Mitel TA7100

CONFIGURATION NOTES

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

Contents

1 SCOPE

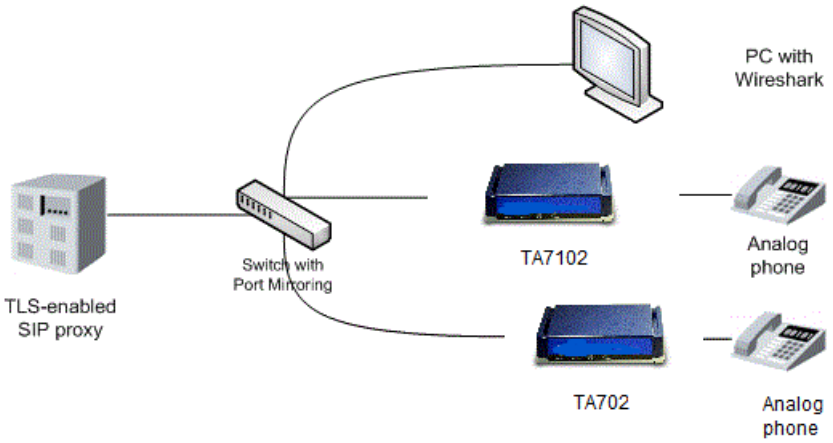
This document describes the steps required to configure the Mitel unit loaded with the DGW v2.0 firmware for secure SIP signalling and secure media (SRTP) operation. This is not a complete key-exchange, TLS or general security tutorial. For more information on those topics, please see the links section.

1.1 ACRONYMS AND DEFINITIONS

RTP	Real Time Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SRTP	Secure Real Time Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
Wireshark	Network sniffing and capture tool

1.2 SETUP DESCRIPTION

In this scenario, the endpoints used are Mitel Terminal Adapters. The units must be loaded with Dgw v2.0. We will use the freely available openSIPS (www.opensips.org) as the SIP proxy and configure it for TLS operation.



1.3 BASICS OF SECURITY EXCHANGES

At the level at which we are working, establishing a TLS connection is fairly straightforward. In practice, at a lower level, there are quite a lot of additional complications to guard against various possible attacks.

This is the overall exchange in order to build the TLS link and bring it “up”:

The client (Mitel Terminal Adapters) 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.

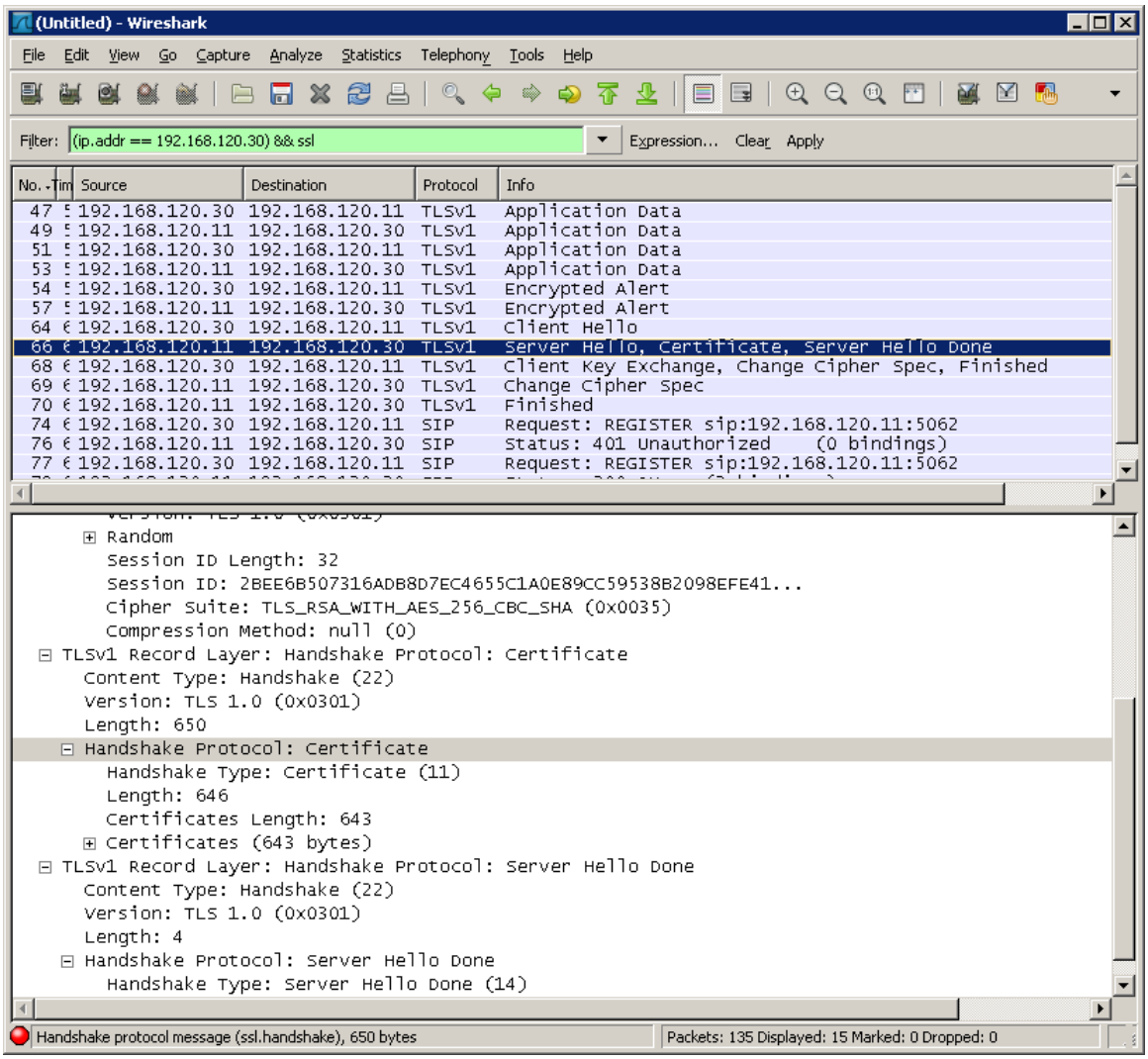
The client verifies the server certificate (validations are configured via the TlsCertificateValidation variable).

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 Wire shark capture.



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

- the server 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 fails, your 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.

2 INSTALLATION

2.1 INSTALLING A TLS-ENABLED SERVER/PROXY

Using two Mitel Terminal Adapters 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 www.opensips.org/docs. Otherwise skip this section.

Please note that (at the moment of this writing) by default open sips is configured 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.

2.2 ABOUT CERTIFICATES

In order to enable TLS on the Mitel Terminal adapters, you will need at least a CA certificate that will validate that the certificate presented by the server is valid. This certificate must be uploaded to the Mitel Terminal adapters. In order to use the Wire shark features that are described later, a copy of the SIP server certificate containing its private key (this will be used to decrypt the TLS) will also be needed. The certificates need to be in ITU X.509 format.

