Virtualne privatne mreže zasnovane na WireGuardu

Begić, Marko

Undergraduate thesis / Završni rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:256171

Rights / Prava: Attribution 3.0 Unported/Imenovanje 3.0

Download date / Datum preuzimanja: **2024-07-23**

Repository / Repozitorij:

Faculty of Organization and Informatics - Digital Repository

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
V A R A Ž D I N

Marko Begić

Virtualne privatne mreže zasnovane na Wireguardu

ZAVRŠNI RAD

Varaždin, 2023.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Marko Begić

Matični broj: K-45386/16izv

Studij: Primjena informacijske tehnologije u poslovanju

Virtualne privatne mreže zasnovane na Wireguardu

ZAVRŠNI RAD

Mentor:

Doc. dr. sc. Nikola Ivković

Varaždin, rujan 2023.

Marko Begić

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

_____

Sažetak

Ovaj završni rad istražuje razlike između dva VPN protokola. Glavni dio odnosi se na pojašnjavanje rada svakog od njih, te kasnije usporedbom. OpenVPN i WireGuard su dva često korištena VPN protokola, svaki sa svojim prednostima i manama. OpenVPN je stariji i uspostavljeniji protokol s bogatom poviješću i širokom podrškom. On podržava različite kriptografske algoritme i mogućnosti konfiguracije, čineći ga izuzetno prilagodljivim za razne scenarije. Sa druge strane, WireGuard je noviji protokol koji se ističe jednostavnošću i brzinom. Koristi manje resursa i ima manji kod, što ga čini bržim i manje izloženim potencijalnim sigurnosnim ranjivostima. WireGuard također nudi bolju mobilnost i mogućnost brzog prebacivanja između Wi-Fi i mobilnih mreža. Ključna razlika između njih je u njihovoj filozofiji dizajna. Dok je OpenVPN fleksibilan i podržava različite konfiguracije, WireGuard je jednostavan i fokusiran na osnovne funkcionalnosti. Ova jednostavnost čini ga lakšim za postavljanje i održavanje. Odabir između OpenVPN-a i WireGuarda ovisi o specifičnim potrebama korisnika. Ako tražite fleksibilnost i veću kontrolu, OpenVPN može biti bolji izbor. S druge strane, ako vam je važna brzina, jednostavnost i mobilnost, WireGuard je vrijedan razmatranja.

Ključne riječi: WireGuard, OpenVPN, kriptiranje, VPN, tuneliranje

SADRŽAJ

1. Uvod

Pri korištenju interneta, svakom korisniku jedan od najvažnijih faktora jest faktor sigurnosti i zaštite njegovih privatnih podataka. Ti podaci su bez adekvatne zaštite kontinuirano izloženi mogućnostima krađe i napada i iz tog razloga kreirane su i implemenetirane VPN mreže.

Virtualna privatna mreža (VPN) proširuje privatnu mrežu preko javne mreže i stoga omogućuje uređajima da međusobno komuniciraju kao da su povezani u istu privatnu mrežu.

Podaci koji se šalju kriptirani su radi povjerljivosti, enkapsulirani i poslani putem javne mreže primatelju. Ako bi paket bio uhvaćen tijekom prijenosa, sadržaj paketa ostaje nerazumljiv bez ključeva za kriptiranje. Danas, kada su mnoge organizacije raširene na različitim lokacijama, stvaranje kriptiranog virtualnog tunela bez obzira na lokaciju zaposlenika ili tvrtke, omogućuje višu razinu učinkovitosti i sigurnosti.

Ovaj završni rad sa teorijskog aspekta objasnit će što su to virtualne privatne mreže, kako funkcioniraju i zašto ih koristiti, a poseban naglasak bit će stavljen na WireGuard protokol, kao i usporedbu njegovih karakteristika sa OpenVPN-ovim protokolom.

WireGuard je protokol kreiran sa ciljem da pruži veću brzinu i jednostavnost korištenja, kao i veću sigurnost, te bolje performanse svojim korisnicima od postojećih konkurenata.

To je primarni cilj ovog rada- objasniti zašto korisnici koriste VPN-ove, te koje je novosti na području virtualnih privatnih mreža donio WireGuard kao i može li on ostvariti konkurentnu prednost pred korisnicima već poznatim i sigurnim, OpenVPN-om.

2. Definiranje virtualnih privatnih mreža

Virtualna privatna mreža način je simulacije privatne mreže preko javne mreže npr. preko Interneta. Naziva se virtualnom jer ovisi o korištenju virtualnih veza koje su privremene i nemaju stvarnu fizičku prisutnost.

Virtualna privatna mreža (VPN) proširuje privatnu mrežu preko javne mreže i tako omogućuje uređajima da međusobno komuniciraju kao da su povezani u istu privatnu mrežu

Poslani podaci koji se šalju putem javne mreže kriptirani su radi povjerljivosti, te ukoliko bi paket bio uhvaćen tijekom prijenosa sadržaj ostaje nerazumljiv bez ključeva za kriptiranje.

VPN koristi niz tehnologija za kriptiranje podataka kao što su IPSec, L2TP/IPSec, SSL i TLS. Njihovom zajedničkom primjenom stvara se tunel kroz koji se kriptirani podaci prosljeđuju od izvorne do odredišne točke putem poslužitelja.

Većina organizacija danas se nalazi na različitim lokacijama diljem svijeta što je problem jer zbog strogih mrežnih sigurnosnih mjera pristup materijalima u dislociranim tvrtkama je otežan, te je upravo to jedan od razloga zbog kojih je osmišljen VPN-kako bi rješio problem otežanog pristupa podacima.

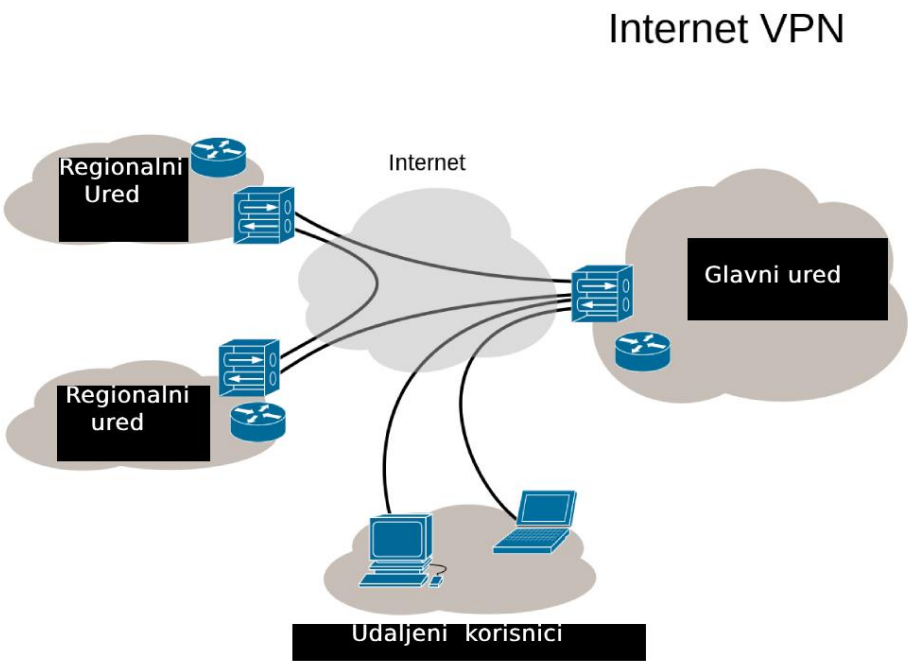
Odnosno, kada se koristi za tvrtke, VPN dopušta samo ovlaštenom osoblju pristup podacima organizacije putem Interneta. Uz pomoć VPN-a organizacija koja ima urede na različitim lokacijama može dijeliti svoje podatke sa svojim zaposlenicima, bez obzira gdje se oni nalaze. To im jamči sigurnost jer su njihove IP adrese maskirane, čak i dok pristupaju javnim Wi-Fi mrežama. VPN značajno smanjuje prijetnju kibernetičkih napada i kršenja sigurnosti stvaranjem kriptiranog virtualnog tunela.

No treba naglasiti kako VPN korisniku nudi povećanu, ali ne i potpunu privatnost jer mnogi pružatelji VPN usluga bilježe sve informacije koje prođu kroz mrežu (Erwin i sur, 2009).

VPN-ovi rade u tri koraka:

- Kriptiraju poslane podatatke
- Podaci se smještaju u sigurnu kapsulu i šalju kroz privatni tunel stvoren na internetu koji maskira izvornu IP adresu.

