UNIVERZITET U BEOGRADU
ELEKTROTEHNIČKI FAKULTET

IMPLEMENTACIJA I ANALIZA VPN TUNELA

Master rad

Mentor:
Dr Zoran Čiča, docent

Kandidat:
Tanja Savić 2014/3266

Beograd, Avgust 2016.

SADRŽAJ

1. UVOD

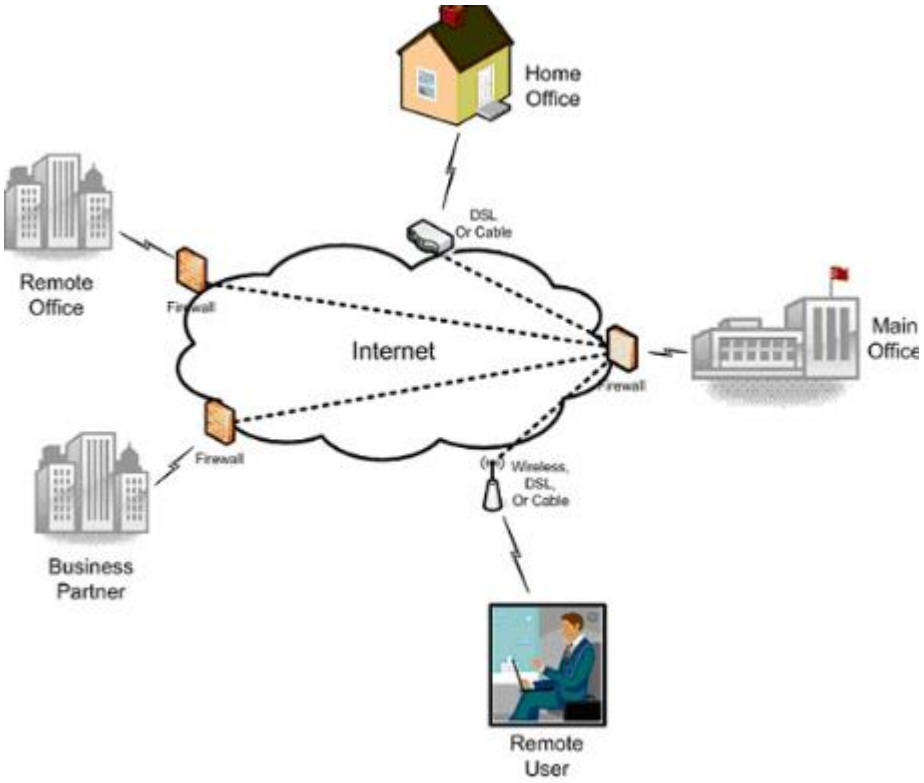
Virtuelna privatna mreža (VPN) omogućava stvaranje privatnih mreža širom Interneta, omogućujući privatnost i bezbednost korisnika virtuelne privatne mreže bez obzira što podaci putuju kroz javnu mrežu (Internet). Tipično se koristi tunelski prenos pri kreiranju VPN mreže. Tuneliranje je postupak ugradnje (enkapsulacije) podataka protokola jedne mreže u protokol druge mreže što omogućuje stvaranje transparentnih komunikacionih kanala između krajnjih čvorova. VPN se koriste za povezivanje udaljenih korisnika i nepovezanih privatnih mreža preko javne mreže kao što je Internet, čime se dobija na ekonomičnosti i fleksibilnosti u odnosu na tradicionalna rešenja poput iznajmljenih linija. Koristeći Internet kao infrastrukturu, napravi se poseban, zaštićen tunel kroz koji se vrši prenos podataka, a kojima samo korisnik VPN mreže ima pristup. Potrebno je da se obezbedi siguran prenos podataka određenim mehanizmima koji bi sačuvali tajnost i integritet podataka, i obezbedili autentifikaciju korisnika, što predstavlja osnovne elemente bezbednosti svake mreže. VPN ima brojne primene i koristi, ali osnovna je da ljudima koji su u pokretu ili rade od kuće obezbedi pristup podacima sa nekog "glavnog" računara koji nije na toj lokaciji. VPN omogućava kompanijama i organizacijama da poboljšaju postojeću infrastrukturu uz istovremeno smanjenje troškova poslovanja.

Postoji više načina implementacije VPN. Svaka od implementacija ima svoje prednosti i nedostatke, što je jedan od segmenata koji ovaj rad obrađuje. U radu su predstavljeni protokoli za realizaciju VPN, načini njihovog rada, kao i njihovi potencijalni sigurnosni rizici.

U drugom poglavlju prikazani su osnovni koncepti VPN tehnologije i opšte osobine. U trećem poglavlju opisane su VPN tehnologije: OpenVPN, IPSec, GRE, PPTP i L2TP tuneli. Opisani su njihovi načini rada, osnovni zahtevi, načini prenosa, tehnike koje koriste da bi se sačuvala autentičnost i poverljivost podataka. U četvrtom poglavlju prikazane su konfiguracije pomenutih VPN tehnologija, načini uspostave tunela kroz veb interfejs rutera, poređenja tehnologija, sa posebnim apektom na metode bezbednosti i sigurnost prenosa. U petom poglavlju opisana je analiza i zaključci prethodno konfigurisanih protokola.

2. VPN (VIRTUAL PRIVATE NETWORK)

VPN (*Virtual Private Network*) je tehnologija koja omogućava sigurno povezivanje računara u virtuelne privatne mreže. Za razliku od privatnih mreža koje koriste iznajmljene linije za slanje podataka, virtuelna privatna mreža stvara sigurni kanal između dve krajnje tačke. VPN može da poveže mnogobrojne lokacije na velikim udaljenostima kao što radi WAN (*Wide Area Network*).



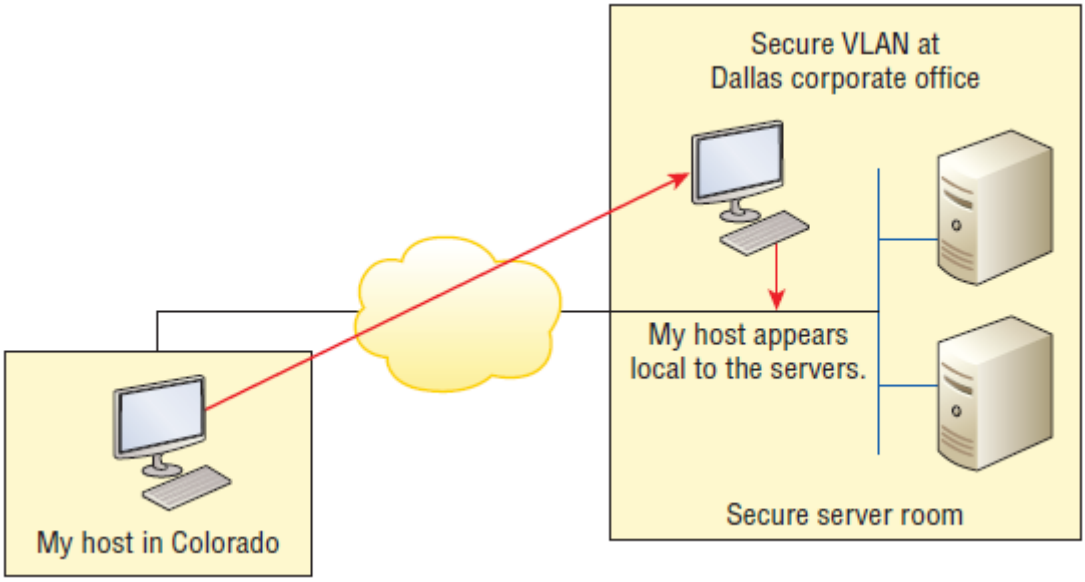
2.1 Primena VPN-a (Virtual Private Network)
(preuzeto sa: http://www.keyword-suggestions.com/cmVtb3RlIGFjY2Vzcw/)

Na slici 2.1 prikazana je VPN primena u praksi, povezivanje različitih segmenata u virtuelnu privatnu mrežu.

