

Connecting Devices

Description of options for connecting various routers (Mikrotik, Zyxel Keenetic, etc.) to SafeUTM for site-to-site VPN using IPsec IKEv2 protocol.

Devices that are not described in this manual as a rule can be connected using similar settings.

When combining networks using a VPN, LANs in different offices should not overlap.

The choice of crypto algorithms on remote devices.

When configuring third-party devices, you must explicitly specify the crypto algorithms used for the connection. SafeUTM supports the most up-to-date and at the same time sufficiently secure algorithms that do not load the server and devices. At the same time, outdated algorithms and those considered unsafe (MD5, SHA1, AES128, DES, 3DES, Blowfish, etc.) are not supported. When configuring third-party devices, as a rule, you can enter several supported algorithms at the same time. In fact, one algorithm of each kind is needed. Unfortunately, not all devices support the best algorithms, so SafeUTM supports several at once. Find below the list of algorithms of each type in descending order of priority for selection.

- **Phase 1 (IKE):**

- encryption:
 - **AES256-GCM**
 - **AES256**
- integrity (hash):
 - for **AES256-GCM** - not required, since integrity check is built into AEAD algorithms.
 - for **AES256**, by priority: **SHA512, SHA256**.
- prf (random value generation function):
 - as a rule, it is configured automatically, depending on the choice of integrity algorithms (therefore, in the example below, the value of prf is PRF-HMAC-SHA512).
 - for AES-GCM, you may need to specify explicitly. In this case, by priority: **AESXCBC, SHA512, SHA384, SHA256**.
- DH (Diffie-Hellman Group):
 - **Curve25519 (group 31)**
 - **ECP256 (group 19)**
 - **modp4096 (group 16)**
 - **modp2048 (group 14)**

- **modp1024 (group 2)**
- Timeouts:
 - **Lifetime:** 14400 seconds
 - **DPD Timeout** (for L2TP/IPsec): 40 seconds
 - **DPD Delay:** 30 seconds
- **Phase 2 (ESP):**
 - encryption:
 - **AES256-GCM**
 - **AES256**
 - integrity:
 - for **AES256-GCM** - not required, since integrity check is built into AEAD algorithms
 - for AES-256, by priority: **SHA512, SHA384, SHA256**
 - DH (Diffie-Hellman Group, PFS). **ATTENTION! if not specified, it will connect, but rekey will not work after a while:**
 - **Curve25519 (group 31)**
 - **ECP256 (group 19)**
 - **modp4096 (group 16)**
 - **modp2048 (group 14)**
 - **modp1024 (group 2)**
 - Timeouts:
 - **Lifetime:** 3600 seconds

Example

- **Phase 1 (IKE)** (one of the lines is needed):
 - AES256-GCM\PRF-HMAC-SHA512\Curve25519
 - AES256\SHA512\PRF-HMAC-SHA512\ECP384
 - AES256\SHA256\PRF-HMAC-SHA256\MODP2048
- **Phase 2 (ESP)** (one of the lines is needed):
 - AES256-GCM\ECP384
 - AES256\SHA256\MODP2048

An example of setting up a pfSense connection to SafeUTM via IPsec is shown in the screenshots below:

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm

AES256-GCM

Algorithm

128 bits

Key length

SHA512

Hash

31 (Elliptic Curve 25519, 256 bit)

DH Group

Delete

Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm

+ Add Algorithm

Phase 2 Proposal (SA/Key Exchange)

Protocol

ESP

Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.

Encryption Algorithms

☐ AES

128 bits

☐ AES128-GCM

128 bits

☐ AES192-GCM

Auto

☒ AES256-GCM

128 bits

☐ Blowfish

Auto

☐ 3DES

☐ CAST128

Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.

Hash Algorithms

☐ MD5

☐ SHA1

☒ SHA256

☐ SHA384

☐ SHA512

☐ AES-XCBC

Note: Hash is ignored with GCM algorithms. MD5 and SHA1 provide weak security and should be avoided.

