Uspostavljanje ad hoc virtualne privatne mreže

Kupanovac, Leon

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Stručni studij

USPOSTAVLJANJE AD HOC VIRTUALNE PRIVATNE MREŽE

Završni rad

Leon Kupanovac

Osijek, 2018.

SADRŽAJ

1. UVOD

U današnjim suvremenim društvima postoji niz različitih institucija i sustava koji osiguravaju zaštitu osobnih podataka, prava i imovine, no još je uvijek potrebno voditi računa o brojnim postojećim sigurnosnim rizicima, kao što su i rizici vezani uz mogućnost neovlaštenog pristupa povjerljivim informacijama. Povećanje mrežne sigurnosti predstavlja jednu od osnovnih zadaća i u većini današnjih poslovnih okruženja. Kako bi se spriječili neovlašteni pristupi sustavima poduzimaju se različite mjere zaštite. Neke od tih mjera obuhvaćaju primjenu vatrozida, slanje enkriptiranih podataka te kreiranje i primjenu virtualnih privatnih mreža.

Neovisno o tome koliko sustav ima kvalitetnu zaštitu, paralelno s razvojem novih tehnoloških rješenja i novih načina komunikacije između uređaja, povećavaju se i ranjivosti i sigurnosni rizici u sustavima. Virtualna privatna mreža, odnosno VPN (engl. *Virtual Private Network*), predstavlja tehnologiju namijenjenu sigurnom povezivanju privatnih mreža u zajedničku virtualnu privatnu mrežu putem javne mrežne infrastrukture, Interneta. Pomoću VPN-a ostvaruje se siguran „tunel“ za prosljeđivanje podataka između krajnjih točka u mreži.

U ovom radu, pri izradi teorijskog djela rada korišteni su sadržaji preuzeti iz referencirane relevantne literature vezane uz VPN mreže te je nakon izrade praktičnog dijela rada opisan postupak proveden pri kreiranju i testiranju VPN mreže.

Ovaj završni rad sastoji se od pet poglavlja. Nakon prvog, uvodnog poglavlja, u drugom je poglavlju opisan način zaštite informacija i primjene VPN tehnologije. Isto tako, u drugom poglavlju su opisani i protokoli koji se primjenjuju u VPN mrežama, podjela VPN mreža te je objašnjen koncept rada na daljinu. U trećem poglavlju opisan je provedeni praktični primjer konfiguriranja VPN konekcije i postavki MikroTik usmjerivača. U četvrtom poglavlju provedena je analiza VPN mrežnog prometa uz primjenu Wireshark aplikacije te su opisani protokoli koji se koriste pri razmjeni podataka mrežom. U zaključnom, petom poglavlju rada, ukratko su navedeni osnovni razlozi primjene VPN mreža opisanih u radu.

2. VIRTUALNE PRIVATNE MREŽE (VPN)

Informacije koje se razmjenjuju mrežom potrebno je primjereno zaštititi. Uz same informacije, često su pod sigurnosnim rizikom od potencijalnih napada i različite mrežne aplikacije [8].

Pri razmatranju primjene mrežnih aplikacija, sigurnosni rizici obuhvaćaju slučajeve u kojima napadač može:

- izmijeniti vrijednost određenog zapisa u skrivenom HTML kodu,
- izmijeniti identifikaciju sesije kako bi mogao preuzeti sesiju od nekog drugog korisnika,
- obrisati zapise koji se uobičajeno bilježe prilikom pronalaska logičkog propusta pri obradi dobivenih podataka, a koji se kasnije mogu koristiti za napad,
- unositi podatke u određenu bazu podataka nakon dobivanja pristupa bazi.

Prilikom primjene mrežnih aplikacija često se mogu uočiti određeni propusti koji se u pravilu ne bi smjeli pojavljivati. Problemi mogu nastati u trenutku kada aplikacija mora izvršiti prihvaćanje i obradu rizičnog unosa. Zbog takvog unosa može doći do ugrožavanja pouzdanosti rada same aplikacije.

Uz navedeno, prisutno je još nekoliko dodatnih razloga nastanaka sigurnosnih rizika koji se pojavljuju zbog propusta vezanih za pouzdanost mrežnih aplikacija. Najznačajniji od njih je nedovoljno detaljno definiranje sigurnosnih mehanizama koje primjenjuju pojedine mrežne aplikacije, pri čemu često izostaje provedba detaljne provjere načina rada u svakom od mogućih primjera napada.

Sljedeći problem predstavlja činjenica da uslijed niza dostupnih razvojnih okruženja, svatko, pa čak i ako nema dostatno znanje o implementiranju sigurnosnih mehanizama, ima mogućnost izrađivanja Internet aplikacija, pa je problem takvih aplikacija upravo njihova ranjivost u slučaju potencijalnih sigurnosnih rizika. Uslijed ubrzanog nastanka različitih oblika sigurnosnih rizika, odnosno razotkrivanja postojećih propusta, povećava se mogućnost ugroze mrežnih aplikacija. Zbog toga postoji mogućnost da se pri primjeni mrežnih aplikacija naiđe i na poneki novi sigurnosni rizik koji je nastao naknadno.

Idući problem vezan je uz ograničenja koja se često odnose na raspoloživo vrijeme te na dostupne resurse pri izradi mrežnih aplikacija, pa se pri isporuci aplikacija mora voditi računa o navedenim ograničenjima.

Da bi se mrežne aplikaciju mogle adekvatno zaštititi primjenjuje se nekoliko osnovnih zaštitnih mehanizama. Takvi mehanizmi implementiraju se u aplikacije i primjenjuju u cilju povećanja sigurnosnih razina. Glavna namjena tih mehanizama je vezana uz mogućnost upravljanja korisničkim pristupom, kako ne bi došlo do neovlaštenog pristupa određenim korisničkim podacima i pojedinim funkcijama.

Nadalje, nužno je voditi računa i o sprječavanju unosa podataka od strane krajnjeg korisnika, koji time mogu djelovati na samu aplikaciju. Stoga je potrebno voditi računa i kontrolirati funkcionalnost mrežne aplikacije kako bi se aplikacija u potpunosti zaštitila od napada. Na posljetku, potrebno je osigurati upravljivost aplikacijom, pri čemu je administratoru sustava potrebno omogućiti nadzor nad konfiguracijom same aplikacije.

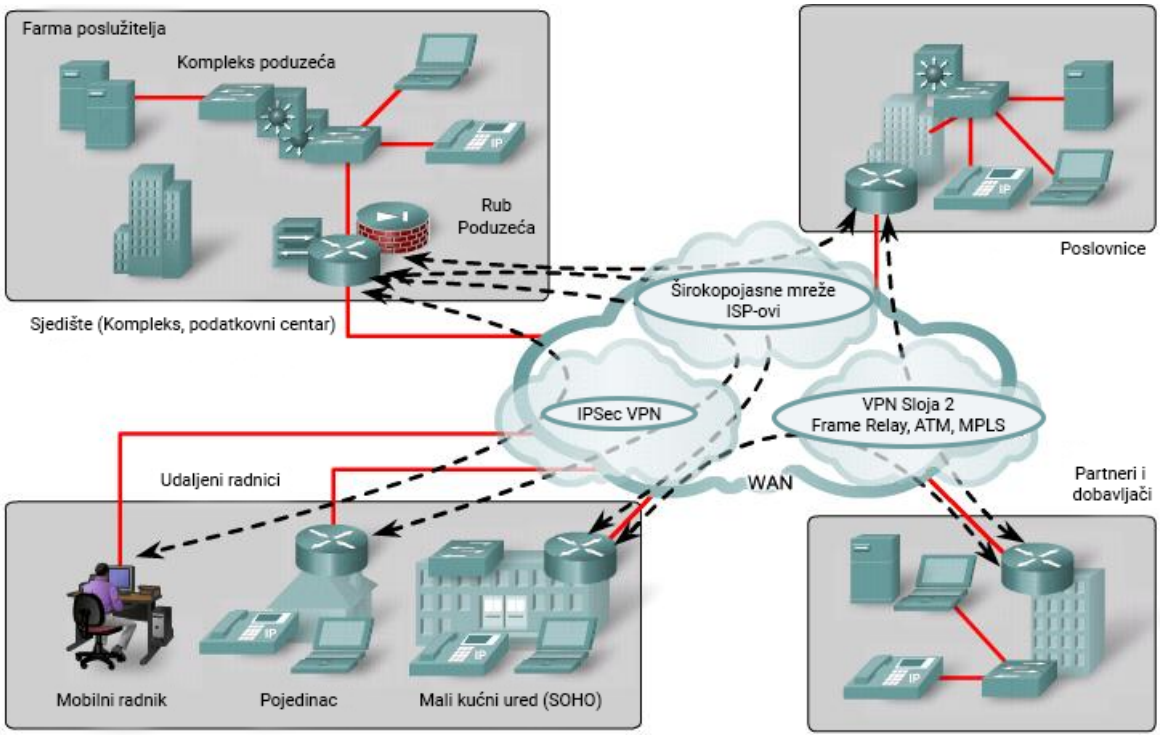
Jedan od mogućih načina napada na Internet aplikaciju je napad za koji je potrebno odgovarajuće predznanje o načinu rada njegovih zaštitnih mehanizama. Zbog toga se može osmisliti napad koji ima mogućnost zaobilaženja svih postojećih zaštitnih mehanizama. Kod većine mrežnih aplikacija se pri upravljanju mogu koristiti neki od sljedećih zaštitnih mehanizama, a to su prema [9]:

- upravljanje pristupom,
- upravljanje sesijom,
- autentikacija.

2.1. Primjena virtualnih privatnih mreža

Sve više tvrtki uviđa prednosti primjene VPN mreža jer one omogućuju udaljeni rad. S razvojem ICT tehnologija, omogućavanje rada na daljinu više ne predstavlja značajan problem kao što je to bilo ranije. Tada je bilo nužno ugraditi specijalnu opremu na udaljenu lokaciju (modemi, terminali) s kojom bi se omogućila tek ograničena pokretljivost (na jednoj fiksnoj udaljenoj lokaciji). Danas se podaci i razni multimedijski sadržaji mogu putem iste mrežne konekcije prenositi u stvarnom vremenu, bez obzira na fizičku lokaciju udaljenog čvora.

Rad na daljinu ne predstavlja samo rješenje kojim se može ostvariti određena ušteda u radu, već omogućuje neometani rad i dostupnost sustava čak i u slučaju određenih nepredviđenih situacija koje mogu nastupiti. Zbog neometanog izvršavanja zadataka potrebno je omogućiti rad sustava i u trenutcima vremenskih nepogoda, prirodnih katastrofa, prometnih gužvi i drugih nepredviđenih događaja koji bi mogli zaustaviti djelatnike da dođu na svoje radno mjesto. Upotrebljavanjem rada na daljinu, tvrtke omogućuju veću dostupnost svojih programskih rješenja unatoč različitim vanjskim čimbenicima [10].



