Mitel TA7100

58014900 REV00

ENABLING SECURITY FEATURES IN DGW FIRMWARE

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). 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

Mitel TA7100 Enabling Security Features in Dgw Firmware
58014900 REV00 - May 2016

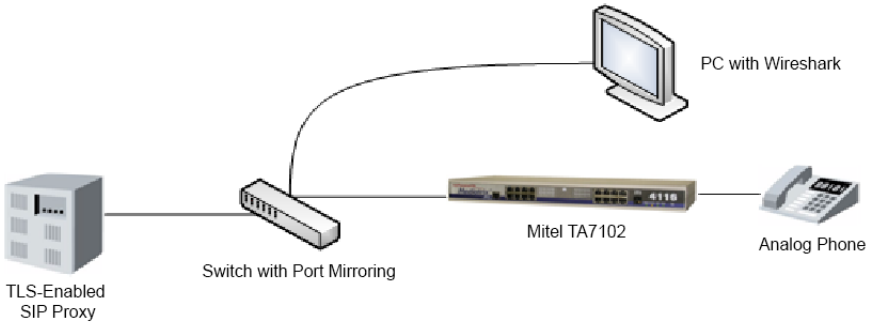
Enable Security Features in Dgw

This document describes the steps required to configure a Mitel 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 endpoint used is a Mitel TA7102 unit. The Mitel unit must be loaded with Dgw. If the Mitel TA7100 device is loaded with SIP v5.0, please refer to the *Technical Bulletin Upgrading from SIP 5.0 to Dgw* to update your firmware, as this is outside the scope of this document. We will use the freely available openSIPS (http://www.opensips.org) as the SIP proxy and configure it for TLS operation.

NOTE: *This Configuration Notes apply to Mitel TA7100 models.*



TLS-Enabled Server/Proxy Installation with openSIPS

Using two Mitel 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 Mitel 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 usage of the certificate e.i. as a:
  - 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 using the Configuration Backup and Restore procedure. Since certificates have a validity period (start date and expiry date), the use of NTP (Network Time Protocol) is mandatory when using the security features.

The Mitel 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 transferred certificate must be in the following format:

- Privacy Enhanced Mail (PEM) (host or others)
- Distinguished Encoding Rules (DER) (others)

When transferring a host certificate, the certificate must be appended to the private key to form one PEM file. The private key must not be encrypted. You can transfer a certificate by using the HTTP or HTTPS protocol, but Media5 recommends to use HTTPS.

When contacting a HTTPS server, the Mitel unit establishes a TLS connection by (among others):

- negotiating cipher suites
- checking the server certificates validity (dates)

To enable a TLS connection on Mitel units, at least one CA certificate is needed to validate that the certificate presented by the server is valid. This certificate must be uploaded to the Mitel units. The Mitel unit then checks the server s identity by validating the host name used to contact it against the information found in the server s certificate. If the validation fails, the Mitel unit refuses the secure

connection. To troubleshoot why a certificate validation has failed, the syslog messages level cna be increased.

For example in a setup for two Mitel 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 units would require a Host certificate. 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.

To be able to use the Wireshark features, a copy of the SIP server certificate containing its private key (this will be used to decrypt the TLS) will be needed. The certificates need to be in ITU X.509 format. The Mitel unit contains embedded security certificates formatted as per ITU x.509 and RFC 3280.

