

Setting Up SIP Media Encryption



Lisa Hallingström

Paul Donald

Bogdan Musat

Adnan Khalid

Per Johnsson

Rickard Nilsson

Table of Contents

How To Use SIP Media Encryption with Ingate Firewall/SIParator®.....	3
--	---

How To Use SIP Media Encryption with Ingate Firewall/SIParator®

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

The settings for SIP media encryption are made on the **Media Encryption** page under **SIP Services**.

First, switch the media encryption on.

The screenshot shows the configuration interface for SIP Media Encryption. The 'Media Encryption' tab is active. Below the tab, there are two radio button options: 'Enable media encryption' (which is selected) and 'Disable media encryption'.

Group the encryption algorithms that you want to use. There are predefined crypto suite groups, but you might need to define your own if you have special requirements.

Crypto Suite Groups (Help)			
Edit Row	Name	Suite	Delete Row
<input type="checkbox"/>	+ All transcodable	Cleartext (no encryption)	<input type="checkbox"/>
<input type="checkbox"/>		SRTP sdesc. (AES-CM 128, SHA1 32)	<input type="checkbox"/>
<input type="checkbox"/>		SRTP sdesc. (AES-CM 128, SHA1 80)	<input type="checkbox"/>
<input type="checkbox"/>	+ Cleartext	Cleartext (no encryption)	<input type="checkbox"/>
<input type="checkbox"/>	+ SRTP encryption	SRTP sdesc. (AES-CM 128, SHA1 32)	<input type="checkbox"/>
<input type="checkbox"/>		SRTP sdesc. (AES-CM 128, SHA1 80)	<input type="checkbox"/>

Select for each interface or VLAN if media going in or out from that interface/VLAN should be encrypted, and which encryption algorithms to allow.

If the Firewall/SIParator should terminate encrypted media streams coming in to one interface (and send it out unencrypted or encrypted with a different algorithm), you must allow transcoding for that interface.

SIP Media Encryption Policy (Help)				
Edit Row	Media Via Interface/VLAN	Suite Requirements	Allow Transcoding	Delete Row
<input type="checkbox"/>	Internal (eth0 untagged)	-	No	<input type="checkbox"/>
<input type="checkbox"/>	External (eth1 untagged)	SRTP encryption	Yes	<input type="checkbox"/>

For interfaces (VLANs) not explicitly configured above, you need to select a default media encryption.

Default Encryption Policy [\(Help\)](#)

Suite requirements: Allow transcoding:

Yes No

When SIP media encryption is used, the SIP signaling should also be encrypted (using TLS). If it isn't, the encryption keys will be sent unencrypted over the network.

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

Save/Load Configuration
Show Configuration
User Administration
U

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

Duration of limited test mode:

seconds