For certificate creation, we recommend the FAQ page from the openssl project:

http://www.openssl.org/support/faq.html#USER3

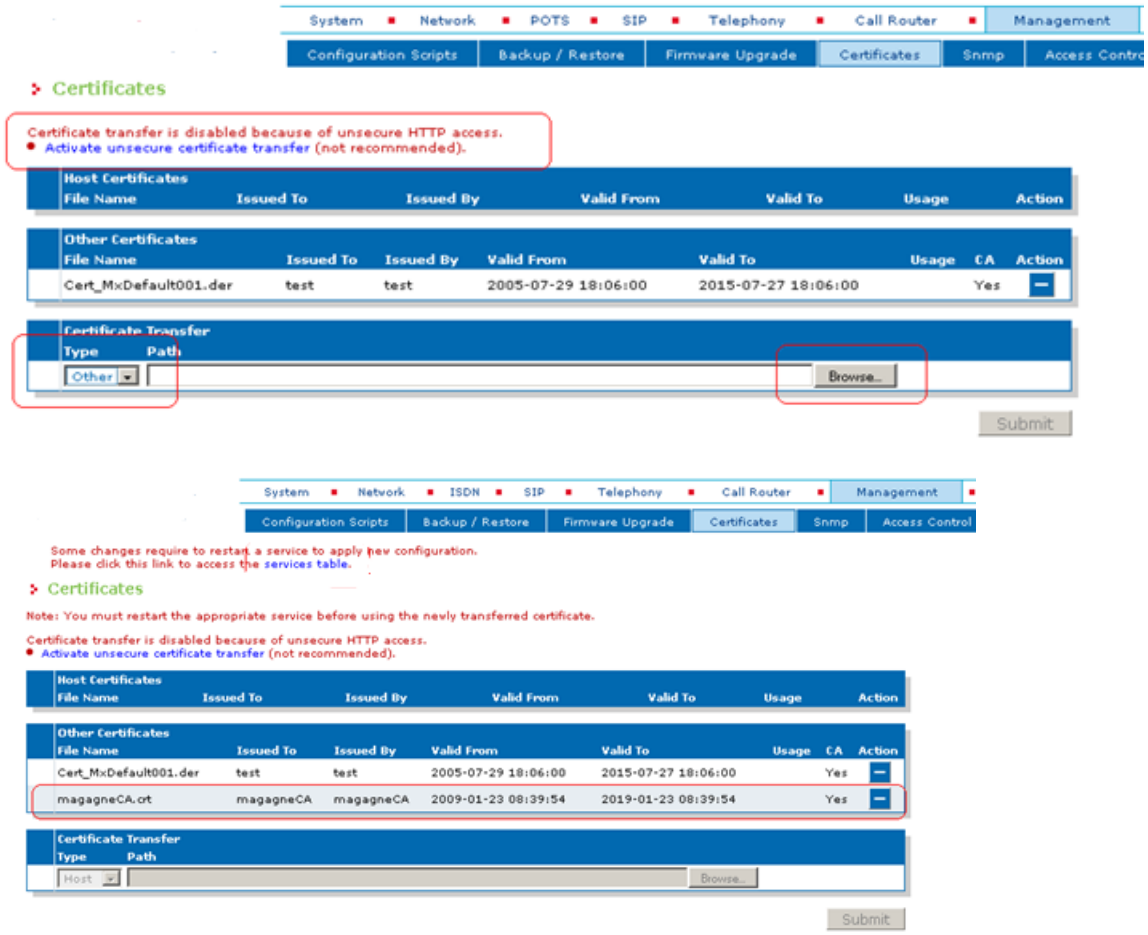
2.3 INSTALLING CERTIFICATES ON THE MITEL UNIT

Navigate to the Management-> Certificates section.

Activate unsecured certificate transfer.

Select the certificate type Other, then click Browse. A pop-up explorer window appears and allows you to browse your local file system to locate the server's CA certificate file (usually with a .crt extension), using format X.509.

When the certificate is loaded, the required services must be restarted. This can be done by following the provided link at the top of the web page.



It is important to know the distinction between a "*Host*" and "*Other*" certificate.

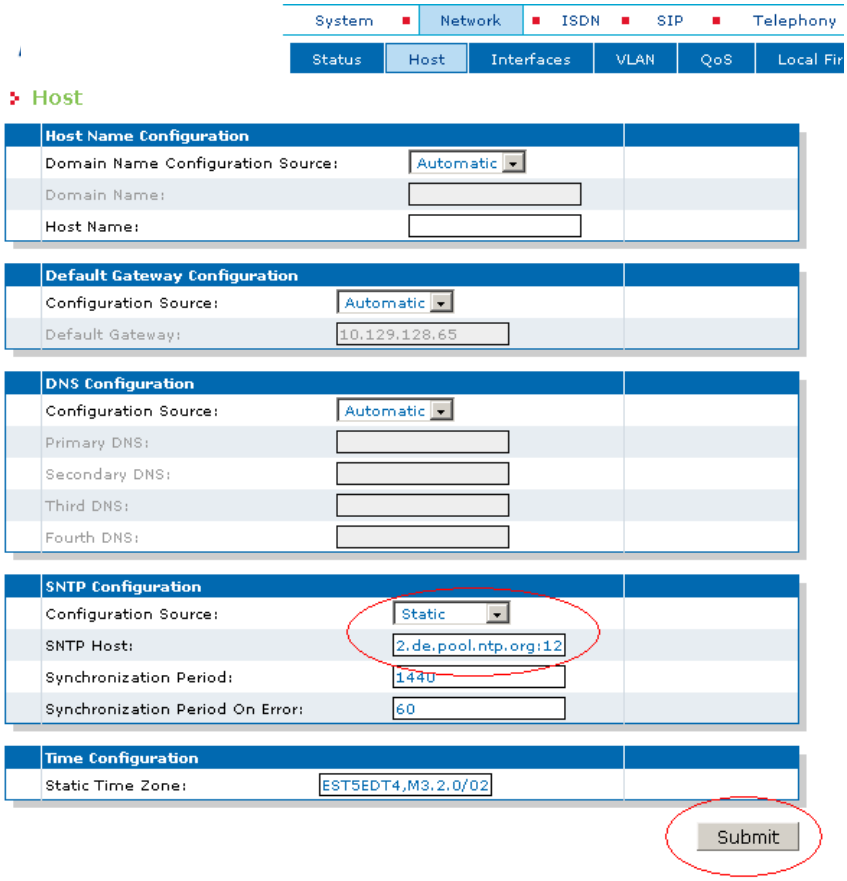
An "*Other*" certificate is simply a CA certificate used to validate the certificate of the server to which TA7102 is trying to connect.

A "Host" certificate is a server certificate that is required if TA7102 acts as a TLS server and presents its certificate to other clients. An example of this would be two Mediatrix gateways with no SIP proxy in the middle. At least one of the units will require a Host certificate. If only one unit has a Host certificate, the calls will be allowed in only one direction (Unit 1 calls Unit 2). For bi-directional calls, both Mitel Terminal adapters would require a Host certificate.