Slika 2.1 Shema tipova udaljenih pristupa [12]

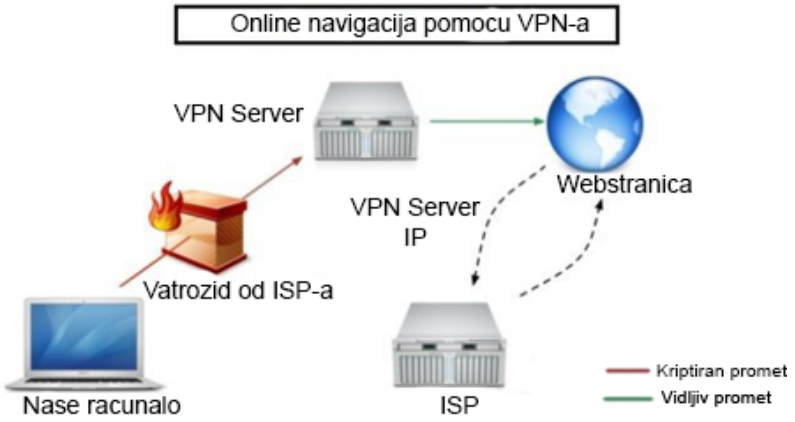
Shema na slici 2.1 prikazuje način povezivanja čvorova koji se nalaze na udaljenim lokacijama. Određene pristupne točke povezuju se sa sjedištem, a ostale sa različitim pristupnim točkama. Na primjer, djelatnik se od doma može povezati sa sjedištem tvrtke, a odvojena podružnica sa sjedištem te sa pristupnim točkama suradnika i dobavljača.

Pri uspostavljanju konekcije mogu se primijeniti [12]:

- starije metode poput ATM (*Asynchronous Transfer Mode*) tehnologije, *Frame Relay* tehnologije ili privatnih unajmljenih veza
- novije metode poput VPN-a koje koriste pristup Internetu putem postojećih konekcija.

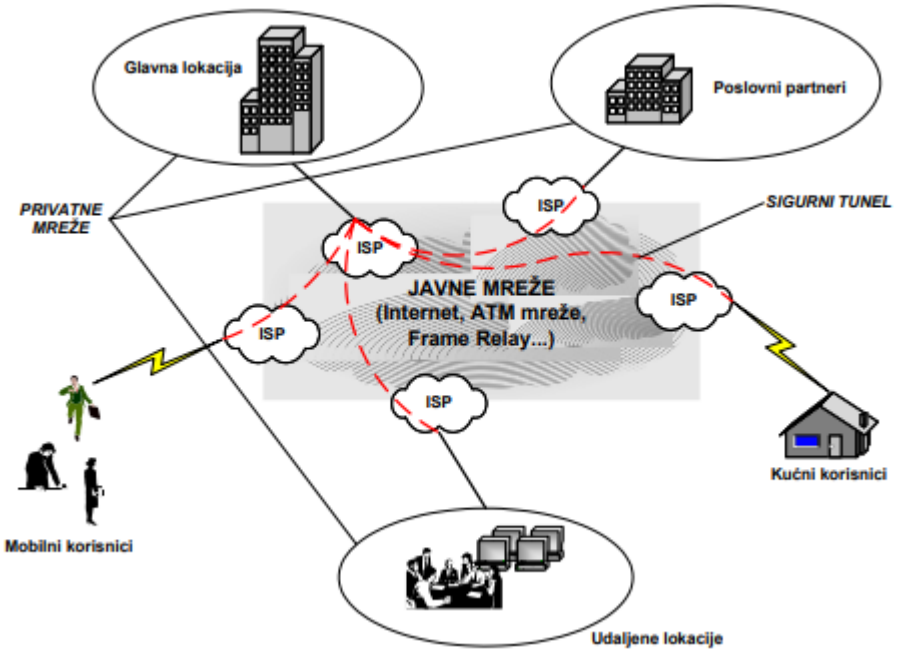
2.2. Značajke virtualnih privatnih mreža

U virtualnim privatnim mrežama koristi se kriptirani način komunikacije. VPN radi slično kao *proxy* servis jer pružatelj mrežnih usluga, odnosno ISP (engl. *Internet Service Provider*) vidi samo vezu s *proxy* serverom. Osnovna razlika je u tome što ISP može lako vidjeti zahtjeve od *proxy*-ja budući da ti zahtjevi nisu kriptirani, a to znači da je pri jednostavnom pretraživanju i dalje sve vidljivo. Slika 2.2 prikazuje funkcioniranje online navigacije s VPN-om.



Slika 2.2: Online navigacija s VPN-om [13]

U odnosu na privatne mreže koje koriste iznajmljene linije za slanje podataka, VPN putem javne mreže kreira sigurni kanal između umreženih krajnjih točaka. Slika 2.3 prikazuje različite mogućnosti primjene VPN tehnologije [14].



Slika 2.3: Mogućnosti korištenja VPN tehnologije [14]

2.3. Protokoli u virtualnim privatnim mrežama

Postoje četiri vrste protokola koje VPN pružatelji usluge nude, a to su PPTP, OpenVPN, Chamelenon i L2TP/IPsec.

PPTP protokol (engl. *Point to Point Tunneling Protoco*l) je među najjednostavnijim i najstarijim protokolima. Za enkripciju koristi 128-bitnu enkripciju. Većinu vremena je bio glavni izbor svim privatnim i poslovnim korisnicima zbog svoje brzine i sigurnosti. Iako je i dalje brz, više nije dovoljno siguran. Naknadno je otkriveno da sadrži određene sigurnosne propuste [15].

L2TP/IPsec protokol kombinira značajke L2TP (engl. *Layer 2 Tunnel Protoco*l) protokola i IPsec (engl. *Internet Protocol Securit*y) protokola koji se koristi za kriptiranje. Navedenom kombinacijom se dobiva malo sporiji protokol od PPTP-a, ali bitno sigurniji.

Ono što protokoli za kreiranje tunela ne omogućuju je zaštita podataka koji se razmjenjuju među udaljenim čvorovima. U cilju povećanja razine zaštite koriste se IPsec protokoli koji

predstavljaju najbolji odabir za sigurnu komunikaciju u mreži. IPSec je predstavljen kao skupina protokola za enkripciju te autentikaciju, koji omogućuje usklađeni rad različitih protokola [16].

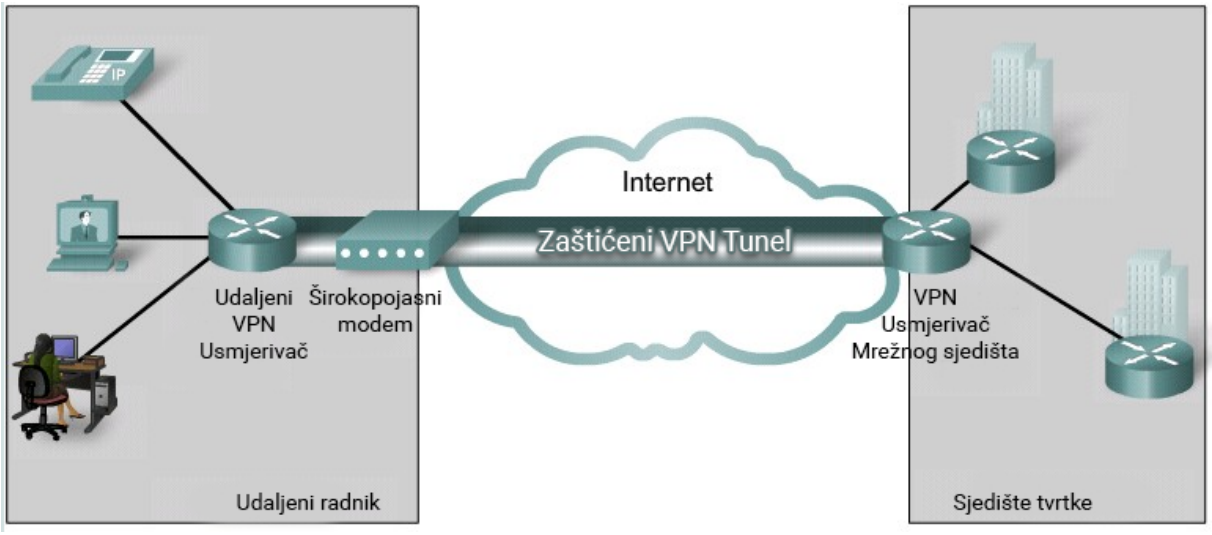
2.4. Podjela virtualnih privatnih mreža

Najsigurnija vrsta VPN-a naziva se *Secure VPN*. Riječ je o VPN-u koji koristi enkripciju nad podacima i autentifikaciju korisnika. Za navedeno koriste se algoritmi i protokoli kao što su SSL, IPsec protokol, TLS, i L2TP. VPN ima mogućnost pristupa mreži samo uz autentifikaciju, no komunikacija ne smije biti kriptirana. Glavni mehanizmi sigurnosti *Secure VPN*-a trebaju biti jednaki u svim mrežnim segmentima, odnosno potreban je dogovor oko protokola i sigurnosti [15].

Druga vrsta VPN-a jest *Trusted VPN*. Pružatelj usluge kod *Trusted VPN*-a sve modificira. Glavni razlog primjene *Trusted VPN*-a jest da krajnji korisnik ima povjerenja u pružatelja usluge da će ispravno uspostaviti vezu u VPN-u kako bi povezanost bila što sigurnija, a krajnji korisnik zaštićen. Samo pružatelj usluge ima informacije o krajnjem korisniku i njegovom pretraživanju na Internetu. Nitko osim njega nema informacije kada se korisnik spoji na VPN server, ali pri tome korisnik ne zna koja se zaštita koristi i kako je ona implementirana [15].

2.5. Virtualne privatne mreže i rad na daljinu

Na lokacijama udaljenih korisnika sve se češće koriste videokonferencije i VoIP (engl. *Voice over Internet Protocol*) pri radu [12]. Kako bi rad na daljinu bio omogućen, potrebno je ostvariti određene preduvjete. Osnovni preduvjet vezan je uz primjenu komunikacijskih linkova veće propusnosti koje omogućuju žične ili bežične širokopojasne pristupne tehnologije. Kako bi uspostavljanje konekcije između udaljenih lokacija bilo uspješno, potrebno je osigurati i određenu opremu.



Slika 2.4 Shema primjera VPN veze [12]

Komponente koje su potrebne na lokaciji udaljenog korisnika:

- računalo (stolno ili prijenosno), internetski pristup, VPN klijent ili usmjerivač

Komponente koje su potrebne na lokaciji tvrtke:

- mrežni uređaji za agregaciju, autentikaciju i terminaciju konekcija virtualnih privatnih mreža te usmjerivači

Pri povezivanju udaljenih lokacija koristi se javno dostupna internetska mreža, pa u kontekstu omogućavanja privatne komunikacije kroz javnu mrežu ključnu ulogu imaju virtualne privatne mreže.

VPN je vezan uz sljedeće značajke:

- očuvanje povjerljivosti (engl. *confidentiality*) podataka – kriptiranje podataka
- očuvanje integriteta (engl. *integrity*) podataka – generiranje *hash* funkcije
- onemogućavanje dupliranja (engl. *anti-replay*) paketa – pridjeljivanje rednog broja paketima.
- autentikaciju (engl. *authentication*) – PSK moduliranje ili digitalno potpisivanje.

Osnovni razlozi primjene virtualnih privatnih mreža vezani su uz ostvarivanje virtualne konekcije pomoću koje se međusobno povezuju udaljeni korisnici te uz ostvarivanje privatne komunikacije uz kriptiranje podataka.

Prednosti virtualnih privatnih mreža su [18]:

- mogućnost korištenje standardnog internetskog pristupa
- primjena algoritama za enkripciju podataka i autentikaciju korisnika
- dodavanje novih korisnika bez izmijene postojeće infrastrukture.

