Implementacija virtualnih privatnih mreža

Klopotan, Lucija

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Lucija Klopotan

IMPLEMENTACIJA VIRTUALNIH PRIVATNIH MREŽA

ZAVRŠNI RAD

Varaždin, 2021.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Lucija Klopotan

Matični broj: 47080/18-R

Studij: Poslovni sustavi

IMPLEMENTACIJA VIRTUALNIH PRIVATNIH MREŽA

ZAVRŠNI RAD

Mentor:

Doc. dr. sc. Nikola Ivković

Varaždin, Rujan 2021.

Lucija Klopotan

Izjava o izvornosti

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

Autorica potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Širenjem interneta i njegovom stalnom upotrebom kod korisnika javlja se potreba za zaštitom podataka na internetu. Od početka interneta radilo se na razvijanju mreže koje bi mogla pružiti siguran prijenos podataka i koja bi bila široko dostupna. Upravo tu ulogu ima VPN. Zahvaljujući velikom broju pružatelja usluga dostupan je gotovo svima, a njegova svrha je zaštita podataka i anonimnost korisnika mreže. U ovom završnom radu objašnjena je svrha VPN-a, način na koji on funkcionira te kako se razvijao kroz povijest. Osim toga, u praktičnom dijelu rada implementiran je VPN na dva načina te je obrazloženo koji način je bolji za korištenje i u kojem slučaju.

Ključne riječi: Virtualna privatna mreža, sigurnost, internet, prijenos podataka, IP adresa, poslužitelj, protokol, veza, tunel.

Sadržaj

1. Uvod ... 1
2. Razvoj virtualnih privatnih mreža ... 2
3. Standardni prijenos podataka ... 5
3.1. Domena ... 5
3.2. Sustav domenskih imena ... 6
4. Pojam VPN-a ... 8
4.1. Virtualna privatna mreža ... 8
4.1.1. Enkripcija ... 8
4.1.2. Enkapuslacija ... 10
4.1.3. Tuneliranje ... 10
4.2. Karakteristike VPN-a ... 11
4.3. Prijenos podataka virtualnom privatnom mrežom ... 12
5. VPN protokoli ... 13
5.1. IPsec ... 13
5.2. L2TP ... 14
5.3. OpenVPN ... 16
6. Podjela virtualnih privatnih mreža ... 17
6.1. Site-to-Site VPN ... 17
6.2. Remote-Access VPN ... 18
7. Prednosti i nedostaci VPN-a ... 19
7.1. Prednosti ... 19
7.2. Nedostaci ... 20
8. Implementacija virtualne privatne mreže ... 21
8.1. Implementacija VPN-a na Microsoft Azureu ... 21
8.2. Instalacija TunnelBear VPN-a ... 27
9. Zaključak ... 28
Popis literature ... 29
Popis slika ... 31
Popis tablica ... 31

1. Uvod

Sigurnost podataka jedna je od najvažnijih stvari prilikom korištenja interneta. U svakom trenutku mrežom se kreću privatni podaci korisnika koji su izloženi krađi i zloupotrebi. Kako bi se ti podaci zaštitili i sakrili koristi se virtualna privatna mreža. Iako je to pojam koji se često spominje rijetki zapravo znaju što je to i na koji način funkcionira. Ovaj završni rad objasnit će što je to VPN, kako funkcionira te kako se implementira.

Ovaj završni rad podijeljen je na teorijski i implementacijski dio. U teorijskom dijelu je objašnjeno kako su se kroz povijest razvijali internet i VPN mreže. Nakon toga je opisano kako izgleda standardan prijenos podataka mrežom, što je to domena te na koji način se dohvaćaju podaci prilikom pretraživanja interneta. U glavnom dijelu rada slijedi detaljna razrada VPN-a. Objašnjene su karakteristike VPN-a, koje su to metode kojima se štite podaci prilikom prijenosa internetom te kako funkcionira prijenos podataka virtualnom privatnom mrežom. Osim toga, objašnjena su dva načina povezivanja koje VPN koristi te koje su njihove razlike. Nakon obrađene teorije navedeni su glavne prednosti i nedostaci VPN-a. U praktičnom dijelu implementiran je VPN na dva načina: instalacija VPN-a od strane pružatelja usluge i implementacija *remote-access* VPN-a uz pomoć platforme Microsoft Azure. S obzirom na kompleksnost implementacije Azure VPN-a, detaljno su opisani koraci koje je potrebno napraviti kako bi se realizirao VPN. Nakon završetka obje implementacije napravljen je kratki osvrt na implementaciju te je uspoređeno koja implementacija je bolja.

Cilj ovog rada je prikazati na koji način se koristi VPN, koje su njegove prednosti i nedostaci te koji je razlog zbog kojeg bi netko koristio VPN. Osim toga, cilj je usporediti razliku između kreiranja vlastitog VPN-a i instalacije aplikacije od pružatelja usluge te dati osvrt na temlju kojeg bi budući korisnici mogli odlučiti žele li koristiti VPN i ako da, na koji način ga žele implementirati.

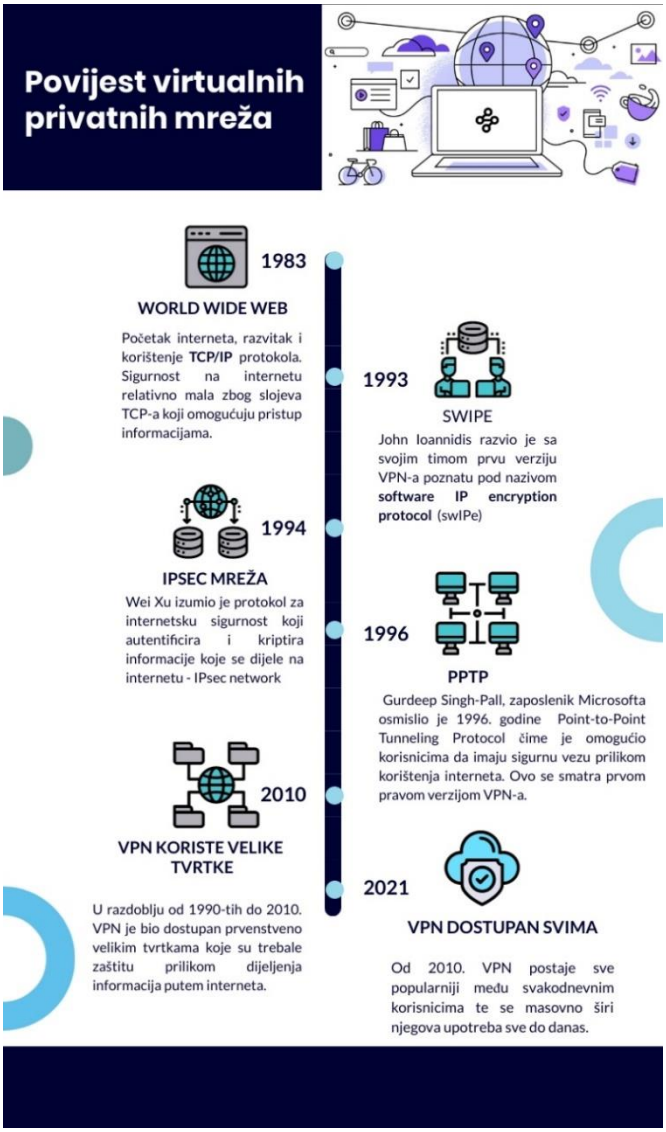
2. Razvoj virtualnih privatnih mreža

Od samog začetka interneta pa sve do danas, broj korisnika se drastično povećavao. Samim time povećava se i protok informacija i podataka između korisnika što na kraju dovodi i do povećanja nesigurnosti i velike izloženosti tih informacija. Ako uzmemo sve to u obzir, od početka korištenja interneta postoji potreba za zaštitom privatnih podataka. U ovom poglavlju će biti objašnjeno na koji način se ta zaštita provodila u djelo u samim početcima te kako je došlo do razvitka virtualne privatne mreže kakvu poznajemo danas.

Internet kakav poznajemo danas razvijao se dugi niz godina poboljšavajući postepeno brzinu, sigurnost, raširenost i dostupnost. Razvoj interneta započeo je početkom 60-tih godina prošlog stoljeća kada se javila potreba za tehnologijom koja će omogućiti dijeljenje informacija između priznatih institucija i sveučilišta koja su se nalazila na geografski udaljenim lokacijama. Prvi zapisi u kojima se opisuje mogućnost komuniciranja i slanja informacija te povezanosti cijelog svijeta putem interneta nalaze se u dopisima američkog znanstvenika J.C.R Licklidera, tadašnjeg zaposlenika popularnog američkog sveučilišta „*Massachusetts Institute of Technology*“ (u daljnjem tekstu: MIT). [1]

Kako je potreba za razmjenom informacija rasla, američki odjel za obranu krenuo je u istraživanje i implementaciju mogućnosti komuniciranja putem tehnologije između udaljenih lokacija. Grupa stručnjaka je tako početkom 1960-tih osnovala eksperimentalni program „*Advanced Research Projects Agency Network“* (u daljnjem tekstu: ARPANET) kojemu je cilj bio poboljšati komunikaciju između računala te koji je s vremenom postao preteča današnjeg interneta. Prva uspješna izmjena podataka između dva čvora dogodila se 1969. godine kada je s jednog računala na drugo poslana jednostavna poruka sa sadržajem „LOGIN“. Iako nije uspješno prenesena cijela poruka s jednog računala na drugo, ovaj događaj označio je početak jednog novog razdoblja u kojemu će se razviti internet kakvog poznajmo danas. [2]

Nakon izuma ARPANET-a, 1983. godine osnovan je "*Transmission Control Protocol/Internet Protocol*" (u daljnjem tekstu: TCP/IP) koji je bio podloga za osnivanje World Wide Weba[1]. Navedeni protokol sastoji se od 4 sloja: sloj podatkovne veze, mrežni sloj, transportni sloj i aplikacijski sloj. Sloj podatkovne veze omogućuje pristup podacima koji se šalju putem mreže te time čini komunikaciju putem interneta nesigurnom. Kako su to bili samo začeci interneta, nije ni bilo potrebe za prevelikom sigurnošću jer je u komunikaciji sudjelovao relativno mali broj računala (većinom fakulteti i sveučilišta). Kako je broj korisnika rastao, tako se povećavala potreba za sigurnošću podataka koji su se prenosili. Tada se na sveučilištu *„Colombia University"* okupio tim stručnjaka na čelu s Johnom Ioannidisom koji su počeli istraživati sigurnost prijenosa podataka na internetu. Njihov rad rezultirao je razvojem protokola „*Software IP encryption protocol*„ (u daljnjem tekstu: swIPe) što se smatra prvom verzijom virtualne privatne mreže. [3]



Slika 1. Povijest VPN-a [autorski rad]

Nakon izuma swIPe protokola, stručnjaci su nastavili s razvojem protokola koji će moći u potpunosti zaštititi podatke prilikom prijenosa mrežom. 1994. godine Wei Xu stvorio je protokol pod nazivom *„Internet Protocol Security"* (u daljnjem tekstu: IPsec) koji je omogućava autentikaciju i kriptiranje podatkovnih paketa pružajući siguran prijenos paketa od računala do računala. Narednih godina se radilo na poboljšavanju protokola kako bi postao što napredniji, sigurniji i brži. Potreba za mrežom koja omogućuje potpunu sigurnost