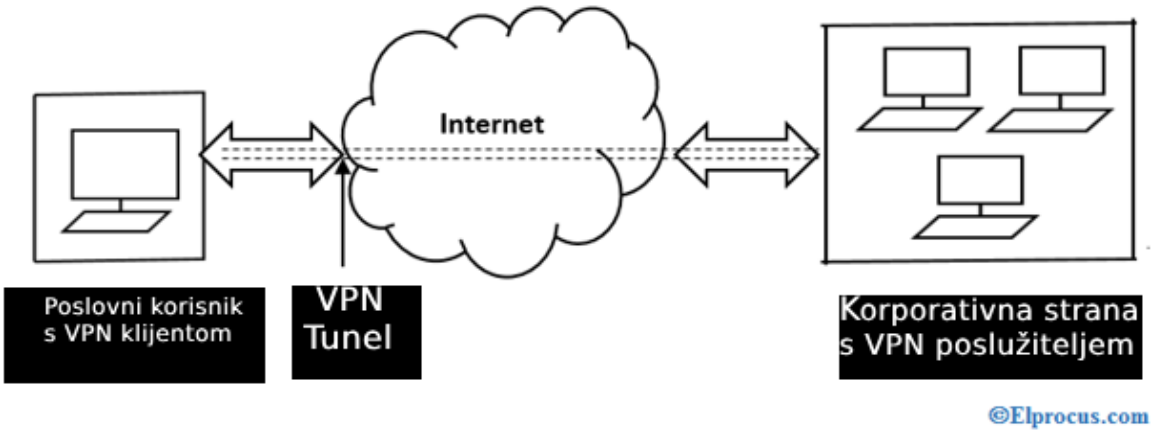
- Adresa primatelja dobiva kapsule i dekriptira informacije, ali pritom izvorna adresa ostaje sakrivena



Slika 1: Korištenje VPN-a u svrhu dijeljenja i pristupa poslovnim informacijama iz ureda na različitim lokacijama (slika je izrađena prema izvoru:https://en.wikipedia.org/wiki/Virtual_private_network)

2.1. Vrste VPN-ova

- VPN s udaljenim pristupom koji omogućuje korisniku da se spoji na zatvorenu mrežu i otvori svaku uslugu i izvor koji su dostupni iz daljine (Amankatiyar i sur., 2014).



Slika 2: Daljinski pristup VPN-a (slika je izrađena prema izvoru: https://www.elprocus.com/virtual-private-network-working-its-types/)

- Site-to-Site VPN također je poznat kao VPN od prijemnika do prijemnika i obično ga koriste velike tvrtke ili organizacije s uredima na različitim lokacijama.

1. VPN temeljen na intranetu koriste uglavnom uredi sličnih tvrtki ili organizacija koji su na taj način povezani koristeći Site-to-Site VPN.
2. VPN temeljen na ekstranetu znači korištenje Site-to-Site VPN-a koji tvrtke koriste kako bi se spojile sa drugim tvrtkama. Site-to-Site VPN-ovi grade virtualni most koji spaja mreže na raznim lokacijama kako bi se one spojile na internet te održava sigurnu i privatnu komunikaciju među tim mrežama (Hopkins i Green, 2019).

2.2. Enkripcija, enkapsulacija i tuneliranje

Kako je navedeno na IBM-u pomoću kriptiranja tj. enkripcije ostvaruje se sigurnost podataka, u smislu da ih nitko osim pošitalja i primatelja ne može pročitati. Tijekom slanja podataka koriste se različite metode kriptiranja kao npr. AES, DES, RSA, te se podaci tijekom slanja pretvaraju u znakove tj. vrši se njihovo kriptiranje putem navedenih metoda. Metoda može biti simetrična što znači korištenje isključivo privatnog ključa pomoću kojeg se kriptiraju tj. dekriptiraju podaci, a može biti i asimetrična što znači da se za kriptiranje i dekriptiranje podataka koristi privatni i javni ključ.

Hash poruke i digitalni potpisi se dodaju na stvarnu poruku kako bi se osigurala nepromijenjivost podataka u slanju od pošiljatelja do primatelja. Oni zapravo služe kao dodatna zaštita. Kada primatelj zaprimi stvarnu kriptiranu poruku on zaprima i *hash* poruku koja se mora poklapati sa lokalno generiranom hash porukom, a ukoliko to nije slučaj to ukazuje da je došlo do izmjene poruke u tijeku slanja. Također da bi poruka bila sigurna ključevi pošiljatelja i primatelja poruke se moraju poklapati.

Na primjer, kod komunikacije dvije osobe, pošiljatelj kriptira poruku koristeći svoj privatan ključ, a javni ključ dijeli sa primatelj kako bi on mogao dekriptirati poruku. Na taj način zapravo se potvrđuje sam pošiljatelj. Ukoliko primatelj poruku ne može dekriptirati svojim ključem to znači da ona nije sigurna ni autentična (Carmouche, 2006).

Enkapsulacija funkcionira tako da sakrije pakete podataka unutar drugih paketa, što zauzvrat omogućuje VPN-ovom softveru da podatke učini neotkrivenim tijekom pregledavanja interneta. Djeluje kao kamuflaža za podatke tako što ih čini neprepoznatljivima kao osjetljive podatke u prijenosu preko mreže.

Cilj enkapsulacije, kao i kriptiranja jest, osigurati siguran prijenos podataka od pošiljatelja do primatelja.

“Unutar infrastrukture međusobno povezanih mreža, tuneliranje predstavlja tehniku prijenosa podataka namijenjenih određenoj mreži preko druge mreže. Protokol kojim se implementira tuneliranje, umjesto da šalje originalni okvir, enkapsulira okvir u dodatno, posebno oblikovano, zaglavlje. Takvo zaglavlje osigurava informacije nužne za usmjerivanje enkapsuliranih podataka kroz mrežu koja služi za prijenos do odredišta. Enkapsulirani podaci šalju se između krajnjih točaka tunela. Tunel je logički put kroz koji enkapsulirani podaci prolaze kroz mrežu koja je medij za prijenos. Kada takav okvir dođe do svog odredišta, iz njega se ekstrahiraju korisni podaci koji se zatim šalju na ciljno odredište. Tuneliranje uključuje čitav proces enkapsulacije, prijenosa i ponovne ekstrakcije originalnih podataka (CARNet, 2003).”

2.3. VPN protokoli

VPN ovisi o metodama tuneliranja za prijenos podataka.

IPsec protokol je skup protokola (IKE, AH i ESP) koji obuhvaćaju mehanizme za zaštitu prometa na razini trećeg sloja OSI mrežnog modela.

IPsec je izvorno definirao dva protokola za osiguranje IP paketa: *Authentication Header* (AH) i *Encapsulating Security Payload* (ESP). Prvi pruža cjelovitost i autentičnost podataka i usluge protiv ponavljanja, a drugi osigurava sve što I prvi, ali uz to kriptira i provjerava autentičnost podataka.

I AH i ESP procedure osiguravaju sigurnost, pouzdanost i provjeru podrijetla podataka. AH provjerava cijeli IP paket osim zaglavlja koja se ne mogu potvrditi, budući da ih mijenjaju međučvorovi.

AH i ESP isporučuju dvije vrste načina rada: tunelski i transportni način rada. Transportni način rada u *IPSec-u* omogućuje kriptiranje I autentifikaciju samo korisničkih podataka, ostavljajući originalno IP zaglavlje nepromijenjenim, dok tunelski način rada dodaje sigurnosni omotač iznad cijelog IP paketa, uključujući IP zaglavlje. Transportni način često se koristi za sigurnu komunikaciju između pojedinačnih uređaja, dok se tunelski način često koristi za sigurnu komunikaciju između cijelih mreža.

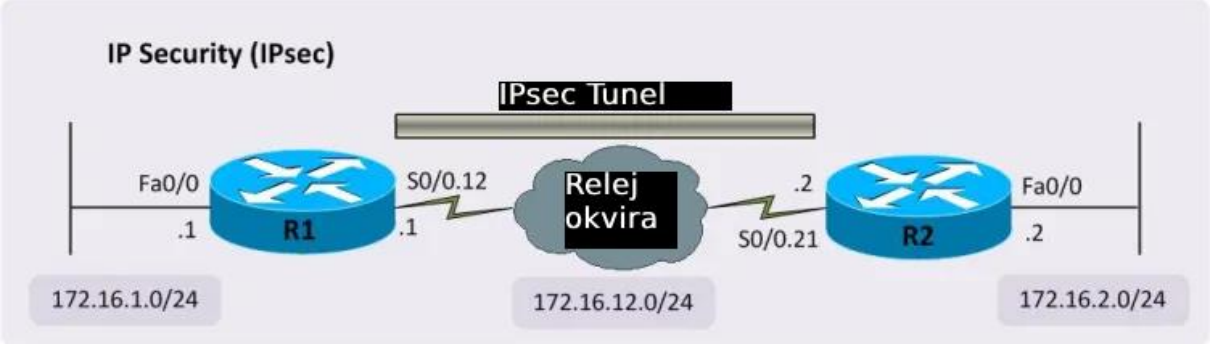
IPsec paket također uključuje *Internet Key Exchange* (IKE), koji se koristi za generiranje zajedničkih sigurnosnih ključeva za uspostavljanje sigurnosne asocijacije (SA). SA-ovi su potrebni za procese kriptiranja i dekriptiranja za pregovaranje o razini sigurnosti između dva entiteta. Poseban usmjerivač ili vatrozid koji se nalazi između dvije mreže obično upravlja procesom SA pregovaranja. SA je "ugovor" između dvije *IPsec* krajnje točke koje se koriste za stvaranje zaštitnih mehanizama i ključeva koji će biti u upotrebi tijekom sljedećeg prijenosa podataka. Zbog toga standard *IP Sec* propisuje i mehanizam unaprijed dijeljenog ključa (PSK) *I Internet Key Exchange* (IKE) protokol.

