Experimentálne porovnanie výkonu OpenVPN pri použití rôznych kryptografických algoritmov

Michal Petrucha, Ladislav Bačo

RNDr. Jaroslav Janáček, PhD.

Fakulta matematiky, fyziky a informatiky
Univerzita Komenského, Bratislava

26. mája 2014

Zadanie projektu

Úloha

Cieľom projektu je experimentálne zistiť vplyv použitého kryptografického algoritmu na maximálnu prenosovú rýchlosť dosiahnuteľnú medzi dvomi počítačmi pri nasadení OpenVPN, resp. vplyv na vyťaženia procesora v prípade, že dosiahnutá maximálna prenosová rýchlosť bude limitovaná inými faktormi. Na riešenie projektu je možné využiť sieťové laboratórium KI.

- statický kľúč vs. certifikáty, privátne a verejné kľuče
  - výhody: jednoduchšie nastavenie, žiadne PKI
- minimálna konfigurácia:

server

```
dev tun
ifconfig $SERVER_VPN_IP $CLIENT_VPN_IP
secret $STATIC_KEY
```

client

```
dev tun
remote $SERVER_IP
ifconfig $CLIENT_VPN_IP $SERVER_VPN_IP
secret $STATIC_KEY
```

- ďalšie parametre:
  - HMAC autentifikácia paketov: `auth SHA512`
  - šifrovací algoritmus: `cipher AES-256-CBC`
  - veľkosť kľúča: `keysize n`
  - kompresia: `comp-lzo yes|no`

- `nc, pv`
- gigabit ethernet, bez OpenVPN
  - `/dev/zero` $\approx$ 112 MBps
  - `/dev/urandom` $\approx$ 5 MBps ??
  - `video.mp4` $\approx$ 80 MBps
  - bottleneck: HDD $\rightarrow$ ramdisk
- s OpenVPN:
  - 40 šifrovacích algoritmov
  - 25 hašovacích funkcií
  - kompresia
  - aspoň dva druhy súborov (nulový, náhodný)
  - obojsmerné posielanie
  - $40 \cdot 25 \cdot 2 \cdot 2 \cdot 2 = 8000$ testov!!
- to určite nechceme robiť ručne. . .

Testovací skript
Inicializácia

- ramdisk, adresáre pre test
- náhodný súbor z `dev/urandom`, odoslanie klientovi nulový súbor z `/dev/zero`
- generovanie kľúča, odoslanie klientovi
- vytvorenie, sychnronizácia a spoločná podmnožina použiteľných šifier a hašov

```
openvpn --show-ciphers, openvpn --show-digests
sort $TEST_DIR/ciphers.* | uniq -d | awk '{print $1}'
> $CIPHERS
```

- Testovacie prostredie:
  - Debian GNU/Linux 7.4, Intel Pentium 4@2.80GHz, 1GB RAM
  - OpenVPN 2.2.1
  - OpenSSL 1.0.1e-2+deb7u6
- `for COMP in no yes; do`
  `for DIGEST in $(cat $DIGESTS); do`
  `for CIPHER in $(cat $CIPHERS); do`
- vygenerovanie konfiguračných súborov, štart OpenVPN
- posielanie súborov z klienta na server a zo servera na klienta

```
BEFORE=$(get_time)
nc $(get_peer_ip) $NC_PORT < $1
AFTER=$(get_time)
echo "$AFTER - $BEFORE" | bc -l
```

  - fungujú iba CBC šifry!
  - neukončovanie `nc` listenera → sleep

Výsledky

- 30 hodín, 1000 GB v 3200 testoch, 16 šifier, 25 hašov
-

Záver

- TODO

Odkazy:

- https://github.com/laciKE/openvpn_test/
- https://openvpn.net/index.php/open-source/documentation/miscellaneous/78-static-key-mini-howto.html