VPN se uklapa negde između LAN (*Local Area Network*) i WAN (*Wide Area Network*) mreža. Sa WAN mrežom često simulira LAN vezu, jer računar na jednoj LAN mreži povezuje se sa drugom udaljenom LAN mrežom i koristi resurse na daljinu. Definicija povezivanja LAN (ili VLAN (*Virtual Local Area Network*)) na WAN mrežu može zvučati isto kao i upotreba VPN-a. Međutim, VPN predstavlja mnogo više. Tipična WAN mreža povezuje dve ili više udaljenih LAN mreža koristeći ruter i neku tuđu mrežu, npr. ISP (*Internet Service Provider*). Lokalni računar i ruter vide ove mreže kao udaljene mreže, a ne kao lokalne mreže ili lokalne resurse. Ovo bi predstavljalo WAN u opštoj definiciji. Pomoću VPN-a lokalni host je deo udaljene mreže koristeći WAN link za

konekotvanje na udaljenu LAN mrežu. To znači da je omogućen pristup resursima udaljene LAN mreže i taj pristup je siguran.

Slika 2.2 prikazuje primer hosta koji koristi VPN konekciju iz jednog grada ka drugom, koja omogućava pristup udaljenim mrežnim uslugama i serverima, kao da je host na istoj VLAN mreži kao i serveri. VPN dozvoljava hostu da se poveže na te resurse lokalno pristupajući VLAN-u kroz VPN preko WAN-a. Druga opcija bi bila otvaranje sopstvene mreže i servera svima na Internetu ili na drugom WAN servisu. U tom slučaju sigurnost ne bi postojala [2].



2.2 Primena VPN-a (*Virtual Private Network*)
(preuzeto iz: [2])

2.1. Osnove i koncept

Osnovni koncept VPN tehnologije je implementacija sigurnog prenosa između privatnih mreža, preko javne mreže.

Kada računar šalje podatke prema drugom računaru na udaljenoj mreži, podaci koji u tom slučaju izlaze iz lokalne mreže moraju proći kroz gejtvej uređaj koji štiti tu mrežu i koji predstavlja izlaz na Internet za tu LAN mrežu i putovati kroz javnu mrežu. Na drugoj strani takođe moraju proći kroz gejtvej, uređaj koji štiti odredišni računar na udaljenoj mreži i predstavlja izlaz na Internet na tu mrežu. U četvrtom poglavlju konfiguracije su ostvarene upravo na ovaj način i pokazuju praktičnu primenu VPN-a između dve LAN mreže (*LAN to LAN*). VPN štiti poslate podatke automatskim šifriranjem prilikom slanja podataka između dve udaljene privatne mreže i enkapsuliranjem u IP pakete. Na odredištu, paketi se automatski dešifruju. Osnovni cilj VPN-a je da ograniči pristup podacima koji se prenose i to samo korisnicima VPN mreže. Sami korisnički paketi se na ulasku u tunel enkapsuliraju u odgovarajući format (npr. IP datagrame u slučaju da tunel ide preko Internet mreže). Ovaj proces se naziva tunelovanje paketa

2.2. Osnovni zahtevi i elementi Virtuelne privatne mreže

Da bi prenos bio siguran i pouzdan, postoji nekoliko zahteva koje VPN tehnologija mora ispuniti. VPN mora osigurati proveru identiteta korisnika i ograničiti pristup samo ovlašćenim korisnicima. Autentifikacija obezbeđuje da samo autentifikovani korisnici imaju pristup zaštićenoj

mreži. VPN je zadužen za dodeljivanje klijentskih adresa unutar privatnih mreža, da bi obezbedio upravljanje adresama. Integritet podataka (*Data Integrity*) - kojim se proverava da izvorni sadržaj poruke nije promenjen prilikom prenosa preko Interneta, na njenom putu do konačnog odredišta. Poverljivost podataka obezbeđuje zaštitu sadržaja poruke primenom enkripcije. Na taj način informacija postaje neupotrebljiva i nedostupna potencijalnom napadaču. VPN mora sadržati mehanizme za generisanje ključeva neophodnih za šifrovanje podataka prilikom prenosa kroz tunel. VPN treba da obezbedi podršku za razne protokole (IP, IPX (*Internet Packet Exchange*) itd.)

Postoji više aspekata koje VPN mora zadovoljiti:

- Skalabilnost
- Sigurnost
- VPN servisi
- Uređaji
- Upravljanje
- Ušteda
- Kompatibilnost sa širokopojasnom tehnologijom

Skalabilnost podrazumeva da VPN rešenje treba da podrži sve od malih kancelarijskih konfiguracija, pa do velikih korporacijskih implementacija. Sigurnosni pojmovi kao što su tunelovanje, šifrovanje i autentifikacija paketa neophodni su za sigurnost prenosa podataka preko javnih mreža. Osim toga autentifikacija korisnika i kontrola pristupa neophodne su za dodelu odgovarajućih ovlašćenja i prava pristupa mrežnim resursima. Upravljanje i nadgledanje VPN mreže je izuzetno važno radi podešavanja rada VPN-a u skladu sa korisničkim zahtevima, kao i za detektovanje grešaka u radu i potencijalnih napada. Ušteda: Povezivanje korporativnih udaljenih kancelarija sa njihovim najbližim Internet provajderom i kreiranje VPN tunela sa autentifikacijom i enkripcijom, obezbeđuju ogromnu uštedu u odnosu na tradicionalne iznajmljene point-to-point linije. Kompatibilnost sa širokopojasnom tehnologijom: Za korisnike koji putuju, udaljene kancelarije, bilo koji Internet pristup može obezbediti vezu sa VPN-om. Ovo omogućava korisnicima da iskoriste prednost pristupa Internetu putem DSL-a (*Digital Subscriber Line*) tehnologije, kablovskih modema i dr

2.3. Vrste VPN-a na osnovu uloge koju obavlja

VPN se deli na nekoliko kategorija prema ulozi koju obavlja u poslovanju. Postoje tri različite kategorije:

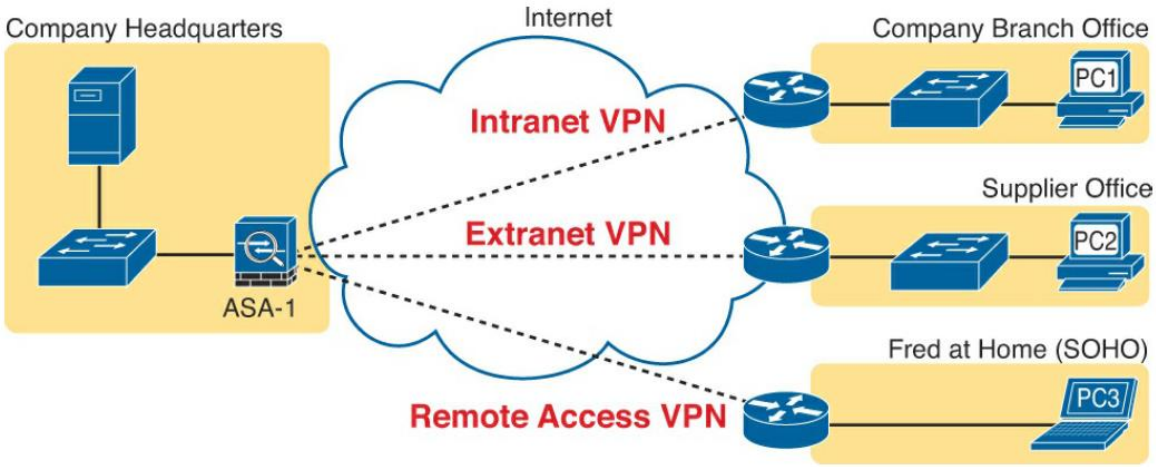
- VPN rešenja za udaljeni pristup (*Remote Access*)
- Intranet VPN (*site-to-site*)
- Extranet VPN

VPN rešenja sa udaljenim pristupom (*Remote Access*) dozvoljavaju udaljenim korisnicima, koji npr. rade na daljinu siguran pristup korporativnoj mreži bilo gde i bilo kada da im je to potrebno. Povezuju se udaljeni korisnici ili manji udaljene kancelarije sa računarskom infrastrukturom organizacije.