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

openssl

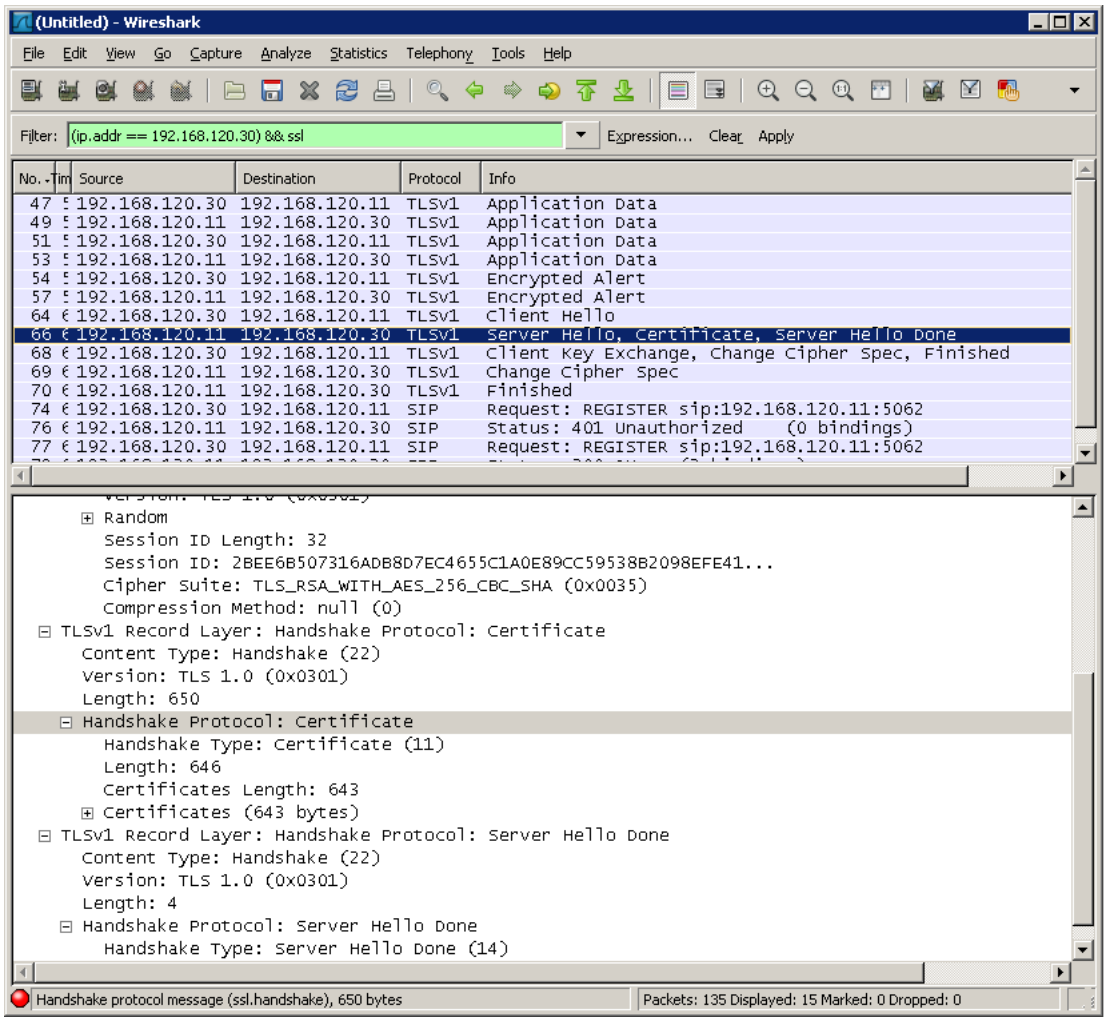
Basics of Security Exchanges

At the level at which we are working, establishing a TLS connection may seems 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 (Mitel) 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.

Enalbing Security Features

Installing Certificates on the Mitel Unit

Prerequisite You must have an SNTP server for time tracking.

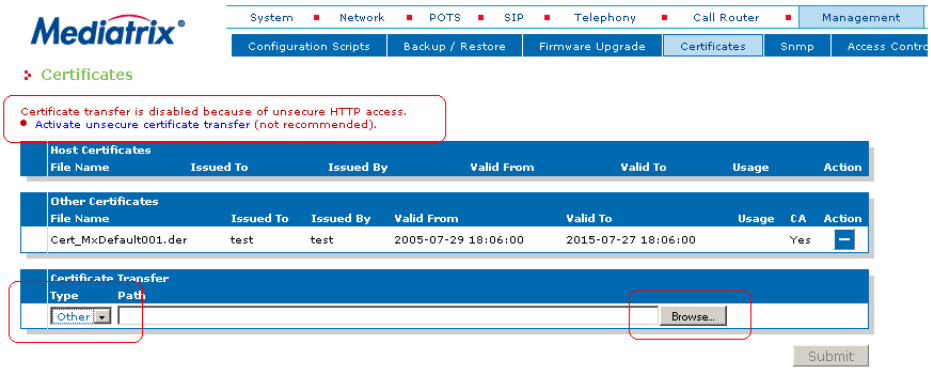
Steps

1. Go to Management>Certificates.
2. ClickActivate unsecure certificate transfer.
3. From the Type dropbox, select Other.
4. Click Browse.

