|  |  |  |
| --- | --- | --- |
|  | UNIVERZITET U NOVOM SADU  **FAKULTET TEHNIČKIH NAUKA U NOVOM SADU** |  |

Nataša Spremo

**PRIMENA VIRTUALNE PRIVATNE MREŽE**

DIPLOMSKI RAD

- Osnovne akademske studije -

Novi Sad, 2021. godine

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | УНИВЕРЗИТЕТ У НОВОМ САДУ ● **ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА**  21000 НОВИ САД, Трг Доситеја Обрадовића 6 | | | |
| **КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА** | | | |
| Редни број, **РБР**: | | |  | |
| Идентификациони број, **ИБР**: | | |  | |
| Тип документације, **ТД**: | | | Монографска публикација | |
| Тип записа, **ТЗ**: | | | Текстуални штампани документ/ ЦД | |
| Врста рада, **ВР**: | | | Дипломски рад | |
| Аутор, **АУ**: | | | Наташа Спремо | |
| Ментор, **МН**: | | | др Бранислав Атлагић, доцент | |
| Наслов рада, **НР**: | | | Развој клијентске Веб апликације за аквизиционо управљачке системе | |
| Језик публикације, **ЈП**: | | | Српски ( латиница ) | |
| Језик извода, **ЈИ**: | | | Српски/енглески | |
| Земља публиковања, **ЗП**: | | | Србија | |
| Уже географско подручје, **УГП**: | | | Војводина | |
| Година, **ГО**: | | | 2020. | |
| Издавач, **ИЗ**: | | | Ауторски репринт | |
| Место и адреса, **МА**: | | | Факултет техничких наука (ФТН), Д. Обрадовића 6, 21000 Нови Сад | |
| Физички опис рада, **ФО**: (поглавља/страна/ цитата/табела/слика/графика/прилога) | | | 10/30/13/3/18/0/0 | |
| Научна област, **НО**: | | | Електротехничко и рачунарско инжењерство | |
| Научна дисциплина, **НД**: | | | Примењене рачунарске науке и информатика | |
| Предметна одредница/Кључне речи, **ПО**: | | | Мрежа, комуникација, TCP, IPsec, безбедност на интернету | |
| **УДК** | | |  | |
| Чува се, **ЧУ**: | | | Библиотека ФТН, Д. Обрадовића 6, 21000 Нови Сад | |
| Важна напомена, **ВН**: | | |  | |
| Извод, **ИЗ**: | | | Фали | |
| Датум прихватања теме, **ДП**: | | |  | |
| Датум одбране, **ДО**: | | |  | |
| Чланови комисије, **КО**: | | Председник: | др Ранко поповић, ред.проф |
|  | | Члан: | др Милана Бојанић, доцент | Потпис ментора |
|  | | Члан, ментор: | др Бранислав Атлагић, доцент |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | UNIVERSITY OF NOVI SAD ● **FACULTY OF TECHNICAL SCIENCES**  21000 NOVI SAD, Trg Dositeja Obradovića 6 | | | |
| **KEY WORDS DOCUMENTATION** | | | |
| Accession number, **ANO**: | | |  | |
| Identification number, **INO**: | | |  | |
| Document type, **DT**: | | | Monographic publication | |
| Type of record, **TR**: | | | Textual material, printed/CD | |
| Contents code, **CC**: | | | Bachelor thesis | |
| Author, **AU**: | | | Nataša Spremo | |
| Mentor, **MN**: | | | dr Branislav Atlagić, assistant professor | |
| Title, **TI**: | | | Applying Virutal Private Network | |
| Language of text, **LT**: | | | Serbian | |
| Language of abstract, **LA**: | | | Serbian/English | |
| Country of publication, **CP**: | | | Serbia | |
| Locality of publication, **LP**: | | | Vojvodina | |
| Publication year, **PY**: | | | 2020. | |
| Publisher, **PB**: | | | Author’s reprint | |
| Publication place, **PP**: | | | Faculty of Technical Sciences, D. Obradovića 6, 21000 Novi Sad | |
| Physical description, **PD**: (chapters/pages/ref./tables/pictures/graphs/appendixes) | | | 10/30/13/3/18/0/0 | |
| Scientific field, **SF**: | | | Electrical and computer engineering | |
| Scientific discipline, **SD**: | | | Applied computer science and informatics | |
| Subject/Key words, **S**/**KW**: | | | Network, communication, TCP, IPsec, security on internet | |
| **UC** | | |  | |
| Holding data, **HD**: | | | Library of Faculty of Technical Sciences, D. Obradovića 6, 21000 Novi Sad | |
| Note, **N**: | | |  | |
| Abstract, **AB**: | | | Фали | |
| Accepted by the Scientific Board on, **ASB**: | | |  | |
| Defended on, **DE**: | | |  | |
| Defended Board, **DB**: | | President: |  |
|  | | Member: |  | Menthor's sign |
|  | | Member, Mentor: | dr Branislav Atlagic, assistant professor |  |

|  |  |  |
| --- | --- | --- |
|  | УНИВЕРЗИТЕТ У НОВОМ САДУ ● **ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА** 21000 НОВИ САД, Трг Доситеја Обрадовића 6 | Датум: |
|  |
| **ЗАДАТАК ЗА ИЗРАДУ ДИПЛОМСКОГ (BACHELOR) РАДА** | Лист/Листова: |
|  |

*(Податке уноси предметни наставник - ментор)*

|  |  |
| --- | --- |
| Врста студија: | ☒ Основне академске студије  ☐ Основне струковне студије |
| Студијски програм: | Примењено софтверско инжењерство |
| Руководилац студијског програма: | др Александар Селаков |

|  |  |  |  |
| --- | --- | --- | --- |
| Студент: | Наташа Спремо | Број индекса: | **ПР 27/2016** |
| Област: | Примена рачунарских мрежа у инфраструктурним системима | | |
| Ментор: | др. Бранислав Атлагић | | |
| НА ОСНОВУ ПОДНЕТЕ ПРИЈАВЕ, ПРИЛОЖЕНЕ ДОКУМЕНТАЦИЈЕ И ОДРЕДБИ СТАТУТА ФАКУЛТЕТА  ИЗДАЈЕ СЕ ЗАДАТАК ЗА ДИПЛОМСКИ (Bachelor) РАД, СА СЛЕДЕЋИМ ЕЛЕМЕНТИМА:   * проблем – тема рада; * начин решавања проблема и начин практичне провере резултата рада, ако је таква провера неопходна; * литература | | | |

