MGU security configuration

OPERATIONAL DIRECTIONS

Mitel®

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

1 GENERAL

1.1 INTRODUCTION

Security methods for the MGU or MGU2 media gateways mean things like port authentication and encryption of both signaling and media. SRTP is supported for media encryption.

See the MGU DESCRIPTION and the MGU2 DESCRIPTION for a general introduction and more details on security for the MGU/MGU2.

1.1.1 GENERAL, ON PORT AUTHENTICATION

The IEEE802.1X standard is used for port access control authentication. The LAN must support IEEE802.1X signaling and there must be an authentication server (i.e. RADIUS) server handling the authentication, according to EAP-TLS. If the authentication is successful, the media gateway gets access to the LAN, and will be accessible by the Service Node.

The Media Gateway supports 802.1x over wired LAN with EAP-TLS as the supported authentication method. The switch port to which the Media Gateway Unit is connected must be configured for 802.1X authentication of multiple hosts. That is, you must be able to connect multiple hosts to this single port for 802.1X authentication. When one client (MGU eth0 - signaling) is authenticated, all the other clients (MGU eth1 - media) are also authenticated for access to the LAN.

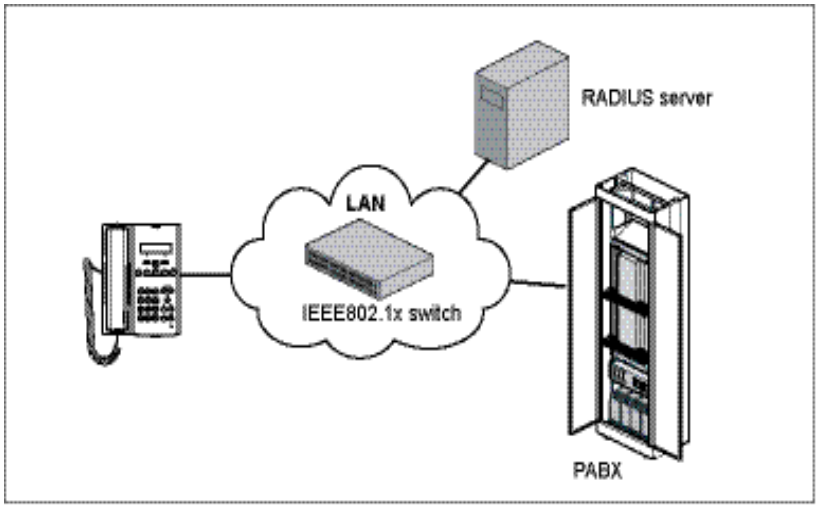

Figure 1: Components involved in the LAN access control

1.1.2 GENERAL, ON IPSEC

IPsec can be used to secure signaling between MGU and a remote IPsec peer (a remote Service Node or Gateway/Firewall). For example, IPsec may be used in a branch node scenario where Service Nodes are located in a head office in a trusted network behind a Firewall (FW) and MGUs in branch offices while signaling over the Internet, as shown by figure below.

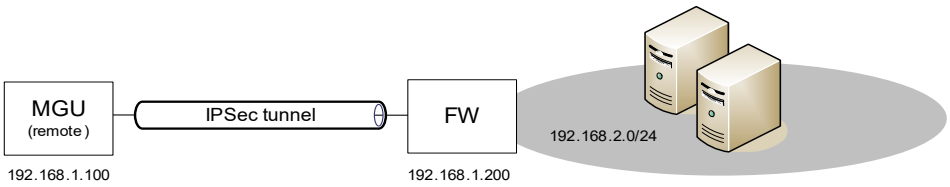

Figure 2: IPsec tunnel example

IPsec may be used to secure all IP datagrams except media (RTP, RTCP, etc.). This includes the Service Node signalling (SCTP protocol on ports 2816-2818), Recorded Voice Announcement (RVA) download from HTTP server on port 80, and SSH login on port 22. It is however, possible to limit the IPsec policy to certain ports or protocols, e.g. securing only Service Node signalling.

IPsec is supported natively by the linux kernel and management of IPsec by the **setkey** and **racoon** commands in the **ipsec-tools** suite. There is a helper command in MGU called **ipsec** that wraps these commands to simplify setup and activation if IPsec. For more advanced or specific IPsec configurations, it might however be needed to manually create or modify a configuration. Refer to manual pages of racoon, racoon.conf, setkey and ipsec for more information about these commands.