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

5. Click **Restart required services**.

Result:



Adding the OpenSIPS Gateway

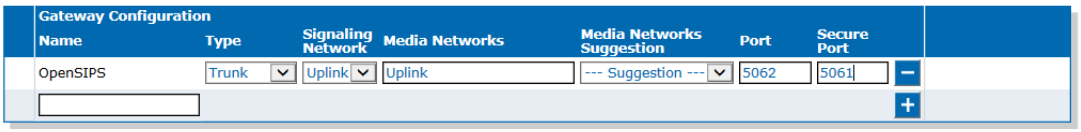
Steps

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.



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 dropbox, 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:

Assigning a Specific Proxy Server to the OpenSIPS Gateway

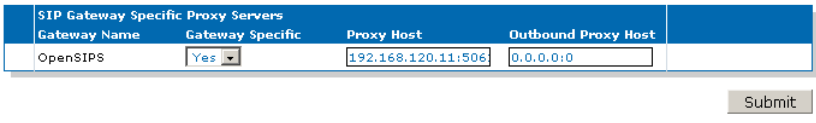
Steps

1. Go to SIP> Servers.
2. In the Proxy Servers table, from the Gateway Specific dropbox, 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:



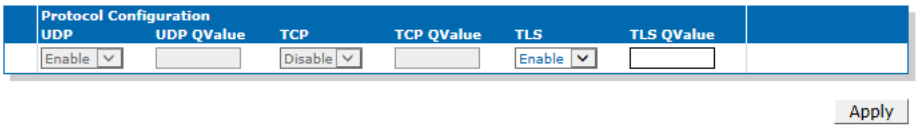
Enabling Secure Signaling (TLS)

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

Steps

1. Go to SIP> Transport tab.
2. In the Protocol Configuration table, TLS dropbox, select Enable.
3. Click Apply.
4. Follow the link located at the top of the web page to start the appropriate service.
5. Please notice the configuration field for the previously discussed port 16000.

Result: On Mitel units of models TA7100, the Ready LED will turn to a steady green. A syslog



message will also be sent saying "establishing persistent connection"

NOTE: The status of the TLS link can also be found under SIP`> Transport page and in the syslog.

Enabling Secure Media (SRTP)

Prerequisite Encrypted/secure signaling must be configured

Steps

1. Go to Media > Security.
2. In the Security table, Mode dropbox, select Secure.
3. From the Key Management Protocol dropbox, select the protocol.

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

4. From the dropbox, select the encryption algorithm.

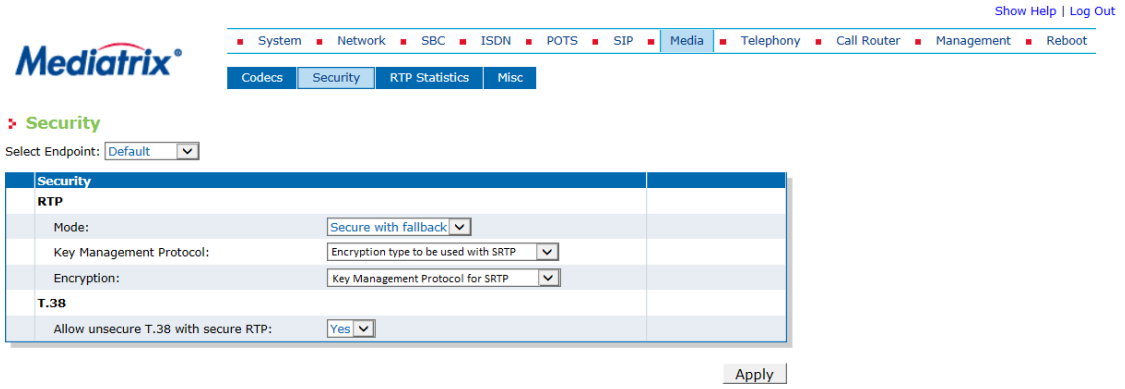
NOTE: The Mitel unit supports AES with 128 bits.