**НАСЛОВ ДИПЛОМСКОГ (BACHELOR) РАДА:**

|  |
| --- |
| Примена виртуелне приватне мреже |

**ТЕКСТ ЗАДАТКА:**

|  |
| --- |
| Развити конзолну апликацију где клијент и сервер иницијално комуницирају преко TCP протокола на локалној мрежи. Омогућити повезивање клијента преко нове VPN адресе са сервером, уколико је виртуелна приватна мрежа активирана. Могућа даља комуникација преко VPNа или затварање везе. |

|  |  |
| --- | --- |
| Руководилац студијског програма: | Ментор рада: |
|  |  |

|  |
| --- |
| Примерак за: ☐ - Студента; ☐ - Ментора |

Образац **Q2.НА.15-04** - Издање 1

**SPISAK SKRAĆENICA**

|  |  |
| --- | --- |
| ***VPN*** | ***Virtual Private Network*** |
| ***IP*** | ***Internet Protocol*** |
| ***IPsec*** | ***Internet Protocol Security*** |
| ***TCP*** | ***Transmission Control Protocol*** |
| ***UDP*** | ***User Datagram Protocol*** |
| ***WAN*** | ***Wide Area Network*** |
| ***QoS*** | ***Quality Of Service*** |
| ***OSI model*** | ***Open Systems Interconnection model*** |
| ***LAN*** | ***Local Area Network*** |
| ***DTLS*** | ***Datagram Transport Layer Security*** |
| ***MPPE*** | ***Microsoft Point-To-Point Encryption*** |
| ***SSTP*** | ***Secure Socket Tunneling Protocol*** |
| ***MPVPN*** | ***Multi Path Virtual Private Network*** |
| ***SSH VPN*** | ***Secure Shell VPN*** |
|  |  |

**SPISAK KORIŠĆENIH SLIKA**

|  |  |
| --- | --- |
| ***Slika 1.1*** | ***Prikaz rada VPN mreže*** |
| ***Slika 2.1*** | ***Prikaz VPN terminologije*** |
| ***Slika 4.1.1*** | ***Klijent-server arhitektura*** |
| ***Slika 6.1.1*** | ***Konzolna aplikacija servera*** |
| ***Slika 6.1.2*** | ***Konzolna aplikacija klijenta*** |
| ***Slika 6.1.3*** | ***Server-klijent komunikacija preko nove adrese*** |
| ***Slika 6.1.4*** | ***Korisnički interfejs Tunnel Bear aplikacije na Windows platformi*** |
| ***Slika 6.1.5*** | ***Korisnički interfejs Tunnel Bear aplikacije na Android platformi*** |

**SPISAK LISTINGA**

|  |  |
| --- | --- |
| ***Listing 6.1.1*** | ***Inicijalizalija servera*** |
| ***Listing 6.1.2*** | ***Konektovanje klijenta sa već pokrenutim serverom*** |
| ***Listing 6.1.3*** | ***Dobavljanje VPN IP adrese na serverskoj strani*** |
| ***Listing 6.1.4*** | ***VPN otvaranje konekcije na serverskoj strani*** |
| ***Listing 6.1.5*** | ***Prijem poruke na klijentskoj strani*** |
| ***Listing 6.1.6*** | ***Otvaranje VPN konekcije na strani klijenta*** |

**Sadržaj**

[1. Uvod 8](#_Toc69994602)

[2. Osnove VPN-a 9](#_Toc69994603)

[2.1 VPN Tehnologije 10](#_Toc69994606)

[2.2 Kriterijumi odabira VPN provajdera 12](#_Toc69994607)

[3. Sigurnosni mehanizmi 13](#_Toc69994608)

[3.1 IPsec 14](#_Toc69994610)

[3.2 SSL/TLS 15](#_Toc69994611)

[4. Konzolne aplikacije 15](#_Toc69994612)

[4.1 Klijent-server arhitektura 15](#_Toc69994614)

[5. Opis korišćenih tehnologija i alata 16](#_Toc69994615)

[6. Opis programskog rešenja 17](#_Toc69994616)

[7. Zaključak 23](#_Toc69994617)

[8. Literatura 24](#_Toc69994618)

# **Uvod**

U današnje vreme, u pogledu bezbednosti, kako u privatnom tako i u poslovnom okruženju, od najveće važnosti je zaštita podataka i informacija koje razmenjujemo svakodnevno putem interneta.

Ukoliko se korisnici nalaze van kuće, u nekom restoranu, hotelu, aerodromu ili drugom javnom mestu, najveći broj njih će koristiti bežične javne tačke za pristup internetu, odnosno WiFi. Posmatrano sa bezbednosnog aspekta, najveći izazov predstavlja sigurnost korišćenja ovakvih pristupnih tačaka, jer korisnici nemaju uvid ko sve koristi navedenu tačku za pristup i da li se nadgleda i snima razmena podataka putem te WiFi pristupne tačke.

Kada govorimo o potrebi korisnika za radom na daljinu, odnosno radom od kuće, koji podrazumeva pristupanje resursima software-as-a-service (SaaS), koji pripadaju određenoj organizaciji ili instituciji, neophodno je da se takav rad obavlja na bezbedan način, kako ne bi došlo do moguće kompromitacije podataka kojima korisnik pristupa.

Kako bi korisnici zaštitili svoje mrežne aktivnosti, privatnost i sprečili da dođe do kompromitacije podataka organizacije preporuka je korišćenje virtuelne privatne mreže, odnosno VPN (eng. Virtual Private Network) pristup. VPN tehnologija kreira privatni, šifrovani tunel za aktivnosti na mreži i znatno otežava bilo kome da prati ili nadgleda šta korisnik radi dok je na mreži. Takođe, VPN tehnologija omogućava kompanijama bolju zaštitu od mogućeg gubitka i kompromitacije podataka, tako što se između korisničke mreže, bilo da se koristi javni ili privatni WiFi, pravi bezbedan i šifrovan tunel, preko javnog interneta do mreže organizacije.