Note that you also have to configure the remote IPsec peer device to match the MGU IPsec configuration. Refer to remote peer device's documentation.

Using IPsec will degrade signalling performance in MGU. Most noticeable on signalling latency. Degradation is very much dependent on actual configuration, e.g. chosen algorithms, key-lengths and authentication method.

1.2 GLOSSARY

For a complete list of abbreviations and glossary, see the description for *ACRONYMS, ABBREVIATIONS AND GLOSSARY*.

1.3 REFERENCES

1. **IEEE 802.1X**, an IEEE Standard for port based Network Access Control (PNAC) It is part of the IEEE 802.1 group of networking protocols, and provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
2. **X.509**, an ITU-T Standard for public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.
3. **RFC 2408**, Internet Security Association and Key Management Protocol (ISAKMP).
4. **RFC 2409**, Internet Key Exchange (IKE)
5. **RFC 4302**, IP Authentication Header (AH)
6. **RFC 4303**, IP Encapsulating Security Payload (ESP).

2 PREREQUISITES

2.1 PREREQUISITES, FOR PORT AUTHENTICATION

The following shall be done before executing these operational directions:

- The MGU or MGU2 descriptions shall have been read, especially the security chapters.
- The media gateway does not have a real time clock, which means a “local” NTP server needs to be accessible to set correct time. The time is important when validation on certificates is made.
- An appropriate LAN, an NTP server for time, an IEEE 802.1X switch and a RADIUS server shall be available.
- Before configuration and activation are made, the certificates (root and client certificates) and password (client key) files need to be available. Also the identity string needs to be available.
- Before the authentication, the media gateway only has limited access to the LAN, as decided and configured by the LAN provider. The authentication is performed periodically (intervals as configured on the LAN switch).
- The MGU/MGU2 shall be installed and running.

2.2 PREREQUISITES, FOR IPSEC

The following shall be done before executing these operational directions:

- The MGU or MGU2 descriptions shall have been read, especially the security chapters.
- An NTP server for IPsec shall be available (if IPsec is used).
- For IPsec between Media gateway and Firewall, you also need an IPsec enabled MX-ONE Service Node, Router or Gateway (Firewall), supporting IKE version 1.
- The MGU/MGU2 shall be installed and running.

3 AIDS

I/O terminal.

4 PROCEDURE

4.1 PROCEDURE, FOR PORT AUTHENTICATION

The procedure for the configuration of security in the MGU is like this:

1. Decide which level of security is required for the LAN and the MGUs.
2. Enable automatic port access control.
3. Configure correct date and time (via NTP).
4. Select which security method(s) to use (if any).
5. Configure and activate the security methods (if wanted).
6. Verify the configuration by doing a status check.

4.2 PROCEDURE, FOR IPSEC

To setup an IPsec connection on MGU, the following steps may be taken (similar steps need to be made on remote peer device):

1. Decide peer authentication method; RSA signed keys (certificates) or pre-shared keys.
2. Prepare certificates or pre-shared keys depending on the authentication method chosen.
3. Make sure correct time & date is set on MGU (see section “local NTP configuration”).
4. Decide to use tunnel or transport mode and the scope (policy) of transport/tunnel.
5. Decide which protocols (ESP or AH), crypto and key size, hash algorithms and diffie-hellman group to use for IKE/ISAKMP SA and IPsec SA., or use default settings (ESP with AES-128 and HMAC-SHA1 and DH group 2).
6. Create the IPsec tunnel/transport with the ipsec command.
7. Edit optional settings in generated configuration files.
8. Activate IPsec connection. Note that the IPsec connection is not created until MGU receives IP datagrams matching the IP address, protocol and port matching the configured IPsec policy.
9. Verify connectivity.

For detailed command examples, refer to manual page of the **ipsec** command on MGU.

5 EXECUTION, ENABLING PORT ACCESS CONTROL

5.1 LOCAL NTP CONFIGURATION

5.1.1 GENERAL

On the limited access LAN (before port authentication is made) a local NTP server needs to be accessible to be able to set correct date and time on the media gateway.

To configure local NTP, use the command *localNTP*.

5.1.2 PREREQUISITES

Local NTP server must be accessible.

