value="2"/>	<input type="text" value="Any"/>	<input type="text" value="To Site B_37"/>	<input type="text" value="Forward"/>	<input type="text" value="To Site B"/>	<input type="text"/>	<input type="text"/>
<input type="text" value="3"/>	<input type="text" value="Any"/>	<input type="text" value="To Site B_38"/>	<input type="text" value="Forward"/>	<input type="text" value="To Site B"/>	<input type="text"/>	<input type="text"/>

rows.

4.8. Apply Configuration

Select **Administration** from the main menu, followed by **Save/Load Configuration** to display the screen below. Click on **Apply configuration** to proceed with saving and loading the configuration.

The screenshot shows the 'inGate SIParator' web interface. At the top left is the logo, and at the top right is a 'Log out' button. Below the logo, it says '1 other administrator(s) currently logged in.' A horizontal menu contains buttons for 'Basic Configuration', 'Administration' (highlighted in red), 'Network', 'Logging', 'SIP Services', 'SIP Traffic', 'Failover', 'Virtual Private Networks', 'Quality of Service', and 'About'. Below this is a second row of buttons: 'Save/Load Configuration' (highlighted in red), 'Show Configuration', 'User Administration', 'Upgrade', 'Table Look', 'Date and Time', 'Restart', and 'Change Language'. The main content area is divided into two sections. The left section, titled 'Test Run and Apply Conf' with a '(Help)' link, contains the text 'Duration of limited test mode:', a text input field with '30' and the label 'seconds', and an 'Apply configuration' button. The right section, titled 'Show Message About Unapplied Changes', contains three radio button options: 'On every page' (selected), 'On the Save/Load Configuration page', and 'Never'.

inGate SIParator [Log out](#)

1 other administrator(s) currently logged in.

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

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

Test Run and Apply Conf [\(Help\)](#)

Duration of limited test mode:

seconds

Show Message About Unapplied Changes

- ☒ On every page
- ☐ On the Save/Load Configuration page
- ☐ Never

5. Interoperability Compliance Testing

The interoperability compliance test included SIP feature and serviceability testing.

The feature testing included basic call, hold, transfers, conference, call forwarding, bridging, quality of service, and VoIP survival. The basic call scenarios utilized various audio codecs, such as G.711 and G.729, with and without IP media shuffling.

The serviceability testing included disconnecting the SIParator Ethernet cables.

5.1. General Test Approach

All tests were performed manually. The focus is on verifying that basic SIP features continue to work across sites via the SIParator.

For quality of service tests, different priority levels were configured for SIP signaling versus RTP media packets on the SIParator, and a network analyzer was utilized to verify the proper setting of the priority level for SIP messages in each direction.

The serviceability testing focused on verifying the ability of SIParator to recover from loss of network connectivity.

5.2. Test Results

All test cases were executed and passed.

6. Verification Steps

This section provides the tests that can be performed to verify proper SIP configuration between Avaya SIP Enablement Services and the Ingate SIParator.

6.1. Verify Avaya SIP Enablement Services at Site A

From the Linux shell of Avaya SES at Site A, use the “trustedhost -L” command to verify the private network IP address of the SIParator is listed as a trusted host.

```
craft@SES-DevCon1> trustedhost -L
```

Third party trusted hosts.		
Trusted Host	CCS Host Name	Comment
-----	-----	-----
192.45.20.78	192.45.20.77	

6.2. Verify Avaya SIP Enablement Services at Site B

From the Linux shell of Avaya SES at Site B, use the “trustedhost -L” command to verify the public network IP address of the SIParator is listed as a trusted host.

```
craft@SES-DevCon60> trustedhost -L
```

Third party trusted hosts.		
Trusted Host	CCS Host Name	Comment
-----	-----	-----
192.45.21.5	192.45.60.10	

6.3. Verify Ingate SIParator

Establish a SIP call between Site A and Site B, and verify the status of the connection by selecting **SIP Traffic** from the main menu followed by **SIP Status**. Verify the **State** is “Established”, as shown below. Also manually verify that there is connected audio path between the two endpoints.

The screenshot shows the Ingate SIParator web interface. At the top, the logo "inGate SIParator" is displayed next to a "Log out" button. Below the logo, it states "1 other administrator(s) currently logged in." A main menu bar contains buttons for Basic Configuration, Administration, Network, Logging, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, and About. A secondary menu bar below SIP Services includes SIP Methods, Filtering, User Database, Authentication and Accounting, Dial Plan, Routing, and SIP Status (highlighted). The main content area is titled "Active Sessions (1 sessions)" and contains a table with the following data:

Start	Caller	Callee	State	Call-ID / Media
16:36:06	<sip:78001@devconnect.com:5061>	<sip:38001@devconnect.com>	Established	0dcb889248db1561
		(192.45.20.55:34008) → 192.45.60.131:34008	UDP Audio	
		(192.45.60.131:34008) → 192.45.20.55:34008	UDP Audio	

Below the table, the "Monitored SIP Servers" section states "There are no monitored SIP servers." The "Registered Users (0 users)" section states "There are no registered users." At the bottom, the Ingate logo is shown next to the text: "Page generated for 'admin' 2006-06-29 16:36:09 +0000. Ingate SIParator 4.4.1. Copyright © 2006 Ingate Systems AB."

7. Support

Technical support on the Ingate SIParator can be obtained through the following:

- **Email:** ussupport@ingate.com

8. Conclusion

These Application Notes describe the configuration steps required for the Ingate SIParator 4.4.1 to successfully interoperate with an Avaya SIP Telephony environment consisting of Avaya Communication Manager 3.1.1, Avaya SIP Enablement Services 3.1, and Avaya 4600 Series SIP and H.323 Telephones.

9. Additional References

This section references the product documentation relevant to these Application Notes.

- *Administrator Guide for Avaya Communication Manager*, Document 03-300509, Issue 2, February 2006, available at <http://support.avaya.com>.
- *Installing and Administering SIP Enablement Services R3.1*, Document ID 03-600768, Issue 1.4, February 2006, available at <http://support.avaya.com>.
- *SIP Support in Release 3.1 of Avaya Communication Manager Running on the S8300, S8400, S8500 series, and S8700 series Media Server*, Document 555-245-206, Issue 6, February 2006, available at <http://support.avaya.com>.
- *Ingate SIParator 4.4 Getting Started Guide*, available from the SIParator 4.4 installation CD.
- *Ingate SIParator 4.4 User Manual*, available from the SIParator 4.4 installation CD.

©2006 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.