NOTE: The choice "NULL" will not encrypt the RTP. This option should only be selected for debugging purposes.

5. Click Apply

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.

Result: The RTP/SAVP states that the endpoint is attempting to initiate a secure media connection.



Troubleshooting

Enabling TLS Debugging on Wireshark

Prerequisite Wireshark must be configured for TLS sniffing. The public keys associated with the server certificate are needed.

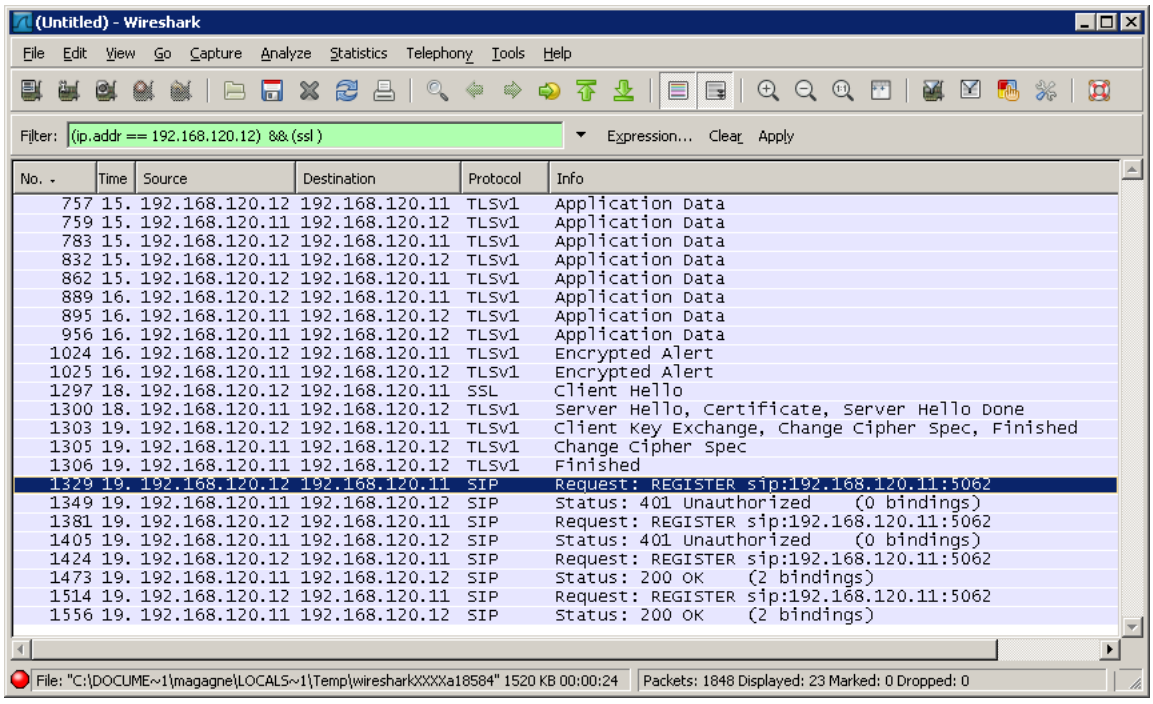
Steps

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 seperating them with a semi-colon ";".

5. Start the Wireshark capture.
6. Restart the SIPEP service on the Mitel unit or reboot the unit.
7. Once the unit is rebooted and the "Ready" LED is lit on the Mitel unit, stop the packet capture.
8. Using the "ssl" filter in the capture should show the SIP packets between the two endpoints.

