

Enabling Security Features in Dgw

All Mediatrix Units

DGW 49.2.2941

2023-08-09

Table of Contents

Enable Security Features in DGW	4
TLS-Enabled Server/Proxy Installation with openSIPS	5
Certificates	6
Basics of Security Exchanges	8
Enabling Security Features	10
Importing Certificates on the Mediatrix Unit	10
Adding the OpenSIPS Gateway	10
Assigning a Specific Registrar Server to the OpenSIPS Gateway	11
Assigning a Specific Proxy Server to the OpenSIPS Gateway	11
Enabling Secure Signaling (TLS)	12
Enabling Secure Media (SRTP) on All Endpoints	13
Enabling Secure Media (SRTP) on a Specific Endpoint	14
Troubleshooting	16
Enabling TLS Debugging on Wireshark	16
REGISTER Messages Not Being Answered	17
Server Internal Error (or Similar Messages)	17
Mikey and SDES Mismatch	18
Audio Issues with Secured Media (SRTP)	19
Annexes	21

Table of Contents

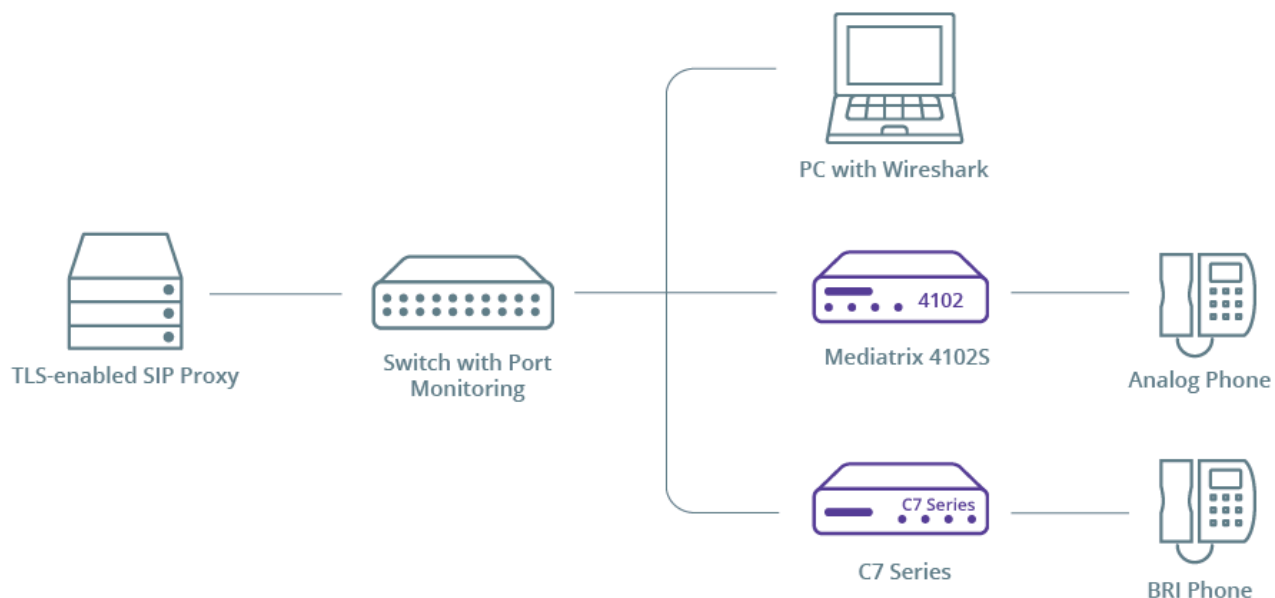
Online Help	22
DGW Documentation	23
Copyright Notice	24

Enable Security Features in DGW

This document describes the steps required to configure a Mediatrix unit loaded with the DGW firmware for secure SIP signalling and secure media (SRTP) operation.

This is not a complete key-exchange, TLS or general security tutorial. For more information on these topics, please see the links section.

In this scenario, the endpoints used are a Mediatrix 4102 and a Mediatrix C740 BRI Gateway units. Both Mediatrix units must be loaded with DGW. We will use the freely available openSIPS (<http://www.opensips.org>) as the SIP proxy and configure it for TLS operation.



TLS-Enabled Server/Proxy Installation with openSIPS

Using two Mediatrix gateways connected back-to-back using a SIP trunk would be sufficient to demonstrate the use of the new security features. However, we prefer to demonstrate the configuration of the units and test scenarios in a more real-world environment by using a separate TLS-enabled SIP proxy. For this purpose, we have chosen openSIPS as it is free and easy to configure for basic use.

For more information on setting up openSIPS, please refer to the openSIPS installation documentation at <http://www.opensips.org/docs>

Note: If already completed, skip this section.

Please note that at the moment of writing this, openSIPS is configured by default to keep the TLS links up for a period of 2 minutes. We have made a small code modification that allows the links to stay up for 120 minutes. See the annex for more information on how to procede.

Certificates

The Mediatrix unit uses digital certificates, which are a collection of data used to verify the identity of individuals, computers, and other entities on a network.

Certificates contain:

- the certificate's name
- the issuer and issued to names
- the validity period (the certificate is not valid before or after this period)
- the use of certificates such as:
 - **TlsClient:** The certificate identifies a TLS client. A host authenticated by this kind of certificate can act as a client in a SIP over TLS connection when mutual authentication is required by the server.
 - **TlsServer:** The certificate identifies a TLS server. A host authenticated by this kind of certificate can serve files or web pages using the HTTPS protocol or can act as a server in a SIP over TLS connection.
- whether or not the certificate is owned by a Certification Authority (CA)

Although certificates are factory-installed new ones can also be added. Since TLS certificates are validated in terms of time (certificate validation/expiration date, etc.), the use of NTP (Network Time Protocol) is mandatory when using the security features.

The Mediatrix unit uses two types of certificates:

- **Host Certificates:** used to certify the unit (e.g.: a web server with HTTPS requires a host certificate).
- **Others:** Any other certificate including trusted CA certificates used to certify peers (e.g.: a SIP server with TLS).

The Conf, Cwmp, Eth, Fpu, Nlm, Sbc, and SipEp services are considered secure as they require certificate validation to establish a secure connection to a remote host. The following parameters, available by the CLI, are used to determine whether or not the connection to the remote host should be validated with the service certificate. By default, the parameters are always set to a value requiring validation.

- `Conf.ScriptsTransferCertificateValidation`
- `Cwmp.TransportCertificateValidation`
- `Eth.Eap.CertificateValidation`
- `Fpu.MfpTransferCertificateValidation`
- `Nlm.PCcaptureTransferCertificateValidation`
- `Sbc.CertificateValidation`
- `SipEp.InteropTlsCertificateValidation` (also available in the DGW Web page under SIP/Interop)

The certificates must be uploaded to the Mediatrix units. They define how a Mediatrix unit will certify the remote host in order to mark it as secure and suitable for a TLS connection. If the Mediatrix unit does not trust the remote certificate (i.e. does not authenticate it with either one of the 3 methods: HostName, trustedCertificate, DnsSrv), then the Mediatrix unit will not establish the connection.

By default it is not possible to upload a Host certificate without first clicking on Activate unsecure certificate transfer. This is because the certificate upload will be done in clear text, which means the private key will be susceptible to interception. Establishing a connection without certificate validation, i.e. establishing an unsecure connection, should only be used :

- for testing purpose,
- if one cannot identify the required CA cert, or
- the CA cert has mismatched Common Name/Subject Alternate Name. (In this case there is no fallback, it will fail if the name does not match)

Certificates are used to secure the following connections:

- SIP
- Configuration Web pages
- File transfers (scripts, firmwares, etc.) with HTTPS
- Configuration using TR-069
- Wired Ethernet Authentication with EAP (802.1x)

One common use of the host certificate is to allow HTTPS Web access to the unit (which in this case, the device is the TLS server). For more details refer to the [Technical Bulletins - Creating a Media5 Host Certificate with Open SSL](#) document on the [Media5 Documentation Portal](#).

