OpenVPN

Petr Machota

X36MTI

Úvod

OpenVPN je program pod licencí GPL, poskytuje možnosti tvorby jednoduchého tunelového spojení nebo komplexnějších VPN sítí. OpenVPN není postaven na technologii IPSec, není kompatibilní ani s jinými řešeními (Cisco, Zyxel atd.)

Co je VPN, k čemu slouží

Virtual **P**rivate **N**etwork

Definice: *VPN je komunikační prostředí, ve kterém je řízen přístup ke komunikaci mezi jednotlivými entitami z definovaného souboru, je vytvořeno nějakou formou rozdělení společného komunikačního média, a kde tato nižší vrstva komunikačního média poskytuje síťové služby na ne-exkluzivní bázi.*

Slouží pro vytváření virtuálních podsítí nějaké větší sítě, nebo naopak k vytvoření jedné virtuální sítě napříč internetem a přes více fyzických sítí.

Hlavní vlastnosti OpenVPN

- Volně dostupný (OpenSource)
- Podpora mnoha platforem - Linux, Solaris, OpenBSD, FreeBSD, NetBSD, MacOS X a Windows 2000/XP.
- Celý program běží v user mode, a není tedy potřeba patchovat kernel (za předpokladu, že máte zapnutou podporu pro TUN/TAP zařízení)
- Podpora režimů 1:1 (tunel) nebo N:1 (režim klient/server)
- Možnost použití sdíleného klíče a/nebo SSL certifikátů
- Relativně jednoduchá konfigurace, logy
- Šifrování pomocí SSL/TLS
- Vysoká odolnost při použití na nekvalitních linkách
- Volitelná komprese
- Podpora HTTP a SOCKS proxy. To je výhodné především pro RoadWarrior režim, klient se tak může připojit téměř odkudkoliv
- jediný program (stejný pro server i klienta, funkce se rozlišuje konfigurací)

Virtuální síťový adaptér

Komunikace a zabezpečení probíhá pomocí virtuálního adaptéru (jak u serveru tak i klienta). Jsou možné dvě varianty:

- TUN – Virtuální Point to Point síťové rozhraní (pracuje s IP rámci)
- TAP – Virtuální Ethernet síťové rozhraní (pracuje s Ethernet rámci)

Komunikace je možná jen mezi dvěma stejnými zařízeními (TUN ↔ TUN, TAP ↔ TAP). Pro instalaci v prostředí Windows je připraven ovladač virtuálního adaptéru. Virtuální síťový adaptér se pro sytém chová jako normální adaptér, lze jej normálně konfigurovat, funguje zachytávání paketů a lze z něj udělat například síťový most (bridge). Pro režim TUN je připravená i podpora IPv6, režim TAP technologii IPv6 podporuje už z principu (pracuje s ethernetovými rámci, nezáleží na obsahu nesených dat).

Provozní režimy sítě

V rámci sítě OpenVPN

- Point-to-point - jinak označován také jako tunel, jde o přímé propojení dvou počítačů virtuálním spojením.
- Multi point-to-point - je v podání OpenVPN stejný jako klient-server, pouze není dovoleno směrování mezi klienty sítě OpenVPN.
- Klient-server - počítače konfigurované jako klient se připojují k počítači nastaveného jako server. Je povolené směrování uvnitř sítě (mezi klienty) OpenVPN.

Vzhledem k ostatním sítím

- Routing - vnitřní síť OpenVPN má vlastní adresu, pakety se musí směrovat do této sítě (síť je tak oddělená od jiných sítí)
- Bridging - síť OpenVPN se přemostěním stává součástí nějaké jiné sítě, IP adresy klientů jsou z rozsahu této „větší“ sítě. Výhodou je např. přenos broadcastových paketů (na rozdíl od směrované sítě), nevýhodou je potenciálně menší bezpečnost.

Autentizace, šifrování, certifikáty a další nástroje zabezpečení

Autentizace

- Žádná - nedochází k žádnému ověřování komunikujících stran ani příchozích paketů
- Sdílenými klíči - komunikující strany se ověřují pomocí sdílených klíčů. Klíče jsou použity i pro šifrování paketů - pakety tak lze ověřit.
- X.509 certifikáty - komunikující strany se navzájem ověřují pomocí SSL certifikátů
- Uživatelským jménem + heslem - OpenVPN má i podporu pro externí ověřovací skripty, v instalaci je přítomen ukázkový ověřovací skript napsaný v jazyku Python.

Šifrování

- Sdílenými klíči - pakety jsou šifrovány sdílenými klíči, které znají obě komunikující strany
- Algoritmy SSLv3/TLSv1 - k zašifrování paketů jsou použity algoritmy nabízené standardem SSLv3/TLSv1, použití konkrétního algoritmu lze nastavit v konfiguraci.
- Výměna certifikátů a klíčů šifrováno Diffie-Hellmann algoritmem - DH algoritmus na základě předgenerovaného klíče vygeneruje klíč použitý na šifrování ověřovacích certifikátů a jiných klíčů.