[1] Kolekcija web stranica koje su pohranjene na web poslužiteljima, a povezane su s lokalnim računalima putem interneta

prilikom razmjene podataka putem interneta bila je sve bliže ispunjenju cilja. Napokon, 1996. godine, Microsoftov zaposlenik Gurdeep Singh-Pall započeo je s razvojem protokola *„Point-to-Point Tunneling Protocol“* (u daljnjem tekstu: PPTP) koji će moći ispuniti sva očekivanja korisnika omogućujući im sigurnu internetsku vezu. Ovaj protokol smatra se početkom virtualne privatne mreže kakvu poznajemo danas. [4]

Do kasnih 2000-tih godina, VPN je bio korišten većinom od strane velikih kompanija koje su bile u mogućnosti priuštiti si takvu tehnologiju. Velikim tvrtkama trebao je privatni i sigurni način komunikacije kao i mogućnost sigurnog dijeljenja poslovnih datoteka između ureda koji su bili smješteni u različitim dijelovima svijeta. VPN mreža ispunila je sve njihove potrebe te je povezala urede smještene na različitim lokacijama u jednu privatnu poslovnu mrežu. Osim toga, učinila je poslovanje mnogih kompanija znatno sigurnijim. Kako je vrijeme prolazilo, VPN mreža postajala je sve popularnija i korištenija zbog sigurnosti koju je pružala. Početkom 2000-tih godina na tržištu su se počele pojavljivati razne tvrtke koje su pružale virtualnu privatnu mrežu. U tom razdoblju je VPN postao puno pristupačniji običnim, svakodnevnim korisnicima interneta s obzirom na to da su drastično pale cijene pružanja usluge. Osim toga, korisnici su shvatili kako im VPN pruža različite mogućnosti kojih do tada nisu bili ni svjesni.[3]

Kako se internet razvijao, sa sobom je donosio i određeni niz restrikcija i novih izazova. Neki od njih uključuju blokiranje sadržaja ovisno o geo-lokaciji, cenzuriranje sadržaja, hakiranje i špijuniranje. No korištenjem virtualne privatne mreže takve stvari više nisu predstavljale problem. Promjenom IP adrese mogao se lako riješiti problem geo-lokacije i dostupnosti sadržaja na internetu kao i problem cenzuriranja. Sigurnost koju pružaju VPN protokoli je riješila probleme hakiranja i špijunaže. Sve to je s vremenom dovelo do masovne raširenosti i primjene VPN-a na dnevnoj bazi u gotovo svim zemljama svijeta. Danas se VPN većinom koristi kako bi se moglo pristupiti sadržaju poput Netflixa ili društvenih mreža koje su ograničene u pojedinim državama. To je jedan od glavnih razloga zbog čega se iz godine u godinu povećava njegova upotreba i raširenost. [3] Osim toga, radi se i na osnivanju novih protokola koji će ubrzati i pojednostaviti VPN. Jedan od takvih protokola je i *WireGuard*.[2][4]

[2] Jednostavan protokol koji predstavlja šifrirani tunel između dvije točke te se zasniva na jednostavnosti i dostupnosti.[4]

3. Standardni prijenos podataka

Kako bi se u potpunosti shvatila svrha VPN-a i na koji način funkcionira, potrebno je prvo objasniti na koji način funkcionira internet te koje su razlike između standardnog prijenosa podataka i prijenosa podataka putem privatne virtualne mreže. Prilikom objašnjavanja načina funkcioniranja interneta opisat će se što su to domene, IP adrese i poslužitelji te na koji način se podaci na internetu prenose. Svi navedeni pojmovi su preduvjet razumijevanja na koji način funkcioniraju internet i VPN mreže.

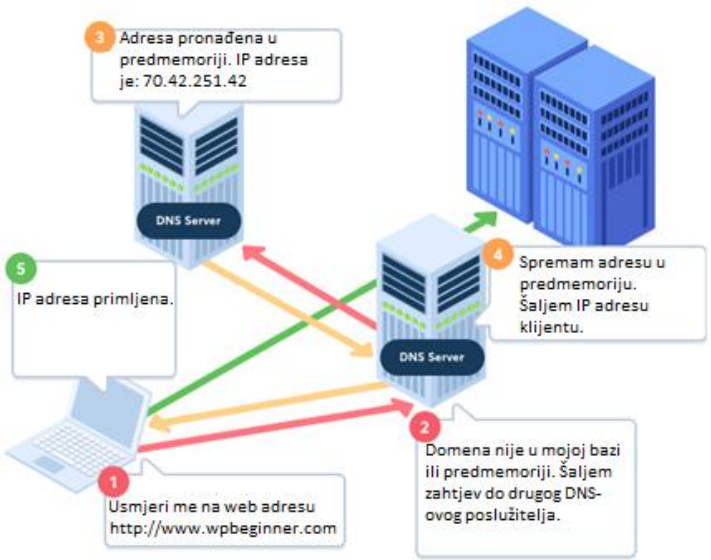
Internet predstavlja globalnu mrežu međusobno povezanih uređaja koji mogu međusobno komunicirati. Kako bi se znalo gdje točno treba dostaviti podatke, svaki uređaj ili lokalna mreža spojena na internet mora imati jedinstvenu oznaku uz pomoć koje komunicira s ostalim uređajima. Ta oznaka naziva se IP adresa te predstavlja jedinstveni niz brojeva koji jednoznačno identificiraju određeni uređaj u mreži (primjer IP adrese: 66.249.66.1). S obzirom na to da svaka internetska stranica ima svoju IP adresu, a ovakve nizove brojeva je teže za pamtiti problem je riješen uvođenjem internetske domene. [5]

3.1. Domena

Internetska domena predstavlja tekstualni naziv stranice koji zamjenjuje IP adresu kako bi pretraživanje internetom bilo jednostavnije i brže. [5]. Kako bi se dočarala razlika između internetske domene i IP adrese može se uzeti primjer pravih adresa stanovanja. Geografski gledano, svaka lokacija na zemlji se može odrediti geografskom širinom i duljinom. Tako je primjerice geografska lokacija Empire State Buildinga *40.7484° N, 73.9857° W.* No, poprilično je teško pamtiti niz brojeva za svaku lokaciju koju želimo posjetiti. U tu svrhu postoje adrese lokacija, u ovom slučaju adresa za Empire State Building je 20 W 34th St, New York, NY 10001, USA. Ovakve tekstualne lokacije puno je lakše zapamtiti od niza brojeva pa su takvi nazivi raširenija i korištenija. Ista stvar događa se prilikom korištenja interneta. Umjesto pamćenja niza brojeva za svaku stranicu koju korisnik želi posjetiti potrebno je zapamtiti samo domenu stranice (npr. google.com).

3.2. Sustav domenskih imena

Kada korisnik unese naziv web stranice i pritisne na pretraži, računalo šalje zahtjev za tom stranicu do poslužitlja *Domain Name System* (u daljnjem tekstu: DNS). DNS predstavlja decentralizirani sistem poslužitelja čija je svrha pretvaranje naziva domene u IP adresu koja je povezana s navedenim nazivom. [6] Kada zahtjev dođe do određenog DNS-ovog poslužitelja, prvo se provjerava ima li spremljen zapis u vlastitoj bazi podataka, ako je pronalazak zapisa u vlastitoj bazi podataka neuspješan poslužitelj DNS-a šalje zahtjev do drugog poslužitelja DNS-a i tako sve dok ne dođe do poslužitelja koji sadrži traženi zapis. Pronađena IP adresa vrati se do početnog poslužitelja gdje ju on pohranjuje u svoju predmemoriju u slučaju da mu ponovno dođe zahtjev za istom IP adresom. Nakon toga vraća traženu IP adresu do računala koje je poslalo zahtjev. [5] DNS-ove poslužitelje može se usporediti s telefonskim imenom koji se nalazi na mobitelu. Umjesto da pamtimo sve brojeve telefona, spremamo ih u imenik kako bi ih kasnije bilo lakše za pronaći. U ovom primjeru, domena bi predstavljala ime i prezime kontakta koji se pretražuje dok bi IP adresa predstavljala broj telefona ili mobitela.



Slika 2. Dohvaćanje doemene web stranice [5]

Nakon dohvaćanja IP adrese potrebno je na dobivenu IP adresu poslati zahtjev za dohvaćanje web stranice. Prilikom dohvaćanja stranica na internetu razlikujemo klijentsku i poslužiteljsku stranu. Klijent je bilo koji uređaj spojen na internetsku mrežu s kojeg se šalje

zahtjev za određenom stranicom kao npr. mobitel, laptop ili računalo. S druge strane poslužitelj predstavlja uređaj, odnosno računalo, na kojem je pohranjena tražena web stranica ili aplikacija te koja vraća odgovor na klijentov zahtjev.

Osim klijenta i poslužitelja, između njih se nalazi još nekoliko komponenata koje su bitne za uspješnu razmjenu podataka na internetu [7]:

- **Internetska veza** - omogućava uspješno spajanje na internet
- **TCP/IP protokol** - odlučuje na koji način će se podaci kretati putem interneta
- **DNS-ov poslužitelj** - dohvaća IP adresu tražene stranice
- **HTTP protokol** - definira jezik između klijenta i poslužitelja
- **Komponentne datoteke** – podaci za prijenos koji čine web stranicu

Prvi korak dohvaćanja internetske stranice je dohvaćanje IP adrese s DNS-ovog poslužitelja što je objašnjeno u prethodnim poglavljima. Nakon što je dohvaćena IP adresa željene internetske stranice HTTP protokol šalje zahtjev na poslužitelj u kojemu traži da poslužitelj pošalje kopiju web stranice. Osim zahtjeva, šalju i razne druge informacije kao što je IP adresa klijenta, lokacija uređaja, IP adresa rutera i ostale potrebne informacije kao korisničko ime ili lozinka. Zahtjev za stranicom, zajedno sa svim ostalim podacima, putuje do poslužitelja putem TCP/IP protokola. Ako poslužitelj odobri pristup stranici, putem TCP/IP protokola pošalju se paketi u kojima se nalaze komponentne datoteke stranice. Kada ti paketi doputuju do klijenta web preglednik ih sastavi te prikaže krajnjem korisniku. [7]

Ono što je problematično u procesu slanja i primanja paketa putem mreže jest njihova sigurnost. Već je spomenuto ranije kako se uz zahtjev za prikaz web stranice šalju i razne informacije poput IP adrese i lokacije uređaja. Osim takvih informacija često se u paketima šalju razne lozinke, korisnička imena i drugi povjerljivi podaci. S obzirom da se ti podaci šalju u paketima putem javne mreže te nisu pretjerano zaštićeni vrlo im je lako pristupiti i pročitati ih. Uzmimo na primjer da osoba A sjedi u kafiću i spojena je na internetsku mrežu. Na tu istu internetsku mrežu spojene su i sve druge osobe u kafiću. Osoba A odluči provjeriti stanje na bankovnom računu ili obaviti online kupovinu te unosi sve potrebne podatke u aplikaciju ili na web stranicu. Osoba B koja također sjedi u kafiću presretne podatkovne pakete koji se šalju putem mreže od računala osobe A do poslužitelja te preuzme sve povjerljive podatke. S obzirom da ti podatkovni paketi nisu bili osigurani osoba B ih vrlo kao može pročitati i zloupotrijebiti. Upravo je to razlog zbog kojeg je preporučena upotreba virtualne privatne mreže. [8]

4. Pojam VPN-a

Virtualna privatna mreža ili VPN je pojam koji se danas spominje vrlo često. Gotovo svaka osoba koja koristi internet čula je za pojam VPN-a dok se velika većina korisnika njime i koristi. No što točno predstavlja virtualna privatna mreža i koja je njena uloga na internetu? Ovo poglavlje objasnit će što je to točno VPN te kako je građen. Osim toga, objasnit će i na koji način se prenose podaci putem VPN-a te koje su razlike između korištenja obične mreže i virtualne privatne mreže.