Note that by default it is not possible to upload a Host certificate without first clicking on **Activate unsecured certificate transfer**. This is because the certificate upload will be done in clear text, which means **the private key will be susceptible to interception!**

Important: Mitel recommends uploading Host certificates from a PC that is connected directly to the gateway.

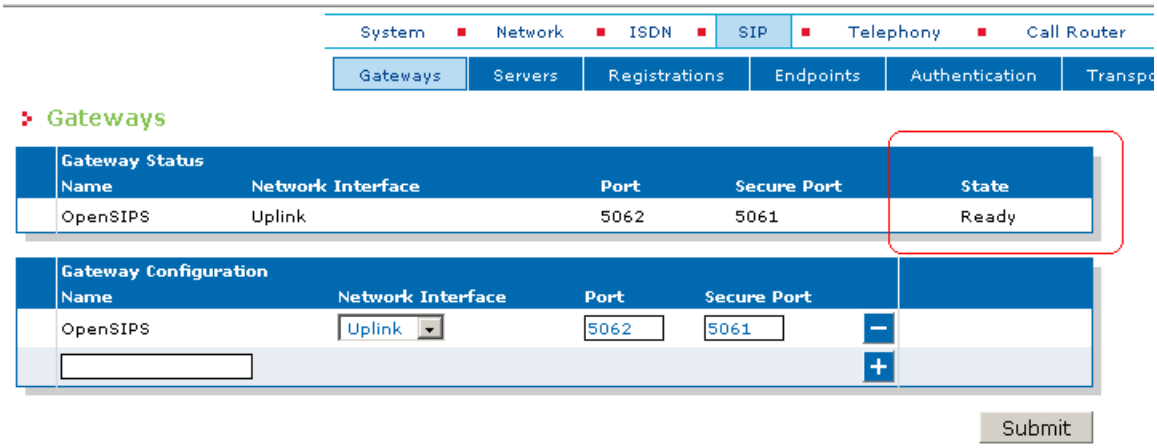
Note! Warning: Since certificates have a start date and expiry date, the use of NTP (Network Time Protocol) is now **mandatory** on the Mitel Terminal adapters when using the security features. To setup the NTP server, go to the *Network-> Host* section and configure your NTP server accordingly.



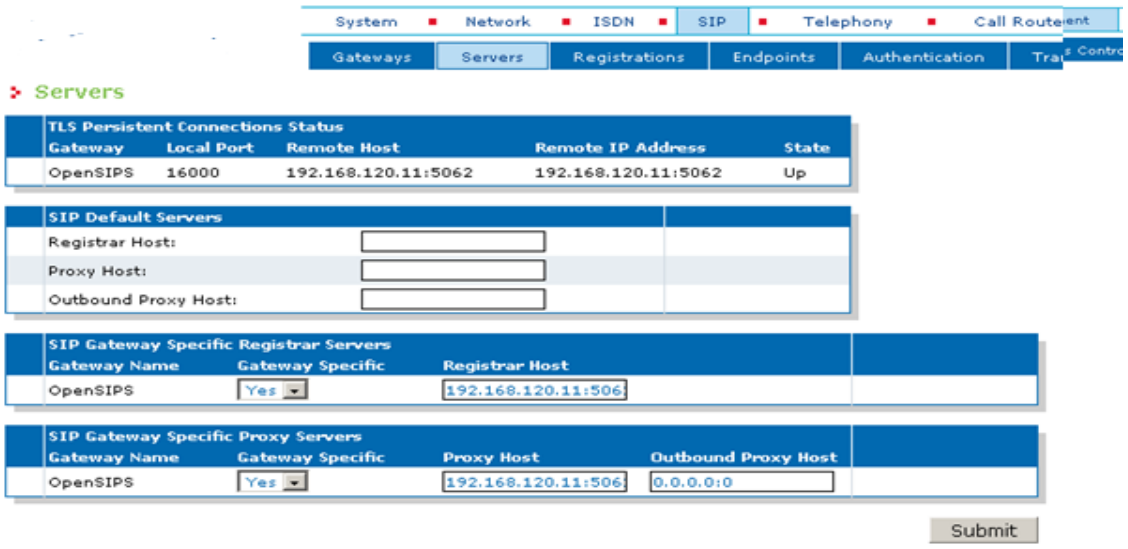
2.4 MITEL UNIT CONFIGURATION

2.5 SIP GATEWAY CONFIGURATION

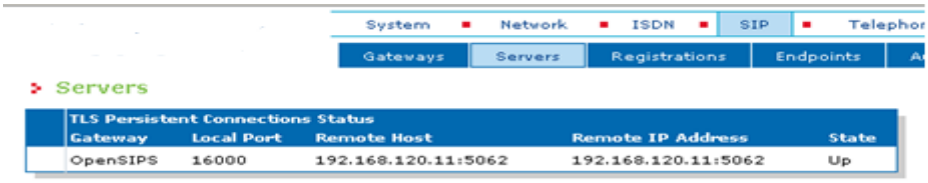
Before using TLS, the SIP gateway needs to be properly configured. To do that, go to the *SIP-> Gateways* section.



In this example, the gateway called “OpenSIPS” is listening on port 5062. To configure the gateway, click the **Servers** tab.



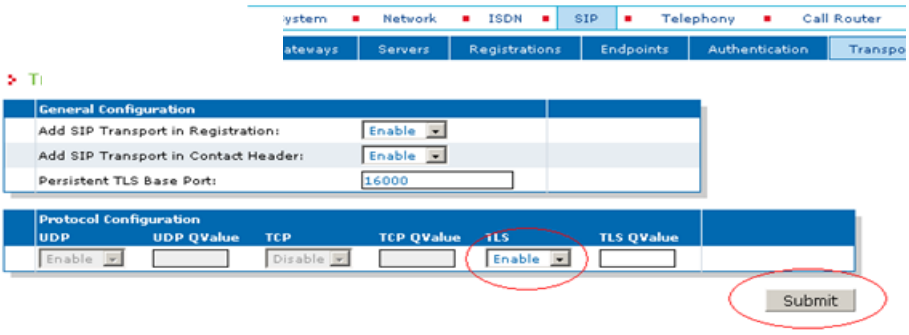
For settings that are gateway-specific, use the *Gateway Specific* sections. In the previous example, the settings are valid only for the “OpenSIPS” gateway. Both the SIP Registrar and SIP Proxy are configured to 192.168.120.11 on port 5062.