IPsec osigurava postupke koji su sigurni za dobivanje sigurne IP komunikacije od jedne do druge točke. AH i ESP ne upravljaju nužno razmjenom ključeva.

IPsec se koristi za zaštitu osjetljivih podataka, kao što su financijske transakcije, medicinska dokumentacija i korporativna komunikacija tijekom mrežnog prijenosa. Također se koristi za osiguranje virtualnih privatnih mreža (VPN), gdje *IPsec* tuneliranje kriptira sve

podatke koji se šalju između dvije krajnje točke. *IPsec* se također može koristiti za pružanje provjere autentičnosti bez enkripcije.

Enkripcija na sloju prikaza ili transportnim slojevima modela *Open Systems Interconnection* (OSI) može sigurno prenijeti podatke bez korištenja IPsec-a. Na aplikacijskom sloju, *Hypertext Transfer Protocol Secure* (HTTPS) izvodi kriptiranje. Na transportnom sloju, protokol *Transport Layer Security* (TLS) osigurava kriptiranje. Međutim, kriptiranje i provjera autentičnosti na ovim višim razinama povećavaju mogućnost izlaganja podataka i napada (Loshin, 2021).



Slika 3: *IPsec* (*Internet security protocol*) (slika je izrađena prema izvoru: https://medium.com/webeagle/a-comprehensive-guide-to-internet-security-protocol-ipsec-e77f3d392c96)

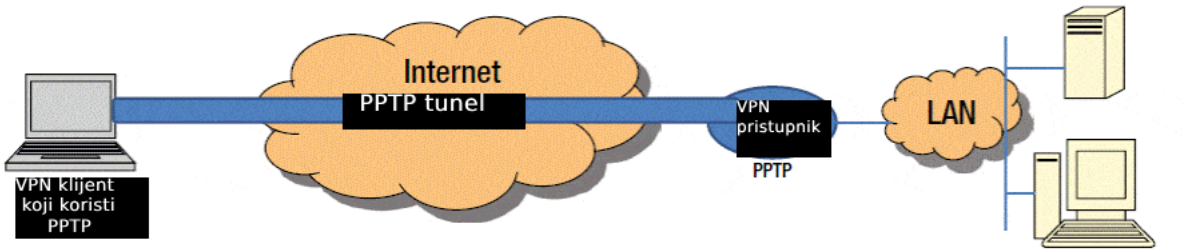
Protokol tuneliranja od točke do točke (PPTP) skup je komunikacijskih pravila koja reguliraju sigurnu implementaciju virtualnih privatnih mreža (VPN), što organizacijama omogućuje metodu proširenja vlastitih privatnih mreža preko javnog interneta putem "tunela".

Izraz "od točke do točke" odnosi se na vezu koju generira PPTP. Omogućuje jednoj točki pristup drugoj određenoj točki putem Interneta. Izraz "tuneliranje" odnosi se na način na koji je jedan protokol/algoritam enkapsuliran unutar drugog odgovarajućeg. U PPTP-u, protokol od točke do točke omotan je unutar TCP/IP protokola koji omogućuje internetsku vezu. Stoga, iako je veza stvorena preko Interneta, PPTP veza uspostavlja izravnu vezu između dva klijenta/lokacije, dajući sigurnu vezu. PPTP je brz zbog niske razine enkripcije i sposoban je ponuditi brzo povezivanje.

Korištenjem PPTP-a, velika organizacija s distribuiranim uredima može stvoriti veliku lokalnu mrežu (LAN) tj VPN koristeći infrastrukturu mreže širokog područja (WAN), poput mreže javnog davatelja internetskih usluga (ISP). Ovo je isplativije od postavljanja mrežne infrastrukture na takve udaljenosti.

PPTP je poboljšana verzija PPP-a, na temelju okvira za autentifikaciju i kriptiranje. Kao i sve tehnologije tuneliranja, PPTP se koristi za enkapsulaciju podataka, stvarajući rutu za protok podataka kroz IP mrežu.

PPTP koristi dizajn klijent-poslužitelj koji radi na sloju 2 OSI modela. Nakon što se uspostavi VPN tunel, PPTP podržava dvije vrste protoka informacija, jedna su kontrolne poruke za upravljanje i eventualno prekidanje VPN veze. Kontrolne poruke prolaze izravno između VPN klijenta i poslužitelja. Drugi su paketi podataka koji prolaze kroz tunel, tj. do ili od VPN klijenta. PPTP koristi *General Routing Encapsulation*, TCP port 1723 i IP port 47.



Slika 4: PPTP (Protokol tuneliranja od točke do točke) (slika je izrađena prema izvoru: https://networkencyclopedia.com/point-to-point-tunneling-protocol-pptp/

Layer Two Forwarding (L2F) Ciscov je protokol za tuneliranje koji koristi virtualne dial-up mreže za siguran prijenos paketa podataka. Funkcionalnost L2F slična je protokolu tuneliranja od točke do točke (PPTP), koji je razvio PPTP forum pod vodstvom Microsofta.

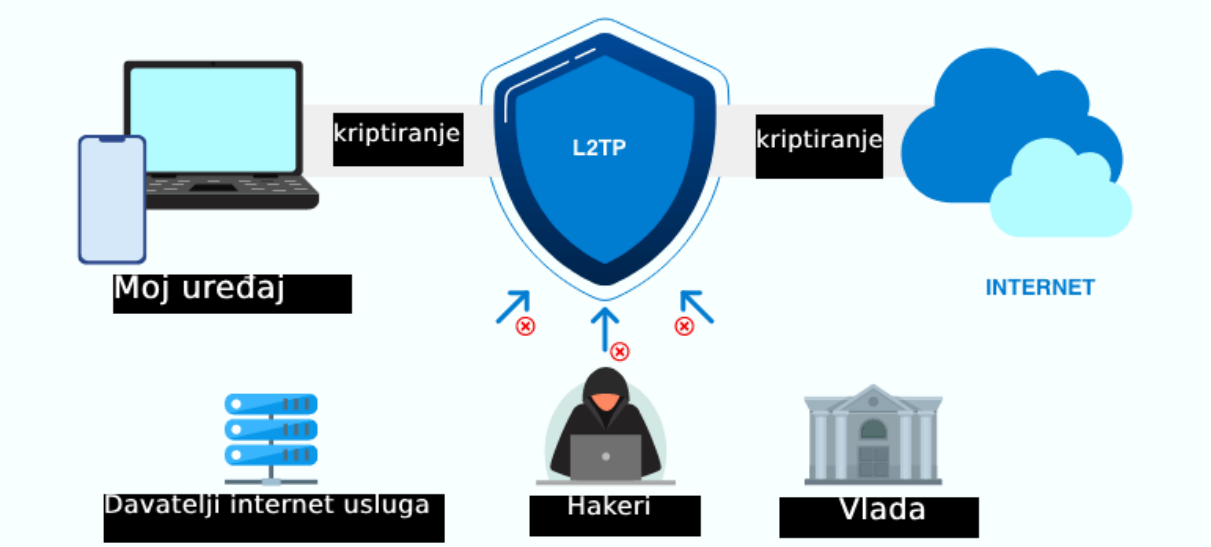
L2F je dio *Layer 2 Tunneling Protocol* (L2TP) standarda (RFC 2661).

L2F stvara mrežne i korisničke veze od točke do točke (PPP) i omogućuje protokolima visoke razine stvaranje tunela preko sloja veze, uključujući kontrolu podatkovne veze visoke razine (HDLC) ili SLIP okvire. Ovi tuneli odvajaju poslužitelj i terminalne točke kako bi se olakšao pristup mreži.

Layer 2 Tunneling Protocol (L2TP) je računalni mrežni protokol koji koriste davatelji internetskih usluga (ISP) kako bi omogućili operacije virtualne privatne mreže (VPN). L2TP je sličan protokolu sloja podatkovne veze u referentnom modelu OSI, ali je zapravo protokol sloja sesije.

Priključak protokola korisničkog datagrama (UDP) koristi se za L2TP komunikaciju. Budući da ne pruža nikakvu sigurnost za podatke poput enkripcije i povjerljivosti, protokol kriptiranja kao što je *Internet Protocol Security* (IPsec) često se koristi s L2TP.

L2TP je "nadogradnja" protokola tuneliranja od točke do točke (PPTP). To je spajanje dvaju protokola, jednog od *Microsofta* (PPTP) i jednog od *Cisca*(L2F). Ovi protokoli su imali svoje prednosti i ograničenja, a L2TP je bio stvoren kako bi se ispravile neke od tih ograničenja I dodala podrška za sigurnosne mehanizme kao što je Ipsec. L2TP je bio diznajniran tako da omogući stvaranje tunela za prijenos različitih tipova podataka, uključujući ne samo IP pakete, već I druge mrežne protokole. Također je važno napomenuti da je L2TP bio razvijen kao otvoren standard I pružio je mogućnosti za interoperabilnost među različitim vendorima i operativnim sustavima.