Certifikáty

- CA - Certifikační Autorita - jde o podpisový certifikát, kterým se podepisují generované certifikáty. Generované certifikáty klientů musí mít být podepsané stejnou CA jako certifikát serveru, jinak nedojde k úspěšnému ověření. Vlastní CA si může vygenerovat každý, není standardně nijak provázané s firemní ani jinou politikou.
- Tvorba klientských certifikátů - k tvorbě je nutné mít k dispozici podpisový certifikát CA, vygenerovaný certifikát může být chráněn heslem. OpenVPN má předpřipravené skripty zjednodušující generování certifikátů i certifikačních autorit.
- Revokace, CRL - v případě že se klientský certifikát dostane do nepovolaných rukou, lze z dat jeho kopie vygenerovat záznam o zneplatnění konkrétního certifikátu. Seznam zneplatněných certifikátů (Certificate Revocation List) server načte a respektuje ho.

Další nástroje zabezpečení

- Soubor jména uživatele na serveru - aby se mohl klient úspěšně připojit do sítě OpenVPN, musí na serveru existovat soubor pojmenovaný stejně jako uživatelské jméno klienta. V těchto souborech může být nastavení specifické pro každého klienta, ale může klidně prázdný.
- Snížení privilegií demona - konfigurací lze nastavit chování, kdy si demon OpenVPN sám, po úspěšném spuštění sníží práva (např. z root práv na nižší)
- Kontrola a případné zrušení spojení při neaktivitě - komunikující strany mohou posílat tzv. udržovací dotazy, pokud na ně nedostanou v určitém čase odpověď, spojení uzavřou.
- Omezení počtu záznamů v routovací tabulce na uživatele - lze omezit maximální počet záznamů na klienta v routovací tabulce uchovávané na OpenVPN serveru.
- Omezení maximálního počtu připojení za sekundu - ochrana proti zahlcení počítače na kterém OpenVPN běží.
- Nastavení MAC a řízení přístupu pomocí MAC - virtuální síťové adaptéry umožňují nastavení MAC adresy. Na jejím základě lze filtrovat přístup, nebo přidělovat IP adresy DHCP serverem.
- Značkování datagramů unikátním identifikátorem - každý paket má unikátní identifikátor z generované posloupnosti. Platnost identifikátoru dokáže příjemce ověřit.
- Sliding-window a time-window - souvisí s řízením zpoždění paketů a při doručování mimo pořadí. Sliding-window definuje omezení na základě číslování paketů, time-window definuje omezení na základě časového razítka.

Řízení provozu

- Nastavení maximální velikosti rámce - lze určit maximální velikost ethernetového rámce.
- Nastavení maximální délky přijímací/odesílací fronty - omezení velikosti přijímací/odesílací fronty pro OpenVPN
- Omezení maximální rychlosti odchozích dat - řízení maximálního vytížení fyzického připojení.
- Nastavení TOS paketů podle obsahu nákladu - položka TOS fyzických paketů je nastavena podle TOS paketů nesených uvnitř (virtuálních).
- Komprese (LZO) - volitelné využití LZO komprese dat.
- Maximální počet připojených uživatelů - omezení maximálního počtu připojených uživatelů na server.

Provoz

Pro připojení klientů na OpenVPN server je nutné, aby měli klienti přístup k portu, na kterém OpenVPN server naslouchá. Tento port lze jednoduše definovat v nastavení serveru i klientů. OpenVPN mutliplexuje všechny připojení přes jeden port, není problém ho používat za nakonfigurovaným firewallem, či NATem.

Server i klienti lze konfigurovat pomocí parametrů předané příkazovou řádkou v okamžiku spuštění, ale mnohem výhodnější a přehlednější je konfiguraci uložit do souboru, který si OpenVPN načte. Server běží jako služba (Windows i třeba Debian), lze jej tedy jako službu ovládat (spouštět, ukončovat, restartovat....)

OpenVPN loguje funkci programu, udržuje seznam připojených uživatelů a seznam přidělených IP adres jednotlivých uživatelům v souboru.

Samotný OpenVPN je textový program, existuje však několik projektů třetích stran, které zprostředkovávají funkce skrze grafické uživatelské rozhraní (GUI). V instalačním balíku poslední betaverze OpenVPN je takovýto program pro systém Windows ve volitelných doplňcích.

Zdroje

http://www.root.cz	OpenVPN - VPN jednoduše (2 díly)
http://www.svetsiti.cz	VPN (1) - historie, definice...
http://pc.poradna.cz	Jak na OpenVPN - minimanuál
http://openvpn.net	Oficiální stránky - manuál, návody
Markus Feilner	OpenVPN Building and Integrating Virtual Private Networks
Charlie Hosner	OpenVPN and the SSL VPN Revolution (pdf)
James Yonan	The User-Space VPN and OpenVPN (ppt)
Google & Wikipedia	