<Naziv projekta>

Studentski tim: Dubravko Lukačević
Dominik Marjanović
Tomislav Markovac
Josip Trbuščić

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

Sadržaj

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

3 FreeBSD

3.1 FreeBSD VPN over IPsec

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)