5.1.3 EXECUTION

1. Key the command *localNTP -a -n <ip-address>*

Example: *localNTP -a -n 192.168.1.10*

See the command on-line help, *localNTP –h*, for details.

5.2 SUPPORTED METHODS

5.2.1 GENERAL

EAP-TLS (Extensible Authentication Protocol, which is part of the IEEE 802.1X Standard) is the preferred and supported method by the media gateway. It can be activated by the *net8021x* command.

Note: Other methods can also be used, but they are not managed by the command *net8021x*, and these methods need to be configured and activated directly by the *wpa_supplicant* command (See “man wpa_supplicant” for details).

When using EAP-TLS the authentication is done with certificates. The digital certificates must be in X.509 version 3 format with the file extension .pem.

The certificates are installed on the media gateway using the *net8021x* command.

See the command on-line help, *man net8021x -h*, for details.

Decide which method to use.

5.2.2 PREREQUISITES

--

5.2.3 EXECUTION

If EAP-TLS shall be used:

1. Key the command *net8021x*.

5.3 CONFIGURATION AND ACTIVATION

5.3.1 GENERAL

5.3.2 PREREQUISITES

Before configuration and activation are made, the certificates (root and client certificates) and password (client key) files need to be available. Also the identity string needs to be available.

5.3.3 ENABLE AUTOMATIC LAN ACCESS CONTROL

Follow the steps below to enable automatic LAN access control on the Media Gateway:

1. Copy the files needed to a temporary directory on the MGU.
2. Enter the *net8021x* command.

Example: *net8021x -l ./clientCert1024.pem -c ./cacert.pem -i test@test.se -p ./privateKey.pem -a*

The command will create a “/etc/wpa_supplicant.conf” file and the security files will be copied to “/etc/wpa_cert” directory. The “/etc/wpa_supplicant.conf” will contain the port authentication configuration referring to the security files residing in “/etc/wpa_cert/” directory.

The command will also configure the *wpa_supplicant* service to be started.
A reboot of the MGU is needed to activate the service after the configuration is done.

5.4 STATUS CHECK

5.4.1 GENERAL

The authentication status can be shown by using the ***wpa_cli*** command.

If an error message is shown, check the following:

- The Radius server is running OK.
- The definition of the root and client certificates is correct in the “/etc/wpa_supplicant.conf” configuration file.
- The definition of the client key and client key password is correct in “/etc/wpa_-supplicant.conf” the configuration file.
- The date and time set on the media gateway is correct (set by the NTP).

5.4.2 PREREQUISITES

5.4.3 EXECUTION

Status check of the port authentication can be made by using the ***wpa_cli -status*** command.

5.4.4 EXAMPLE

Do a status check of the MGU port authentication:

Ex: “**wpa_cli status**”

Output example:

```
Selected interface 'eth0'
bssid=01:80:c2:00:00:03
freq=0
ssid=
id=0
mode=station
pairwise_cipher=NONE
group_cipher=NONE
key_mgmt=IEEE 802.1X (no WPA)
wpa_state=COMPLETED
ip_address=10.105.68.5
address=00:08:5d:79:1f:3e
Supplicant PAE state=AUTHENTICATED
suppPortStatus=Authorized
EAP state=SUCCESS
selectedMethod=13 (EAP-TLS)
EAP TLS cipher=ECDHE-RSA-AES256-SHA
```

6 EXECUTION, ENABLING IPSEC

6.1 ENABLING IPSEC (SECURE SIGNALING)

6.1.1 CREATE, ACTIVATE OR REMOVE IPSEC CONFIGURATIONS

The **ipsec** command with switches **--create** and **--name=nickname** are used to create a new IPsec configuration. The nickname may contain letters [a-z,A-Z] and numbers [0-9]. The configuration is activated at next MGU re-boot, or optionally activated immediately by using the --start switch.

To remove a IPsec configuration, use **--remove** --name=nickname switch. An active IPsec connection can be deactivated with the **--stop** switch.

6.1.2 IPSEC SCOPE (POLICY)

The IPsec policy may be applied for IP datagrams between a source IP address (MGU) and a destination IP address or network. The policy is by default applied for all ports (TCP/UDP) and IP protocols, but may be limited to certain ports and/or protocols. For initial configuration it might be useful to limit the policy to the SCTP signalling protocol to allow SSH login for instance.