U primjeni su dvije vrste pristupnih rješenja, a to su [18]:

- s lokacije na lokaciju (engl. *site-to-site*) – za povezivanje udaljenih lokacija sa centralnima uz primjenu virtualnih privatnih mreža
- „udaljeni pristup“ (engl. *remote access*) – za povezivanje pojedinačnih krajnjih čvorova na centralnu lokaciju.

Topologija virtualnih privatnih mreža sastoji se od [18]:

- računalne mreže
- pristupnih uređaja koji provode usmjeravanje i enkripciju te dekriptiranje mrežnog prometa
- internetske konekcije
- softvera kojim se upravlja VPN konekcijama.

Temelj djelotvornosti VPN-a je privatnost podataka i sigurnost, odnosno zaštita podataka enkapsulacijom i/ili enkripcijom. Enkapsulacijom se omotava postojeći paket dodatnim slojem zaštite. Kada paket koji je enkapsuliran stigne na svoj cilj, vrši se raspakiravanje paketa i taj paket se prosljeđuje na konačno odredište. Cijeli proces enkapsulacije, prijenosa i raspakiravanja naziva se tuneliranjem.

Virtualne privatne mreže koriste sljedeće metode tuneliranja i kriptiranja mrežnog prometa zbog uspostavljanja sigurne privatne konekcije s jednog na drugi krak mreže kroz javnu Internetsku mrežu. Sigurne VPN veze se temelje na povjerljivosti, integritetu podataka i autentikaciji.

- Povjerljivost - zaštita podataka od prisluškivanja, uz primjenu metoda enkapsulacije i enkripcije.
- Autentikacija – način provjere komunicira li se zbilja s onim stranama za koje se pretpostavlja. Pri autentifikaciji koriste se digitalni certifikati i ključevi.
- Integritet - VPN koristi *hash* funkcije kako bi se provjerilo je li došlo do promjene podataka pri prijenosu.

Pri tuneliranju koristi se javna internetska mreža kako bi se omogućio prijenos korisničkih podataka kao da se razmjenjuju unutar privatne mreže. Početni paket se omotava dodatnim zaglavljem koje očitavaju usmjerivači.

3. KREIRANJE AD-HOC VIRTUALNE PRIVATNE MREŽE

Virtualne privatne *ad hoc* mreže obuhvaćaju koncept koji međusobno povezuje virtualizaciju mreže i *ad hoc* mrežne tehnike kako bi se ostvarila transparentna, pouzdana i samoorganizirana usluga. Riječ je o virtualnoj mrežnoj strukturi koja koristi tehnike *ad hoc* umrežavanja kako bi se omogućilo sigurno povezivanje čvorova u mrežu [19].

U nastavku je opisano kreiranje VPN-a pomoću operacijskog sustava *Microsoft Windows XP* s ciljem *ad hoc* povezivanja udaljenih računala u lokalnu mrežu putem Interneta, odnosno javne mreže. VPN prosljeđuje podatke kroz javnu mrežu putem kreiranih tunela. Naime, pri slanju i primanju podataka među računalima koja nisu međusobno izravno povezana u mrežu, prvo se mrežni promet kriptira, pa se zatim šalje pomoću Interneta do odredišnog računala koje se nalazi u virtualnoj mreži, a koje onda taj promet dekriptira [20].

Postoje različita VPN rješenja (npr. različita softverska rješenja, usluge operatera i dr.), a u nastavku je prikazano kreiranje VPN-a na klijentu uz pomoć ugrađenog servisa *Windows* sustava.

Cjelokupni proces stvaranja virtualne privatne mreže može se podijeliti u tri dijela:

- konfiguriranje usmjerivača – obuhvaća mrežne postavke usmjerivača
- konfiguriranje servera – obuhvaća postavke servera za VPN
- konfiguriranje klijenta – obuhvaća konfiguriranje udaljenih računala s kojima se želi povezati.

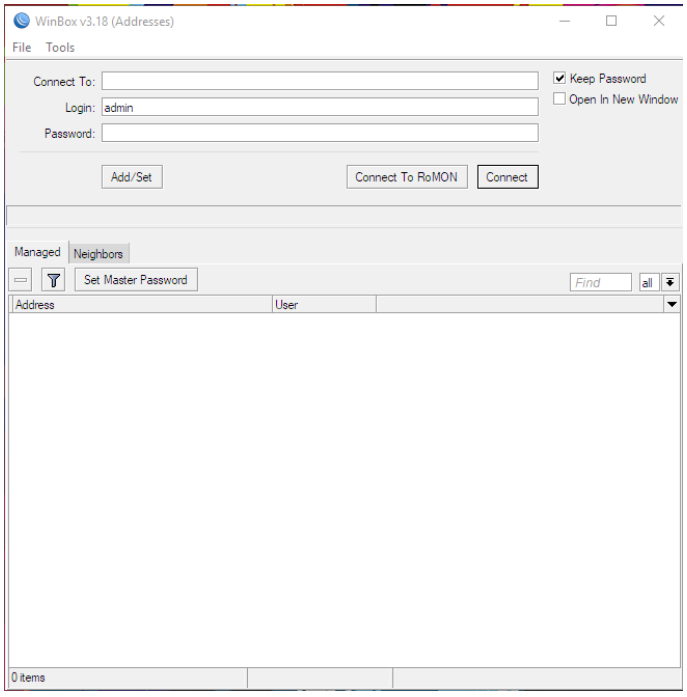
3.1. Postupak konfiguracije

Klasična lokalna mreža sastoji se od međusobno povezanih krajnjih uređaja putem odgovarajućih mrežnih uređaja (npr. usmjerivača). U toj mreži određeni čvor ima ulogu poslužitelja. Jedini i glavni uvjet da taj čvor izvršava svoju funkciju jest da bude konstanto dostupan te da sadrži odgovarajući operacijski sustav.

Kod manjih lokalnih mreža računala i uređaji često nemaju dodijeljenu statičnu IP adresu nego dinamičku. DNS server na strani pružatelja Internetskih usluga im dodjeljuje tu adresu za vrijeme povezivanja na Internet. Za konstantne konekcije dinamička adresa traje najčešće 24 sata. Kako bi se izbjeglo konstantno traženje IP adrese kod udaljene mreže, može se koristiti besplatna usluga Internetskog servisa (npr. https://dyn.com/dns/) koji javlja adresu lokalne udaljene mreže. Na ovoj web stranici potrebno je stvoriti korisnički račun (on je besplatan), te se mora odrediti korisničko ime, ime poddomene, lozinka. Navedeni podaci se nakon toga upisuju u postavke usmjerivača.

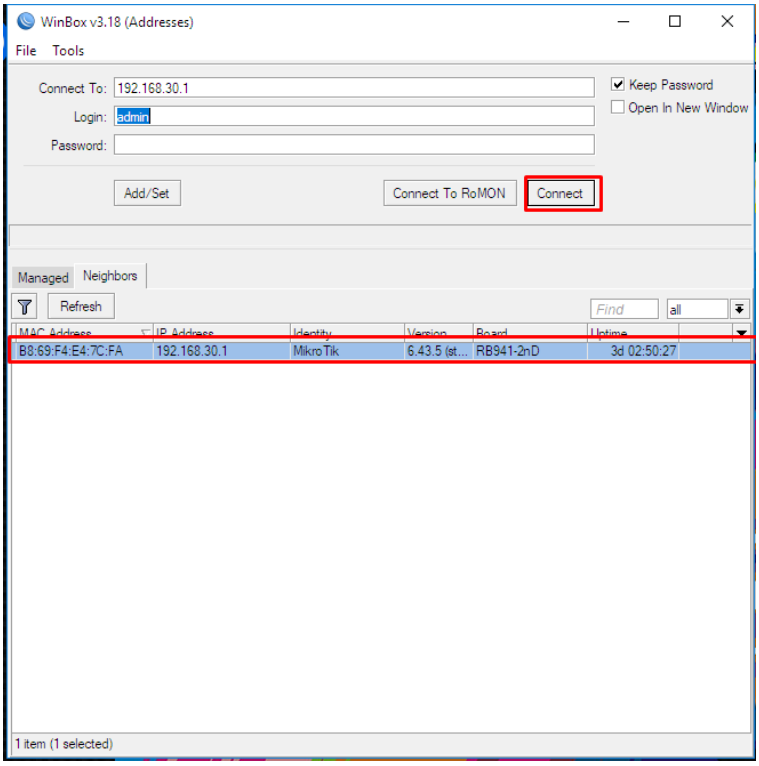
Da bi se upisale sve potrebne i ispravne postavke u usmjerivaču, potrebno je pokrenuti odgovarajuću aplikaciju i pristupiti postavkama usmjerivača. Tamo se upisuje korisničko ime i pristupna lozinka. U ovom radu je korišten MikroTik HAP-LITE RB941-2ND-TC Access Point, a za njegovo konfiguriranje program WinBox, koji se može pronaći na sljedećoj stranici: https://MikroTik.com/download [21].

Prvi korak za postavljanje usmjerivača je preuzimanje programa *WinBox* i njegovo pokretanje.



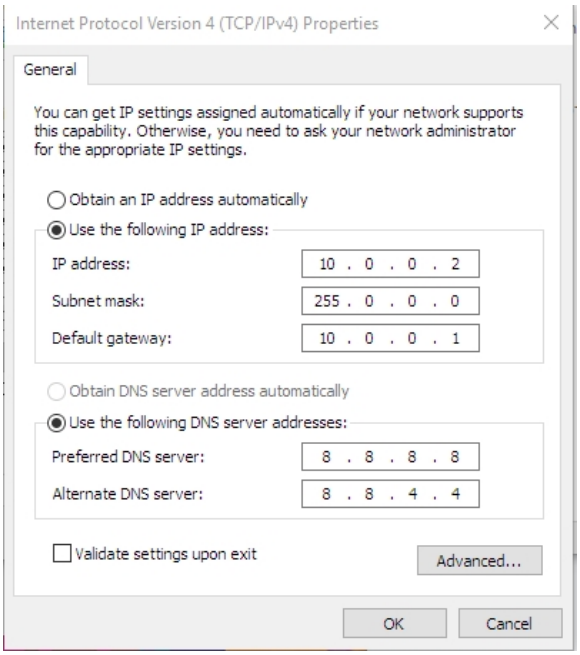
Slika 3.1 Prikaz prozora WinBoxa prilikom prvog pokretanja

Nakon pokretanja *WinBox* programa potrebno je odabrati opciju *Neighbours* u izborniku, te zatim označiti MAC adresu MikroTik usmjerivača i stisnuti gumb *Connect*.



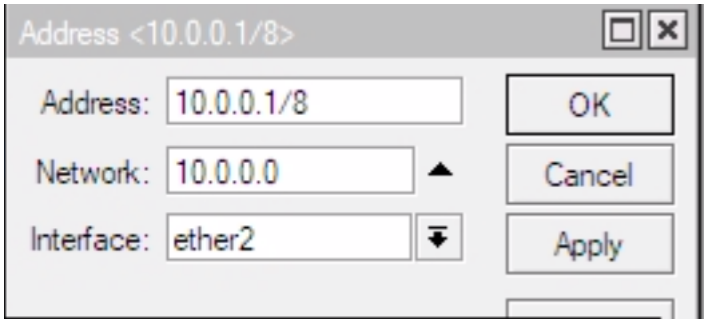
Slika 3.2 Konfigurator MikroTik usmjerivača

Računalu je dodijeljena IP adresa: 10.0.0.2, prema prikazu slike 3.3.



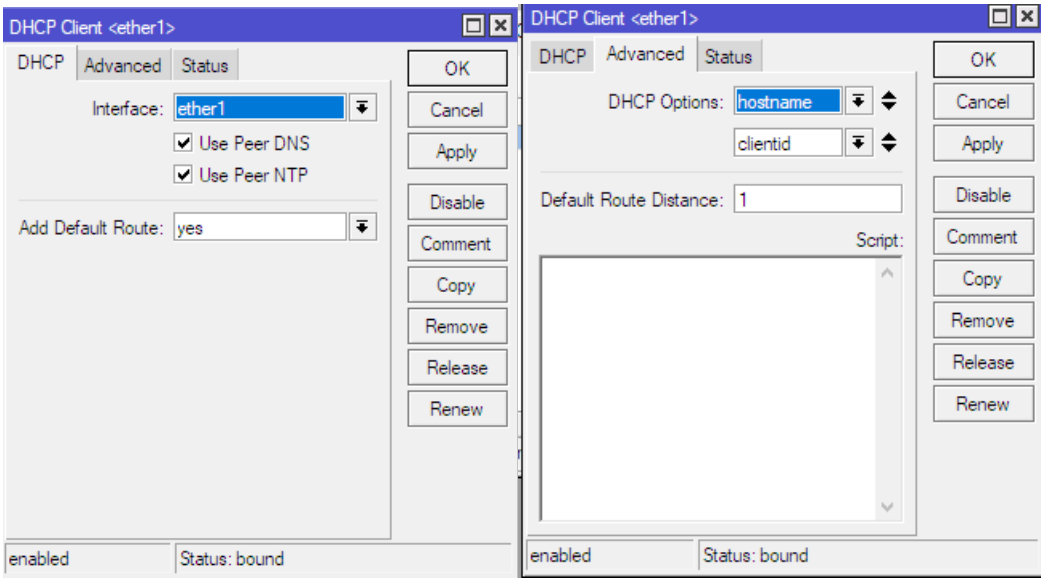
Slika 3.3 Dodjeljivanje IP adrese

Zatim je potrebno odabrati sučelje *ether2* i dodijeliti mu IP adresu. U izborniku *Winbox*-a potrebno je odabrati opciju *Addresses* te unutar izbornika *Adress List* upisati odabranu adresu.



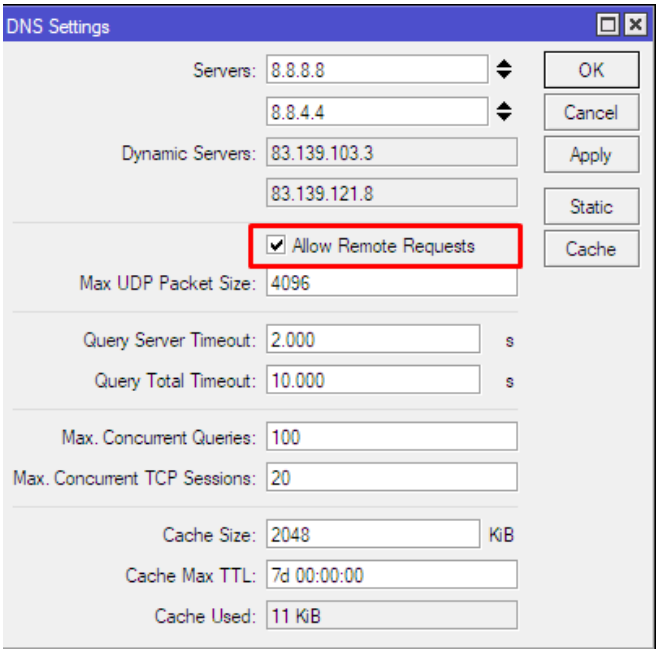
Slika 3.4 Adresiranje aktivnog sučelja usmjerivača

Zatim je potrebno konfigurirati DHCP klijenta na *ether1* sučelju usmjerivača, prema prikazu na slici 3.5.



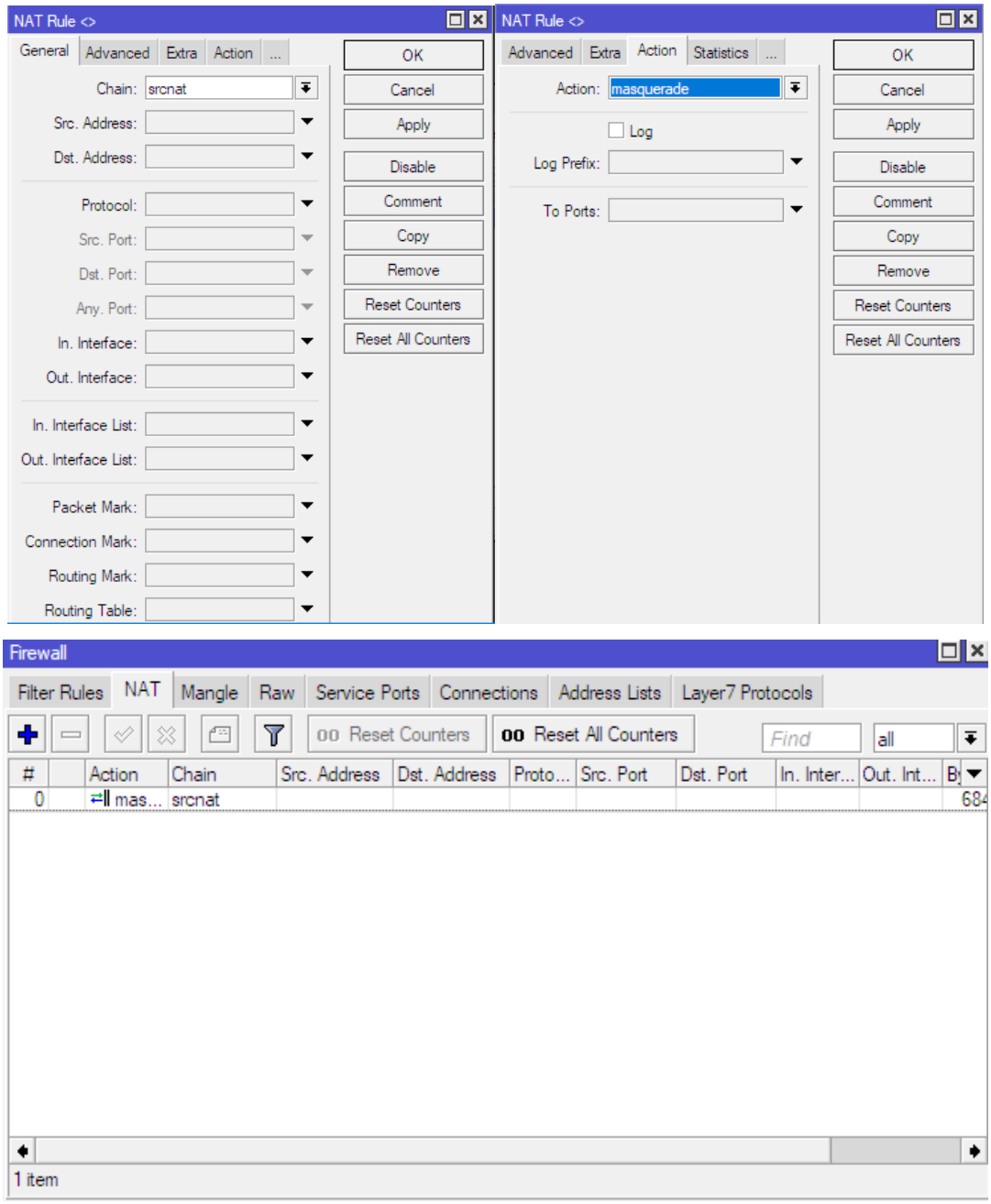
Slika 3.5 Prikaz postavki DHCP klijenta

Nakon konfiguriranja DHCP klijenta, potrebno je konfigurirati dodatne postavke usmjerivača. Za početak je potrebno u *DNS Settings* označiti opciju *Allow Remote Requests* (slika 3.6).



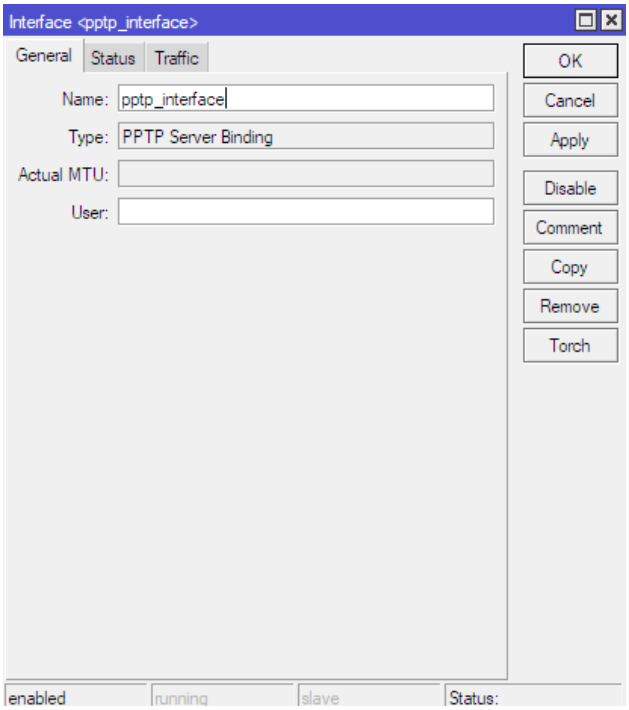
Slika 3.6 Prikaz DNS postavki

Zatim je potrebno pokrenuti postupak maskiranja IP adresa i definirati pravila prevođenja IP adresa iz lokalnih u javne. Iz izbornika *IP* u *Winbox*-u potrebno je odabrati *IP*, zatim *Firewall*, opciju *NAT* i dodati novo pravilo. Unutar kartice *General* treba postaviti *Chain* na *srcnat* i potvrditi. U idućem koraku untar kartice *Action* potrebno je dodati opciju *Masquerade* i potvrditi ju (slika 3.7).



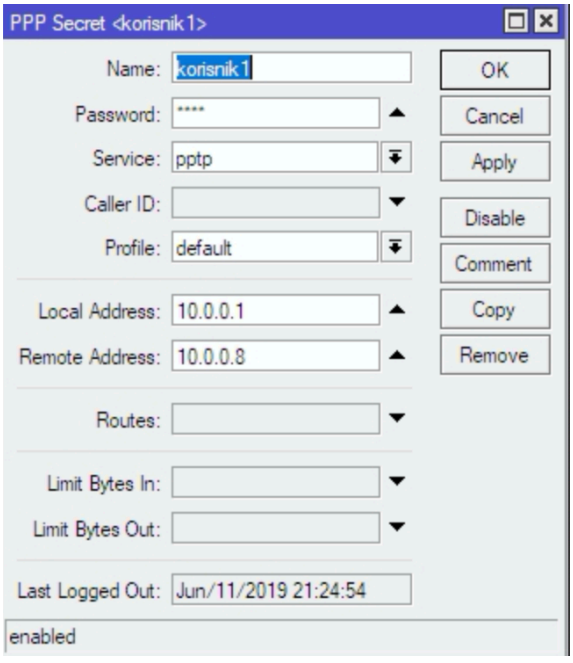
Slika 3.7 Dodavanje pravila za prevođenje IP adresa

U narednom koraku potrebno je konfigurirati PPTP server na usmjerivaču. Iz izbornika *PPP* u *Winbox*-u potrebno je odabrati opciju *PPTP Server Binding*, kao na slici 3.8 Za naziv je odabran *pptp_interface*.



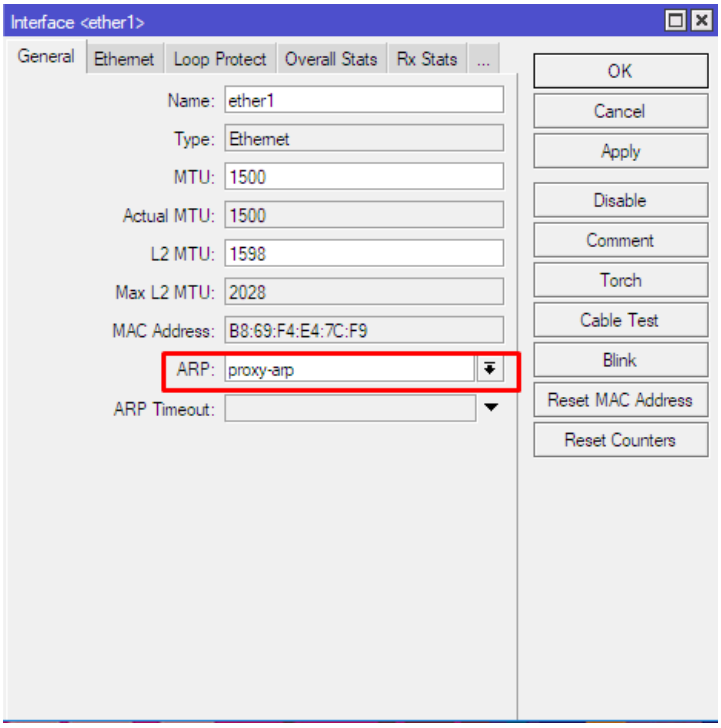
Slika 3.8 Definiranje PPTP server sucelja

Zatim je potrebno u izborniku *PPP* odabrati karticu *Secrets*, gdje se nalazi lokalna baza PPP korisnika i njihovih oznaka. U tom izborniku potrebno je definirati korisnike koji će se moći povezati na VPN. Potrebno je unijeti ime, lozinku, za uslugu odabirati *pptp*, lokalni adresu i adresu udaljenog čvora (slika 3.9).



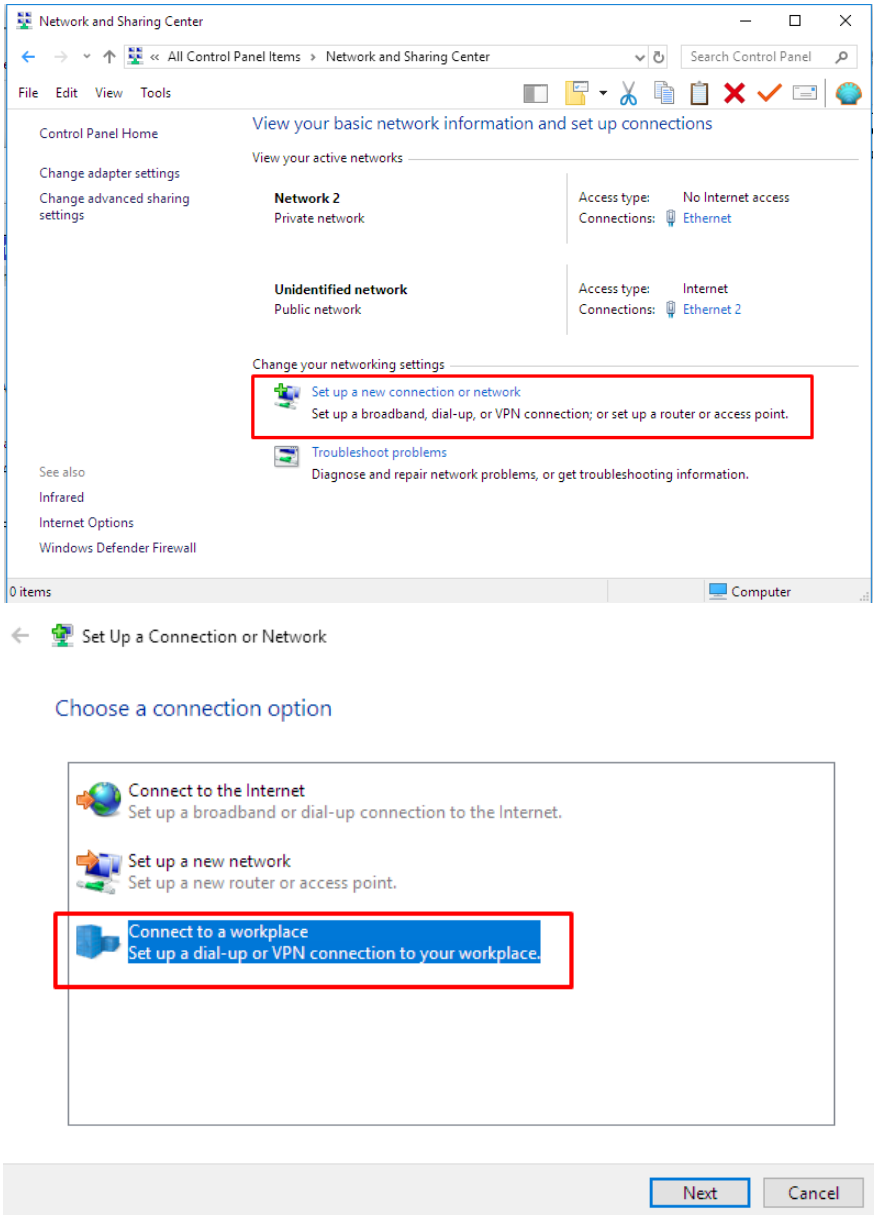
Slika 3.9 Prikaz postavki u izborniku PPP Secret

Idući korak je konfiguriranje *proxy arp* funkcije na usmjerivaču kojom se usmjerivač javlja na ARP zahtjeve namijenjene nekom uređaju u mreži, preuzimajući zadaću daljnjeg usmjeravanja paketa kroz mrežu. Iz izbornika *Interface List* potrebno je odabrati *ether1*, a unutar *ether1* opciju *proxy arp* (slika 3.10).



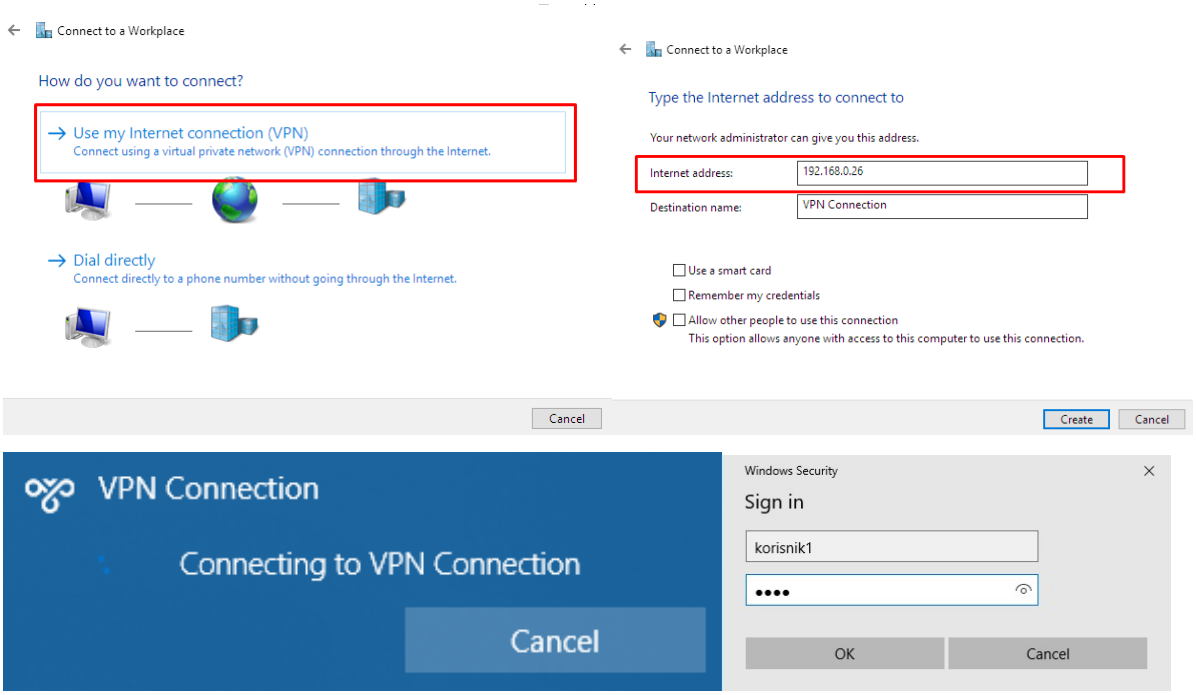
Slika 3.10 Proxy arp na sučelju usmjerivača

Idućih nekoliko koraka potrebno je provesti u *Windows* operacijskom sustavu, gdje se vrši povezivanje na VPN. Nakon otvaranja izbornika *Start* potrebno je otvoriti *Control Panel*, a zatim u *Control Panel*-u odabirati opciju *Network and Sharing Center* te opciju *Set up a Connection or network* (slika 3.11).



Slika 3.11 Control Panel izbornik

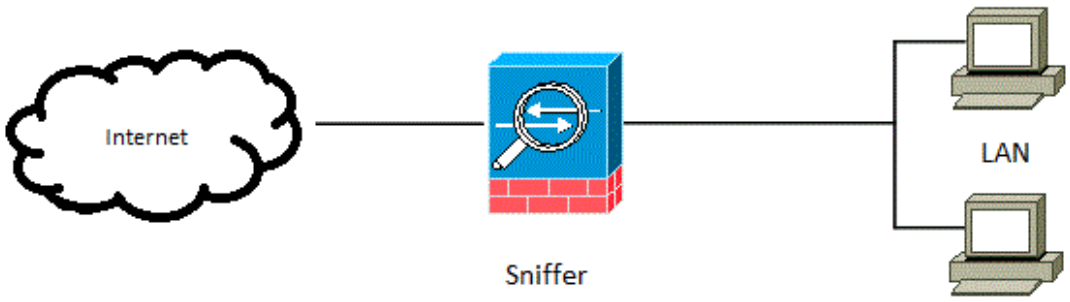
Nakon toga, potrebno je odabrati opciju *Connect to a workplace*, zatim *Use my Internet connection (VPN)* te kao Internet adresu upisati IP adresu 192.168.0.26, odabrati *Next* i ulogirati se s podacima kreiranim u *Winbox*-u (slika 3.12).



Slika 3.12 Povezivanje na kreirani VPN

4. ANALIZA PROMETA VIRTUALNE PRIVATNE MREŽE

Analiza mrežnog prometa je postupak kojim se mrežni paketi podvrgavaju analizi. Presretanje paketa implicira njihovo čitanje uz primjenu odgovarajuće aplikacije.