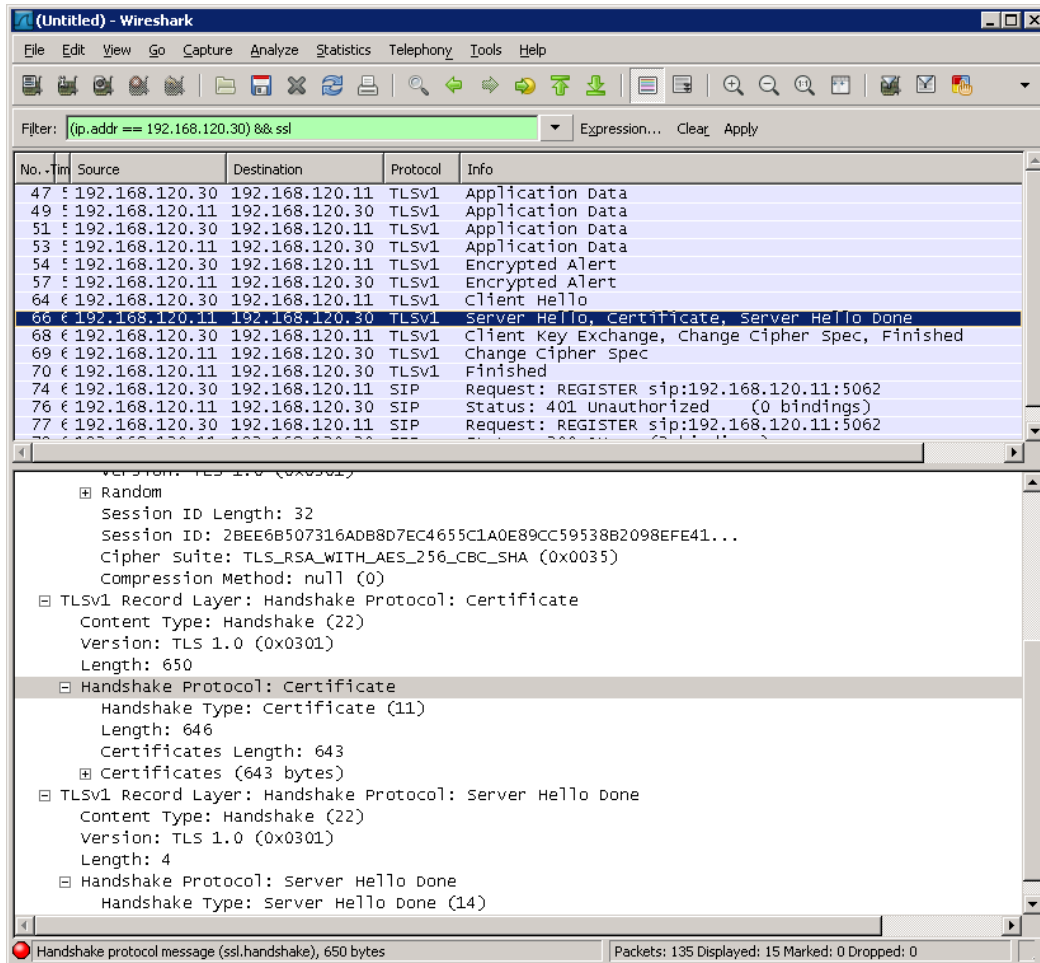
Basics of Security Exchanges

At the level at which we are working, establishing a TLS connection may seem fairly straightforward. However in practice, at a lower level, there are a lot of additional complications to consider to insure a protection against various possible attacks.

Here is an example of an overall exchange in order to build a TLS link and bring it "up"

- The client (Mediatix) initially connects to the server on a configured TCP port (16000 is the default source port, the destination port is the configured SIP proxy port).
- The client sends a "Client Hello" message with the supported TLS/SSL protocol version, cipher specifications and compression algorithms.
- The server replies with a "Server Hello" message with the selected cipher and the server certificate.
- The client verifies the server certificate (validations are configured via the `TlsCertificateValidation` variable).
- The client generates a secret and encrypts it with the server's public key. This encrypted secret is then sent to the server.
- The client and the server use the secret to create the same symmetric encryption key.
- The client and the server switch to encrypted communication by using the previously agreed cipher and the key just established

This brief exchange can be seen in the following Wireshark capture.



When obtaining the server certificates during the early negotiation, the following information will be checked by the client:

- the server's signature,
- the CA (Certification Authority) who signed the certificate,
- validate that the server identified in the certificate is the same as the one that presented it,
- the expiration date of the certificate.

If any of these steps fail, the TLS link will not go "up". For those familiar with HTTPS, this is essentially the same procedure but using a SIP server/proxy instead of a HTTPS server.

Enabling Security Features

Importing Certificates on the Mediatrix Unit

Before you start

You must have an SNTP server for time tracking.

Steps

- 1) Go to **Management/Certificates**.
- 2) Click **Activate unsecure certificate transfer**.
- 3) From the **Type** selection list, select **Other**.
- 4) Click **Browse**.

Note: CA certificate files usually have a .crt extension, using format X.509.

- 5) Click **restart required services**.

Result

Mediatrix®

System ■ Network ■ POTS ■ SIP ■ Telephony ■ Call Router ■ Management

Configuration Scripts Backup / Restore Firmware Upgrade Certificates Snmp Access Control

✚ Certificates

Certificate transfer is disabled because of unsecure HTTP access.
 • [Activate unsecure certificate transfer \(not recommended\)](#).

