Propojování sítí pomocí VPN

Petr Krčmář

ROOT.CZ_ vpsFree.cz

17. září 2022

O mně

- linuxák od roku 1998
- správce serverů
- lektor a konzultant
- šéfredaktor Root.cz
- člen vpsFree.cz
- organizátor LinuxDays
- můj web je petrkrcmar.cz

ROOT.CZ_ vpsFree.cz

Prezentace už teď na webu

https://www.petrkrcmar.cz

ROOT.CZ_ vpsFree.cz

Co je a není VPN?

- pro většinu lidí VPN = služba pro změnu IP
  - obvykle pro ochranu, anonymizaci či změnu geolokace
  - to jsou konkrétní **komerční služby**, ty tu neřešíme
- VPN = Virtual Private Network
  - česky **soukromá virtuální síť**
- umožňuje rozšířit místní síť napříč veřejnou sítí (obvykle internet)
- počítače v této VPN si pak vyměňují data jako na místní síti
  - uživatel pak může vzdáleně přistupovat k místním zdrojům
  - existuje i řada jiných scénářů použití VPN

Proč používat VPN

- je to **levné** řešení využívající veřejnou síť
  - výrazně levnější než skutečná privátní síť
  - nemusíme řešit skutečné linky napříč světem
- máme ho plně **pod kontrolou**
  - provozovatel virtuální sítě určuje pravidla
  - naše IP adresy, naše směrování, náš firewall…
- snadno **rozšiřitelná** mnoha způsoby
  - přidání dalších uzlů je snadné
  - změna topologie jen změnou konfigurace

ROOT.CZ_ vpsFree.cz

Co nám VPN nabízí

- dva základní prvky: **tunelování** a **šifrování**
  - oba obvyklé, ale šifrování není povinné ani nutné
- především tunelování vybraného provozu do naší sítě
  - vytváříme propoje (tunely) napříč veřejnou sítí
  - máme pod kontrolou **směrování** na všech stranách
  - tunelujeme provoz mezi zdrojem a cílem komunikace
- bezpečnost je zajištěna šifrováním
  - protistrany používají silný autentizační mechanismus
  - integrita zpráv zamezuje jejich podvržení
  - šifrování komunikace brání v odposlechu

VPN z pohledu sítě

- VPN je realizována jako **podsíť** nadřazené sítě
  - stále je ale součástí sítě, kterou využívá
  - bez nadřazené sítě nebude fungovat
- z pohledu uživatele jde ale o **samostatnou síť**
  - síť jen pro vybrané uzly s vlastními adresami
  - uvnitř této sítě jsme sami a je to naše území
- z pohledu sítě jde o **další podsíť**
  - musíme do ní zajistit směrování
  - všechny komunikující uzly ji musejí znát
- uzly VPN slouží jako brána mezi veřejnou a soukromou sítí
  - mají přístup do obou sítí a překládají mezi nimi
- je možné takto **překonat NAT** a dostat se za něj

ROOT.CZ_ vpsFree.cz

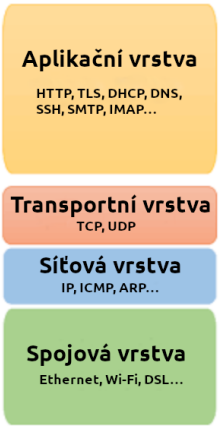
Tuneluju, tuneluješ, tuneluje

- základem všech VPN jsou **tunelovací protokoly**
- umožňují přesouvat data mezi sítěmi pomocí **zapouzdření**
- data po sítí běhají ve formě datových zpráv
  - každá má hlavičku (obálka) a náklad (zpráva uvnitř)
  - směruje se obvykle podle **cílové adresy** v hlavičce
- zapouzdření = přidání další hlavičky (obálka v obálce)
  - z celého původní zprávy (včetně hlavičky) se stává náklad
  - ten **zabalíme** do nové zprávy = přidáme novou hlavičku
- zařízení po cestě se pak dívají jen na první (vnější) hlavičku
  - data doputují až do cílové stanice
  - tam je protistrana vybalí (odstraní hlavičku) a použije
- tato metoda dovoluje soukromým datům překonat veřejnou síť

ROOT.CZ vpsFree.cz

Tunelování na různých vrstvách

- OSI a TCP/IP model
  - sedmivrstvý vs. čtyřvrstvý model
- vrstvy: spojová, síťová, transportní, aplikační
- různé VPN na **různých vrstvách**
  - vlastně rozbíjejí jednoduchý modelový pohled
  - často vrstvy duplikují nebo vkládají nové
- můžeme jít od spojové vrstvy (MPLS, VLAN…)
- přes síťovou vrstvý (GRE, PPTP, IPsec…)
- až po aplikační (OpenVPN, WireGuard…)