4.1. Virtualna privatna mreža

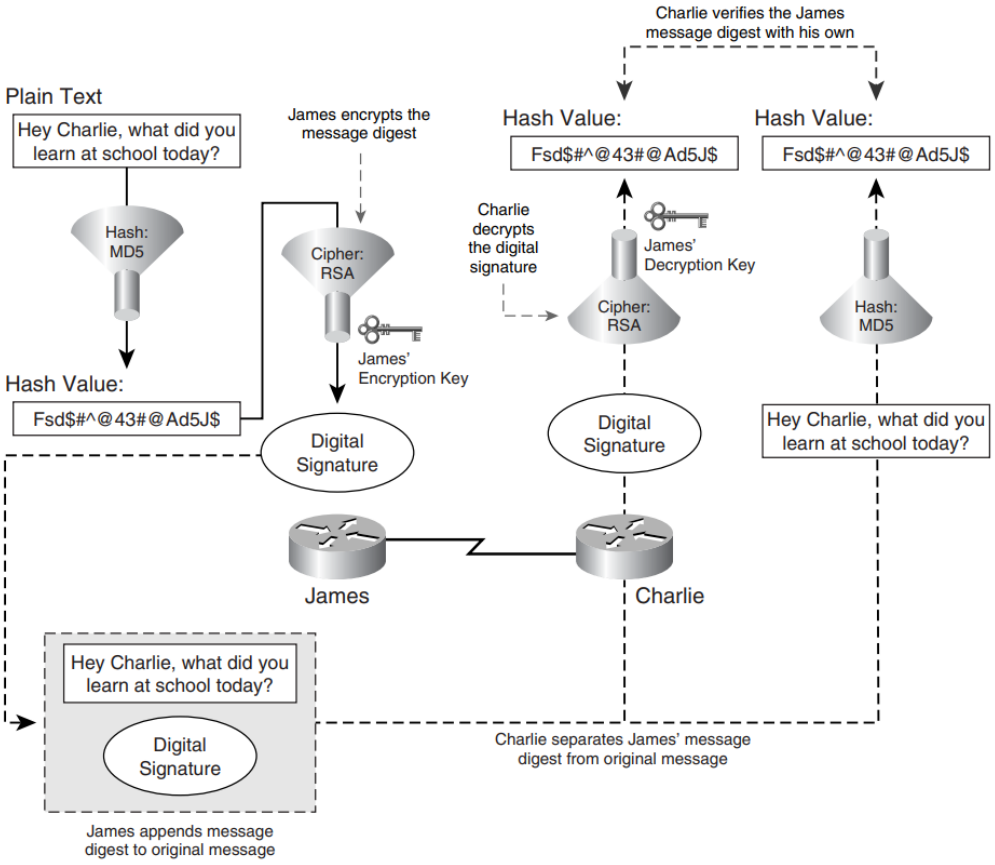
Prema J.Snaderu [9, str. 155], virtualna privatna mreža predstavlja proširenje osnovne mrežne infrastrukture, a služi za privatno i sigurno slanje podataka putem interneta. Glavni cilj takve mreže je stvoriti iluziju prividne privatne mreže, dok se u stvarnosti koristi javna mrežna infrastruktura kao što je internet. Kako bi se ostvarila privatnost na internetu, VPN koristi metode poput enkripcije, enkapsulacije i tuneliranja koje će biti opisane u ovom poglavlju.

4.1.1. Enkripcija

Enkripcija osigurava da samo primatelj i pošiljatelj mogu pročitati podatke koji se šalju putem mreže. Podaci se prilikom slanja zamjenjuju nizom različitih znakova, odnosno kriptiraju se uz pomoć raznih metoda kao što su RSA, AES, DES i Triple Des. Kriptiranje se može obaviti na dva načina – simetričnom ili asimetričnom metodom. Kod asimetrične metode koriste se dva ključa, javni i privatni, uz pomoć kojih se šifrira i dešifrira poruka. S druge strane simetričnom metodom se koristi samo privatni ključ koji služi za šifriranje i dešifriranje poruke. Obje metode pružaju siguran prijenos podataka na internetu. [10]

Kako bi se osiguralo da podaci koji stignu do primatelja nisu mijenjani prilikom prijenosa, na stvarnu poruku dodaju se jedinstvene poruke, odnosno tzv. *hash* poruke ili digitalni potpisi. *Hash* poruka predstavlja niz različitih znakova koji pružaju dodatnu zaštitu kod slanja poruke. Prilikom primanja poruke primatelj zaprima *hash* poruku i stvarnu kriptiranu poruku. Ako se dobiveni *hash* u poruci ne poklapa s lokalno generiranom *hash* porukom došlo je do izmjene podataka prilikom slanja poruke te se gubi autentičnost poruke. Poruka također nije sigurna ako se ključevi primatelja i pošiljatelja ne poklapaju, odnosno primatelj ne može dešifrirati poruku ključem koji posjeduje. [11]

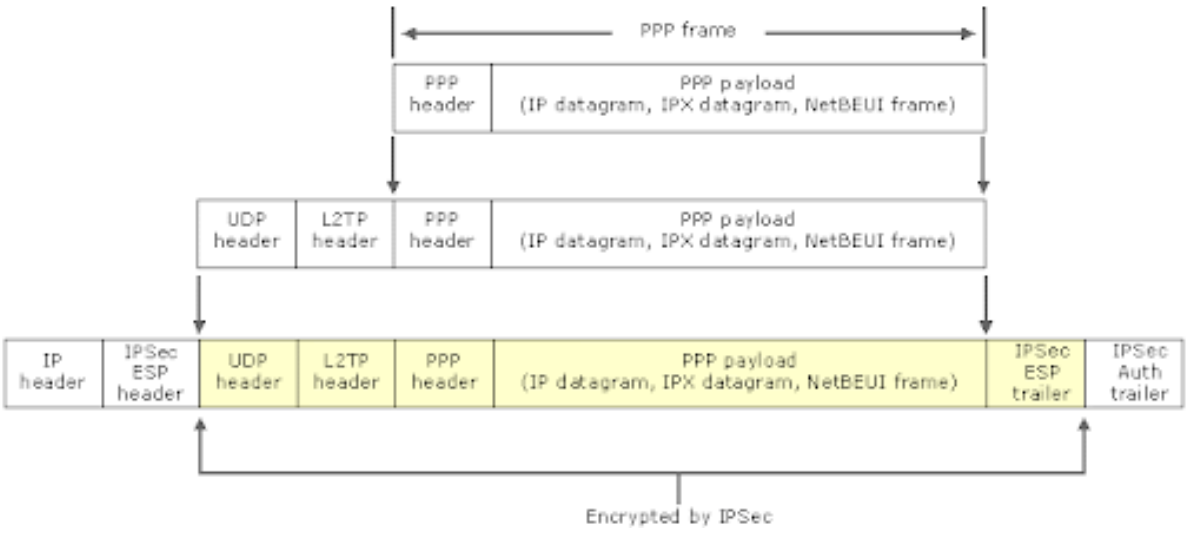
Primjerice, ako gledamo komunikaciju između dvoje ljudi, osoba A kriptira poruku sa svojim privatnim ključem, dok svoj javni ključ podijeli s osobom B kako bi ona mogla dešifrirati poslovnu poruku. Ako ključ koji posjeduje osoba B ne odgovara onom ključu koji je potreban za dešifriranje to bi značilo kako je poruka koja je došla do primatelja neautentična te čak i nesigurna. Osim toga, ključevi su tu kako bi se osigurala i neporecivost pošiljatelja. Ako za neku poruku postoji točno određeni par privatnog i javnog ključa, pošiljatelj ne može poreći kako on nije poslao poruku jer ga se može povezati s ključem kojim je šifrirana poruka. Kao što je navedeno u primjeru iznad, poruka se može dešifrirati samo ako se koristi javni ključ pošiljatelja. [11] Proces slanja i primanja kriptirane poruke koji je opisan iznad vizualno je prikazan na slici 2.



Slika 3. Kriptiranje podataka. [11, str.8]

4.1.2. Enkapuslacija

Enkapsulacija se brine o skrivanju paketa koji se šalju putem mrežne infrastrukture. Enkapsulacija radi tako da svaki sloj u protokolu enkapsulira podatke iz viših slojeva tako što im dodaje novo zaglavlje. To omogućuje siguran prijenos podataka preko interneta jer štiti osjetljivost podataka. Cilj enkapsulacije i enkripcije je osigurati da podaci sigurno stignu od primatelja do pošiljatelja. U slučaju da se ti paketi uspiju pronaći i sastaviti, enkripcija će se pobrinuti da podaci ne budu čitljivi onome tko nema potreban ključ da ih dešifrira. [12] Primjer enkapsulacije prikazan je na slici ispod.



Slika 4. Enkapsulacija podataka [13]

4.1.3. Tuneliranje

„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 zatim između krajnjih točaka tunela.“ **Tunel** predstavlja poveznicu ili put između dvije krajnje točke po kojem se kreću enkapsulirani podaci. Kada podaci dođu na kraj tunela, iz okvira se izdvajaju podaci koji su korisni, a zatim se šalju do svog odredišta. Pojam tuneliranja uključuje proces enkapsulacije, prijenosa te dešifriranja originalnih podataka iz poslanog okvira. [14, str. 6]

Moguća su dva načina uspostavljanja VPN mreže [15]:

- **Dobrovoljno tuneliranje** (eng. *Voluntary Tunneling*) - Slučaj kada računalo ili usmjernik koristi klijentsku programsku podršku za tuneliranje pri uspostavljanju VPN-a, npr. kada modemski korisnik prvo uspostavi vezu sa svojim ISP-om da bi mogao uspostaviti tuneliranje kroz internet
- **Obavezno tuneliranje** (eng. *Compulsory Tunneling*) - Većina poslužitelja s modemskim ulazima koje koriste ISP-ovi imaju implementiranu mogućnost automatskog kreiranja tunela za modemskog korisnika.

4.2. Karakteristike VPN-a

Glavni cilj virtualne privatne mreže je siguran i privatan prijenos podataka putem mreže. Kako bi taj cilj bio ispunjen VPN mora zadovoljavati nekoliko karakteristika odnosno ciljeva kako bi pružila određenu zaštitu i sigurnost.

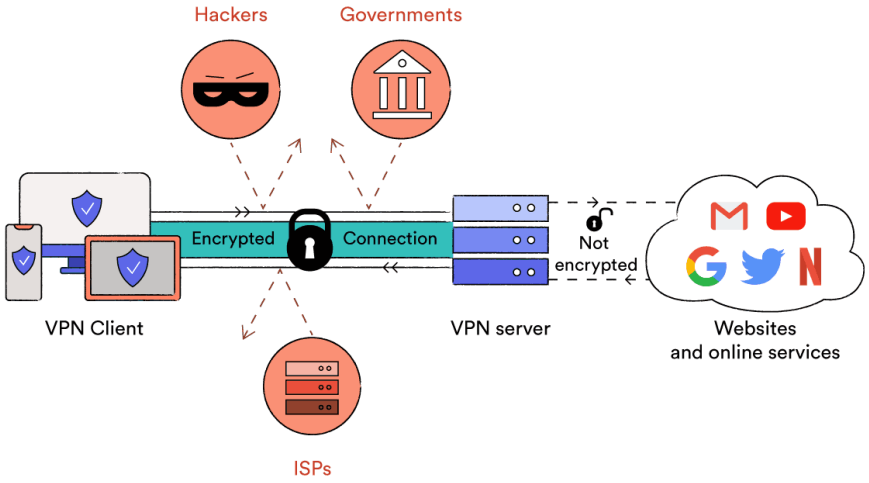
Tablica 1. Karakteristike VPN-a

Sigurnost podataka	podaci u svakom trenutku moraju biti zaštićeni i dostupni samo autoriziranim korisnicima
Integritet podataka	podaci ne smiju biti mijenjani prilikom transporta kroz mrežu
Autentifikacija pošiljatelja	podaci moraju biti poslani s autentičnog i sigurnog izvora
Neporecivost pošiljatelja	u svakom trenutku se mora znati tko je pošiljatelj kako bi se izbjeglo lažno negiranje slanja poruke.

