How to Install an Ingate E-SBC in Stand-alone Firewall mode or DMZ / LAN mode for an Aastra Teleworker Solution.

March, 2013

Table of Content

Versions: Ingate Firewall/SIParator version 5.0.1

Revision History:

Revision	Date	Author	Comments
1.3	2013-02-14	Ingate Systems	
1.4	2013-02-27	Ingate Systems	
1.5	2013-03-20	Ingate Systems	

Introduction

This document describes how to install a Teleworker solution using an Ingate E-SBC solution for A700 and MX-ONE.
The installation supports usage of BluStar, AMC, SIP DECT and SIP Phones.

The chapter references in this document are referring to the document "Startup Tool - Getting Started Guide" found at the PDF link below. The Startup Tool Guide also has information about the two supported topologies Firewall mode (section 4.4.1) and DMZ/LAN mode (section 4.4.4).
https://www.ingate.com/appnotes/Ingate_Startup_Tool_Getting_Started_Guide.pdf

Required info	**(Your Notes)**
Ingate E-SBC unit	
IP addresses and net masks	
Default gateway	
DNS servers	
MAC address (printed on the Ingate unit)	
PBX IP-address and port numbers to use for XML and SIP configuration	
12 digit license key from Ingate Systems	
Startup Tool – Getting Started Guide	
PC with internet connection	
IMPORTANT: Authentication on the PBX must be setup with strong passwords before starting the Ingate installation. It is strongly recommended that passwords with a minimum length of 10 characters are used, mixed with numbers and uppercase and lowercase letters and special characters.	
If DMZ/LAN mode will be used, port forwarding for XML, SIP signaling and media port must be setup on the existing firewall before starting the installation (see chapter 4.4.4 section 7 in the PDF link above for more information)	

10 step installation guide

1) Preparations

If you have not already done so:

A) Download and install the Ingate Startup Tool TG to your PC from the following link: http://www.ingate.com/Startup_Tool_TG.php (Note that your antivirus program might block the program, if needed please change your settings to allow the Startup tool TG) (See chapter 2 for more details).
B) If the Ingate Software Firewall/SIParator® solution will be used instead of an Ingate hardware unit, please see separate installation guide for installation instructions.

2) Start the configuration

Do the following:

A) Connect an Ethernet cable to the port "Eth0" on the Ingate hardware unit and turn on the power switch.
B) Start the Startup Tool TG on your PC and choose "Ingate Firewall/SIParator", then click "Next". If you receive an error message saying: "The application has failed to start because its side-by-side configuration is incorrect" you need to download and install Microsoft visual c++Redistributable (vcredist_x86.EXE) from the following link: http://www.microsoft.com/download/en/details.aspx?id=26347
C) Select "Configure the unit for the first time", and make sure that NONE of the other options are selected. If SIP trunking is desired, please contact your local Aastra dealer or contact Ingate Systems directly. (See chapter 4.1 for more details).
D) In the "Inside (Interface Eth0)" field enter the Internal LAN IP address to be assigned to the Ingate. This is the IP-address that the Ingate will use to talk to the PBX on the LAN. (See Chapter 4.1 for more details) (Ensure that your PC and the Ingate unit (Eth0) have different IP-addresses but are in the same LAN segment/subnet). (See Chapter 3. For more details).
E) Enter the MAC address of the Ingate unit. The MAC address can be found on a sticker attached to the Ingate unit.
F) In the field "Select a Password", enter the password, at your choice to be assigned to the Ingate unit. Please observe that the unit might be opened for external administration in which case it is critical to choose a strong password (see chapter 4.1 for more details).
G) In the field "Interface on your PC" choose the interface on your PC connected to your LAN where the Ingate (Eth0) is located.
H) Press the now active "Contact" button to have the Startup Tool TG find the Ingate unit on the network. (See Chapter 4.1 for more details)

3) Activate your licenses

Go to the "Licenses and Upgrades" tab and do the following (note that this step will not be available if the licenses have already been installed on the Ingate):

A) In the "Your Ingate Web Account" field enter your user name and password that you have created at www.ingate.com, if you have not already created a login, simply click on the "Create" button and create a new account (see Chapter 4.3.1 for more details).
B) In the "Connect and Register this unit with the Ingate Web" press "Connect" (see chapter 4.3.2 for more details).
C) In the "Fetch and Install purchased modules/licenses" field, enter the 12 digit license key in the purchase code area and press install. The license key opens up the Ingate licenses required (see chapter 4.3.3 for more details).