Slika 4.1 Pozicija sniffera unutar mreže

Dohvaćeni paket se nakon njegovog snimanja i lokalnog registriranja prosljeđuje na odredište. Promet u mreži se samo snima, bez izmjene ili bilo kakvog blokiranja.

```
0000  33 33 00 01 00 03 4c cc  6a 62 91 04 86 dd 60 01   33····L· jb····`·
0010  fe eb 00 1e 11 01 fe 80  00 00 00 00 00 00 fd 49   ········ ·······I
0020  d8 37 c6 eb d4 a9 ff 02  00 00 00 00 00 00 00 00   ·7······ ········
0030  00 00 00 01 00 03 e3 57  14 eb 00 1e 6e ce cf 0d   ·······W ····n···
0040  00 00 00 01 00 00 00 00  00 00 04 77 70 61 64 00   ········ ···wpad·
0050  00 01 00 01                                       ····
```

Slika 4.2 Izgled nedekodiranog paketa

Softver za analizu mrežnog prometa naziva se analizator paketa ili „*sniffer*“. Takav alat ima svojstvo prikazivanja paketa bez informacijskih zaglavlja (eng. *header*). Oni mogu dešifrirati informacije koje su specifične za pojedini protokol te ih mogu prikazati u čitljivom obliku. Analizatori paketa mogu sav promet snimati na jedan od dva načina. Prvi način je pasivno osluškivanje više odredišnih poruka (npr. bežični mrežni promet), dok je drugi način presretanje prometa.

Postoje također dodatne mogućnosti alata, a neke od tih mogućnosti su:

- automatsko pronalaženje pogreške u prijenosu
- pronalaženje uzroka pogreške
- prikazivanje dobivenih podataka u grafičkom obliku (količina prometa, vremenski grafovi…)
- stvaranje ispitnih paketa koji mogu biti ispravni i neispravni (da bi se testirala ispravnost prijenosa i mogućnost oporavka od pogreške).

Postoje dvije vrste rješenja, a ona mogu biti softverska ili hardverska. Softverska rješenja su uobičajeno šire primjenjiva te mogu analizirati niz različitih protokola. Koristi ih se da bi se otkrio uzrok određenih nepravilnosti pri odvijanju komunikacijskih procesa. Hardverska rješenja imaju mogućnost jako brzo analizirati mrežni promet, a umanjuju mogućnost mijenjanja mrežnog prometa uslijed ispitivanja.

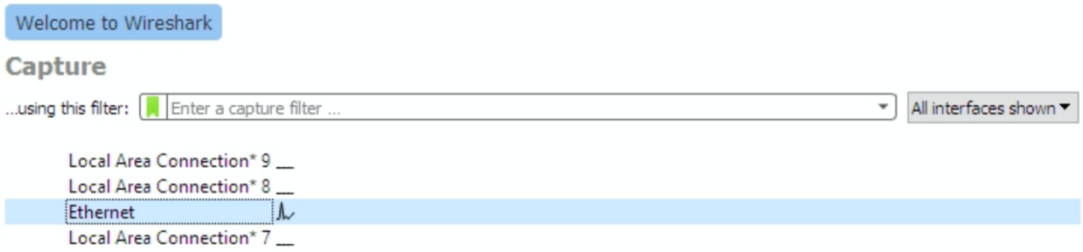
Primjeri korištenja analizatora su:

- kontrola podataka u prijenosu
- akumulacija statističkog mrežnog prometa
- otkrivanje pokušaja upada u neki sustav
- otkrivanje mrežnih pogrešaka
- izoliranje sustava od mrežnih kvarova.

4.1. Primjena Wireshark mrežnog analizatora

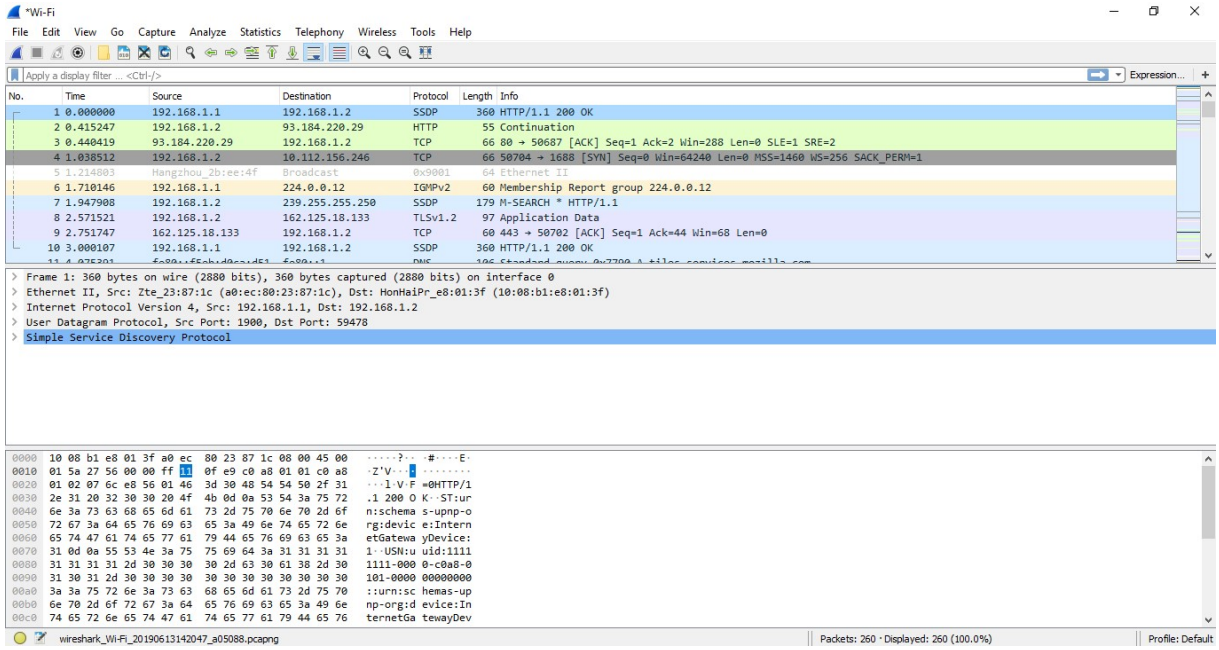
Wireshark je besplatni *open source* softver za analizu prometa. Njegova trenutna inačica je 2.6.1 (v2.6.1-0-g860a78b3) objavljena 2018. godine. Softver je dostupan za sve operacijske sustave, a u ovom radu korištena je inačica za *Windows 10* operacijski sustav.

Prvi korak dohvaćanja prometa je odabir mrežnog sučelja za snimanje. *Wireshark* automatski prepoznaje sučelja i nudi ih korisniku. Nakon odabira sučelja, započinje snimanje.



Slika 4.3 Prikaz mogućnosti snimanja

Prije snimanja postoji mogućnost odabira različitih opcija unutar *Wireshark*-a (slika 4.3). Nakon postavljanja opcija, softver započinje snimanje.



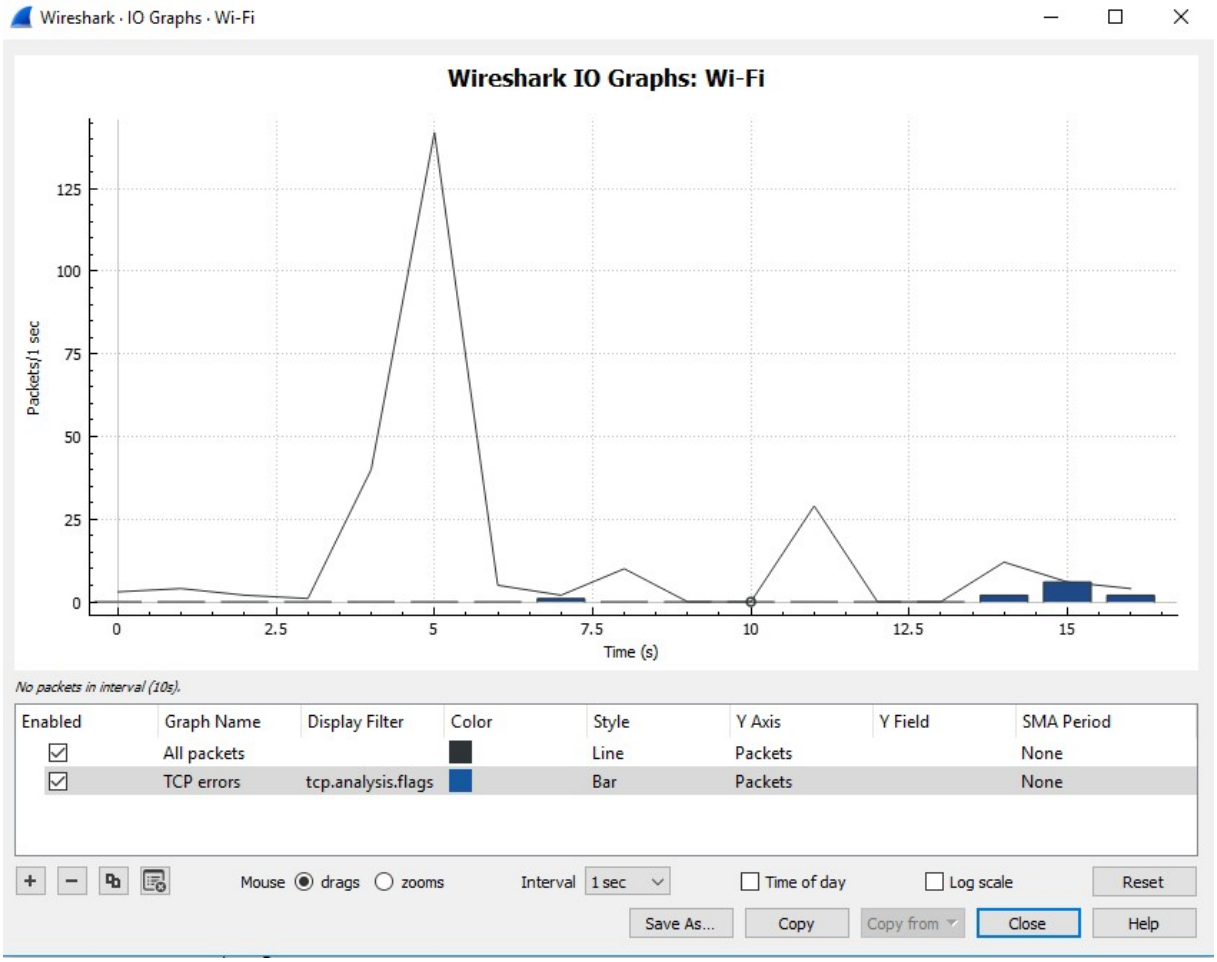
Slika 4.4 Prikaz snimljenih paketa

Prikazani paketi su samo jedan dio mrežnog prometa koji se koriste ukoliko postoji problem koji se želi detaljno ispitati. *Wireshark* nudi mogućnost sumiranja mrežnog prometa, što je ujedno i najkorisnija opcija ovog softvera. Neki od parametara prilikom sumiranja ukupnog prometa su:

- filtriranje prometa po nekoj definiranoj ciljnoj točki

- grafičko prikazivanje i raspodjela prometa prema protokolu
- hijerarhijsko prikazivanje protokola
- srednje vrijeme odziva nekog servisa.