Intranet VPN (*site-to-site*) dozvoljava kompaniji da poveže svoje udaljene lokacije na korporativnu kičmu mreže sigurno, preko javnog medijuma kao što je Internet umesto zahtevanja više skupih WAN povezivanja kao što je Frame Relay ili iznajmljene linije.

Extranet VPN dozvoljava dobavljačima, kupcima, partnerima da budu povezani na korporativnu mrežu na ograničen način za poslovnu (*busines-to-business*) komunikaciju [2].

Slika 2.5.1 prikazuje vrste VPN-a na osnovu uloge koju obavlja u poslovanju:



2.5.1 Remote Access, Intranet VPN, Extranet VPN
(preuzeto iz: [10])

2.4. Prednosti VPN-a

Usled sve veće popularnosti i mogućnosti pristupa Internetu kao i pojeftinjenja mrežne opreme, osnovna prednost upotrebe VPN-a je značajna ušteda u odnosu na cenu korišćenja privatnih iznajmljenih linija ili međugradskih/internacionalnih telefonskih poziva. VPN se sve češće koristi kao alternativno rešenje u odnosu na WAN jer uštede mogu biti ogromne, a pri tome se dobija i na fleksibilnosti pošto je danas pristup Internetu široko raspostranjen. Komunikacioni putevi korišćenjem VPN-a mogu se uspostaviti brzo, jeftino i sigurno. Pored sigurnosti kao osnovne prednosti, VPN mreže odlikuje i fleksibilnost, tj. mogu se lako koristiti na svim uređajima koji se povezuju na Internet. Operativni sistemi ne igraju nikakvu ulogu u mogućnosti upostavljanja VPN tunela. Kao primer u ovom radu vidi se konfigurisanje PPTP tunela, gde je server podignut na Windows 7 operativnom sistemu, a tunel je konfigurisan na ruteru koji radi u Linux operativnom sistemu.

VPN je pogodno koristiti ukoliko kompanija ima okruženje sa više odvojenih lokacija, a kvalitet usluge nije osnovni kriterijum. U slučaju manjeg broja odvojenih lokacija, pri čemu je kvalitet usluge osnovni zahtev, korišćenje iznajmljenih linija je pogodnije rešenje jer je znatno lakše implementirati i kontrolisati QoS na iznajmljenim linijama nego u Internet mreži.

3. VPN PROTOKOLI TUNELOVANJA

Tunelovanje ili enkapsulacija predstavlja metodu u kojoj se umesto slanja originalnih paketa, oni enkapsuliraju dodatnim zaglavljem, koje sadrži informacije neophodne za rutiranje do krajnjeg odredišta tog paketa. Enkapsulirani podaci putuju između krajnjih tačaka tunela. Tunel je logička putanja kroz koju se usmeravaju paketi. Tunelovanje uključuje čitav proces enkapsulacije, prenosa i ponovne ekstrakcije originalnih podataka.

3.1. Protokoli

Postoji više protokola koji podržavaju kreiranje tunela za VPN mreže. Među poznatijima se izdvajaju:

- OpenVPN
- GRE (*Generic Routing Encapsulation*)
- IPSec (*IP Security)*
- PPTP (*Point-To-Point Tunneling Protocol*)
- L2TP (*Layer 2 Tunneling Protocol*)
- L2F (*Layer 2 Forwarding*)
- DLSW (*Data Link Switching*)
- ATMP (*Ascend Tunnel Management Protocol*)
- Mobile IP

3.2. OpenVPN

OpenVPN je programski paket koji se koristi za implementaciju virtuelnih privatnih mreža. OpenVPN koristi SSL/TLS (*Secure Socket Layer /Transport Layer Security*) protokol za uspostavu sigurne komunikacije između tačaka VPN veze. Podaci koji se razmenjuju prenose se TCP ili UDP protokolom. TCP osigurava pouzdanu isporuku podataka (vrši ponovno slanje izgubljenog ili neispravnog paketa). UDP je jednostavniji, ne vrši proveru razmene podataka i pogodan je za komunikaciju gde se greške dozvoljavaju (video prenos). OpenVPN u radu koristi virtuelne mrežne interfejse korišćenjem TUN (*network TUNnel*) ili TAP (*network tap*) upravljačkih programa. Stvarajući virtuelne mrežne interfejse VPN klijent je u stanju da kriptuje sav odlazni saobraćaj bez potrebe za ikakvim promenama na postojećim aplikacijama kod klijenta. OpenVPN omogućuje prenos različitih tipova podataka (Ethernet okviri, IPX ili NETBIOS paketa).

Autentifikacija korisnika je omogućena korišćenjem tajnog ključa, sertifikata ili proverom korisničkog imena i šifre. Za brzu kompresiju podataka u realnom vremenu koristi se LZO (*Lempel-Ziv-Oberhumer*) biblioteka koja podatke kompresuje pre postupka enkripcije. OpenVPN može da se uspostavlja primenjujući NAT (*Network Address Translation*), mehanizam koji omogućuje prevođenje javnih adresa u privatne.

U ovom radu konfigurisan je jedan OpenVPN tunel koji komunikaciju vrši preko TCP protokola, uspostavljajući TUN virtuelni point-to-point link, sa uključenom opcijom NATovanja.

3.2.1. Osnovni sigurnosni koncepti

Zaštita podataka koji se razmenjuju prilikom upotrebe OpenVPN-a ostvaruje se enkripcijom i zaštitom integriteta podataka. Za enkripciju se koriste različiti simetrični i asimetrični algoritmi šifrovanja, dok se za zaštitu integriteta poruka koriste funkcije za izračunavanje heš algoritma.

OpenVPN koristi OpenSSL, programski paket koji omogućava robusnu implementaciju i podršku za SSL v2/3 i TLS v1 (*Transport Layer Security*) sigurnosne protokole. SSL tehnologijom se kriptuje veza tako da podaci koji se razmenjuju ne mogu biti dešifrovani u slučaju da ih napadač presretne.

