WireGuard

nová a jednoduchá linuxová VPN

Petr Krčmář

15. listopadu 2018

Prezentace už teď na webu

www.petrkrcmar.cz

Když potřebujeme…

- vytvořit bezpečné spojení mezi počítači
- propojit několik různých sítí
- chceme to jednoduše a rychle

Řešení je spousta

- OpenVPN
  - klasické řešení
  - hodně centralizované
- Tinc VPN
  - moderní, snadné na správu
  - celé v uživatelském prostoru
- IPSec
  - umí vyřešit téměř vše
  - velmi komplexní


WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL

WireGuard je...

- tunelovací mechanismus na L3 pro IPv4 a IPv6
- celý umístěný v linuxovém jádře jako ovladač síťového zařízení
- postavený na moderních kryptografických principech
- používá UDP, umí procházet firewally
- má vlastní autentizační model podobný SSH
- je přímým konkurentem OpenVPN i IPsec
- jednoduše, bezpečně, prakticky
- stále se velmi intenzivně vyvíjí
- autorem je Jason Donenfeld

Vlastnosti

- využívá standardní funkce jádra
- síťový stack, šifrovací funkce…
- API: udp_tunnel, GRO, GSO, NAPI
- z uživatelského hlediska velmi přívětivý
- nestaráte se o stav, spojení, démony…
- jednoduše ovládáte další síťové rozhraní
- pro ovládání používáte standardní nástroje

ROOT.CZ vpsFree.cz

Vlastnosti

- využívá standardní funkce jádra
- síťový stack, šifrovací funkce…
- API: udp_tunnel, GRO, GSO, NAPI
- z uživatelského hlediska velmi přívětivý
- nestaráte se o stav, spojení, démony…
- jednoduše ovládáte další síťové rozhraní
- pro ovládání používáte standardní nástroje
- pro srovnání
  - OpenVPN: 100K řádek (+ OpenSSL)
  - WireGuard: 4K řádek

Síťové rozhraní

- WireGuard nevynalézá kolo, používá běžné nástroje
- základní jednotkou je pro něj **síťové rozhraní**
- vytvoří se rozhraní, přidělí adresy a klíče
- je to standardní rozhraní = vše s ním funguje
  - firewall, routování, porty pro služby…

```
# ip link add wg0 type wireguard
# ip address add 10.1.2.3/24 dev wg0
# ip route add default via wg0
```

ROOT.CZ vpsFree.cz

Ale co klíče?

- používá se asymetrická kryptografie s ECDSA
- pro správu klíčů slouží utilita wg
- klíč protistrany je pevně **svázán s IP adresou**
- přijmeme jen pakety šifrované správným klíčem
- zároveň se kontroluje IP adresa odesílatele (v rozsahu VPN)
- výsledek: pakety vycházející z rozhraní jsou z ověřeného zdroje
- můžeme otevřít službu konkrétní IP adrese
- z rozhraní WireGuardu nevyjdou podvržené IP adresy odesílatele

Správa klíčů

- rozhraní WireGuard
  - svůj privátní klíč
  - UDP port pro příjem
  - seznam povolených peerů
- každý peer
  - identifikován veřejným klíčem
  - seznam povolených IP adres
  - volitelně IP adresa a port protistrany

Generování klíčů

- pomocí utility wg
- nejprve vytvoříme soukromý, pak odvodíme veřejný

```
# wg genkey > private.key
# wg pubkey < private.key > public.key
```

- zapsáno na jednom řádku

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

Konfigurace serveru a klienta

- Server

```
[Interface]
PrivateKey = gHeQBpcVehP7W/bv8qS9H3LTALzOMXL8P+cvYdWUJ00=
ListenPort = 41414

[Peer]
PublicKey = AHmaac4JO5gidkLYbR7nubrV65Uw6ERWF2jiDCJa/mA=
AllowedIPs = 10.1.2.3/32,10.1.3.0/24

[Peer]
…
```

- Klient

```
[Interface]
PrivateKey = UKtbzCH76EghvKgd7b6D/YSwYXobEAlKXEdGM/HywnA=
ListenPort = 21414

[Peer]
PublicKey = TrK66uhx0psmfSsTo72Jp3CsbMXPB2MAOhm11INXK3U=
Endpoint = 203.0.113.20:41414
AllowedIPs = 0.0.0.0/0
```

Zpracování paketu

- odesílání
  - vygeneruje se nový paket
  - projde síťovým stackem a routovací tabulkou
  - WireGuard podle cílové adresy najde *peera*
  - zašifruje paket jeho veřejným klíčem
  - pošle UDP paket na poslední známou adresu a port
- příjem
  - na UDP port WireGuardu je přijat paket
  - paket je dešifrován privátním klíčem
  - zapamatujeme si adresu a port protistrany
  - zkontruluje se, zda IP adresa odesílatele odpovídá *peerovi*
  - pokud ano, je paket propuštěn do síťového stacku
- komunikace je bezestavová
- neodpovídá se na neautentizované pakety
- pokud se nic neposílá, žádná komunikace neprobíhá