4) Setup your Network interfaces

Go to "Network Topology" tab and do the following:

A) At "Product Type", select "Firewall".
B) Enter the IP address and net mask of the inside LAN (interface Eth0). (See chapter 4.4.1 for more details)
C) Enter the outside WAN (Interface Eth1) IP address and net mask based on instructions from your ISP (Internet service provider) (see chapter 4.4.1 for more details).
D) Enter the default gateway for the Ingate SIParator based on instructions from your ISP, note this field will only be available if you have not chosen "Use DHCP to obtain IP" under outside WAN (interface eth1) (see chapter 4.4.1 for more details).
E) Enter the DNS servers for the Ingate Firewall based on instructions from your ISP (see chapter 4.4.1 for more details).

5) Upload your configuration

Go to "Upload Configuration" tab and do the following:

A) Verify that the option "Logon to web GUI and apply settings" is selected.
B) Press the "Upload" button.
C) Press "OK" if you get a message that the Ingate will change operational mode.
D) Press "OK" when you get a confirmation that the configuration has been updated (see chapter 4.7 for more details).

6) Configuration

In a new Internet browser window login with the username: admin and the password that you set in step 2 of this guide (note that if the browser does not automatically start, you can start your Internet browser manually and access the Ingate using the IP-address that you set on Eth0 in step 4 of this guide).

A) Click on "Basic configuration" and click on the "Certificates" tab, add a new row under "Private Certificates" and give the certificate a suitable name in the name field.
B) Click on the "Create new button" and in the "Common Name (CN)" field enter the public IP-address of the Ingate, enter your domain name instead if you have a domain that you want to use instead of the public IP-address.

Note that you have 2 options how you can sign and use the certificate, you can either create a self-signed certificate on the Ingate or you can create a CSR (Certificate Signing Request) on the Ingate and use an external CA (Certificate Authority) to sign the certificate request, using an external CA is the recommended way and Aastra have a list of CA's that are supported, please see the Aastra documentation for the list of supported CA's. Use alternative 1 or alternative 2 below based on how you will sign the certificate:

Alternative 1: Create Certificate Signing Request on the Ingate and sign the request by external CA:

- Make sure that you have entered correct info in the Common Name (CN) field in previous step.
- Press the "Create an X.509 certificate request" button and when the request has been created press the save button.
- Press the "View/Download" button for the new certificate request.
- Press the "Download certificate/certificate request (PEM format)" and save it locally on your computer, this is the request CSR that you will send to an external CA (Certificate Authority) for signing, please see the Aastra documentation for a list of supported CA's that you can use for signing.
- When you have got the signed certificate back from the CA, you can press the "Import" button for the Ingate signing request that you created and under the section "Import Signed Certificate" press the "Chose File" button and import the certificate that you got from your CA and finally press the save button.

Alternative 2: Create an Ingate Self signed certificate:

- Make sure that you have entered correct info in the Common Name (CN) field in previous step.
- Press the "Create a self-signed X.509 certificate" button and when the certificate has been created press the save button.
- Press the "View/Download" button for the new certificate.
- Press the "Download certificate/certificate request (PEM format)" button and save it locally on your computer. Note, the downloaded certificate has to be installed as a trusted Root CA certificate, either manually on your phones, or by installing the certificate on an Aastra configuration server, please see the Aastra documentation for more information about installing certificates on the phones.

C) In the Ingate web-GUI click on the "Rules and Relays" tab followed by another click on the "Relays tab".
D) Click on the "Add new rows" button and in the "IP-Address drop down list" choose your external IP-address that you configured on interface eth1 in step 4 of this guide.
E) In the port field, enter port number 22222.
F) Under the section "Relay to…" and in the field "DNS Name or IP Address" enter the IP-address of your IP-PBX on your LAN.
G) "Under the section "Relay to…" and in the field "Port" enter port number 22222, enter another port number if your IP-PBX is configured to use another port number. (Port 22222 and 22223 are Aastra specific and is used for XML configurations of the Aastra phones.)
H) Under "Relay Type" chose "Semi-transparent TCP port forwarding"
I) Under "Allow access from…" choose WAN.
J) Under "Time Class" chose 24/7 and press the "Save" button.
K) Click on the "Add new rows" button again and in the "IP-address drop down list" chose your external IP-address that you configured on interface eth1 in step 4 of this guide.
L) In the port field enter port number 22223.
M) Under section "Relay to…" and in the field "DNS Name or IP Address" enter the IP-address of your IP-PBX on your LAN.
N) Under the section "Relay to…" and in the field "Port" enter port number 22222, enter another port number if your IP-PBX is configured to use another port number.
O) Under "Relay Type" chose "TLS/SSL decryption"
P) Under "Allow access from…" choose WAN.
Q) Under "Certificate for TLS/SSL" chose the certificate that you created earlier.
R) Under "Time Class" chose 24/7 and press "Save".
S) Note that if you have an Aastra configuration server on your LAN side that you want to be available also for your remote users, you can add another "Relay" as specified in this step, if you don't want the configuration server to be available from the WAN side just skip this step and move on to the next step. Click on the "Add new rows" button and chose your external IP-address under "IP Address", set port to 444, under "Relay To" and in "DNS Name or IP Address" enter the IP-address of the configuration server on the LAN, set port to 444 or any other port that you have configured on the configuration server, set "Relay Type" to "TLS/SSL decryption", set "Network" to WAN, under "Certificate for TLS/SSL" chose the certificate that your created earlier, set "Time Class" to 24/7 and press save.
T) Click on the "SIP Services" tab followed by the "Remote SIP Connectivity" tab and enable the "Enable Remote NAT Traversal" option, change the value in the field "NAT timeout for TCP" from 150 to 40 and press "Save".
U) If you will configure the Ingate in DMZ/LAN mode behind your existing firewall then go to the tab "Basic configuration" then click on the tab "SIParator Type" and select "Enable SIParator" and choose "DMZ/LAN" in the drop down list and press "Save". Click on the SIP Services tab and then click on the Basic tab, in the field "Public IP Address for NATed firewall" enter the public IP-address that you have on you existing firewall