OpenSSL podržava veliki broj različitih kriptografskih algoritama:

- Simetrične algoritme: Blowfish, CAST, DES (*Data Encription Standard*), AES (*Advanced Encryption Standard*), IDEA (*International Data Encyption Algorithm*), RC2 (*Rivest Cipher*), RC4 i RC5

- Asimetrične algoritme: DSA (*Digital Signature Algorithm*), RSA (*Rivest-Shamir-Adleman*), DH (*Diffie-Helman*)

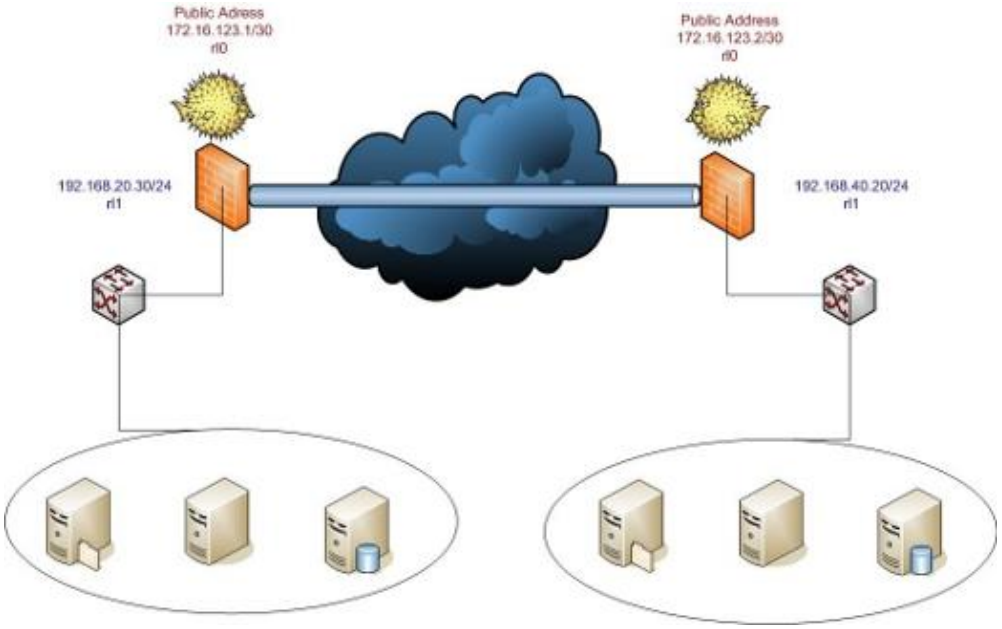
- Sertifikate: X509

- Heš funkcije: HMAC (*hash message authentication code*), MD2 (*Message-Digest*), MD4, MD5, MDC2, SHA (*Secure Hash Algorithm*), RIPEMD (*RACE Integrity Primitives Evaulation Message Digest*) [6].

3.3. IPSec

IPSec (*Internet Protocol Security*) je protokol koji obezbeđuje sigurnost prilikom prenosa na Internetu. IPSec je protokol trećeg sloja (*Layer 3*). Koristeći mehanizme enkripcije i autentifikacije osigurava integritet podataka i siguran prenos kroz tunel.

Na slici 3.3.1 prikazana je IPSec tehnologija, prosta konfiguracija između dve LAN mreže. Prikazane su javne IP adrese dobijene od provajdera, između kojih je formiran tunel i vrši se prenos.



3.3.1 IPSec tehnologija
(preuzeto sa: http://stuffresearch.tor.hu/?p=64)

IKE (*Internet Key Exchange*) služi za određivanje sigurnosnih parametara i razmenu ključnih informacija između entiteta koji učestvuju u komunikaciji. Sigurnosni parametri definišu vezu između dva ili više entiteta, način na koji će upotrebiti sigurnosne servise u cilju uspostave međusobne sigurne komunikacije. Kroz taj proces dva entiteta se moraju međusobno autentifikovati i dogovoriti zajedničke ključeve.

Protokoli i standardi koji se koriste prilikom uspostave IPSec-a su:

- Diffie-Hellman-ova metoda razmene ključeva
- Enkripcija koja se zasniva na javnim ključevima za digitalno potpisivanje tokom Diffie-Hellman-ove razmene ključeva. Osigurava identitet obe strane u komunikaciji i izbegava mogućnost tzv. man-in-the-middle napada.
- DES (*Data Encription Standard*) ili 3DES (*Triple Data Encription Standard*) standard za šifriranje podataka
- HMAC (*Hashing Message Authentication)* u sprezi sa MD5 (*Message-Digest algorithm 5)* i SHA (*Secure Hash Algorithm*) algoritmima.

3.3.1. Protokoli za bezbednost

Dva primarna sigurnosna protokola koja koristi IPsec su AH (*Authentication Header*) i ESP (*Encapsulating Security Payload*).

i) AH (Authentication Header)

AH protokol obezbeđuje autentifikaciju za podatke i IP zaglavlje paketa koristeći heš metodu za autentifikaciju paketa. Pošiljalac generiše u jednom smeru autentifikaciju (heš vrednost) i onda primalac generiše, takođe, heš vrednost. Ako je paket promenjen, autentifikacija se neće izvršiti i propašće paketi. IPSec se oslanja na AH protokol za garantovanje autentičnosti.

ii) ESP (Encapsulating Security Payload)

ESP obezbeđuje pouzdanost, proveru identiteta, porekla i integriteta podataka, ograničenu tajnost protoka saobraćaja analizama protoka saobraćaja.

Postoji 5 komponenti ESP-a:

- Poverljivost (enkripcija)
- Integritet podataka
- Autentifikacija
- Anti-replay service
- Protok saobraćaja

Poverljivost (enkripcija) omogućuje uređaju koji šalje da enkriptuje pakete pre slanja u cilju sprečavanja prisluškivanja. Poverljivost je obezbeđena korišćenjem simetričnih algoritama enkripcije kao što su DES ili 3DES. Enkripcija se konfiguriše nezavisno, ali odabrana enkripcija mora biti ista na obe krajnje tačke VPN tunela.

Integritet podataka dozvoljava prijemniku da verifikuje da li su primljeni podaci negde promenjeni usput. IPSec koristi sume kao jednostavne provere podataka.

Autentifikacija osigurava da je konekcija napravljena sa ispravnim partnerom. Prijemnik može da autentifikuje izvor paketa garantujući i potvrđujući izvor informacija.

Anti-replay service je baziran na prijemniku. Usluga je efikasna jedino ako prijemnik proverava redni broj. Ponavljajući napad je situacija kada haker napravi kopiju autentifikovanog paketa i prenosi je na namenjenu lokaciju. Kada duplikat, autentifikovani IP paket stigne na destinaciju, može potpuno da poremeti usluge. Polje redni broj je napravljeno da osujeti ovu vrstu napada.

Protok saobraćaja: Da bi osetljivost protoka saobraćaja funkcionisala, mora najmanje jedan tunel biti odabran. To je najefikasnije, ako je implementiran bezbednosni gejtvej, uređaj kroz koji sav saobraćaj mora proći, jer je to vrsta okruženja koja može da sakrije pravi izvor i odredište podataka, za sve koji pokušavaju da probiju sigurnost mreže.

3.3.2. Enkripcija

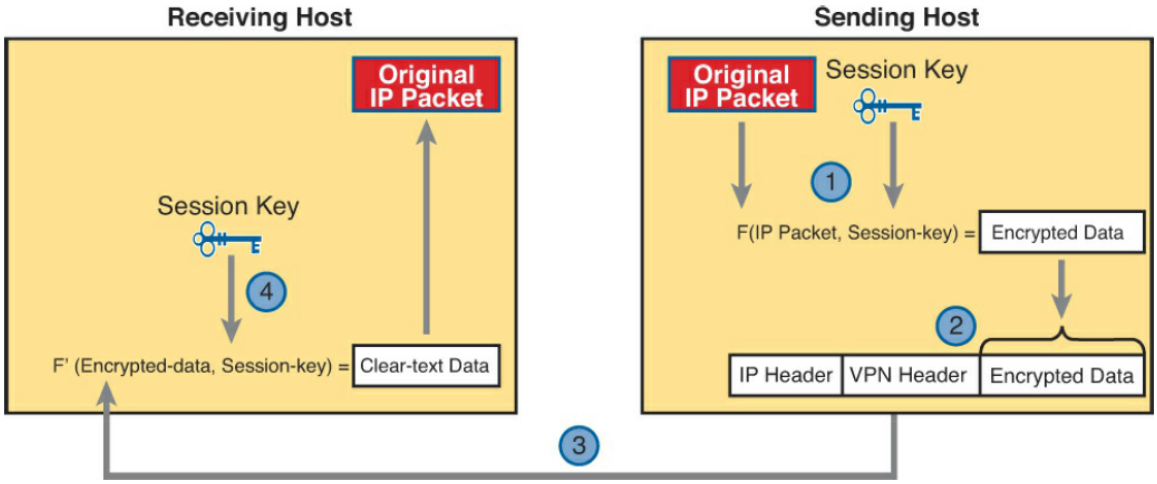
VPN kreira privatnu mrežu preko javne mrežne infrastrukture, ali da bi se održala tajnost i bezbednost potrebno je koristiti IPSec sa VPN-om. IPSec koristi razne tipove protokola za obavljanje šifrovanja (enkripcije). Tipovi algoritama šifrovanja (enkripcije) koji se danas koriste su:

- Simetrično šifrovanje
- Asimetrično šifrovanje

Simetrično šifrovanje: Ovo šifrovanje zahteva tajni ključ (*shared secret*) za enkripciju i dekripciju. Svaki kompjuter enkriptuje podatke pre slanja informacija preko mreže, istim ključem koji se koristi i za enkriptovanje (predaja) i dekriptovanje podataka (prijem). Primeri simetričnih ključeva za enkripciju su: DES (*Data Encryption Standard*), 3DES (*Triple DES*) i AES (*Advanced Encryption Standard*).

