Virtual Private Network

Halar, Ljudevit

Sveučilište Jurja Dobrile u Puli

Fakultet Informatike

LJUDEVIT HALAR

VIRTUAL PRIVATE NETWORK

Završni rad

Pula, rujan 2022. Godine

Sveučilište Jurja Dobrile u Puli

Fakultet Informatike

LJUDEVIT HALAR

VIRTUAL PRIVATE NETWORK

Završni rad

JMBAG: 0303075728, redovni student

Studijski smjer: Sveučilišni preddiplomski studij Informatika

Kolegij: Osnove IKT

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijske i komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor: doc. dr. sc. Snježana Babić

Pula, rujan 2022. Godine

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za prvostupnika _____ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljeni način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

_____

Student

U Puli, _____

IZJAVA O KORIŠTENJU AUTORSKOG DJELA

Ja, _____ dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj Završni rad pod nazivom _____

_____

koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____

Potpis

_____

SADRŽAJ

1. UVOD 1
2. OPĆENITO O VIRTUALNIM PRIVATNIM MREŽAMA 2
3. VRSTE VPN-A 4
   3.1 Site-to-site VPN 4
   3.2 Remote Access VPN 5
   3.3 Tuneliranje 6
4. VPN PROTOKOLI 7
   4.1 IPsec 7
   4.1.1 AH (Authentication Header) 9
   4.1.2 ESP (Encapsulated Security Payload) 11
   4.1.3 IKE (Internal Key Exchange) 13
   4.2 PPTP (Point-to-Point Tunneling Protocol) 14
   4.3 L2F (Layer 2 Forwarding) 15
   4.4 L2TP (Layer 2 Tunnel Protocol) 16
   4.5 SSL (Secure Socket Layer) 17
   4.6 SSTP(Secure Socket Tunneling Protocol) 21
   4.7 SSL/TLS (Secure Sockets Layer/Transport Layer Security) 22
5. MPLS (Multiprotocol Label Switching) 23
6. MPLS VPN 26
   6.1 Point-to-point 26
   6.2 Layer 2 VPN (VPLS) 27
   6.3 Layer 3 VPN (VPRN) 28
7. PREDNOSTI I MANE VPN-A 29

8. PRIMJER PRIMJENE VPN-A....33
9. BUDUĆI RAZVOJ VPN TEHNOLOGIJE....37
10. ZAKLJUČAK....40
11. LITERATURA....41

SAŽETAK

U današnje doba, ljudi su gotovo postali nezamislivi bez svakodnevnog korištenja interneta i modernih tehnologija. Svaki pojedinac koristi Internet bilo u privatne ili poslovne svrhe, a time pristupa mreži koja nije uvijek sigurna. VPN nudi korisnicima sigurno povezivanje na Internet, kao i zaštitu privatnih podataka korisnika. U ovom radu cilj je objasniti VPN tehnologiju, protokole i pojasniti koje su prednosti, a koje mane korištenja VPN. Pojasniti što je to MPLS, a što je MPLS VPN. Isto tako je uzet za primjer jedan VPN koji se koristi u agenciji, te pojasniti budući razvoj VPN tehnologije.

ABSTRACT

In today's age, people have become almost unimaginable without the daily use of the Internet and modern technologies. Every individual uses the Internet either for private or business purposes, and thus accesses a network that is not always secure. VPN offers users a secure connection to the Internet, as well as protection of users' private data. In this paper, the goal is to explain VPN technology, protocols and clarify the advantages and disadvantages of using VPN. Explain what MPLS is and what MPLS VPN is. Also, one VPN was taken as an example that is used in the agency, and to clarify the future development of VPN technology.

1. UVOD

Danas je nemoguće zamisliti ljudski život bez interneta i modernih tehnologija. Svaki pojedinac koristi internet bilo u privatne ili poslovne svrhe, a samim time pristupa mreži koja nije uvijek najsigurnija. Razvitkom tehnologije VPN-a (engl. Virtual Private Network), čovjek je omogućio svakom pojedincu da zaštiti svoju privatnost na internetu.

Kada se govori o Virtual Private Network-u, može se reći da je to tehnologija koja omogućava sigurno povezivanje računala u virtualne privatne mreže preko dijeljenje ili javne mrežne infrastrukture. Iako je većina ljudi danas čula ili se susrela s VPN-om, malo ih zapravo zna što je VPN i kako on zapravo radi.

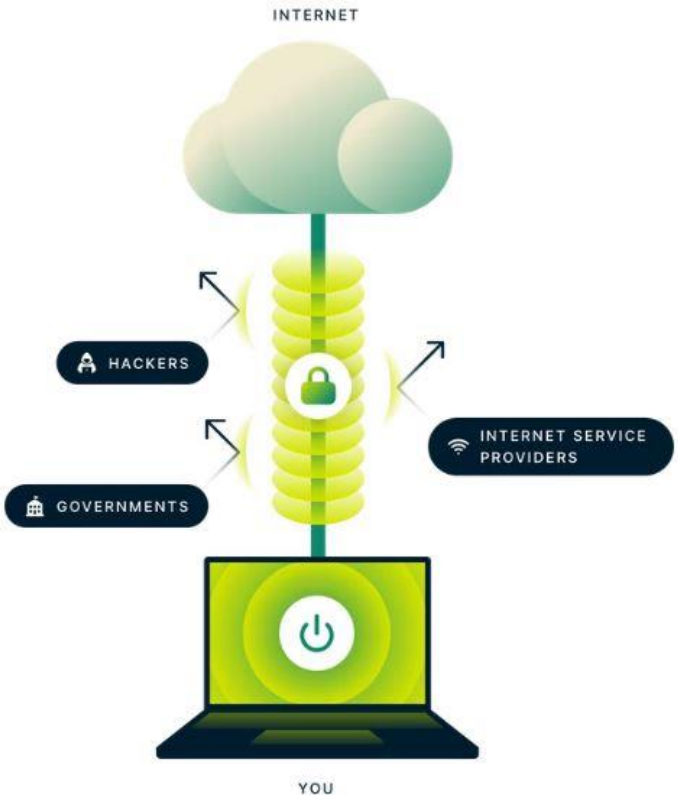
Cilj ovoga završnog rada je objasniti što je to zapravo Virtual Private Network, pojasniti osnovne VPN-a, vrste VPN tehnologija, te Multiprotocol Label Switching i Multiprotocol Label Swtiching VPN. Proći kroz prednost i mane VPN tehnologije, opisati primjer VPN-a u jednoj agenciji i pojasniti budućnost razvoja VPN tehnologije.

Završni rad je podijeljen u jedanaest poglavlja.

Prvo poglavlje je uvod. U drugom poglavlju je opisan pojam VPN-a, i osnovne stvari vezane uz VPN. U trećem poglavlju su vrste VPN-a, kojih je tri i vrlo su bitne da razumijevanje VPN tehnologije. Četvrto poglavlje su VPN protokoli, te kako pojedini od njih funkcionira. U petom poglavlju se nalazi MPLS i njegove osnove, a u šestom poglavlju opis MPLS VPN tehnologije, odnosno kako MPLS funkcionira kao VPN. U sedmom poglavlju su prednosti i mane VPN-a. Osmo poglavlje je opis primjera primjene VPN-a u agenciji, a deveto poglavlje je razvoj VPN-a u budućnosti. Zaključak seminarskog rada je deseto poglavlje i jedanaesto poglavlje je literatura korištena u ovome radu.

2. OPĆENITO O VIRTUALNIM PRIVATNIM MREŽAMA

Virtualnu privatnu mrežu (eng. „Virtual Private Network“) je najjednostavnije objasniti kao način simulacije privatne mreže putem javne mreže, kao što je Internet.
Postoje tri vrste virtualne privatne mreže, a to su: softverske virtualne privatne mreže, hardverske virtualne privatne mreže i kombinacije softverskih i hardverskih virtualnih privatnih mreža, a one omogućuju sigurnu vezu između „peer“- ova preko javne mreže. Ta sigurna veza se postiže šifriranjem, autentifikacijom, tuneliranjem paketa i vatrozidom. (Scott et al., 1999.)



Slika 1. Prikaz zaštićene veze između nas i Interneta
Izvor: (https://www.expressvpn.com/what-is-vpn)

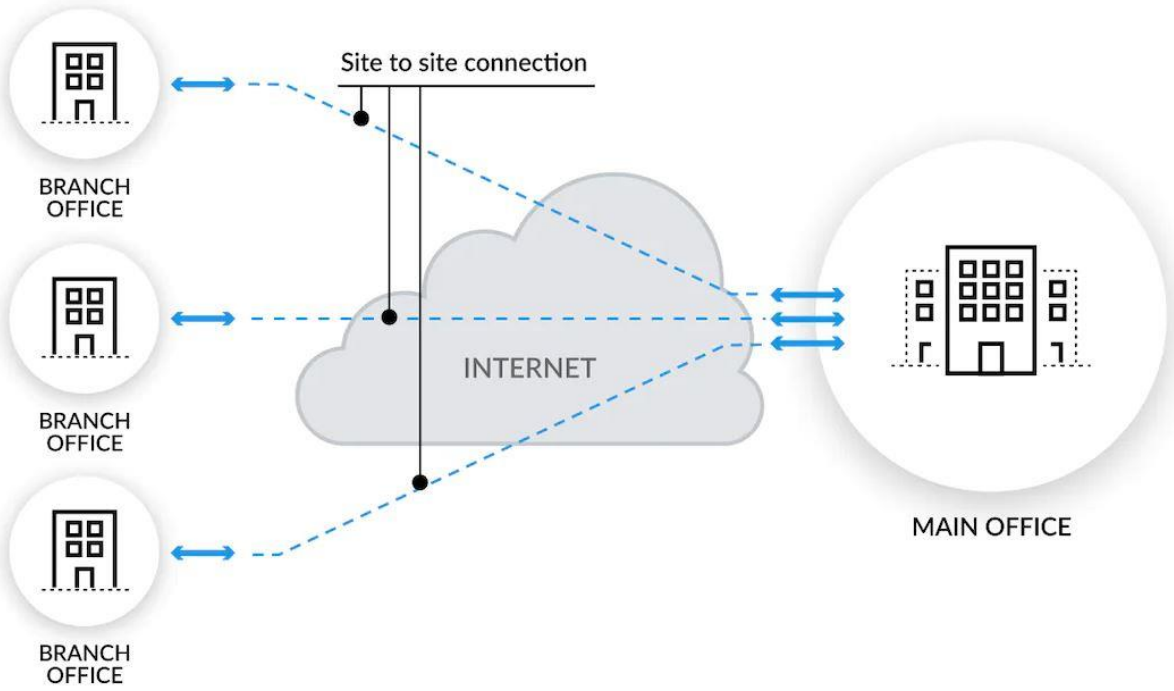
Na slici 1. je prikaz VPN poslužitelja „Express VPN“, koji sav internetski promet šalje kroz „tunel“ koji štiti od hakera, vlade i davatelja internetskih usluga.
Kad se pristupa web stranici bez VPN-a, povezivanje s tom web stranicom se vrši preko davatelja internetskih usluga (eng. „Internet Service Provider“ – ISP) , koji svakom pojedincu dodjeljuje jedinstvenu IP adresu, koja se koristi za identifikaciju korisnika na web stanici. Pošto davatelj internetskih usluga upravlja i usmjerava sav promet, on može vidjeti koje web stranice pojedini korisnik posjećuje, a aktivnost na stranicama je povezana s jedinstvenom IP adresom (ExpressVPN, 2022.) .

