OpenVPN

Petr Machota

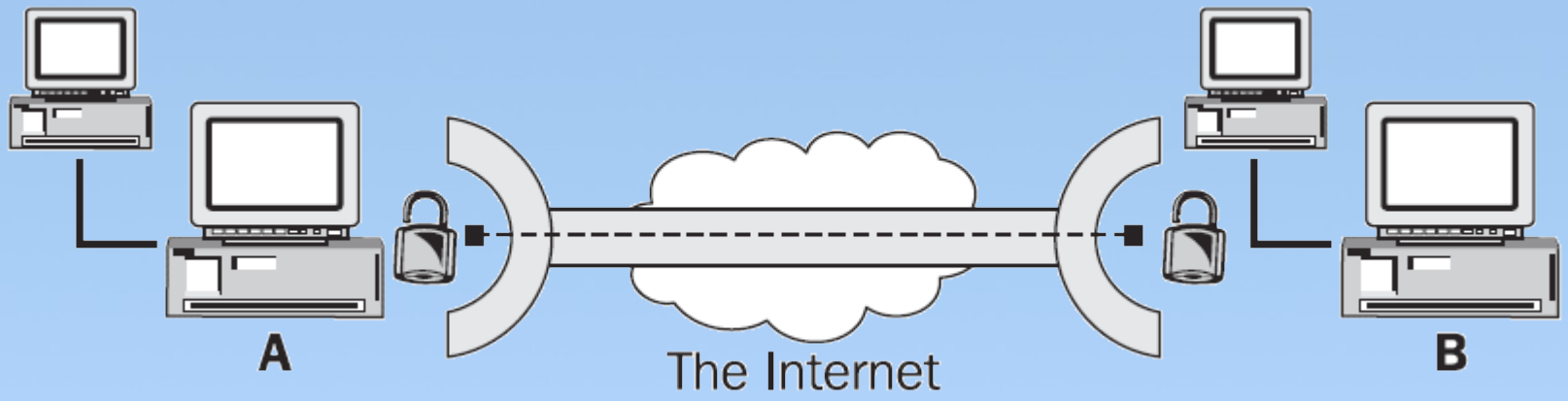
X36MTI

Obsah prezentace

- Co je VPN
- Co je OpenVPN
- Virtuální síťový adaptér
- Provozní režimy VPN sítě
- Zabezpečení
- Autentizace, šifrování a další nástroje zabezpečení
- Řízení přístupu a provozu
- Praxe - firewall, NAT, bridging
- Literatura
- Vaše otázky, závěr

Co je VPN

- **V**irtual **P**rivate **N**etwork
- Definice
- Vytváření virtuálních podsítí nějaké větší sítě
- Vytvoření jedné virtuální sítě napříč internetem a přes více fyzických sítí



Co je OpenVPN

- Open sourcový projekt na tvorbu VPN
- Není postaven na IPSec
- Není kompatibilní s jinými řešeními VPN

Hlavní přednosti

- Podpora mnoha platforem
- Podpora režimů 1:1 a N:1
- Možnost použití sdíleného klíče a/nebo SSL certifikátů
- Relativně jednoduchá konfigurace, dobré logování

Co je OpenVPN

Hlavní přednosti (2)

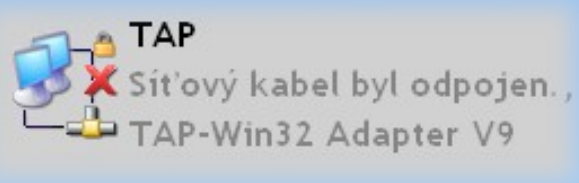
- Bezpečnost (záleží na nastavení)
- Vysoká odolnost při použití na nekvalitních linkách
- Volitelná komprese
- Podpora HTTP a SOCKS proxy
- Jediný program (pro server i klienta)
- Pro Windows instalátor, pro Debian balíček
- Možnost softwaru třetích stran (GUI)

Virtuální síťový adaptér

- Probíhá přes něj veškerá komunikace
- Dvě varianty

TUN

- Virtuální point-to-point rozhraní
- Pracuje s IP rámci



TAP

- Virtuální ethernet rozhraní
- Pracuje s ethernet rámci

Virtuální síťový adaptér

- Komunikace je možná pouze mezi stejnými zařízeními
- Lze ho konfigurovat jako reálný adaptér
- Využitelný jinými nástroji (zachytávání paketů, bridging)
- Pro Windows je připraven ovladač - snadná instalace
- Podpora IPv6

Provozní režimy VPN sítě

V rámci sítě OpenVPN

- Point-to-point
- Multi point-to-point
- Klient-server

Vzhledem k ostatním sítím

- Routing
- Bridging

Autentizace, šifrování a další...

Autentizace

- Žádná
- Sdílenými klíči
- X.509 certifikáty
- Uživatelským jménem a heslem

Šifrování

- Žádné
- Sdílenými klíči
- Algoritmy SSLv3/TLSv1
- Výměna certifikátů a klíčů šifrována DH algoritmem

Autentizace, šifrování a další...

Certifikáty

- Certifikační autorita (CA)
- Tvorba klientských certifikátů
- Možnost ochrany heslem
- Revokace, CRL (Certificate revocation list)

Autentizace, šifrování a další...

Další nástroje zabezpečení

- Soubor jména uživatele na serveru
- Snížení práv démona
- Kontrola a případné zrušení spojení při neaktivitě
- Omezení maximálního počtu připojení za sekundu
- Nastavení a kontrola podle MAC adresy
- Značkování datagramů unikátním identifikátorem
- Sliding-window a time-window

Řízení provozu

- Routování provozu do VPN
- Nastavení maximální velikosti rámce
- Nastavení maximální délky přijímací/odesílací fronty
- Omezení rychlosti odchozích dat
- Nastavení TOS paketů podle nákladu
- Komprese (LZO)
- Maximální počet připojených uživatelů

Praxe - firewall, NAT, bridging

- Jeden port - povolit (přesměrovat)
- Routing
- Bridging
- Windows Vista
- GUI
- Různé druhy připojení, propustnost

Literatura

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

...a to je vše přátelé

Děkuji za pozornost