Asimetrično šifrovanje: Uređaji koji koriste asimetrično šifrovanje koriste različite ključeve za enkripciju od onih koje koriste pri dekriptovanju. Ovi ključevi se zovu privatni i javni ključevi. Privatni ključevi enkriptuju heš iz poruke i kreiraju digitalni potpis, koji je verifikovan

dekriptovanjem koristeći javni ključ. Javni ključ enkriptuje simetrični ključ za sigurnu distribuciju do prijemnog hosta, koji onda dekriptuje taj simetrični ključ koristeći svoj zadržani privatni ključ. Nije moguće da se vrši enkripcija i dekripcija koristeći isti ključ. Primer asimetričnog ključa: RSA (*Rivest, Shamir i Adleman).*



3.3.2.1 IPSec proces enkripcije
(preuzeto iz: [10])

Četiri koraka sa slike 3.3.2.1 su:

1. Predajna strana (npr. udaljeni ruter u kancelariji) smešta originalne pakete i ključ sesije u formulu za enkriptovanje, računajući enkriptovane podatke.
2. Predajna strana enkapsulira podatke u paket, koji uključuje novo IP zaglavlje *(IP Header*) i VPN zaglavlje (*VPN Header*).
3. Predajna strana šalje novi paket na namenjenu destinaciju
4. Prijemna strana, pokreće odgovarajuću formulu za dekripciju, uzimajući enkriptovane podatke i ključ sesije - (ista vrednost ključa koja je bila u upotrebi na VPN uređaju koji šalje) - da dekriptuje podatke [2].

3.4. GRE

GRE (*Generic Routing Encapsulation protocol*) je komunikacioni protokol za uspostavljanje direktne, point-to-point konekcije između mrežnih čvorova (nodova). GRE tuneli se koriste kada je potrebno da IP paketi budu poslati iz jedne mreže u drugu, bez procesiranja ili tretiranja kao IP paketa od strane usputnih rutera. U većini slučajeva radi se o umetanju u IP pakete radi prenosa preko TCP/IP mreža. Rutiranje kroz tunel se obavlja na osnovu zaglavlja protokola preko kojih se tunel uspostavlja. Na odredištu (izlaznoj strani tunela) izvlače se GRE paketi. Iz njih se izvlači paket izvornog protokola i prosleđuje ka krajnjem odredištu.

Karakteristike GRE tunela:

- GRE koristi polje u GRE zaglavlju tako da bilo koji protokol mrežnog sloja (Layer 3) može biti korišćen pri prenosu kroz tunel.
- GRE nema kontrolu protoka.
- GRE ne nudi bezbednost.

- GRE kreira dodatni overhead za pakete koji prolaze kroz tunel – najmanje 24 bajta (*bytes*)

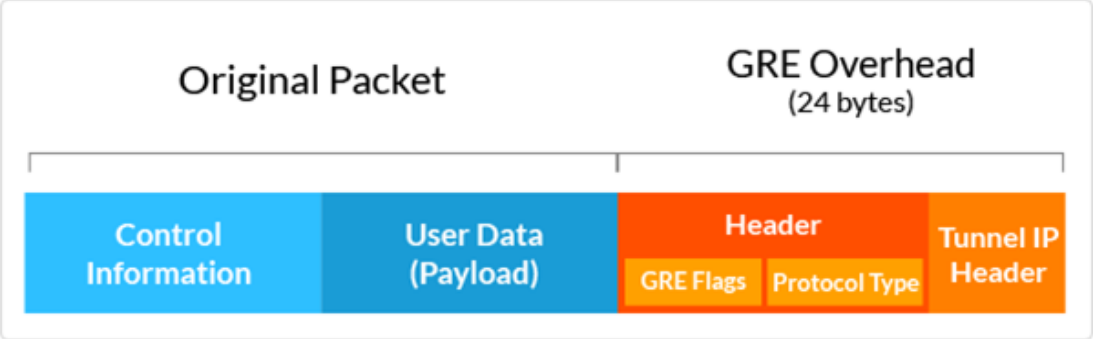
GRE protokol ima veliki broj prednosti:

- Povezivanje lokalnih mreža s podrškom za različite protokole u jedinstvenu virtuelnu privatnu mrežu.
- Realizacija virtuelnih privatnih mreža preko širokopojasnih mreža (*Wide Area Networks*).
- Mogućnost povezivanja lokalnih mreža zasnovanih na radu različitih protokola preko jedinstvene, javne mreže.
- Obezbeđuje rešenje za mreže sa ograničenim brojem skokova (*hops*), tj. ograničenim mogućnostima usmeravanja.
- Zahteva manje resursa od svojih alternativa (npr. IPSec VPN).

3.4.1. Prenos podataka kroz GRE tunel

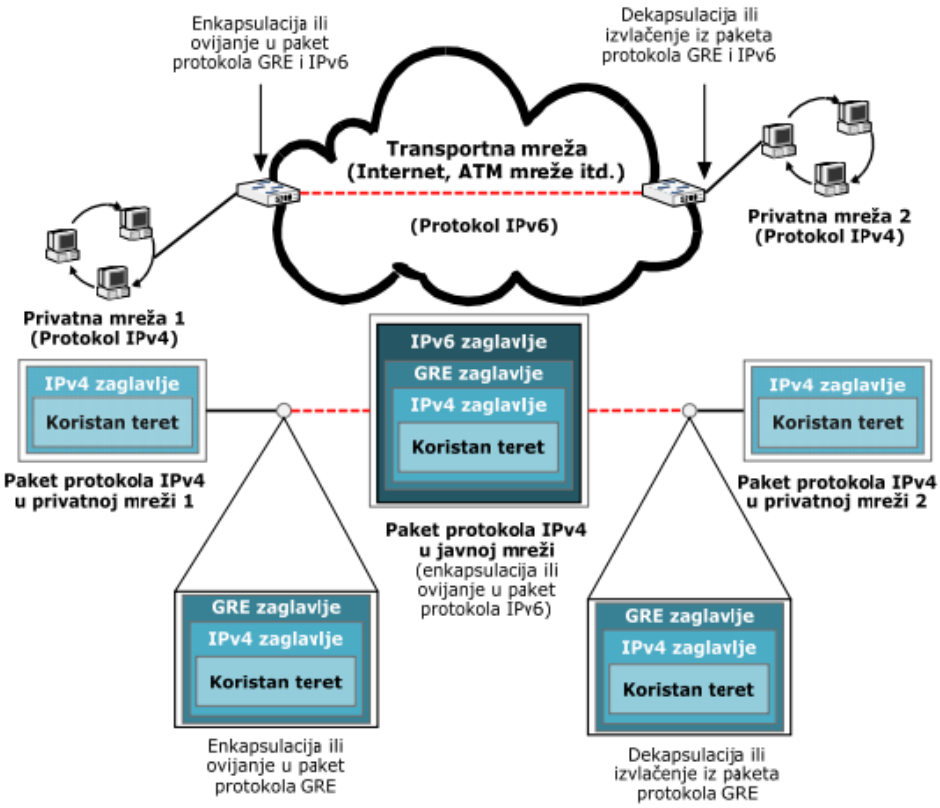
GRE radi tako što enkapsulira korisni deo paketa, unutar spoljašnjeg IP paketa. Da bi se jedan enkapuslirani paket preneo, GRE tunel mora biti uspostavljen. To je virtuelna point-to-point konekcija između dve mreže. Sa uspostavljenim tunelom, GRE paket može putovati direktno između dve krajnje tačke. To da je tunel virtuelan znači da, iako paket putuje kroz druge rutere, ti drugi ruteri ne analiziraju enkapsulirani paket. Drugi ruteri samo prosleđuju paket do odredišne tačke tunela. Na odredišnom kraju tunela paket se dekapsulira i analizira se njegova korisna nosivost[2][10].