Host Certificates						
File Name	Issued To	Issued By	Valid From	Valid To	Usage	Action

Other Certificates							
File Name	Issued To	Issued By	Valid From	Valid To	Usage	CA	Action
Cert_MxDefault001.der	test	test	2005-07-29 18:06:00	2015-07-27 18:06:00	Yes	Yes	—

Certificate Transfer	
Type	Path
Other	Browse...

Adding the OpenSIPS Gateway

Steps

- 1) Go to **SIP/Gateways**.
- 2) In the **Gateway Configuration** table, in the **Name** field, enter **OpenSIPS**.
- 3) Click **+**.

4) Complete the fields as follows:

- From the **Type** selection list, select **Trunk**.
- From the **Signaling Network** selection list, select **Uplink**.
- In the **Port** field, enter 5062.
- In the **Secure Port** port field, enter 5061.

5) Click **Apply**.

Result

The **OpenSIPS** gateway will be available under the **SIP > Servers** page.

Gateway Configuration							
Name	Type	Signaling Network	Media Networks	Media Networks Suggestion	Port	Secure Port	
OpenSIPS	Trunk	Uplink	Uplink	--- Suggestion ---	5062	5061	-
							+

Assigning a Specific Registrar Server to the OpenSIPS Gateway

Steps

- 1) Go to **SIP/Servers**.
- 2) In the **Registrar Servers** table, from the **Gateway Specific** drop box, select **Yes**.
- 3) In the **Registrar Host** field, enter the server IP address or FQDN.

Note: For gateway-specific settings, use the **Gateway Specific** sections.

4) Click **Submit**

Result

SIP Gateway Specific Registrar Servers		
Gateway Name	Gateway Specific	Registrar Host
OpenSIPS	Yes	192.168.120.11:5061

Assigning a Specific Proxy Server to the OpenSIPS Gateway

Steps

- 1) Go to **SIP/Servers**.
- 2) In the **Proxy Servers** table, from the **Gateway Specific** drop box, select **Yes**.

- 3) In the **Proxy Host** field, enter the server IP address or FQDN.

Note: For gateway-specific settings, use the **Gateway Specific** sections.

- 4) Click **Submit**

Result

SIP Gateway Specific Proxy Servers				
Gateway Name	Gateway Specific	Proxy Host	Outbound Proxy Host	
OpenSIPS	Yes ▾	192.168.120.11:5061	0.0.0.0:0	

Submit

Enabling Secure Signaling (TLS)

Information

.

Steps

- 1) Go to **SIP/Transport** tab.
- 2) In the **Protocol Configuration** table, from the **TLS** dropbox, select **Enable**.

IMPORTANT: The Mediatrix unit does not support a mix of both TLS and non-TLS links. Once TLS is enabled, it is enabled for all configured SIP gateways

- 3) Click **Apply**.
- 4) Follow the link located at the top of the Web page to start the appropriate service.

Result

Protocol Configuration					
UDP	UDP QValue	TCP	TCP QValue	TLS	TLS QValue
Enable ▾		Disable ▾		Enable ▾	

Apply

The Ready LED will turn to a steady green. The SipEp Notification messages #303 and #310 are sent once the TLS connection is established. For example:

Syslog message: USER.INFO: SipEp: 1400-SIP Endpoint: 303-TLS connection with remote host 10.5.128.14:5063 is now ready to be used for SIP gateway default.

Syslog message: USER.INFO: SipEp: 1400-SIP Endpoint: 310-Server 10.5.128.14:5063 is now reachable for SIP gateway default.

Enabling Secure Media (SRTP) on All Endpoints

Before you start

Encrypted/secure signaling must be configured.

Steps

- 1) Go to **Media/Security**.
- 2) From the **Select Endpoint** selection list, choose **Default**.
- 3) In the **Security** table,
 - a) From the **Mode** drop box, select **Secure** or **Secure with fallback**.
 - b) From the **Key Management Protocol** drop box, select the protocol.

Note: Enabling **SDES** instead of **MIKEY** will make the SIP INVITEs slightly different. Choosing the **SDES** protocol will add the `a=crypto` line within the SDP Media Attributes while choosing the **MIKEY** protocol will add the `a=key-mgmt:mikey` line within the SDP Session Attributes.

- c) From the drop box, select the **AES_CM_128** encryption algorithm.
- d) From the **Allow Unsecure T.38 with Secure RTP** selection, choose if unsecure **T.38** is allowed with RTP.