VPN tip konekcija počeo je da se razvija još u vreme dial up modema, međutim to se ne smatra pravom virtualnom privatnom mrežom. Poslednjih nekoliko godina VPN je postao vrlo popularan zbog mnoštva vrlina koje poseduje. Naročito od kad je sve više korporacija bilo primorano da organizuje i omogući bezbedan rad od kuće. S obzirom da je ova vrsta mreže pristupačna svima, koriste je, pored kompanija, i individualni korisnici. Sigurnost, skalabilnost, niska cena, lakoća implementacije, univerzalnost najčešće su osobine koje opisuju virtualne privatne mreže.

S obzirom da se pri svakom konektovanju, nakon autentifikacije korisnika, formira već pomenuti tunel između dva čvora, pruža potpunu privatnost od spoljašnjih činioca na internetu. Pošto se koriste javne mreže troškovi su dosta niski kada se uporede sa troškovima potrebnim za iznajmljivanje privatnih linija ili implementaciju privatnih Intranet mreža. Lakoća implementacije kao jedna od osobina znači da nema potrebe za promenom postojeće infrastrukture javnih mreža, pa se VPN implementira samo na strani korisnika. Zbog enkapsulacije podataka moguće je koristiti i podatke koji pripadaju nerutabilnim protokolima. Takođe se štedi i na broju globalnih IP adresa koje kompanija mora da poseduje, što opet smanjuje cenu implementacije virtuelnih privatnih mreža.

Aplikacije koje se obično koriste, bilo da su imejl, veb, poruke, društvene mreže i sl, zasnivaju se na IP (Internet Protocol) protokolu. Iako su razvijeni određeni standardi, nisu sve internet aplikacije bezbedne, određen broj aplikacija i dalje nije usaglašen sa važećim propisima o načinu deljenja i zaštite podataka. Neujednačen stav o načinu zaštite podataka ostavlja prostora mogućim zloupotrebama od strane napadača, odnosno hakera, koji zbog ovakvih propusta jednostavno mogu doći do ličnih podataka korisnika, kao što su broj tekućeg računa, kreditne kartice, kućne adrese i sl.

VPN kreira privatni tunel preko otvorenog interneta. Ideja je da sve što korisnik pošalje bude enkapsulirano i šifrirano u ovom privatnom komunikacijskom kanalu, pa čak i ako dođe do presretanja poslatih paketa, isti ne mogu biti dešifrovani. VPN predstavlja vrlo moćan i važan alat u zaštiti i bezbednosti korisnika i njihovih podataka, ali ima i svoja ograničenja. Ovde se postavlja pitanje ograničenja VPN-a i razumevanje gde se nalazi krajnja tačka VPN servera. Ukoliko se korisnik nalazi u Srbiji, a povezuje se na VPN server u drugoj državi, celokupan saobraćaj na internetu će biti prikazan kao da je korisnik pristupio iz mreže te druge države, odnosno neće biti vidljivo da je korisnik pristupio iz IP opsega Republike Srbije.

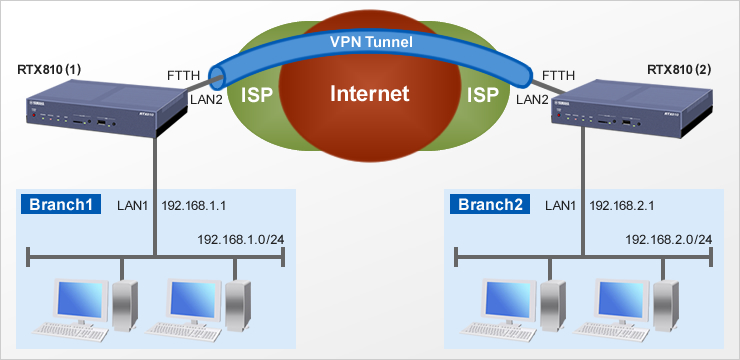
Dva najčešća tipa VPN-a su: korporativni ili poslovni VPN servis koji predstavlja poslovno orijentisano rešenje koje omogućava zaposlenima da se udaljeno povežu na korporativnu mrežu i korisnički VPN servis koji pojedincima omogućava da privatno surfuju od kuće. [1]

# **OSNOVE VPN-a**

Virtuelna privatna mreža je mreža jedne institucije ili grupe korisnika realizovana preko javne ili deljene infrastrukture (Internet, provajderske mreže). Razlozi za uvođenje ove tehnologije su brojni, među kojima su i sigurnosni problemi, bolja organizacija saobraćaja i rutiranja, nedostatak podrške za QoS, problem broja IP adresa i migracija na Ipv6.

Glavna funkcionalnost VPN mreže jeste sigurna komunikacija između autentifikovanih korisnika u čiji sadržaj nemaju uvid spoljni posmatrači. Korisnici mogu biti na geografski udaljenim lokacijama i nesmetano koristiti virtualnu privatnu mrežu, ukoliko imaju ispravne kredencijale. Prednosti VPN-a su brojne, neke od kojih su brzina, fleksibilnost, privatnost, skalabilnost i finansijske prednosti.

Sam princip rada VPN-a uvodi pojam tunelovanja (eng. *Tunneling*). Tunelovanje je sastavni deo ove mreže i predstavlja prenos paketa podataka namenjenih privatnoj mreži preko javne mreže. Ruteri javne mreže nemaju informaciju da prenose pakete koji pripadaju privatnoj mreži i VPN pakete tretiraju kao normalan saobraćaj. Pojam tunel uvodi se zbog toga što su podaci koji putuju tunelom razumljivi samo onima koji se nalaze na njegovom izvorištu i odredištu. Početak i kraj tunela se nalaze u VPN mrežama. Kada enkapsulirani paket stigne na odredišnu adresu vrši se deenkapsulacija i prosleđivanje podataka na konačno odredište. Ceo proces enkapsulacije, transporta i deenkapsulacije naziva se tunelovanje (Slika 1.1).