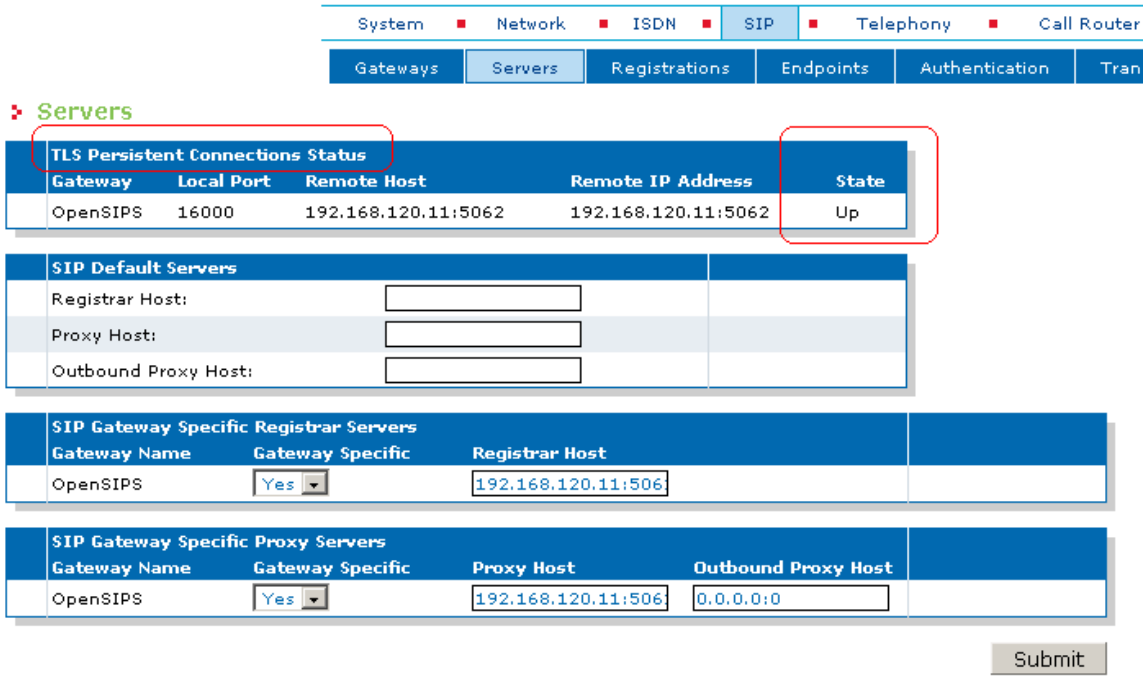
2.6 ENABLING SECURE SIGNALLING (TLS)

The Mitel unit does not support mixing TLS and non-TLS links. This means that it is not possible to configure separate gateways (*SIP-> Gateways*) using secure and non-secure links. Once TLS is enabled, it is enabled for all configured gateways.

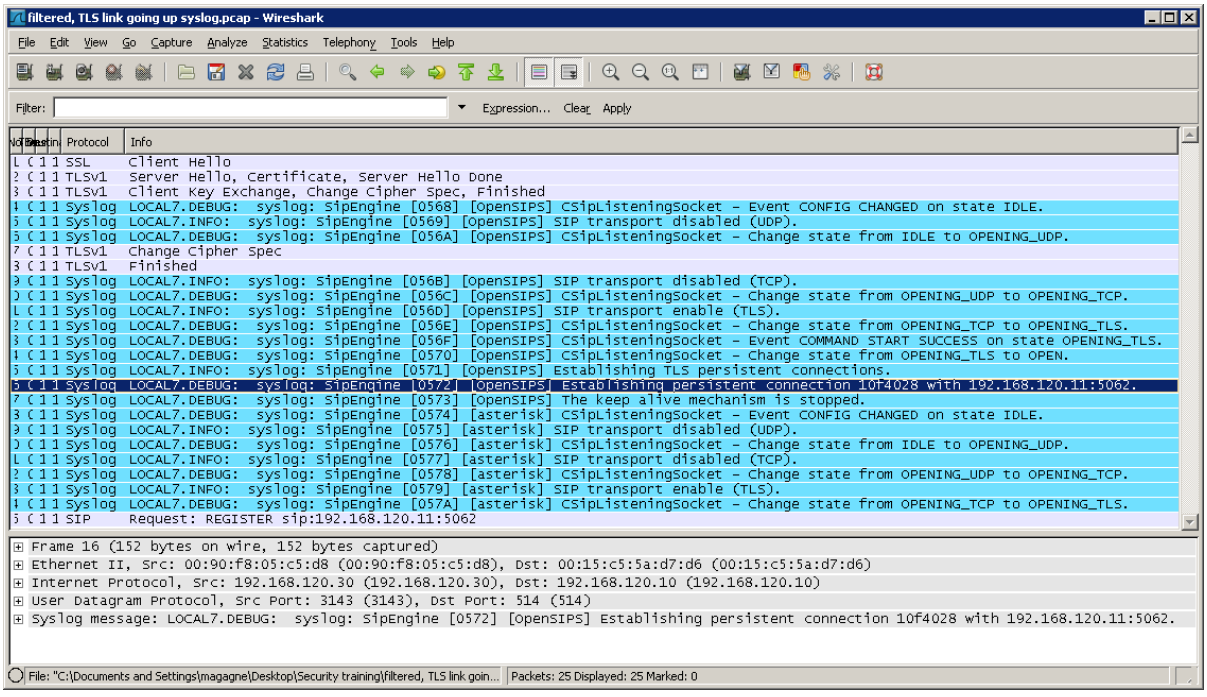
Go to the *SIP-> Transport* tab and simply enable TLS, click *Submit* and follow the link to start the appropriate service. Please notice the configuration field for the previously discussed port 16000.



If the TLS link is established, the “Ready” LED on the Mitel unit turns on steady green. The status of the TLS link can also be found in the web page and in the syslog.



A syslog message will be sent saying “establishing persistent connection”

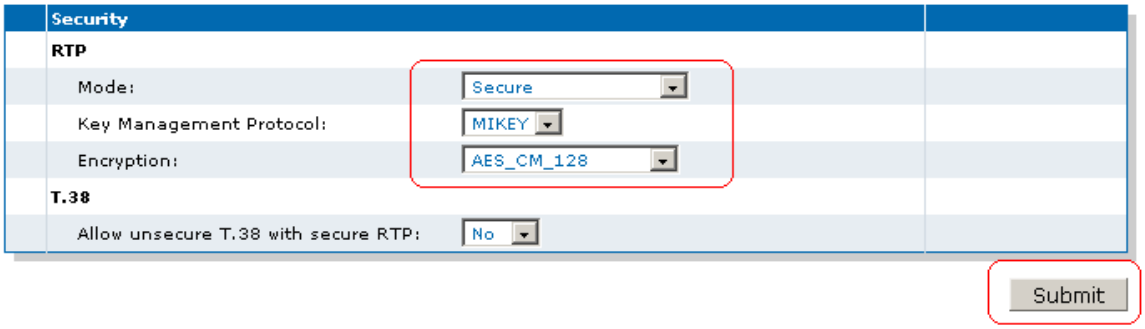


2.7 ENABLING SECURE MEDIA (SRTP)

Now that encrypted signaling is configured, the media streams can also be encrypted and secured. Without encryption, RTP is still vulnerable to interception.