Kada se pojedinac poveže na VPN, njegov uređaj uspostavlja sigurnu vezu s VPN poslužiteljem. Sav internetski promet i dalje prolazi kroz davatelja internetskih usluga, ali ga on više ne vidi i ne zna njegovo konačno odredište. Web stranice koje korisnik posjećuje više ne vide njegovu IP adresu, već IP adresu VPN poslužitelja, koju koriste mnogi drugi korisnici i koja se stalno mijenja (ExpressVPN, 2022.) .

3. VRSTE VPN-A

3.1 Site-to-site VPN

Kada se spominje Site-to-site VPN, misli se na virtualnu privatnu mrežu koja je postavljena između više mreža. To može biti korporativna mreža u kojoj više ureda međusobno surađuje ili mreža poslovnice sa središnjim uredom i više lokacija poslovnica. Site-to-site VPN je posebno koristan za tvrtke kojim je prioritet privatan, zaštićeni promet i osobito su korisni za organizacije s više od jednog ureda na različitim lokacijama. Organizacije najčešće drže bitne podatke i aplikacije potrebne za poslovanje tvrtke na središnjim serverima, koji se nalaze na glavnoj mreži. Za pristup tim podacima, korisnici koji nisu smješteni fizički u organizaciji, tim podacima i aplikacijama pristupaju pomoću Site-to-site VPN-a (Fortinet, 2022.) .

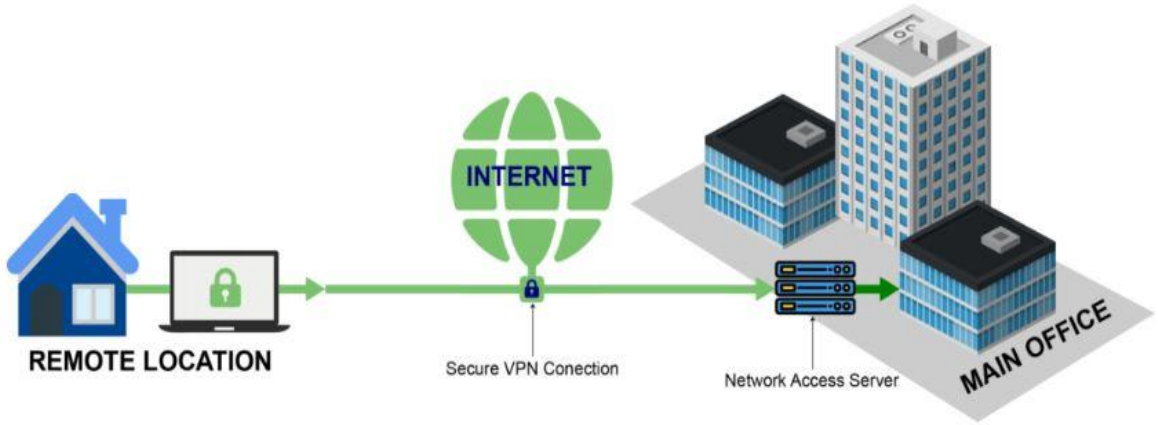


Slika 2. Primjer Site-to-site VPN-a

Izvor: (https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn)

3.2 Remote Access VPN

Remote Access VPN služi za postavljanje privremene veze između dva ili više korisnika i središnje lokacije. Može se reći da je Remote Access VPN, koristan alat za organizacije s djelatnicima koji često rade od kuće ili sa poslovnog puta. Ako radnici trebaju pristupi privatnim ili osjetljivim informacijama, koje se nalaze na glavnom serveru u tvrtki, mogu se povezati na VPN s udaljenim pristupom. Tako svaki zaposlenik dobiva pristup podacima koji su mu potrebni za obavljanje posla (Fortinet, 2022.) .



Slika 3. Primjer Remote Access VPN-a
Izvor: (https://www.greyson.com/remote-access-vpn-guide/)

Kao što se vidi na slici 3. , Remote Access VPN, koristi se kako bi se radnici spojili s različitih lokacija i ponašali se kao da su u glavnom uredu spojeni na njihovu mrežu, odnosno servere.

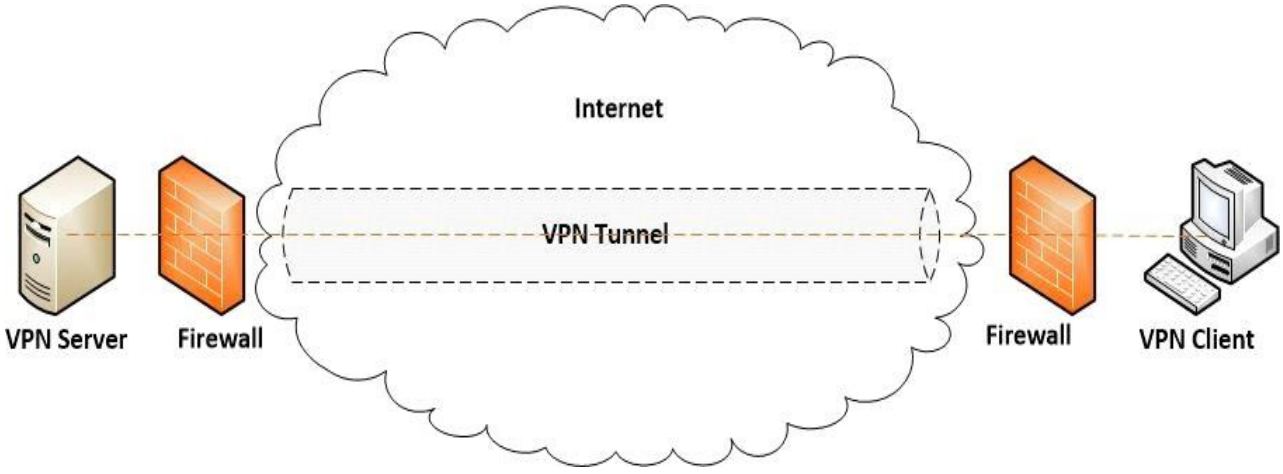
3.3 Tuneliranje

Tuneliranje je tehnika kojom se vrši prijenos podataka jedne mreže preko sigurnosnog tunela. Podaci koji se šalju mogu biti jedinice podatka protokola nekog drugog protokola, a protokol kojim se implementira tuneliranje, enkapsulira originalnoj podatkovnoj jedinici posebno oblikovano zaglavlje.
Zaglavlje koje je oblikovano sadrži dodatne podatke za usmjeravanje kako bi enkapsulirani paket stigao do svojeg odredišta. Nakraju se enkapsulirani podaci šalju između krajnjih točaka tunela (Mujarić, n.d.) .

Mujarić (n.d.) tvrdi da „postoje dva načina za uspostavljanje VPN mreže preko davatelja internetskih usluga:

- Dobrovoljno tuneliranje (engl. Voluntary Tunneling) - Slučaj kada računalo ili usmjerivač 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.,
- Obvezno tuneliranje (engl. Compulsory Tunneling) - Većina poslužitelja s modemskim ulazima koje koriste ISP-ovi imaju implementiranu mogućnost automatskog kreiranja tunela za modemskog korisnika.“

Na slici 4. je prikaz prijenosa podataka putem interneta, preko VPN tunela od VPN servera do krajnjeg korisnika, uz što imamo i vatrozid s obje strane.



Slika 4. Tuneliranje podataka preko VPN-a
Izvor: (https://www.vpnmentor.com/blog/ultimate-guide-to-vpn-tunneling/)

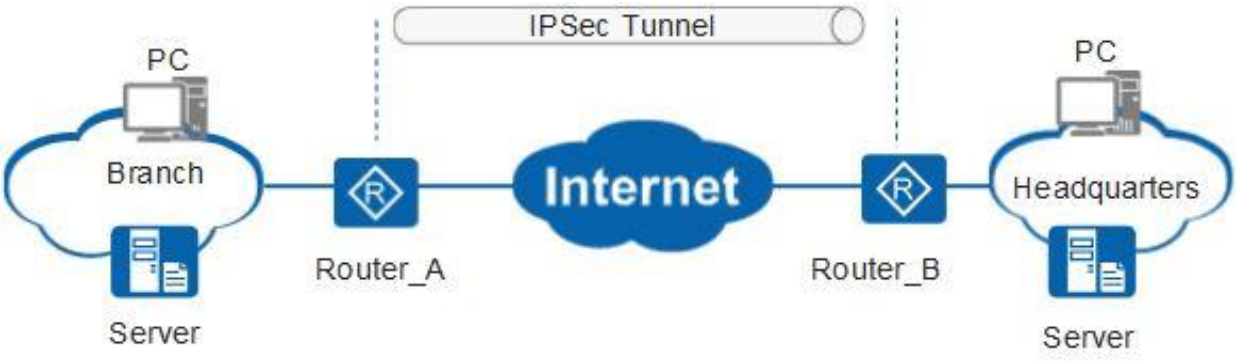
4. VPN PROTOKOLI

4.1 IPsec

IPSec je skup protokola koji se sastoji od paketa za uspostavljanje VPN konekcije. Protkoli koje koristi IPSec su :

- Zaglavlje provjere autentičnosti („Authentication Header - AH“)
- Enkapsulacija sigurnosnog tereta („Encapsulating Security Payload - ESP“)
- Internetska razmjena ključeva („Internet Key Exchange - IKE“)
- metode provjere autentičnosti i algoritme šifriranja

IPSec protokol određuje koje sigurnosne protokole i algoritme će odabrati, kao i način na koji se razmjenjuju sigurnosni ključevi između komunikacijskih kolega, na način da ponudi protokole gornjeg sloja s mrežnim sigurnosnim uslugama uključujući kontrolu pristupa, autentifikaciju izvora podataka, enkripciju podataka, itd (Hillstonenet, 2022.) .



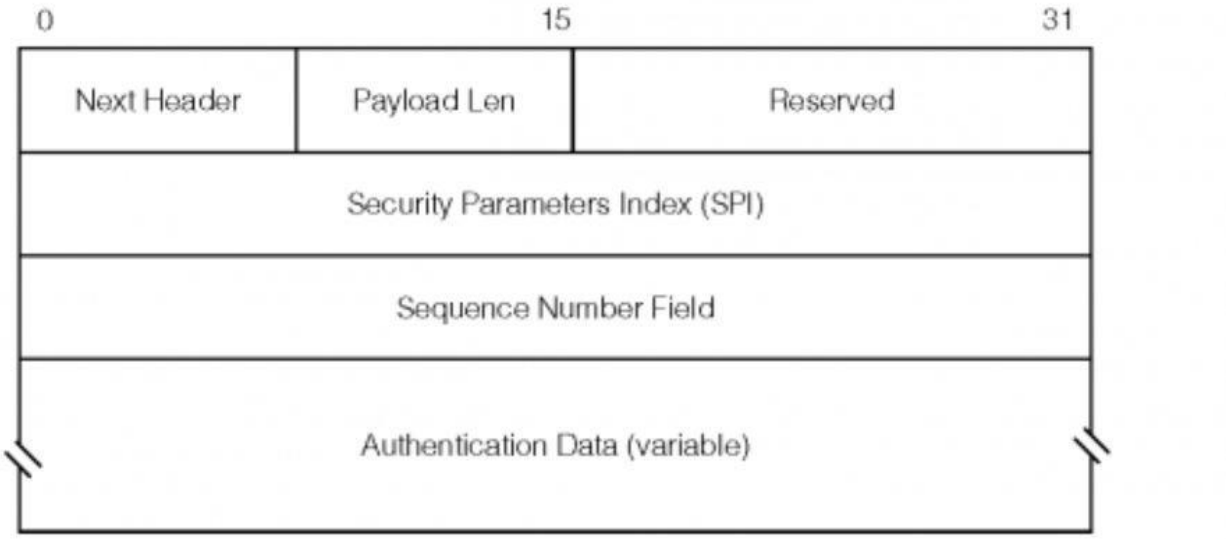
Slika 5. Primjer IPsec tuneliranja podataka site-to-site
Izvor:(ttps://support.huawei.com/enterprise/en/doc/EDOC1100041799/f2298f86/using-ipsec-vpn-to-implement-secure-interconnection-between-lans)

Doraswamy i Harkins (2003.) tvrde da „kroz rad IPSec-a koriste se sljedeći protokoli i standardi:

- Diffie-Hellman metodu za razmjenu ključeva - glavni ključ koji se koristi za generiranje regularnih ključeva se ne prenosi istim medijem kao i ostali podaci za spajanje
- DES ili 3DES standard za šifriranje podataka - enkripcijski podatkovni standard
- HMAC - kombinirano orijentirana autentifikacija koda
- Digitalna uvjerenja izdana od strane odgovarajućeg .“

4.1.1 AH (Authentication Header)

Zaglavlje provjere autentičnosti (eng. Authentication Header) je protokol koji se koristi za provjeru autentičnosti. Ujedno se koristi i za zaštitu od napada prilikom ponovljenog slanja paketa. IBM (2021.) tvrdi da „U slučaju da se koristi više zaglavlja , zaglavlje provjere autentičnosti uvijek mora biti postavljeno iza svih zaglavlja koja se procesiraju na svakom čvoru preko kojih određeni paket putuje, a ispred svih zaglavlja koja se procesiraju samo na odredišnom čvoru.“



Slika 6. Authentification Header
Izvor: (https://security.foi.hr/wiki/index.php/VPN_pomo%C4%87u:_L2TP/IPSEC-a.html)

Kao što se vidi na slici 6., Security FOI (2013.) tvrdi da se „zaglavlje za provjeru autentičnosti sastoji se od :

- Sljedećeg zaglavlja (Next Header) – S maksimalnom duljinom od 8 bita ,te identificira protokol zaglavlja koje slijedi
- Duljina tereta (Payload Length) – sastoji se od 8 bite, te pokazuje ukupnu duljinu AH zaglavlja 11
- Indeks sigurnosnih parametara (SPI, Security Parameter Index) – 32-bitno polje čija je vrijednost proizvoljna
- Rezervirano (Reserved) – polje rezervirano za buduću uporabu,sastoji se od 16 bita
- Redni broj (Sequence Number) – 32-bitna vrijednost koja predstavlja brojač. Služi za sprečavanje napada ponovljenim slanjem paketa
- Autentifikacijski podaci (Authentication Data) – polje se sastoji od n 32-bitnih jedinica, predstavlja najvažniji dio AH zaglavlja. Ovo polje sadrži ICV vrijednost (engl. Integrity Check Value) vrijednost za provjeru integriteta“

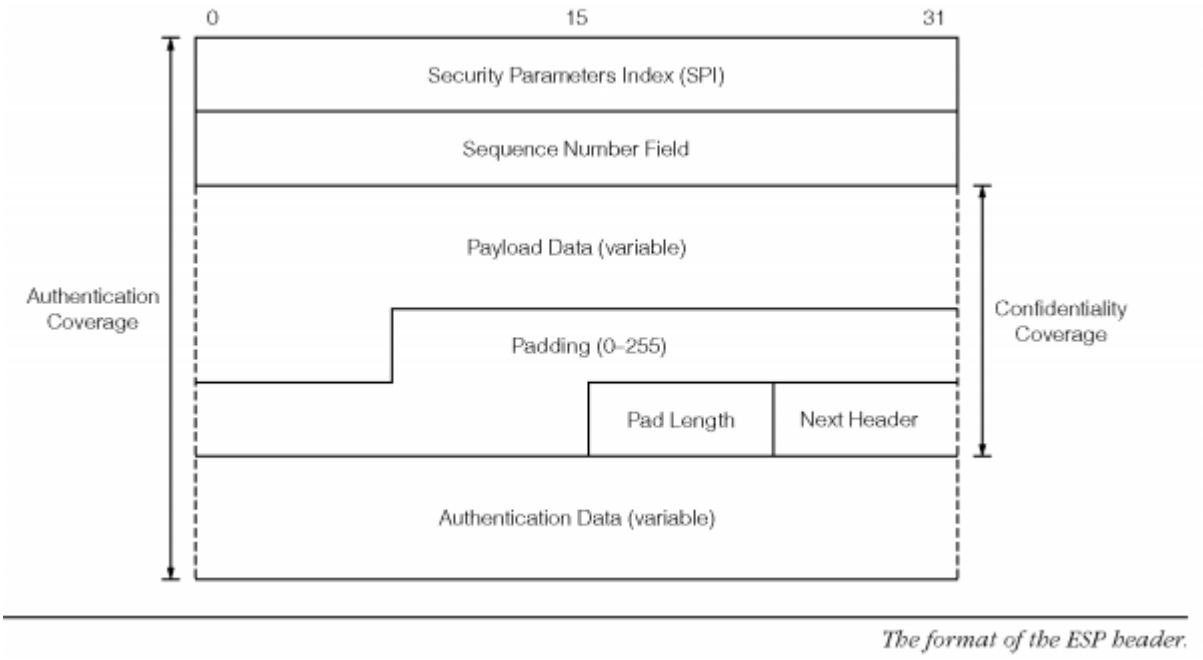
4.1.2 ESP (Encapsulated Security Payload)

IBM (2021.) tvrdi „Protokol Encapsulating Security Payload (ESP) pruža povjerljivost podataka, a također opcionalno pruža autentifikaciju izvora podataka, provjeru integriteta podataka i zaštitu od ponovnog prikazivanja. „

ESP zaglavlje ima mogućnost više usluga a neke se preklapaju s uslugama AH zaglavlja:

- Povjerljivost podatkovnog paketa (postignuta zahvaljujući enkripciji)
- Utvrđivanje autentičnosti porijekla podataka
- Zaštita od napada ponavljajućim paketima (zahvaljujući mehanizmu brojača, kao kod AH zaglavlja)
- Ograničena povjerljivost podatkovnog toka (uporabom sigurnosnih gateway-a)

Razlika između EPS-a i AH-a je u tome što ESP ima opciju enkripcije, dok oba protokola pružaju autentifikaciju, provjeru integriteta i zaštitu od ponavljanja. (IBM, 2021.)



Slika 7. Encapsulated Security Payload protocol
Izvor: (https://security.foi.hr/wiki/index.php/VPN_pomo%C4%87u:_L2TP/IPSEC-a.html)

Na slici 7. je ESP zaglavlje, Security FOI (2013.) tvrdi da „se sastoji od:

- SPI – jednako kao i kod AH, definira se jedinstveni SA skup sigurnosnih parametara,
- Sequence Number Field – također je jednak kao i kod AH,
- Payload Data – polje proizvoljne duljine sadrži podatkovni dio IP paketa i ispunu, mogu biti eksplicitno sadržani podaci koji služe za kriptografsku sinkronizaciju (npr. Inicijalizacijski vektor - IV), ako to zahtjeva kriptografski algoritam koji se koristi,
- Next header – kao i kod AH, identificira tip podataka koji slijedi nakon ESP zaglavlja,
- Payload Lenght – definira duljinu ispune,
- Authentication Data – polje proizvoljne duljine i nije obavezno, a koristi se samo u slučaju kada je u SA skupu sigurnosnih parametara specificirana usluga autentifikacije.“

4.1.3 IKE (Internal Key Exchange)

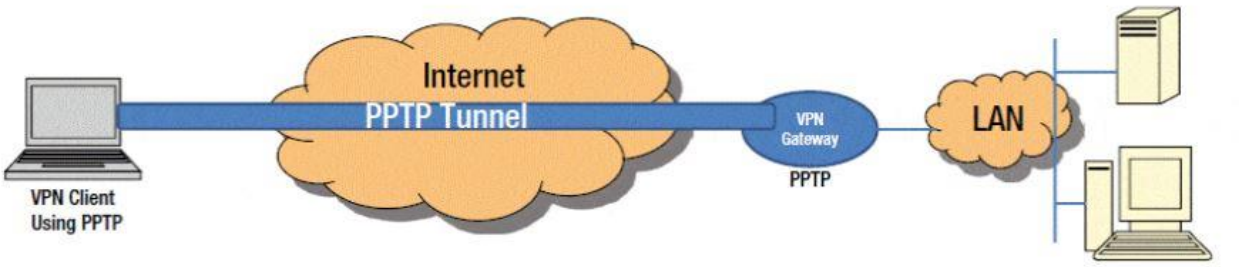
Internet Key Exchange (IKE) je standardni protokol koji se koristi za postavljanje sigurnog i provjerenog komunikacijskog kanala između dva korisnika putem virtualne privatne mreže. IKE omogućava i osigurava sigurnost za VPN komunikaciju, udaljeni hosting i pristup mreži. On je dio IPsec-a, a u njemu IKE definira automatski način komunikacije i provjere autentičnosti za IPsec SA (Sigurnosno udruženje - sporazum ili ugovor između dva IPsec peera ili krajnje točke) (TechTarget, 2022.) .

(TechTarget, 2022.) tvrdi da su „poboljšanja u IKEv2 u odnosu na IKEv1 su sljedeća:

- zahtijeva manju propusnost
- zahtijeva manje kriptografskih mehanizama za zaštitu paketa
- zahtijeva samo jedan mehanizam početne razmjene s četiri poruke
- podržava mobilne platforme, uključujući pametne telefone
- podržava osiguranje Stream Control Transmission Protocol (SCTP) prometa
- pruža veću otpornost na napade uskraćivanja usluge (DoS)
- dolazi opremljen s ugrađenim prevođenjem mrežnih adresa (NAT) potrebnim za podršku usmjerivačima koji izvode prijevode
- automatski otkriva je li IPsec tunel još aktivan tako da IKE može automatski ponovno uspostaviti vezu ako je potrebno
- omogućuje fragmentaciju poruka i omogućuje IKEv2 rad u područjima gdje IP fragmenti mogu biti blokirani i SA se možda neće uspjeti uspostaviti
- omogućuje rekeying za izgradnju novih ključeva za SA „

4.2 PPTP (Point-to-Point Tunneling Protocol)

PPTP je protokol sloja podatkovne mreže širokog područja, temeljen na protokolu PPP (Point-to-Point protokolu). PPTP omogućuje enkapsulaciju i usmjeravanje mrežnog prometa preko nezaštićene javne mreže kao što je Internet. Point-to-Point Tunneling Protocol omogućuje stvaranje virtualnih privatnih mreža, koje tuneliraju TCP/IP promet kroz Internet. (Network Encyclopedia, 2022.)



Slika 8. Point-to-Point Tuneling Protocol

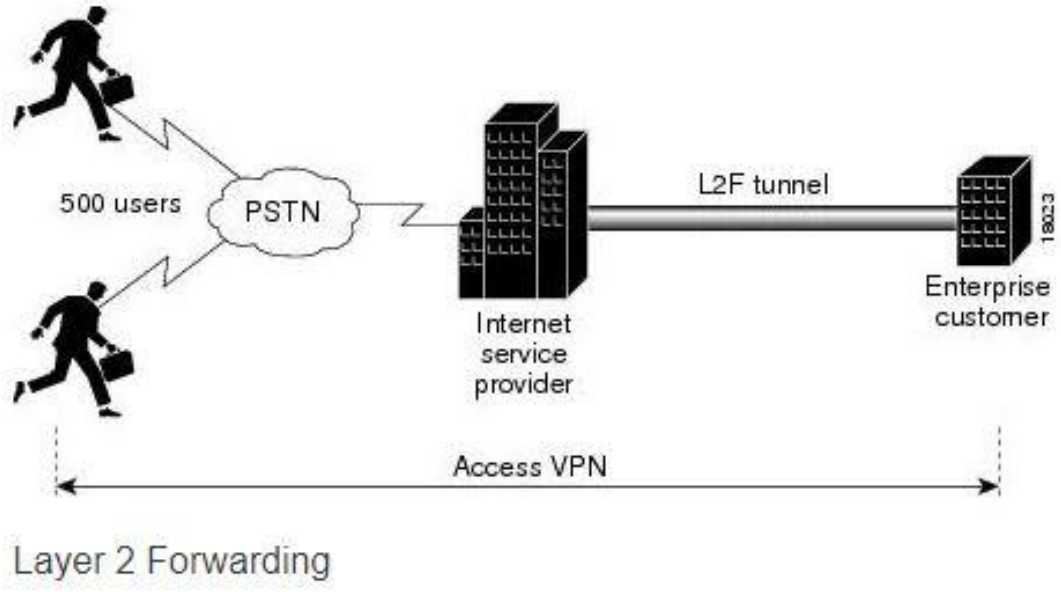
Izvor: (https://networkencyclopedia.com/point-to-point-tunneling-protocol-pptp/)

Microsoft Corporation, (1997.) tvrdi da „ PPTP protokol uključen je u operativne sustave Windows NT® Server verzija 4.0 i Windows NT Workstation verzija 4.0.“ Računala s operativnim sustavima Windows mogu koristiti protokol tuneliranja od točke do točke za sigurno povezivanje VPN klijenta preko javnih podatkovnih mreža kao što je internet. Protokol tuneliranja od točke do točke mogu koristiti i računala koja su spojena na lokalnu mrežu za stvaranje virtualne privatne mreže preko LAN-a. Moguće je i virtualno privatno umrežavanje telefonije putem korištenja javnih telefonskih mreža. PPTP uvelike pomaže pojednostavljenju smanjenja troškova rješenja implementacije za pristup na daljinu za neko poduzeće i njihove korisnike, jer im pruža sigurnu i kriptiranu komunikaciju preko javnih telefonskih linija i interneta (Microsoft Corporation,1997.).

4.3 L2F (Layer 2 Forwarding)

Layer Two Forwarding (L2F) je protokol za tuneliranje koji koristi virtualne mreže za siguran prijenos podataka. Način na koji radi L2F sličan je protokolu tuneliranja od točke do točke (PPTP) (Techopedia, 2022.) .

Prilikom korištenja protokola od točke do točke s L2F protokolom, PPP osigurava vezu između pozivnog klijenta i mrežnog pristupnog poslužitelja koji prima poziv. Klijent koji pokreče PPP vezu završava se na poslužitelju mrežnog pristupa koji se nalazi kod davatelja PPP usluga koji je najčešće davatelj internetskih usluga(eng. Internet Service Provider - ISP). Na slici 9. je prikaz 500 korisnika koji šalju podatke preko javne komutirane telefonske mreže koja se povezuje na davatelja internetskih usluga i preko L2F tunela šalju poslovnom kupcu (Network Encyclopedia,2022.) .



Slika 9. Prikaz Layer 2 Forwarding-a
Izvor: (https://networkencyclopedia.com/layer-2-forwarding-l2f/)

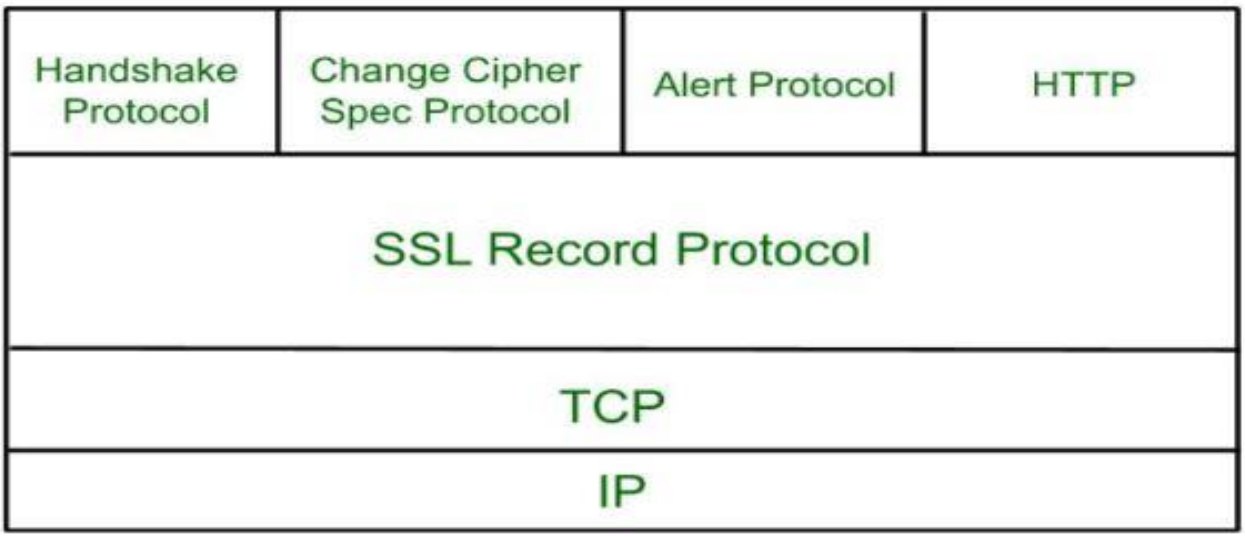
4.4 L2TP (Layer 2 Tunnel Protocol)

Layer 2 Tunneling Protocol (L2TP) su veze, koje se ujedno nazivaju i virtualne linije, a omogućavaju pristup za udaljene korisnike dopuštajući mrežnim sustavima poduzeća, da upravljaju IP adresama dodijeljenim udaljenim korisnicima (IBM, 2021.). L2TP sam po sebi ne osigurava enkripciju niti autentifikaciju, pa se uz njega koristi IPSec protokol (ExpressVPN, 2016.).

Postoje dva L2TP tunela, dobrovoljni tunel i obavezni tunel. Na dobrovoljnom tunelu, tunel završava kod udaljenog klijenta, dok obavezni tunel završava kod davatelja internetskih usluga. Prilikom korištenja dobrovoljnog tunela, vezu stvara udaljeni korisnik, korištenjem L2TP klijenta za tuneliranje podataka. Rezultata korištenja dobrovoljnog tunela, udaljeni korisnik šalje L2TP pakete svom davatelju internetskih usluga koji te pakete prosljeđuje mreži tvrtke. Kada se koristi obavezni L2TP tunel, udaljeni domaćin (eng. host) uspostavlja vezu sa davateljem internetskih usluga i uspostavlja L2TP vezu između udaljenog korisnika i mreže tvrtke. Isto tako u L2TP obaveznom tunelu je bitno za naglasiti da iako naš davatelj internetskih usluga uspostavlja vezu, korisnik odlučuje kako će zaštiti promet korištenjem VPN-a. Glavna razlika između dobrovoljnog i obaveznog tunela je da uz dobrovoljni tunel davatelj internetskih usluga ne mora podržavati L2TP, dok kod obaveznog tunela mora. (IBM, 2021.)

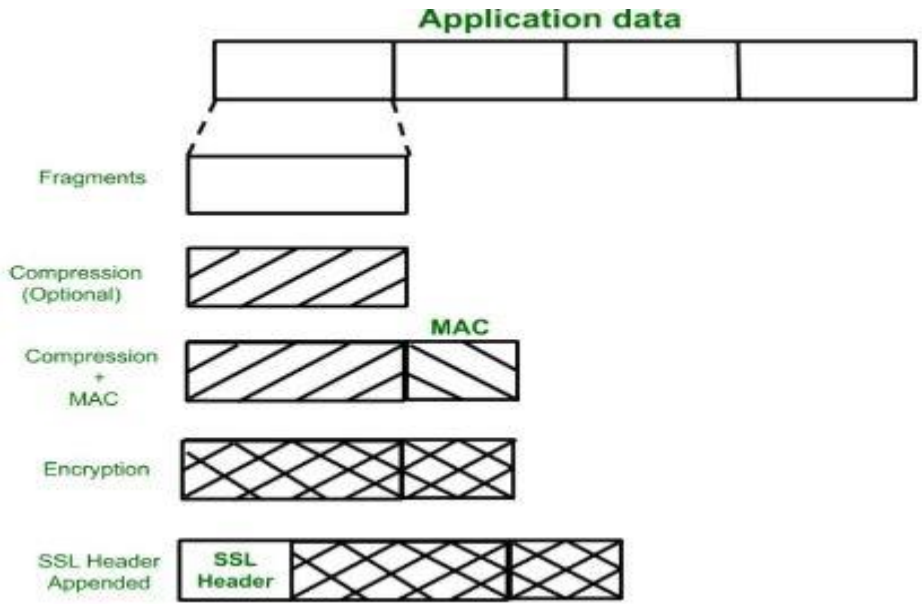
4.5 SSL (Secure Socket Layer)

Secure Socket Layer (SSL) je internetski sigurnosni protokol, a pruža sigurnost podacima koji se prenose između web preglednika i poslužitelja. Šifriranjem veze SSL postiže siguran prijenos podataka između web poslužitelja i web preglednika. Kao što prikazuje slika 10., razlikujemo četiri Secure Socket Layer protokola, protokol SSL zapisa (eng. SSL record protocol), protokol rukovanja (eng. Handshake protocol), protokol promjene šifre (eng. Change-cipher spec protocol) i protokol upozorenja (eng. Alert protocol). (GeeksforGeeks, 2022.)



Slika 10. SSL protokol
Izvod: (https://www.geeksforgeeks.org/secure-socket-layer-ssl/)

Protokol SSL zapisa (eng. SSL record protocol) pruža povjerljivost i integritet poruke. Na slici 11. je prikaz protokol SSL zapisa. U aplikacijskom podatku, podaci su podijeljeni na dijelove ("Fragmente") koji se sažimaju i na koje se dodaje kod za provjeru autentičnosti poruke ("MAC"). Nakon toga vrši se enkripcija koja se dodaje SSL zaglavlju. (GeeksforGeeks, 2022.)



Slika 11. Protokol SSL zapisa
Izvod: (https://www.geeksforgeeks.org/secure-socket-layer-ssl/)

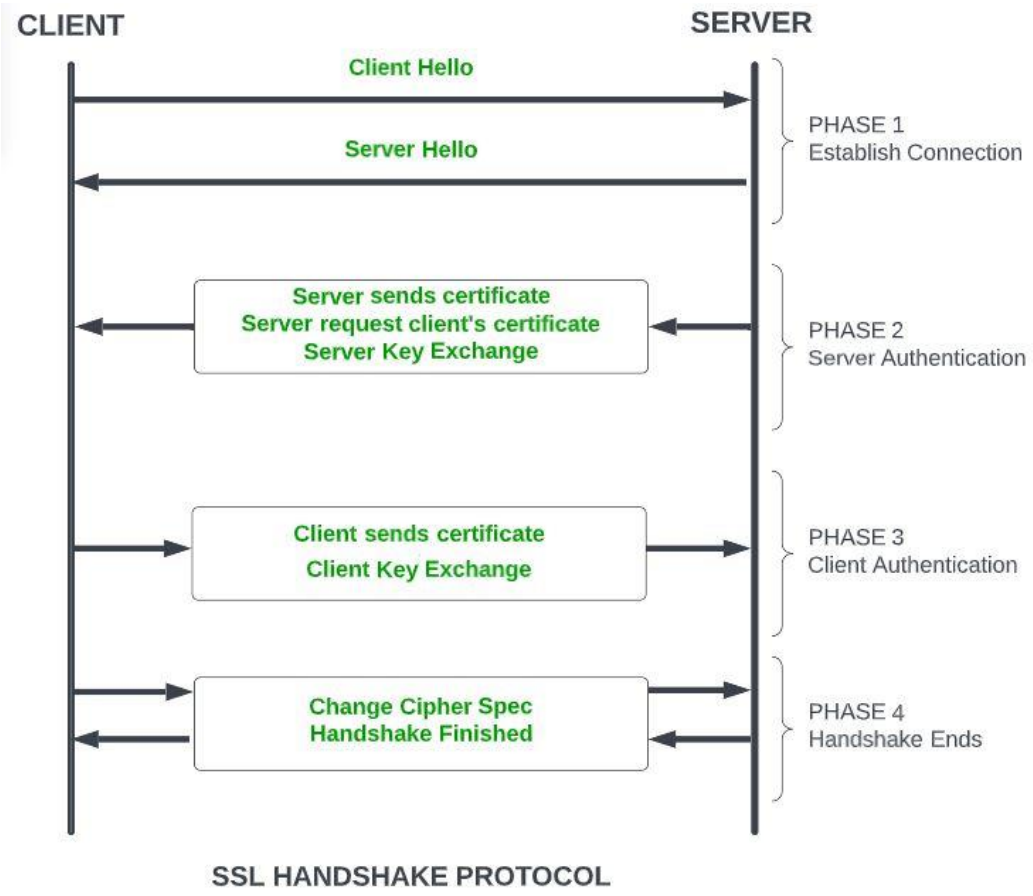
Protokol rukovanja (eng. Handshake Protocol), koristi se za uspostavljanje komunikacije između klijenta i servera. Ovaj protokol omogućuje klijentu i poslužitelju da se međusobno autentificiraju slanjem niza poruka. Protokol rukovanja koristi četiri faze (Slika 12.) da završi svoj ciklus. (GeeksforGeeks, 2022.)

Faza 1: klijent i poslužitelj međusobno razmjenjuju "Hello" pakete. Radi sigurnosti, u ovoj fazi paket šifra i verzija protokola se razmjenjuju.

Faza 2: poslužitelj korisniku šalje svoj certifikat i traži certifikat od korisnika, a istodobno traži razmjenu ključeva.

Faza 3: klijent odgovara na poslužiteljov upit za slanje svojeg certifikata i ključa razmjene od klijenta.

Faza 4: kada su klijent i poslužitelj uspješno authentificirani, završava se postupak protokola rukovanja. (GeeksforGeeks, 2022.)



Slika 12. Protokol rukovanja kroz faze

Izvod: (https://www.geeksforgeeks.org/secure-socket-layer-ssl/)

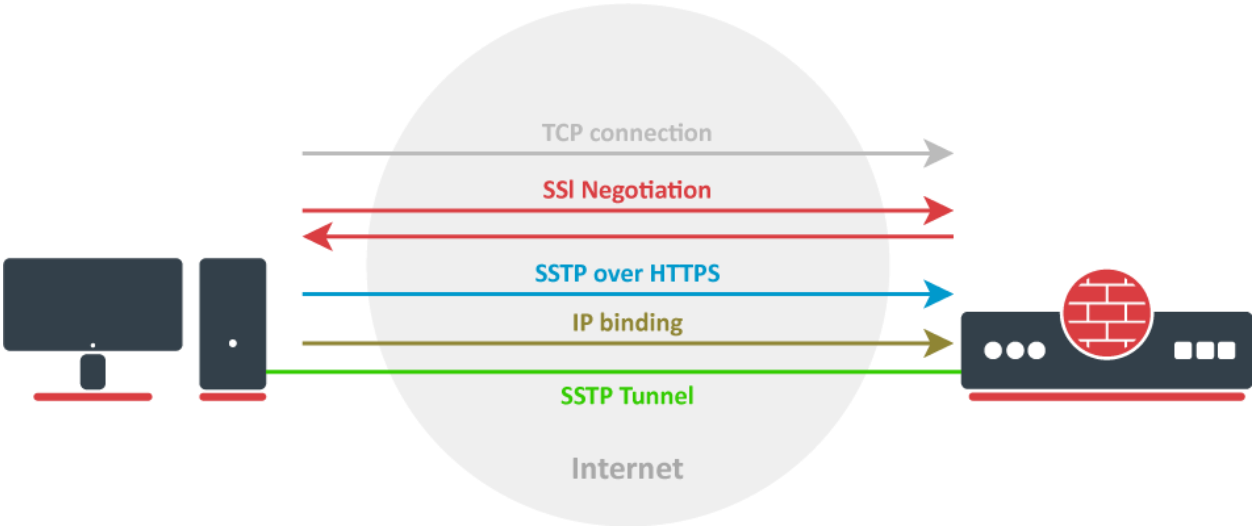
Protokol promjene šifre (eng. Change-cipher spec protocol) je protokol koji koristi SSL zapisni protokol. Njegova svrha je izazvati kopitanje stanja čekanja u trenutno stanje. Ako protokol rukovanja nije gotov, izlaz SSL zapisa biti će u stanju čekanja. Kada se izvrši protokol rukovanja stanje se mijenja u trenutno stanje. Protokol šifre sastoji se od poruke dugačke 1 bajt i ima samo jednu vrijednost. (GeeksforGeeks, 2022.)

Protokol upozorenja (eng. Alert Protocol) je protokol koji se koristi za prijenos upozorenja povezanih sa SSL-om ravnopravnom entitetu. Svaka poruka u ovom protokolu sadrži 2 bajta. (GeeksforGeeks, 2022.)

4.6 SSTP(Secure Socket Tunneling Protocol)

Secure Socket Tunneling Protocol (SSTP) je protokol virtualne privatne mreže koji omogućuje prolaz VPN prometa kroz većinu vatrozida.

Uz SSTP VPN protokol, sav promet prolazi kroz šifrirani tunel koristeći iste sigurnosne protokole i portove koji uspostavljaju HTTPS veze. Samim time djelatnici neke organizacije imaju omogućeno spajanje na daljinu bez brige od zabrane vatrozida. (Techslang, n.d.)



Slika 13. SSTP prolazi kroz vatrozid

Izvor: (https://help.mikrotik.com/docs/display/ROS/SSTP)

4.7 SSL/TLS (Secure Sockets Layer/Transport Layer Security)

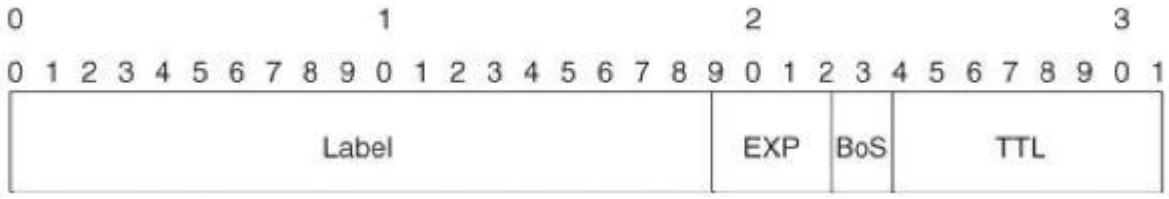
SSL/TLS protokoli funkcioniraju kao jedan protokol, a oba protokola se upotrebljavaju za postavljanje VPN veze. U toj VPN vezi mrežni preglednik ima ulogu klijenta, a pristup korisnika je ograničen isključivo na određene aplikacije umjesto cijele mreže. Ovaj protokol se najviše koristi za web stranice poput e-trgovina, jer pruža sigurnu sesiju od mrežnog preglednika do aplikacijskog poslužitelja. Mrežni preglednici imaju ugrađeni SSL/TLS i zato sve sigurne URL adrese imaju "https" umjesto "http". (Jurić, 2022.)

5. MPLS (Multiprotocol Label Switching)

Multiprotocol Label Switching je mrežna tehnologija koja se koristi oznakama (eng. label) prikvačenim na pakete za njhovo usmjeravanje kroz mrežu. MPLS dodjeljuje oznake svakom paketu podataka, kontrolirajući njihovu putanju. Velika prednost MPLS je ta što poboljšava brzinu prometa, tako da korisnici koji su povezani na mrežu ne osjete zastoje. (De Ghein, 2007.)

MPLS zaglavlje

Na slici 15. je prikaz MPLS zaglavlja, i može se vidjeti da je ono zapravo polje od 32 bita s određenom strukturom. Sastoji se od oznake (eng. Label) - polje veličine 20 bita i s njime se prosljeđuju MPLS paketi, eksperimenta (eng. Experimental) - polje veličine 3 bita koje usmjerivači koriste za odlučivanje postavljanja reda čekanja paketa, dna hrpe (eng. Bottom of Stack) – polje veličine 1 bit koje predstavlja zadnju oznaku prije IP paketa i vremena života (eng. Time to Live) - polje veličine 8 bita koje opisuje životni vijek MPLS paketa. (De Ghein, 2007.)



Slika 14. MPLS zaglavlje

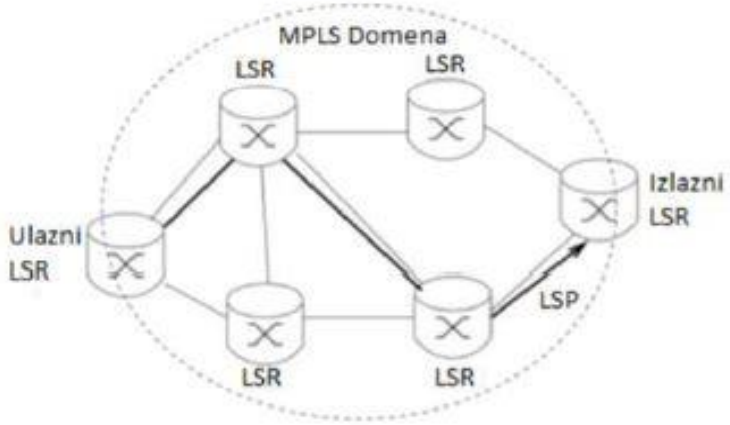
Izvor:(https://books.google.hr/books?hl=hr&lr=&id=AUG1DAAAQBAJ&oi=fnd&pg=PT31&dq=mpls&ots=-dVQAMV8WE&sig=CD9pghe_akgmqH5yov3XyDhX2RY&redir_esc=y#v=onepage&q=mpls&f=false)

MPLS usmjerivači

LSR je usmjerivač koji spada u fizički dio mreže koji podržava tehnologiju MPLS. Kompatibilan je s MPLS-om u pogledu primanja i predaje paketa na podatkovnom sloju. LSR usmjerivači mogu brzo usmjeravati podatkovne pakete bez potrebe za provjerom tablica usmjeravanja. (Susitaival, 2004.)

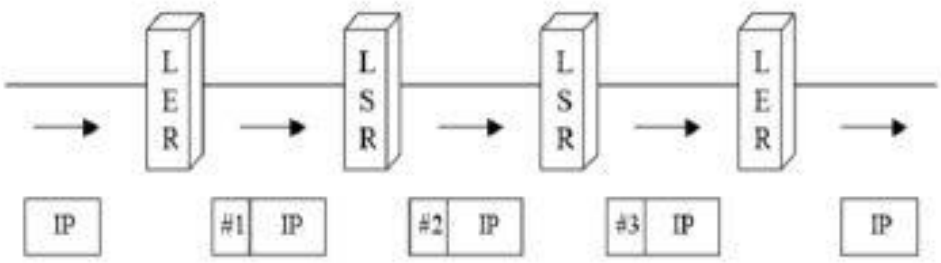
Susitaival (2004.) tvrdi da „Postoje tri različite vrste LSR-a, a razlikuju se prema lokaciji i položaju na LSP putu paketa a to su:

- ulazni LSR-rubi LSR prima paket i dodaje mu oznaku te ga šalje u MPLS domenu
- tranzitni LSR-nalazi se usred LSP-a, prebacuje MPLS pakete na sljedeći put u LSP-u
- izlazni LSR-LSR koji prima pakete i uklanja oznaku i isporučuje dalje. „



Slika 15. MPLS model prosljeđivanja

Izvor:(https://www.netlab.tkk.fi/tutkimus/fit/publ/thesis_Susitaival_04.pdf)



Slika 16. Prolazak paketa kroz LSR

Izvor:(http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.589.6130&rep=rep1&type=pdf)

Na slici 17. se vidi da kod ulaznog LSR-a, oznake se stavljaju na neoznačene pakete, a kod izlaznog LSR-a te oznake se uklanja. LSP (Label Swithed Path) sadrži niz povezanih LSR-ova koji predstavljaju putanju u MPLS mreži kojom putuju označeni paketi jedne veze. Prvi LSR na LSP putu je ulazni LSR, dok je posljednji LSR na LSP putu izlazni LSR. Paket na ulaznim i izlaznim usmjerivačima dobiva oznaku pri čemu može putovati LSR-ovima kroz mrežu. Na rubnom izlaznom usmjerivaču ta oznaka se ponovno skida i paket nastavlja svojim putem. (Ruela,n.d.)

6. MPLS VPN

MPLS VPN je fleksibilna metoda za prijenos i usmjeravanje nekoliko vrsta mrežnog prometa pomoću MPLS okosnice. Razlikuju se tri vrste MPLS VPN-a; Point-to point , Layer 2 i Layer 3. (Wallace, 2015.)

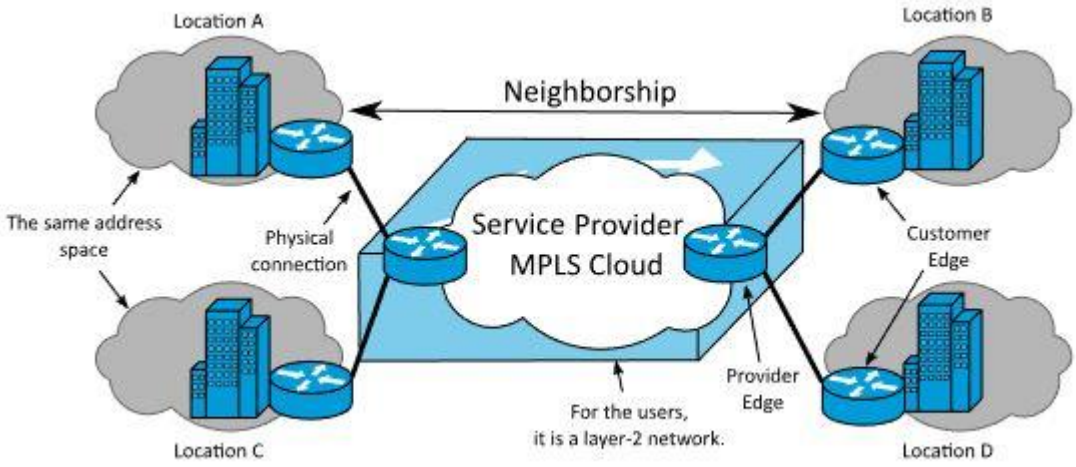
6.1 Point-to-point

Point-to-point MPLS VPN-ovi koriste VLL (virtual leased lines) za pružanje Layer 2 povezivanja od točke do točke između dva mjesta.

Point-to-point MPLS VPN koristi virtualne zakupljene linije (eng. virtual leased lines) za mogućnost Layer2 povezivanja od točke do točke između dva mjesta.
Najčešći primjer poduzeća kako koristi Point-to-point VPN je enkapsuliranjem multipleksiranih vremenskih podjela kanala krugova koji su priključeni na udaljene terminalne jedinice ili prosljeđivanjem neusmjerenih distribuiranih mrežnih protokola 3 (DNP3)prometa preko mreže do glavnog računalnog sustava za nadzor (Wallace, 2015).

6.2 Layer 2 VPN (VPLS)

Layer2 MPLS VPN koji se još naziva i virtualnom privatnom LAN uslugom, koristi se za usluge "prebacivanja u oblak" i pruža mogućnost širenja VLAN-a između stranica. Na slici 18. je logički prikaz Layer 2 MPLS VPN-a iz kojeg se može vidjeti MPLS Cloud, te da se podaci usmjeravaju u njega. L2 VPN-ovi se koriste za usmjeravanje glasovnog, video i AMI prometa između trafostanica i lokacija podatkovnog centra (Wallace, 2015).

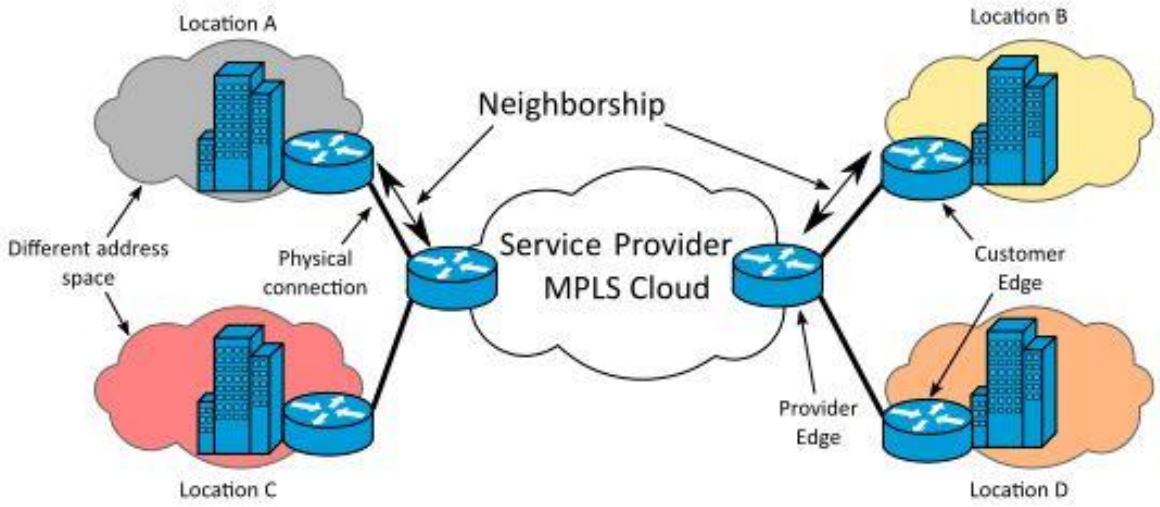


Slika 17. Logički prikaz Layer 2 MPLS VPN-a

Izvor: (https://en.wikipedia.org/wiki/File:L2_MPLS_VPN_en.svg)

6.3 Layer 3 VPN (VPRN)

Layer3 VPN koristi virtualni routing and forwarding sistem za segmentiranje tablica usmjeravanja svakog korisnika koji koristi uslugu. Kupac i usmjerivač pružatelja usluga su ravnopravni i imaju razmijenu podataka u oba smjera kao što se vidi na slici 19. Layer3 VPN se u praksi ne postavlja na lokalne mreže zbog svoje kompleksnosti, ali može se koristiti za usmjeravanje prometa između lokacija poduzeća i podatkovnog centra. (Wallace, 2015.)



Slika 18. Izgled Layer 3 MPLS VPN-a

Izvor: (https://en.wikipedia.org/wiki/File:L3_MPLS_VPN_en.svg)

7. PREDNOSTI I MANE VPN-A

VPN je jedan od najbržih i najboljih načina kako surfati internetom, a da se pri tome ostvari sigurnost i privatnost. Na slici 20. je prikaz prednosti i mana VPN-a. U nastavku će svaka od njih biti pojašnjena. Za primjer je uzet VPN proizvođača „NordVPN“.