Sve navedene karakteristike najbolje se vide na primjeru kriptiranja podataka. Taj proces se brine da podaci ostanu neotkriveni čak i u slučaju da se enkapsulirani podaci pronađu i sastave. Integritet podataka osigurava se dodavanjem *hash* poruka ili digitalnog potpisa. Na ovaj način se štiti integritet poruke te se osigurava da podaci nisu mijenjani što je izuzetno bitno ako se mrežom šalju informacije vrlo iznimne važnosti. Uz to se koriste kriptografske metode opisane u prethodnim poglavljima kako bi se osigurala autentifikacija poruke i neporecivost pošiljatelja. [11]

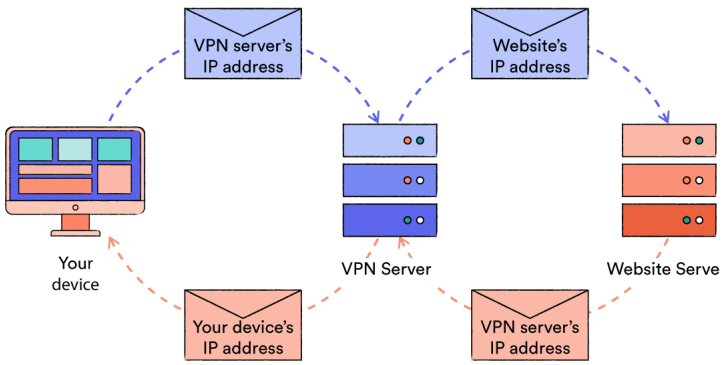
4.3. Prijenos podataka virtualnom privatnom mrežom

VPN pruža veliku razinu sigurnosti prilikom prijenosa privatnih podataka zbog načina na koji ih prenosi putem interneta. Osim toga, pruža i puno veću razinu pristupa geo-ograničenom sadržaju kao i veliku razinu privatnosti. Nakon što se podatkovni paketi kriptiraju i enkapsuliraju, tunelima putuju do VPN poslužitelja odakle se prosljeđuju na odredišnu adresu putem nesigurne javne mreže. Na taj način se osigurava siguran transport podataka putem nesigurne javne mreže.



Slika 5. VPN mreža [16]

Svaki VPN provider ima rasprostranjeno na stotine poslužitelja diljem svijeta od kojih najbliži ili najslobodniji obrađuje primljeni zahtjev. VPN poslužitelj prosljeđuje primljeni zahtjev na traženu IP adresu. S obzirom da je upit prema odredišnoj IP adresi poslan iz VPN poslužitelja, izvorišna IP adresa toga zahtjeva pripada VPN poslužitelju. Primljeni odgovor VPN poslužitelj prosljeđuje natrag do klijenta. U tom slučaju ako netko prati IP adresu od odredišta do izvorišta, najdalje što može doći je VPN poslužitelj. [8]



Slika 6. Putovanje zahtjeva za prikaz web stranice putem VPN-a [16]

5. VPN protokoli

Virtualne privatne mreže koriste razne protokole pomoću kojih postavljaju tunele putem kojih informacije mogu sigurno putovati u mreži od uređaja do uređaja. Najpoznatiji protokoli koji se koriste kod VPN mreža su PPTP, L2TP, IPsec, OpenVPN, SSTP i IKEv2. Neki od navedenih protokola bit će opisani u nastavku.

5.1. IPsec

J. Snader [9, str. 308] navodi kako je *„Internet Protocol security“* (u daljnjem tekstu: IPsec) jedan od najpoznatijih protokola koji se koriste prilikom implementacije VPN mreže kao i glavni protokol koji se koristi na internetu. IPsec se koristi za postavljanje tunela i sigurne veze između računala kako bi se osigurao siguran transport podataka na internetu, a sastoji se od sljedećih protokola:

- *„Authentication protocol“* – autentifikacija i osiguranje integriteta podataka
- *„Encapsulating Security Protocol“* – enkapsulacija podataka
- *„Internet Key Exchange“* – upravljanje javnim i privatnim ključevima

Autentikacijski protokol se brine za autentifikaciju podataka koji se prenose mrežom. On osigurava da su svi podaci iz pouzdanih izvora i da nisu mijenjani prilikom prijenosa mrežom. Bitno je za napomenuti kako se u ovom protokolu ne odvija nikakva vrsta enkripcije i enkapsulacije, već samo provjera pouzdanosti. S druge strane, ESP protokol se brine za enkripciju IP zaglavlja svakog podatkovnog paketa koji se prenosi mrežom, odnosno zadužen je za osiguravanje da podaci ne budu lako čitljivi prilikom prijenosa internetom. ESP protokol također svakom paketu daje vlastito zaglavlje kako bi ga zaštitio prilikom putovanja mrežom. Uz autentifikaciju i enkapsulaciju IKE protokol pruža sve bitne funkcije upravljanja ključevima koji su potrebni kod kriptiranja podataka, odnosno ključni protokol za razmjenu ključeva. [9]

IPsec protokol ima dva načina rada: transportni način i tunelirajući način. Transportni način povezivanja ime je dobio po mrežnom sloju kojeg štiti – transportnom sloju (eng. *transport layer*) te služi za uspostavljanje veze između dva fiksna uređaja pružajući time *end-to-end* sigurnost i zaštitu. Kod transportnog načina, kod prijenosa podataka šifrira se samo podatkovni dio IP datagrama[3] (podatkovnih paketa), dok zaglavlja ostaju u originalnom

[3] Podatkovni paketi namjenjeni za prijenos putem *Internet Protocol*a (odnosno IP-a).

obliku. Kod ovog načina rada, usmjerivači u mreži mogu pročitati IP adrese izvorišta i odredišta što omogućuje lakše analiziranje i čitanje podataka koji se šalju. [14]

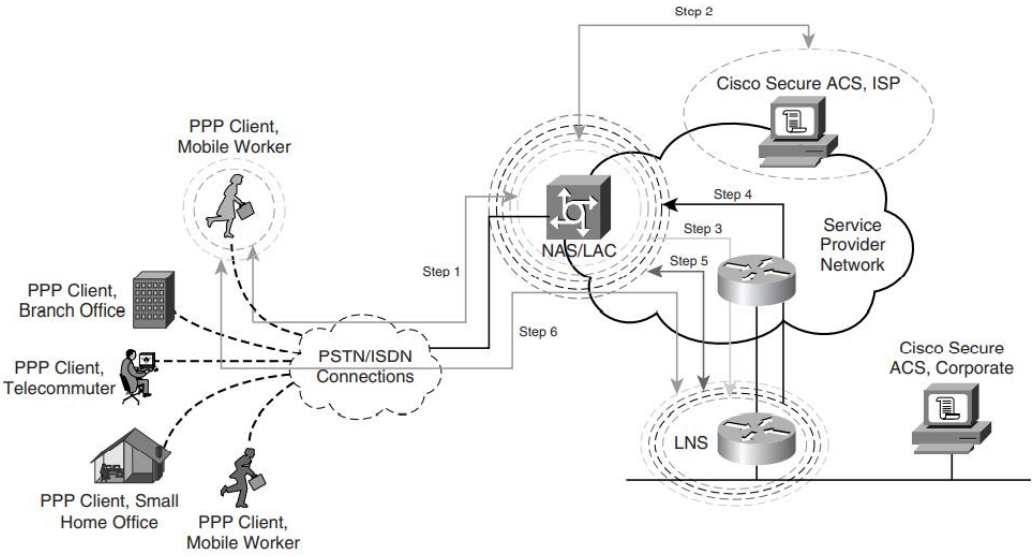
Tunelirajući način rada koristi se za realizaciju VPN mreže odnosno za spajanje dvije mreže ili spajanje uređaja i mreže (npr. mreža određenih poduzeća i kućna mreža). Tunelirajući način spajanja uspostavlja se uz pomoć sigurnosnih prolaza (eng. *security gateway*). U ovakvom slučaju, kućna mreža i uredska mreža spojene su putem VPN-a uz pomoć sigurnosnih prolaza. Ovi prolazi se brinu o šifriranju i dešifriranju podataka te o provjeri autentičnosti. Glavna razlika između transportnog i tunelirajućeg načina je pakiranje podataka za slanje. Tunelirajući način rada kreira novi IP datagram unutar kojeg se nalazi stari datagram dok transportni način samo dodaje zaglavlje unutar već postojećeg IP datagrama. [9]

5.2. L2TP

„Layer 2 Tunneling Protocol“ (u daljnjem tekstu: L2TP) predstavlja klijent-poslužitelj protokol koji služi za enkapsulaciju podatkovnih paketa na drugom mrežnom sloju, odnosno podatkovnom sloju. L2TP omogućuje enkapsuliranje PPP[4] okvira i njihovo slanje putem interneta. L2TP koristi UDP protokol i nizove L2TP poruka za održavanje tunela preko IP mreža. Moguće je i stvaranje više tunela istovremeno između istih krajnjih točaka. Ovaj protokol sastoji se od dvije glavne komponente: L2TP pristupnog koncentratora (eng. *„L2TP Access Concentrator“* , u daljnjem tekstu: LAC) i L2TP mrežnih poslužitelja (*„L2TP Network Server“*, u daljnjem tekstu: LNS). [14]

LAC predstavlja stranu klijenta mreže i nalazi se na switch infrastrukturi između udaljenih priključnih čvorova (eng. *remote dialup nodes*) i pristupnog poslužitelja. LAC služi kako bi primio dolazne pakete te ih proslijedio do L2TP poslužitelja koji se nalazi na udaljenoj mreži. LNS s druge strane predstavlja poslužiteljsku stranu VPDN (eng. *virtual private dial-up network*) arhitekture te se u mreži poduzeća. [9]

[4] Protokol koji omogućuje autentikaciju te pruža metode za šifriranje i kompresiju podataka



Slika 7. L2TP protokol [11, str.11]

Slika 6. prikazuje primjer postavljanja i korištenja L2TP tunela. Koraci za postavljanje tunela [14]:

1. Udaljeni korisnik inicira PPP spoj prema svojem pružatelju internetske usluge (u daljnjem tekstu: ISP)
2. ISP prihvaća zahtjev i uspostavlja PPP vezu
3. ISP zahtijeva dobio korisničko ime
4. U ISP-ovoj bazu podataka korisničko ime je povezano sa servisima i LNS krajnjom točkom.
5. LAC pokreće L2TP tunel prema LNS-u
6. Ukoliko LNS prihvati spoj, LAC enkapsulira PPP u L2TP i prosljeđuje podatke preko odgovarajućeg tunela.
7. LNS prihvaća okvire, odvaja L2TP zaglavlja te ih obrađuje kao normalne PPP okvire
8. LNS koristi PPP autentikaciju kako bi utvrdio identitet korisnika i dodijelio mu IP adresu