Slika 5: *L2TP protocol* (slika je izrađena prema izvoru: https://dataprot.net/guides/what-is-l2tp/

SSL (*Secure Socket Layer*) i TLS (*Transport Layer Security*) popularni su kriptografski protokoli koji se koriste kako bi web komunikacija bila sigurna i otporna na neovlaštene upade. PKI koristi TLS protokol za uspostavljanje sigurnih veza između klijenata i poslužitelja preko interneta, osiguravajući da su proslijeđene informacije kriptirane i da ih vanjska treća strana ne može pročitati.

SSL je bio prethodnik TLS-a koji se primarno koristi za osiguranje veze klijent-poslužitelj, također se koristi za zaštitu e-pošte, VoIP poziva i drugih veza. Veze zaštićene TLS-om pokazat će svoj sigurni status prikazivanjem HTTPS (*Hypertext Transfer Protocol Secure*) u adresnoj traci web preglednika.

SSL protokol osigurava privatnost podataka koji se prenose između klijenta i poslužitelja, on omogućuje klijentu autentifikaciju identiteta poslužitelja.

Kada korisnikov poslužitelj ima digitalni certifikat, preglednici s omogućenim SSL-om mogu sigurno komunicirati s njime, koristeći SSL. Pomoću SSL-a jednostavno se može uspostaviti sigurnosna web stranica na Internetu ili na privatnom intranetu. Preglednik koji ne podržava HTTP preko SSL-a ne može zahtijevati URL-ove koristeći HTTPS. Preglednici bez SSL-a ne dopuštaju podnošenje obrazaca koji zahtijevaju sigurnu komunikaciju.

SSL koristi sigurnosno rukovanje za pokretanje sigurne veze između klijenta i poslužitelja. Tijekom rukovanja klijent i poslužitelj dogovaraju se o sigurnosnim ključevima koji će se koristiti za sesiju i algoritmima koji će se koristiti za kriptiranje. Klijent provjerava autentičnost poslužitelja; po izboru, poslužitelj može zatražiti certifikat klijenta. Zatim SSL kriptira i dekriptira sve informacije u HTTPS zahtjevu i odgovoru poslužitelja, uključujući:

- URL koji je zatražio klijent
- Sadržaj bilo kojeg poslanog obrasca
- Pristup informacijama o autorizaciji, poput korisničkih imena i lozinki
- Podatke koji se šalju između klijenta i poslužitelja

3. WIREGUARD

WireGuard je novi VPN protokol otvorenog koda koji koristi najsuvremeniju kriptografiju i ima za cilj nadmašiti postojeće VPN protokole kao što su IPsec i OpenVPN. Izvorno je objavljen za *Linux* kernel, ali sada je višeplatformski i može se široko koristiti. Iako je WireGuard još uvijek u razvoju, već se može smatrati jednim od najsigurnijih, brzih i najjednostavnijih rješenja u VPN industriji.

WireGuard je lako razumljivo i moderno VPN rješenje. Cilj mu je biti brži, jednostavniji i štedljiviji od IPsec-a. Također želi pružiti bolje performanse od OpenVPN-a. Za razliku od OpenVPN-a, koristi smanjeni broj (najsuvremenijih) kriptografskih metoda. WireGuard je dizajniran kao univerzalni VPN za rad na ugrađenim uređajima i superračunalima.

WireGuard je VPN protokol nove generacije za sigurno tuneliranje otvorenog koda. Radi na *Layer 3* sigurnom mrežnom tunelu za IPv4 I IPv6 i koristi nove kriptografske protokole.

WireGuard se temelji na UDP protokolu, a njegov model provjere autentičnosti temelji se na autentificiranim ključevima SSH-a. WireGuard ima manje od 4000 linija, prvobitno je dizajniran za *Linux Kernel*, ali je sada implementacija moguća na androidu, mac-OS-u, BSD-u, IOS-u i za windowse. Konstrukcija sa manjim brojem linija koda znači da je WireGuard puno lakše provjeriti radi sigurnosnih propusta. Reviziju WireGuarda može obaviti jedna osoba, dok je revizija golemih IPSec ili OpenVPN-ovih baza kodova težak zadatak čak i za cijeli tim sigurnosnih stručnjaka. WireGuardova manja kodna baza također podrazumijeva minimalnu površinu za napad koju kibernetički kriminalci mogu iskoristiti (Donenfeld, 2020).

Za razliku od drugih istaknutih VPN protokola, WireGuard koristi najnovije metode za kriptiranje i osiguranje podataka, što ga čini težim za probijanje i lakšim za implementaciju sigurnosnih inovacija.

Ono što ga čini sigurnim jest sljedeće:

1) WireGuard je softver otvorenog koda, što znači da šira VPN zajednica može pomoći u rješavanju bilo kakvih problema, provjeriti kod i poboljšati njegov dizajn. Činjenica da je otvorenog koda također pomaže osigurati da tajne značajke ne narušavaju privatnost i sigurnost korisnika.

2) Minimalni kod: u usporedbi s drugim VPN protokolima, WireGuard se sastoji od

znatno manje koda (4000 linija koda). Zbog toga je hakerima teže pronaći ranjivosti u softveru. To također znači da je stručnjacima lakše identificirati slabe točke i implementirati poboljšanja.

3) Moderna enkripcija: mnoge metode kriptiranja koje koriste drugi protokoli smatraju se zastarjelima i stoga su osjetljive na hakiranje. WireGuard koristi samo najnovije dostupne alate za kriptiranje za sigurnost i brzinu.

WireGuard uspostavlja VPN tunel između dva udaljena računala kako bi se sigurno enkapsulirao sav promet internetskog protokola (IP) između njih. Glavni ciljevi dizajna WireGuarda jednostavnost, brzina i sigurnost. Jedan od ciljeva kod dizajna WireGuarda bio je izbjeći pohranjivanje prije autentifikacije i ne slati nikakve odgovore na neautentificirane pakete.

Da bi se uspostavio tunel, administrator sustava treba samo konfigurirati IP adresu i dugoročni javni ključ za udaljeno računalo. WireGuard VPN implementiran je u nekoliko tisuća redaka koda koji se može izvoditi na više platformi, ali radi performansi, obično se pokreće unutar jezgre operativnog sustava (Lipp i sur, 2019).

WireGuard tunel koristi kriptirane pakete protokola korisničkog datagrama (UDP) kao sredstvo komunikacije. Svako Wireguard sučelje ima privatni ključ, javni ključ, UDP port i popis peera s njihovim odgovarajućim javnim ključevima. Ti se javni ključevi koriste za provjeru autentičnosti i mogu se prosljeđivati u konfiguracijskim datotekama bilo kojom izvanpojasnom metodom (Donenfeld, 2020).

WireGuard koristi mali skup kriptografskih konstrukcija i instancira ih s pažljivo odabranim modernim algoritmima kako bi pružili snažnu sigurnost, kao i visoke performanse:

- Dh: sve *Diffie-Hellmanove* operacije koriste eliptičku krivulju *Curve25519* koja koristi privatne i javne ključeve od 32 bajta
- Hash: sve hash operacije koriste *BLAKE2* hash funkciju koja vraća 32-bajtni hash
- Aenc: provjerena enkripcija za rukovanje i prometne poruke koristi *AEAD shemu*

ChaCha20Poly1305 gdje ključ ima 32 bajta

- Xaenc: enkripcija kolačića koristi proširenu AEAD konstrukciju pomoću

- *XChaCha20Poly1305*
- Mac: sve MAC operacije koriste ključnu MAC varijantu *BLAKE2s* hash funkcije, koja vraća 16-bajtnu oznaku;
- Hkdfn: sve ključne derivacije koriste HKDF konstrukciju koristeći *BLAKE2* kao temelj hash funkcija (Lipp i sur, 2019).

3.1. Način rada WireGuarda

WireGuard VPN protokol radi korištenjem najsuvremenije tehnologije kriptiranja i mrežnog koda za stvaranje kriptiranog tunela računala i VPN poslužitelja. WireGuardov jedinstveni dizajn i metode kriptiranja naglašavaju brzinu i sigurnost.

Dok većina VPN protokola koristi AES-256 enkripciju, WireGuard koristi noviju, *ChaCha20* autenticiranu enkripciju. Obje metode su simetrični oblici enkripcije, ali *ChaCha20* ima kraći ključ. Iako *ChaCha20* koristi kraći ključ, važno je napomenuti da duljina ključa nije jedini faktor koji utječe na sigurnost kriptiranja. Sigurnost algoritma ovisi i o njegovom dizajnu, otpornosti na različite napade I matemtičkim svojstvima. *ChaCha20* je dizajniran s ciljem pružanja visoke razine sigurnosti I brzine, unatoč kraćem ključu. Također *ChaCha20* se često koristi u kombinaciji s drugim sigurnosnim mehanizmima, kao što je algoritam za autentifikaciju *Poly1305*, kako bi se osigurala dodatna sigurnost I zaštita podataka tijekom komunikacije.

Dakle, *ChaCha20*-ova pojednostavljena metoda enkripcije čini ga bržim od AES-256 bez ugrožavanja sigurnosti.