ROOT.CZ_ vpsFree.cz

Co tunelujeme

- VPN se liší podle toho, jakou vrstvu přenáší
- základní rozdělení je L2 vs. L3
- L2 vytváří bridge (síťový most) a přenáší **celý Ethernet**
  - nezávislá na vyšších protokolech, ale náročnější
  - pro zařízení je transparentní, vidí vše
- L3 vytváří routery (směrovaná síť) a přenáší **jen IP**
  - oddělení do samostatné IP sítě s vlastní adresací
  - zařízení vidí jinou síť a jen IP provoz
- různé tunelovací protokoly umí různé varianty (někdy i obě)
- obvykle **chcete L3**
  - lépe škáluje, filtruje a řídí

ROOT.CZ_ vpsFree.cz

Běžné tunelovací protokoly

- GRE – Generic Routing Encapsulation
  - původně vyvinuto v Cisco
  - jednoduché použití, manuální konfigurace
- PPTP – Point-to-Point Tunneling Protocol
  - rozšířený díky Microsoftu, je ve Windows
  - zranitelný kvůli slabé autentizaci MS-CHAPv2
- L2TP/IPsec – spojení dvou protokolů
  - opět dobře podporováno ve Windows
  - L2TP zajišťuje tunelování, IPsec bezpečnost
- OpenVPN – aplikační implementace využívající TLS
  - multiplatformní, běží v uživatelském prostoru
  - umí tunelovat L2 i L3, velmi rozšířená
- WireGuard – velmi moderní a výkonná
  - snadná na konfiguraci, předvybrané protokoly
  - původně v linuxovém jádře, pak i aplikační implementace

ROOT.CZ_ vpsFree.cz

Příklad využití VPN

- propojení **dvou bodů** jednoduchým tunelem
  - velmi jednoduché na konfiguraci, jen samotný tunel
  - například k propojení dvou serverů
  - nebo jako další prvek ochrany – služba přes VPN
- připojení vzdáleného **uživatele** (road warrior)
  - jeden přípojný bod (koncentrátor), více uživatelů
  - síť je rozšířena o další uživatele, kteří využívají služeb
  - řeší se na koncových zařízeních (notebook, mobil…)
- propojení několika samostatných **sítí** (poboček)
  - řeší se na směrovačích v síti (hraničních nebo samostatných)
  - pobočky jsou připojeny k veřejné síti (internet)
  - pomocí VPN ale vytvářejí oddělenou síť pro soukromou komunikaci

ROOT.CZ_ vpsFree.cz

Směrování mezi sítěmi

- obvykle největší problém při implementaci VPN
  - většina problémů na fórech vůbec **nesouvisí s VPN**
- řada adminů na síťování narazí až s VPN
  - do té doby jen jednoduché sítě „domácího typu“
  - dvě sítě (LAN/WAN), jeden odchozí směr
- s VPN ale přichází **složitější topologie** a více sítí
- nejobvyklejší problém: *„Pingám na server, ale nic za ním“*
  - tunel je správně navázaný, ale síť není dokonfigurovaná
  - provoz nejde správně do tunelu nebo za ním do správné sítě
  - často je vyřešen jen jeden směr (obvykle odchozí)
  - pakety se pak ztrácejí na cestě zpět = nepingá to

Síťová dosažitelnost

- VPN nemusí být nutně navazována jen v internetu
  - může být vedena už vytvořenou podsítí
- jednotlivé uzly VPN ale musejí být **síťově dosažitelné**
- typicky alespoň jedna strana musí být kontaktovatelná
  - obvykle to znamená veřejnou IP adresu
  - postačuje na jedné straně – kontakt naváže druhá
  - stačí protunelovat příslušné porty
- z jedné strany lze projít i přes NAT
  - pozor na timeout, při nečinnosti se NAT zavře
  - pak nelze zvenčí komunikovat, pomůže **keepalive**

ROOT.CZ_ vpsFree.cz

Firewally

- při prvním nasazení VPN je potřeba obvykle nastavit firewally
- na **vnějším rozhraní** uzlů VPN
  - musíme otevřít příslušné porty do internetu
  - bude na ně přicházet tunelovaná komunikace
- na **vnitřním rozhraní** a v naší síti
  - objeví se tam provoz z jiných sítí
  - ty budou mít jiné síťové rozsahy
  - musíme povolit jejich procházení v obou směrech

Povolení forwardingu (předávání)