5.3. OpenVPN

OpenVPN jedan je od novijih protokola kod virtualnih privatnih mreža. Zbog njegove jednostavnosti prilikom instalacije i održavanja, kao i velike razine sigurnosti, ovaj protokol je jedan od najpopularnijih protokola koji se koriste kod izrade VPN mreža. Sastoji se od podatkovnog kanala koji prenosi IP datagrame korisnika i kontrolnog kanala. OpenVPN multipleksira oba kanala prema VPN-u, odnosno šalje signale iz oba kanala jednom linijom pritom koristeći iste portove. OpenVPN enkapsulira kontrolne i podatkovne pakete u UDP datagram te koristi TLS protokol za autentifikaciju i razmjenu ključeva. OpenVPN može prenositi IP datagrame kao i Ethernet okvire što mu omogućuje da radi na IP sloju ili na sloju podatkovne mreže. To mu pruža veću fleksibilnost prilikom prenošenja podatkovnih paketa. [9]

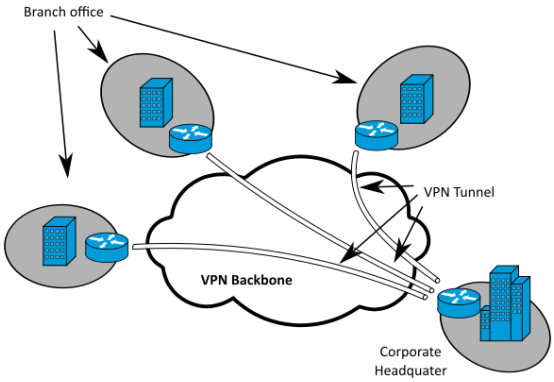
OpenVPN je zbog dostupnosti, prilagodljivosti i sigurnosti brzo postao jedan od najpopularnijih protokola. Implementacija OpenVNP-a se sastoji od preuzimanja i instalacije paketa na strani klijenta i poslužitelja te osnovne konfiguracije na obje stane. Nakon toga VPN se može koristiti stalno ili samo privremeno. Zbog jednostavnosti i sigurnosti koju pruža, mnogi pružatelji VPN usluge danas koriste OpenVPN protokol kod usluge koju nude. [17]

6. Podjela virtualnih privatnih mreža

Ovisno o načinu povezivanja, virtualne privatne mreže mogu se podijeliti na *Site-to-Site* VPN i *Remote-Access* VPN. Obje vrste virtualnih privatnih mreža će se detaljnije obraditi u ovom poglavlju.

6.1. *Site-to-Site* VPN

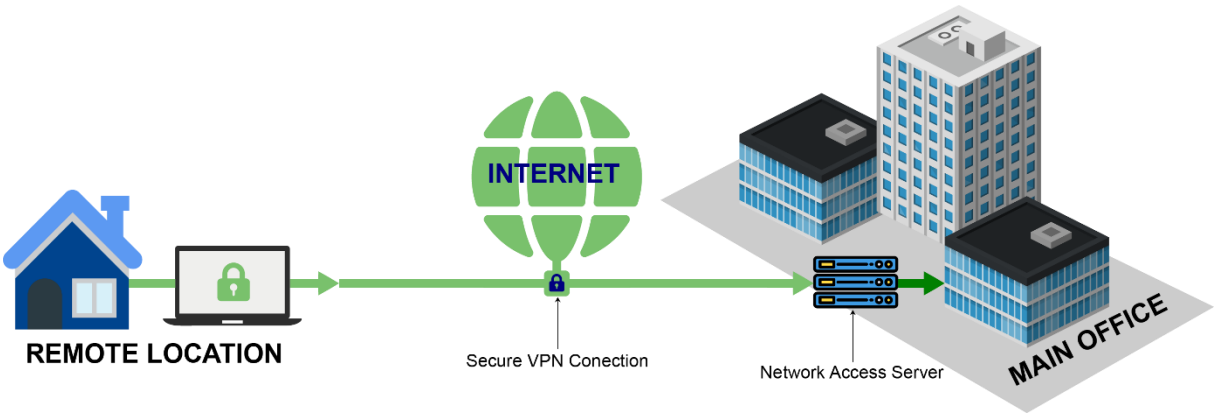
Site-to-Site predstavlja sigurnu vezu između dvije ili više mreža putem VPN-a. Ovakav način povezivanja većinom se koristi kod većih organizacija koje imaju urede na više različitih geografskih lokacija, a potreban im je način kako bi mogli neprestano i sigurno pristupati i koristiti korporativnu mrežu. Uz pomoć ovakvog načina spajanja organizacija može bez problema spojiti glavnu mrežu sa geografski udaljenim uredima i tako omogućiti svojim zaposlenicima pristup resursima sigurnim putem. Ovakva mreža osmišljena je kao otvorena dvosmjerna poveznica između dvije ili više lokacija za lakši i sigurniji pristup podacima te je većinom postavljena uz pomoć IPsec protokola. *Site-to-site* može se također podijeliti na dvije podvrste: **intranet VPN i ekstranet VPN**. Intranet se koristi za povezivanje više različitih lokacija unutar jedne organizacije dok se ekstranet koristi za povezivanje različitih organizacija kao npr. matična tvrtka i podružnice. Ovaj VPN radi na sljedeći način: uz pomoć *Site-to-Site* povezivanja poslužitelji iz svih podružnica se spoje na glavni poslužitelj te dobiju pristup potrebnim podacima. Zaposlenici u podružnici tada mogu pristupiti svim podacima organizacije koji su na poslužitelju. Posljednjih godina, a pogotovo 2020-te ovakav način povezivanja se drastično smanjio. Kako velika većina radi od kuće, nema potrebe za preusmjeravanje prometa kroz podatkovni centar organizacije, već se zaposlenici mogu spojiti direktno na glavni poslužitelj i tako pristupiti svim potrebnim podacima. Ovakav način spajanja bit će objašnjen u nastavku [18]



Slika 8. *Site-to-Site* VPN [19]

6.2. *Remote-Access* VPN

U zadnje vrijeme se često pojam *„remote“* veže za rad izvan ureda. U današnje vrijeme sve je popularnije raditi od kuće i imati tzv. *„home office“,* no tu se javlja problem pristupa povjerljivim informacijama koje se nalaze unutar organizacijske mreže. ***Remote-Access* VPN** rješava navedeni problem omogućujući zaposlenicima mogućnost pristupa osjetljivim informacijama organizacije s bilo kojeg mjesta, a da pritom ti podaci ostanu sigurni čak i ako se koristi javna mrežna infrastruktura. Iako ovakav način spajanja radi slično kao *Site-to-site* VPN, postoji jedna bitna razlika. *Remote-Access* VPN podrazumijeva spajanje bilo kojeg uređaja s bilo koje lokacije na poslužitelj dokle god ima pristupne podatke. Taj poslužitelj brine se da podaci koji putuju budu šifrirani kako ih nitko osim primatelja i poslužitelja ne bi mogao pročitati. S druge strane *Site-To-Site* pristup povezuje dva poslužitelja te podrazumijeva poslužitelj-poslužitelj komunikaciju. *Remote-access* VPN danas je puno popularniji nego *Site-to-Site* povezivanje. *Site-to-Site* su većinom koristile organizacije gdje su zaposlenici radili u uredu. Kako se popularizirao rad od kuće, većina organizacija je premjestila svoje podatke na poslužitelj u *cloudu* što je omogućilo *remote-access* spajanje. [20]



Slika 9. *Remote-access* VPN [21]

7. Prednosti i nedostaci VPN-a

Razvoj i popularizacija virtualnih privatnih mreža donosi puno pogodnosti za korisnike. Uspoređujući otvorenu mrežu i virtualnu privatnu mrežu možemo naći puno razlika kao i puno benefita koje pruža virtualna privatna mreža. No osim prednosti VPN sa sobom nosi i određene nedostatke. Iako su ti nedostaci u puno manjem broju nego prednosti, ipak treba biti svjestan da oni postoje.

7.1. Prednosti

Neke prednosti VPN-a su već ranije navedene kao vrlo bitno obilježje VPN-a. Jedna od najznačajnijih prednosti je tako **internetska sigurnost.** Kao što je već navedeno, virtualna privatna mreža osmišljena je kako bi osigurala prijenos podataka na internetu. S obzirom da je danas takozvani *Cyber-crime* vrlo raširen, korisnicima je važno da mogu zaštiti bitne informacije kao što su podaci o bankovnim karticama ili podaci o identitetu te privatne lozinke, emailove i korisničke račune. Sigurnost koju pruža ovakav način spajanja na internet vrlo je teško nadmašiti bilo kojom drugom metodom pa je zbog toga to najvažnija prednost VPN-a. Osim toga, vrlo bitna prednost je i **ukidanje geo-restrikcija** koje koriste određene stranice poput streaming platformi kao što su Netflix i Hulu. Promjenom IP adrese se vrlo lako može pristupiti onom sadržaju koji je namijenjen samo za određenu državu. Osim toga, VPN pruža **anonimnost** na internetu. U današnje vrijeme kada su podaci jedna od najvrednijih stvari i kada se na dnevnoj bazi prikupljaju podaci o korisnicima na gotovo svim internetskim stranicama, anonimnost na internetu je vrlo vrijedna stvar. VPN mreža osigurava anonimnost korisnika promjenom IP adrese kao i raznim metodama enkripcije podataka, osiguravajući tako da ti podaci ne dospiju u krive ruke. [22]

Još jedna prednost VPN-a koja nije toliko poznata je **mogućnost uštede** prilikom online kupovine. Često trgovine, aviokompanije, hoteli i resorti postavljaju različite cijene za svoje korisnike, ovisno o tome iz kojeg dijela svijeta oni obavljaju svoju kupovinu te na taj način ostvaruju puno veći profit. Tako bi istu avionsku kartu osoba iz bogatije države mogla puno skuplje platiti nego osoba koja dolazi iz slabije razvijene države. [22]

7.2. Nedostaci

Kada se priča o VPN-u, većinom se spominju njegove prednosti, no nedostaci su itekako prisutni iako mnogi za njih ni ne znaju. Jedan od glavnih nedostatka korištenja VPN-a je **sporija internetska veza**. Usporenost veze događa se zbog enkripcije i enkapsulacije podataka koji se prenose kao i zbog udaljenosti poslužitelja. U tom slučaju podatkovnim paketima treba duže da stignu do željene lokacije što direktno utječe na brzinu internetske veze. Pozitivna stvar je da se ovaj problem može izbjeći ukoliko je računalo s kojeg se šalju podaci ima jak procesor. Osim problema s brzinom, postoje i **problemi s vezom prema udaljenom poslužitelju** koji mogu uzrokovati isključenje VPN-a. Problem s vezom je jedan od najčešćih problema s kojima se susreću korisnici VPN-a. U takvom slučaju, svi podaci koji se u tom trenutku nalaze u mreži, uključujući IP adresu, postaju izloženi i vidljivi. Kako bi se se spriječio gubitak sigurnosti mnogi VPN pružatelji danas implementiraju takozvani *KillSwitch*. *KillSwitch* osigurava da se u slučaju prekida veze sa poslužiteljem automatski isključi i internetska veza kako bi se zaštitili podaci korisnika. [22]

Još jedan nedostatak VPN-a je taj što on **većinom nije besplatan**. Neki pružatelji VPN usluga imaju određeni limit prijenosa podataka u besplatnoj verziji, dok se sve preko zadanog limita dodatno naplaćuje. No puna usluga konstantne sigurnosti i neograničenog prometa nije besplatna. Iako su VPN mreže poznate po tome što pružaju sigurnost prilikom pretraživanja interneta, jedan od njihovih nedostataka je i **povremena nesigurnost korisnika**. Iako se ne događa često i velika većina pružatelja to ne radi, neki pružatelji VPN usluge mogu sakupljati podatke korisnika te ih prodavati trećim stranama time ugrožavajući sigurnost svojih korisnika. Kada podaci dođu do VPN-ovog poslužitelja, poslužitelj ih lokalno pohranjuje te ih zatim prodaje drugim tvrtkama. Ovakav scenarij je češći s pružateljima koji nude VPN usluge besplatno. [22]