**Slika 1.1** Prikaz rada VPN mreže

Jedna od glavnih funkcionalnosti VPN mreža je maskiranje ili promena prave IP adrese korisnika. Iako VPN provajderi preduzimaju jake mere da zaštite informacije korisnika, dešavaju se greške poput tzv. IP leak-a ili greške pri konekciji na server.

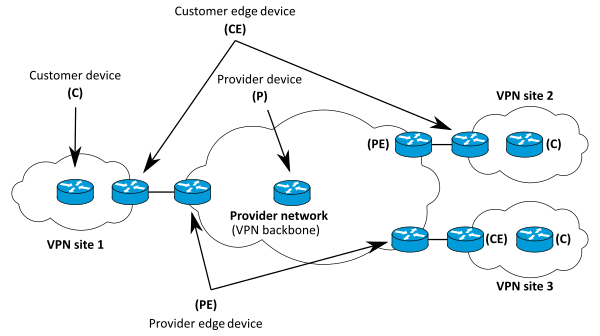
Trenutno postoji široka ponuda provajdera virtualnih privatnih mreža na internetu. Prilikom odabira treba temeljno ispitati sigurnost i bezbednost samog provajdera i usluga koje pruža.



## **VPN Tehnologije**

Postoji više vrsta i podela VPN tehnologija:

* Podela prema tome kome pripadaju uređaji i gde su u VPN (Provider Provisioned VPN):
  1. C – customer device – uređaj koji se nalazi unutar korisničke mreže i nije direktno povezan sa mrežom provajdera. C uređaji nisu svesni VPN mreže.
  2. CE – customer edge device – uređaj koji se nalazi na granici korisničke mreže koji omogućuje pristup PPVPN.
  3. PE – provider edge device – uređaj ili set uređaja na granici provajder mreže koji povezuje korisničku mrežu uz pomoć CE uređaja. PE uređaji su svesni VPN mreže i održavaju stanje VPN-a.
  4. P – provider device – uređaj koji funkcioniše unutar provajder mreže i ne povezuje se direktno ni sa jednim korisničkim endpoint-om. Može pružiti rutiranje za mnoge provajder-operabilne tunele koji pripadaju različitim korisnicima PPVPN-a. Iako je P uređaj glavni činilac u implementaciji PPVPN-a, nije VPN-aware i ne održava VPN stanje, kao provider edge device [2].



**Slika 2.1** Prikaz VPN terminologije [2]

* Podela prema tome ko ih realizuje

1. Provider provisioned
2. Customer enabled

* Podela prema vrsti servisa
  1. Site-to-site (LAN-to-LAN)
     + Intranet (lokacije jedne institucije)
     + Extranet (povezivanje različitih institucija)
  2. Remote access
     + Compulsory (access server inicira VPN vezu)
     + Voluntary (klijent inicira VPN vezu)
* Podela prema sloju rada u ISO/OSI modelu
  1. Layer 1
  2. Layer 2
  3. Layer 3
* Podela prema poverljivosti podataka
  1. Trusted VPN
  2. Secure VPN
  3. Hybrid VPN

Dok individualni korisnici najčešće vrše interakciju preko remote access VPN mreža, kompanije više koriste site-to-site VPN. VPN-ovi mogu biti kategorizovani kao host-to-network tj remote access ako se jedan uređaj poveže sa mrežom, ili site-to-site ukoliko se povezuju dve mreže. U slučaju kompanija, remote access koriste radnici pri povezivanju na poslovni intranet van svoje kancelarije. Site-to-site dozvoljava povezivanje saradnika sa dve geografski udaljene strane u jednu virtualnu privatnu mrežu.

Što se tiče poverljivosti podataka, VPN može koristiti oba tipa mehanizama. Trusted VPN koristi privatne mreže iznajmljene od komunikacionih provajdera, dok secure VPN radi na principu kriptovanja poruka koje se šalju preko javnih komunikacionih mreža. Ukoliko se pored trusted koristi i secure mehanizam, kao što se, na primer, na jedan gateway može primeniti i IPsec i SSL i kao takav naziva se hybrid gateway, takav VPN se takođe naziva hibridnim.

Implementacije poverljivih (*eng* trusted) VPN mreža napredovale su od iznajmljivanja privatnih linija preko telekomunikacionih prodavaca do privatnih IP mreža koje pružaju internet provajderi. Iako ne pružaju sigurnost, olakšavaju grupisanje, tj. kreiranje segmenata unutar WAN mreža. Dodatno, olakšavaju kontrolu nad ovim segmentima jer se to može vršiti sa jednog mesta i najčešće dolazi uz garantovani QoS od strane provajdera.

Kako je internet vremenom postao popularan kao komunikacioni medijum, sigurnost je postala sve veća briga i problem kako po korisnike tako i po provajdere. Kako se ispostavilo da poverljivi VPNovi ne nude nikakav vid sigurnosti na mreži, počeo je razvoj protokola koji bi dozvolili da se saobraćaj preko interneta kriptuje tako da bude poznat samo krajnjim učesnicima komunikacije, a tokom slanja kroz javnu mrežu bude neutvrđen sadržaj. Ovaj koncept rada podseća na tzv. tunel između dva krajnja korisnika, tako da čak i ako presretač upadne u komunikaciju ne može dešifrovati saobraćaj, niti može promeniti podatke a da krajnja strana to ne primeti. Mreže koje se zasnivaju na kriptovanju saobraćaja zovu se sigurnosne (*eng* secure) VPN mreže. [14]

## **Kriterijumi odabira VPN provajdera**

Najtipičniji kriterijumi po kojima se VPN mreže ocenjuju su:

* brzina konekcije,
* zaštita privatnosti, uključujući privatnost pri registrovanju i nivou enkripcije,
* broj servera i njihove lokacije,
* upotrebljivost interfejsa,
* cena,
* metodi online plaćanja,
* skladištenje korisničkih podataka