Source address is by default the MGU eth0 IP address, destination address and network is specified with the ipsec command switches **--dst-address=address** and **--dst-network=CIDR**, respectively.

Source and destination ports is specified with switch **--src-port=PORT** and **--dst-port=PORT**. Protocol is specified with **--ip-proto=IPPROT** (number or name according to /etc/protocols).

See also “Tunnel or Transport Mode” below.

6.1.3 TUNNEL OR TRANSPORT MODE

Tunnel mode is usually used if the remote (destination) side is a (VPN) gateway, router or firewall that terminates the IPsec connection (IPsec SA), and where Servers on remote side are in a trusted network. When tunnel mode is used then all IP traffic to and from MGU and the specified network is secured (unless limited policy is applied), thus after enabling the tunnel there is no chance to login to MGU in case tunnel failed. During initial installation it is recommended to verify IPsec with transport first, and then change to tunnel mode if needed.

An IPsec SA in tunnel mode is created by the ipsec command if a destination network is specified, using the switch **--dst-network=CIDR.** Note that you may specify for example 192.168.1.100/32 to imit the the tunnel to one destination address (192.168.1.100).

Transport mode is usually used if the remote (destination) is a Service Node that terminates the IPsec connection (IPsec SA). In transport mode then only the IP traffic between the MGU and destination is secured, thus it is possible to connect (insecure) from another host even if the IPsec transport fails to establish.

An IPsec SA in transport mode is created by the ipsec command if only a destination address is specified, using the switch **--dst-address=ADDR**, for example –dst-address=192.168.1.100. The switch --dst-network shall not be used in this case.

6.1.4 PRE-SHARED KEYS

The ipsec command may be used to set pre-shared keys for local (MGU) and remote peer. There should be one key-phrase for the remote peer and one for MGU. It is recommended to use different keys on local (MGU) and remote peer.

To set keys with ipsec, add switches **--src-preshared-key=KEYPHRASE** for MGU key and **--dst-preshared-key=KEYPHRASE** for remote peer key.

Note that there may only be one key per peer and only one key per MGU (latest defined keys will override). It is also possible to edit keys by hand in the pre-shared keys file (see files section) which may be recommended to avoid traces of the keys in history logs, etc. Refer to man page of ipsec command for more information.

6.1.5 DIGITAL CERTIFICATES

The ipsec command may be used to install and update digital certificates (X.509) when using RSA signed keys as authentication method. Note that certificates for IPsec must be stored in PEM file format, but it is possible to convert from other formats using the openssl command. Using the openssl command it is also possible to create self-signed certificates as well.

There should be three PEM formatted files that needs to be copied to MGU: The public part of the trusted CA certificate, and the public and private parts of the client certificate (MGU certificate).

First time installation of certificates might have to be done off-line (e.g. in a safe environment). The command will copy the files to a pre-configured directory (see “IPsec configuration files”).

Certificates have to be updated before they expire. If not, the IP connectivity to the MGU will be lost and on-site configuration is needed.

To install certificates, use ipsec command with the **--install-certs** switch:

ipsec --install-certs --ca-cert-file=CA_PEM_file --cert-file-public=MGU_public_PEM_file --cert-file-private=MGU_private_PEM_file to install in IPsec (racoon) certificate directory. Filenames may include a relative or absolute path. Note that you may use the --install-certs switch in conjunction with the ipsec --create command, to install certs and create IPsec configuration in one command. You may also omit the --install-certs switch to use certificates from the pre-configured certificate location.

6.1.6 OPTIONAL SETTINGS

There are further IP configurations that cannot be made with the ipsec command, in case default settings is not sufficient. For instance, changing lifetime, crypto, hash-alogrithm, etc. for IPsec SAs.

These configurations shall be made directly in common and generated configuration files (see “IPsec configuration files”).

For further information how to edit these files, refer to man page of racoon.conf.