Result:



REGISTER Messages Not Being Answered

TLS is enabled on one of the Mitel 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.

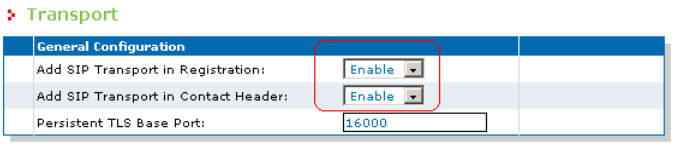
For example, the default openSIPS installation requires adding the SIP transport field in the registration and contact headers.

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. ClickApply.

Result:



Mikey and SDES Mismatch

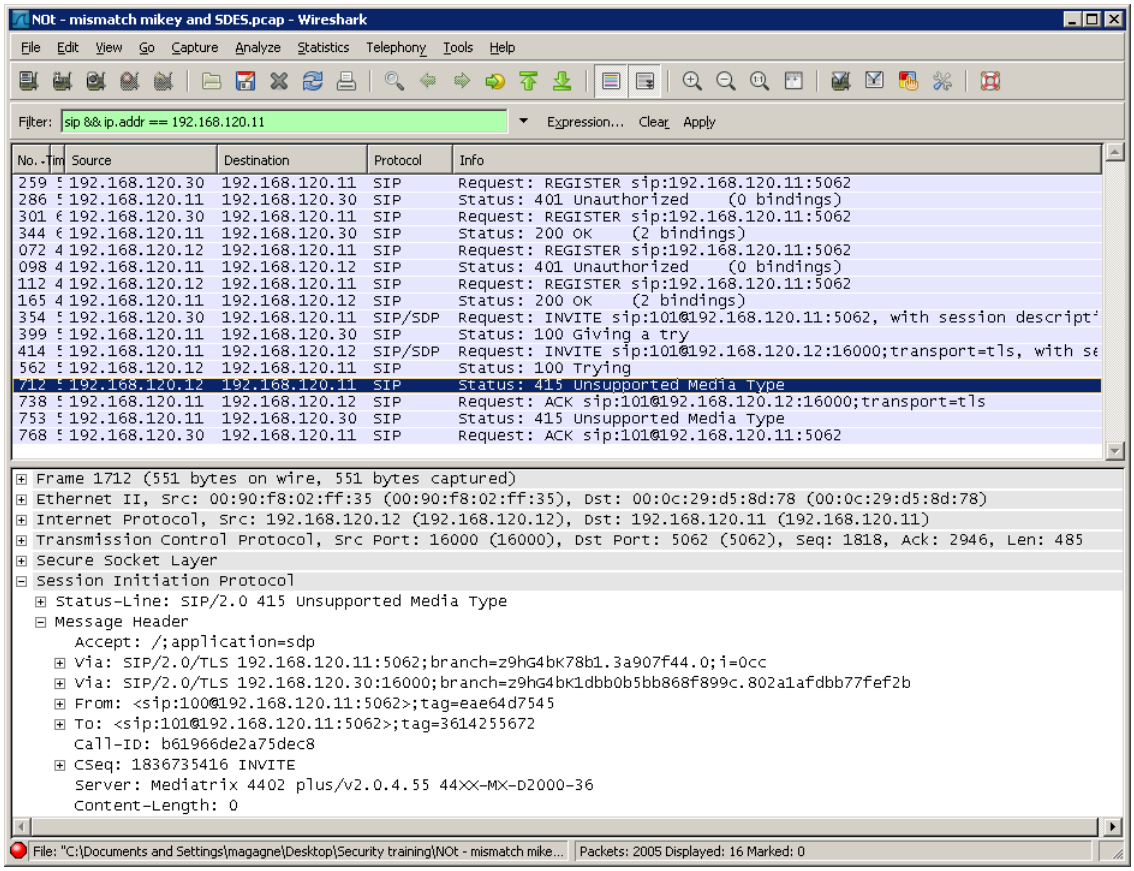
This document explains why it is highly recommended to choose only one single key management protocol.

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.



Annexes

Support Portal

- 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"
```

Mitel
Powering connections

mitel.com