Postavka adrese je virtualna adresa lokalnog WireGuard peera. To je IP adresa virtualnog mrežnog sučelja koje WireGuard postavlja za peer. Kada se promet usmjerava na virtualno WireGuard sučelje, WireGuard mora znati kamo poslati taj promet na "pravoj" mreži. Postavka *Endpointa* za svaki *peer* govori WireGuardu "stvarnu" IP adresu i port na koji bi u konačnici trebao slati promet.

Kao i kod drugih mrežnih sučelja, IP adresa za WireGuard sučelje definirana je mrežnim prefiksom koji lokalnom hostu govori koje su druge IP adrese dostupne na istoj virtualnoj podmreži kao i sučelje.

Važno je da *peerovi* mogu slati kriptirane WireGuard UDP pakete jedni drugima na određene internetske krajnje točke. Svaki *peer* može, prema izboru, unaprijed specificirati poznatu vanjsku IP adresu i UDP krajnje točke tog *peera*. Razlog što je to opcionalno je taj

što ako nije specificirano i WireGuard primi ispravno autentificirani paket *peera*, koristit će vanjski izvor IP adrese za određivanje krajnje točke.

Budući da javni ključ jedinstveno identificira peer, vanjski izvor IP kriptiranog WireGuard paketa koristi se za identifikaciju udaljene krajnje točke *peera*, omogućujući *peerovima* da se slobodno kreću između različitih vanjskih IP-ova, npr. mobilnih mreža (Donenfeld, 2020).

DNS se može iskoristiti za podršku dinamički adresiranih *peerova* jer će razni WireGuard uslužni programi razriješiti DNS imena prilikom konfiguracije *peera*, a postoje i skripte za podršku koje se mogu koristiti za povremeno ponovno rješavanje *peer* adresa.

U početku je WireGuard objavljen za jezgru Linuxa, glavnu komponentu operativnog sustava Linux poznatu po sigurnosti i brzini. WireGuard u potpunosti radi na kernelu, za razliku od drugih VPN protokola koji moraju ulaziti i izlaziti iz kernela u korisnički prostor. To daje WireGuardu brže i sigurnije mogućnosti umrežavanja.

WireGuard radi dodavanjem mrežnog sučelja (ili više njih), poput eth0 ili wlan0, pod nazivom wg0 (ili wg1, wg2, wg3 itd.). Ovo mrežno sučelje tada se može normalno konfigurirati pomoću ifconfig(8) ili ip-address(8), s rutama za njega dodanim i uklonjenim pomoću route(8) ili ip-route(8), i tako dalje sa svim uobičajenim mrežnim uslužnim programima . Specifični WireGuard aspekti sučelja konfiguriraju se pomoću alata wg(8). Ovo sučelje djeluje kao sučelje tunela.

WireGuard pridružuje IP adrese tunela s javnim ključevima i udaljenim krajnjim točkama (Ghimiray, 2022).

Umjesto složenosti IPsec-a i xfrm slojeva, WireGuard na jednostavan način daje virtualno sučelje, wg0 na primjer, kojim se zatim može upravljati pomoću standarda pomoćnih programa ip i ifconfig. Nakon konfiguriranja sučelja s privatnim ključem (i po izboru unaprijed podijeljenim simetričnim ključem), te javnih ključeva uređaja s kojima će se komunicirati tuneliranje se jednostavno odvija.

Razmjene ključeva, spajanja, prekidanja, ponovna povezivanja itd. nadalje se odvijaju transparentno i pouzdano, a administrator ne treba brinuti o tome (Donenfeld, 2020).

WireGuard VPN pružatelji usluga nude jednostavnu aplikaciju koja se instalira na osobne ili poslovne uređaje, a koja zaposlenicima tvrtke omogućuje siguran pristup ključnim resursima kao što su *SaaS* alati temeljeni na oblaku, lokalna pohrana podataka i druga rješenja.

Zaposlenik jednostavno treba osigurati da je povezan s WireGuard klijentom prije nego što pokuša pristupiti resursima tvrtke (poput prijave u *Salesforce*), inače neće uspjeti.

WireGuard VPN poslužitelj uspostavlja tunel između zaposlenika i korporativne mreže nakon uspješne prijave, tako da se nakon toga može privatno pristupiti bilo kojem resursu unutar mreže, a da nitko ne može prisluškivati vezu zaposlenika.

WireGuard VPN tunel koristi WireGuard protokol, koji je kriptografski siguran pristup upravljanju javnim ključevima, ali može podržati različite algoritme uključujući *ChaCha20* za simetričnu enkripciju, *Poly1305* za autentifikaciju, *BLAKE2s* za raspršivanje, UDP kao TLP i HKDF za stvaranje ključa. WireGuard koristi enkripciju s javnim ključem, a ne upravljanje certifikatima.

3.2. OpenVPN

OpenVPN jedan je od novijih protokola koji je među korisnicima postao popularan zbog sigurnosti koju priža, svoje prilagodljivosti i dostupnosti, a uz to je jednostavan za instaliranje i održavanje.

OpenVPN je softverski proizvod otvorenog koda pod GNU *General Public License* (GPL) koji se može koristiti za uspostavljanje VPN komunikacije između dva računala unutar poslovne lokalne mreže preko javne komunikacijske infrastrukture. Koristi posebne sigurnosne protokole i 256-bitnu enkripciju i sposoban je proći kroz prevoditelje mrežnih adresa i vatrozide. Omogućuje računalima međusobnu provjeru autentičnosti korištenjem unaprijed podijeljenog tajnog ključa, certifikata ili korisničkog imena i lozinke (Kovačić i Sknedžić, 2017).

Kako navodi Mash svrha OpenVPN-a je omogućiti korisnicima postavljanje sigurne veze od točke do točke ili stranice do stranice stvaranjem sigurne VPN veze. Kao i *Secure Socket Tunneling Protocol* (SSTP), OpenVPN se oslanja na *Secure Sockets Layer/Transport Layer Security* (SSL/TLS) za autentifikaciju i razmjenu ključeva kriptiranja. OpenVPN koristi port 443 za slanje enkapsuliranih podataka preko SSL/TLS kanala. OpenVPN koristi prilagođeni sigurnosni protokol enkapsulacije podataka temeljen na SSL-u i TLS-u, umjesto korištenja *Point-to-Point* (PPP) ili *Layer Two Tunneling Protocol* (L2TP) kao što je SSTP. OpenVPN koristi biblioteku OpenSSL-a za implementaciju enkripcije podataka i kontrolu, dopuštajući korištenje svih šifara dostupnih u ovom paketu, uključujući vojni AES algoritam s 256-bitnim ključem.

OpenVPN uključuje opcije provjere autentičnosti korištenjem vjerodajnica za pristup (korisničko ime i lozinka), certifikata ili unaprijed podijeljenog tajnog ključa. To nudi značajnu fleksibilnost za upravljanje širokim rasponom aplikacija i uređaja, uključujući kompatibilnost s NAT-om (*Network Address Translation*)

OpenVPN je kompatibilan sa širokim rasponom platformi koje pokrivaju sve popularne operativne sustave kao što su Windows, macOS, Linux, Android, iOS i specijalizirane platforme, uključujući Solaris i OpenBSD. Microsoftove upute pokazuju koliko relativno jednostavna može biti migracija sa SSTP-a na OpenVPN uz pravo tehničko znanje. Postavljanje OpenVPN poslužitelja na Linuxu relativno jednostavno.

3.3. Usporedba WireGuard-a i OpenVPN-a

Uporedba WireGuard i OpenVPN bazirat će se na ključnim aspekatima kao što su sigurnost, privatnost, brzina i jednostavnost korištenja. Također istaknut će njihove glavne karakteristike i prednosti.

Primarni ciljevi WireGuarda su poboljšati postojeće virtualne privatne mrežne protokole jednostavnošću, brzinom, lakoćom korištenja i smanjenjenjem mogućnosti napada mreže korištenjem najsuvremenije kriptografije.

OpenVPN koristi više tehnika VPN enkripcije i ima preko 60 milijuna preuzimanja. Zbog duge prisutnosti u industriji, OpenVPN koristi većina VPN klijenata na tržištu, kako komercijalni tako i korporativni klijenti unatoč pojavi novih i jakih konkurenata.

Unatoč razlikama između ova dva protokola, zajednički im je cilj da budu brzi, sigurni, stabilni i pouzdani.

WireGuard protokol je najpoznatiji po:

- Iznimno brzoj vezi.
- Omogućuje višestruko prebacivanje između mreža.
- Mogućnosti manualnog postavljanja VPN mreže.

OpenVPN je najpoznatiji po:

- Pristupu cenzuriranim regijama poput Kine, Rusije i drugih.

- Postojanju najsigurnijeg protokola u klasi.
- Korištenju OpenSSL za kriptografiju.
- Temeljito je ispitan i popularan dugo vremena na tržištu.

Kodna baza WireGuarda se sastoji od oko 4000 linija koda. S druge strane, OpenVPN ima preko 70.000 linija. Nadalje, modificirane verzije OpenVPN-a dosežu do 600.000 linija koda.