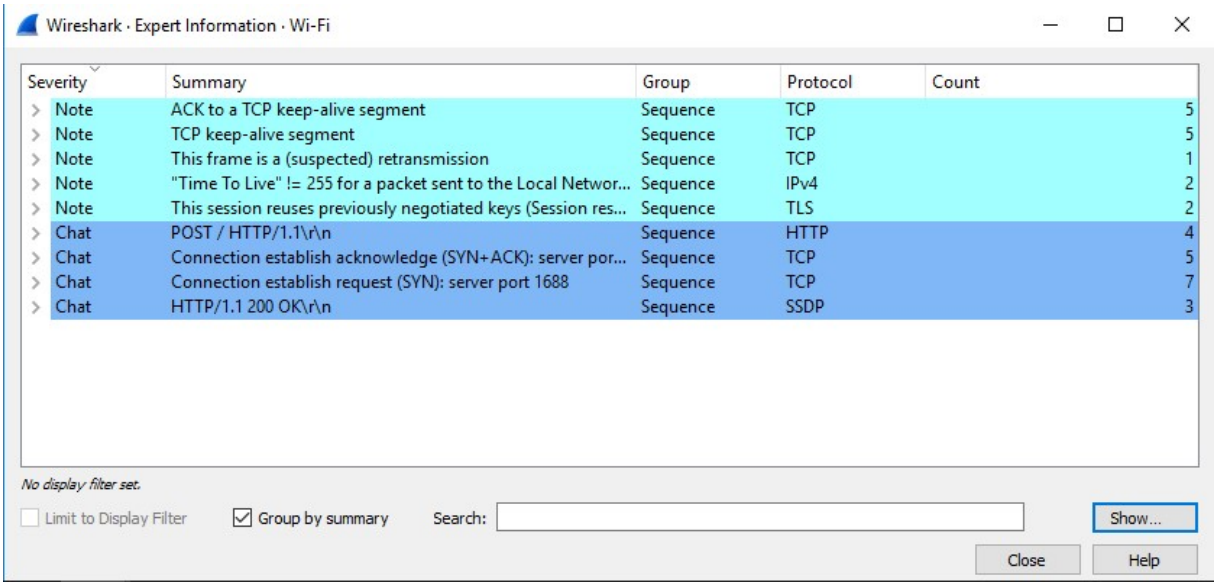
Wireshark također može prikazivati statističke podatke. Glavni primjer toga je da se za HTTP protokol može računati opterećenje po IP adresama. Isto tako, za TCP protok se može prikazati *Round Trip Time* (RTT) graf.



Slika 4.5 Grafički prikaz sumiranog prometa

Također se može analizirati sumirani promet, a neki od alata su:

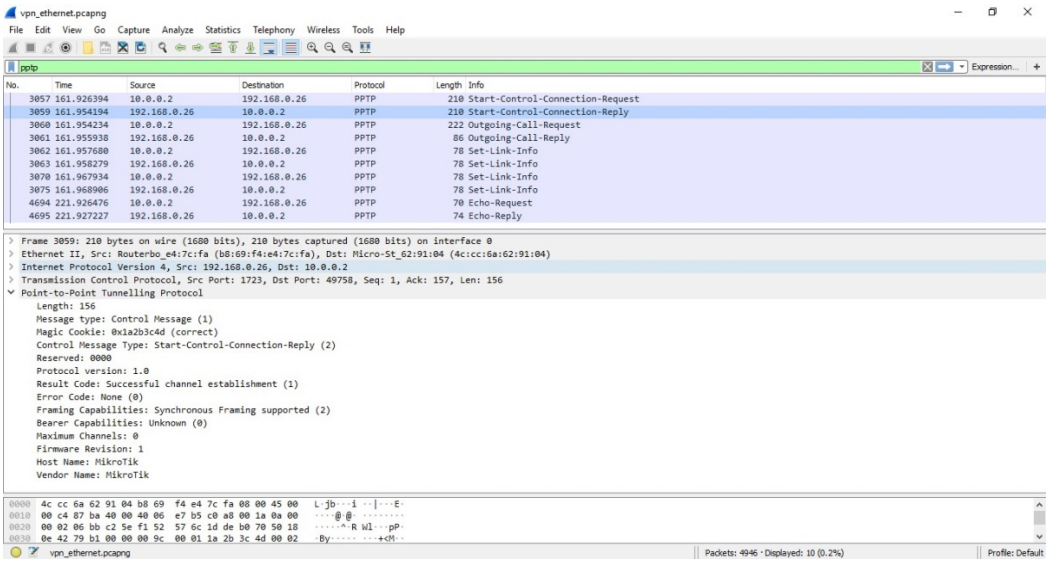
- praćenje upita i odgovora između neka određena dva čvora
- dešifriranje određenog mrežnog paketa
- prikazivanje relevantnih podataka - relevantni podaci predstavljaju sumirani prikaz podataka o određenim defektima i upozorenjima o protokolima (slika 4.6.).



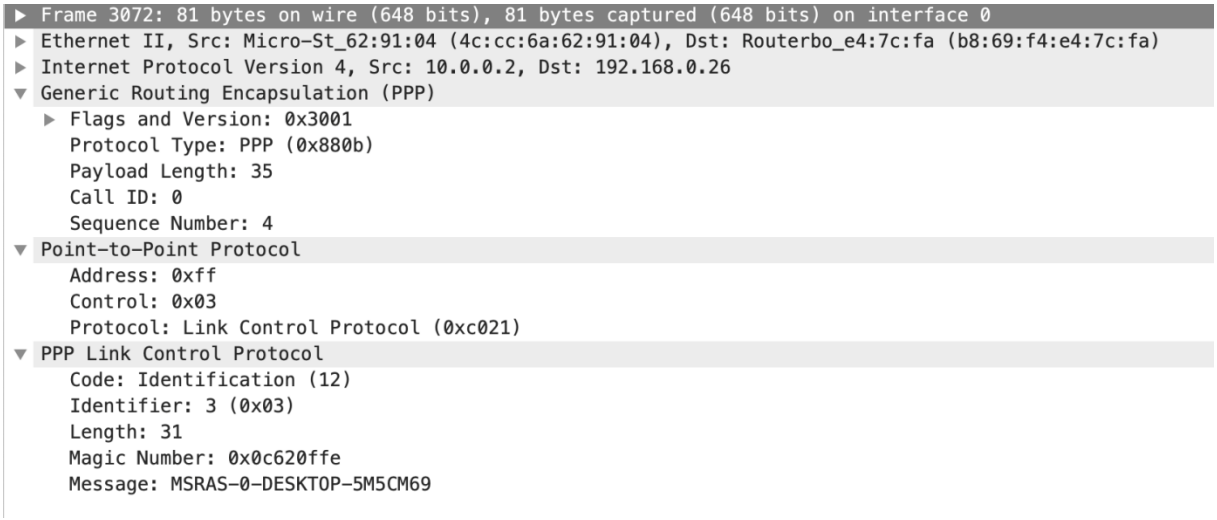
Slika 4.6 Prikaz relevantnih podataka

4.2. Analiza mrežnog prometa u kreiranoj virtualnoj privatnoj mreži

Prilikom snimanja VPN prometa pomoću *Wireshark*-a potrebno je napomenuti da se analiza provodi za PPTP, TCP i PPP protokole. Na slici 4.7 može se primijetiti da se mrežni promet odvija uz primjenu IP protokola verzije 4, zatim TCP protokola te PPTP protokola. Kod PPTP protokola, opcija *lenght* označava dužinu poruke koja se šalje, dok je *magic cookie* znak podatka koji se razmjenjuje između poslužitelja i klijenta, a pritom se koristi za praćenje, autentičnost i obavještavanje klijenta u sustavu o prisutnosti poslužitelja. Razlikuje se od običnog paketa podataka jer ne sadrži čitljive podatke, samo informacije o ruti paketa uz primjenu kojih se može doći do poslužitelja. Također je moguće vidjeti da se šalje zahtjev za uspostavu konekcije i odgovor MikroTik-a na taj zahtjev. PPP protokol se koristi za prijenos IP i drugih paketa kroz kreirani link. Paket može biti enkapsuliran i unutar PPPoE zaglavlja koje koriste mnogi pružatelji Internetskih usluga za širokopojasni pristup Internetu (slika 4.8).