PFS key group

31 (Elliptic Curve 25519, 256 bit)

Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Connecting SafeUTM to MikroTik Using PSK

If there is a public IP address on the MikroTik device, follow the steps below to configure the SafeUTM connection to MikroTik.

Step 1.

Setting up SafeUTM

1. In SafeUTM, open the tab **Services -> IPsec -> Devices**, click on the icon (+), and fill in the following fields:

• **Connection name** - specify an arbitrary name for the connection. Maximum 42 characters.

• **Connection type** - select **Outcoming**, since the connection is made from UTM to MikroTik.

• **Remote device address** - specify the external IP address of the MikroTik device.

- **Authentication type** - select the **PSK**
- **PSK** - a random PSK key will be generated. You will need it to set up a connection in MikroTik.
- **UTM identifier** - the key you enter will be used to identify the outgoing connection.
- **Home local network** - list all **UTM LANs** that will be available in an IPsec connection, i.e. will be visible to the opposite side.

- **Remote local networks** - list all **MikroTik LANs** that will be available in an IPsec connection, i.e. will be visible to the opposite side.

IPsec

Head office

Branch office

Devices

Connection name

Test connection

Connection type

☒ Outcoming

Connect Safe UTM to remote device

☐ Incoming

Connect remote device to Safe UTM

Remote device address

172.16.150.4

For example, 198.168.32.10 or example.com

Authentication type

☐ Certificate

Provides a high level security, but is not supported by some devices

☒ PSK

Provides a low level security, supported by most devices

PSK

]XMH7ov^eWn\+D,A~-Q{Oixd#R,tu*



UTM identifier

test_key_id

Depends on the settings of the remote device.

Home local network

192.168.105.0/24

Subnet

Add

Remote local networks

192.168.105.0/24

Subnet





Add

Add connection

Cancel

2. After filling in all the fields, click **Add connection**. Your connection will appear in the list of connections:

IPsec



Head office




Branch office

Devices

Here you can configure an IPsec connection between Safe UTM and remote devices

+ Add

Outcoming connections:

Title	Statuses	Operations
Test connection	<div>off</div> 172.16.150.4	  

Step 2.

You can configure the MikroTik device in several ways - through the GUI, and through the device console.

Connecting MikroTik to SafeUTM Using PSK

If there is a public IP address on SafeUTM, follow the steps below to configure the connection of the MikroTik device to SafeUTM.

Step 1.

You can configure the MikroTik device in several ways - through the GUI, and through the device console

Step 2.

Setting up SafeUTM

1. In SafeUTM, open the tab **Services -> IPsec -> Devices**, click on the icon (+), and fill in the following fields:

- **Connection name** - specify an arbitrary name for the connection. Maximum 42 characters.
- **Connection type** - select **Incoming**, since the connection to UTM is being made.
- **Authentication type** - select the PSK type.
- **PSK** - insert the PSK key received from MikroTik.

- **Remote side identifier** - insert the MikroTik ID (Key ID parameter in `/ip ipsec peers`).
- **Home local network** - list all **UTM LANs** that will be available in an IPsec connection, i.e. will be visible to the opposite side.

- **Remote local networks** - list all MikroTik LANs that will be available in an IPsec connection, i.e. will be visible to the opposite side.

IPsec

Head office

Branch office

Devices

Connection name

Test

Connection type

☐ Outcoming

Connect Safe UTM to remote device

☒ Incoming

Connect remote device to Safe UTM

Authentication type

☐ Certificate

Provides a high level security, but is not supported by some devices

☒ PSK

Provides a low level security, supported by most devices

PSK

sdffeSFjHFJNEH

Remote side identifier

test_key_id

For inbound connection identification

Home local network

192.168.105.0/24

Subnet

Add

Remote local networks

192.168.100.0/24

Subnet

Add

Add connection

Cancel

2. After filling in all the fields, click **Add connection**. Your connection will appear in the list of connections.

IPsec

2

Head office

Branch office

Devices

Here you can configure an IPsec connection between Safe UTM and remote devices

+ Add

Incoming connections:

Title	Statuses	Operations
Test	Off	<div></div> <div></div> <div></div>

Connecting SafeUTM to MikroTik Using Certificates

Connection with certificates is used because it is more secure than a PSK connection, or in cases when the device does not support PSK.