- pokud potřebujeme komunikovat se **sítí za tunelem**
  - platí o obou stranách nebo jen o jedné
  - chceme projít VPN a kontaktovat stroj vedle
- prvním krokem je zapnout **forwarding**
  - stroj začne zpracovávat pakety určené jiným uzlům
  - odbaví je podle směrovací tabulky

Zapnutí forwardingu

```
# sysctl -w net.ipv4.ip_forward=1
# sysctl -w net.ipv6.conf.all.forwarding=1
# sysctl -p
```

ROOT.CZ_ vpsFree.cz

Směrování provozu

- obvykle největší úskalí při propojování sítí
- uzly VPN znají jen síťový rozsah na rozhraní VPN
  - ten může být stejný, jakou používá celá síť na druhé straně
- zbytek sítě ale **nezná topologii** za VPN
  - ta může být poměrně komplikovaná
  - může zahrnovat několik dalších podsítí
- při pokusu o komunikaci přes tunel pak selže směrování
  - počítač netuší, kam má poslat provoz pro neznámou síť
  - pokud to netuší ani výchozí brána, jsou data zahozena
- je potřeba zajistit **plnění směrovacích tabulek**
  - v jednodušších situacích staticky
  - ve složitějších s použitím routovacích protokolů (OSPF, BGP…)

ROOT.CZ vpsFree.cz

Adresní plán

- pozor na **kolize adres** v jednotlivých sítích
- nedostatek IPv4 adres = používáme kolizní privátní rozsahy
  - RFC1918: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8
- všechny propojené sítě musejí používat **unikátní rozsahy**
  - jinak dojde ke konfliktu při směrování
  - směrovač nebude vědět, kterým směrem komunikaci poslat
- řešení jsou nepříjemná, je možné využít NAT
  - na hranicích sítí překládat do nekolizního rozsahu
  - lepší je přeadresovat a vyhnout se kolizi
- s veřejnými adresami tento problém odpadá
  - v **IPv6** neřešíme – všechny adresy jsou unikátní

ROOT.CZ_ vpsFree.cz

Obvyklý scénář problému

- vytvoříme VPN s koncem tunelu někde **uvnitř sítě**
  - třeba na diskovém poli, kam protunelujeme porty
- výsledek: přes VPN komunikujeme s polem, ale s **nikým jiným**
  - můžeme využívat jen služeb běžících přímo na poli
  - třeba k tiskárně vedle už se ale nepřipojíme
- důvod: o naší síti za VPN ví jen pole, kde **končí tunel**
  - má ve směrovací tabulce místní rozsah, rozsah VPN a výchozí bránu
- ostatní stroje (třeba tiskárna) ale adresní rozsah VPN **nezná**
  - komunikace z VPN jí tedy přijde (z cizích adres)
  - ale ona neví, kam odpovědět – pošle na výchozí bránu
  - ta rozsah také nezná a komunikaci zahodí

Možná řešení

- ukončit VPN na směrovači, který je v síti výchozí bránou
  - stroje v síti stále rozsah VPN neznají
  - komunikaci pro neznámý cíl pošlou **bráně**
  - ta rozsah zná a pošle komunikaci tunelem
- naučit všechny stroje v síti nový rozsah
  - přidat jim do **směrovací tabulky** nový záznam
  - buď manuálně (pro malé instalace) nebo pomocí DHCP
  - stroje pak vědí, komu komunikaci pro síť za VPN poslat
- přidat záznam do směrovací tabulky **výchozí brány**
  - neznámý obsah putuje do výchozího směrovače
  - ten rozsah VPN zná a ví, komu ho má doručit
  - neoptimální dvojitá cesta sítí, ale funguje to

ROOT.CZ_ vpsFree.cz

Nástroje pro analýzu

- `ping` – kontrola průchodnosti sítě
  - základní přehled o stavu konkrétního směru
  - testuje průchodnost v obou směrech pomocí zpráv ICMP
- `traceroute` – vyhledání používané cesty
  - umožňuje sadou dotazů objevit cestu
  - snadno odhalíme, zda pakety proudí správným směrem
- `tcpdump` – zobrazování konkrétních paketů
  - zaznamenává a zobrazuje provoz na síti
  - hluboký pohled do komunikace, interpretuje známé protokoly
- Wireshark – grafický analyzátor sítě
  - umí nahrát a graficky zobrazit komunikaci na síti
  - interpretuje protokoly, umí načíst záznam z tcpdumpu

ROOT.CZ_ vpsFree.cz

Děkuji za pozornost

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz

ROOT.CZ_ vpsFree.cz