Upotrebom manjeg broja linija koda, WireGuard smanjuje površinu za mogući napad, a time su i manje šanse za potencijalni kibernetički napad.

Uz manji broj linija koda programeri mogu lakše identificirati ranjivosti i kod se može brzo revidirati. Stoga je manja vjerojatnost da će hakeri identificirati sigurnosne propuste u WireGuardu.

Čak i uz ogromnu bazu kodova, OpenVPN nije osjetljiv na napade. Jedna od prednosti postojanja u industriji gotovo dva desetljeća je temeljita provjera, a uz to, OpenVPN ima veliku zajednicu s raznim dionicima koji osiguravaju njegovu stabilnost rada.

WireGuard i OpenVPN su softverske aplikacije otvorenog koda. To svakome olakšava pristup i reviziju izvornog koda i drugih aspekata.

WireGuardov kod je daleko manji u usporedbi s OpenVPN kodom, međutim za razliku od WireGuarda, OpenVPN je izdržao test vremena i prošao je nekoliko revizija, drugim riječima čak i s više od 70 000 linija koda i samim time potrebom za većim timom stručnjaka, OpenVPN je dobro provjeren protokol.To je zato što je postoji već dugi niz godina i većina VPN veza se oslanja na njega.Bez obzira na to, WireGuard ga sustiže i nakon masovnog usvajanja na tržištu ovaj protokol će dobiti istu pozornost kao OpenVPN. Prednost mu je što se s manje linija koda može revidirati nekoliko puta više nego OpenVPN u kratkom razdoblju.

Često korištene šifre i tehnike kriptiranja za WireGuard uključuju ChaCha20 i Poly1305. ChaCha20 se koristi za enkripcije, dok se Poly1305 koristi za autentifikaciju podataka. Također može koristiti druge kriptografske tehnike kao što Curve25519, BLAKE2, SipHash24 i HKDF.

S druge strane, OpenVPN obično koristi AES, *Blowfish* i *Camelliu*. Osim toga, budući da se OpenVPN oslanja na OpenSSL može koristiti druge kriptografske tehnike kao što su Chacha20, Poly1305, SEED, CAST-128, DES, SHA-2, SHA-3, BLAKE2, RSA, DSA, *Diffie–Hellman* razmjenu ključeva itd.

OpenVPN koristi najprovjerenije tehnike šifriranja koje su pouzdanije za razliku od

WireGuardovih novijih algoritama.

Unatoč tome, kada se ta dva protokola primijenjuju u praksi dolazi do obrata po pitanju sigurnosti. Na primjer, WireGuardova, iako novija, tehnologija enkripcije predstavlja manju sigurnosnu prijetnju iz razloga što je ChaCha20 evoluirao tijekom vremena i sada ima preko 20 razina sigurnosti.

Za reviziju WireGuarda potrebno je manje vremena zahvaljujući minimalnoj veličini koda.Navedeno potvrđuje i priznanje od tehnoloških divova poput *Googlea* i sigurnijeg operativnog sustava, Linuxa.

Nadalje, kriptografska agilnost je sposobnost sigurnosnog sustava da se automatski prebacuje između algoritama, protokola i drugih tehnika kriptiranja.

OpenVPN ima prednost u kripto-agilnosti u odnosu na wireguard. OpenVPN može koristiti različite kriptografske pakete I algoritme, što omogućuje korisnicima da prilagode svoje postavke sigurnosti prema svojim potrebama. To može povećati sigurnost, ali također može povećati složenost konfiguracije.

Wireguard, s druge strane, ima fiksni stup kriptografskih algoritama za svaku verziju protokola. To može pojednostaviti konfiguraciju I održavanje, alo može ograničiti mogućnosti prilagodbe. Kripto-agilnost OpenVpn-a može biti korisna u situacijama gdje je potrebna veća prilagodljivost sigurnosnim postavkama, dok wireguard može biti privlačan zbog svoje jodnostavnosti I brzine.

OpenVPN se ističe u prevladavanju internetske cenzure jer može koristiti TCP umjesto UDP-a s priključkom 433, koji također koristi HTTPS čime se otežava razlikovanje OpenVPN prometa od normalnog, sigurnog web prometa.

Zahvaljujući ovom triku, OpenVPN je vrlo učinkovit u cenzuriranim zemljama poput Kine, Rusije i Turske. U normalnim okolnostima preporučeno je korištenje UDP-a za poboljšanje brzine, ali TCP je mnogo sigurniji i pouzdaniji za cenzurirana područja, jedini nedostatak je to što je TCP puno sporiji od UDP-a. WireGuard jedva zaobilazi cenzuru i podložan je *Deep Packet* inspekciji i ne podržava tuneliranje preko TCP-a, uz to njegove UDP veze se lako otkrivaju.

U usporedbi između WireGuarda i OpenVPN-a, WireGuard nudi bolju mobilnost.

WireGuard pruža bolju mogućnost prebacivanja između Wi-Fi i mobilnih mreža u odnsosu na OpenVPN. Mnogi korisnici interneta imaju tendenciju prekidanja i ponovnog

spajanja OpenVPN-a kada mijenjaju mreže i zbog toga dolazi do prekida veze.

Uz ostalo, WireGuard koristi manje tehnika enkripcije od svoje konkurencije, stoga ima niže troškove kriptiranja. Posljedično, vrijeme kriptiranja je kraće i zahtijeva manje podataka za postizanje sigurnosti pri korištenju VPN-a. Niži troškovi enkripcije bitni su kod korištenja mobilne propusnosti pay-as-you-go. Sa OpenVPN-om, koristi se više podataka zbog njegovih ogromnih troškova kriptiranja tijekom tuneliranja.

Što se tiče brzine i performansi, WireGuard je brži jer se uglavnom oslanja na UDP veze. Osim toga, koristi manje CPU resursa u mobilnim uređajima, ugrađenim sustavima i usmjerivačima.

S druge strane, Open VPN je brz, ali ne kao WireGuard kada se koristi UDP. Međutim, kad se bira pouzdanost i zaobilaženje ograničenja, brzina se smanjuje jer se mora koristiti TCP veza. TCP veza daje prednost pouzdanosti u odnosu na brzinu.

Također, budući da OpenVPN ima veće troškove kriptiranja i koristi više CPU resursa, to može biti problematično za uređaje koji nemaju CPU visokih performansi, poput usmjerivača i ugrađenih sustava, uostalom baterija se brže troši zbog velike upotrebe CPU-a. Osim toga, OpenVPN nikada nije bio najbolja opcija u pogledu performansi jer čak i drugi zastarjeli protokoli daju bolje rezultate.

WireGuard bolje koristi *multi-threading* u modernim procesorima, što OpenVPN nije u potpunosti iskoristio. WireGuard je proveo *benchmark* visokih performansi s istim parametrima na IPSec, WireGuard i OpenVPN protokolu.Gotovo svaki VPN u industriji koristi OpenVPN.

WireGuard još ne uživa ovu popularnost, ali uskoro će imati sličnu prisutnost kao OpenVPN s masovnim usvajanjem. Naime, premda je tek nedavno ušao u industriju, već je stvorio ime za sebe.

OpenVPN je mnogo stariji i respektabilniji protokol u industriji što će uvijek izazivati povjerenje i veću lojalnost tehničkih korisnika.

Međutim, ne može se poreći WireGuard-ova brzina postizanja konkurentnosti i nedvojbeno je bolji od OpenVPN-a u raznim aspektima, uključujući brzinu, bazu koda, performanse i upotrebljivost. Kod odabira koji protokol koristiti, potrebno je odlučiti koji aspekt je korisniku primaran. Bez obzira na to, oba su protokola izvrsna za svakodnevnu upotrebu.

Zbog jednostavnog koda, programerima je lako podesiti WireGuard da radi ili podržava više uređaja, isključujući naslijeđene sustave koji neće podržavati nove protokole. Osim toga, WireGuard ima izvrsnu upotrebljivost i podršku za više platformi. Na mobilnim