Note: **T.38** packets will never be encrypted. The setting **Allow Unsecure T.38 with Secure RTP** will make possible to use **T.38**, otherwise it will be rejected. If not using **T.38** for faxing, to avoid an impact on the number of simultaneous calls a Mediatrix unit can handle in SRTP, set the **Allow Unsecure T.38 with Secure RTP** parameter to **No** and refer to the [Standard Fax Configuration](#) document to disable **T.38** Fax Transmission.

- 4) In the **SRTP Preferences** table,
 - a) From the **Crypto Mode When Sending Offer** drop box, select the preferred mode.
 - b) From the **Crypto Mode When Sending Answer** drop box, select the preferred mode.
 - c) From the **Crypto Context Behavior** drop box, select the preferred behavior.

Note: For more information about the recommended **SRTP Preferences**, please refer to [Recommended SRTP Preferences for a Typical VoIP Network](#) section of the [Setting the Security Parameters of the RTP Stream](#) document.

Note: For troubleshooting the SRTP interoperability, please refer to the [SRTP Troubleshooting](#) document.

- 5) Click **Apply**.

Result

All new SIP exchanges will contain RTP/SAVP negotiation elements.

Select Endpoint: Default ▾

Security	
RTP	
Mode:	Secure ▾
Key Management Protocol:	Key Management Protocol for SRTP ▾
Encryption:	AES_CM_128 ▾
T.38	
Allow unsecure T.38 with secure RTP:	No ▾

SRTP Preferences	
Crypto Mode When Sending Offer:	Mode when sending SDP offer with SRTP ▾
Crypto Mode When Sending Answer:	Mode when sending SDP answer with SRT ▾
Crypto Context Behavior:	Behavior of the SRTP Context ▾

Enabling Secure Media (SRTP) on a Specific Endpoint

Before you start

Encrypted/secure signaling must be configured.

Steps

- 1) Go to **Media/Security**.
- 2) From the **Select Endpoint** selection list, choose an endpoint.

Note: The list of available endpoints will vary depending on the type of unit being used.

- 3) In the **Security** table, from the **Mode** drop box, select **Secure** or **Secure with fallback**.
- 4) From the **Key Management Protocol** drop box, select the protocol.

Note: Enabling **SDS** instead of **MIKEY** will make the SIP INVITEs slightly different. Choosing the **SDS** protocol will add the a=crypto line within the SDP Media Attributes while choosing the **MIKEY** protocol will add the a=key-mgmt:mikey line within the SDP Session Attributes.

- 5) From the drop box, select the **AES_CM_128** encryption algorithm.
- 6) Click **Apply**.

Result

All new SIP exchanges going through the specified endpoint will contain RTP/SAVP negotiation elements.

Select Endpoint: Chosen Endpoint 

Security	
RTP	
Endpoint Specific:	Yes 
Mode:	Secure 
Key Management Protocol:	Key Management Protocol for SRTP 
Encryption:	AES_CM_128 

Troubleshooting

Enabling TLS Debugging on Wireshark

Before you start

To configure Wireshark for TLS packet capture, the private key associated with the server certificate are needed to decrypt TLS packets.

Steps

- 1) Go to **Edit/Preferences**.
- 2) Click + next to **Protocols**.
- 3) Select **SSL**.
- 4) Fill the **RSA keys list** field.

Note: The field specifies the binding between an IP address, a port, a protocol, and a RSA decryption key. Enter the IP address of the server, the SIP port, and the path to the file containing the server private key. Several such bindings may be specified by separating them with a semi-colon ";".

- 5) Start the Wireshark capture.

Note: TLS sessions using Diffie-Hellman based ciphers (DHE, ECDH, ECDHE) cannot be decrypted by Wireshark.

- 6) Restart the SipEp service on the Mediatrix unit or restart the unit.
- 7) Once the unit is restarted and the "Ready" LED is lit on the Mediatrix unit, stop the packet capture.
- 8) Using the "ssl" filter in the capture should show the SIP packets between the two endpoints.

