

Mikrotik IKEv2 client configuration

[Order now](#) | [Download](#) | [FAQ](#)

Configuring Mikrotik as an IKEv2 Client.

Make sure you have an up to date routerOS system.

Version must be at least: 6.49.7

```
[admin@VPN-CLIENT] > system package print
Flags: X - disabled
#   NAME                                VERSION
SCHEDULED
0   ntp                                6.49.7
1   ppp                                6.49.7
2   dhcp                                6.49.7
3   mpls                                6.49.7
4   security                            6.49.7
5   advanced-tools                      6.49.7
6   system
```

```

6. 49. 7
7   openflow
6. 49. 7
8   multicast
6. 49. 7
9   routing
6. 49. 7

```

Open a one-time link to obtain authorization data and a root certificate.

Download the certificate and place it on the Mikrotik router using the Winbox program

Import the certificate into the system

To create an IKEv2 connection, we will use the console

Open a terminal and enter the following commands

Replace the authorization data with the data that is in the one-time link

the example contains the following data. You need to replace them with your own.

Name	Issuer	Common Name	Subject Alternative Name	Key Size	Days Valid	Trusted	SCEP
dev.softkeel.com.crt_0	CN=PUQ VPN,O=PUQ sp. z o.o.,OU=PUQ VPN,L=Warszaw,C=PL	PUQ VPN		4096	3650	yes	

Import dialog box:

Name:

File Name:

Buttons: Import, Cancel

It is a strong recommendation to use only the terminal command line in setup. We encountered cases when, during the configuration of Mikrotik through *winbox*, some parameters were not correctly entered into the configuration. Commands entered through the terminal are always correctly processed.

```

/ip ipsec settings
set accounting=no
/ip ipsec mode-config
add name=MY_VPN responder=no

```

```

/ip ipsec policy group
add name=MY_VPN

/ip ipsec profile
add dh-group=modp1024 enc-algorithm=aes-256 name=MY_VPN

/ip ipsec peer
add address=dev.softkeel.com exchange-mode=ike2 name=MY_VPN profile=MY_VPN

/ip ipsec proposal
add name=MY_VPN pfs-group=none

/ip ipsec policy
add dst-address=0.0.0.0/0 group=MY_VPN proposal=MY_VPN src-address=0.0.0.0/0 template=yes

/ip ipsec identity
add auth-method=eap \
eap-methods=eap-mschapv2 generate-policy=port-strict \
mode-config=MY_VPN \
peer=MY_VPN policy-template-group=MY_VPN \
certificate=dev.softkeel.com.crt_0 \
my-id=user-fqdn:mikrotik \
username=mikrotik \
password=NX9%B3&3YG

```

After the work done, you can see the connection status in the IP->IPsec configuration

You also need to configure the traffic routes you need at your discretion.

The screenshot shows the Mikrotik WinBox interface. The main window is titled 'IPsec Remote Peer <77.87.125.200>' and displays the configuration for a remote peer. The 'ID' field is set to 'dev.softkeel.com'. The 'State' is 'established'. The 'Remote Port' is '4500'. The 'Dynamic Address' is '0.0.0.0'. The 'Side' is 'initiator'. The 'Uptime' is '00:01:07'. The 'Last Seen' is '00:01:06'. The 'PH2 Total' is '1'. The 'Tx/Rx Bytes' are '67 / 99'. The 'Tx/Rx Packets' are '1 / 1'. The 'Terminal' window at the bottom shows the command 'show ipsec peers' and the output '1 item (1 selected)'. The 'Address List' window is also open, showing a table with columns 'Address', 'Network', and 'Interface'. The table contains two entries: '10.0.110.14/24' with network '10.0.110.0' and interface 'bridge1', and '192.168.129.2...' with network '192.168.129.0' and interface 'bridge1'.

Address	Network	Interface
10.0.110.14/24	10.0.110.0	bridge1
192.168.129.2...	192.168.129.0	bridge1