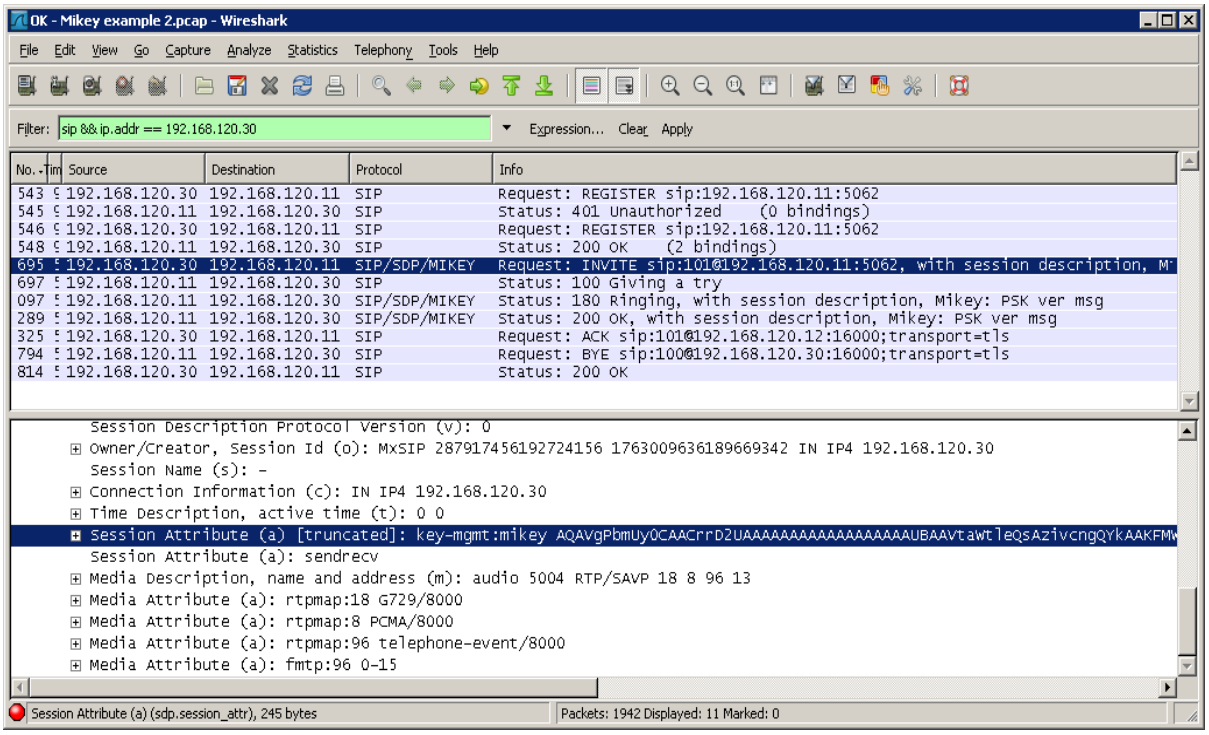
Do as follows:

1. Go to the Telephony -> CODECs page and enable secure RTP by changing the Mode to Secure.
2. Choose a Key Management Protocol. The Mitel unit supports both MIKEY and SDES.
3. Choose the encryption algorithm. Currently the Mitel unit supports AES with 128 bits. The choice “NULL” will not encrypt the RTP. This should be selected only for debugging purposes.
4. Click Submit.

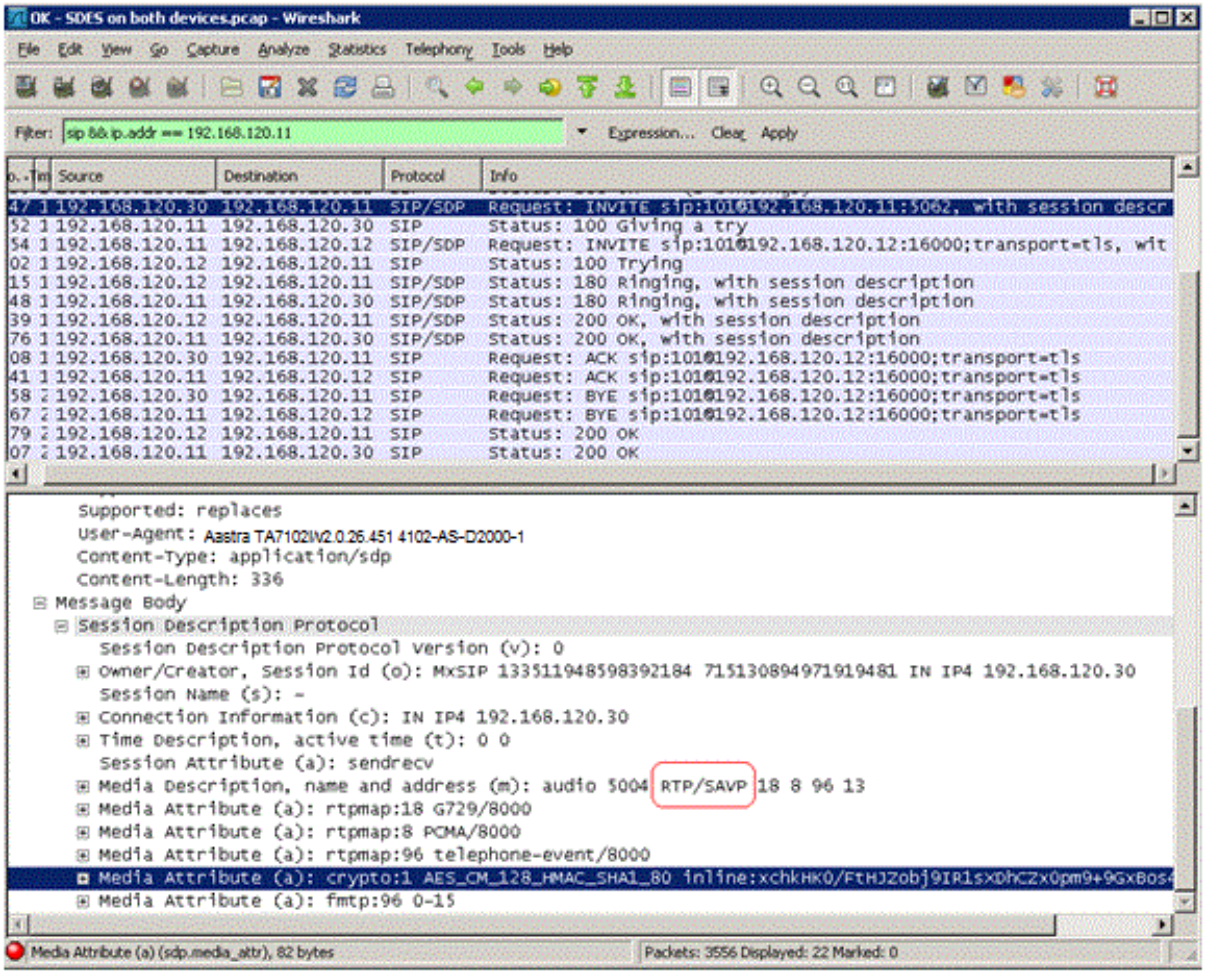


Note! Note: T.38 packets will never be encrypted. Setting “Allow unsecured T.38 with secure RTP” will allow using T.38, otherwise it would be rejected.

In the following Wireshark trace, the Mikey parameters are sent in the INVITE SDP.



Enabling SDES instead of Mickey, the INVITE will be slightly different. SDES parameters will be added to the SDP Media Attributes instead of the Session Attributes.