U procesu enkapsulacije GRE "prepakuje" paket koji šalje. To se postiže dodavanjem dva dodatna zaglavlja, jedan se identifikuje kao GRE paket, a drugi obezbeđuje novi izvor i odredište IP adrese. Primer GRE enkapsulacije prikazan je na slici 3.4.1.1:



3.4.1.1 Primer GRE enkapsulacije
(preuzeto iz: [10])

GRE tunel se uspostavlja na nivou rutera i razlikuje se u zavisnosti od vrste hardvera koja se koristi. Slika 3.4.1.2 pokazuje, da je potrebno da se podesi interfejs IP adrese u tunel i pružanje javnih IP adresa za oba kraja GRE tunela. Na paket koji se šalje (paket iz privatne mreže), dodaje se GRE zaglavlje i vrši se enkapsulacija. Paket prolazi kroz tunel, na izlazu se vrši dekapsulacija i izvlači se korisni deo paketa (informacija koja je trebalo da se prenese).



3.4.1.2 Mehanizam GRE tuneliranja (preuzeto iz: [4])

3.5. PPTP

PPTP (*Point-to-Point Tunneling Protocol*) je protokol koji se koristi u realizaciji virtuelnih privatnih mreža. PPTP enkapsulira PPP (*Point-to-Point Protocol*) okvire u IP datagrame za prenos preko javne mreže kao što je Internet ili preko privatne unutrašnje mreže. PPTP koristi TCP konekciju da kreira, održava i prekine tunel i modifikovanu verziju GRE paketa koji enkapsulira PPP okvire kao tunelske podatke. Korisni deo enkapsuliranog PPP okvira može biti enkriptovan ili kompresovan, ili oboje. PPTP omogućava dostupnost unutrašnje mreže između PPTP klijenta (VPN klijent koji koristi PPTP protokol) i PPTP servera. U ovom radu u poglavlju četiri prikazana je jedna ovakva mreža, gde je PPTP server podignut na Windows mašini, a PPTP klijent koji šalje zahtev za vezu je konfigurisan na ruteru. PPTP klijent može biti već dodat u jednu IP unutrašnju mrežu koja može da komunicira sa PPTP serverom (nalaze se u istom mrežnom opsegu) ili PPTP klijent može da šalje zahtev pristupnom mrežnom serveru NAS (*Network Access Server*) da upostavi IP konekciju kao u slučaju *dial-up* Internet korisnika. Dakle, rad PPTP protokola zasniva se na GRE i PPP protokolu.

Autentifikacja koja se javlja tokom procesa kreiranja PPTP konekcije koristi iste autentifikacione mehanizme kao i PPP konekcija, kao što su EAP (*Extensible Authentication Protocol*), MS-CHAP (*Microsoft Challenge-Handshake Authentication Protocol*), CHAP, SPAP (*Shiva Password Authentication Protocol*) i PAP (*Password Authentication Protocol*).

PPTP nasleđuje enkripciju i kompresiju korisnog dela paketa, od PPP protokola. Mehanizam koji se koristi je MPPE (*Microsoft Point-to-Point Encryption*), da enkriptuje korisne delove paketa za čiji prenos se koristi MS-CHAP metoda autentifikacije. MPPE obezbeđuje samo enkripciju linka, Ne omogućava s kraja na kraj (*end-to-end*) enkripciju. *End-to-end* enkripcija predstavlja prenos

podataka između klijentske aplikacije i servera domaćina resursa ili usluge koju zahteva klijentska aplikacija. Ukoliko je potrebna *ent-to-end* enkripcija, IPSec se može koristiti da enkriptuje IP saobraćaj s kraja na kraj, nakon što je PPTP tunel uspostavljen. Ovim se prikazuje da najveći stepen bezbednosti pruža IPSec tunel [11].

Uspostavljanje virtuelne privatne mreže primenom protokola PPTP ostvaruje se uspostavom dvostruke veze između odgovarajućih PPTP klijenta i PPTP servera. Veza sastoji se od:

- Kontrolne veze (*Control Connection*)
- PPTP tunela (*Tunnel Protocol*)

3.5.1. Kontrolna veza

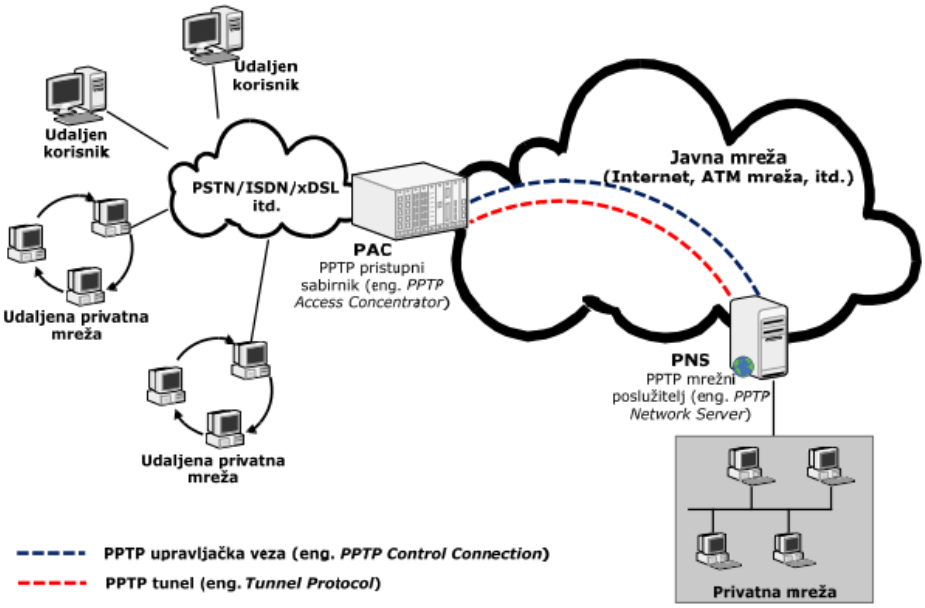
Početni korak pre uspostave PPTP tunela između PPTP klijenta i PPTP servera predstavlja uspostavljanje kontrolne veze. To je TCP veza u sklopu koje se izmenjuju upravljački i kontrolni podaci protokola PPTP. Ova veza je logički povezana sa podacima koji prolaze kroz tunel. Po uspostavi odgovarajuće TCP veze server i klijent ostvaruju kontrolnu vezu izmenom poruka Connection-Request i Connection-Replay.

3.5.2. PPTP tunel (Tunel protokol)

Drugi korak pri aktivaciji PPTP protokola predstavlja formiranje tunela između PPTP klijenta i odgovarajućeg PPTP servera. Ovaj tunel koristi se za prenos svih korisničkih paketa. PPP paketi obavijeni su GRE zaglavljem čiji ključan parametar ujedno označava i kojoj sesiji pojedini PPP paket pripada.