8. Implementacija virtualne privatne mreže

Implementacija virtualne privatne mreže bit će prikazana na dva načina. Prva implementacija realizirana je korištenjem platforme *Microsoft Azure cloud* na kojoj je kreiran i konfiguriran VPN klijent koji će se preuzeti na računalo gdje će biti instaliran. Drugi način je preuzimanje VPN aplikacije od pružatelja usluge. Za tu svrhu, preuzeta je i instalirana aplikacija TunnelBear. Implementacija VPN-a na Microsoft Azureu napravljena je prema Microsoft dokumentaciji za implementaciju *Point-To-Site* (*remote-access*) VPN-a. [23]

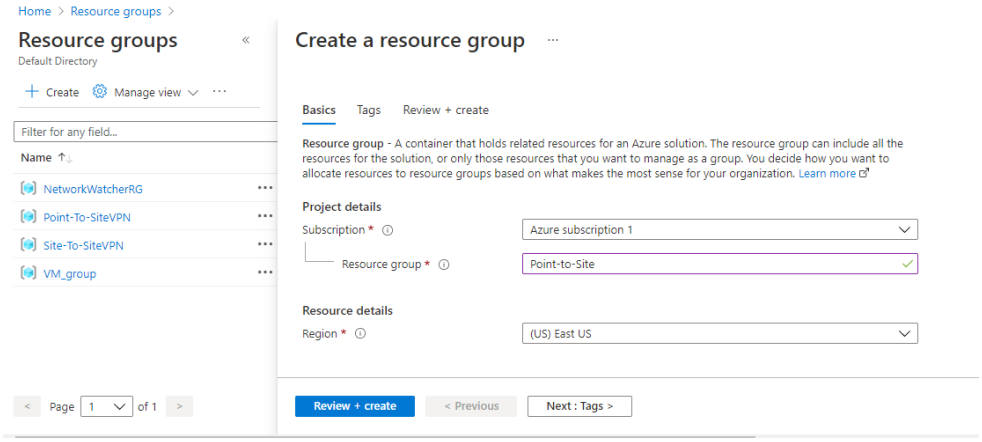
8.1. Implementacija VPN-a na Microsoft Azureu

VPN implementacija putem Azure portala funkcionira na sljedeći način: Potrebno je kreirati VPN klijenta, virtualni prolaz (u daljnjem tekstu: *VPN Gateway*[5]) i virtualni uređaj koji će međusobnim spajanjem omogućiti da se lokalno računalo spoji na virtualnu mrežu te sigurno šalje podatke putem interneta. Lokalno računalo će putem VPN klijenta slati svoje podatke do VPN *Gatewaya*, a *gateway* će ih zatim usmjeriti do virtualnog uređaja koji u ovom slučaju predstavlja Azureov poslužitelj. Virtualni uređaj je udaljeni *desktop* preko kojeg se na siguran način mogu razmjenjivati podaci.

Prije nego se počne s realizacijom VPN-a potrebno je ispuniti dva preduvjeta. Glavni preduvjet je da postoji Microsoft Azure račun koji omogućava korištenje svih potrebnih resursa za implementaciju. Drugi preduvjet je poznavanje vrste VPN-a koji je potrebno implementirati. Kako je već ranije navedeno postoji *remote-access* i *site-to-site* povezivanje.

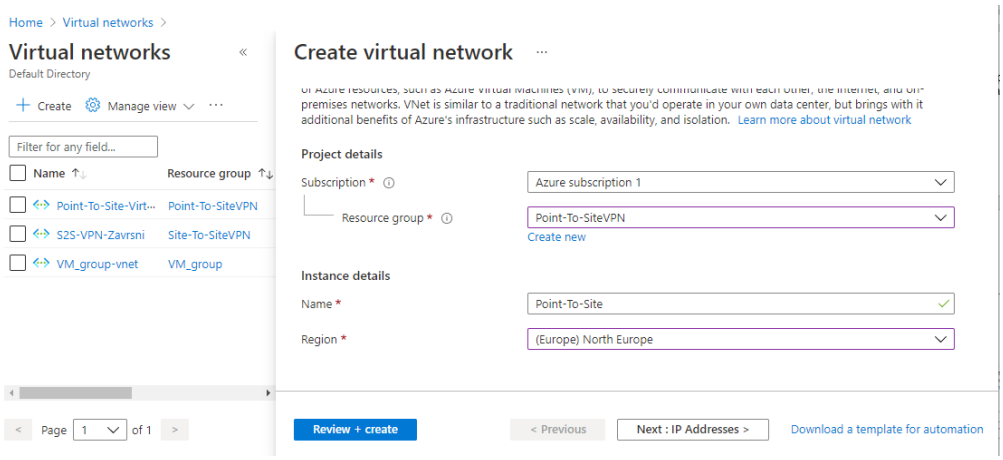
Prvi korak u kreiranju VPN-a je kreiranje resursne grupe. Resursna grupa predstavlja kolekciju u koju se spremaju virtualni uređaji, poslužitelji, baze i IP adrese. U ovom slučaju, u kolekciju su spremljeni VPN konfiguracija, VPN *Gateway*, IP adresa i poslužitelj koji su kreirani za potrebe implementacije VPN-a. Kako bi se resursna grupa kreirala potrebno je u traci za pretraživanje unijeti „*Resource group"*. Iz izbornika se odabere opcija *Resource group* i nakon što se učita stranica sa svim resursnim grupama odabere se gumb „*Create*". Otvara se prozor u kojemu se odabire pretplatnički račun, regija u kojoj će se nalaziti VPN i naziv grupe. Klikom na „*Create and review*" validiraju se uneseni podaci nakon čega se pojavljuje gumb „*Create*". Klikom na taj gumb kreira se resursna grupa (slika 9).

[5] Gateway predstavlja posebnu vrstu virtualnog mrežnog pristupnika koji služi za slanje šifriranog prometa između Azure virtualne mreže i lokalnog uređaja putem javne mreže.



Slika 10. Kreiranje resursne grupe (portal.azure.com)

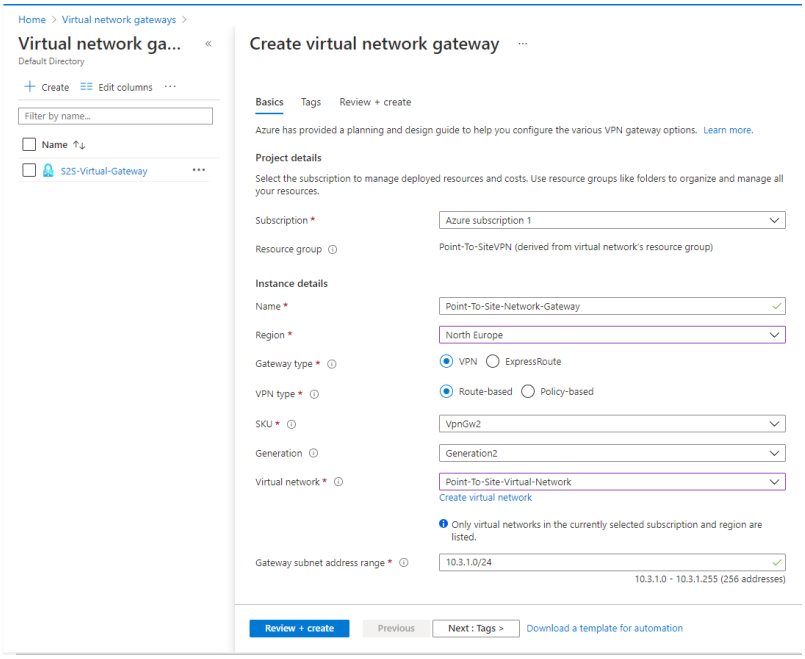
Nakon kreiranja resursne grupe potrebno je kreirati virtualnu mrežu. U traku za pretraživanje unosi se „*Virtual Network*“. Otvara se stranica sa virtualnim mrežama gdje se klikom na gumb „*Create*“ otvara prozor za unos nove virtualne mreže (slika 10). Odabire se resursna grupa u koju se želi spremiti virtualna mreža, postavlja se naziv mreže, odabire se regija u kojoj će se nalaziti virtualna mreža te se odabire gumb „*IP addresses*“. Otvara se prozor u kojemu se odabire adresni prostor[6] IP adresa te dodaje podmreža i njezin raspon adresa. Nakon toga se validiraju podaci te se kreira virtualna mreža klikom na gumb „*Create.*“ Ova virtualna mreža služit će za povezivanje klijenta, poslužitelja, virtualnog prolaza te za sigurnu komunikaciju i razmjenu podataka između njih.



Slika 11. Kreiranje virtualne mreže (portal.azure.com)

[6] Količina memorije koja je dodijeljena za sve moguće adrese koje pripadaju uređajima poput lokalnog računala, rutera, poslužitelja itd. Poznata i kao raspon mogućih IP adresa.

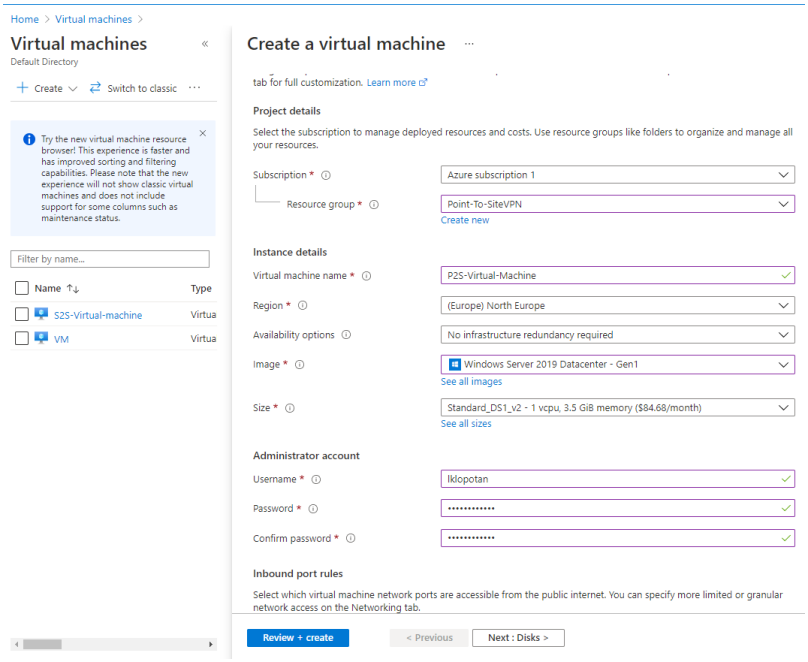
Nakon što je kreirana virtualna mreža potrebno je kreirati virtualni *gateway. Gateway* se kreira tako da se u tražilicu unese *„Virtual Network Gateway“* i na stranici koja se otvori klikne se na gumb *„Add“.* Otvara se forma za unos potrebnih podataka (slika 12.) Na formu se unosi naziv *gatewaya*, regija u kojoj se nalazi *gateway* (mora odgovarati regiji u kojoj se nalazi VPN), tip *gatewaya* i tip VPN-a. U ovom slučaju, tip VPN-a je *route-based* što znači da se VPN referencira na temelju rute koja odlučuje koji se promet šalje kroz tunel na temelju odredišne IP adrese. *Policy-based* VPN ne usmjerava promet na temelju rute već koristi dodatna pravila koja odlučuju o usmjeravanju prometa. Također se odabire tzv. *„Stock keeping unit“* (u daljnjem tekstu: SKU) koji označava na koji način će se naplaćivati usluga. Ovisno o odabranom SKU-u postavljaju se performanse VPN-a. Nakon što su ispunjeni svi podaci potrebno je odabrati VPN za koji se konfigurira *Gateway*. U sekciji „*Public IP address“* odabire se *„Create new*“ kako bi se kreirala nova javna IP adresa *gatewaya* te se unosi željeno ime za IP adresu. Nakon toga je potrebno validirati podatke te stvoriti *gateway* klikom na „*Create*“. Kreiranje *gatewaya* može potrajati do 45 minuta.



