WireGuard

WireGuard je nová linuxová VPN, která vyniká svou jednoduchostí a výkonem. Najdete ho v linuxovém jádře, naše virtualizační platforma vpsAdminOS ho podporuje a má příslušný modul zavedený. Podporu WireGuardu ověříte pomocí příkazu `lsmod`, který vám vypíše všechny zavedené moduly v jádře.

```
# lsmod | grep wireguard
```

Pokud máte svůj VPS spuštěný na vpsAdminOS, nemusíte se o nic starat a podpora je připravená. Stačí jen nainstalovat do operačního systému správné utility.

Instalace

Balíčky s modulem pro jádro není třeba instalovat, na sdíleném jádře je stejně není možné nainstalovat. Budete tedy potřebovat jen balíček `wireguard-utils`. Ten obsahuje potřebné nástroje pro správu naší VPN.

Pozor na to, že balíček ještě není součástí aktuálního Debianu 10 Buster. Je možné jej ale snadno přidat z Backports, tedy doplňkového repozitáře nových balíků.

Do souboru `/etc/apt/sources.list` přidáme následující řádek:

```
deb http://deb.debian.org/debian buster-backports main
```

Poté už můžeme rovnou instalovat:

```
# apt update
# apt install wireguard-tools -t buster-backports
```

Generování klíčů

Ve VPN vytvořené pomocí WireGuardu jsou jednotlivé stroje identifikovány pomocí kombinace veřejného klíče a privátní IP adresy. Nejprve je potřeba na každé straně vytvořit pár klíčů. Použijeme k tomu utilitu wg, která slouží pro konfiguraci VPN.

```
# wg genkey | tee wg-private.key | wg pubkey > wg-public.key
```

V aktuálním adresáři vzniknou dva soubory: `wg-private.key` se soukromým klíčem a `wg-public.key` s klíčem veřejným. Veřejný klíč pak musíme předat všem účastníkům, kteří se s námi budou ve VPN spojovat.

Konfigurace

WireGuard má vlastní konfigurační soubor, ve kterém je popsáno nastavení našeho stroje a všech jeho komunikačních partnerů. Do tohoto souboru budeme vkládat svůj soukromý klíč a veřejné klíče všech ostatních.

Konfigurační soubor můžeme uložit kamkoliv, ale výchozí stav je `/etc/wireguard/`. V tomto adresáři také utility hledají své konfigurace, doporučujeme uložit soubor sem, třeba s názvem `wg0.conf`. Příklad konfiguračního souboru:

```
[Interface]
Address = 192.168.100.1/24
PrivateKey = QD8zBS9nCwzhBrr6W9rEtcegvCwRk1SDFZFjSL3bMGQ=
[Peer]
AllowedIPs = 192.168.100.2/32
PublicKey = TcCK+JJLHZcH9zdLRqtJ7cHiCJH2a6iBN2TjVi6zIxw=
Endpoint = 192.0.2.123:51820
```

První část `[Interface]` se týká lokálního stroje a říká, jakou adresu bude používat na rozhraní VPN. Další sekce `[Peer]` budeme opakovat pro každého partnera, uvedeme pro něj povolený rozsah IP adres, jeho veřejný klíč a volitelně skutečnou IP adresu, na kterou se připojujeme.

Položka `Endpoint` je nepovinná, ale vždy alespoň jedna ze stran ji musí mít nastavenou. Typicky používáme jeden centrální bod (server), ke kterému se budou připojovat cestující klienti. Ti nemusejí mít veřejnou IP, proto u nich nastavíme `Endpoint` našeho stabilního serveru.

Spuštění VPN

Nyní už stačí jen konfiguraci použít. Slouží k tomu utilita `wg-quick`, která se umí o rozhraní starat. Pokud jsme soubor s naší VPN nazvali `wg0.conf`, stačí zavolat následující příkaz:

```
# wg-quick up wg0
```

Stav máme vždy možnost zjistit pouhým spuštěním utility `wg` bez parametrů.

```
# wg
interface: wg0
  public key: xcC08j4bC0Z756eokOM1nezhbTU6k25XGSeTmEpVKUQ=
  private key: (hidden)
  listening port: 51820
peer: TcCK+JJLHZcH9zdLRqtJ7cHiCJH2a6iBN2TjVi6zIxw=
  endpoint: 192.0.2.123:51820
  allowed ips: 192.168.100.2/32
```