6.1.7 VERIFYING IPSEC CONNECTIVITY

When the IPsec tunnel/transport has been started with the ipsec command, it is recommended to verify that the tunnel/transport is working properly. There are many ways to do accomplish this, and optionally you might verify connectivity from remote device (e.g. the VPN gateway), thus steps below is just an example:

- From remote peer, send IP packets to MGU, e.g. using ping. There might be some lost packets or “unreachable destination” before IPSec is established. Note: Since MGU is server, the remote peer is normally the IPsec initator, hence it is important to verify IPsec activation in this direction to avoid later IPsec proposal mismatch issues.
- On MGU, use “racoonctl -ll show-sa isakmp” to check IKE/ISAKMP SA (show-sa isakmp) has been established. Using -l or -ll gives some more information.
- On MGU, use “racoonctl show-sa ipsec” to check that bytes has been sent in both directions of the IPSec SA (there is one SA in each direction between MGU and IPsec destination).
- Verify that connection with the MX-ONE Service Node can be made.

```
root@localhost:/home/admin> racoonctl -ll show-sa isakmp

Destination             Cookies                                 Created
10.105.68.60.500        022365d924ef0519:703f9ee98023afd3       2015-05-04 12:37:21


root@localhost:/home/admin> racoonctl show-sa ipsec
10.105.68.54 10.105.68.60

esp mode=transport spi=266192963(0x0fddc843) reqid=0(0x00000000)
        E: aes-cbc  bc31a0ac 98924ff1 585d6413 fbedb274
        A: hmac-sha1  89e1acea f22af30f 7d6dde47 139e1846 f18fb283
        seq=0x00000000 replay=4 flags=0x00000000 state=mature
        created: May  4 14:05:30 2015   current: May  4 14:05:38 2015
        diff: 8(s)      hard: 3600(s)   soft: 2880(s)
        last: May  4 14:05:31 2015      hard: 0(s)      soft: 0(s)
        current: 544(bytes)     hard: 0(bytes)  soft: 0(bytes)
        allocated: 4    hard: 0 soft: 0
        sadb_seq=1 pid=6456 refcnt=0
10.105.68.60 10.105.68.54
        esp mode=transport spi=130192034(0x07c292a2) reqid=0(0x00000000)
        E: aes-cbc  75fbb2f7 c5825b8a 15627523 d2c16aac
        A: hmac-sha1  45d50236 212c3a5d 95794eba 408315c9 35021937
        seq=0x00000000 replay=4 flags=0x00000000 state=mature
        created: May  4 14:05:30 2015   current: May  4 14:05:38 2015
        diff: 8(s)      hard: 3600(s)   soft: 2880(s)
        last: May  4 14:05:31 2015      hard: 0(s)      soft: 0(s)
```

current: 256(bytes) hard: 0(bytes) soft: 0(bytes)

allocated: 4 hard: 0 soft: 0

sadb_seq=0 pid=6456 refcnt=0

Also the MGU syslog file (/var/log/syslog) contains information about successful establishment of ISAKMP SA and IPsec SAs:

May 5 06:05:39 localhost racoon: INFO: ISAKMP-SA established 10.105.68.54[500]-10.105.68.60[500] spi:ef50162240d3ea63:3a19910510ef8700

May 5 06:05:40 localhost racoon: INFO: initiate new phase 2 negotiation: 10.105.68.54[0]<=>10.105.68.60[0]

May 5 06:05:40 localhost racoon: INFO: IPsec-SA established: ESP/Transport 10.105.68.60[0]->10.105.68.54[0] spi=227461701(0xd8eca45)

May 5 06:05:40 localhost racoon: INFO: IPsec-SA established: ESP/Transport 10.105.68.54[0]->10.105.68.60[0] spi=139048678(0x849b6e6)

If there is a failure to establish the IPsec connectivity with peer, then the syslog file may be checked for errors. Many issues can be solved this way. To pinpoint an issue further it might also be useful to increase log level in racoon.conf file as explained in its man page (note however that increasing log level will have negative impact on performance, and is some cases IKE negotiation might fail due to timeouts).

6.1.8 IPSEC CONFIGURATION FILES

The following file contains common settings for IPsec configurations:

/etc/racoon.conf

The following files are created for each IPsec configuration:

/etc/racoon/**remote-address.conf**

/etc/sysconf/network-scripts/ifcfg**-nickname**

Pre-shared key for a configuration is stored as an entry (there is one entry per host, including MGU) in:

/etc/racoon/psk.txt

Digital (X.509) certificates, public and private parts are stored as PEM files in:

/etc/racoon/certs/

It is important that the pre-shared key file and the PEM files with private keys are kept inaccessible for other users than root.

7 TERMINATION

Inform the department or person responsible for telephony matters if any alteration of the security configuration is made.

Since MGU data have been changed, a reboot of the MGU shall be done.