Pri analiziranju VPN usluga takođe treba uzeti u obzir i da li web sajt koristi potencijalno nametljivu tehnologiju poput third-party ili permanentnih kolačića. Da li se vrši obfuskacija, to jest da li servis pruža metod obfuskacije VPN saobraćaja tako da nije lako detektovan ili blokiran od strane nacionalnih vlada ili korporacija. [5]

# **SIGURNOSNI MEHANIZMI**

Širok spektar (obično komercijalnih) entiteta pruža usluge VPN-a za razne svrhe, ali u zavisnosti od pružaoca usluga i aplikacije, često ne stvaraju istinsku „privatnu mrežu“. Ipak, termin je sve više zastupljen. Šira javnost uglavnom koristi termin VPN usluga ili samo VPN posebno za komercijalni proizvod ili uslugu koji koristi VPN protokol za podešavanje internetskog saobraćaja korisnika, tako da se IP adresa servera dobavljača usluge javnosti čini kao IP adresa korisnika. U zavisnosti od pravilno implementiranih karakteristika, saobraćaj, lokacija i / ili stvarna IP adresa korisnika mogu biti sakriveni od javnosti, pružajući tako željene funkcije pristupa Internetu, kao što su zaobilaženje cenzure Interneta, maskiranje IP adresa (ne sme se mešati sa anonimnošću ), i geo-deblokada. Korisnički internet promet sigurno podešavaju samo između javnog interneta i korisnikovog uređaja i obično ne postoji mogućnost da se uređaji korisnika povezani na isti „VPN“ vide. Ovi VPN-ovi mogu biti zasnovani na tipičnim VPN protokolima ili na više maskirnih VPN implementacija poput SoftEther VPN-a, ali se koriste i proki protokoli poput Shadovsocks. Ovi VPN-ovi se obično prodaju kao usluge zaštite privatnosti.

Na strani klijenta, uobičajena VPN postavka po dizajnu nije klasičan VPN, ali obično koristi VPN interfejse operativnog sistema za hvatanje korisničkih podataka za slanje. To uključuje virtuelne mrežne adaptere na računarskim OS-ima i specijalizovane „VPN“ interfejse na mobilnim operativnim sistemima.

Korisnici moraju uzeti u obzir da kada se preneseni sadržaj ne šifruje pre ulaska u VPN, ti podaci su vidljivi na primajućoj krajnjoj tački (obično je to veb lokacija javnog VPN provajdera), bez obzira na to da li je sam omotač VPN tunela šifrovan za transport između čvorova. Jedini siguran VPN je tamo gde učesnici imaju nadzor na oba kraja celokupne putanje podataka ili je sadržaj šifrovan pre nego što uđe u tunel provajdera.

VPN-ovi ne mogu da čine mrežne veze potpuno anonimnim, ali obično mogu da povećaju privatnost i sigurnost. Da bi sprečili otkrivanje privatnih podataka, VPN-ovi obično dozvoljavaju samo potvrđeni udaljeni pristup korišćenjem protokola tuneliranja i tehnika šifrovanja.

VPN model zaštite obezbeđuje:

• poverljivost takva da čak i ako se mrežni saobraćaj njuška na nivou paketa, napadač će videti samo šifrovane podatke

• potvrda identiteta pošiljaoca kako bi neovlašćenim korisnicima onemogućio pristup VPN-u

• integritet poruke za otkrivanje bilo kakvih slučajeva neovlašćenog korišćenja prenetih poruka.

Sigurni VPN protokoli uključuju sledeće [2]:

* Internet Protocol Security (IPsec) koristi šifrovanje, enkapsulirajući IP paket unutar IPsec paketa. Deenkapsulacija se dešava na kraju tunela, gde se originalni IP paket dešifruje i prosleđuje na predviđeno odredište.
* Transport Layer Security (SSL / TLS) može tunelirati promet čitave mreže ili osigurati pojedinačnu vezu. Brojni dobavljači pružaju VPN mogućnosti za daljinski pristup putem SSL-a. SSL VPN se može povezati sa lokacija na kojima IPsec nailazi na probleme sa prevođenjem mrežnih adresa i pravilima zaštitnog zida.
* Datagram Transport Layer Security (DTLS) - koristi se u Cisco AniConnect VPN i OpenConnect VPN za rešavanje problema koje SSL / TLS ima sa tuneliranjem preko TCP (tuneliranje TCP preko TCP može dovesti do velikih kašnjenja i prekida veze).
* Microsoft Point-to-Point Encryption (MPPE) radi sa Point-to-Point Tunneling Protocol-om i u nekoliko kompatibilnih implementacija na drugim platformama.
* Microsoft Secure Socket Tunneling Protocol (SSTP) tunelira protokol od tačke do tačke (PPP) ili protokol tuneliranja sloja 2 (Layer 2 Tunneling Protocol) kroz SSL / TLS kanal.
* Multi Path Virtual Private Network (MPVPN). Kompanija Ragula Sistems Development poseduje registrovani zaštitni znak „MPVPN“.
* Secure Shell VPN (SSH) - OpenSSH nudi VPN tuneliranje (različito od prosleđivanja portova) radi osiguranja udaljenih veza sa mrežom ili inter-mrežnih veza. OpenSSH server pruža ograničen broj istovremenih tunela. Sama VPN funkcija ne podržava ličnu potvrdu identiteta.
* WireGuard je protokol. U 2020. godini podrška za VireGuard je dodata i jezgru Linuk i Android, što je otvorilo VPN dobavljačima za usvajanje. Podrazumevano, VireGuard koristi Curve25519 za razmenu ključeva i ChaCha20 za šifrovanje, ali takođe uključuje mogućnost pre-deljenja simetričnog ključa između klijenta i servera. Gotovo svi komercijalni VPN-ovi prihvatili su ovaj protokol kao zadati.

Krajnje tačke tunela moraju biti potvrđene da bi se mogle uspostaviti sigurni VPN tuneli. VPN-ovi sa daljinskim pristupom koje su kreirali korisnici mogu da koriste lozinke, biometriju, dvofaktorsku autentifikaciju ili druge kriptografske metode. Tuneli network-to-network često koriste lozinke ili digitalne sertifikate. Oni trajno čuvaju ključ kako bi se tunel mogao automatski uspostaviti, bez intervencije administratora [2].