Slika 12. Kreiranje virtualnog *Gatewaya* (portal.azure.com)

Nakon toga je potrebno kreirati virtualni uređaj uz pomoć kojega će se realizirati VPN mreža. U tražilicu se unosi „*Virtual machine*“ te se otvara prozor sa svim virtualnim uređajima. Klikom na „*Create*“ otvara se prozor gdje se konfigurira virtualni uređaj. Podaci koje je potrebno unijeti su sljedeći: naziv resursne grupe, naziv uređaja, lokacija uređaja,

operacijski sustav uređaja te korisničko ime i lozinka. Potrebno je zapamtiti ime i lozinku jer su one bitne kasnije kod spajanja na uređaj.



Slika 13. Kreiranje virtualnog uređaja (portal.azure.com)

Kako bi se autentificirali korisnici koji se spajaju na Azure VPN, koriste se certifikati. Ti certifikati funkcioniraju na sljedeći način: Uz pomoć Windows powershella se kreiraju dva certifikata – korijenski certifikat i klijentski certifikat.

Kako bi se kreirao korijenski certifikat potrebno je otvoriti Windows powershell i unijeti sljedeću naredbu:

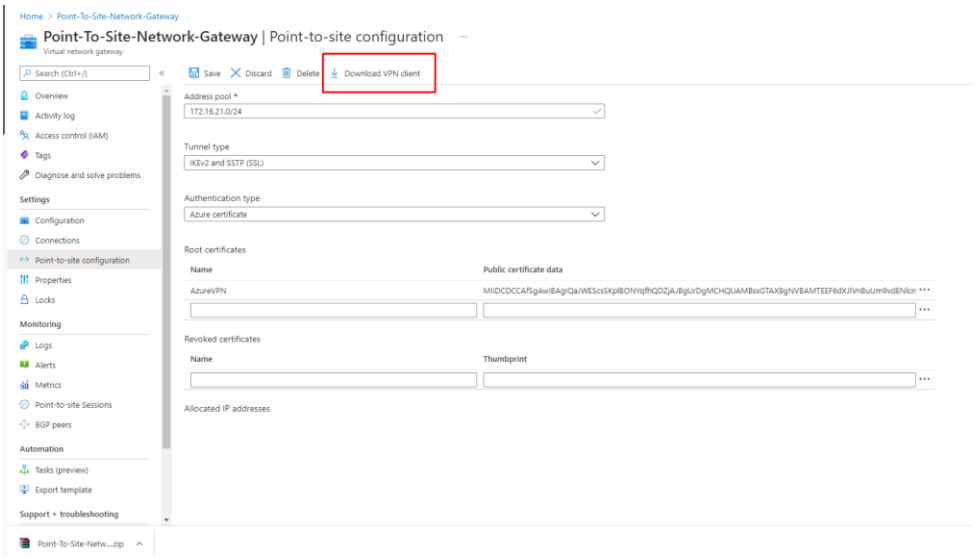
```
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature -Subject "CN=NameofyourRootCert" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
```

