

How to setup Proton VPN WireGuard on MikroTik routers

1. Open the MikroTik configuration panel

To do this, open a command line (using Terminal on Linux and macOS, or PowerShell on Windows) and enter:

```
ssh user@192.126.88.1
```

[Read more about using the command line with MikroTik](#)

2. Download a WireGuard configuration file

[Learn how to download a WireGuard configuration file from Proton VPN](#)

4. Route all internet traffic through a VPN server

Enter the following in the command line (hitting enter after each line):

```
/ip firewall address-list add address=192.168.88.0/24 list=under_protonvpn
```

```
/ip firewall mangle add action=mark-connection chain=prerouting src-address-list=under_protonvpn new-connection-mark=under_protonvpn passthrough=yes
```

5. Create WireGuard configurations

Enter the following in the command line (hitting enter after each line). Your WireGuard private key, endpoint port, and public key can be found by opening the configuration file you downloaded in step 2 with any text editor.

```
/interface/wireguard/add name=protonwg01 private-key="<your private key>" comment="ProtonVPN interface"
```

```
/interface/wireguard/peers/add endpoint-address=37.120.217.82 endpoint-port=51820 public-key="<your peer public key>" allowed-address=0.0.0.0/1,128.0.0.0/1 interface=protonwg01
```

```
/ip/address/add address=10.2.0.2/30 interface=protonwg01
```

```
/ip/dns/set servers=10.2.0.1 allow-remote-requests=yes
```

```
/routing/table/add name=protonvpn_wg fib
```

```
/ip/firewall/mangle/add chain=prerouting src-address-list=under_protonvpn action=mark-routing new-routing-mark=protonvpn_wg passthrough=yes
```

```
/ip/route/add routing-table=protonvpn_wg dst-address=0.0.0.0/0 gateway=protonwg01 comment="ProtonVPN Wireguard default route"
```

6. Implement a kill switch (optional, but highly recommended)

Enter the following in the command line (hitting enter after each line):

```
/interface/bridge/add name=protonvpn_blackhole protocol-mode=none
```

```
/routing/table/add name=protonvpn_blackhole fib
```

```
/ip/firewall/mangle/add chain=prerouting src-address-list=under_protonvpn action=mark-routing new-routing-mark=protonvpn_blackhole passthrough=yes
```

```
/ip/route/add routing-table=protonvpn_blackhole gateway=protonvpn_blackhole
```

7. Exclude VPN traffic from FastTrack (important!)

Start by listing all firewall rules:

```
/ip firewall filter print
```

Remove the two [FastTrack](#) rules (the default rule and dummy rule). To do this, enter the following command twice, using the numbers shown then you listed all the firewall rules.

```
/ip firewall filter remove <number>
```

9. Reduce [MSS](#)

Enter the following in the command line:

```
/ip firewall mangle add action=change-mss chain=forward new-mss=1360 passthrough=yes protocol=tcp  
connection-mark=under_protonvpn tcp-flags=syn tcp-mss=!0-1375
```

10. Restart your router

Don't forget step 7 – removing the FastTrack rules!