Mullvad VPN - Wireguard

First, we need to add a Wireguard interface in the Mikrotik router to auto-generate a key pair. We will copy the private key and import it into the Mullvad device configuration page. Mullvad will use the imported private key to generate a public key. Mullvad will use this public key to encrypt data packets back to the Mikrotik firewall.

```
interface/wireguard/add name=Mullvad
```

```
interface/wireguard/print
Flags: X - disabled; R - running
 0  R name="Mullvad" mtu=1420 listen-port=26477 private-
key="qG7LMj39vPGUAX+FtFBZu5DVJH2q3nH6CSDa4ociPGM="
     public-key="Fea2vkJ2H2Tk0apEn7t2ivXx7ssTs+w23zkm3mOp+xo="
```

Once you have the private key from the Wireguard interface you'll need to login into Mullvad and browse to "My account" and then click on "Manage devices and ports". It should take you to a page that looks like the one shown below.

Manage devices and ports

My devices (3/5)

> To make it easier to manage devices, we are adding names to identify them.
> This feature has been added to the 2022.2-beta1 desktop app and will be gradually added to other platforms.
>
> *You can still view the corresponding WireGuard keys under the device name.*

Stunning Coral
WireGuard key `im5NSh3eq4lgw3rHu+eBRad7KK3eKbEvyhAm5d5Ixm8=`
Created 2022-06-06 🗑

Spicy Toucan
WireGuard key `nbI8RGEvfnz2b11r+IkN2v5xxJTNLujWwNOf2tQFbxg=`
Created 2022-06-06 🗑

Sensible Mole
WireGuard key `Y7OgUquWcjXYK5DW8Rvgcg1VgbGE+TZ8KTApSgaRGyU=`
Created 2022-06-06 🗑

You can create a device automatically using our app (recommended) or by generating a WireGuard configuration file .

Port forwarding

Port forwarding makes it possible for remote computers to access a specific computer or service within a private local area network (LAN).

Next, you'll want to click on the "WireGuard configuration file" link. Your web page should look similar to the page below.

1. Choose your platform

■ Windows **🍎 macOS** **🐧 Linux** **🍎 iOS**

🤖 Android/Chrome OS

2. Generate a WireGuard key

Generate key	No key generated

Manage keys ⌃

Manage WireGuard keys

Use	Public key	Created	Revoke
✕	im5NSh3eq4lgw3rHu+eBRad7KK3eKbEvyhAm5d5Ixm8=	2022-06-06	✕
✕	nbI8RGEvfnz2b11r+IkN2v5xxJTNLujWwNOf2tQFbxg=	2022-06-06	✕
✕	Y7OgUquWcjXYK5DW8Rvgcg1VgbGE+TZ8KTApSgaRGyU=	2022-06-06	✕

qG7LMj39vPGUAX+FtFBZu5DVJH2g3nH6CSDa4ociPGM=	Import key

Next, you'll take the private key you saved from your Mikrotik configuration and import it. Once your private key is imported it should look similar to the image below. You can see that Mullvad created the public key from the private key.

1. Choose your platform

Windows   **macOS**   **Linux**   **iOS**

Android/Chrome OS

2. Generate a WireGuard key

Generate key   `Fea2vkJ2H2Tk0apEn7t2ivXx7ssTs+w23zkm3mOp+xo=`   ✓

Manage keys ⌃

Manage WireGuard keys

Use	Public key	Created	Revoke
✕	im5NSh3eq4lgw3rHu+eBRad7KK3eKbEvyhAm5d5Ixm8=	2022-06-06	✕
✕	nbI8RGEvfnz2b11r+IkN2v5xxJTNLujWwNOf2tQFbxg=	2022-06-06	✕
✕	Y7OgUquWcjXYK5DW8Rvgcg1VgbGE+TZ8KTApSgaRGyU=	2022-06-06	✕
⦿	Fea2vkJ2H2Tk0apEn7t2ivXx7ssTs+w23zkm3mOp+xo=	2022-06-06	✕

`Enter private key`   **Import key**

The next step is to scroll down and pick a server and other options you may be interested in. Once you picked your options you'll click "Download file" to retrieve the configuration needed to finish the peer configuration in the firewall.

We never get access to your private key, only the public key is sent to us. The private key is stored locally in your browser so that you can create multiple files from the same key and as soon as you leave this page, it is deleted.

3. Select one or multiple exit locations

🚩 USA ⌄   🏢 Chicago, IL ⌄   ☰ us4-wireguard ⌄

Advanced settings ⌄

4. Configure Content Blocking

Select the type of content to block

[Select All]   [None]

☐ Ads   ☐ Trackers   ☐ Malware   ☐ Adult content   ☐ Gambling

5. Generate and download configuration

[📄 Download file]   [🔳 Generate QR code]

Once the configuration is downloaded, open it in a text editor to retrive the rest of parameters to finish the Wireguard peer configuration. Below is an example of a configuartion file.

```
[Interface]
PrivateKey = qG7LMj39vPGUAX+FtFBZu5DVJH2q3nH6CSDa4ociPGM=
Address = 10.67.171.164/32,fc00:bbbb:bbbb:bb01::4:aba3/128
DNS = 10.64.0.1

[Peer]
PublicKey = MRZsEblqO4wlq0WPnZgp5X9ex4Z2FHm9bljO/a/Mznk=
AllowedIPs = 0.0.0.0/0,::0/0
Endpoint = 68.235.43.82:51820
```

You'll need the Address, PublicKey, AllowedIPs and Enpoint information for the configuration below.

```
interface/wireguard/peers/add interface=Mullvad endpoint-
address=68.235.43.82 endpoint-port=51820 allowed-address=0.0.0.0/0 public-
key="MRZsEblqO4wlq0WPnZgp5X9ex4Z2FHm9bljO/a/Mznk="
```

```
ip/address/add interface=Mullvad address=10.67.171.164/32
```

The commands below are used to setup a routing table, NAT and a address list to assign specific IPs to be routing out of the firewall using the Mullvad VPN.

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

```
ip/route/add dst-address=0.0.0.0/0 gateway=Mullvad routing-table=Mullvad
```

The command below will allow you to specify which IPs you want to route out the Mullvad VPN.

```
ip/firewall/address-list/add list=Mullvad-VPN address=172.16.5.20
```

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

```
ip/firewall/nat/add action=masquerade chain=srcnat src-address-list=Mullvad-
VPN
```