ROOT.CZ vpsFree.cz

Jednoduchost

- všechno ostatní je pro správce transparentní
- vytvoří se rozhraní, přidají se peery
- identity jsou tvořeny jen veřejnými klíči
- je možné rovnou komunikovat
- zbytek vypadá bezestavově, je pro správce skryto
- správa je velmi jednoduchá a přímočará

Roaming klientů

- WireGuard používá bezestavový protokol UDP
- neexistuje spojení, nemůže se rozpadnout
- komunikuje se na poslední použitou IP adresu protistrany
  - automatický roaming
- přežije uspání počítače, přesun mezi sítěmi
- při změně IP adresy (eth ↔ wlan) neprobíhá znovupřipojování
- úplně stejně funguje Mosh
- dobře se s tím udělat HA (vysoká dostupnost)

ROOT.CZ vpsFree.cz

Bezpečnost

- používá perfect forward secrecy – každé dvě minuty nový klíč
- používá Noise protocol framework
- Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24
- brání útoku přehráním
- uník vašeho privátního klíče ≠ podvržení identity protistrany
- neumožňuje volit šifrovací schémata – klienti historicky nezatížení
- kód napsán velmi bezpečně
  - při běhu nealokuje paměť
  - neobsahuje parser hlaviček – velikosti jsou statické
  - při přijetí neautentizovaného paketu nemodifikuje stav
  - je malý a dobře auditovatelný

ROOT.CZ vpsFree.cz

Výkon

- vše je v jádře – rychlé a s minimální latencí
  - nemusí se kopírovat pakety do uživatelského prostoru
- používá se rychlá proudová šifra (ChaCha20)
  - srovnatelná s AES-NI, univerzální
- jednoduchý malý kód, omezená stavovost
  - rychlé zpracování paketů
- autor uvádí 4× vyšší tok a 3× rychlejší ping než OpenVPN (AES)

Manuální použití

- použijeme standardní nástroj `ip`
- pro správu klíčů slouží utilita `wg`

```
# ip link add wg0 type wireguard
# ip addr add 10.1.2.3/24 dev wg0
# wg set wg0 private-key ./private.key
# ip link set wg0 up
# wg set wg0 peer TrK66uhx0psmfSsTo72Jp3CsbMXPB2MAOhm11INXK3U= \
  allowed-ips 10.1.2.4/32 endpoint 203.0.113.20:41414
```

Pomocí konfiguračních souborů

- zpracovává utilita `wg-quick`
- hledá konfigurace v `/etc/wireguard/*.conf`
- shellový skript využívající `ip` a `wg`

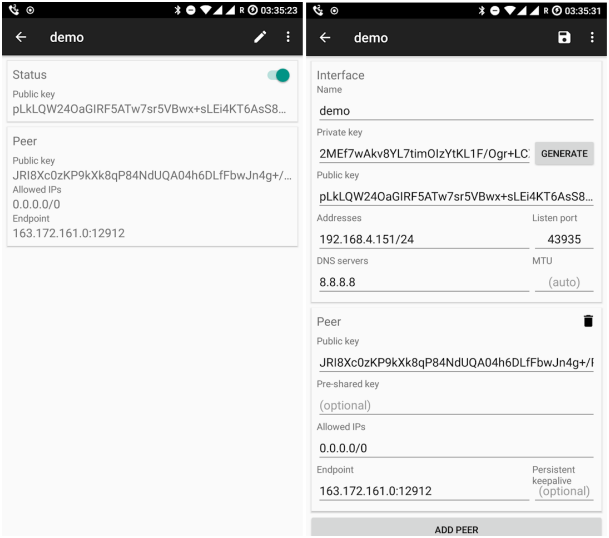
```
# wg-quick up wg0
# wg-quick down wg0
```

Automaticky po startu

- možné integrovat s `interfaces`

```
# cat /etc/network/interfaces
auto wg-client
iface wg-client inet static
        address 10.1.2.3
        netmask 255.255.255.0
        pre-up wg-quick up $IFACE
        post-down wg-quick down $IFACE
```

Klient pro Android



Stav v jádře

- WireGuard zatím není v upstreamu
- patch poslán 31. července 2018
- ke kódu jen málo připomínek, výhradně formální
- největším oříškem knihovna **zinc** s kryptografií
- příliš čerstvá věc, vyžaduje pořádnou revizi
- dopbrá zpráva: pracuje se na tom
- v některém příštím vydání snad bude
- ve vpsAdminOS podporu máme

Odkazy

- WireGuard.com
- `git clone` https://git.zx2c4.com/WireGuard
- Google Play
- přednáška Jasona Donenfelda

ROOT.CZ vpsFree.cz

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz