Virtualne privatne mreže

Mišković, Alen

Sveučilište Jurja Dobrile u Puli
Fakultet informatike u Puli

ALEN MIŠKOVIĆ

VIRTUALNE PRIVATNE MREŽE

Završni rad

Pula, rujan, 2024.

Sveučilište Jurja Dobrile u Puli
Fakultet informatike u Puli

ALEN MIŠKOVIĆ

VIRTUALNE PRIVATNE MREŽE

Završni rad

JMBAG: 0303095040, redoviti student
Studijski smjer: prijediplomski sveučilišni studij Informatike

Predmet: Računalne mreže
Znanstveno područje: Društvene znanosti
Znanstveno polje: Informacijske i komunikacijske znanosti
Znanstvena grana: Informacijski sustavi i informatologija
Mentor: izv. prof. dr. sc. Siniša Sovilj

Pula, rujan 2024.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani/a ALEN MIŠKOVIĆ, ovime izjavljujem da je ovaj seminarski 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 seminarskog rada nije napisan na nedozvoljen 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/ica

_____

U Puli, 2024.

IZJAVA O KORIŠTENJU AUTORSKOGA DJELA

Ja Alen Mišković, dajem odobrenje Sveučilištu Jurja Dobrile u Puli, nositelju prava korištenja, da moj završni rad pod nazivom " Virtualne privatne mreže" upotrijebi da tako navedeno autorsko djelo objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te preslika u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu sa 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.

Potpis

_____

U Puli,_____

Sadržaj

SAŽETAK

S obzirom na sve veću potrebu rada od kuće i obavljanja posla izvan sjedišta organizacije, potrebno je osigurati podatke i datoteke koji su strogo povjerljivi i od velike važnosti za pojedinca i organizaciju u kojoj radi. Zbog toga je danas, unatoč cijeni, sve raširenija uporaba virtualnih privatnih mreža (VPN). Ona pruža sigurnost i zaštitu podataka od zlonamjernih napada te omogućava korisnicima dostupnost svih podataka organizacije na vrlo jednostavan način za korištenje. U radu su objašnjeni tipovi virtualnih privatnih mreža, povijest nastanka virtualnih privatnih mreža, protokoli i druge performanse VPN-a te njene prednosti i nedostatci.

ABSTRACT

Given the increasing need to work from home and perform work outside the headquarters of the organization, it is necessary to secure data and files that are strictly confidential and of great importance to the individual and the organization in which he works. This is why today, despite the price, the use of virtual private networks (VPN) is more and more widespread. It provides security and protection of data from malicious attacks and enables users to access all the organization's data in a very easy-to-use manner. This final work paper explains the types of virtual private networks, the history of the creation of virtual private networks, protocols and other VPN performances, as well as its advantages and disadvantages.

1. UVOD

Tema ovog rada je Virtualne privatne mreže (VPN).

VPN (*engl. Virtual Private Network)* je proširenje osnovne mrežne infrastrukture, a služi kako bi korisnici mogli sigurno slati podatke putem interneta. To je softver koji pomaže osigurati pristup internetu uspostavljanjem zaštićene i privatne veze.

U početku su VPN koristile samo velike tvrtke i kompanije koje su si to mogle priuštiti, a u kasnijim 2000-tim godinama, broj korisnika se povećao.

VPN se definira kao interkonekcija lokalne mreže koja koristi kriptirane načine međusobne komunikacije, odnosno produžuje privatnu mrežu preko javne mreže, što omogućuje korisnicima slanje i primanje osjetljivih podataka, na način da su njihova računala izravno spojena na isti privatni LAN (lokalnu mrežu) , iako fizički, oni nisu u istoj mreži. [4]

U radu će biti objašnjeni tipovi VPN-a, povijest i razvoj VPN-a, princip rada i arhitektura VPN, tehnologije i sigurnost te protokoli.

Kada su ljudi započeli s radom od kuće, velike organizacije i firme su trebale zaštiti svoje podatke i datoteke od zlonamjernih napada. Stoga su, kako bi omogućili svojim djelatnicima online rad od kuće, počeli sve više ulagati u virtualne privatne mreže.

Ono što je prije bilo dostupno samo velikim organizacijama, postalo je sve traženije među privatnim i poslovnim korisnicima. Zbog istog razloga su i zahtjevi i performanse VPN-a postali sve veći, a konkurencija na tržištu jača.

2. OSNOVE VIRTUALNIH PRIVATNIH MREŽA

U ovom poglavlju bit će definirat će se virtualna privatna mreža, povijest razvoja virtualnih privatnih mreža, osnovni principi, tipovi te arhitektura virtualnih privatnih mreža – u nastavku VPN. [1]

VPN (*engl. Virtual Private Network)* je proširenje osnovne mrežne infrastrukture, a služi kako bi korisnici mogli sigurno slati podatke putem interneta. Omogućuje povezivanje korisnika, poslovnih partnera i kupaca koji su geografski odvojeni. Potrebno je opisati povijest razvoja virtualnih privatnih mreža kako bi se razumjela bit istih. [1]

Slika 1. Prikaz zaštićene mreže između korisnika i Interneta

Izvor: https://infolab.hr/blog/radite-od-kuce-lokalni-cloud-i-vpn/

2.1. Povijest i razvoj VPN-a

Razvoj tehnologije obilježio je 21. stoljeće. Tehnologija se neprestano razvija i koristi u poslovne i privatne svrhe. Broj korisnika interneta se iz dana u dan povećava zahvaljujući napretku u razvoju tehnologije. Korisnicima Internet omogućava brzi protok informacija i podataka, a kako tehnologija napreduje, tako se i količina protoka informacija i podataka povećava jer je korisnika sve više. Korisnicima interneta najvažnije je zadržati mrežne aktivnosti privatnima te osigurati zaštitu podataka. To je moguće ostvariti koristeći razne načine zaštite privatnih podataka. [1]

60-ih godina prošlog stoljeća započeo je razvoj interneta. Internet se, u tom periodu, opisuje kao mogućnost komuniciranja i slanja podataka između korisnika te povezanost cijelog svijeta. Ti podatci se nalaze u spisima američkog znanstvenika J.C.R Licklidera koji je u to vrijeme radio na sveučilištu „Massachusetts Institute of Technology“ (u daljnjem tekstu MIT). [1]

Za razvoj koncepcije interneta zaslužno je troje ljudi i jedna konferencija; Vannevar Bush je jedan od osnivača ARPAneta, matematičar Norbert Wiener zaslužan za pokretanje istraživačkog polja kibernetike te konferencija o umjetnoj inteligenciji (Dartmouth Artificial Intelligence conference) održana 1956. godine na Dartmouth College u Vermontu. [6]

Vannevar Bush je u srpnju 1945. objavio članak “As we may think” u kojem govori o korištenju informatičke tehnologije kojom će se stvoriti “memex” – uređaj na kojem će pojedinac moći pohranjivati svoje podatke iz udobnosti svoga naslonjača. [6]
Matematičar Norbert Wiener je razvio princip kibernetike kombinacijom čovjeka i elektronike koji je 1948. objavio u knjizi “Cybernetics”. [6]

1956. godine na Dartmouth College u Vermontu održana je konferencija koja je okupila veliki broj znanstvenika u raspravi o umjetnoj inteligenciji. Utvrđeno je da se snaga računala udvostručuje u kratkom periodu i da strojevi mogu postati inteligentni poput ljudi, samo je pitanje kada će se to dogoditi. [6]

1960-tih godina grupa stručnjaka krenula je u provedbu eksperimentalnog programa *„Advanced Research Projects Agency Network“* (u daljnjem tekstu ARPANET) čiji je cilj poboljšanje uvjeta za komunikaciju između dva računala. Godine 1969. dogodila se prva uspješna razmjena podataka kada je s jednog računala na drugo poslana poruka „LOGIN“. Taj događaj je bio prekretnica u razvoju interneta. [2]

Kako su to bili samo početci razvoja interneta, nije ni bilo prevelike potrebe za sigurnošću podataka koje su razmjenjivali, ali s vremenom se to promijenilo.
Tim stručnjaka na čelu s s Johnom Ioannidisom okupio se na sveučilištu „Colombia University“ te su počeli istraživati sigurnost prijenosa podataka na internetu. Rad je

rezultirao razvojem protokola „Software IP encryption protocol„ (u daljnjem tekstu: swIPe) što se smatra prvom verzijom virtualne privatne mreže. [3]

U početku su VPN koristile samo velike tvrtke i kompanije koje su si to mogle priuštiti, a u kasnijim 2000-tim godinama, broj korisnika se povećao. Velikim tvrtkama trebao je privatni i sigurni način komunikacije. Bilo je potrebno osigurati poslovne podatke te ih brzo dijeliti s jednog kraja svijeta na drugi u najsigurnijim mogućim uvjetima. VPN mreža ispunila je sve njihove potrebe te je povezala urede smještene na različitim lokacijama u jednu privatnu poslovnu mrežu. [3]

Početkom 2000-tih godina na tržištu su se počele pojavljivati razne tvrtke koje su pružale virtualnu privatnu mrežu te je VPN postao dostupan svakodnevnim korisnicima interneta. [3]

2.2. Osnovni principi virtualnih privatnih mreža

VPN je kratica za virtualnu privatnu mrežu. To je softver koji pomaže osigurati pristup internetu uspostavljanjem zaštićene i privatne veze. VPN omogućava privatno pregledavanje, skrivanje IP adrese i sprječava praćenje putem internetskog poslužitelja. [7]

VPN se definira kao interkonekcija lokalne mreže koja koristi kriptirane načine međusobne komunikacije, odnosno produžuje privatnu mrežu preko javne mreže, što omogućuje korisnicima slanje i primanje osjetljivih podataka, na način da su njihova računala izravno spojena na isti privatni LAN (lokalnu mrežu) , iako fizički, oni nisu u istoj mreži. [4]

VPN je potrebna ako se želi ostati siguran kada se koriste javne Wi-Fi pristupne točke. Također se koristi ako se želi učiniti svoje aktivnosti na internetu sigurnijima, pristupiti većem broju internetskih sadržaja te se pobrinuti da nema praćenja na internetu. [7]

Može se reći kako je VPN jedno vrlo popularno rješenje za problem sigurne komunikacije budući da su alternativna rješenja često neusporedivo skuplja, a uz to je i puno fleksibilniji zbog mobilnosti korisnika. [8] [4]

Stvaranje virtualne mreže predstavlja presložen proces. Ova procedura stvaranja može se razdvojiti na tri dijela i to na:

- konfiguriranje usmjerivača (rutera) (kada je potrebno konfigurirati ruter mreže na koji se korisnik namjerava spojiti, a iza kojeg se nalazi server),
- konfiguriranje poslužitelja odnosno servera - potrebno je konfigurirati server te
- konfiguriranje klijenata, tj. konfiguriranje udaljenih računala s kojih se želimo spajati u ured. [4]

2.3. Tipovi virtualnih privatnih mreža

Dva su načina implementacije VPN servisa:
1. VPN usluga koja se može „kupiti“ i praktički odmah koristiti bez puno tehničkog znanja. Privatni korisnici ga kupuju kao uslugu u oblaku.
2. I servis koji se mora implementirati na privatni ili poslovni poslužitelj i koji traži puno više tehničkog ICT znanja. Drugi tip je programski alat koji se instalira u korporativne mreže i na vlastite poslužitelje ili postoji kao dio hardverske komponente vatrozida ili usmjerivača. [5]

Osim prema načinu implementacije, VPN-ovi se razlikuju i po funkcionalnosti.
To su oni koji se koriste da se pojedinac (klijent) spoji na poslužitelj, odnosno u određenu lokalnu mrežu (engl. Remote access VPN) i oni koji omogućavaju spajanje dviju udaljenih lokalnih mreža, te se time ostvaruje siguran i transparentan rad svih korisnika i poslužitelja obiju mreža. [5]

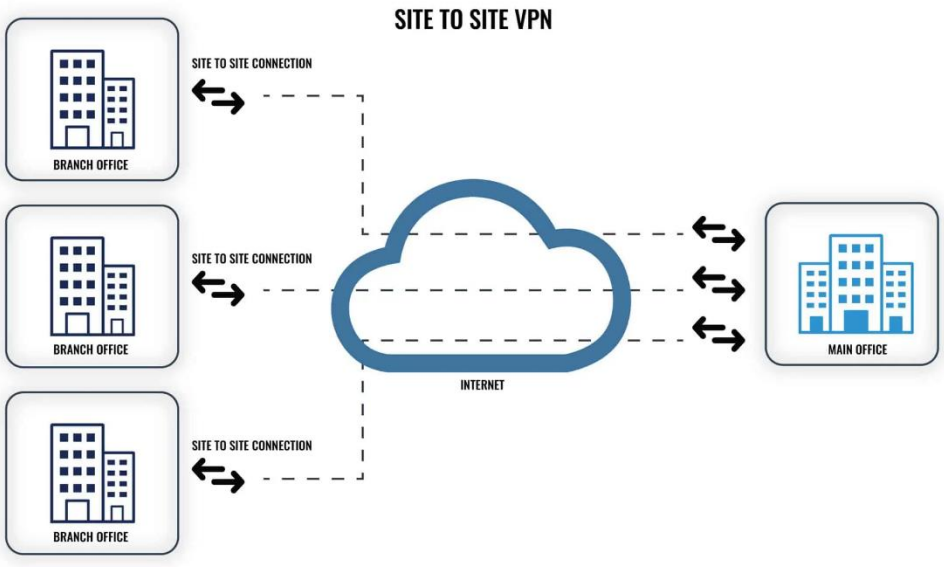
Prvi tip je site-to-site VPN. Kada se spominje site-to-site VPN, misli se na virtualnu privatnu mrežu koja je postavljena između više mreža. To može biti korporativna mreža u kojoj više ureda međusobno surađuje ili mreža poslovnice sa središnjim uredom i više lokacija poslovnica. Site-to-site VPN je 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. [5]

Tvrtke su tradicionalno koristile site-to-site VPN za povezivanje svoje poslovne mreže i udaljenih podružnica. Ovaj pristup funkcionira kada tvrtka ima interni podatkovni centar. Međutim, sada kada je većina tvrtki premjestila svoje podatke u oblak, više nema smisla da korisnici moraju prolaziti kroz interni podatkovni centar da bi došli do oblaka kada umjesto toga mogu ići na oblak izravno. [9]

Zbog toga tvrtke moraju postaviti mrežnu topologiju s pristupom oblaku ili aplikacijama podatkovnog centra. To navodi organizacije da postave mrežne arhitekture koje ne ovise o vraćanju cjelokupnog prometa u sjedište. [9]

Slika 2. Primjer site to site VPN



Izvor: https://www.comparitech.com/blog/vpn-privacy/business-site-to-site-vpn/

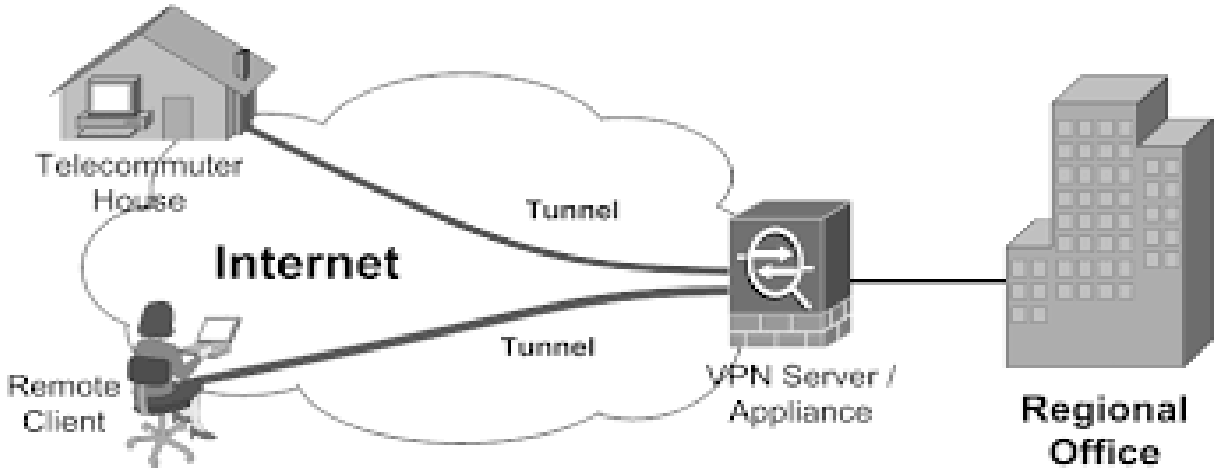
Drugi tip; Remote Access VPN služi za postavljanje privremene veze između dva ili više korisnika i središnje lokacije. Može se reći da je Remote Access VPN koristan alat za poduzeća s djelatnicima koji često rade od kuće ili s puta. Ako djelatnici trebaju pristup privatnim informacijama koje se nalaze na glavnom serveru firme, mogu se povezati na VPN s udaljenim pristupom. Tako svaki zaposlenik dobiva pristup podacima koji su mu potrebni za obavljanje posla gdje god se nalazio i u sigurnom okruženju. [5]

Mnoge organizacije održavaju internu mrežu koja pouzdanim korisnicima omogućuje pristup datotekama, programima, porukama i privatnim resursima. Ako su svi korisnici na istoj lokaciji, jednostavno je upravljati tko se može spojiti na intranet. [10]

„Intranet (engl., od intra- + engl. net: mreža) je privatna računalna mreža neke tvrtke, institucije i sličnoga, zasnovana na internetskim tehnologijama (npr. protokolima TCP/IP). Omogućuje održavanje internih mrežnih stranica, sigurnu i učinkovitu razmjenu podataka među zaposlenicima i dr. Za razliku od interneta, dostupna je samo određenomu krugu korisnika. Poslužitelj za mrežni pristup može biti dostupan samo osobama spojenim na određeni internetski pristupnik.“ [29]

Međutim, djelatnicima koji rade izvan sjedišta firme, potrebno je osigurati siguran pristup informacijama bez obzira na lokaciju gdje se nalaze. VPN s daljinskim pristupom to olakšava. Intranet se može učiniti dostupnim samo putem određenog poslužitelja na koji se povezuje VPN klijentski softver organizacije. [10]
Kako bi se održala sinergija, organizacija može imati sve udaljene zaposlenike koji instaliraju VPN klijent na svoje uređaje, dok također konfiguriraju svoje uredske usmjerivače za slanje i primanje podataka putem istog poslužitelja. Za dodatnu sigurnost, klijent može uspostaviti šifrirani VPN tunel između svog uređaja i poslužitelja. [10]

Slika 3. Primjer Remote Access VPN



Izvor: https://www.researchgate.net/figure/Remote-access-VPN-1_fig2_256843676

2.4. Arhitektura VPN-a

VPN tehnologija razvijena je kako bi se udaljenim korisnicima i podružnicama omogućio pristup korporativnim aplikacijama i resursima. Da bi se osigurala sigurnost, privatna mrežna veza uspostavlja se pomoću šifriranog protokola. [11]

Konceptualna arhitektura IP VPN zasniva se na dva osnovna principa:

1. Implementacija VPN specifičnih funkcija i pridruženih struktura podataka ograničena je na periferne elemente mreže čime se postiže dobra skalabilnost puno servisa. [11]
2. U bilo kojem dijelu mreže moguće je identificirati VPN kontekst kome pripada korisnički promet. [11]

Implementacija funkcija VPN u perifernim ruterima mreže odgovara općem zahtjevu za skalabilnost jer se pretpostavlja da se više instanci VPN servisa izvršava koristeći zajedničku infrastrukturu mreže. Ruteri jezgra čuvaju stanja koja su specifična za VPN kao što su VPN rute u tablicama rutiranja, kontrolne ili signalizacijske sesije za uspostavljanje i održavanje VPN tunela.

U idealnom slučaju samo elementi mreže koji su direktno povezani na VPN korisničke uređaje trebaju čuvati i procesirati informacije o VPN. [11]
VPN kontekst kome pripadaju podaci korisnika može se identificirati u bilo kojem dijelu mreže na jedan od sljedećih načina:

1. Postoje uređaji koji podržavaju samo jednu VPN.
2. Postoje uređaji koji implementiraju eksplicitnu podršku za različite VPN kontekste kao što su virtualne instance prosljeđivanja u PE ruterima. [11]

Mehanizmi VPN su transparentni za sve ostale uređaje što se o tipično postiže tuneliranjem kroz jezgru mreže.
Osnovne komponente arhitekture IP VPN: su

1. formiranje i konfiguriranje krajnjih točaka VPN,
2. detekcija članova VPN,
3. uspostavljanje VPN tunela,
4. distribucija informacije o međusobnoj dostupnosti korisnika VPN. [11]

Kod formiranja i konfiguriranja pružatelj usluga mora formirati krajnje točke VPN svakom od perifernih uređaja koji su direktno povezani sa lokacijama korisnika VPN servisa. Na taj način pružatelj usluga uspostavlja relaciju između konkretne lokacije korisnika i odgovarajuće VPN. [11]

Detekcija članova je proces otkrivanja parova krajnjih točaka. Detekcija članova se vrši na više načina;

- administrator može manualno konfigurirati sve PE rutere,
- postoji odgovarajuća programska podrška u mrežnom operativnom sistemu pomoću koje se daljinski izvršava potrebno konfiguriranje,
- pružatelj usluge formira i održava centralnu bazu podataka s informacijama o članovima VPN kojoj svi mogu sigurno pristupiti,
- vrši se automatska detekcija, odnosno PE ruteri izravno međusobno razmjenjuju informacije o članstvu u VPN
- u slučaju CE-baziranih VPN, proces detekcije izravno se odvija između odgovarajućih CE uređaja. [11]

Uspostavljanje VPN tunela može se vršiti manualnim konfiguriranjem ili signalizacijom. To je vrlo dugotrajan i naporan proces podložan greškama. Zato su, bez obzira na tip, usvojene su metode signalizacije za uspostavu VPN tunela. Signalizacija se ostvaruje između ulaznog i izlaznog na rutera pri čemu signalizacijski protokol omogućuje izlaznom PE ruteru da signalizira ulaznom PE ruteru koji identifikator treba koristiti pri formiranju tunela za pakete koji pripadaju istoj VPN. [11]

Krajnje stanice na lokaciji korisnika moraju imati informacije o tome koje su druge krajnje stanice raspoložive i na koji način su one dostupne. Način distribucije informacija ovisi o tipu VPN (CE-bazirane L3 VPN, PE-bazirane L3 VPN, PE-bazirane L2 VPN). [11]

3. TEHNOLOGIJE I SIGURNOST VPN-A

U ovom poglavlju govorit će se o enkripciji, enkapuslaciji i tuneliranju u VPN.

3.1. Enkripcija

Enkripcija je proces pretvaranja običnog teksta u kodirani format. Enkripcija se koristi za zaštitu osjetljivih informacija. Ona osigurava da samo primatelj i pošiljatelj mogu pročitati podatke koji se šalju putem mreže. U informatici se koristi za zaštitu podataka koji se prenose internetom i pohranjuju u računalnim sustavima. [3]

Podaci se zamjenjuju nizom različitih znakova, tj. kriptiraju se pomoću metoda kao što su RSA, AES, DES i Triple Des. Kriptiranje se može obaviti simetričnom i asimetričnom metodom. Simetrična enkripcija je brža i učinkovitija, a asimetrična je sigurnija. [3]

Kod asimetrične metode koriste se dva ključa. Jedan ključ je javni ključ, a koristi se za šifriranje podataka, dok se drugi ključ, privatni ključ, koristi za dešifriranje podataka. Ova vrsta enkripcije koristi se za sigurnu online komunikaciju i transakcije. [13]

Asimetrična enkripcija je enkripcija u kojoj se koriste dva ključa: javni ključ i privatni ključ. Javni ključ se koristi za šifriranje podataka, a privatni ključ za dešifriranje podataka. Privatni ključ mora biti tajan. Ona je sporija i manje učinkovita od simetrične enkripcije, ali je sigurnija. [13]

Simetrična enkripcija, nazivaju ju još i dijeljena tajna enkripcija, vrsta je enkripcije gdje se isti ključ koristi i za šifriranje i za dešifriranje podataka. Ključ se dijeli između pošiljatelja i primatelja. Ona je brža i učinkovitija, ali je manje sigurna jer se ključ mora dijeliti. [3]

Obje metode pružaju siguran prijenos podataka na internetu. Kako bi se osiguralo da se podatci ne mijenjaju prilikom prijenosa do primatelja, na stvarnu poruku dodaju se jedinstvene poruke, digitalni potpisi ili hash poruke. [3]

Hash poruka je niz 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.“ [3]

Enkripcija je ključna tehnika za osiguravanje prijenosa podataka putem interneta. Pojam "simetrija" odnosi se na ravnotežu između dvije strane, dok se "asimetrija" odnosi na nedostatak ravnoteže između dvije strane. Simetrična enkripcija ima nekoliko prednosti i nedostataka:
- brža je i učinkovitija od asimetrične enkripcije,
- lakše ju je implementirati i koristiti,
- pogodna je za šifriranje velikih količina podataka.
- osjetljiva je na napade ako je tajni ključ ugrožen.
- ne pruža autentifikaciju,
- korisna je metoda šifriranja za određene aplikacije.

Asimetrična enkripcija je sigurnija od simetrične enkripcije jer se privatni ključ nikada ne dijeli, što napadaču otežava posao, a prednosti i nedostatci su:
- sigurnija je od simetrične enkripcije,
- javni ključ se može dijeliti bez ugrožavanja sigurnosti,
- omogućuje digitalnim potpisima provjeru autentičnosti,
- složenija je za implementaciju i upravljanje,
- zahtijeva veću procesorsku snagu. [13]

Digitalne uređaje je lako izgubiti i može se ostati bez velike količine važnih podataka. Lozinke za e-poštu hakeri često pogode, a u računalne poslužitelje se može provaliti, Wi-Fi mreže je moguće prisluškivati, a lakovjerne korisnike zavarati phishingom. [12]

Kad se podatci enkriptiraju, samo osobe koje imaju odgovarajuće dekripcijske ključeve mogu ih pročitati. Enkripcija je zadnja crta internetske obrane. [12]

Mogu se koristiti virtualne privatne mreže (Virtual Private Network, VPN), servise za stolna računala i mobilne uređaje koji enkriptiraju sav promet i preusmjeravaju ga preko svojih računalnih poslužitelja kako bi ga učinili nedostupnim drugima. [12]

3.2. Enkapuslacija

Enkapsulacija se brine o skrivanju paketa koji se šalju putem mreže. Obično se vrši prilaganjem samo novog zaglavlja ili novog zaglavlja i podnožja. Princip rada je takav da svaki sloj u protokolu enkapsulira podatke iz viših slojeva tako što im dodaje novo zaglavlje. Na taj način se postiže siguran prijenos osjetljivih podataka. [12]
Cilj je osigurati da podaci stignu od primatelja do pošiljatelja bez neželjenih posljedica. U slučaju da se ti paketi uspiju pronaći, enkripcija će se pobrinuti da podaci ne budu čitljivi onome tko nema potreban ključ da ih dešifrira. [12]

Enkapsulacija je mehanizam koji omogućuje tuneliranje jer je tuneliranje propuštanje paketa kroz mrežu koja ne podržava svoj protokol, a to se radi enkapsulacijom u protokol koji ta mreža podržava. [14]

Kod VPN-a su uključena tri protokola:

1. protokol putnika,
2. protokol enkapsulacije,
3. protokol prijevoznika/isporuke/prijevoza. [14]

Primjerice, IPv6 paketi ne mogu se slati preko IPv4 mreže jer nisu kompatibilni. IPv4 mreže ne mogu usmjeravati IPv6 pakete. Zbog toga se koristi protokol enkapsulacije kao što je GRE. Stavlja se IPv6 paket u GRE paket, a njega u IPv4 paket te se šalje preko IPv4 mreže. Na taj način je uspješno odrađeno tuneliranje kroz IPv4 mrežu. [14]

3.3. Tuneliranje

VPN (Virtual Private Network) osigurava razmjenu podataka preko Interneta ili bilo koje druge javne mreže koristeći tuneliranje. [14]

Za stvaranje tunela potrebno je:

- Protokol operatera što se odnosi na mrežni transportni protokol koji podržava tranzitna mreža. [14]
- Protokol enkapsulacije što se odnosi na protokol koji se koristi za enkapsulaciju sadržaja paketa podataka. GRE (Generic Routing Encapsulation), PPTP (Point to Point Tunneling Protocol), L2F (Layer 2 Forwarding Protocol) i L2TP (Layer Two Tunneling Protocol) su primeri protokola za enkapsulaciju. [14]
- Protokol putnika što se odnosi na protokol koji koriste mreže koje su povezane tunelom. IP (Internet Protocol) i IPX (Internetnetwork Packet Exchange) su primjeri putničkih protokola. [14]

Kao što je objašnjeno u prethodnim poglavljima, VPN veza može biti Site-to-Site između dvije mreže ili Remote Access VPN veza između udaljenog klijenta i VPN servera. [16]

Vrste metoda tuneliranja su:

1. End-to-End tunneling koji povezuje osobno računalo udaljenog korisnika i VPN server. Koristi se u Remote Access VPN vezi. Softver VPN klijenta enkapsulira pakete podataka prije nego što ih pošalje preko tunela do VPN servera. VPN server dekapsulira podatke pre nego što ih proslijedi na korporativni LAN. [16]

2. Node-to-Node tunneling koji povezuje gateway uređaje koji se nalaze na krajevima dvije privatne mreže. Koristi se u Site-to-Site VPN vezi. Gateway uređaj može biti ruter ili neki sličan uređaj koji deluje kao VPN server. [16]

Neki od protokola koji se koriste za tuneliranje su: IP in IP, GRE, OpenVPN, SSTP, IPSec, L2TPIP in IP.

Tuneliranje je najvažnija komponenta virtualnih privatnih mreža i predstavlja prijenos paketa podataka namijenjenih privatnoj mreži preko javne mreže. Ruteri javne mreže ne prepoznaju prijenos paketa koji pripadaju privatnoj mreži i VPN pakete tretiraju kao dio normalnog prometa. [16]

Tuneliranje je metoda pri kojoj, umjesto da se šalju originalni paketi, oni su učahureni dodatnim zaglavljem. Dodatno zaglavlje sadrži informacije potrebne za usmjeravanje paketa kroz mrežu. [16]

Tunel predstavlja logičnu putanju paketa i uvodi se kao takav pojam jer su podaci koji putuju tunelom razumljivi samo onima koji se nalaze na njegovom izvorištu i odredištu. [16]

Cijeli proces enkapsulacije, transporta i deenkapsulacije paketa naziva se tuneliranje. [16]

4. VPN PROTOKOLI

U ovom poglavlju bit će opisani protokoli koje koriste virtualne privatne mreže pomoću kojih postavljaju tunele kako bi informacije sigurno putovale u mreži od uređaja do uređaja. U nastavku su opisani: IPSEC, PPTP, L2F, L2TP, SSL i TLS protokoli.

4.1. IPSEC protokol

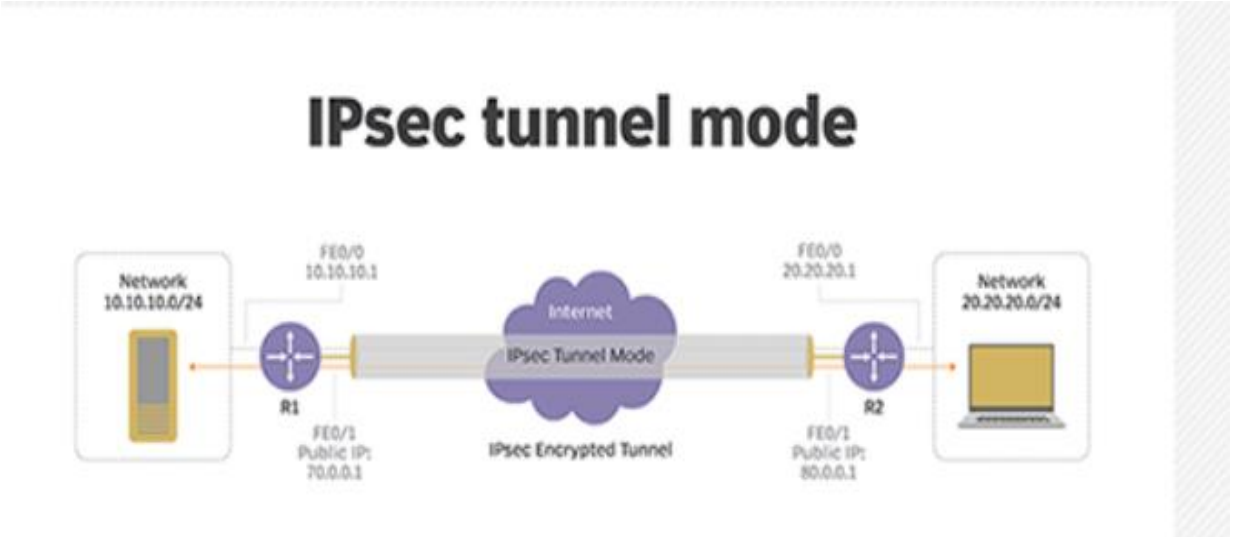
Internet Protocol Security, IPsec, je skup protokola koji obuhvaćaju mehanizme za zaštitu prometa na razini trećeg sloja OSI mrežnog modela.

IPsec služi za postavljanje VPN -a, a radi na principu šifriranja IP paketa, zajedno s autentifikacijom izvora odakle paketi dolaze. [17]

IPsec je skup protokola AH (Authentication Header) , ESP(Encapsulating Security Payload) i IKE (Internet Key Exchange). Uključuje sljedeće korake:

- Razmjena ključeva; ključevi (nizovi znakova za šifriranje) su potrebni za šifriranje. IPsec postavlja ključeve s razmjenom istih između povezanih uređaja, tako da svaki uređaj može dešifrirati poruke drugog uređaja (Slika 4.). [17]

Slika 4. IPsec tuneliranje



Izvor: https://www.techtarget.com/searchsecurity/definition/IPsec-Internet-Protocol-Security

„Svi podaci koji se šalju putem mreže razlažu se na manje dijelove koji se zovu paketi. Paketi sadrže korisni teret ili stvarne podatke koji se šalju, te zaglavlja ili podatke o tim podacima tako da računala koja primaju pakete znaju što s njima učiniti.“ [17]

- Autentifikacija; IPsec omogućuje provjeru autentičnosti za svaki paket (poput žiga). Na taj način osigurava pouzdanost izvora i sprječava djelovanje napadača. [17]

- Šifriranje; IPsec šifrira korisni teret unutar svakog paketa i IP zaglavlja svakog paketa. Tako se čuvaju podatci i ostaju privatni. „Šifrirani IPsec paketi putuju preko jedne ili više mreža do odredišta pomoću transportnog protokola. U ovoj se fazi IPsec promet razlikuje od običnog IP prometa po tome što najčešće koristi UDP (User Datagram Protocol) kao svoj transportni protokol, a ne TCP (Transmission Control Protocol).“ [17]

- Na drugom kraju komunikacije paketi se dešifriraju, a aplikacije (npr. Preglednik) mogu koristiti isporučene podatke. [17]

Kroz rad IPSec koristi sljedeće protokole i standarde: - Diffie-Hellman metodu za razmjenu ključeva, DES ili 3DES standard za šifriranje podataka te HMAC za kombinirano orijentiranu autentifikaciju koda. [17]

4.2. PPTP protokol

PPTP, Point-to-Point Tunneling Protocol, jedan je od najstarijih VPN protokola koji se još uvijek koristi, a postoji od Windowsa 95 i standardan je u svim verzijama Windowsa. Razvio ga je Microsoft za enkapsulaciju drugog protokola nazvanog PPP (Point-to-Point Protocol). [18]

PPTP je najlakši za postavljanje i računalno najbrži. Iz tog je razloga koristan za aplikacije u kojima je brzina najvažnija te na starijim, sporijim uređajima.

Nažalost, PPTP je podložan ozbiljnim sigurnosnim propustima. Njegovi temeljni protokoli za provjeru autentičnosti su nesigurni i opetovano su provaljivani. Iz tog razloga, PPTP se ne preporučuje osim kada je sigurnost apsolutno nebitna. [18]

4.3. L2F protokol

Layer 2 Forwarding (L2F) je tehnologija koja tunelira pakete sloja podatkovne veze u protokolima kao što su Point-to-Point Protocol (PPP) ili Serial Line Internet Protocol (SLIP). [21]

L2F se može koristiti s mogućnostima provjere autentičnosti korisnika putem usluge daljinskog biranja korisnika (RADIUS), dinamičke dodjele adresa i kvalitete usluge (QoS). [21]

Može raditi izravno u drugim mrežnim kontekstima kao što su Frame Relay ili ATM jer pristup tuneliranja nije povezan s IP (Internet Protocol) mrežom. Radi tako da uspostavlja vezu između dial-up klijenta i mrežnog pristupnog poslužitelja (NAS) koji prima poziv kada koristi L2F. [21]

„U L2F, jedina svrha NAS-a je projicirati ili proslijediti PPP okvire od klijenta do udaljenog čvora. U žargonu Cisco mreže ovaj se udaljeni čvor naziva kućni pristupnik.“ [21]

Za udaljenu autentifikaciju korisnika, L2F VPN koristi PPP protokol i druge sustave autentifikacije kao što su TACACS (Terminal Access Controller Access Control System) i RADIUS (Remote Authentication Dial-In User Service). [21]

„Mehanizam provjere autentičnosti za dva korisnika koristi se između SP-a i određenog gatewaya korporativne tvrtke prije izgradnje tunela između lokalne i udaljene mreže.“ [21]

Password Authentication Protocol (PAP) se događa kada se uspostavi veza između poslužitelja i klijenta, klijent isporučuje paket koji sadrži korisničko ime i lozinku korisnika. Korisnik je prijavljen kada je zahtjev za povezivanje autentificiran..

Challenge Handshake Authentication Protocol (CHAP) je mehanizam provjere autentičnosti gdje klijent redovito šalje zahtjev za provjeru autentičnosti poslužitelju s paketom provjere autentičnosti. Redovito se prenose između poslužitelja i klijenta kako bi se provjerio obrazac korisnika/lozinke za autentifikaciju na oba kraja za uspostavu veze. [21]

Radi očuvanja privatnosti, L2F ne pruža enkripciju i umjesto toga se oslanja na protokol koji se tunelira. [21]

4.4. L2TP protokol

L2TP ili Layer 2 Tunneling Protocol spaja najbolje značajke dvaju drugih protokola za tuneliranje; PPTP (Point-to-Point Tunneling Protocol) i L2F (Layer 2 Forwarding Protocol) te se koristi za podršku virtualnim privatnim mrežama (VPN-ovi). [19]

Ne pruža snažnu autentifikaciju pa se često implementira zajedno s IPSec tunneling protokolom kako bi se osigurala veza. [19]

L2TP VPN protokol smatra se najsigurnijim jer sprječava promjenu podataka tijekom kretanja između pošiljatelja i primatelja te šifrira proces autentifikacije i na taj način otežava nekome pristup. [19]

Može pružiti širokopojasni pristup od 100 Mbps ili mu se približiti u većini slučajeva. L2TP je široko podržan na raznim ciljnim platformama, uključujući mobilne uređaje. Budući da L2TP ne pruža nikakve mehanizme provjere autentičnosti ili enkripcije, obično se uparuje s IPSecom kako bi se osigurala enkripcija korisničkih i kontrolnih paketa unutar L2TP tunela. [19]

„L2TP/IPsec dvaput enkapsulira podatke, što može usporiti vezu. Međutim, protokol to nadoknađuje pružajući proces enkripcije/dešifriranja u kernelu i dopuštajući višenitnost koja nije moguća u OpenVPN protokolu. Ova činjenica, teoretski, čini L2TP zajedno s IPsec bržim od OpenVPN-a i sigurnijim od PPTP-a.“ [19]

Ovaj protokol tuneliranja šifrira čak i sam proces autentifikacije, što otežava trećim stranama da uđu i vide prijenos podataka. [19]

4.5. SSL VPN (Secure Sockets Layer) / TLS (Transport Layer Security)

SSL VPN je vrsta virtualne privatne mreže (VPN) koja koristi protokol SSL ili TLS u standardnim web preglednicima za pružanje sigurnih usluga. [20]

SSL VPN veza koristi end-to-end enkripciju (E2EE) za zaštitu podataka koji se prenose između krajnje točke klijentskog softvera uređaja i SSL VPN poslužitelja putem kojeg se klijent sigurno povezuje s internetom. [20]

Koriste ga poduzeća za siguran pristup organizacijskim resursima. [20]

SSL VPN-ovi su važni jer se mogu jednostavno implementirati omogućujući višu razinu kompatibilnosti s klijentskim platformama i konfiguracijama za udaljene mreže i vatrozide. [20]

Budući da je Radna grupa za internetsko inženjerstvo (IETF) zamijenila SSL sa TLS-om (Transport Layer Security), SSL VPN-ovi koji rade na modernim preglednicima sada koriste TLS za šifriranje i provjeru autentičnosti podataka koji se prenose preko VPN-a. [20]

„SSL VPN-ovi omogućuju korisnicima daljinski pristup ograničenim mrežnim resursima putem sigurnog i autentificiranog puta tako što šifriraju sav mrežni promet i čine da izgleda kao da je korisnik na lokalnoj mreži, bez obzira na geografsku lokaciju.“ [20]

Primarni razlog za korištenje SSL VPN proizvoda je sprječavanje neovlaštenih strana da prisluškuju mrežnu komunikaciju. SSL VPN sustavi nude sigurne i fleksibilne opcije zaposlenicima poduzeća za daljinsko povezivanje s mrežama privatnih poduzeća.

Za implementaciju SSL VPN-a, organizacije mogu kupiti samostalni uređaj koji funkcionira isključivo kao SSL VPN poslužitelj. [20]

SSL VPN-ovi oslanjaju se na TLS protokol, koji je zamijenio stariji SSL protokol, kako bi omogućili autentificiranim korisnicima uspostavljanje sigurnih veza s internim HTTP i HTTPS uslugama putem standardnih web preglednika ili aplikacija. [20]

Postoje dvije vrste SSL VPN-ova: VPN portal i VPN tunel.
SSL portal VPN omogućuje jednu po jednu SSL VPN vezu s udaljenim web stranicama. Pristup se ostvaruje putem web stranice koja djeluje kao portal za druge usluge. [20]

SSL tunel VPN omogućuje korisnicima siguran pristup višestrukim mrežnim uslugama putem standardnih web preglednika. VPN tunel je krug uspostavljen između udaljenog korisnika i VPN poslužitelja. [20]

Jedna od prednosti SSL VPN-a je ta što koristi TLS tehnologiju implementiranu u modernim web preglednicima, tako da nema potrebe za instaliranjem posebnog klijentskog softvera. Zahtijevaju i manje administrativnih troškova i tehničke podrške od tradicionalnih VPN klijenata. [20]
Korisnici na SSL VPN vezama mogu biti ograničeni samo na one aplikacije za koje su im odobreni, a ne na cijelu mrežu. [20]

Jedna potencijalna opasnost javlja se kada korisnici pokušaju postaviti SSL VPN vezu koristeći javno dostupno računalo. U tim slučajevima korisnik može biti ranjiv na napade koji uključuju keyloggere instalirane na nepouzdanom sustavu. [20]

Prednost SSL-a je što različiti dobavljači IPsec VPN-a mogu imati različite zahtjeve za implementacijom i konfiguracijom, a SSL VPN-ovi mogu se implementirati s gotovo svim modernim web preglednicima. [20]

5. PREDNOSTI I NEDOSTATCI VIRTUALNIH PRIVATNIH MREŽA

U ovom poglavlju govorit će se o prednostima i nedostatcima VPN-a.

5.1. Prednosti VPN-a

Internet je prepun opasnosti koje prijete privatnosti i sigurnosti korisnika. Određenim postupcima može se ugroziti sigurnost podataka na internetu te se mogu dogoditi neželjene posljedice koje je potrebno na vrijeme spriječiti kako ne bi ugrozile privatnost korisnika. Pojedine mreže blokiraju određene web stranice čime značajno ograničavaju online slobodu korisnika. [22]

VPN je ulaganje koje se isplati za online privatnost i sigurnost. Štiti korisnike od zlonamjernih napada te krađe podataka. Također, kriptira vezu kako ni Google, Facebook, a ni druge društvene mreže i preglednici ne bi mogli pratiti internetsku aktivnost korisnika. [22]

VPN kriptira vezu, tj. šifrira podatke zbog čega korisnikova aktivnost postaje nečitljiva vanjskim akterima. Nitko ne može vidjeti aktivnost pregledavanja jer izgleda kao slučajan niz brojeva. [22]

Većina VPN-ova koristi AES-256 bitnu enkripciju. 256 je najdulji ključ enkripcije, a što je dulji ključ, to je više vremena potrebno za dekriptiranje. Koriste ju vodeće svjetske sigurnosne agencije i vlade. [22]

VPN skriva stvarnu IP adresu tako da ju mijenja drugom te ju skriva bez obzira na korisnikovu lokaciju. [22]

Neki VPN-ovi mogu blokirati oglase i sprječavati zlonamjerne stranice da zaraze uređaj zlonamjernim softverom. Omogućavaju uživanje u web stranicama kao što je YouTube bez oglasa i dodatno štite od hakera. [22]

Dodatna je prednost što mogu zaobići regionalne geoblokade na stranicama s geografskim ograničenjima (HBO, Netflix, Disney, HULU…). [22]

VPN-ovi mogu omogućiti pristup međunarodnim poslužiteljima za igranje igara. [22]

5.2. Nedostatci VPN-a

VPN ima većinom prednosti, ali kada gledamo negativne strane, nisu zanemarive i treba ih preispitati. Ne podržavaju ih svi uređaji, nekada usporava promet, a besplatne verzije su često ograničene. [23]

Jedan veliki nedostatak korištenja VPN-a jest taj što usporava brzinu interneta jer VPN uvodi dodatni sloj između korisnika i šireg interneta. Zbog toga će brzina biti sporija ako se sadržaj pregledava putem VPN-a. [24]

VPN može utjecati na performanse streaminga. [24]

Drugi veliki nedostatak je zabluda dqa VPN pruža potpunu zaštitu od prijetnji na mreži. VPN ne može zaštititi od uobičajenih mrežnih prijetnji zlonamjernim softverom, prijevarama i krađom identiteta ako korisnik ne promijeni svoje navike ponašanja/aktivnosti na internetu. [24]

6. IMPLEMENTACIJA VIRTUALNIH PRIVATNIH MREŽA U ORGANIZACIJAMA

U većini neprofitnih organizacija mnogi ljudi rade od kuće stvarajući, uređujući i ažurirajući podatke. Zato se moraju povezati na svoju radnu mrežu kako bi pristupili datotekama i podatcima. [25]

Najbolje rješenje koje će organizacijama omogućiti daljinski pristup datotekama je postavljanje virtualne privatne mreže (VPN). U ovom poglavlju će se govoriti o implementaciji VPN u organizacije te zahtjevima i izazovima koje VPN moraju rješavati. [25]

6.1. Postupak postavljanja VPN za pristup datotekama i podatcima organizacije

VPN softver na računalu uspostavlja siguran tunel od točke do točke preko interneta s uredom za udaljeni pristup datotekama. Kako biste se napravila virtualna privatna mreža, potreban je usmjerivač koji ima omogućen VPN. [25]

5 koraka za postavljanje VPN-a:

1. Nabaviti usmjerivač koji odgovara svim potrebama te provjeriti ispunjava li hardverski usmjerivač sljedeće zahtjeve:
    - Usmjerivač mora imati žičanu i bežičnu vezu.
    - Mora imati ugrađenu funkciju virtualne privatne mreže.
    - Mora podržavati do 10 radnih stanica. [25]

2. Koristiti Vodič čarobnjaka za brzi početak za postavljanje.

Ovaj vodič vodi kroz cijeli proces uključivanja kabela, postavljanja bežične mreže i povezivanja na Internet. [25]

3. Odabrati sigurnosne postavke.

Važan dio procesa postavljanja je osigurati najvišu razinu sigurnosti. „Većina organizacija pogrešno prihvaća zadanu lozinku 'lako za pamćenje' koja dolazi s

usmjerivačem.“ Potrebno je odabrati tešku i jaku lozinku kako bi se spriječilo zlonamjernike u pokušajima krađe podataka. [25]

4. Omogućiti korisnicima korake za VPN funkcionalnost:

- Slijediti upute u korisničkom priručniku usmjerivača za omogućavanje VPN.
- U postavkama softvera rutera omogućiti daljinsko upravljanje.
- Stvoriti korisničke račune za svakog korisnika koji želi pristup VPN-u.
- Zatražiti od svakog korisnika da dobije i instalira VPN softver na svoje klijentsko računalo. [25]

5. Povezati se s kućnog računala na ured pomoću VPN-a. [25]

6.2. Skalabilnost i upravljanje

VPN mora zadovoljavati sljedeće zahtjeve:

- autentikaciju korisnika,
- upravljanje adresama,
- šifriranje,
- upravljanje ključevima,
- podršku za razne protokole. [26]

Postoji nekoliko elemenata koje VPN mora sadržati:

- skalabilnost,
- sigurnost,
- VPN servisi,
- uređaji,
- upravljanje. [26]

„Skalabilnost podrazumijeva da svaki element mora biti izveden tako da može podržati VPN platforme od malih uredskih konfiguracija, pa do velikih korporacijskih implementacija.“ Ključna je mogućnost prilagodbe VPN-a prema potrebama propusnosti i načinu veze. [26]

Autentikacija korisnika i kontrola pristupa nužne su za dodjelu odgovarajućih ovlasti i prava pristupa mrežnim resursima. [26]
Uloga VPN servisa je upravljanje propusnošću komunikacijskog kanala, te implementacija funkcija koje osiguravaju kvalitetu usluge. Važni dijelovi VPN tehnologije jesu protokoli koji osiguravaju usmjerivačke servise poput EIGRP (engl. Enhanced Interior Gateway Router Protocol), OSPF (engl. Open Shortest Path First), te BGP (engl. Border Gateway Protocol). [26]
„Upravljanje propusnosti kanala, definicija i primjena sigurnosnih pravila, te nadgledanje mrežnog prometa također nužan element svakog VPN rješenja.“ [26]

IP brojevi mogu biti statični i dinamički. Statička IP adresa se nikada ne mijenja. To olakšava web stranici da se odnosi na određeni ured.
Međutim, većina ureda ima dinamičke IP adrese. To znači da se svaki put kada se resetira i dodjeljuje nova IP adresa. To je problem jer je IP adresa nepoznata i web stranica ju ne zna. [25]

Jedno od mogućih rješenja je natjerati ISP-a da uredu dodijeli statičku IP adresu. Loša strana ovog rješenja je da ISP-ovi naplaćuju statičke IP adrese. [25]

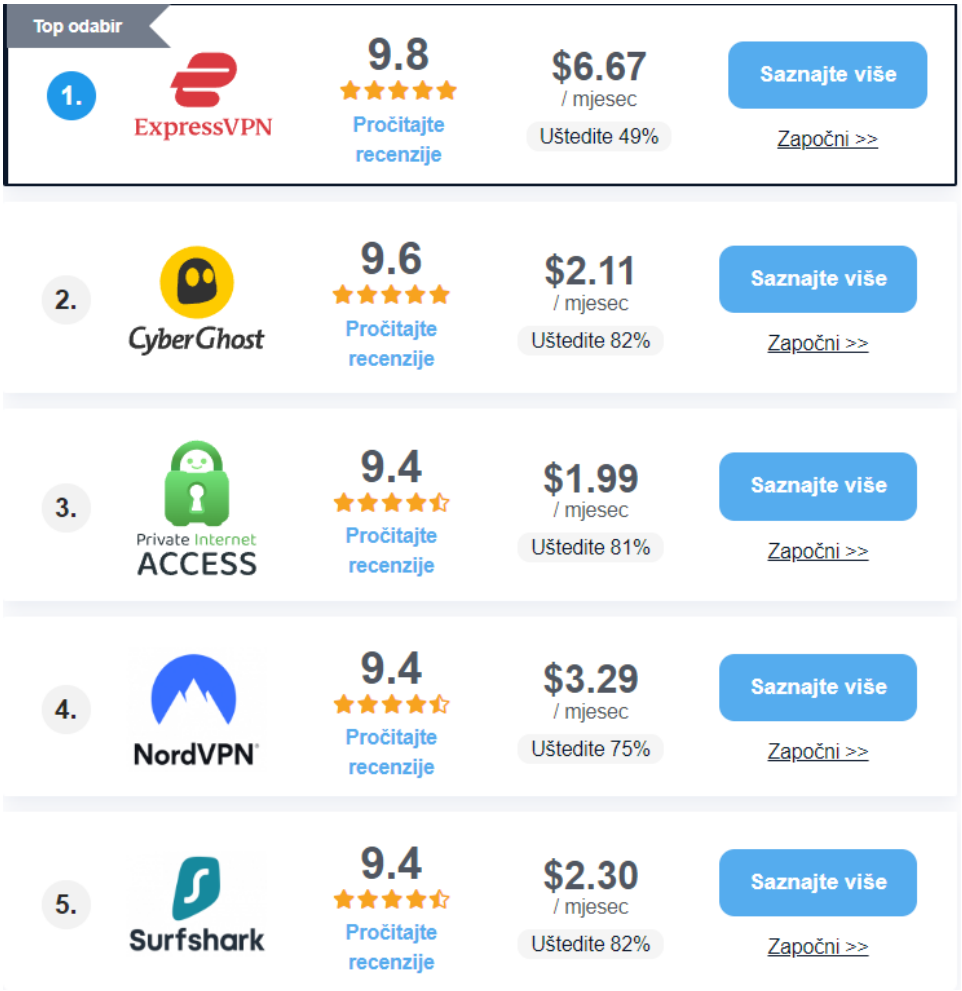
Ako se ne može dobiti statička IP adresu po prihvatljivoj cijeni, drugi bi pristup bio registracija naziva domene i dinamičko ažuriranje poslužitelja naziva domene (DNS) za taj naziv domene kako bi upućivao na određeni ured.
Može se, umjesto registracije vlastitog imena, koristiti besplatno ime koje pruža Dynamic DNS provider. [25]

7. IZAZOVI BUDUĆNOSTI VIRTUALNIH PRIVATNIH MREŽA

VPN-ovi su složeni i velik je izbor na tržištu svih pružatelja usluga koji tvrde da je njihov VPN najbolji. Zbog toga je korisnicima često teško odabrati koji VPN zadovoljava sve njihove potrebe. Izbor se svodi na usporedbu cijene i kvalitete, te kompatibilnosti uređaja. [27]

OpenVPN je trenutno vodeći protokol u VPN industriji. [27]

Slika 5. Prikaz najboljih VPN u Republici Hrvatskoj u 2023. godini.



Izvor: https://hr.wizcase.com/blog/potpuni-vpn-vodic-za-pocetnike/

U ovom poglavlju bit će objašnjeno s kojim se novim sigurnosnim prijetnjama susreću VPN-ovi te kako ih integrirati s drugim tehnologijama.

7.1. Nove sigurnosne prijetnje

Sve je više rada od kuće pa su se s tim načinom rada pojavile i nove prijetnje s kojima se VPN susreću i kojima moraju uspješno odolijevati. [28]

„Phishingom napadač uz pomoć lažiranog maila pokušava navući korisnika na otkrivanje osjetljivih podataka.“ Korisnik dobije mail koji izgleda zanimljivo s ciljem da se klikne na poveznicu ili odgovori na mail. Otvaranje privitka zarazi korisnikovo računalo. [28]

Nedostatak kontrole pristupa očituje se nedostatkom kontrole koga i kako se pušta da se spaja na infrastrukturu organizacije. Rad od kuće znači povećanje udaljenog spajanja na infrastrukturu. [28]

Utvrđeno je kako se u 80% napada koristi probijena lozinka korisnika. Dokazano je da većina korisnika misli da je njihova lozinka jača nego što uistinu je. [28]

Bez korištenja dvofaktorske autentikacije organizacije su ranjive na ovaj napad tj. gubitak ili krađu korisničke lozinke. [28]

Pod naprednom kontrolom smatra se to da se kod korisnika, uz lozinku, provjerava i sam uređaj s kojega se vrši spajanje. Mnogi korisnici spajaju se s privatnih mobitela ili drugoga računala. Kako ti uređaji nisu pod kontrolom organizacije, korisnici ih često koriste za preuzimanje različitih multimedijalnih sadržaja. [28]

I dalje u svijetu nedostaje cyber podrške ili stručnih osoba koje će se baviti sigurnošću na mreži. [28]

8. ZAKLJUČAK

Zaključno, može se reći da su virtualne privatne mreže postale traženije, ali i dostupnije nego ikada.

Zbog sve češćih zlonamjernih napada i sve više softvera koji mogu pristupiti podatcima korisnika i zloupotrijebiti ih, privatni korisnici, kao i organizacije, se sve više odlučuju na korištenje virtualnih privatnih mreža.

Zahtjevi korisnika su sve složeniji pa i performanse moraju biti u skladu sa današnjim zahtjevima. Brzina rada se ne smije gubiti na račun sigurnosti podataka koji su dostupni online. Sigurnost na internetu i prilikom korištenja virtualnih privatnih mreža je ključna za organizacije, firme i privatne osobe.

S obzirom na sve prednosti korištenja virtualnih privatnih mreža, moguće je zanemariti nedostatke koje donose. Potrebno je provoditi više kontrole pri upravljanju informacijama, lozinkama i korisničkim podatcima.

Kao što je rečeno u radu, problem nastaje i pri nedostatku stručnog osoblja i podrške koja će korisnike uputiti u rad virtualnih privatnih mreža.

Mnoge organizacije održavaju internu mrežu koja pouzdanim korisnicima omogućuje pristup datotekama, programima, porukama i privatnim resursima. Ako su svi korisnici na istoj lokaciji, jednostavno je upravljati tko se može spojiti na intranet.

Može se reći da su virtualne privatne mreže jedno popularno rješenje koje korisnicima omogućuje sigurnu razmjenu i pristup poslovnim i privatnim podatcima uz minimalne probleme i poteškoće pri pristupanju istima.

Zbog sve veće popularnosti i konkurencije, i cjenovno su postale dostupnije svim korisnicima, a ne samo velikim firmama i organizacijama što uvelike pridonosi razvoju i kvaliteti VPN-a.

LITERATURA

1. Brief History of the Internet (1997). https://www.internetsociety.org/internet/history-internet/brief-history-internet/#f3 [pristupljeno 26. lipnja 2023].

2. “Who invented the Internet?“ (2019). https://www.history.com/news/who-invented-the-internet [pristupljeno 27. lipnja 2023].

3. Klopoton, L. Završni rad. Varaždin: Sveučilište u Zagrebu, Fakultet organizacije i informatike Varaždin. https://zir.nsk.hr/islandora/object/foi:6848/datastream/PDF/view [pristupljeno 27. lipnja 2023].

4. Posavac, S. Završni rad. Zagreb: Sveučilište u Zagrebu, Fakultet prometnih znanosti. https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A1605/datastream/PDF/view [pristupljeno 27. lipnja 2023].

5. Halar, Lj. Završni rad. Pula: Sveučilište Jurja Dobrile u Puli, Fakultet informatike. https://zir.nsk.hr/islandora/object/unipu%3A7426/datastream/PDF/view [pristupljeno 27.lipnja 2023].

6. Hajdarović, M. (2006). Hrvatski povijesni portal, Povijesni razvoj interneta https://povijest.net/2018/?p=2374 [pristupljeno 28. lipnja 2023].

7. Surfshark, https://surfshark.com/vpn-for-business [pristupljeno 28. lipnja 2023].

8. Carnet (2019). VPN usluge – što su, kako funkcioniraju i kada su korisne, CERT.hr-PUBDOC-2019-6-382 https://www.cert.hr/wp-content/uploads/2019/07/VPN_usluge.pdf [pristupljeno 29. lipnja 2023].

9. What Is a Site- to -Site VPN?, https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn [pristupljeno 29. lipnja 2023].

10. What is a remote access VPN and how does it work? (2022). https://nordvpn.com/blog/remote-access-vpn [pristupljeno 30. lipnja 2023].

11. Stojanović, M, Aćimović- Raspović, V. (2012). Savremene IP mreže: *Arhitekture, tehnologije i protokoli.* Beograd: Akademska misao

12. Što je asimetrična i simetrična enkripcija?, https://www.websiterating.com/hr/vpn/glossary/what-is-asymmetric-symmetric-encryption/ [pristupljeno 30. lipnja 2023].

13. Što je enkripcija podataka i kako se radi? (2017). https://www.tportal.hr/tehno/clanak/sto-je-enkripcija-podatka-i-kako-se-radi-20170704/print [pristupljeno 1. srpnja 2023].
14. VPN Technologies – Generic Routing Encapsulation (2022). https://www.linkedin.com/pulse/vpn-technologies-generic-routing-encapsulation-gre-chidiadi-anyanwu [pristupljeno 1. srpnja 2023].
15. Salić, D. Tuneliranje protokolima kojima to nije osnovna namena, http://www.ftn.uns.ac.rs/ojs/index.php/zbornik/article/view/2448/2171 [pristupljeno 2. srpnja 2023].
16. Lenković, K., Miletić, V., Tuneliranje alatom tinc, https://gaseri.org/hr/nastava/materijali/tinc-virtualna-privatna-mreza/ [pristupljeno 2. srpnja 2023].
17. Kraljević, M. Završni rad. Split: Sveučilište u Splitu, Sveučilišni odjel za stručne studije. https://repozitorij.oss.unist.hr/islandora/object/ossst%3A1349/datastream/PDF/view [pristupljeno 3. srpnja 2023].
18. What is PPTP? https://www.expressvpn.com/what-is-vpn/protocols/pptp [pristupljeno 7. srpnja 2023].
19. What is L2TP VPN Protocol? https://www.vpnunlimited.com/help/vpn-protocols/l2tp-protocol [pristupljeno 7. srpnja 2023].
20. SSL VPN (Secure Sockets Layer virtual private network) https://www.techtarget.com/searchsecurity/definition/SSL-VPN [pristupljeno 7. srpnja 2023].
21. What is L2F? (2021). https://www.tutorialspoint.com/what-is-layer-2-forwarding-l2f [pristupljeno 8. srpnja 2023].
22. Što je VPN i zašto ga trebate u 2023 (2023). https://hr.vpnmentor.com/blog/sve-o-vpn-ovima-vpnmentorov-vodic-kroz-vpn-ove-za-pocetnike/ [pristupljeno 10. srpnja 2023].
23. VPN prednosti i nedostatci (2020). https://besplatniprogrami.org/vpn-prednosti-i-nedostaci/ [pristupljeno 11. srpnja 2023].
24. VPN zaštita: kada je koristiti i u kojoj mjeri (2021). https://pcchip.hr/internet/korisne-aplikacije/vpn-zastita-kada-je-koristiti-i-u-kojoj-mjeri/ [pristupljeno 12. srpnja 2023].

25. How to Setup a VPN to Access Your Office Files Remotely, https://www.silentpartnersoftware.com/blog/nonprofit-data-management/how-to-setup-a-vpn-to-access-your-office-files-remotely/ [pristupljeno 13. srpnja 2023].
26. Carnet (2023). Osnovi koncepti VPN tehnologije, CERT.hr-PUBDOC-2023-02-05 https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf [pristupljeno 14. srpnja 2023].
27. Budućnost VPN tehnologije https://hr.unedose.fr/article/what-is-wireguard-the-future-of-vpn-technology [pristupljeno 15. srpnja 2023].
28. Sigurnost rada na udaljeno (2021). https://www.netokracija.com/sigurnost-rada-na-udaljeno-najcesce-prijetnje-174585 [pristupljeno 15. srpnja 2023].
29.*Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, (2021). http://www.enciklopedija.hr/Natuknica.aspx?ID=68095 [pristupljeno 17.srpnja 2023].

POPIS SLIKA