## **IPsec**

IPsec je grupa protokola koji se zajedno koriste za postavljanje šifrovanih veza između uređaja. Pomaže u zaštiti podataka poslatih preko javnih mreža. IPsec se često koristi za postavljanje VPN-ova i radi šifrovanjem IP paketa, zajedno sa autentifikacijom izvora odakle paketi potiču.

IPsec, skraćenica od Internet Protocol Securiti, može se izvoditi u transportnom ili tunelskom režimu, od kojih svaki ima značajno različite implikacije, posebno u pogledu bezbednosti. Režim tunela šifriraće i informacije o zaglavlju, kao i podatke koji se prenose, dok će način transporta šifrovati samo podatke. Ključevi moraju biti podeljeni i pošiljaocu i primaocu da bi se pravilno dešifrovao prenos.

IPsec radi na sloju 3 ili mrežnom sloju OSI modela, što mu omogućava da radi nezavisno od bilo koje aplikacije. IPsec VPN stvara tunel između dve krajnje tačke kroz koji može putovati bilo koji broj veza i tipova protokola (veb, e-pošta, prenos datoteka, VoIP). Drugim rečima, pruža kompletnu zaštitu (eng *blanket* coverage). Originalni IP paket podataka se rekapsulira, tako da su sve informacije o protokolu aplikacije skrivene tokom stvarnog prenosa podataka.

IPsec usluge [4]:

* Integritet podataka
* Autentikacija izvora
* Prevencija “snimi i ponovi” napada
* Poverljivost podataka

Dva protokola sa različitim skupom usluga:

1. Authentication Header (AH) – pruža integritet i autentifikaciju, ali ne i poverljivost
2. Encapsulation Security Protocol (ESP) – pruža integritet, autentikaciju i poverljivost. Šire korišćen nego Authentication Header.

## **SSL/TLS**

SSL (Secure Socket Layer) VPN se često nazivaju transparentnim ili bez klijenta, zbog nedostatka bilo kakvog dodatnog VPN softvera na strani klijenta koji mora biti eksplicitno instaliran. SSL komponente potrebne za stvaranje sigurnog kanala iz udaljenog sistema deo su svih glavnih veb pregledača, od kojih je barem jedan uvek dostupan na gotovo svakom savremenom računaru. Jedina nova stavka koja je neophodna je naznačeni SSL VPN server, koji deluje kao prolaz između zaštićene mreže i svih udaljenih sistema.

SSL protokol deluje u sloju 7, aplikativnom sloju, omogućavajući mu da deluje kao proksi za zaštićene resurse. Autentifikacija i klijenta i servera postiže se tokom početne rutine rukovanja, gde se obe strane identifikuju putem digitalnih sertifikata. Proces rukovanja takođe generiše ključeve sesije koji se koriste za šifrovanje celokupnog prometa poslatog i primljenog tokom sesije daljinskog pristupa.

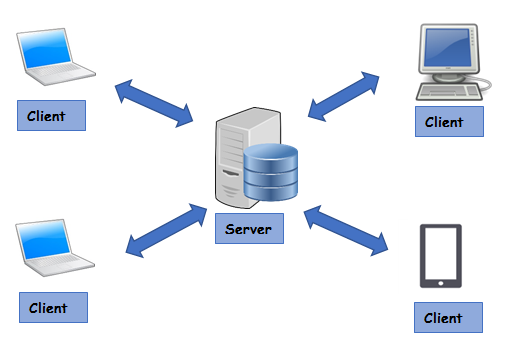
IPsec i SSL imaju svaki svoje prednosti. Dakle, ono što je „bolje“ često se svodi na ono što je najpogodnije za korisnika i njegovu mrežu, ali mnoge organizacije se sve više okreću SSL VPN-ima radi dodatnih dostupnih pogodnosti. [12]

# **Konzolne aplikacije**



## **Klijent-server arhitektura**

Klijent / server arhitektura je računski model u kojem više komponenata radi u strogo definisanim ulogama za komunikaciju. Server hostuje, isporučuje i upravlja većinom resursa i usluga koje klijent troši. Ova vrsta arhitekture zajedničkih resursa ima jedan ili više klijentskih računara povezanih na centralni server preko mreže ili Internet veze (Slika 4.1.1).



**Slika 4.1.1** Klijent-server arhitektura

Klijent-server opisuje vezu programa u aplikaciji koji sarađuju. Ovaj tip arhitekture funkcioniše tako što klijent šalje resurs ili zahtev serveru preko mrežne veze, koji se onda procesuira i dostavlja klijentu. Serverska strana može simultano da prima zahteve od strane više klijenata, dok klijent može biti povezan sa više servera u isto vreme koji pružaju različite usluge [6].

Usluga je apstrakcija kompjuterskih resursa i klijent ne mora da brine o tome kako server radi dok ispunjava zahtev i isporučuje odgovor. Klijent samo mora da razume odgovor koji se zasniva na dobro poznatom protokolu za aplikaciju, odnosno sadržaj i format podataka za zahtevanu uslugu.

Neke od mana ove arhitekture jesu:

* Ako se dešavaju česti i istovremeni klijentski zahtevi ka serveru, može doći do zagušenja prometa i kašnjenja ili potpunog nedostatka odgovora klijentu,
* Budući da je arhitektura centralizovana, ako kritični server otkaže, zahtevi klijenata se ne ispunjavaju. [6]