Nakon toga se kreira klijentski certifikat također u powershellu uz pomoć sljedeće naredbe:

```
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature -Subject "CN=NameOfYourChildCert" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

Nakon kreiranja oba certifikata potrebno je napraviti izvoz podataka nad korijenskim certifikatom na sljedeći način: u powershell se unese naredba *„certmgr“* koja otvara popis svih certifikata na računalu. U folderu *„personal“* potrebno je naći odgovarajući certifikat te desnim klikom otvoriti padajući izbornik. Iz izbornika se odabere opcija “*All tasks*“ koja otvara

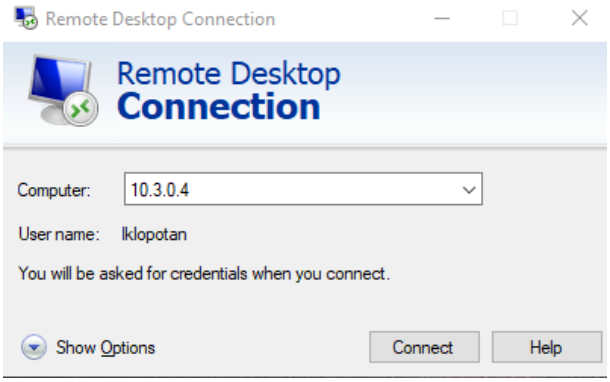
padajući izbornik iz kojeg se izabere opcija *„Export“.* Otvara se čarobnjak za izvoz certifikata. Na prvoj stranici se nudi opcija izvoza privatnog ključa. Tu je potrebno odabrati opciju da se ne izvozi privatni ključ. Klikom na „*Next*“ nudi se odabir izvoznog formata. Tu se odabire format *Base64 encoding*. Nakon toga je potrebno odabrati naziv certifikata i lokaciju na koju ga želimo spremiti. Kada je izvoz završio potrebno je naći spremljeni certifikat te ga otvoriti uz pomoć tekstualnog uređivača. Kopira se dobiveni tekst certifikata te se odlazi na Azure virtualni *gateway* i u izborniku se odabire „*Point-to-site configuration*“. Potrebno je dodati novu konfiguraciju s odgovarajućim certifikatom. Odabire se „*Address pool*“, odnosno raspon IP adresa koje će se nalaziti unutar ove mreže. Nakon toga se odabire protokol za povezivanje te način autentifikacije. Unosi se željeni naziv certifikata te nedavno kopirani certifikat. Sprema se konfiguracija te se na taj način kreira VPN klijent koji će omogućiti spajanje na VPN. Nakon što je spremljena konfiguracija klikom na gumb „*Download VPN Client*“ (slika 13.) preuzima se VPN klijentska konfiguracija. Preuzetu ZIP datoteku je potrebno otpakirati te instalirati jednu od dvije klijentske konfiguracije koje su u njemu, ovisno o operacijskom sustavu i arhitekturi računala. Kako bi instalacija klijenta bila moguća na računalu se mora nalaziti klijentski certifikat. Instalirani VPN klijent bi trebao biti vidljiv na popisu dostupnih mreža u donjem desnom kutu računala.



Slika 14. Konfiguracija VPN klijenta (portal.azure.com)

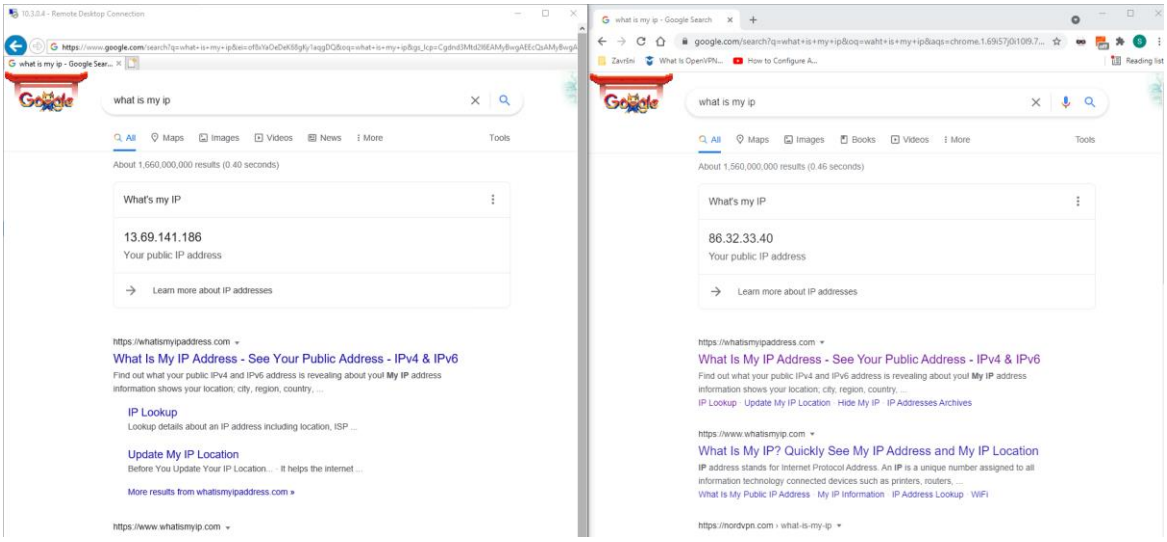
Klikom na novo dodani VPN otvaraju se postavke za spajanje na virtualnu mrežu. Klikom na gumb *„Connect*“ spajamo se na VPN. No iako smo spojeni na virtualnu mrežu naši podaci i dalje nisu zaštićeni. Za to se je potrebno spojiti putem „R*emote desktop connection“*

aplikacije na virtualni uređaj koji je konfiguriran ranije. Kako bi se mogli spojiti na virtualni uređaj potrebno je znati njegovu privatnu IP adresu. Privatna IP adresa navedena je na Azureu kod postavki virtualnog uređaja. Iz navedenih postavki se kopira IP adresa te se otvori „*Remote desktop connection*“ na računalu. Unese se IP adresa i pritisne se gumb „*Connect*“.



Slika 15. Veza na virtualni uređaj

Nakon početnog povezivanja potrebno je unijeti korisničko ime i lozinku koja je postavljena kod kreiranja virtualnog uređaja. Nakon što su potvrđeni pristupni podaci otvara se virtualni *desktop* (slika 16) na kojeg smo spojeni uz pomoć klijentske VPN aplikacije instalirane na našem računalu. Kako bi provjerili radi li privatna mreža ispravno mogu se istovremeno usporediti IP adrese na lokalnom i virtualnom računalu. Na slici 16. prikazana su IP adrese lokalnog računala i virtualnog računala.

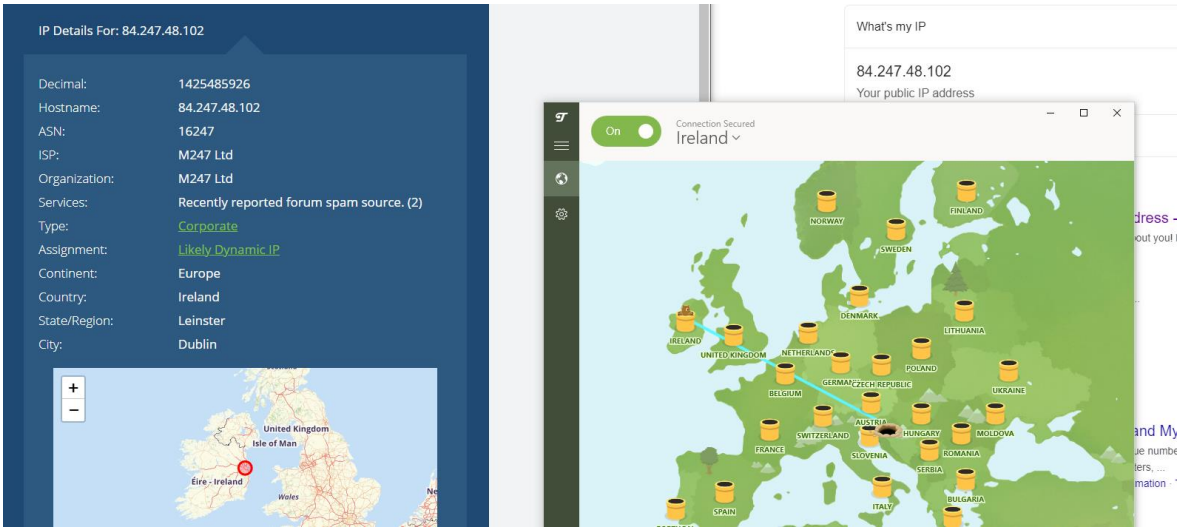


Slika 16. Prikaz različitih IP adresa virtualnog računala (lijevo) i lokalnog računala (desno)

8.2. Instalacija TunnelBear VPN-a

Instalacija TunnelBear VPN-a vrlo je jednostavna. Prvi korak koji je potrebno učiniti je otići na internet te sa službene TunnelBear stranice preuzeti instalacijski paket. TunnelBear nudi dva instalacijska paketa: besplatni paket koji nudi samo 500MB sigurnosnog surfanja i plaćeni paket koji nudi puno više mogućnosti. U svrhu završnog rada preuzeta je i instalirana besplatna verzija VPN-a. Klikom na instalacijsku datoteku pokreće se instalacija i otvara se prozor za odabir mjesta za pohranu programa. Kada se odabere mjesto za pohanu i klikne na gumb *„Install*“ treba pričekati par minuta dok instalacija ne završi. Jednom kada je instalacija gotova otvara se prozor za prijavu u aplikaciju. Potrebno je unijeti email i lozinku, prihvatiti uvjete korištenja te potvrditi email adresu putem linka.

VPN se uključuje/isključuje klikom na gumb On/Off u gornjem lijevom kutu. Kada je VPN uključen jednostavno se odabire lokacija s koje želimo da se dohvaćaju podaci koje tražimo putem interneta nakon čega možemo krenuti razmjenjivati podatke putem sigurne VPN mreže. Kako bi provjerili da li VPN doista radi, nakon što odaberemo lokaciju u aplikaciji, tražimo koja je naša IP adresa putem internet stranice „*WhatIsMyIPAddress.com*“. Nakon toga na toj istoj stranici možemo provjeriti koja je lokacija IP adrese našeg računala. IP adresa i lokacija uređaja prikazane su na slici 19.



Slika 17.TunnelBear promjena IP adrese

9. Zaključak

Posljednjih godina popularnost VPN-a vrtoglavo raste. Uz povoljne i široko dostupne pružatelje usluge radi se na njegovoj sigurnosti i na razvoju novih protokola. Razvoj naprednijih protokola enkripcije i zaštite podataka povećao je sigurnost i učinkovitost VPN-a, a porastom konkurencije i broja pružatelja usluge se smanjila cijena korištenja VPN-a pa je samim time i njegova primjena postala sve šira i češća. Primarna svrha i prednost VPN-a je zaštita privatnih podataka. Osim zaštite podataka najčešće se koristi za pristup ograničenim web lokacijama i za očuvanje anonimnosti na internetu. Glavni nedostatak VPN-a je usporenost mreže koju uzrokuje spora veza sa VPN-ovim poslužiteljem. Drugi rječi, ali ozbiljniji nedostatak je izloženost privatnih informacija korisnika. Pružatelji VPN usluga mogu biti potencijalno opasni jer mogu čuvati i prodavati privatne informacije korisnika. Zbog toga treba dobro proučiti VPN uslugu kao i pružatelja usluge prije nego se odlučimo za njezino korištenje. S obzirom da postoje dvije vrste VPN-a, prije same implementacije potrebno je proučiti koja vrsta VPN-a je potrebna te se nakon toga odlučiti želi li se implementirati posebno konfiguriran VPN ili će se preuzeti VPN nekog pružatelja usluge.

U ovom radu su obrađene dvije implementacije: instalacija TunnelBear aplikacije te implementacija posebno konfiguriranog VPN klijenta putem Azureovog poslužitelja. Instalacija već konfigurirane aplikacije je vrlo jednostavna za instalaciju i korištenje, dok za vlastitu implementaciju treba imati određena znanja o tehničkim stvarima kako bi se znali postaviti svi potrebni parametri za konfiguraciju. Osim kompliciranije implementacije, Azure naplaćuje svoje usluge prema potrošnji dok TunnelBear ima fiksnu mjesečnu cijenu s neograničenom prijenosom podataka. Glavne prednosti TunnelBeara su jednostavnost i dostupnost. Čak i ako korisnik nema instaliranu aplikaciju potrebno je svega nekoliko minuta da se aplikacija preuzme i krene koristiti. S druge strane, da bi se Azure VPN implementirao i konfigurirao potrebno je otprilike 2 sata. Glavna prednost Azure VPN-a je da se može instalirati na neograničen broj računala te sva ta računala mogu imati pristup udaljenim podacima.

Ono što se može zaključiti je da je za svakodnevnu upotrebu puno jednostavnije koristiti uslugu nekog VPN pružatelja. Jednostavnost i dostupnost koji oni pružaju sasvim je dovoljna za potrebe velike većine korisnika. Posebno konfigurirani VPN poput Azureovog preporuča se za korištenje kod organizacije koje imaju potrebu za centraliziranom pohranom podataka. Neovisno o vrsti implementacije, VPN postaje sve značajniji u svakodnevnom životu zbog sigurnost i anonimnosti koju pruža u svijetu gdje se veliki dio komunikacije odvija online.

Popis literature

[1] Internet society (bez dat.) *Brief History of the Internet* [Na internetu]. Dostupno: https://www.internetsociety.org/internet/history-internet/brief-history-internet/#f3 [pristupano 26.07.2021.].

[2] “Who invented the Internet?“ (28.10.2019.). History [Na internetu]. Dostupno: https://www.history.com/news/who-invented-the-internet

[3] I. Zagradanin, „The history of VPN“, 04.04.2021. [Na internetu]. Dostupno: https://www.geosurf.com/blog/history-of-vpn-the-quest-for-a-better-internet [pristupano 26.07.2021.].

[4] D. Crawshaw, „Everything VPN Is New Again“, *Communications of the ACM*, sve. 64, izd. 4, str. 130-134. travanj 2021.

[5] E. Staff, „Beginner’s Guide: What is a Domain Name and How Do Domains Work?“, 26.03.2021. [Na internetu]. Dostupno: https://www.wpbeginner.com/beginners-guide/beginners-guide-what-is-a-domain-name-and-how-do-domains-work/ [pristupano 23.08.2021.].

[6] A.S. Tanenbaum, N. Feamster i D. J. Wetherall, *Computer Networks*,6. izd., Hockham: Pearson, 2021

[7] „How the Web works“ (bez dat.). MDN Web Docs [Na internetu]. Dostupno: https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works [pristupano: 23.08.2021].

[8] vpnMentor (12.12.2017.) “What is a VPN and how does it work?“ Youtube [Video datoteka]. Dostupno: https://www.youtube.com/watch?v=_wQTRMBAvzg&ab_channel=vpnMentor [pristupano: 13.8.2021.]

[9] J.C.Snader, VPNs Illustrated: Tunnels, VPNs, and IPsec. Upper Saddle River, NJ, USA: Addison-Wesley Professional. 2005.

[10] IBM(bez dat.) *„What is encryption? Data encryption defined“* [Na internetu]. Dostupno: https://www.ibm.com/topics/encryption [pristupano:13.8.2021.].

[11] J.H. Carmouche, IPsec virtual private network fundamentals an introduction to VPNs. Indianopolis, Indiana, USA: Cisco Press. 2006.

[12] „What is a VPN?“ (bez dat.). Datashield [Na internetu]. Dostupno: https://www.datashieldprotect.com/blog/what-is-a-vpn [pristupano: 17.08.2021.]

[13] VPN Encapsulation [Slika] (bez dat.) Dostupno: http://ww2.cs.fsu.edu/~bogdanov/SysAdminSp04/Agenda/week12/vpn.htm [pristupano 21.08.2021.]

[14] CARNet (bez dat.) *Osnovni koncepti VPN tehnologije* [Na internetu]. Dostupno: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf [pristupano 02.09.2021.].

[15] E. Mujarić, „Tuneliranje“, (bez dat.). [Na internetu]. Dostupno: http://mreze.layer-x.com/s060100-0.html [pristupano: 28.08.2021.].

[16] How Does a VPN Work? VPN Encryption & Tunneling Explained [Slika] (bez dat.) Dostupno: https://www.top10vpn.com/what-is-a-vpn/how-does-a-vpn-work/ [pristupano 13.08.2021]

[17] „What Is OpenVPN & How Does OpenVPN Work?“ (bez dat.). CactusVPN [Na internetu]. Dostupno: https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-openvpn/ [pristupano: 28.08.2021.].

[18] „Site-to-Site VPN: How it Works and Do You Need One?“ (27.08.2021.). Impact [Na internetu]. Dostupno: https://www.impactmybiz.com/blog/blog-site-to-site-vpn/?fbclid=IwAR0mytlTXY5R3MZ9B-AW_GhlkGVkzffr93uiy-B5M-dXMuOxGi64TXVIFMI [pristupano: 28.08.2021.].

[19] Site-toSite VPN [Slika] (bez dat.) Dostupno: https://commons.wikimedia.org/wiki/File:Site-to-site_VPN-en.svg [pristupano 28.08.2021.]

[20] „Remote Access VPN: Give Your Employees the Access They Need“ (bez dat.). OpenVPN [Na internetu]. Dostupno: https://openvpn.net/for/remote-access/ [pristupano 27.08.2021.].

[21] Remote-access VPN [Slika] (bez dat.) Dostupno: https://www.greyson.com/remote-access-vpn-guide/ [pristupano 28.08.2021.]

[22] „7 Advantages and Disadvantages of VPN | Risks & Benefits of VPN“ (bez dat.) Hitechwhizz [Na internetu]. Dostupno: https://www.hitechwhizz.com/2020/02/7-advantages-and-disadvantages-risks-benefits-of-vpn.html [pristupano 25.08.2021]

[23] „Configure a Point-to-Site VPN connection using Azure certificate authentication: Azure portal“ (19.08.2021.) Microsoft Documentation [Na internetu]. Dostupno: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal [pristupano 02.09.2021.]

Popis slika

Slika 1. Povijest VPN-a [autorski rad] 3
Slika 2. Dohvaćanje doemene web stranice [5] 6
Slika 3. Kriptiranje podataka. [11, str.8] 9
Slika 4. Enkapsulacija podataka [13] 10
Slika 5. VPN mreža [16] 12
Slika 6. Putovanje zahtjeva za prikaz web stranice putem VPN-a [16].....12
Slika 7. L2TP protokol [11, str.11].....15
Slika 8. Site-to-Site VPN [19].....17
Slika 9. Remote-access VPN [21].....18
Slika 10. Kreiranje resursne grupe (portal.azure.com) 22
Slika 11. Kreiranje virtualne mreže (portal.azure.com).....22
Slika 12. Kreiranje virtualnog Gatewaya (portal.azure.com) 23
Slika 13. Kreiranje virtualnog uređaja (portal.azure.com).....24
Slika 14. Konfiguracija VPN klijenta (portal.azure.com) 25
Slika 15. Veza na virtualni uređaj 26
Slika 16. Prikaz različitih IP adresa virtualnog računala (lijevo) i lokalnog računala (desno) .26
Slika 17.TunnelBear promjena IP adrese 27

Popis tablica

Tablica 1. Karakteristike VPN-a.....11