Result

No.	Time	Source	Destination	Protocol	Info
757	15.	192.168.120.12	192.168.120.11	TLSv1	Application Data
759	15.	192.168.120.11	192.168.120.12	TLSv1	Application Data
783	15.	192.168.120.12	192.168.120.11	TLSv1	Application Data
832	15.	192.168.120.11	192.168.120.12	TLSv1	Application Data
862	15.	192.168.120.12	192.168.120.11	TLSv1	Application Data
889	16.	192.168.120.12	192.168.120.11	TLSv1	Application Data
895	16.	192.168.120.11	192.168.120.12	TLSv1	Application Data
956	16.	192.168.120.11	192.168.120.12	TLSv1	Application Data
1024	16.	192.168.120.12	192.168.120.11	TLSv1	Encrypted Alert
1025	16.	192.168.120.11	192.168.120.12	TLSv1	Encrypted Alert
1297	18.	192.168.120.12	192.168.120.11	SSL	Client Hello
1300	18.	192.168.120.11	192.168.120.12	TLSv1	Server Hello, Certificate, Server Hello Done
1303	19.	192.168.120.12	192.168.120.11	TLSv1	Client Key Exchange, Change Cipher Spec, Finished
1305	19.	192.168.120.11	192.168.120.12	TLSv1	Change Cipher Spec
1306	19.	192.168.120.11	192.168.120.12	TLSv1	Finished
1329	19.	192.168.120.12	192.168.120.11	SIP	Request: REGISTER sip:192.168.120.11:5062
1349	19.	192.168.120.11	192.168.120.12	SIP	Status: 401 Unauthorized (0 bindings)
1381	19.	192.168.120.12	192.168.120.11	SIP	Request: REGISTER sip:192.168.120.11:5062
1405	19.	192.168.120.11	192.168.120.12	SIP	Status: 401 Unauthorized (0 bindings)
1424	19.	192.168.120.12	192.168.120.11	SIP	Request: REGISTER sip:192.168.120.11:5062
1473	19.	192.168.120.11	192.168.120.12	SIP	Status: 200 OK (2 bindings)
1514	19.	192.168.120.12	192.168.120.11	SIP	Request: REGISTER sip:192.168.120.11:5062
1556	19.	192.168.120.11	192.168.120.12	SIP	Status: 200 OK (2 bindings)

File: "C:\DOCUME~1\magagne\LOCALS~1\Temp\wiresharkXXXXa18584" 1520 KB 00:00:24 Packets: 1848 Displayed: 23 Marked: 0 Dropped: 0

REGISTER Messages Not Being Answered

TLS is enabled on one of the Mediatrix gateways and not on the second gateway.

Issue: The REGISTER requests from the second gateway are not being answered.

Reason: The proxy is expecting the SIP message to be SSL encapsulated.

Procedures to solve the issue: Restart the Wireshark capture and enable TLS on the second gateway. Restart the required services.

Server Internal Error (or Similar Messages)

Some servers/proxies will require Interop variables to be enabled.

For example, the default openSIPS installation requires adding the SIP transport field in the registration and contact headers.

Enabling Interop Variables

Steps

- 1) Go to **SIP/Transport**.
- 2) In the **General Configuration** table, set the **Add SIP Transport in Registration** and **Add SIP Transport in Contact Header** variables to **Enable**.
- 3) Click **Apply**.

Result

General Configuration		
Add SIP Transport in Registration:	Enable	
Add SIP Transport in Contact Header:	Enable	
Persistent Base Port:	16000	
Failback Interval:	15	
TLS Certificate Trust Level:	Locally Trusted	
TCP Connect Timeout:	127	
Add rport:	Disable	