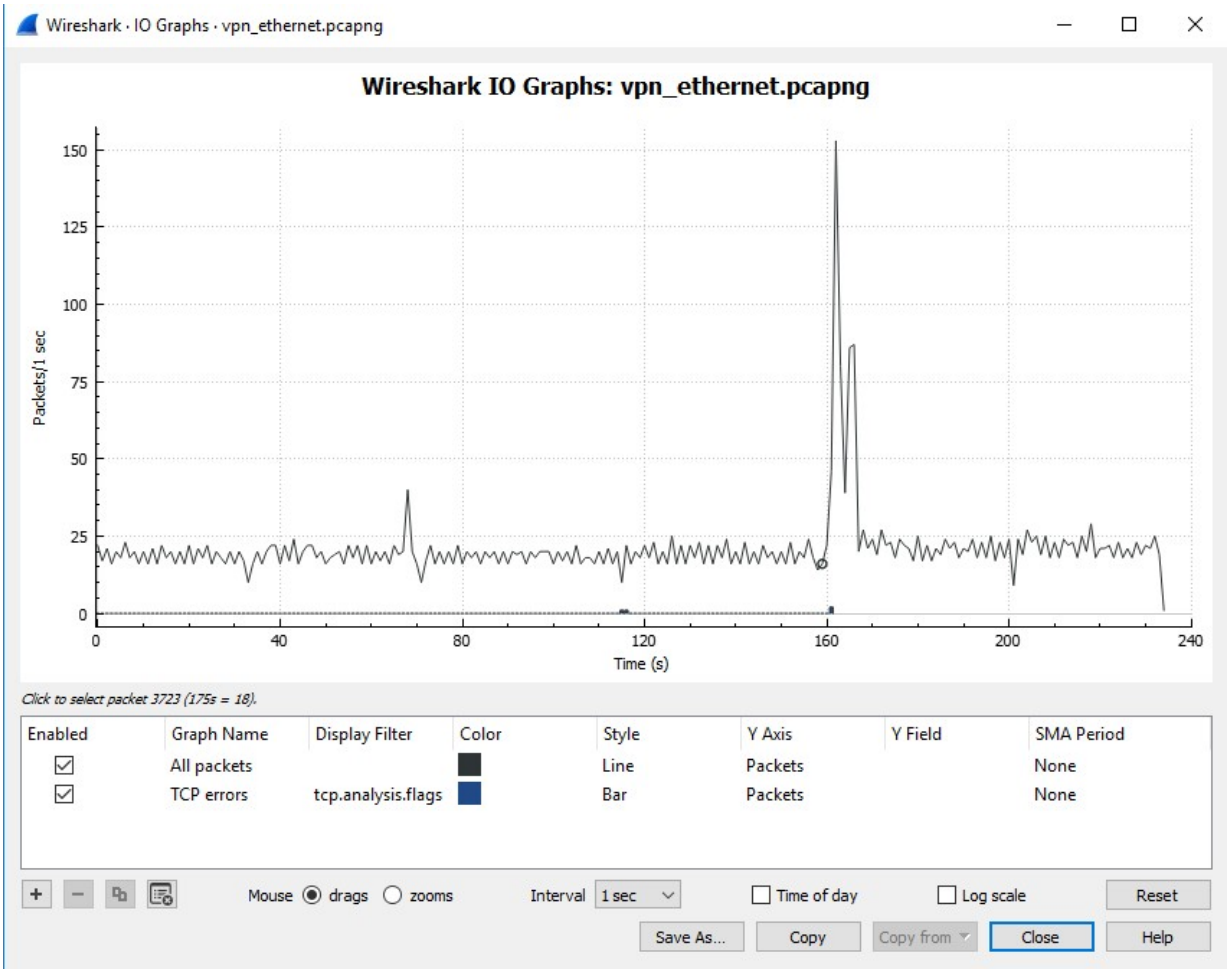


Slika 4.7 Prikaz snimljenih paketa uz korištenje VPN-a



Slika 4.8 Opis sadržaja PPP paketa

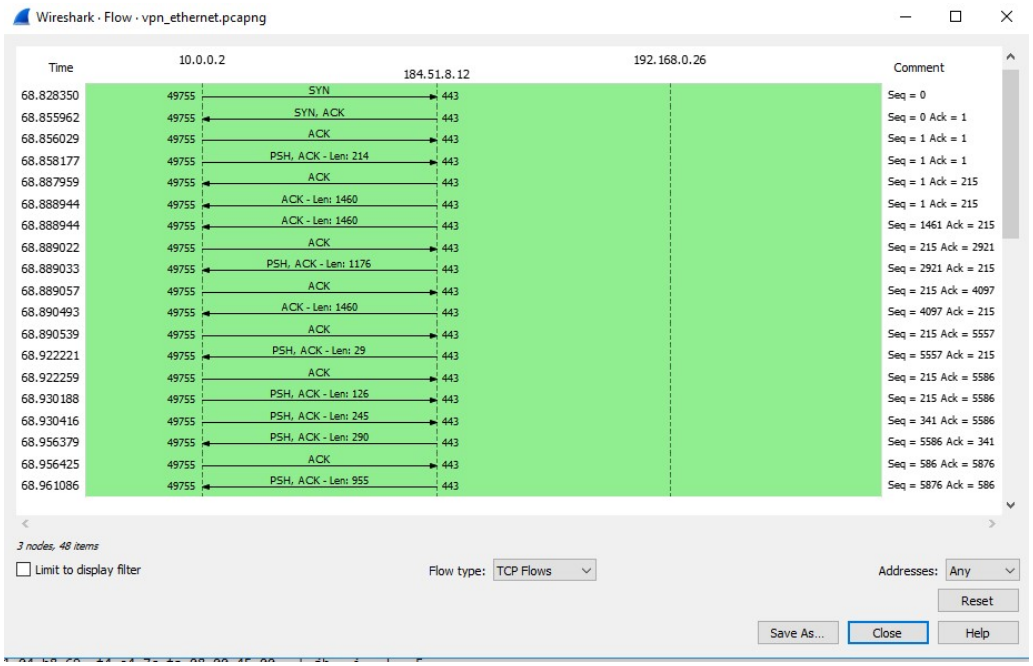
Wireshark IO grafikon pokazuje cjelokupni promet koji se vidi u *Capture* datoteci, a on se obično mjeri u razmijenjenim bajtovima ili paketima po sekundi. U zadanom je prikazu na osi *x* interval u sekundi, a na *y* osi je broj paketa po sekundi. Ovakav prikaz se koristi kako bi se otklonili eventualni problemi pri provedbi komunikacije (slika 4.9).



Slika 4.9 Prikaz IO grafa uz korištenje VPN-a

Grafikon na slici 4.10 prikazuje postupak uspostave konekcije između poslužitelja i klijenta. Kada se veza uspostavi, podatkovni paketi počinju se razmjenjivati. Osnovni detalji o paketima prikazani su na IO grafikonu toka. Može se očitati vrijeme prijenosa paketa, veličina podatkovnog okvira, redni broj okvira i TCP portovi koji se koriste pri uspostavljenoj konekciji. Također se može koristiti metoda ispitivanja postupka retransmisije zbog potencijalnog gubitka paketa ili vremenskog ograničenja.

TCP protokol koristi nekoliko zastavica. Zastavica SYN se koristi za označavanje pokretanja TCP sesije. Zastavica ACK označava da je odredište paketa primilo podatke poslane s izvora. Nakon što je TCP konekcija uspostavljena, za svaki poslani paket potrebno je poslati potvrdu primitka. Zastavica PSH vezana je uz označavanje slanja podataka.



Slika 4.10 Prikaz analize grafa uz korištenje VPN-a

5. ZAKLJUČAK

Većina postojećih poslovnih subjekata nastoji implementirati ICT rješenja kao okosnicu suvremenog načina poslovanja. Implementacija ICT rješenja odnosi se i na tehnologije koje se koriste Internetskim uslugama. Korištenjem Interneta privatni i poslovni subjekti suočili su se s jednim novim problemom, a to je sigurnost komunikacije putem Interneta. Naime, s razvojem Interneta paralelno se razvija i težnja za kompromitiranjem privatnih i poslovnih podataka koji se razmjenjuju putem Interneta. U tom kontekstu, jedno od temeljnih pitanja koje bi trebalo uzeti u obzir je pitanje sigurnosti korištenja i dijeljenja informacija putem javne Internetske mreže.

Iz navedenog razloga danas su razvijeni sustavi koji štite prijenos podataka te sprječavaju njihovo kompromitiranje. Jedan takav sustav je i VPN koji danas dobiva sve širu primjenu u privatnom i poslovnom svijetu jer omogućuje sigurnije pretraživanje sadržaja na Internetu, kao i prijenos informacija Internetom, a čija je primjena opisana i analizirana u ovom radu.

LITERATURA

[1] Širokopojasni pristup. Dostupno na:
http://www.fer.unizg.hr/_download/repository/Sirokopjasni-pristup.pdf (2.4.2018.)
[2] Priručnik za usluge fiksne telefonije/T-com. Dostupno na:
https://www.hrvatskitelekom.hr/telefon (12.4.2018.)
[3] Internetworking Technology Handbook, Cisco System, 2008. Dostupno na:
http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook (5.4.2018.)
[4] Bežični širokopojasni pristupni sustav. Dostupno na:
http://www.ericsson.hr/etk/revija/Br_1_2_2002/wireless.htm#2 (10.4.2018.)
[5] Šparica, N., Bežični širokopojasni pristupni sustav, Revija 1-2, 2002. 12-18.
[6] Tipparaju, V., Local Multipoint Distribution Service (LMDS), Citeeseer X, November, 1999.
[7] HTTP protokol. Dostupno na:
http://docbook.rasip.fer.hr/or_smil/10b_HTTP/Example/HTTP%20protokol.pdf (11.4.2018.)
[8] Bokefode, J. D. Ubale, S. A., Apte Sulabha, S. i D. G. Modani, Analysis of DAC MAC RBAC Access Control based Models for Security, International Journal of Computer Applications 104 (2014), br. 5, 6–13
[9] Khan, K. M., Developing and evaluating security-aware software systems, IGI Global, 2012.
[10] Rad na daljinu postat će pravilo, a ne iznimka. Dostupno na:
http://www.poslovni.hr/after5/rad-na-daljinu-postat-ce-pravilo-a-ne-iznimka-168752
(13.4.2018.)
[11] Biz Mags. Dostupno na: www.ebizmags.com/wp-content/plugins/cforms/.../15-E!DynamicsPrijava.doc (15.4.2018.)
[12] Cisco CCNA Curriculum 4.0, obrada: autor. Dostupno na:
https://www.ferit.unios.hr/dokumenti/struka/ciscoakademija/CCNA_Exploration_DS_0623.pdf
(16.4.2018.)
[13] PC chip. Dostupno na:
http://pcchip.hr/Internet/sto-je-vpn-za-sto-se-koristi/ (16.4.2018.)
[14] Osnovni koncept VPN tehnologije. Dostupno na:
https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf
(20.4.2018.)
[15] VPN i tehnologija iza njega. Dostupno na:
http://pcchip.hr/softver/posao-i-financije/vpn-i-tehnologija-iza-njega/ (25.4.2018.)

[16] Filipaj, I., Pongrac, D. i Žigman, D. Dinamičke skalabilne virtualne privatne mreže, Polytechnic & Design Vol. 2, No. 1, 2014., 1-9.
[12] Sudar – Kulčar, M.„„Zaštita privatnosti i sigurnosti pohranjenih podataka s osvrtom na izravni marketing“, Politička misao, Vol.42, No. 4, 2006., 93-101.
[18] Tarantola, A., VPNs: What They Do, How They Work, and Why You're Dumb for Not Using One. Dostupno na:
https://gizmodo.com/5990192/vpns-what-they-do-how-they-work-and-why-youre-dumb-for-not-using-one (23.4.2018.)
[19] Hoebeke, J., Adaptieve ad-hocusmjerivačing en haar toepassing op Virtuele Private Ad-hocNetwerken, 2009. Dostupno na:
file:///C:/Users/Leon/Downloads/Phd%20Jeroen%20Hoebeke%20(1).pdf (17.4.2018.)
[20] Stvaranje virtualne privatne mreže. Dostupno na:
http://www.java.hr/node/194 (2.5.2018.)
[21] Konfiguriranje virtualne privatne mreže, predložak za laboratorijske vježbe, Informacijska sigurnost, FERIT, Osijek, 2016. Dostupno na:https://loomen.carnet.hr/enrol/index.php?id=8267 (04.07.2019.)

POPIS SLIKA

SAŽETAK

U današnjemu modernom i urbaniziranom svijetu svakako je imperativ pri poslovanju svake organizacije na adekvatnoj zaštiti relevantnih podataka. Upravo iz navedenoga razloga na tržištu postoji mnogo različitih sigurnosnih rješenja. VPN je tehnologija koja omogućuje sigurno povezivanje privatnih mreža u zajedničku virtualnu mrežu kroz javnu mrežnu infrastrukturu. Na taj način su podaci koji se razmjenjuju mrežom zaštićeni. U ovom radu opisana je zaštita informacije i primjena VPN-a. Isto tako, u radu je opisan postupak kreiranja VPN mreže i način konfiguriranja VPN postavki usmjerivača te uporaba Wireshark programa za prikaz i analizu VPN mrežnog prometa.

Ključne riječi: VPN, zaštita podataka, sigurnost

SUMMARY

In today's modern and urbanized world, it is certainly imperative in the business of each organization to adequately protect the relevant data. For the same reason, there are many different security solutions on the market. VPN is a technology that allows to securely connect private networks to a shared virtual network through public network infrastructure. In this way, the data exchanged with the network is protected. This paper describes the protection of information and the application of VPN. The process of creating a VPN network, and how to configure the VPN settings for the router also described. Furthermore, in this paper it is also described how to use the Wireshark program to view and analyze the VPN network traffic.

Key words: VPN, data protection, security

ŽIVOTOPIS

Leon Kupanovac rođen je 5.8.1995. godine u Osijeku u Republici Hrvatskoj. Odrastao je u Donjem Miholjcu, a trenutačno živi u Osijeku. Školovanje je započeo 2002. godine u Osnovnoj školi Ante Starčevića Viljevo (samo 1. razred osnovne škole), a ostatak školovanja (od 2. do 8. razreda) je dovršio u Osnovnoj školi Augusta Harambašića Donji Miholjac. Sve razrede osnovne škole završio je sa odličnim uspjehom. Godine 2010. upisao se u komercijalni smjer u Srednjoj školi Donji Miholjac. Završni rad bio mu je ocjenjen odličnim, a prosječni prolazak na maturi mu je bio dobar. Na Fakultet elektrotehnike, računarstva, i informacijskih tehnologija Osijek (FERIT) upisao se 2014. godine. Također, završio je obuku za servisera osobnih računala i servera koja je trajala 155 sati datuma 19.11.2016. godine u EDUNOVI školi informatike i managementa.