# OpenVPN aneb jak na to

(psáno na základě zkušeností s verzemi 2.0.x až 2.3.x)

## Informační zdoje

http://openvpn.net/index.php/open-source.html

## Instalace a současné problémy TAP driveru

Odkaz pro stažení pro windows  
http://openvpn.net/index.php/download/community-downloads.html  
**Zde zatím důrazně doporučuji** (rozdíl od verze 2.3.x) **release I1xx** používající starší (a z hlediska rozhraní zastaralý) NDIS5 TAP driver. Při pokusu o nasazení novějšího I6xx releasu s NDIS6 driverem **přibližně v 08/2014** došlo na Windows7 / Server 2008 R2 / Server 2012 k jeho/openvpn zablokování a nefunkčnosti tunelu.. Proces po spuštění nešel zabít a použitý adpatér odinstalovat. Musel jsem několikrát restartovat produkční server při pokusech o zjištění původu závady, než jsem zkusil vrátit se zpět k I1xx větvy. **edit k 08/2015 - zdá se že závada, ať již jakákoliv byla odstraněna, alespoň tedy užití NDIS6 na straně klienta funguje v pořádku.**

Nainstalujte default set komponent, můžete odebrat volbu přidat OpenVPN do PATH.  
OpenSSL Utilities a OpenVPN RSA Cert... jsou vhodné / potřebné pouze pro stanici kde se budou případně vytvářet certifikáty.

V současné době je balíček easyRSA, který byl dříve součástí openVPN, samostatný. Odkaz je na výše linkované stránce, nebo k dostání např. přímo zde, stále se vyvíjí:  
https://github.com/OpenVPN/easy-rsa

## Teorie spojení

Je možno vytvořit tunel s TAP či TUN zařízeními na obou koncích, s tím, že topologie je vždy pár nebo hvězdice (eg. jeden server ostatní klienti). TAP je ethernet level. Přináší to sice větší overhead, ale také možnost použití IPX a podporu všech druhů IP broadcastů. To se u her hodí (často je využívána adresa 255.255.255.255 i u novějších aplikací, což způsobuje na nových systémech Windows sekundární problémy). TAP adaptér je plnohodnotný eth. adpatér, lze na něm standardními způsoby konfigurovat IP, DNS, DHCP, .... je možné ho zapojovat do mostů či dělat s ním jakékoliv další věci...

TUN pak emuluje přímo IPv4, v novějších verzích i IPv6. Má výhodu menšího overheadu a tedy i vyšší efektivity, je třeba síťovou topologii nastavit skrze OpenVPN.

OpenVPN dále umožňuje povolit či zakázat komunikaci mezi jednotlivými klienty. (Nejde o navázání přímého spojení ale o komunikaci skrze server). *Netestováno jinak než ve stavu povoleno.*

Přenosový protokol může být UDP i TCP - TCP je však zbytečné, protože v obou přídech si případná TCP spojení uchovávají svou kontrolu uvnitř tunelu.

Pozn: Je například možné vytvořit standardní UDP-TAP síť a tu spojit síťovým mostem s TCP-TAP sítí pro klienty s velmi omezenými cílovými porty a protokoly (a provozovat pak tento například na portu 80, 8080, či 443).

## Konfigurace serveru i klienta

Je v zásadě shodná. Liší se v první řade v tom, že server zadává parametr "local" udávající IP adresu pro bind, a client pak analogicky zadává parametr "remote" udávající cílový server.

## Tvorba certifikátů

Lze použít jakékoliv certifikáty se strukturou CA crt, user crt, user private key pro každého účastníka. Server navíc potřebuje (možná už neplatí?) předgenerovaný soubor DH.

## Nasazení

Je vhodné postupovat v následujícím pořadí:

1. Rozhodnutí ohledně užití TAP či TUN tunelování
2. Volba umístění a OS serveru  
   souvisí s výběrem tunelu, na -nixových systémech lze TAP tunely lépe krotit, například kvůli odstínění DHCP z různých fyzických sítí při spojování stejných podsítí v jednu atp.  
   O tomto problému s DHCP více ve FAQ
3. Tvorba certifikátů pro autentizaci  
   Doporučuji, nyní od openVPN oddělený, easyRSA projekt pro správu certifikátů (PKI - Public Key Infrastructur, je v kryptografii označení infrastruktury správy a distribuce veřejných klíčů z asymetrické kryptografie.)  
   Možno se také rozhodnout pro pass-only řešení (netestováno).  
   Na Windows možno použít "Úložiště certifikátů" a využít tak i smartcard a podobné.
4. OPT: Pokud je nutno řešit IP konfiguraci centrálně z server configu(nestačí automatické přiřazování přes rozsah, typicky u TUN konfigurací) či na straně dalších klientů (např přípojené body při routing více podsítí skrze TUN), vytvořit tyto příkazy k konfiguračním souboru a otestovat je na vzorku.
5. Tvorba "redistribuovatelného" balíčku či nástroje pro automatickou tvorbu per-user balíčků s konfigurací. První řešení vhodnější pro menší skupiny. Balíček = obsahuje configfile nastavený na neutrální jméno uživatelského certifikátu, a CA certifikát, ideálně uložený ve složce pojmenované podobně jako configfile. Do tého složky pak také příjdou jednotlivé uživatelské certifikáty a privátní klíče.
6. První oživení serveru
7. Oživování uživatelských instalací
8. Řešení problémů s firewallem, broadcasty atd., nesnažte se předjímat situaci před prvními nasazeními. Vhodná řešení ve FAQ.
9. Hotovo