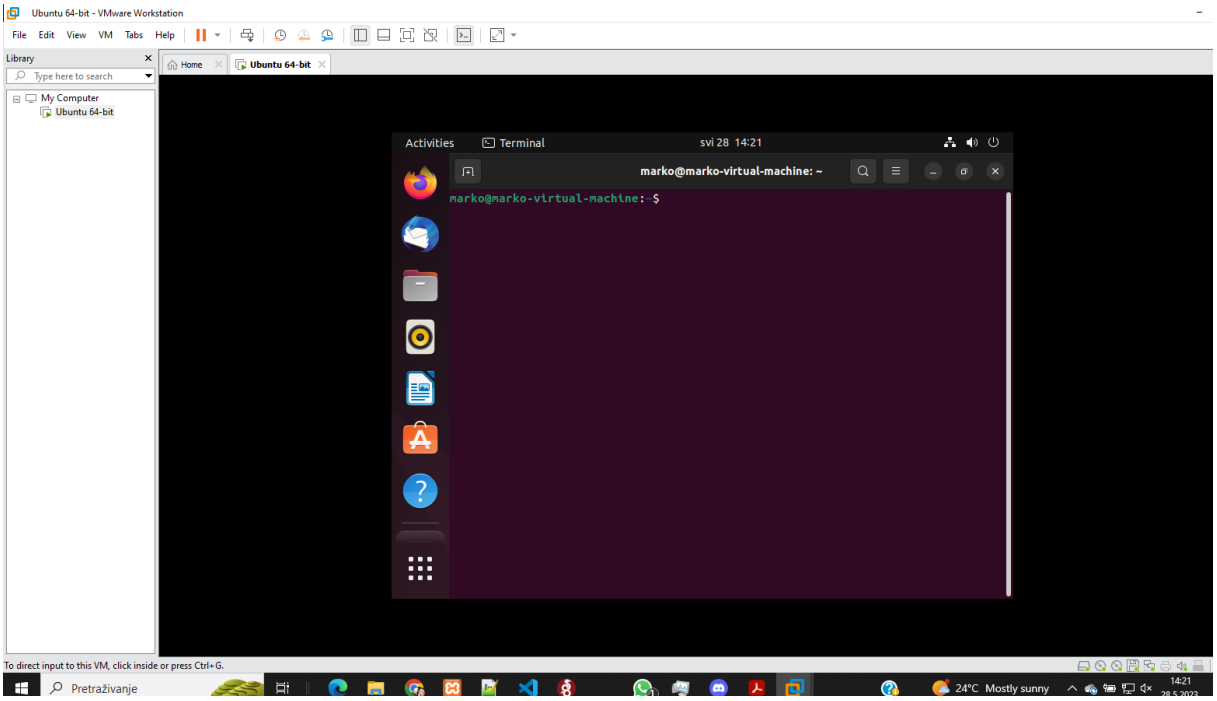
uređajima većina popularnih VPN-ova nudi WireGuard protokol.

Što se tiče jednostavnosti korištenja, WireGuard je jednostavan u usporedbi s OpenVPN-om. To se također može pripisati njegovoj manjoj bazi koda, što ga čini boljom opcijom za ugrađene sustave. OpenVPN je bilo i još uvijek je teško konfigurirati ručno (Zoltan, 2022).

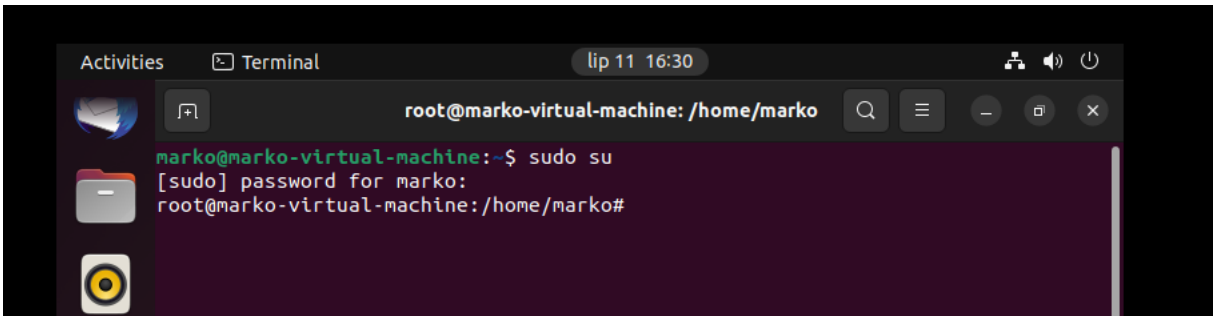
4. Instalacija i testiranje Wireguarda

Za samu implementaciju i testiranje virtualne privatne mreže instalirao sam *VMware Workstation* koja slovi za jednu od najpoznatijih softverskih aplikacija koja omogućuje virtualizaciju računalnih sustava na radnim stanicama.

Prije instalacije samog wireguarda potrebno je instalirati neki od operacijskih sustava u virtualnoj mašini. Ubuntu je popularna Linux distribucija operativnog sustava koja se temelji na Debianu. On je izabran zbog jednostavnosti korištenja, stabilnosti i sigurnosti, te je definitivno najkorišteniji sustav za VPN-ove. Najviše objašnjenih uputa,videa i prezentacija u vezi wireguarda upravo je rađeno u Ubuntu-u.



Na slici se vidi sučelje Ubuntu-a u kojem je kreirana „markova“ virtualna mašina. Nakon pripreme servera, potrebno je instalirati Wireguard na sami server.



„Sudo su“ je naredba kojom se pokreću administratorske opcije, te je potrebno upisati lozinku koju smo unijeli prilikom instalacije virtualne mašine.

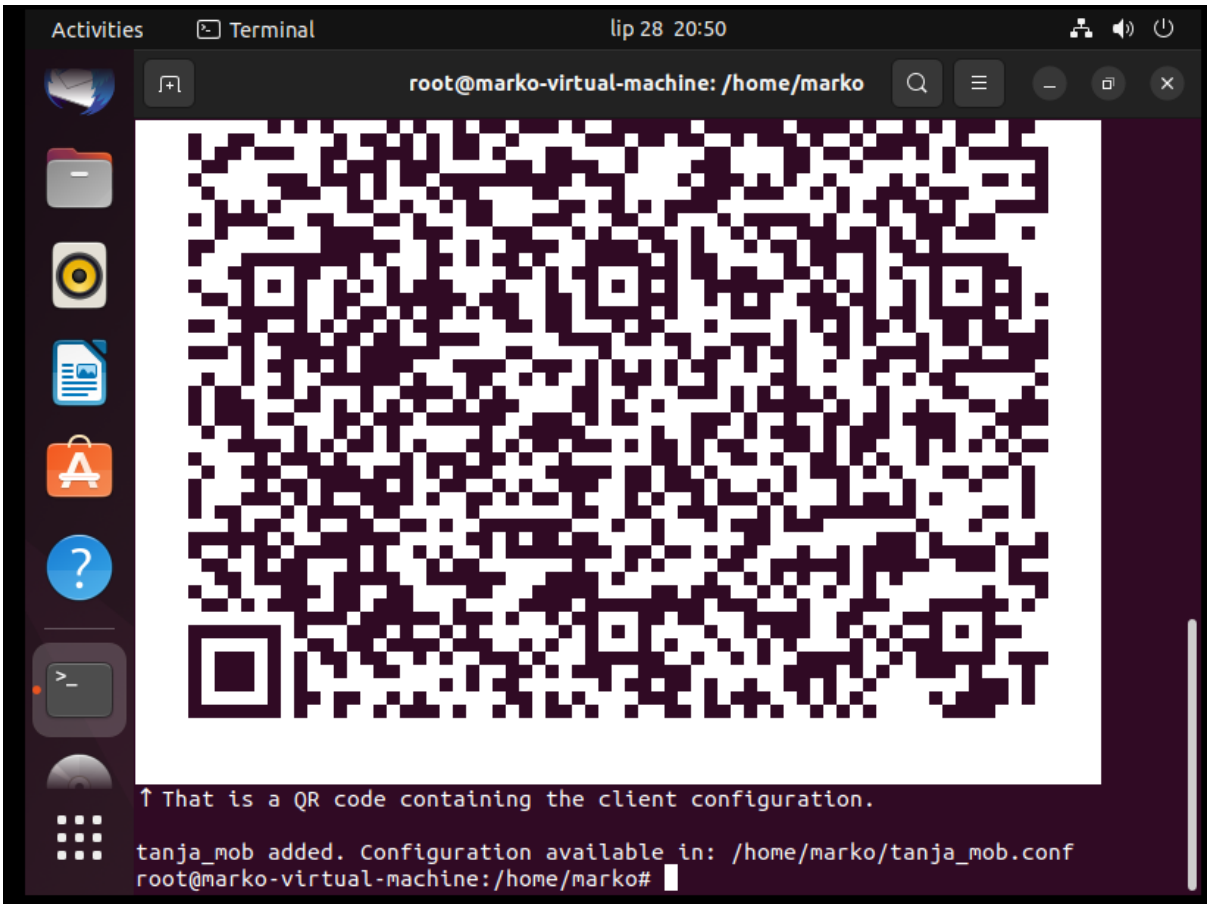
Nakon toga potrebno je skinuti skriptu za instalaciju na lokalni server. To se radi uz pomoć komande“wget –O wireguard.sh http://get.vpnsetup.net/wg“ s kojom skidamo spremnu skriptu za instalaciju.

