Što je VPN poslužitelj i kako ga postaviti

Studentski tim: Dubravko Lukačević
Dominik Marjanović
Tomislav Markovac
Josip Trbuščić

Mentor: izv. prof. dr. sc. Miljenko Mikuc

Sadržaj

Sadržaj **2**

1 Uvod **3**

2 Windows **4**
2.1 Windows 10 VPN 4
2.2 SoftEther VPN 5

3 FreeBSD **6**
3.1 FreeBSD VPN over IPsec 6
3.2 Postavljanje FreeBSD poslužitelja 6
3.2.1 Konfiguracija 6

4 Linux **8**
4.1 OpenVPN za Ubuntu distribuciju Linux operacijskog sustava 8

Literatura **9**

A Dodatak A: Indeks (slika, tablica, ispisa koda) **10**

1 Uvod

Virtualna privatna mreža (engl. VPN, virtual private network) je tehnologija koja omogućava sigurno povezivanje privatnih mreža preko javne mrežne infrastrukture. VPN je razvijen kako bi se geografski udaljenim korisnicima omogućio siguran pristup privatnoj mreži. [1] Do potrebe za takvom tehnologijom je došlo devedestih godina te se ona u početku razvijala samo za velike organizacije koje su zahtjevale siguran prijenos osjetljivih podataka putem interneta. Kroz godine komercijalizacija interneta je omogućila većini država pristup najvećoj mreži što je drastično povećalo broj potencijalnih žrtava tadašnjih hakera. Nakon brojnih provala u sustave velikih tvrtki svakodnevni korisnici su postali svjesni loše sigurnosti interneta zbog čega raste potražnja tehnologija koje poboljšavaju mrežnu sigurnost.

Zaštita podataka se osigurava šifriranjem i dodavanjem posebnih zaglavlja na postojeći paket kako bi se osigurala njegova autentičnost, integritet i povjerljivost, koji su neki od osnovnih sigurnosnih zahtjeva. Šifriranje se odnosi na postupak pretvaranja izvornog teksta u šifrirani tekst pri čemu se koriste ključevi i prikladni algoritmi (npr. AES, RSA). Obrnuti proces, dešifriranje, provodi se kako bi samo korisnik koji posjeduje odgovarajući ključ mogao čitati izvoran tekst. U kontekstu mrežne sigurnosti šifriranje korstimo za zaštitu zaglavlja i podataka koji se nalaze unutar paketa. [2]

Jedan od najpoznatijih i najsigurnijiih skupova protokola koji se koristi u VPN tehnologijama je sigurni IP (engl. Internet Protocol Security, IPsec). IPsec uključuje protokole mrežnog sloja kako bi se omogućila sigurna razmjena podataka između parova mreža (engl. network-to-network), računala (engl. host-to-host) ili računala i mreža (netowrk-to-host). Neki od korištenih protokola su AH (engl. Authentication Header) kojim se postiže autentičnost paketa i ESP (engl. Encapsulating Security Payload) čija je zadaća da osigura povjerljivost podataka i informacija. Uz IPsec često korišteni skupovi protokola su: OpenVPN, PPTP, SoftEther i WireGuard.

U današnje vrijeme moguće je birati između mnogo pružatelja VPN usluga od kojih su neki besplatni dok su ostali dostupni kroz mjesečne ili godišnje pretplate. Besplatne VPN usluge se možda čine kao dobro rješenje za siguran prijenos podataka, ali pružatelje takvih usluga ništa ne sprječava od prodaje naših podataka ili korištenja istih u vlastitu korist. Još jedna opcija je postavljanje vlastitog VPN poslužitelja što može izgledati kao dugotrajan i naporan posao, ali ovakvo rješenje nam omogućava da sami odlučimo kako želimo zaštititi prijenos vlastitih podataka. U ostatku rada se nalazi pregled, usporedba i upute za instalaciju poznatijih VPN tehnologija na različitim platformama.

2 Windows

2.1 Windows 10 VPN

2.2 SoftEther VPN

3 FreeBSD

3.1 FreeBSD VPN over IPsec

Ovo poglavlje će uključivati postavljanje VPN-a na FreeBSD inačici operacijskog sustava BSD.