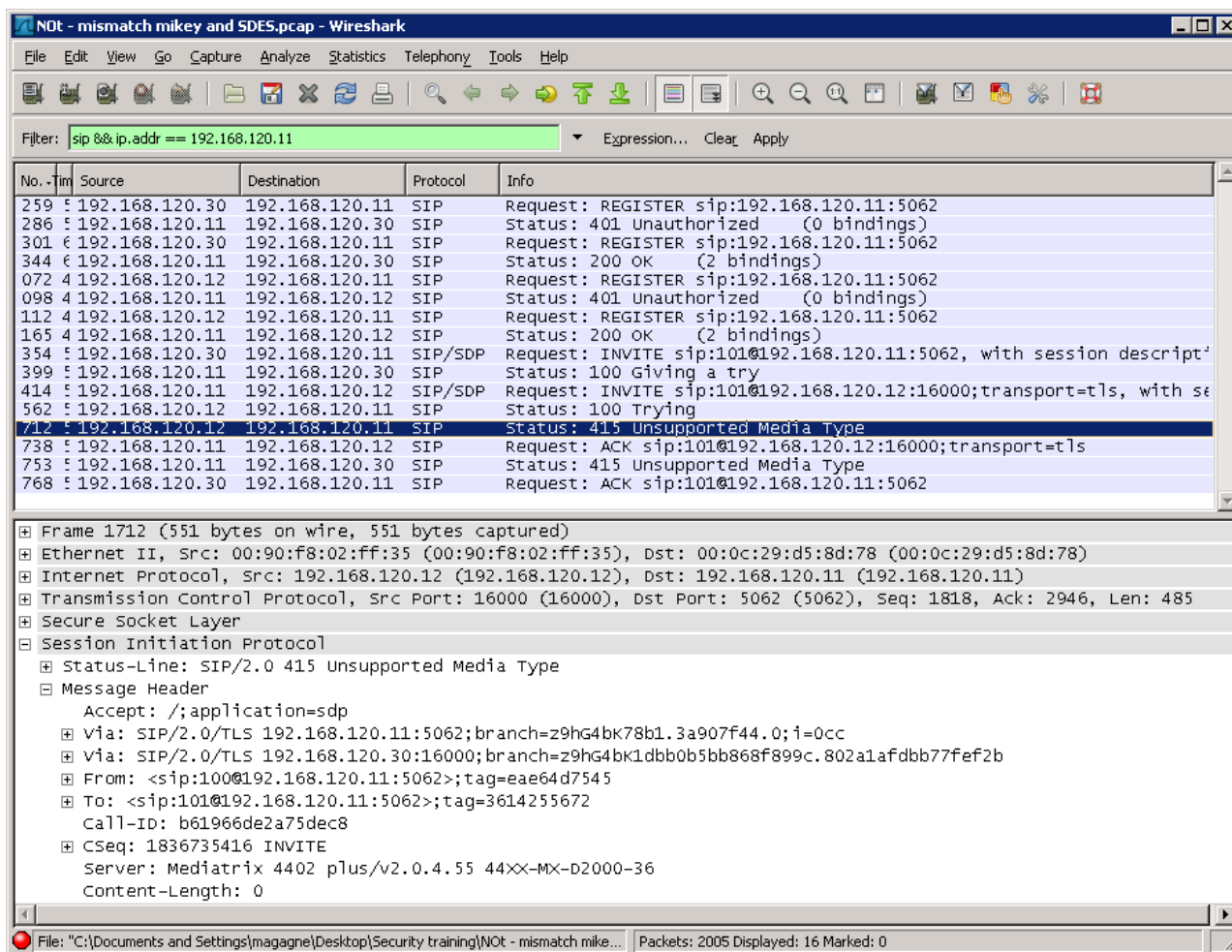
Mikey and SDES Mismatch

This document explains why it is highly recommended to choose only one single key management protocol.

In the following example, SDES is configured on endpoint 1 (192.168.120.30) and Mikey on endpoint 2 (192.168.120.12)

The gateway 192.168.120.12 returns a **SIP 415 Unsupported Media** error because it is not configured to manage SDES.

The following Syslog message should also be seen: syslog: SdpTools [D3A2] Received the wrong key management protocol. Secure stream disabled.



Audio Issues with Secured Media (SRTP)

This document explains how to detect an audio issue with a Mediatrix gateway when the media is secured with SRTP.

In the following example, both gateways are configured with different **SRTP Preferences** configurations. This situation may be encountered when the SRTP behaviors with different SIP devices are not compatible.

The gateway 192.168.121.5 is configured to keep the cryptographic elements while the the gateway 192.168.121.10 is configured to regenerate the cryptographic elements.

After some times, when the Mediatrix detects that the incoming SRTP stream cannot be decrypted, it will send the following notification message: Mipt: 1600-Media IP Transport: 110-The call ##### on endpoint XYZ detected an SRTP cryptographic error. The secured RTP stream is not properly decoded.