Na taj način se PPP paketi multipleksiraju i demultipleksiraju tokom prolaska kroz tunel upostavljenog između servera i klijenta. Vrednost koja se koristi kao ključan parametar GRE zaglavlja definiše se prilikom uspostave sesije preko upravljačke veze.

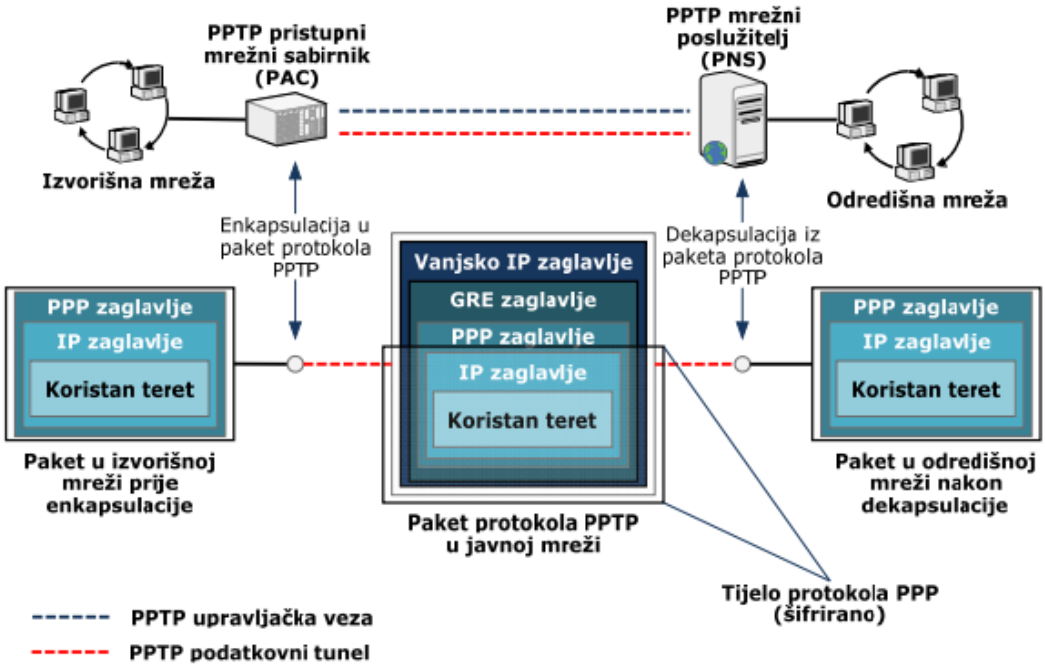
Na slici 3.5.2.1 prikazana je uspostava upravljačke veze i PPTP tunela:



3.5.2.1 PPTP arhitektura
(preuzeto iz: [4])

3.5.3. Struktura PPTP paketa

Celokupna struktura paketa PPTP protokola prikazana je na slici 3.5.5.1. Prikazan je primer paketa koji se razmenjuje u PPTP tunelu.



3.5.5.1 PPTP paket
(preuzeto iz: [4])

U izvorišnoj mreži ili na izvorišnom računaru se upotrebom PPTP klijenta paketi namenjeni nekom računaru u udaljenoj privatnoj mreži šifruju ili kompresuju, ili oboje i ubacuju u PPP pakete. Ti paketi se ugrađuju u pakete protokola GRE. Dodaje im se zaglavlje protokola upotrebljenog u mreži preko koje se uspostavlja tunel. Kada paketi stignu do krajnje tačke tunela (PPTP server), iz njih se izvlači izvorni PPP paket (dekapsulira). Uz pomoć podataka iz PPP zaglavlja paketi se usmeravaju prema krajnjem odredištu, zatim se dešifruju izvorni podaci i proverava autentičnost pošiljaoca [4].

3.6. L2TP

L2TP (*Layer 2 Tunneling Protocol*) je protokol koji predstavlja kombinaciju PPTP i L2F (*Layer 2 Forwarding*) tehnologije. L2TP enkapsulira PPP okvire, koji se šalju preko IP, X.25, Frame Relay ili ATM (*Asynchronous Transfer Mode*) mreža. Trenutno je definisan samo L2TP preko IP mreža. L2TP koristi UDP protokol. Kada je poslat paket preko neke unutrašnje mreže, L2TP okviri se enkapsuliraju kao UDP poruke. L2TP se može koristiti kao protokol tunelovanja preko Interneta ili privatne mreže.

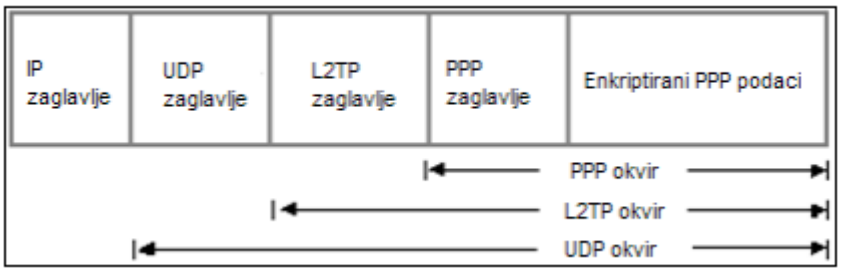
L2TP koristi UDP poruke preko IP unutrašnje mreže za oba, održavanje tunela i podatke koji se prenose. Korisni deo enkapsuliranog okvira može biti enkriptovan ili kompresovan ili oboje. Enkripcija za L2TP konekcije je obezbeđena od strane IPSec ESP-a, pa je preporuka, ukoliko je potreban siguran prenos da se L2TP koristi u kombinaciji sa IPSec-om.

Autentifikacija koja se koristi tokom kreiranja L2TP tunela mora biti ista kao i autentifikacioni mehanizmi koje koriste PPP konekcije: EAP, MS-CHAP, CHAP, SPAP, PAP.

L2TP radi na drugom sloju OSI modela (*Open Systems Inteconnection Basic Reference Model)*. Koristi se kao protokol tunelovanja za IP, X25, Frame Relay ili ATM [12].

3.6.1. L2TP načini rada

Paketu koji treba da se pošalje mrežom dodaje L2TP zaglavlje na što se dodaje UDP zaglavlje. Na kraju paket se enkapsulira dodavanjem IP zaglavlja koje sadrži IP adrese klijenta i servera, što je prikazano na slici 3.6.1.1.



3.6.1.1 Način prenosa podataka korišćenjem L2TP protokola (preuzeto iz: [4])

Krajnje tačke L2TP tunela se nazivaju LAC (*L2TP Access Concentrator*) i LNS (*L2TP Network Server)*. LAC se nalazi na strani klijenta. Klijent šalje zahtev za uspostavom veze. LNS se nalazi na strani servera.

L2TP podržava obavezno definisane i proizvoljno definisane tunele (*voluntary*).

Način rada obavezno definisanog tunela:

Udaljeni korisnik inicira PPP spoj prema svom ISP-u. ISP prihvata spoj i PPP sesija je uspostavljena. ISP zahteva delimičnu autentifikaciju da bi dobio korisničko ime. U ISP-ovoj bazi podataka korisničko ime je povezano sa servisima i LNS krajnjim tačkama. LAC inicira L2TP tunel prema LNS-u. Ukoliko LNS prihvati spoj, LAC enkapsulira PPP u L2TP i prosleđuje podatke preko odgovarajućeg tunela.