The *RTP/SAVP* is a flag which states that the endpoint is attempting to initiate a secure media connection. Seethe text in red in the above example.

3 TROUBLESHOOTING

To troubleshoot when using security, Wireshark must be configured for TLS sniffing.

The following are a few examples of issues that may be encountered while configuring TLS.

3.1 ENABLING TLS DEBUGGING ON WIRESHARK

Once the TLS link is up, it is no longer possible to read the SIP packets as they are TLS-encrypted. To debug TLS, Wireshark needs to be configured to decrypt them. For this step, the public keys associated with the server certificate are needed.

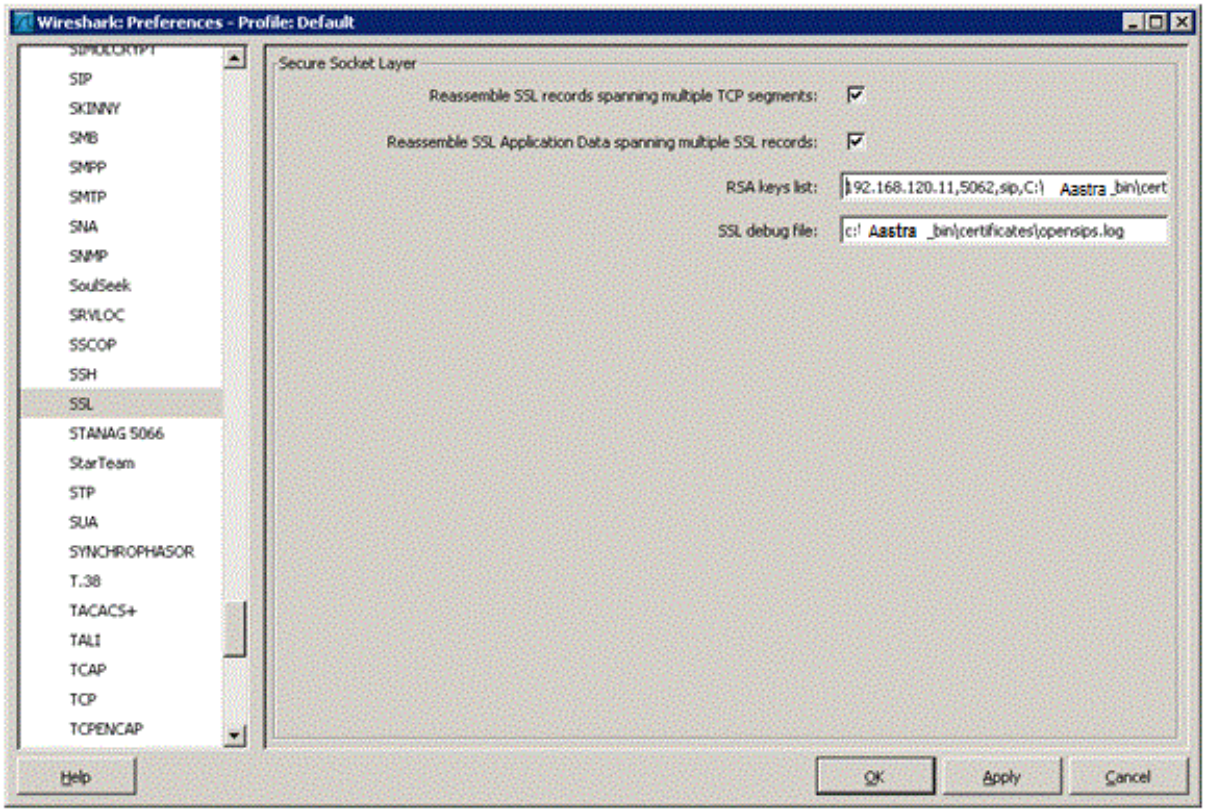
Do as follows:

1. In the Edit/Preferences dialog, select the Protocols/SSL node and fill the RSA key list. 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 ";".

   Example: The server is located at 192.168.120.11 and listens on port 5062

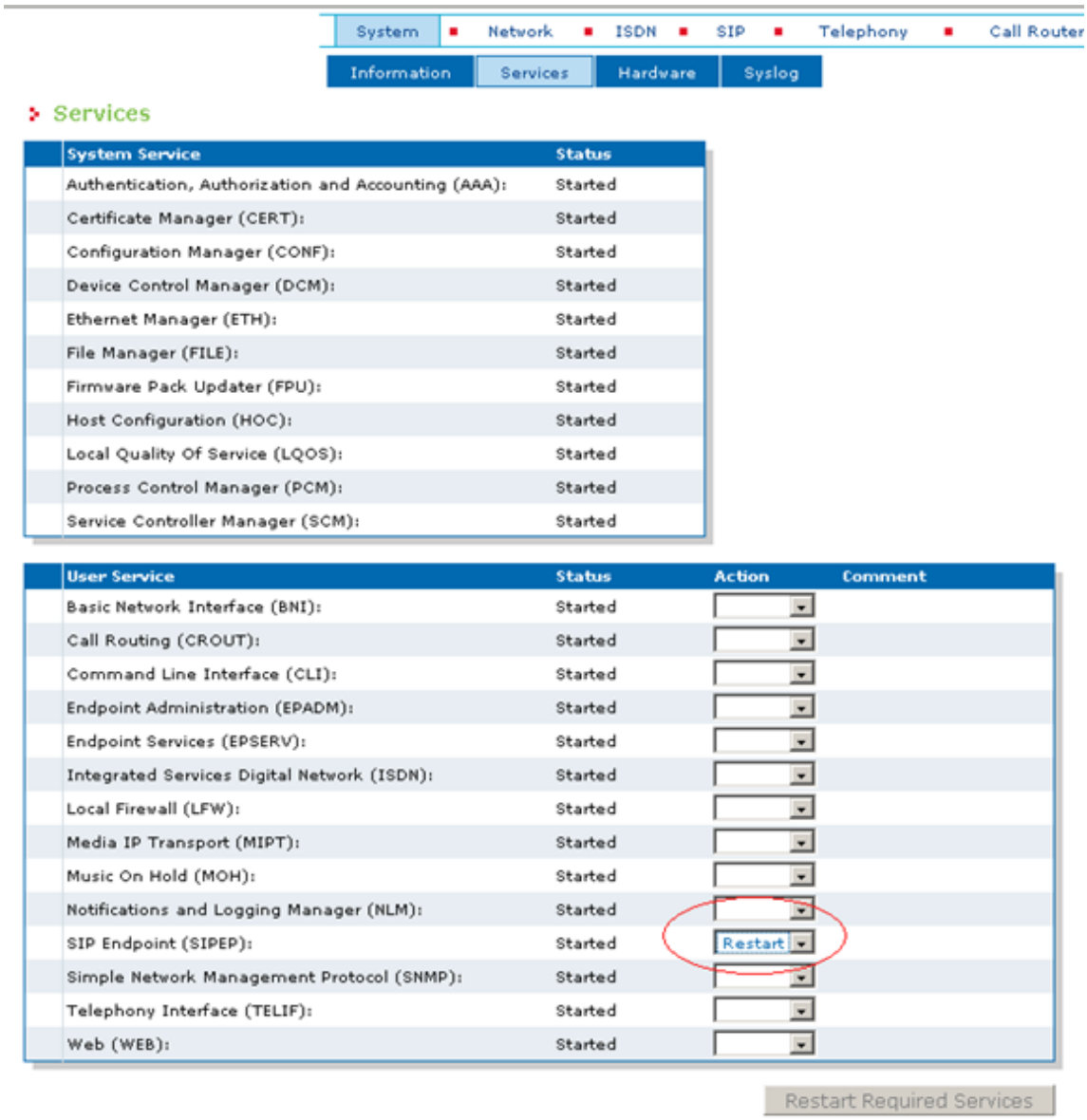
   192.168.120.11,5062,sip,C: \certificates\192.168.120.11.key

   When having difficulty decrypting SIP packets, the "SSL debug file" may be used to determine what is going wrong.