and finally press save. Note that if you are using the DMZ/LAN mode, you also need to setup port forwarding on your existing firewall to the Ingate for XML ports, SIP signalling and media ports (see chapter 4.4.4 in the Ingate StartUp Tool guide, section 7 for details).

7) TLS and SRTP encryption

This step will configure the Ingate to encrypt SIP signalling using TLS and encrypt media using SRTP, if you do not require encryption, move on to next step.

A) Click on the "SIP services" tab followed by "Signalling encryption" and choose "Any" under SIP transport.
B) Set "Check Server Domain Match" to "Yes".
C) Add a new row under "TLS Connections On Different IP Addresses" and choose your external IP-address in the "IP address" field, set the "Own Certificate" field to the certificate that you created in the previous steps. Set "Use CN FQDN" to NO and set "Require Client Cert" to NO, finally set "Accept Methods" to "Any".
D) In the "Making TLS Connections" section choose the certificate that you created in the previous steps and set "Use methods:" to "SSLv3 or TLSv1 (v2 hello)" in the drop down list and finally press "Save".
E) Click on the "Media encryption" tab and choose "Enable media encryption".
F) Add a new row under "SIP Media Encryption Policy" and set "Media Via Interface/VLAN" field to "Inside (eth0 untagged)", set "Suite Requirements" to "Clear text" and set "Allow transcoding" to "Yes".
G) Add another row under "SIP Media Encryption Policy" and set "Media Via Interface/VLAN" field to "Outside (eth1 untagged)", set "Suite Requirements" to "Any (transcodable)" and set "Allow transcoding" to "Yes". (Note! if you only want to allow encrypted SRTP media on the Wan side you can choose SRTP in the "Suite Requirements" instead).
H) Set "Default Encryption Policy" to "Encrypted (transcodable)", set "Allow transcoding" to "Yes".
I) Enable the option "Require TLS for all cryptos but clear text" under the "Require TLS" section.
J) Set "RTP Profile" to "Prefer RTP/SAVP (sdescriptions)" and press "Save".
K) Click on the "Interoperability" tab and add a new row under "Remove via Headers" and enter the IP-address of your PBX in the "DNS Name or IP address" field.
L) Go further down on the Interoperability page and Set "URI Encoding" to "Use Registration".
M) Enable "Match only on username" under "User Matching" and press save at the bottom of the page.

8) Setup Dial plan

A) Click on the "Network" tab and under "Networks and Computers" add a new row and in the name field set the name to "AastraPBX", under the section "Lower Limit" and in the field "DNS Name or IP Address" enter the

IP-address of the Aastra PBX on your LAN, under "Interface/VLAN" chose inside (eth0 untagged) and press save.

B) Click on the "Rules and Relays" tab followed by the "Rules" tab and in the "Client" field chose "AastraPBX" instead of the LAN definition in the drop down list and press the save button.

C) Click on the "SIP traffic" tab followed by the "Dialplan" tab and set "Use Dial Plan" to ON.

D) Add a new row under "Matching From Header" and enter "RemoteUsers" in the name field, enter the asterisk * character in the UserName field to match any username, enter the IP-address of your Aastra PBX in the "Domain Field". (Note that it is possible to use the "Regr Expr" field instead of the username and domain fields to enter Regular Expressions for flexible matching on users and domains, please see the links at the end of this document for more information about this). Set the "Transport" field to "Any". (Note that if you only want to allow TLS signalling on the WAN side you can enter only TLS in the Transport field instead). Set "Network field to WAN".