For the correct operation of certificate connections, it is necessary that the time on MikroTik be synchronized via NTP. To do this, it is sufficient for the device to have access to the Internet.

The creation of outgoing IPsec connections using certificates to MikroTik below version 6.45 does not work due to the inability to use modern crypto algorithms in certificates.

Step 1.

Setting up SafeUTM

1. In SafeUTM, open the tab **Services -> IPsec -> Devices**, click on the icon (+), and fill in the following fields:

- **Connection name** - specify an arbitrary name for the connection. Maximum 42 characters.
- **Connection type** - select **Outcoming**, because the connection is made from UTM.
- **Authentication type** - specify the type of **Certificate**.
- **Address of the remote device** - specify the external IP address of MikroTik.

- **Certificate signing request**

Provides a high level security, but is not supported by some devices

☐ PSK

Provides a low level security, supported by most devices

Certificate signing request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBIjCBYQIBADBWMQ4wDAYDVQQKDAVJZG
VjbzEMMAoGA1UECwwDVVRNMTYwNAYD
VQQDDC1kZXZpY2VfNWQwNmZhY2E0MDU3
NGFhYWJhNDdmNDgxZTJkMWFhMTEuaXBz
ZWMwWTATBgqhkhjOPQIBBgqhkhjOPQM
BBwNCAATIdAvmxlkkCFJ+u3YDB8ItI+61
mQk7BtqmnZelh8rv36gkyaJRC1y2y3h76XaW
mguzKLv6DV+fYQU/RLON7o3LoBEw
DwYJKoZIhvcNAQkOMQIwADAKBggqhkhjOPQ
```



The UTM.csr file must be sent for signing to the remote device

MikroTik for signing.

2. After the request is signed, you will need to continue configuring the connection in SafeUTM.

Do not close the settings tab!

Step 2.

Setting up MikroTik

At this stage, you should configure MikroTik to continue configuring UTM.

The **UTM.csr** file obtained from SafeUTM must be uploaded to the MikroTik file storage. To do this, open the **File** section, click **Browse**, select the file and upload it.

You can configure MikroTik in several ways - through the GUI, and through the device console.

Two files will appear in the MikroTik file system which you need to download in order to upload to UTM later.

	UTM.crt	.crt file	1000 B	Sep/25/2018 10:46:59	Download
	cert_export_device_712c6384ca0c4b378d727f6ff2a5d4cb.ipsec.crt	.crt file	1208 B	Sep/25/2018 10:46:59	Download
	cert_export_mk_ca.crt	.crt file	1184 B	Sep/25/2018 10:46:59	Download

The file of the type `cert_export_device_<random character set>.ipsec.crt` is a **signed UTM certificate**. The file of the type `cert_export_mk_ca.crt` is **the root certificate of MikroTik**.

At this point, the MikroTik setup can be considered complete.

Step 3.

Finishing up the SafeUTM setup

Go back to SafeUTM to the tab with the device connection settings and continue filling in the following fields:

- **Signed UTM certificate** - upload a signed UTM certificate to MikroTik.
- **Remote Device Root Certificate** - download the MikroTik root certificate.
- **Home local networks** - list all **UTM LANs** that will be available in an IPsec connection, i.e. will be visible to the opposite side.

- **Remote local networks** - list all **MikroTik local networks** that will be available in an IPsec connection, i.e. will be visible to the opposite side.

Signed UTM certificate

```
ZWMmWTATBgcqhkJOPQIBBggqhkJOPQMBB
wNCAATIdAvmxlkkCFJ+u3YDB8ItI+61
mQk7BtqmnZelh8rv36gkyaJRC1y2y3h76XaW
mguzKLv6DV+fYQU/RLON7o3LoBEw
DwYJKoZihvcNAQkOMQIwADAKBggqhkJOPQ
QDAgNIADBFAiAuLNhNIZ0OGAUY4IeJ
S0NzNDZaI2OX2nuQR84m/5GJ9QlhAJ+5g+p
uD7Ibl+xgvuA7Yk2LI/1rUjhXUpzx
4UjFpye1
-----END CERTIFICATE REQUEST-----
```

↑ Upload

Remote device root certificate