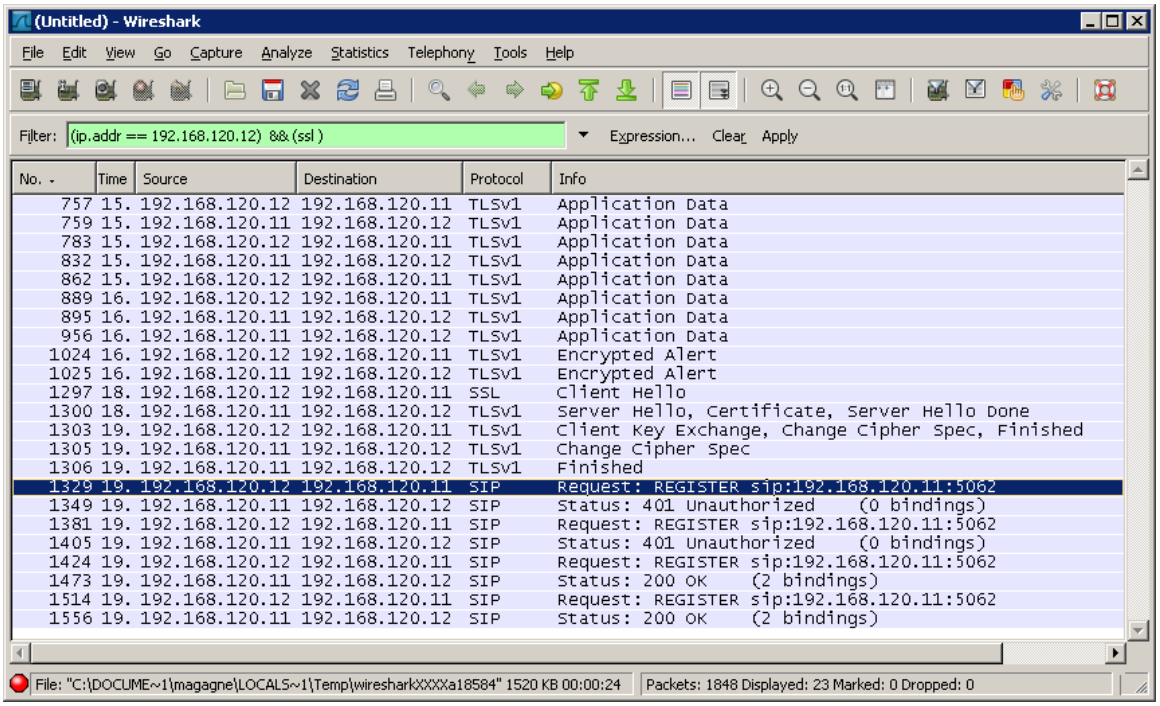
2. Start the Wireshark capture.

3. Restart the SIPEP service on the Mitel unit or simply reboot the Mitel unit. This will enable the TLS renegotiation.



4. When the unit is rebooted and the “Ready” LED is lit on the Mitel unit, stop the packet capture.

5. Using the “ssl” filter in the capture should show the SIP packets between the two endpoints.



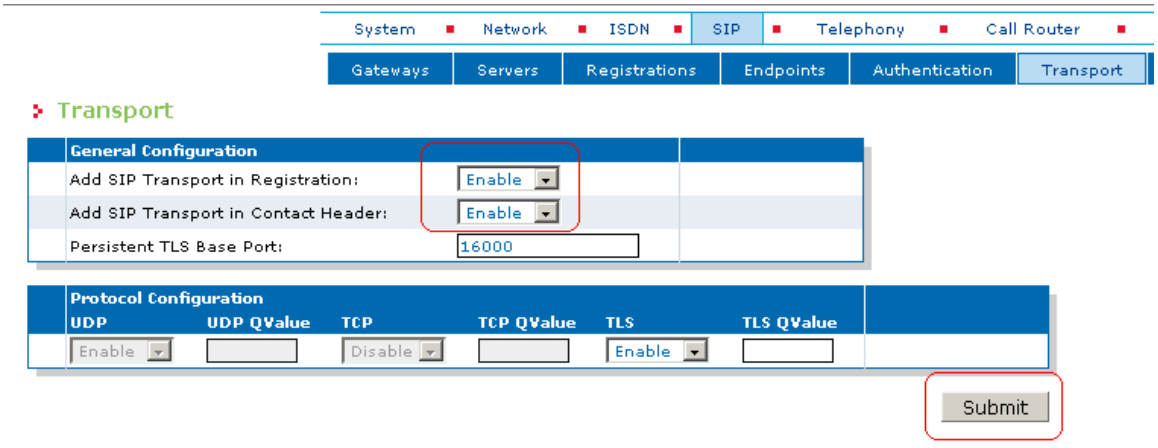
3.2 REGISTER MESSAGES NOT BEING ANSWERED

In the first example, TLS is enabled on one of the Mitel Terminal adapters and not on the second gateway.

The REGISTER requests from the second gateway are not being answered. This is because the proxy is expecting the SIP message to be SSL encapsulated. Simply restart the Wireshark capture and enable TLS on the second gateway. Restart the required services

3.3 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. To do so, set the following variables to **Enable**.



Below is a SIP Register message from one endpoint (192.168.120.30) that has the TLS transport in the Contact Header disabled and also a SIP Register message from the other endpoint that has the Contact Header enabled (192.168.120.12).