# **Opis korišćenih tehnologija i alata**

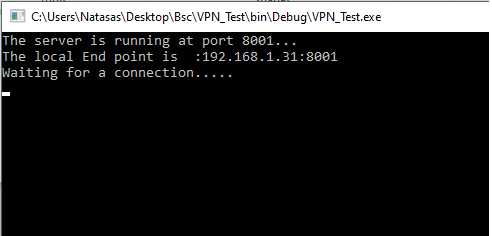
* **C# -** programski jezik opšte namene i namenjen je izradi aplikacija za .NET Framework platformu. Podržava imperativnu, objektno-orijentisanu, funkcionalnu i deklarativnu paradigmu. Spada u grupu novijih programskih jezika i razvijen je od strane kompanije Microsoft. Sintaksno veoma podseća na C i C++ jezike, ali je njegova sintaksa znatno jednostavnija. U ovom jeziku omogućeno je i automatsko rukovanje memorijom zbog čega je sigurnije za programiranje [10].
* **.NET –** besplatna, open-source platforma za razvoj mnogih vrsta aplikacija. Dijeli funkcionalnosti između različitih aplikacija i tipova aplikacija pomoću klasnih biblioteka [11].
* **Visual Studio** – integrisano razvojno okruženje (*eng*. *Integrated development environment IDE*) razvijeno od strane kompanije Microsoft. Posjeduje podrušku za 36 programskih jezika, među kojima je vodeći C#. Koristi Microsoft-ove alate za razvoj različitih vrsta aplikacija poput Windows Forms, Windows Presentation Foundation, Windows Communication Foundation, Microsoft Silverlight, WebApi i Azure-a namenjenog za Cloud okruženja [13].
* **Tunnel Bear** – aplikacija koja pruža servise virtualne privatne mreže. Koristi 256-bitnu enkripciju podataka koji se šalju putem tunela kroz javnu mrežu. Aplikacija je dostupna za korišćenje na gotovo svim platformama, kao što su Windows, Mac, iOS, Android. Moguća je upotreba i u samom pretraživaču (Chrome, Firefox, Opera).

# **Opis programskog rešenja**

Projekat se zasniva na dve .NET Framework konzolne aplikacije. Predstavlja osnovnu komunikaciju klijenta i servera preko TCP konekcije, dobavljanje lokalne IP adrese klijentskog računara, kao i dobavljanje IP adrese dodeljene klijentu od strane VPN provajdera ukoliko je VPN omogućen. Ukoliko server vrati VPN IP adresu, koja se ručno može proveriti u command promptu pod odeljkom PPP adapter, daje klijentu mogućnost da se kreira konekcija preko te IP adrese i tako pruži bezbednu vezu sa serverom.

Pri samom pokretanju aplikacije pokreće se serverska strana na lokalnoj IP adresi i čeka zahtev za konektovanje klijenta (listing 6.1.1, slika 6.1.1).

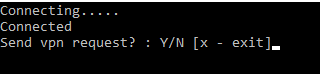
 **Listing 6.1.1** Inicijalizacija servera



**Slika 6.1.1** Konzolna aplikacija servera

Dok server osluškuje na određenoj adresi i portu, klijent, nakon pokretanja, pokušava da se poveže sa istim podacima (listing 6.1.2, slika 6.1.3).

 **Listing 6.1.2** Konektovanje klijenta sa već pokrenutim serverom



**Slika 6.1.2** Konzolna aplikacija klijenta

Kada su klijent i server uspešno povezani, klijent može da šalje zahtev da se dalja komunikacija ostvaruje preko VPN konekcije ukoliko je to moguće. Ako VPN nije uključen, server vraća poruku da trenutno nije moguće ostvariti takvu vezu, međutim ako jeste, traži novu adresu koju je dodelio sam VPN provajder i šalje je klijentu kao podatak uz pomoć kojeg se konektuje na VPN vezu (listing 6.1.3). Nakon toga iskoristi nađenu adresu tako što pokreće servera na njoj koji osluškuje za nove klijente preko VPN adrese (listing 6.1.4).

**Listing 6.1.3** Dobavljanje VPN IP adrese na serverskoj strani

**Listing 6.1.4** VPN otvaranje konekcije na serveru

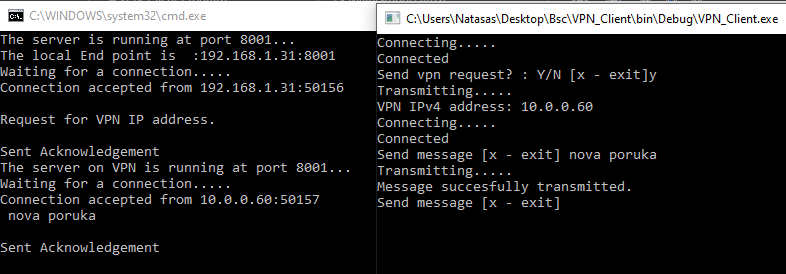
Nakon toga, klijentska strana preuzima poruku i ako dobije novu adresu, preko nje ponovo se konektuje na server (listing 6.1.5, 6.1.6). U suprotnom ponovo se pojavljuje poruka da li želi poslati zahtev.