```
ZWMmWTATBgcqhkJOPQIBBggqhkJOPQMBB
wNCAATIdAvmxlkkCFJ+u3YDB8ItI+61
mQk7BtqmnZelh8rv36gkyaJRC1y2y3h76XaW
mguzKLv6DV+fYQU/RLON7o3LoBEw
DwYJKoZihvcNAQkOMQIwADAKBggqhkJOPQ
QDAgNIADBFAiAuLNhNIZ0OGAUY4IeJ
S0NzNDZaI2OX2nuQR84m/5GJ9QlhAJ+5g+p
uD7Ibl+xgvuA7Yk2LI/1rUjhXUpzx
4UjFpye1
-----END CERTIFICATE REQUEST-----
```

↑ Upload

Home local network

192.168.100.0/24

Subnet

Add

Remote local networks

192.168.105.0/24

Subnet

Add

Add connection

Cancel

After filling in the fields, click **Add connection**. Your connection will appear in the list of connections.

Connecting MikroTik to SafeUTM by certificates

Connection with certificates is used because it is more secure than a PSK connection, or in cases when the device does not support PSK.

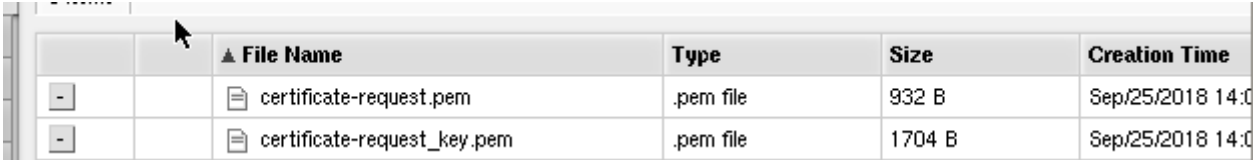
For the correct operation of certificate connections, it is necessary that the time on MikroTik be synchronized via NTP. To do this, it is sufficient for the device to have access to the Internet.

Step 1.

Setting up MikroTik

You can configure MikroTik in several ways - through the GUI, and through the device console.

Two files will appear in the MikroTik file storage which must be downloaded since they are required for further configuration.:



	▲ File Name	Type	Size	Creation Time
-	certificate-request.pem	.pem file	932 B	Sep/25/2018 14:0
-	certificate-request_key.pem	.pem file	1704 B	Sep/25/2018 14:0

- File `certificate-request.pem` is a **certificate signing request**.
- File `certificate-request_key.pem` is a **private key**.

Next, you will need to fill in the **Certificate Signing Request** field in SafeUTM, here is how to configure it.

Step 2.

Setting up SafeUTM

1. In SafeUTM, open the tab **Services -> IPsec -> Devices**, click on the icon (+), and fill in the following fields:

- **Connection name** - specify an arbitrary name for the connection. Maximum 42 characters.
- **Connection type** - select **Incoming**, since the connection to UTM is being made.
- **Authentication type** - select the type **Certificate**.
- **Certificate Signing Request** - Upload the signature request **received from MikroTik**.

- **Home local network** - it is necessary to list all UTM LANs that will be available in an IPsec connection, i.e. they will be visible to the opposite side.

Connection name

Test

Connection type

☐ Outcoming

Connect Safe UTM to remote device

☒ Incoming

Connect remote device to Safe UTM

Authentication type

☒ Certificate

Provides a high level security, but is not supported by some devices

☐ PSK

Provides a low level security, supported by most devices

Certificate signing request