3.2 Postavljanje FreeBSD poslužitelja

Za pristupanje udaljenom poslužitelju koristit ćemo program i istoimeni program ssh. Kako sada prvi puta pristupamo poslužitelju jedini korisnik koji postoji je root. Root je korisnik na unixoidima koji može izvršiti svaku naredbu i pristupiti svakoj datoteci. Njemu pristupamo naredbom

```
$ ssh root@139.59.159.111
```

Kada smo se prijavili na poslužitelja prvu stavr koju moramo napraviti je ažurirati sustav. To ćemo napraviti koristeći FreeBSD-ov upravitelj paketima `pkg` i njegove naredbe `update` i `upgrade`.

```
# pkg update
# pkg upgrade
```

Sada možemo instalirati openvpn.

```
# pkg install openvpn
```

Konfiguracijske datoteke ćemo smjestiti u direktorij `/usr/local/etc/openvpn` koji prvo moramo napraviti.

```
# mkdir /usr/local/etc/openvpn
```

Openvpn nudi predloške konfiguracijskih datoteka stoga ćemo ih kopirati u naš direktorij

```
# cp /usr/local/share/examples/openvpn/sample-config-files/server.conf \
    /usr/local/etc/openvpn/openvpn.conf
```

3.2.1 Konfiguracija

Kako bi mogli zaštititi našu vezu potrebno je kriptirati sav promet između poslužitelja i klijenta. Koristit ćemo asimetričnu enkripciju koja za što su nam potrebni parovi privatnih i javnih ključeva. OpenVPN dolazi sa alatom Easy-RSA koji će nam poslužiti za izgradnju infrastrukture javnog ključa (*engl. PKI - public key infrastructure*). PKI služi kako bi se javni ključevi povezali s pripadajućim osobama ili oragnizacijama. Proces povezivanja izvršava tijelo za certificiranje (*engl. CA - certification authority.* CA također potvrđuje privada li javni ključ osobi navedenoj u certifikatu.

Kako je Easy-RSA omotač oko složene programske knjižnice OpenSSL ona nam je jedini preduvjet te ćemo ju instalirati naredbom

```
# pkg install openssl
```

Nakon toga ćemo kopirati `easy-rsa` skriptu u naš direktorij sa svom konfiguracijom.

```
# cp -r /usr/local/share/easy-rsa /usr/local/etc/openvpn/easy-rsa
```

Sada ćemo se premjestiti u Easy-RSA direktoriji i urediti njegovu konfiguracijusku datoteku `vars`.

```
# cd /usr/local/etc/openvpn/easy-rsa
# vim vars
```

U nastavku su navedena polja koja je potrebno izmjeniti:

```
set_var EASYRSA_REQ_COUNTRY  "<ZEMLJA>"
set_var EASYRSA_REQ_PROVINCE "<ZUPANIJA>"
set_var EASYRSA_REQ_CITY     "<GRAD>"
set_var EASYRSA_REQ_ORG      "<ORGANIZACIJA>"
set_var EASYRSA_REQ_EMAIL    "<EMAIL>"
set_var EASYRSA_REQ_OU       "<ORGANIZACIJSKA JEDINICA>"
set_var EASYRSA_KEY_SIZE     <broj> # duljina rsa ključa u bitovima
set_var EASYRSA_CA_EXPIRE    <broj> # trajanje CA ključa u danima
set_var EASYRSA_CERT_EXPIRE  <broj> # trajanje certifikata u danima
```

Kako je `easy-rsa` skripta pisana za ljusku sh, dok FreeBSD koristi csh potrebno je naredbom `sh` pokrenuti sh ljsuksu.

4 Linux

4.1 OpenVPN za Ubuntu distribuciju Linux operacijskog sustava

Literatura

[1] CARNet CERT. Osnovni koncepti vpn tehnologije, 2003. https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf.

[2] James Henry Carmouche. *IPsec Virtual Private Network Fundumentals*. Cisco Press, 2006.

A Dodatak A: Indeks (slika, tablica, ispisa koda)