Register from 192.168.120.30

REGISTER sip:192.168.120.11:5062 SIP/2.0

Via: SIP/2.0/TLS
192.168.120.30:16000;branch=z9hG4bK840120998b9b8d813.231a4bf34e2eaa130

Max-Forwards: 70

From: <sip:100@192.168.120.11:5062>;tag=2ce647ee6c

To: <sip:100@192.168.120.11:5062>

Call-ID: a1b5ddebef59717a

CSeq: 151405030 REGISTER

Authorization: Digest
username="100",realm="192.168.120.11",nonce="4a5e430d000006aba1954cd956e94d0dc440d94d977f8d3a",uri="sip:192.168.120.11:5062",response="c42b06827c08018c8c34cd0696269193"

Contact: <sip:100@192.168.120.30:16000> (NO TRANSPORT METHOD IN HEADER)

User-Agent: Mitel TA7102i/v2.0.26.451 4102-AS-D2000-1

Content-Length: 0

Invite from 192.168.120.12

INVITE sip:100@192.168.120.11:5062 SIP/2.0

Via: SIP/2.0/TLS
192.168.120.12:16000;branch=z9hG4bK6a4e16b7b478eae83.051f66c579acf19dd

Max-Forwards: 70

From: <sip:101@192.168.120.11:5062>;tag=e437e6cd75

To: <sip:100@192.168.120.11:5062>

Call-ID: 822ebcc6433a7565

CSeq: 1793624545 INVITE

Allow: INVITE, ACK, BYE, CANCEL, REFER, NOTIFY, UPDATE

Contact: <sip:101@192.168.120.12:16000**;transport=tls**>

Min-SE: 1800

Session-Expires: 3600

Supported: timer

Supported: replaces

User-Agent: Mitel TA7102i/v2.0.26.451 4102-AS-D2000-1

Content-Type: application/sdp

Content-Length: 300

Here is the REGISTER for a subsequent working call with the Interop variable enabled.

REGISTER sip:192.168.120.11:5062 SIP/2.0

Via: SIP/2.0/TLS 192.168.120.30:16000;branch=z9hG4bK7006d85fe396d7632.499de40d84094b998

Max-Forwards: 70

From: <sip:100@192.168.120.11:5062>;tag=586e1a152b

To: <sip:100@192.168.120.11:5062>

Call-ID: 83216656d213ac84

CSeq: 1378359313 REGISTER

Authorization: Digest username="100",realm="192.168.120.11",nonce="4a669cc80000000b95e8ef28fe0ce518d557d54ad3cc655a",uri="sip:192.168.120.11:5062",response="214ede0b4eda7b7e6d6d2e03eb013755"

Contact: <sip:100@192.168.120.30:16000;**transport=tls**>

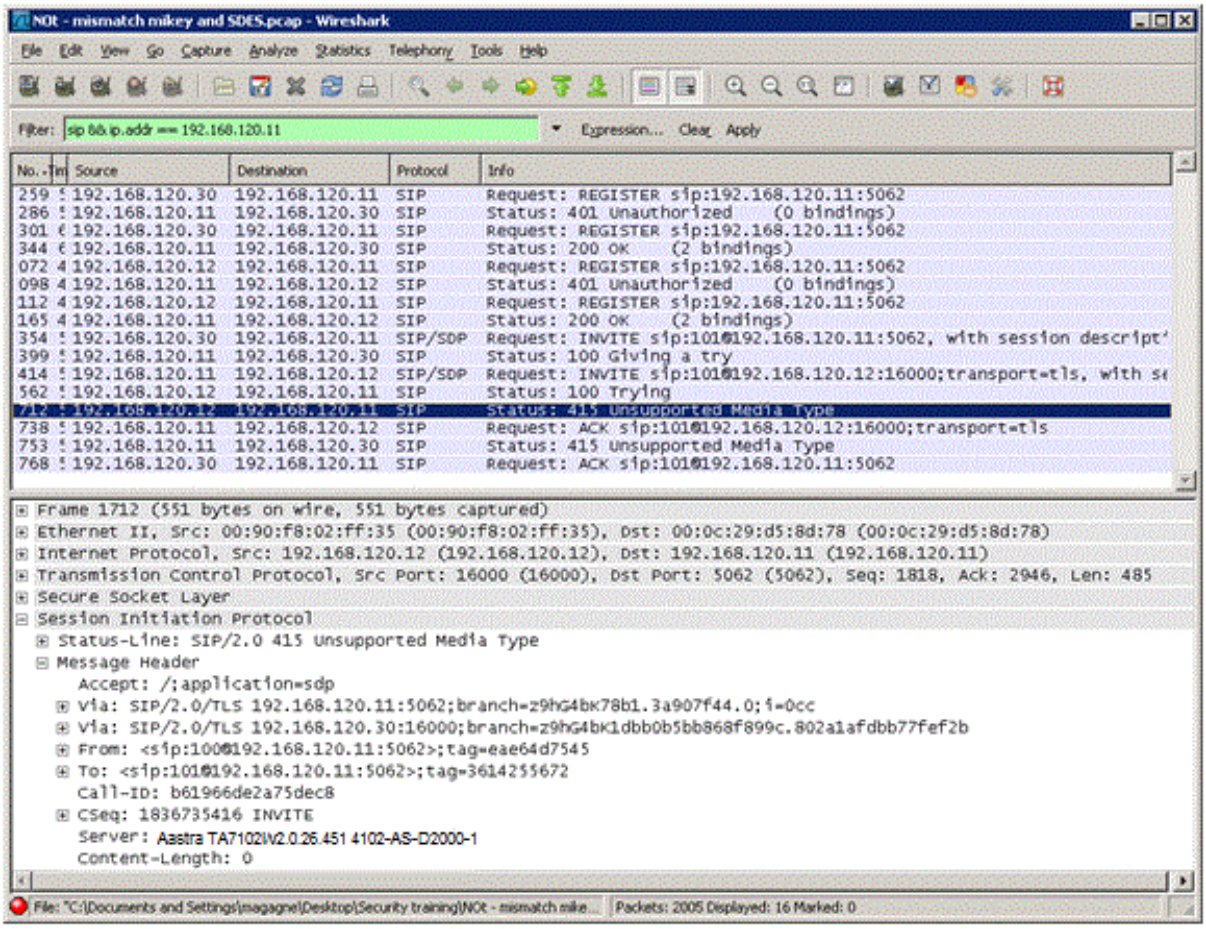
User-Agent: Mitel TA7102i/v2.0.26.451 4102-AS-D2000-1

Content-Length: 0

3.4 MIKEY AND SDES MISMATCH

It is strongly recommended to select 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 will return a SIP 415 Unsupported Media because it is not configured for SDES management.



The following Syslog message should also be seen:

syslog: SdpTools [D3A2] Received the wrong key management protocol. Secure stream disabled.

3.5 ANNEXES

Mitel Knowlegde Base

SSL and Certificates Information

http://www.openssl.org

http://en.wikipedia.org/wiki/X.509 (see links section)

Mikey Information

http://tools.ietf.org/html/rfc3830

SDES Information

http://tools.ietf.org/html/rfc4568

OpenSIPS Configuration Notes

tcp_conn.h:

#define TCP_CHILD_TIMEOUT pour 0 (avoid response delays)

#define DEFAULT_TCP_CONNECTION_LIFETIME pour 12000 (avoid connection drops after 2 minutes of inactivity)

opensips.cfg:

disable_tls = no

listen = tls:192.168.120.11:**5062**

tls_verify_server = 0

tls_verify_client = 0

tls_require_client_certificate = 0

tls_method = TLSv1

tls_certificate = "/home/user/opensips/etc/opensips/cert.pem"

tls_private_key = "/home/user/opensips/etc/opensips/privkey.pem"

#tls_ca_list = "/home/user/opensips/etc/opensips/tls/user/user-calist.pem"