```
ZWMwWTATBgqhkjOPQIBBggqhkjOPQMBB
wNCAAQevvXoFOsEAoSKUS6HMyKrHAS1
8KJtemzkip/9iUeX/b/y0bPuzSqWAGgUjmOiua
dxS0aXLnKCRpiafwBKX6SDHoBEw
DwYJKoZlHvcNAQkOMQIwADAKBgqhkjOPQ
QDAgNHADBEAiAISHrx225H3A26JuWs
fwHS0yHA0zWkhLXzZNxDWjTWQAIGBl00hvZ
qwOCKZZnioOXM/Rn+dnU1XcTyHqS2
WRjImcl=
-----END CERTIFICATE REQUEST-----
```

↑ Upload

Home local network

192.168.100.0/24

Subnet

Add

Remote local networks

192.168.105.0/24

Subnet

Add

Add connection

Cancel

2. After the settings, click **Add connection**. Your connection will appear in the list of connections. Click on the edit connection button to continue the setup.

IPsec

2

Head office

Branch office

Devices

Here you can configure an IPsec connection between Safe UTM and remote devices

+ Add

Incoming connections:

Title	Statuses	Operations
Test	Off	<div><div></div><div></div><div></div></div>



3. The connection settings editing area will appear. You need to download the files that are in the fields **UTM root certificate** and **Signed device certificate** for their subsequent use in MikroTik.

Head office

Branch office

Devices

Connection name

Test

UTM root certificate

```
-----BEGIN CERTIFICATE-----
MIIBuTCCAWCgAwIBAgIUUNHPvEj0gBmWCV
w0eEzzboAs6DPQwCgYIKoZIzj0EAwIw
LDEXMBUGA1UEBRMOMjAyMjA4MzEyMzI1N
TQxETAPBgNVBAMMCElkZWVVRNMB4X
DTlyMDgzMDIzMDU1NFoXDUMyMDgyODIzMD
U1NFowLDEXMBUGA1UEBRMOMjAyMjA4
MzEyMzI1NTQxETAPBgNVBAMMCElkZWVVR
NRNMFkwEwYHKoZIzj0CAQYIKoZIzj0D
AQcDQgAAEMjCQXdcEOYn3eCqmzY0LPbw1Q
```



The UTM.crt file must be sent to the remote device

Signed device certificate

```
-----BEGIN CERTIFICATE-----
MIIBgTCCASigAwIBAgIUUDTDc+4CxZGKdU5o
GQr/9sR5l4RQwCgYIKoZIzj0EAwIw
LDEXMBUGA1UEBRMOMjAyMjA4MzEyMzI1N
TQxETAPBgNVBAMMCElkZWVVRNMB4X
DTlyMDgzMDE2MjU1NFoXDUMyMDgyODE2M
jU1NFowVjEOMAwGA1UECgwFSWRIY28x
DDAKBgNVBAsMA1VUTTE2MDQGA1UEAwwt
ZGV2aWNlX2Q4YTJlNmU4ZDZlMTRkOTU5
ZjEyZTFjZTBiMGU3YzlmLmlwc2VjMFkwEwY
```



The device.crt file must be sent to the remote device

Home LANs:

- 192.168.100.0/24

Remote local networks:

- 192.168.105.0/24

Remote side identifier:

-

Save

Cancel

Problems when reactivating an incoming connection to SafeUTM

If after using this connection you turned it off, for example, as unnecessary, and when trying to re-enable the connection failed to be established, then most likely the remote device got into fail2ban (a tool that tracks attempts to access services in log files, and if it finds repeated unsuccessful authorization attempts from the same IP-address or host, it blocks further attempts).

Connecting Mikrotik to SafeUTM via L2TP/IPsec

Configure the connection by running the following commands:

1. Edit the IPsec profile:

```
ip ipsec profile set default hash-algorithm=sha1 enc-algorithm=aes-256 dh-group=modp2048
```

2. Edit IPsec proposals:

```
ip ipsec proposal set default auth-algorithms=sha1 enc-algorithms=aes-256-cbc, aes-192-cbc, aes-128-cbc pfs-group=modp2048
```

3. Create a connection to SafeUTM:

```
interface l2tp-client add connect-to={server} profile=default disabled=no  
name={interface_name} password="{password}" user="{login}" use-ipsec="yes" ipsec-  
secret="{psk}"
```

Revision #5

Created 27 August 2022 14:08:07 by Val Redman

Updated 13 October 2022 15:32:15 by Val Redman