TLS For SIP Signaling Encryption

Lisa Hallingström

Paul Donald

Bogdan Musat

Adnan Khalid

Per Johnsson

Rickard Nilsson

Table of Contents

Ingate Firewall/SIParator® version: 4.6.2 - 4.7.1

Document version: 1.1

How To Configure TLS in Ingate Firewall/SIParator®

Prerequisites:

- You have access to a CA that will sign your certificate requests
- You have each signing-CAs public certificate
- You understand the GNU X.509 trust model

This is how to configure your Firewall/SIParator to encrypt SIP media or force the SIP clients to use signaling encryption with TLS.

The settings for SIP signaling encryption are made on the **Signaling Encryption** page under **SIP Services**. You also need a certificate, which is created on the **Certificates** page under **Basic Configuration**.

This feature is *only available* when the *Enhanced Security* or the *SIP Trunking* module has been installed.

Certificates

Create certificates on the **Certificates** page.

Add a new row to the **Private Certificates** table and enter a name for this certificate. Press **Create new** and enter the certificate information.

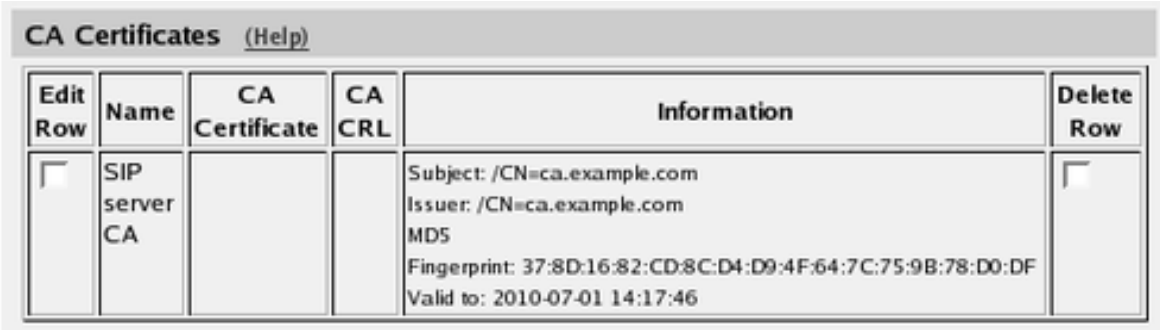
If you want to make TLS connections on the LAN and the Internet, you will need one certificate for each interface. Note: set the certificates CN= field to the IP/DNS name of the interface.

Private Certificates (Help)

Edit Row	Name	Certificate			Information	Delete Row
☐	Inside				Subject: /CN=10.47.3.243 Issuer: /CN=10.47.3.243 MD5 Fingerprint: 96:3F:8A:4A:90:A4:7C:C4:4D:E2:E9:03:51:AD:FA:37 Valid to: 2010-07-21 14:24:58	☐
☐	main cert				Subject: /CN=sip.ingate.com Issuer: /CN=sip.ingate.com MD5 Fingerprint: 5E:5A:C8:DC:A0:DC:42:FE:C0:BB:FA:B5:5C:60:5E:D0 Valid to: 2010-07-01 14:25:20	☐

If the Firewall/SIParator should use TLS to connect to another SIP server, you must upload the CA certificate for that server here. You don't need CA certificates for SIP clients.

Create a new row in the **CA Certificates** table and upload the CA certificate.



Signaling Encryption

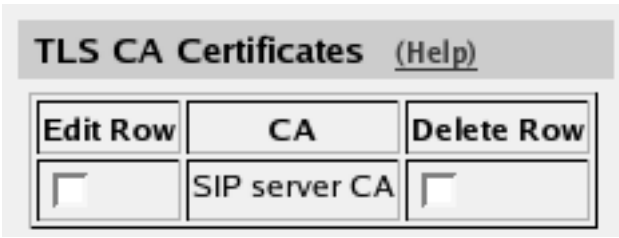
Go to the **Signaling Encryption** page to make TLS settings.

First, select the allowed SIP transports. If you want to allow signaling via TCP or UDP e.g. on the "inside", select "Any".

To initiate TLS signaling, set transport to TLS in the Dial-Plan or DNS override table if the DNS record for a domain has no TLS entry.

