Jak nastavit Proton VPN na routerech MikroTik pomocí WireGuard

protonvpn.com/support/wireguard-mikrotik-routers

Proton VPN můžete nastavit na routeru MikroTik tak, aby všechna zařízení, která se přes něj připojují k internetu, byla chráněna Proton VPN.

V této příručce vám ukážeme, jak to udělat pomocí protokolu WireGuard VPN na routerech MicroTik se systémem RouterOS 7. To vyžaduje účet Proton VPN

Získejte Proton VPN

Jak nastavit Proton VPN WireGuard na routerech MikroTik (aktualizace)

1. Stáhněte si konfigurační soubor WireGuard

Otevřete jej pomocí libovolného textového editoru.

Přečtěte si, jak stáhnout konfigurační soubor WireGuard z Proton VPN

Všimněte si, že nemůžete použít uložený konfigurační soubor. Proton VPN nikdy neukládá vaše soukromé klíče, takže uložené konfigurační soubory je nemají. Musíte vytvořit a stáhnout nový konfigurační soubor.

2. Otevřete konfigurační panel MikroTik

Chcete-li to provést, otevřete příkazový řádek (pomocí Terminálu v systému Linux a macOS nebo PowerShell v systému Windows) a zadejte:

```
ssh uživatel@192.168.88.1
```

Přečtěte si více o použití příkazového řádku s MikroTik

3. Vytvořte nové rozhraní WireGuard

Pomocí příkazového řádku zadejte následující text a klepněte na <enter>. Chcete-li najít svůj soukromý klíč, vyhledejte řádek začínající **PrivateKey=** v konfiguračním souboru WireGuard, který jste stáhli v kroku 1.

```
/interface wireguard
add listen-port=13231 mtu=1420 name=wireguard-inet private-
key=”váš soukromý klíč”
```

Všechny následující kroky budou zahrnovat zadávání příkazů do příkazového řádku.

4. Přidejte IP adresu do rozhraní, které jste právě vytvořili:

```
/ip adresa
přidat adresu=10.2.0.2/30 interface=wireguard-inet
network=10.2.0.0
```

5. Přidejte server WireGuard jako peer

Přidejte adresu koncového bodu, port koncového bodu a veřejný klíč z konfiguračního souboru WireGuard. Hledejte řádky začínající **PublicKey=** a **Endpoint=** .

Pokud například konfigurace říká Endpoint=103.107.197.2:51820, zadejte endpoint-address=103.107.197.2 a endpoint-port=51820

```
/interface wireguard peers
add allow-address=0.0.0.0/0 endpoint-address=xxxx endpoint-
port=xxxxx interface=wireguard-inet persistent-keepalive=25s
public-key="váš veřejný klíč"
```

6. Povolte pro toto rozhraní maškarádu

Poznámka: Toto nastavení předpokládá, že používáte výchozí adresu místní sítě, kterou používá MikroTik. Pokud jste to změnili, použijte místo toho tuto adresu pro **scr-address=** .

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=wireguard-inet
src-address=192.168.88.0/24
```

7. Přesměrujte veškerý internetový provoz přes WireGuard

```
/ip trasa
add disabled=no distance=1 dst-address=0.0.0.0/1
gateway=10.2.0.1 pref-src="" routing-table=main scope=30
potlačit-hw-offload=no target-scope=10
add disabled=no distance=1 dst-address=128.0.0.0/1
gateway=10.2.0.1 pref-src="" routing-table=main scope=30
potlačit-hw-offload=no target-scope=10
```

8. Nakonfigurujte nastavení DNS

```
/ip dns
nastavit servery=10.2.0.1
/ip dhcp-client
nastavit 0 use-peer-dns=ne
```

9. Přesměrujte IP adresu WireGuard přes bránu hlavního poskytovatele

Nahraďte **xxxx** adresou koncového bodu z konfiguračního souboru (**Endpoint=**).

```
/ip trasa
add disabled=no dst-address=xxxx/32 gateway=[/ip dhcp-client
get [find interface=ether1] gateway] routing-table=main
potlačení-hw-offload=no
```

Pokud to nefunguje, budete muset nahradit **gateway=[/ip dhcp-client get [find interface=ether1] gateway]** za **gateway=xxxx** , kde **xxxx** je adresa vaší vlastní internetové brány. Váš poskytovatel internetových služeb (ISP) by měl být schopen poskytnout tuto adresu.

10. Restartujte router

A máte hotovo! Váš router by nyní měl chránit všechna internetová připojení, která poskytuje, pomocí Proton VPN.