Slika 19. Prednosti i mane VPN-a

Izvor:*(https://nordvpn.com/blog/pros-and-cons-of-vpn/)*

Prednosti

Osigurava podatke – mrežni podaci prenose se na velike udaljenosti putem različitih poslužitelja prilikom surfanja internetom. To uključuje najosobnije stvari poput poruka, lozinki, itd. Ako podaci nisu šifrirani, treće strane (kao što su pružatelji internetskih usluga, državni službenici ili kibernetički kriminalci) mogu im pristupiti i koristiti ih protiv bilo koga. Rizik je posebno velik kod korištenja nezaštićenih javnih Wi-Fi mreža.
VPN kriptira promet tako da nitko ne može vidjeti što se radi ili tko pristupa mreži.
Poželjno za imati je Premium VPN pružatelja usluga jer oni koriste najbolje algoritme šifriranja podataka, te omogućavaju najsigurnije surfanje na internetu (Ilevičius, 2021.) .

Štiti online privatnost – svaki korisnik koji se služi internetom bez sigurnosti ostavlja tragove koji mogu puno reći o njegovim online navikama. Davatelji internetskih usluga imaju pristup svim podacima, te često gledaju podatke svojih klijenata. (Ilevičius, 2021.) U državama poput SAD-a, podaci svakog korisnika se legalno mogu prodati organizacijama, koje koriste te podatke u svoje svrhe. Korištenjem VPN usluge korisnici nemaju problema i brige o svojoj privatnosti (Vasconcellos, 2021.) .

Maskira IP-adresu - svaki korisnik ima svoju jedinstvenu IP adresu, koja ako nije zamaskirana, može biti zlouporabljena za praćenje lokacije i identiteta. VPN uslugom korisnikova IP adresa se maskira i samim time stranice koje on posjećuje više ne vide IP adresu korisnika već IP adresu VPN-a.
Također pomoću maskiranja IP adrese korisnici mogu pristupiti stranicama i uslugama koje nisu dostupne u njegovoj zemlji. (npr. Netflix ne nudi isti izbor filmova u svakoj državi) (Ilevičius, 2021.).

Zaštita u neprijateljskom okruženju - ako se korisnik nađe u zemlji gdje je jako niska internetska sloboda, VPN je odličan jer može pojedinca zaštiti od posljedica surfanja webom, koje se mogu reflektirati na stvaran život. (Ilevičius, 2021.)

Prigušivanje propusnosti - davatelji internetskih usluga mogu u bilo kojem trenutku prigušiti brzinu interneta. Skrivanjem korisnikove aktivnosti putem VPN poslužitelja davatelj internetskih usluga više nema mogućnost prigušivanja brzine interneta. (Vasconcellos, 2021.)

Bolje iskustvo online igranja - česti problem online igranja su DDoS (eng. Denial of Service) napadi koji uskraćuju usluge ili servise korisnika. VPN je odlično rješenje za zaštitu od tih napada i zabrane igranja jer korisnik ne koristi svoju IP adresu, već adresu VPN poslužitelja. (Ilevičius, 2021.)

Mane

Sporiji Internet - najveća mana VPN-a je smanjenje internet brzine korisnika. Prolaskom korisnikovog prometa kroz VPN poslužitelj gubi se brzina jer je potrebno vrijeme za šifriranje aktivnosti. Najčešće usporavanje internet brzine preko VPN-a dešava se kada se korisnik prijavljuje na poslužitelj u drugoj regiji. (Vasconcellos, 2021.)

Nisu svi VPN-ovi sigurni - pogreška koju mnogi rade je što se pouzdaju u besplatne VPN poslužitelje, jer sve što je besplatno nije pouzdano. Samim time što je VPN besplatan možemo zaključiti da trguju na način da prodaju podatke svojih korisnika. Isto tako besplatni VPN nema jaku infrastrukturu, što rezultira zagušenjem i smanjenjem brzine. (Ilevičius, 2021.)

Premium VPN košta – svaki dobar VPN poslužitelj košta, ali za uslugu i sigurnost koju pruža svakako se isplati. (Ilevičius, 2021.)

VPN ne štiti od dobrovoljnog prikupljanja podataka - VPN ne štiti od dobrovoljnog davanja podataka. U mnogim od ovih slučajeva korisnik sam daje svoje podatke samo korištenjem usluga nekih stanica poput Facebook-a i Google-a. Slično tome, VPN neće zaštititi od nesigurnog ponašanja na mreži. Korisnik mora koristiti zdrav razum i kada je u pitanju sigurnost. (Ilevičius, 2021.)

Isplatili se onda korištenje VPN-a?

S internetskim prijevarama koje se danas brzo šire i radom na daljinu otvara sve korisnike interneta stalnim internetskim prijetnjama. Prednosti korištenja VPN-a jasno nadmašuju nedostatke. No, kao što je već spomenuto, korisnik mora pažljivo odabrati svog pružatelja VPN usluga i izbjegavati nesigurne besplatne VPN usluge.

8. PRIMJER PRIMJENE VPN-A

Za primjer primjene Virtualne privatne mreže uzet je, Watchguard Mobile VPN with SSL, koji koristi agencija.

U ovom poglavlju je prikaz kako izgleda spajanje od kuće korisnika agencije, te kako se pristupa svim podaci iako korisnik nije spojen na lokalnoj mreži u agenciji.

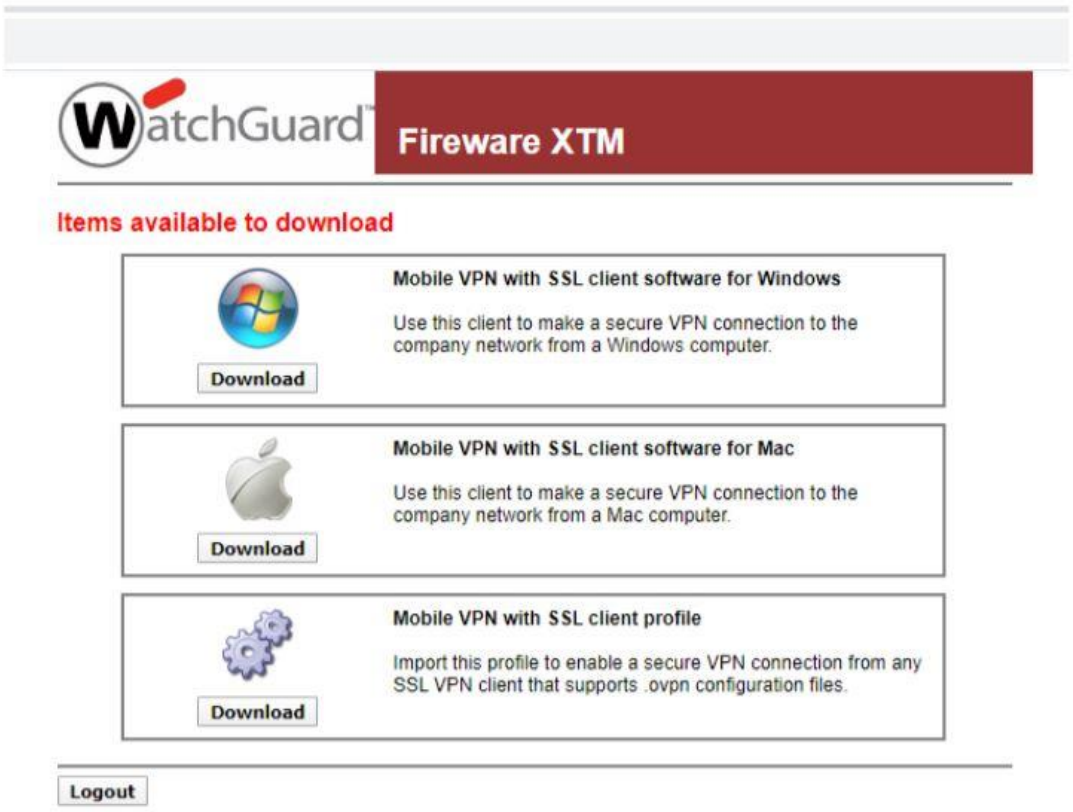
Bitno je za naglasiti da je korisnik registriran u domeni, te da mu je dodijeljen username i password od strane administratora agencije.

Prvi korak je prijava u VPN sustav pomoću web preglednika, te otići na web adresu VPN poslužitelja.

Slika 20. Prikaz SSL VPN portala

Izvor: Obrada autora

Na slici 21. je prikaz WatchGuard SSL VPN portala, na kojem korisnik upisuje korisničko ime, lozinku i domenu kojoj želi pristupiti. Korisničko ime i lozinka je jedinstvena za svakog korisnika i dodijeljena od strane administratora agencije u Active Directory-ju. U padajućem izborniku se bira domena kojoj korisnik pristupa.



Slika 21. Watchguard izbornik za instalaciju VPN-a

Izvor: Obrada autora

Na slici 22. je Watchguard izbornik za instalaciju VPN-a. Watchguard firmware daje opcije za Instalaciju Mobile VPN with SSL client software za Windows-e, za Mac(Apple) i uvoz profila za omogućavanje sigurne VPN povezanosti od bilo kojeg SSL VPN klijenta.

Slika 22. Instalacija Mobile VPN-a

Izvor: Obrada autora

Slika 23. prikazuje Setup za instalaciju Mobile VPN-a sa SSL klijentom. Nakon odrade instalacije korisnik mora dati dopuštenje i instalacije drivera „TAP-Windows Provider V9 network adapter“, proizvođača OpenVPN Technologies, Inc., što se i vidi na slici 24.

Slika 23. Instalacija drivera za VPN

Izvor: Obrada autora

Nakon instalacije drivera, otvara se prozor aplikacije, slika 25., u koji se trebaju upisati sljedeći podaci, kako bi se korisnik povezao na server od agencije, i mogao pristupiti podacima i aplikacijama kojima se agencija koristi.

Slika 24. Aplikacija WatchGuard Mobile VPN with SSL

Izvor: Obrada autora

Ako su podaci uspješno i ispravno upisani, pojavljuje se skočni prozor, kao što se vidi na slici 26., da je korisnik uspješno povezan na VPN i spreman za korištenje svih podataka i aplikacija agencije, kao da je fizički u njoj .

Slika 25. Uspješna povezanost na VPN

Izvor: Obrada autora

9. BUDUĆI RAZVOJ VPN TEHNOLOGIJE

Korištenjem VPN-a na bežičnoj mrežnoj infrastrukturi , podiže se uvelike sigurnost rada. Makar VPN nema direktan utjecaj na autentifikaciju korisnika prilikom spajanja, ona osigurava sigurnost unutar bežične mreže. Zato se može i reći da se VPN tehnologija neće detaljnije promatrati, jer se radi o unutarnjoj sigurnosti, a ne o mehanizmu od neovlaštenog pristupa korištenja bežične mreže.

