HTTP tunel pomocou OpenVPN

Marek Bečka

České vysoké učení technické v Praze
Fakulta elektrotechnická

12. mája 2008

Možnosti

Čo všetko môžeme použiť na tunelovanie dát:

- ARP
- DNS
- HTTP (proxy)

HTTP Connect – Popis

- Používa sa pri komunikácii cez HTTP proxy.
- *Nízkoúrovňová* narozdiel od ostatných metód HTTP protokou.
- Vytvára TCP spojenie na špecifikovanú *adresu* a *port*.

- Mechanizmus, ktorý umožňuje odoslať data bez zásahu proxy.
- Proxy nemusí vždy poznať URL, na ktorú pristupujeme.
- Pri šifrovanom spojení pomocou SSL to ani nie je možné.

HTTP Connect – Obmedzenia

- Z bezpečnostných dôvodov nie je možné vytvárať spojenia na ľubovolné porty.
- Obmedzenie len na nevyhnutné „*well–known*“ porty.
- Väčšinou funguje aspoň 443 TCP, inak by nebolo možné pristupovať na web cez HTTPS protokol.

HTTP Connect – Ukážka

Požiadavka od klienta na vytvorenie spojenia:

HTTP 1.0

```
CONNECT server.example.com:443 HTTP/1.0
Proxy-authorization: basic aGVsbG86d29ybGQ=
```

HTTP 1.1

```
CONNECT server.example.com:443 HTTP/1.1
Host: server.example.com:443
Proxy-authorization: basic aGVsbG86d29ybGQ=
```

OpenVPN – Vlastnosti

- Opensource VPN riešenie.
- Bezpečnostný model založený na SSL.
- Používa protokol SSLv3/TLSv1.
- Authentifikácia pomocou *certifikátov*, predvzdielaných *kľúčov* alebo *mena* a *hesla*.

- Pracuje v „*user–mode*“, používa TAP alebo TUN zariadenie.
- Funguje ako *tunel* (1:1) ale aj ako *klient–server* (N:1).
- Dokáže komunikovať pomocou UDP aj TCP protokolu.
- Podporuje SOCKS a HTTP proxy.

OpenVPN – Vygenerovanie certifikátov

OpenVPN obsahuje skripty pre uľahčenie generovanie certifikátov:

Certifikačná autorita

```
vars
clean-all
build-ca
```

Certifikáty

```
build-key-server server
build-key client
```

Diffie–hellman

```
build-dh
```

OpenVPN – Konfigurácia klienta

openvpn-client.conf

```
client                                  # režim klient
remote server.example.com 443           # vzdialený server

# http proxy, basic autentifikácia z konzoly
http-proxy proxy.local.net 3128  stdin basic

dev tap                                 # použijeme TAP zariadenie
proto tcp                               # komunikácia cez TCP

ca   /etc/openvpn/ca.crt                # certifikačná autorita
cert /etc/openvpn/client.crt            # certifikát klienta
key  /etc/openvpn/client.key            # kľúč klienta

persist-key                             # zachová pri reštarte
persist-tun                             # zachová pri reštarte
pull                                    # nastavenia od servera
comp-lzo                                # kompresia
```

OpenVPN – Konfigurácia servera

openvpn-server.conf

```
# režim server, nami pridelený subnet pre VPN
server 10.125.253.0 255.255.255.0

ca   /etc/openvpn/ca.crt          # certifikačná autorita
cert /etc/openvpn/server.crt      # certifikát servera
key  /etc/openvpn/server.key      # kľúč servera
dh   /etc/openvpn/dh2048.pem      # diffie-hellman

dev tap                           # použijeme TAP zariadenie
proto tcp                         # komunikácia cez TCP
port 443                          # počúvame na porte 443

# konfigurácia ako default gw pre klientov
push "route 0.0.0.0 0.0.0.0"

comp-lzo                          # kompresia
```

Zhodnotenie

Výhody

- Plnohodnotné TCP spojenie.
- Nízka latencia a réžia.
- Šifrovanie a kompresia dát ako bonus.

Nevýhody

- Metóda Connect môže byť nejakým spôsobom obmedzená.
- Pomerne zložitá konfigurácia a generovanie cerfifikátov.
- Niekedy budeme potrebovať voľný port 443/TCP na serveri.
- Funguje „len“ pod operačným systémom Linux, Solaris, OpenBSD, FreeBSD, NetBSD a Windows 2000/NT/Vista.

Odkazy

HTTP protokol

- Tunneling SSL Through a WWW Proxy
  `http://muffin.doit.org/docs/rfc/tunneling_ssl.html`
- Hypertext Transfer Protocol – HTTP/1.1
  `http://www.w3.org/Protocols/rfc2616/rfc2616.html`

OpenVPN

- OpenVPN Homepage
  `http://openvpn.net/index.php`

Návody

- OpenVPN - VPN jednoduše
  `http://www.root.cz/clanky/openvpn-vpn-jednoduse/`
- Jak na OpenSSL
  `http://www.root.cz/clanky/jak-na-openssl/`