## FAQ aneb Praktické postřehy

Firewall: pokud něco nejde, nebo než to vůbec zkusit, tak ho nejdřív prostě vypnout, otestovat že to jede, a pak zapnout. Ulehčí výrazně diagnostiku *časých* problemů.

Pro malé skupiny na hraní atd, je TAP + automatická konfigurace rozsahu IP nejjednoduší možnost.

Skripty jsou velmi dobří přátelé

Na Windows je pro hraní vhodné mít skript, který posune vybraný adaptér(jméno/id adaptéru je třeba identifikovat manuálně), respektive všechny jeho trasy, v routovací tabulce navrch, jde hlavně/konkrétně o broadcast (255.255.255.255). Ten se podle dostupných pramenů na Windows XP duplikuje na všechny zařízení, na Windows s jádrem 6 (Vista+) už však nikoliv, posílá se pouze na první trasu. Spousta her pro vyhledávání sessions využívá právě tento broadcast, a jeho správné routování do VPN je tak nezbytností.  
Lze to řešit buďto změnou metriky jedné konkrétní trasy příkazem route, nebo pro celý interface pomocí netsh (či jeho powershell protějšku). Metrika trasy na windows se vypočítá součtem metriky interface a samotné trasy. Standardně je *myslím* metrika trasy 255. Osobně preferují nastavit metriku herní VPN na 10, fyzický adaptér na 50 či 100 a bezdrátové adaptéry na 200. Ostatní násobky 10ti jsou pak volná pro ostatní VPN interface (pracovní, virtuální stroje atd).

Pokud potřebujete jednoduchou síťovou topologii, pro jednu firmu s síťovými tiskárnami, sdílenými složkami a tiskárnami na více místech, můžete zvolit asi nejednodušší variantu: jednu, např. /24, podsíť, kde každá fyzická síť má adresy jen z určitého jejího rozsahu, a každá fyzická síť má jeden počítač v ní určen jako bod spojení - fyzický adaptér spojený mostem s TAP tunelem. Tyto počítače obsluhující tunel by měli mít statické IP v rámci nepřidělované oblasti zvolené podsítě, stejně tak internetové brány. Vyvstane však problém, pokud se v síti střetnou více než dva DHCP servery (což se stane, protože každá oblast má typicky svojí bránu/DHCP server). Řešení je že všechny, nanejvýš všechny kromě jednoho, klientské přípojné body, budou mít nastavený filter který nepropustí DHCP pakety do své sítě, a pokud bude jedna oblast nechráněná, tak ani žádné nesmí propustit do VPN. *Takové řešení (1x server, 1x linux klient + fyzická síť, 1x windows klient + fyzická síť a další libovolný počet samostatných klientů) jsem otestoval.*  
Pro linux pak poslouží EBTABLES, který je dostupný i na většině linuxových routerových firmwarech, nejhůře v podobě opt-ware. Na Debianu se mi kupodivu odmítl objevit v repozitáři, ruční stažené balíčku z webu a jeho instalace však proběhla OK. http://ebtables.netfilter.org/  
Na Windows jsme takové řešení bohužel nenašel, a tak pro takový případ doporučuji routovanou TUN síť, kde VPN má vlastní rozsah, rozsahy každé fyzické sítě jsou různé, a jsou pouze routované skrze VPN. *zatím bohužel v tomto nemohu sdílet žádné zkušenosti*.

Na produkčním stroji způsobily verze 2.2.x v součtu během cca 4 let asi 3 vážnější problémy. Jednou došlo k jakémusi přetížení, kdy interface plodil "nekonečně" paketů v jakési smyčce a úplně zahltil síťový subsystém Windows, bylo třeba se připojit přes KVM a restartovat stroj. Podruhé způsobil běžící VPN server při připojení klientem (zřejmě jiné verze) zamrznutí stroje, a potřetí zmiňovaný problém s NDIS6 driverem, který vedl k několika nuceným restartům.