tcpdump -i eth0 -s 1500 -n -v -e 'tcpdump && (sip syslog_level <= 5 string(rtp.seq) matches "^\\d000+\$" string(rtp.seq) matches "6553\\d")'			
No.	Source	Protocol	Info
106769	192.168.121.5	SIP/SDP	Request: INVITE sip:1001@192.168.121.10, in-dialog
106832	192.168.121.10	SIP/SDP	Status: 200 OK
106894	192.168.121.5	SIP	Request: ACK sip:1001@192.168.121.10
109945	192.168.121.10	SRTP	PT=ITU-T G.711 PCMA, SSRC=0xA346B047, Seq=65530, Time=1739923238
109947	192.168.121.10	SRTP	PT=ITU-T G.711 PCMA, SSRC=0xA346B047, Seq=65531, Time=1739923478
109949	192.168.121.10	SRTP	PT=ITU-T G.711 PCMA, SSRC=0xA346B047, Seq=65532, Time=1739923718
109951	192.168.121.10	SRTP	PT=ITU-T G.711 PCMA, SSRC=0xA346B047, Seq=65533, Time=1739923958
109953	192.168.121.10	SRTP	PT=ITU-T G.711 PCMA, SSRC=0xA346B047, Seq=65534, Time=1739924198
109958	192.168.121.10	SRTP	PT=ITU-T G.711 PCMA, SSRC=0xA346B047, Seq=65535, Time=1739924438
110899	192.168.121.5	SRTP	PT=ITU-T G.711 PCMA, SSRC=0xA346B047, Seq=60000, Time=1038601392
112114	192.168.121.10	SRTP	PT=ITU-T G.711 PCMA, SSRC=0xA346B047, Seq=10000, Time=1740164678
113391	192.168.121.5	SIP/SDP	Request: INVITE sip:1001@192.168.121.10, in-dialog
113454	192.168.121.10	SIP/SDP	Status: 200 OK
113516	192.168.121.5	SIP	Request: ACK sip:1001@192.168.121.10
116780	192.168.121.5	Syslog	USER.ERR: Mipt: 1600-Media IP Transport: 110-The call 21 on endpoint FXS1 detected an SRTP cryptographic error. The secured RTP stream is not properly decoded.
117145	192.168.121.5	Syslog	USER.ERR: Mipt: 1600-Media IP Transport: 110-The call 21 on endpoint FXS1 detected an SRTP cryptographic error. The secured RTP stream is not properly decoded.
117353	192.168.121.10	SRTP	PT=ITU-T G.711 PCMA, SSRC=0x27689E98, Seq=60000, Time=3811622713
117508	192.168.121.5	Syslog	USER.ERR: Mipt: 1600-Media IP Transport: 110-The call 21 on endpoint FXS1 detected an SRTP cryptographic error. The secured RTP stream is not properly decoded.
117871	192.168.121.5	Syslog	USER.ERR: Mipt: 1600-Media IP Transport: 110-The call 21 on endpoint FXS1 detected an SRTP cryptographic error. The secured RTP stream is not properly decoded.

This audio issue occurred after the sequence number of one of the SRTP streams had rolled over and the SRTP cryptographic contexts of both peers are desynchronised. This event may also happen when resuming a SIP call on hold.

Note: When an audio issue related to SRTP streams occurred, please refer to the [SRTP Troubleshooting](#) document.

Annexes

Mediatrix Support Portal

<http://www.media5corp.com/support-portal>

Online Help

If you are not familiar with the meaning of the fields and buttons, click **Show Help**, located at the upper right corner of the Web page. When activated, the fields and buttons that offer online help will change to green and if you hover over them, the description will be displayed.

DGW Documentation

Mediatrix devices are supplied with an exhaustive set of documentation.

Mediatrix user documentation is available on the [Media5 Documentation Portal](#).

Several types of documents were created to clearly present the information you are looking for. Our documentation includes:

- **Release notes:** Generated at each GA release, this document includes the known and solved issues of the software. It also outlines the changes and the new features the release includes.
- **Configuration notes:** These documents are created to facilitate the configuration of a specific use case. They address a configuration aspect we consider that most users will need to perform. However, in some cases, a configuration note is created after receiving a question from a customer. They provide standard step-by-step procedures detailing the values of the parameters to use. They provide a means of validation and present some conceptual information. The configuration notes are specifically created to guide the user through an aspect of the configuration.
- **Technical bulletins:** These documents are created to facilitate the configuration of a specific technical action, such as performing a firmware upgrade.
- **Hardware installation guide:** They provide the detailed procedure on how to safely and adequately install the unit. It provides information on card installation, cable connections, and how to access for the first time the Management interface.
- **User guide:** The user guide explains how to customise to your needs the configuration of the unit. Although this document is task oriented, it provides conceptual information to help the user understand the purpose and impact of each task. The User Guide will provide information such as where and how TR-069 can be configured in the Management Interface, how to set firewalls, or how to use the CLI to configure parameters that are not available in the Management Interface.
- **Reference guide:** This exhaustive document has been created for advanced users. It includes a description of all the parameters used by all the services of the Mediatrix units. You will find, for example, scripts to configure a specific parameter, notification messages sent by a service, or an action description used to create Rulesets. This document includes reference information such as a dictionary, and it does not include any step-by-step procedures.

Copyright Notice

Copyright © 2023 Media5 Corporation.

This document contains information that is proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.



media5corp.com