**Listing 6.1.5** Prijem poruke na klijentskoj strani



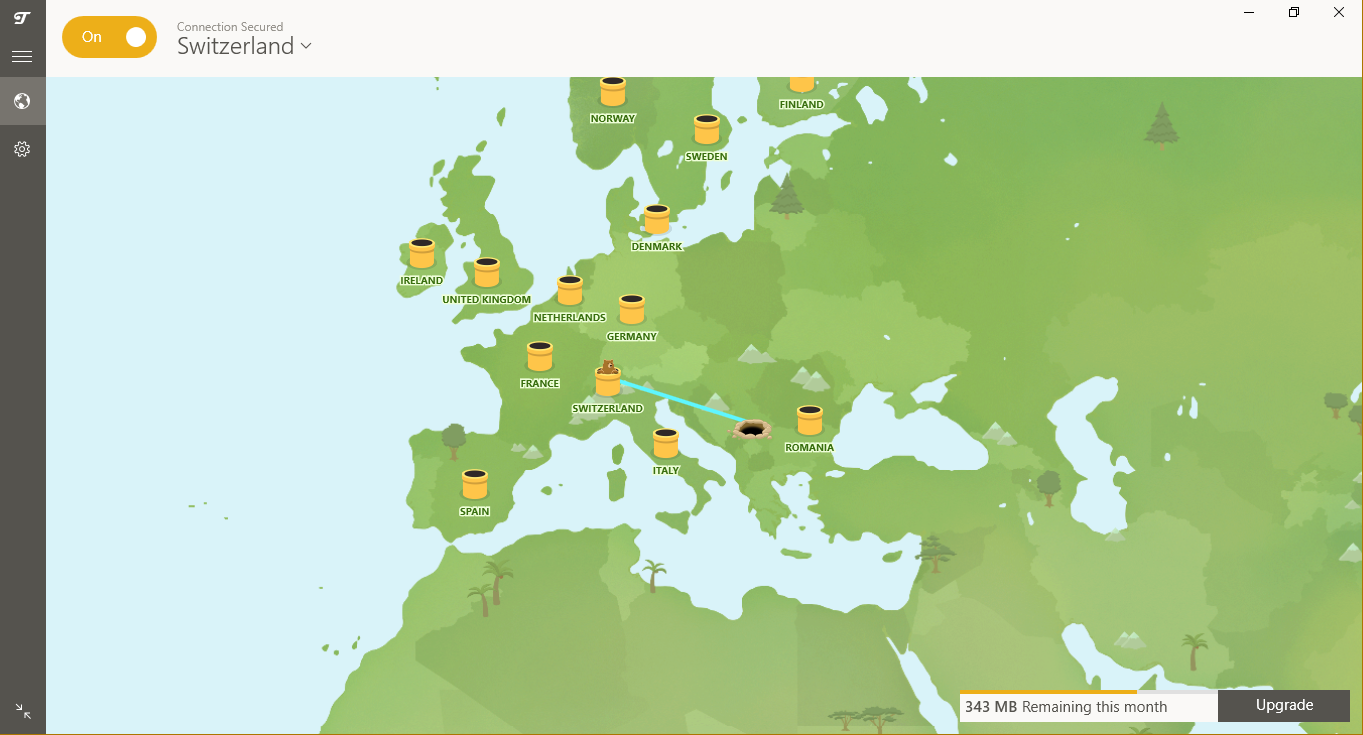
**Listing 6.1.6** Otvaranje VPN konekcije na strani klijenta

Kada se uspešno povežu obe strane, mogu komunicirati preko VPN veze, dok god klijent ne obustavi konekciju, pri čemu se gasi i serverska strana (slika 6.1.9).



**Slika 6.1.3** Server-klijent komunikacija preko nove adrese

Sam softver VPN provajdera koji je korišćen je prikazan na slici 6.2.1. Interfejs je intuitivan i jednostavan. U gornjem levom uglu postoji dugme za aktiviranje i deaktiviranje virtualne privatne mreže. Kada se aktivira, softver automatski dodeli najbliži server kako bi konekcija bila što brža i kvalitetnija. Ipak, ako korisnik nije zadovoljan uvek može izabrati drugi server koji je na raspolaganju i tako „promeniti” svoju lokaciju. Takođe, na android uređaju aplikacija funkcioniše isto (slika 6.2.2).



**Slika 6.1.4** Korisnički interfejs *Tunnel Bear* aplikacije za Windows platformu



**Slika 6.1.5** Korisnički interfejs *Tunnel Bear* aplikacije za Android platformu

# **Zaključak**

VPN (Virtualna privatna mreža) je postala nužnost u dobu kada su online praćenja toliko česta, pogotovo ako korisnik želi zaštititi svoju privatnost i osigurati svoje podatke na računaru koji mogu biti izloženi putem raznih spywarea, malwarea i sl.

VPN stvara privatni „tunel“, zatvorenu vezu koju ne može dekriptovati neka druga strana, kao što su internet provajder (ISP) ili, uopšteno, web stranice. To znači da se podaci koje korisnik šalje više ne mogu presresti i/ili ukrasti.

Virtuelne privatne mreže uglavnom ne pružaju nove funkcionalnosti koje se već ne nudi putem alternativnih mehanizama, ali VPN u većini slučajeva implementira te usluge efikasnije i jeftinije.

Dobre osobine ove mreže su brojne: sigurnost na internetu, prikrivanje privatnih informacija, sprečavanje prigušenja saobraćaja, pristup inače geo-restriktivnom sadržaju, mrežna skalabilnost, niska cena.

Međutim, loše osobine postoje. Male brzine interneta i kompleksna konfiguracija, ukoliko se ne koriste VPN usluge provajdera, su najčešći problemi sa kojima se korisnici susreću. [13]

# **Literatura**

[1] <https://www.cert.rs/files/shares/VPN%20za%20mala%20i%20srednja%20preduzeca.pdf>, **Uvod, tipovi vpn-a**

[2] [https://www.wikiwand.com/en/Virtual\_private\_network#/Security\_mechanisms](https://www.wikiwand.com/en/Virtual_private_network%23/Security_mechanisms), **Sigurnosni mehanizmi**

[3] [https://www.cloudflare.com/learning/network-layer/what-is-ipsec](https://www.cloudflare.com/learning/network-layer/what-is-ipsec/%20)/ , **IPsec**

[4] <http://www.esi.ftn.uns.ac.rs/images/predmet-orm2/2017/07.pdf>, **IPsec**

[5] <https://en.wikipedia.org/wiki/Comparison_of_virtual_private_network_services>

, **Kriterijumi odabira VPN-a**

[6] <https://www.techopedia.com/definition/438/clientserver-architecture>, **Klijent-server arhitektura**

[7] <https://rti.etf.bg.ac.rs/rti/ir4roi/Prezentacije/02%20-%20VPN,%20MPLS,%20IPsec.pdf>

[8] <https://www.cert.rs/files/shares/VPN%20za%20mala%20i%20srednja%20preduzeca.pdf>

[9] <https://docs.microsoft.com/en-us/dotnet/csharp/tour-of-csharp/>, **C#**

[10] [https://docs.microsoft.com/en-us/dotnet/core/introduction#support](https://docs.microsoft.com/en-us/dotnet/core/introduction%23support), **.NET**

[11] <https://visualstudio.microsoft.com/vs/>, **Visual Studio**

[12] <https://www.barracuda.com/resources/Barracuda_SSLVPN_WP_VPN_Technologies> , **SSL/TLS**

[13] <https://www.fortinet.com/resources/cyberglossary/benefits-of-vpn>, **Pros/Cons of VPN**

[14] <https://www.computerworld.com/article/2546283/what-you-need-to-know-about-vpn-technologies.html>, **Trusted/Secured VPNs**