

Mikrotik preparation and configuration

Mikrotik WireGuard VPN module **WISECP**

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

Note: **Enter the following commands one by one and wait for the command to complete.**

Check RouterOS version

Make sure that the version of RouterOS is 7+

```
system/package/print
```

Enabling HTTPS Create your own root CA on your router

```
/certificate  
add name=LocalCA common-name=LocalCA key-usage=key-cert-sign,crl-sign
```

Sign the newly created CA certificate

```
/certificate  
sign LocalCA
```

Create a new certificate for Webfig (non-root certificate)

Note: as common-name=XXX.XXX.XXX.XXX You enter public IP address of the router.

```
/certificate
add name=Webfig common-name=XXX.XXX.XXX.XXX
```

Sign the newly created certificate for Webfig

```
/certificate
sign Webfig ca=LocalCA
```

Enable SSL (*www-ssl*) and specify to use the newly created certificate for Webfig

```
/ip service
set www-ssl certificate=Webfig disabled=no
```

Enable api-ssl and specify to use the newly created certificate for Webfig

```
/ip service
set api-ssl certificate=Webfig disabled=no
```

Enable WireGuard VPN server

The screenshot shows the WinBox interface with the WireGuard configuration window open. The left sidebar contains a tree view with 'WireGuard' highlighted. The main window is titled 'Interface <wireguard1>' and has tabs for 'General', 'Status', and 'Traffic'. The 'General' tab is active, showing fields for Name, Type, MTU, Listen Port, Private Key, and Public Key. The 'Name' field is 'wireguard1', 'Type' is 'WireGuard', 'MTU' is '1420', 'Listen Port' is '7464', 'Private Key' is 'iBnkx5LJ8vsgLNyjedEmwm2gObTa4JHcGChjivAvnM=', and 'Public Key' is 'EiHHaUOd8Vo06uuQ3qcgB0kssQSyN28D+1BZDEzgaXI='. The 'Status' tab shows 'enabled', 'running', 'slave', and 'passthrough'. The 'Traffic' tab is empty. The 'OK' button is highlighted with a red box. The left sidebar also has a red box around the 'WireGuard' icon and a red box around the '+' icon in the WireGuard tab.

Add IP address on Wireguard interface

Safe Mode Session: vpn-test.uuq.pl

Address List

Address	Network	Interface
test 1-248		
+ 10.0.201.1/24	10.0.201.0	ether1-pub
test 181-380		
+ 10.0.203.3/24		
test 182-381		
+ 10.0.204.4/24		
test 190-402		
+ 10.0.206.6/24		
test 196-413		
+ 10.0.207.7/24		
test 196-414		
+ 10.0.208.8/24		
test 171-359		
+ 10.0.208.9/24		
test 202-425		
+ 10.0.208.10/24		
test 210-439		
+ 10.0.208.11/24		
+ 77.87.125.170/25		
puq-5-IPProduct ID:116		
+ 77.87.125.206/25	77.87.125.128	ether1-pub
+ 192.168.88.1/24	192.168.88.0	wireguard1
puq-5-IPProduct ID:116		
+ 192.168.101.1/24	192.168.101.0	puq-5-2-116

Address <192.168.88.1/24>

Address: 192.168.88.1/24

Network: 192.168.88.0

Interface: wireguard1

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Configuring NAT rules on the firewall

Safe Mode Session: vpn-test.uuq.pl

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Reset Counters Reset All Counters Find srcnat

#	Action	Chain	Src. Address	Dst. Address	Src. Ad...
...	puq-5-Product ID:116				
3	src-nat	srcnat	192.168.101.0/24		
...	puq-5-Product ID:116				
4	src-nat	srcnat	192.168.88.0/24		

NAT Rule <192.168.88.0/24>

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address: 192.168.88.0/24

Dst. Address:

Src. Address List:

Dst. Address List:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface: ether1-pub

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Revision #1

Created 25 November 2023 03:34:41 by Ruslan

Updated 25 November 2023 03:42:24 by Ruslan