Skendžić (2014.) tvrdi da je „VPN tehnologija koja omogućava sigurno povezivanje računala u virtualne privatne mreže preko distribuirane ili javne mrežne infrastrukture. Ona podrazumijeva korištenje određenih sigurnosnih i upravljačkih pravila unutar lokalnih mreža. VPN veze mogu se uspostaviti preko različitih komunikacijskih kanala kao što su internet, komunikacijske infrastrukture davatelja internetskih usluga i drugi. Vrlo je bitno kako virtualna privatna mreža preko javne mreže stvara sigurni kanal između dviju krajnjih točaka.“

Osnovna zadaća VPN tehnologije je kreiranje sigurnost kanala za komunikaciju između

privatnih mreža putem javne mreže. Najčešće se koristi kombinacija sklopovskog i programskog pristupa u izradi medija za siguran prijenos podataka. Tijekom komunikacije, podaci iz lokalne mreže prolaze kroz gateway uređaj koji štiti komunikacijski medij. Kada podaci prolaze dolaze u lokalnu mrežu, isti se postupak primjenjuje, te moraju proći kroz gateway uređaj. Time se postiže automatsko šifriranje poslanih podataka između dvije udaljene privatne mreže. Na drugom kraju komunikacijskog kanala se isto tako automatski dešifriraju paketi. (Skendžić, 2014.)

U mrežnom povezivanju; korištenje, implementacija i sigurnost VPN-a se ne razlikuje kod lokalnih bežičnih i žičnih mreža. Razlika je jedino u pristupnom dijelu mreže, dok je sigurnost u potpunosti ista, odnosno ovisi o mrežnoj infrastrukturi. (Skendžić, 2014.)

U budućnosti se mogu očekivati još veća poboljšanja VPN-a, a danas su mane eliminirane korištenjem već spomenutih SSL/TLS enkripcijskih metoda i pojačanim vatrozidom i usmjerivačima kao što je opisano u poglavlju na primjeru Watchguarda u agenciji.

Zaključno se može reći da je najvrjednija stvar koju poduzeće može imati je informacija koju je potrebno zaštiti. Samim time VPN neće nikada izumrijeti, jer svaka organizacija danas želi osigurati svoje podatke i smanjiti troškove i olakšati umrežavanje svojih zaposlenika. Jedino o čemu ovisi daljnji uspjeh VPN-a je kompatibilnost koja nastupa zbog nepostojanja standarda VPN tehnologije među proizvođačima. (Skendžić, 2014.)

Uslijed razvoja i pada cijena mrežne opreme koja se koristi za potrebe Interneta, virtualne privatne mreže se posljednjih godina sve više koriste kao alternativno rješenje. Ističu se svakako i kao najjeftinija metoda.

Prednosti virtualnih privatnih mreža su u:

- fleksibilnosti i skalabilnosti mreže (mogućnost povezivanja novih ili privremenih adresa u kratkom roku);
- umjesto zakupa iznajmljenih linija (ili spajanja korištenjem modema), kod VPN-a se plaćaju (samo) znatno niži troškovi za spajanje preko Interneta;
- manjem trošku za nabavu i održavanje opreme koja se koristi (PC Chip,2016.)

U odnosu na zaista velike prednosti koje se tiču fleksibilnosti i troškova same mreže, virtualne privatne mreže nisu savršene i imaju određene nedostatke, a to su: (Žigman, 2016.)

- pouzdanost - VPN ovisi o kvaliteti usluge davatelja internet usluga koja nije uvijek zadovoljavajuća. Isto tako, ovisi i o načinu primjene VPN veze
- nekompatibilnost opreme različitih proizvođača - neodređeni standardi što dovodi do neispravnog rada protokola kako je predviđeno
- zahtijeva znanje opreme koja se koristi u ostvarivanju potpune zaštite privatne mreže od napada i prijetnji

Svaki bi korisnik osobnog računala morao pratiti razvoj informacijske tehnologije. Mrđen (2006.) tvrdi „kako se one svakodnevno usavršavaju, istodobno je potrebno da se prate i primjenjuju sve moguće sigurnosne komponente umreženih računala i podataka kojima manipulira, tako da se ne bi dogodilo da korisnik nije pripremljen na moguće upade pojedinaca i skupina u sigurnosni sustav programa, a da toga nije bio svjestan ili da nije znao primijeniti najnovija sigurnosna načela u radu s osobnim računalom.“

Reklo bi se da se jasno vide prednosti uporabe VPN mreža, kao što su brzina, fleksibilnost, privatnost i financijske pogodnosti. Posebno je bitna u korištenju korisnika ili poduzeča pri obavljanju poslovanja.

10. ZAKLJUČAK

S internetskim prijevarama koje se brzo množe usred pandemije, rad na daljinu otvara sve korisnike interneta stalnim internetskim prijetnjama i s invazivnim tragačima koji prate svaki korak. VPN tehnologijom se osigurava siguran i brzi prijenos podataka od jednog korisnika do krajnjeg korisnika.

Virtual Private Network je način simulacije privatne mreže putem javne mreže, kao što je Internet. Razlikuju se softverske virtualne privatne mreže, hardverske virtualne privatne mreže i kombinacije softverskih i hardverskih virtualnih privatnih mreža, a one omogućuju sigurnu vezu između „peer“-ova preko javne mreže. Ta sigurna veza se postiže šifriranjem, autentifikacijom, tuneliranjem paketa i vatrozidom.

MPLS VPN je tehnički najbolji, ali i najskuplji način uspostave VPN mreža. Pruža apsolutnu sigurnost i izdvojenost korporacijskog prometa od ostalog prometa javnom mrežom.

Zaključuje se da prednosti korištenja VPN-a jasno nadmašuju nedostatke, no kao što je već spomenuto, korisnik mora pažljivo odabrati svog pružatelja VPN usluga i izbjegavati nesigurne besplatne VPN usluge.

Uspjeh virtualnih privatnih mreža u budućnosti ovisi uglavnom o razvoju tehnologije. Njihova najveća vrijednost krije se u potencijalnom smanjenju troškova poduzeća. Također, dolazi se do zaključka kako VPN iz dana u dan privlači mnoga poduzeća kojima je cilj ojačati svoje umrežavanje te smanjiti troškove u čemu se, uz adekvatno obavljanje zadataka intraneta i ekstraneta, ujedno krije i njegova najveća vrijednost.

11. LITERATURA

Scott, C., Wolfe, P., & Erwin, M., „Virtual Private Network“ , (1999.) Dostupno na: https://books.google.hr/books/about/Virtual_Private_Networks.html?id=OuFQ3t7eF4IC&redir_esc=y

ExpressVPN, „What is a VPN?“, (2022.) Dostupno na: https://www.expressvpn.com/what-is-vpn

Fortinet, „What is a Site-to-Site VPN?“ , (2022.) Dostupno na: https://www.fortinet.com/resources/cyberglossary/what-is-site-to-site-vpn

Mujarić, E., „Virtualna privatna mreža (VPN)“, (n.d.) Dostupno na: http://mreze.layer-x.com/s060000-0.html

Hillstonenet, „Introduction to IPSec VPN“, (2022.) Dostupno na: https://www.hillstonenet.com/support/5.0/en/config_net_ipsec_intro.html

Doraswamy, Harkins, „IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, Second Edition“ , (2003.) Dostupno na: https://www.oreilly.com/library/view/ipsec-the-new/013046189X/

IBM, „Authentication Header, Encapsulating Security Payload“ , (2021.) Dostupno na: https://www.ibm.com/docs/en/i/7.1?topic=protocols-authentication-header, https://www.ibm.com/docs/en/i/7.4?topic=protocols-encapsulating-security-payload

SecurityFOI, „VPN pomoću: L2TP/IPSEC-a“ , (2013.) Dostupno na: https://security.foi.hr/wiki/index.php/VPN_pomo%C4%87u:_L2TP/IPSEC-a.html

TechTarget, „Internet Key Exchange (IKE)“ , (2022.) Dostupno na: https://www.techtarget.com/searchsecurity/definition/Internet-Key-Exchange

Network Encyclopedia, „Point-to-point Tunneling Protocol“, (2022.) Dostupno na: https://networkencyclopedia.com/point-to-point-tunneling-protocol-pptp/

Microsoft Corporation, „Understanding Point-to-Point Tunneling Protocol“, (1997.) Dostupno na: https://wwwdisc.chimica.unipd.it/luigino.feltre/pubblica/unix/winnt_doc/pppt/understanding_pptp.html

Techopedia, „Layer Two Forwarding“, (2022.) Dostupno na: https://www.techopedia.com/definition/25886/layer-two-forwarding-l2f

Network Encyclopedia, „Layer Two Forwarding“, (2022.) Dostupno na: https://networkencyclopedia.com/layer-2-forwarding-l2f/

IBM, „Layer 2 Tunnel Protocol“ , (2021.) Dostupno na: https://www.ibm.com/docs/en/i/7.2?topic=concepts-layer-2-tunnel-protocol

ExpressVPN, „Layer 2 Tunnel Protocol“ , (2016.) Dostupno na: https://www.expressvpn.com/what-is-vpn/protocols/l2tp

GeeksforGeeks, „Secure Socket Layer“, (2022.) Dostupno na: https://www.geeksforgeeks.org/secure-socket-layer-ssl/

Techslang, „What is the Secure Socket Tunneling Protocol (SSTP)?“ , (n.d.) Dostupno na: https://www.techslang.com/definition/what-is-the-secure-socket-tunneling-protocol-sstp/

Jurić, „Različite vrste VPN-ova i kada ih koristiti“ , (2022.) Dostupno na:
https://hr.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/

De Ghein, „MPLS Fundementals“, (2007.) Dostupno na:
https://books.google.hr/books?hl=hr&lr=&id=AUG1DAAAQBAJ&oi=fnd&pg=PT31&dq=mpls&ots=-dVQAMV8WE&sig=CD9pghe_akgmqH5yov3XyDhX2RY&redir_esc=y#v=onepage&q=mpls&f=false

Susitaival, „Adaptive Traffic Engineering in MPLSand OSPF Networks“ , (2004.)
Dostupno na: https://www.netlab.tkk.fi/tutkimus/fit/publ/thesis_Susitaival_04.pdf

Ruela, „MPLS“ , (n.d.) Dostupno na:
https://citeseerx.ist.psu.edu/messages/downloadsexceeded.html

Wallace, „MPLS VPN“ , (2015.) Dostupno na:
https://en.wikipedia.org/wiki/MPLS_VPN#Point-to-point_(pseudowire)

Ilevičius, „VPN pros and cons“ , (2021.) Dostupno na:
https://nordvpn.com/blog/pros-and-cons-of-vpn/

Vasconcellos, „What are the prons and cons of VPNs?“ , (2021.) Dostupno na:
https://www.business.com/vpn/pros-cons/

Skendić, „Sigurnost infrastrukturnog načina rada bežične mreže standarda IEEE“,(2014.) Dostupno na:
https://hrcak.srce.hr/file/190380

PC Chip, „Što je VPN? Za što se koristi?“, (2016.) Dostupno na:
https://pcchip.hr/internet/sto-je-vpn-za-sto-se-koristi/

Žigman, „Spajanje dviju kompanija u VPN“, (2016.) Dostupno na: https://hrcak.srce.hr/file/282527

Mrđen, „Sigurnost umreženih računala pod operativnim sustavom Windows“, (2006.) Dostupno na: https://hrcak.srce.hr/file/11868