If "TLS" is selected, no connections via UDP or TCP will be initiated or accepted, on **any** interface. In this case, you must make sure that all clients and servers that the Firewall/SIParator should communicate with can be reached via TLS.

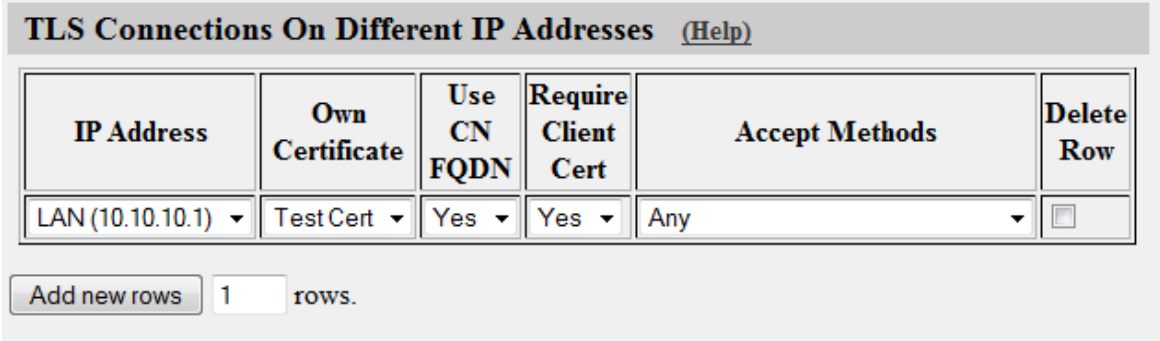
If the Firewall/SIParator should communicate with other SIP servers, you have already imported their CA certificates. In the **TLS CA Certificates** table, you select these certificates to allow them to be used in TLS connections.



In the **TLS Connections On Different IP Addresses** table, create one row for the inside and one for the outside IP address. For each IP address, select which certificate should be used for authentication when a TLS connection is made to that IP address, and if the Firewall/SIParator should require the client to send its own certificate for authentication, too.

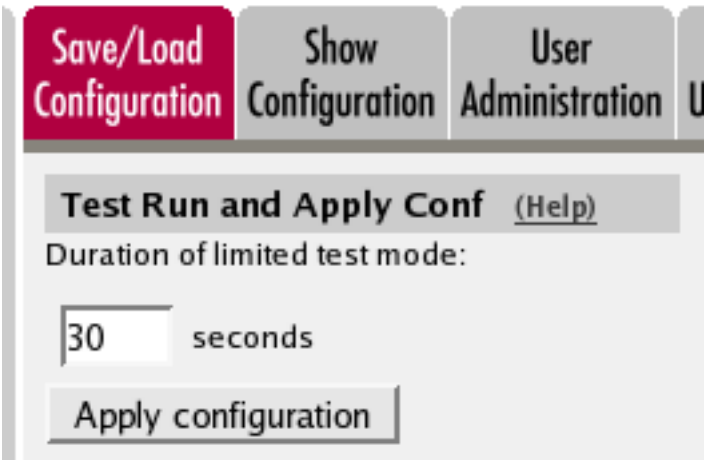
You also select which TLS methods should be accepted for each IP address.

Note that the Firewall/SIParator will not accept TLS connections to an IP address which is not listed in this table!

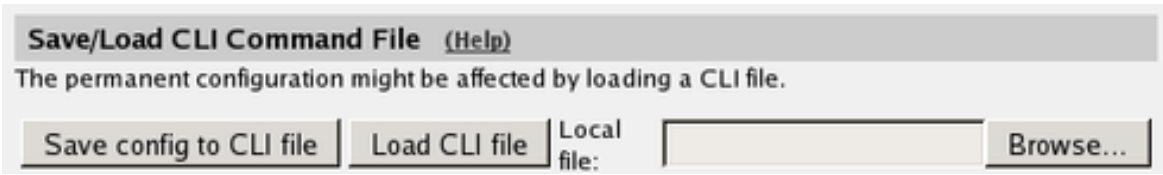


Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



Settings in the Other Server

You need to upload the Firewall/SIParator certificate to the other SIP server if the Firewall/SIParator should be able to make connections to the server.