E) Add another row under "Matching From Header" and enter "WAN" in the "Name" field, enter the asterisk * character in the "UserName" field, enter the asterisk * character in the "Domain" field, set "Tranport" to Any and set "Network" to WAN and press save at the bottom of the page.

F) Add a new row under "Matching Request-URI" and enter InboundInvite in the "Name" field, set the "Tail" field to '-', enter sips?:(.*)@192.168.140.54 in the "Regr Expr" field and replace the IP-address (192.168.140.54) shown in the example here with the IP-address that you have set on your own Aastra PBX. (Note if possible to avoid typos we recommend you to copy the text from this document to a text editor like Notepad and do the editing there and finally copy the text again from Notepad in to the "Regr Expr" field of the Ingate.)

G) Add a new row under "Matching Request-URI" and enter InboundRegister in the "Name" field, set the "Tail" field to '-', enter sips?:(@?)192.168.140.54 in the "Regr Expr" field and replace the IP-address 192.168.140.54 with your on IP-adress set on your Aastra PBX and press save at the bottom of the page.

H) Add a new row under the "Forward To" and enter the name FwdRegisterToPBX in the "Name" field, enter the following in the "Regr Expr" field sip:$1192.168.140.54;transport=tcp?To=%3csip%3a$(to.user)%40192.168.140.54%3e and replace the IP-address 192.168.140.54 with the IP-address that you have set on your Aastra PBX. (It's important to enter the text exactly so use copy and paste if possible to avoid typos).

I) Add a new row under "Forward To" and enter FwdInviteToPBX in the name Field, enter sip:$1@192.168.140.54;transport=tcp in the "Regr Expr" field and replace the IP-address 192.168.140.54 with our own IP-address of the Aastra PBX.

J) Add a new row under the "Dial Plan" section and set "From Header" to "RemoteUsers", set "Request-URI" to "InboundRegister", set "Action" to "Forward", set "Forward To" to "FwdRegisterToPBX".

K) Add a new row under the "Dial Plan" section and set "From Header" to "RemoteUsers", set "Request-URI" to "InboundInvite", set "Action" to "Forward", set "Forward To" to "FwdInviteToPBX".
L) Add a new row under the "Dial Plan" section and set "From Header" to WAN, set "Action" to "Reject" and press save at the bottom of the page.
M) Under the section "Methods in Dial Plan" add a new row and enter REGISTER in the "Method" field and press the save button.

9) Enable IDS/IPS

A) Click on the SIP Traffic tab followed by the IDS/IPS tab and click on the Add new rows button and enter a suitable name in the name field, set active to yes, set client field to WAN, set Request-URI to the asterisk * character to match all requests, set SIP Method to REGISTER, set Window(s) to 10, set Hits to 10, set Blacklisting(s) to 300 and press the save button.
B) Add a new row again and enter a suitable name in the name field, set client field to WAN, set Request-URI to the asterisk * character to match all requests, set SIP Method to INVITE, set Window(s) to 10, set Hits to 10, and set Blacklisting to 300 and press the save button.
C) Check under the section "Packet Filtering IDS/IPS Rules from Ingate Systems" and it should be at least 5 rules listed there. If you don't have any rules listed you can download rule packs from https://www.ingate.com/idsips/ and then install them under Administration -> Upgrade tab.

   Note that the new rows added here will blacklist any IP-address sending 10 or more REGISTER or INVITE methods within 10 seconds and the IP-address will be blacklisted for 300 seconds The values added here are only guidelines and you might need to adjust the values to according to your needs. It is possible to see any blacklisting's under the IDS/IPS Status tab. There is more information about how to configure the IDS/IPS in the firewall reference guide available at www.ingate.com

10) Finalize the configuration

Note that if all your remote users are using static IP-addresses, it is possible to lock down the Ingate unit further by only allowing SIP signalling from specific IP-addresses or networks, and deny all other SIP traffic. This can be done by creating a network group under Network -> Networks and Computers and then use "SIP Signaling Access Control" or "Sender IP Filter Rules", please see the Ingate firewall reference guide chapter 8 and 9 for more information about this, the reference guide is available for download at www.ingate.com.

Finally click on the "Administration" tab and press the "Apply Configuration" button to apply the changes to the Ingate unit. Press "Save configuration" to complete the saving process (see chapter 4.7 for more details).

Useful links:

Regular Expressions and header manipulation:

http://www.ingate.com/appnotes/How_To_use_Regular_Expressions_in_the_Dial_Plan.pdf

http://www.ingate.com/appnotes/How_To_use_Generic_Header_Manipulation.pdf