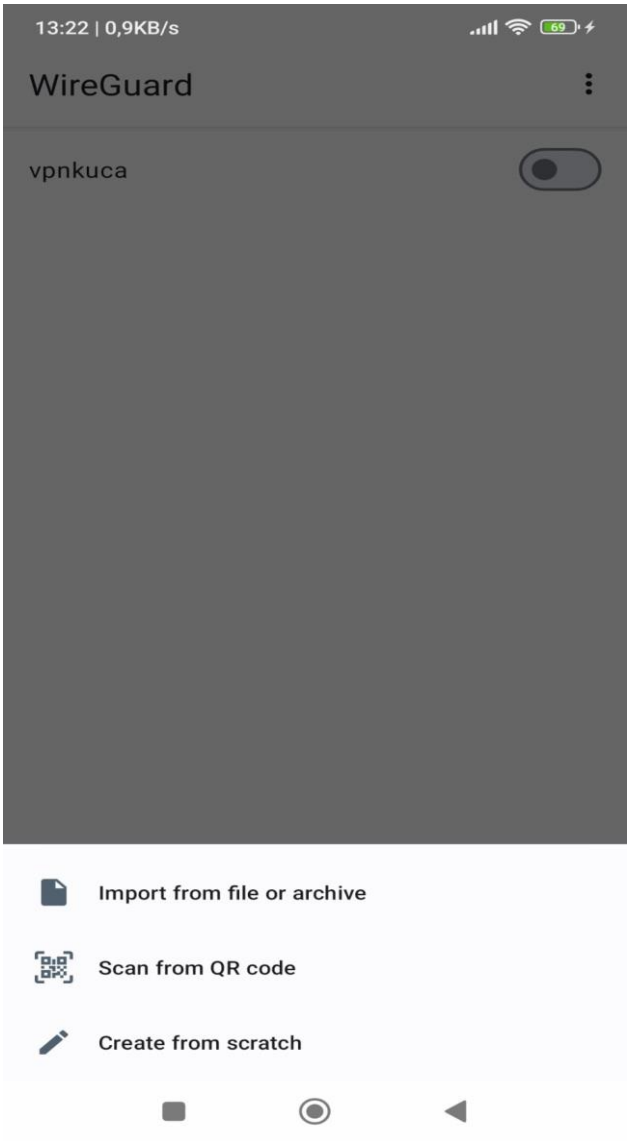
„chmod +x wireguard.sh“ komanda je koja nam daje prava za pokretanje, te se nakon nje uz komandu „bash wireguard.sh“ pokreće skripta za instalaciju.

Prilikom instalacije skripte, automatski se konfiguriraju osnovne postavke, te generiraju ključevi za nas. Naravno, nakon instalacije, možemo prilagoditi konfiguraciju prema našim potrebama.

Nakon što nam je sve instalirano, potrebno je generirati ključeve (javni i privatni) za klijenta, odnosno mobitel s kojim ću se povezati na VPN.

Prilikom dodavanja klijenta pojavi se QR kod (na slici ispod) koji, nakon što smo na mobitel instalirali wireguard, služi da putem mobitela skeniramo kod, te se povežemo na VPN.


Activities
Terminal
lip 28 20:50
root@marko-virtual-machine: /home/marko
↑ That is a QR code containing the client configuration.
tanja_mob added. Configuration available in: /home/marko/tanja_mob.conf
root@marko-virtual-machine:/home/marko#



Na samom mobitelu, imamo tri opcije povezivanja na VPN, ali svakako najjednostavnija je putem skeniranja QR koda.

Nakon uspješnog instaliranja na obje strane, te nakon spajanja s mobitelom, na slici ispod se vidi da smo uspješno povezani. „*Latest handshake*“ nam daje informaciju o vremenu kada su dvije strane posljednji put razmijenile podatke potrebne za uspostavljanje i održavanje sigurne VPN mreže (slika ispod).


18:37 | 1,5KB/s
VPN
29
WireGuard
Interface
Name
vpnkuca
Public key
2WWKAaRrTz9+QGxul5EbCh5WcDnrlnZxv4Ht…
Addresses
10.7.0.2/24
DNS servers
8.8.8.8, 8.8.4.4
Peer
Public key
T7G6eykpUaxfJCJbZHSCLOIHjOr3qdfdgIvXrF…
Pre-shared key
enabled
Allowed IPs
0.0.0.0/0, ::/0
Endpoint
192.168.1.7:51820
Persistent keepalive
every 25 seconds
Transfer
rx: 124 B, tx: 18,29 KiB
Latest handshake
18 sekundi ago

5. ZAKLJUČAK

Glavna prednost VPN tehnologije jest što korisnicima omogućuje preko javne mrežne infrastrukture povezivanje računala u virtualne privatne mreže koje im jamče zaštitu podataka tijekom prijenosa. One funkcioniraju tako da stvaraju privatni tunel kroz Internet od pošiljatelja do primatelja. Uz sigurnost, korisnicima jamče fleksibilnost, brzinu, finacijsku uštedu, ali i privatnost.

VPN ovisi o metodama tuneliranja za prijenos podataka, te postoje različite vrste protokola (IPsec, PPP, PPTP, L2TP itd.)Svi oni imaju svoje prednosti i nedostatke, a koji protokol će korisnik implementirati zavisi o njegovim potrebama i očekivanjima.

Novo rješenje u ovom području jest WireGuard VPN protokol otvorenog koda koji koristi najsuvremeniju kriptografiju i ima za cilj nadmašiti postojeće VPN protokole kao što su IPsec i OpenVPN. Iako je tek odnedavno prisutan, WireGuard se već nametnuo kao jedno od boljih VPN rješenja zbog svoje prilagodljivosti, brzine, jednostavnosti i sigurnosti koju pruža korisnicima. Za razliku od OpenVPN kojeg želi nadmašiti, WireGuard ima daleko manji broj kodnih linija i kao takav manje je podložan napadima, a sa druge strane, iz istog razloga, jednostavnije ga je usavršiti, te u njega implementirati prema potrebi nova sigurnosna rješenja. Jedna od njegovih ključnih prednosti jest i korištenje najnovijih metoda kriptiranja što također povećava njegovu sigurnost i čini ga izravno konkurentnim dosad vrlo prihvaćenom i iznimno sigurnom OpenVPN-u.

S druge strane, WireGuard je mobilniji, jednostavniji i jeftiniji za održavanje i brži, te iako je OpenVPN već dugo na tržištu i kao takav je postigao korisničku lojalnost kroz svoje performanse i kvalitete, predviđanja stručnjaka na temelju dosadašnjih pokazatelja, ukazuju da će WireGuard uskoro ostvariti identičnu korisničku prisutnost.

6. LITERATURA

1. Carmouche, J. H., (2006) : *IPsec virtual private network fundamentals an introduction to VPNs*, Indianopolis, Indiana, USA: Cisco Press.
2. Ervin, M., Scott, C., Wolfe, P., (1999): *Virtual Private Networks: Turning the Internet Into Your Private Network*, O'Reilly & Associates, Inc.
3. Amankatiyar, A., Hemantjain, A., Surana J. (2017): *Research on Tunneling Techniques in Virtual Private Networks*," IJEDR, 5(2) 2321-9939
4. Hrvatska akademska i istraživačka mreža CARNet (2003): *Osnovni koncepti VPN tehnologije*, Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf
5. Kovačić, B., Skendžić, A. (2017): *Open source system OpenVPN in a function of Virtual Private Network, IOP Conference Series: Materials Science and Engineering*, Dostupno na: https://www.researchgate.net/journal/IOP-Conference-Series-Materials-Science-and-Engineering-1757-899X
6. Lipp, B., Blanchet, B., Bhargavan, B. (2019): *A Mechanised Cryptographic Proof of the WireGuard VPN Protocol, Research report,* RR-9269, Inria Paris, Dostupno na: file:///C:/Users/HP/Desktop/op%C4%87enito%20o%20wireguardu%20i%20njegov%20na%C4%8Din%20rada,%20security%20goals.pdf
7. Rubertis, A. i sur. (2013): *Performance evaluation of end-to-end security protocols in an internet of things, In 2013 21st International Conference on Software, Telecommunications and Computer Networks-(SoftCOM 2013*), Dostupno na: https://doi.org/10.1109/softcom.2013.6671893
8. Datashield (bez datuma): *What is VPN?,* Dostupno na: https://www.datashieldprotect.com/blog/what-is-a-vpn
9. Donenfeld, J. (2020): *WireGuard: Next Generation Kernel Network Tunnel,* Dostupno na: https://www.wireguard.com/papers/wireguard.pdf
10. Ghimiray, D.(2022): *WireGuard VPN Protocol: The New, Secure, and Fast VPN Protocol*, Dostupno na: https://www.avast.com/c-wireguard-vpn
11. Hopkins, J. i Green, M. (2019): *OpenVPN-Evaluation Summary and Report, Private Internet Access Blog*, Dostupno na: https://www.privateInternetaccess.com/blog/2017/05/openvpn-2-4-evaluationsummary-report
12. IBM (bez datuma): *What is encryption? Data encryption defined*, Dostupno na :

https://www.ibm.com/topics/encryption
13. Loshin, P. (2021): Ipsec (Internet Protocol Security), TechTarget, Dostupno na: https://www.techtarget.com/searchsecurity/definition/IPsec-Internet-Protocol-Security
14. Mash, R. (bez datuma): *OpenVPN VPN Protocol*, Dostupno na: https://privacyhq.com/documentation/openvpn-vpn-protocol/
15. Zola, A. (2021): *Layer Two Tunneling Protocol (L2TP),* Tachtarget, Dostupno na: https://www.techtarget.com/searchnetworking/definition/Layer-Two-Tunneling-Protocol-L2TP
16. Zoltan, M. (2022): WireGuard vs OpenVPN: *Which Protocol Should You Use?, Privacy affairs*, Dostupno na: https://www.privacyaffairs.com/wireguard-vs-openvpn/