3.6.2. L2TP vrste poruka

L2TP definiše dve vrste poruka:

- Kontrolne poruke
- Poruke koje prenose podatke

Kontrolne poruke su u upotrebi prilikom uspostave, održavanja i prekidanja tunela, dok se poruke koje prenose podatke koriste za enkapsulaciju PPP okvira koji se prenose kroz tunel. Kontrolne poruke definiše kontrolni kanal unutar L2TP-a koji garantuje dostavu. Ukoliko dođe do gubljenja paketa, poruke koje prenose podatke se šalju ponovo, vrši se retransmisija. PPP okviri se preko nepouzdanog kanala šalju enkapsulirani sa L2TP zaglavljima, a zatim i sa prenosnim zaglavljima kao što su UDP, Frame Relay, ATM itd. Kontrolne poruke šalju se preko pouzdanog L2TP kontrolnog kanala. Redni brojevi su nužni u svim kontrolnim porukama koje služe da bi osigurale pouzdanu dostavu kroz kontrolni kanal. Poruke koje prenose podatke mogu imati redne brojeve za utvrđivanje ispravnog redosleda i detekciju paketa koji nedostaju.

L2TP koristi NCP (*Network Control Protocol)* za dodelu IP adresa i autentifikacijske šeme PPP (PAP (*Password Authentication Protocol),* CHAP (*Challenge Handshake Authentication Protocol)* za autentifikaciju korisnika i kontrolu pristupa mrežnim resursima. L2TP obraća pažnju na tajnost, integritet i autentičnost L2TP paketa između krajnjih tačaka tunela. [5].

4. KONFIGURACIJE

U poglavlju 4, prikazane su proste konfiguracije VPN tehnologije: OpenVPN, IPSec, GRE, PPTP, L2TP.

Konfiguracije su uspostavljene na ruterima namenjenim za ćelijske mreže. Ruteri obezbeđuju podršku za fiksne i mobilne aplikacije kao što su *smart metering*, upravljanje i praćenje na daljinu itd. Podržavaju različite radio opsege na 2G, 3G, 4G ćelijskim tehnologijama. Pouzdana su rešenja zahvaljujući dobrim performansama hardverske platforme raznim mogućnostima VPN tehnologije. Podržavaju razna M2M (*Machine-to-Machine*) rešenja.

Sve konfiguracije predstavljaju uspostavljanje tunela između dve LAN mreže (LAN to LAN). Na jednom kraju je ruter na koji je povezan PC računar, a na drugom ruter na koji je povezan laptop. Tuneli se uspostavljaju preko mobilne mreže, pa je za svaku konfiguraciju, neophodno prethodno konektovati ruter na mobilnu mrežu. Isključen je Firewall.

Na slici 4.1 prikazan je proces konekcije rutera na mobilnu mrežu. Za proces konekcije korišćene su MTS SIM kartice.

Konfiguracija za konekciju na mobilnu mrežu:

Mobile Settings:

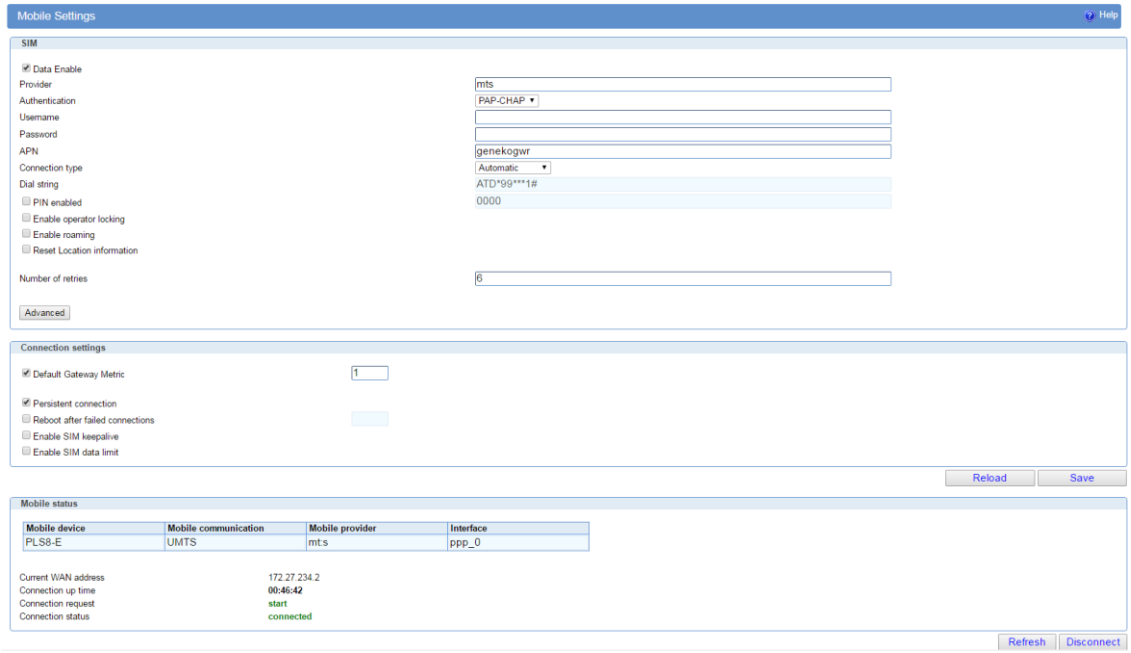
Data Enable: true

Provider: mts

Authentication: PAP-CHAP

APN: genekogwr

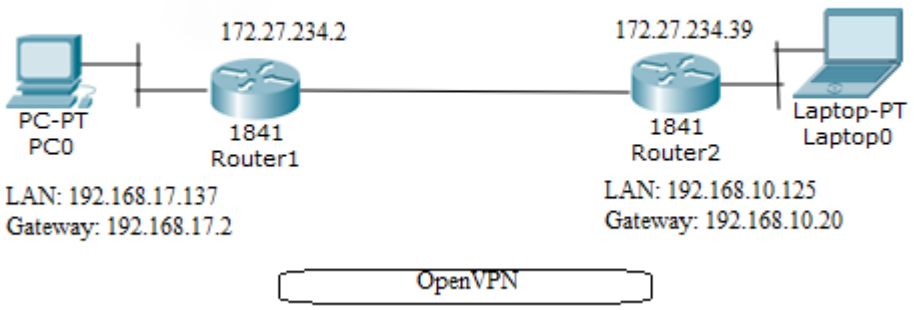
Odabrani provajder je **MTS**, a APN (*Access Point Name*) je **genekogwr**. U dnu strane prikazane na slici 4.1 može se videti IP adresa, dodeljena od MTS mobilnog provajdera: 172.27.234.2



4.1 Konekcija rutera na mobilnu mrežu

4.1. OpenVPN

Na slici 4.1.1 prikazana je prosta OpenVPN konfiguracija.



4.1.1 OpenVPN konfiguracija

OpenVPN je uspostavljen između dva rutera, na čijim krajevima su laptop i PC računar. PC računar i ruter na koji je povezan se nalaze u LAN mreži 192.168.17.0/24 (sa maskom podmreže 255.255.255.0). Laptop i ruter na koji je povezan se nalaze u LAN mreži 192.168.10.0/24 (sa maskom podmreže 255.255.255.0). U ruterima su MTS SIM kartice, sa statičkim IP adresama, dodeljenim od mobilnog provajdera. Statičke IP adrese, dodeljene od mobilnog provajdera su: 172.27.234.2 i 172.27.234.39.

Konfiguracija tunela na ruteru br. 1:

Add New Tunnel

Tunnel Number: 1

Tunnel Name: test

Enable: true

OpenVPN Settings

Interface Type: TUN

Authenticate Mode: pre-shared secret

Encryption Cipher: AES-128-CBC (128 bit)

Hash Algorithm: RSA-SHA1 (160bit)

Protocol: TCP server

TCP Port: 1194

LZO Compression false

NAT Rules: true

Pre-shared Secret: Generate

Local / Remote Group Settings

Redirect Gateway: true

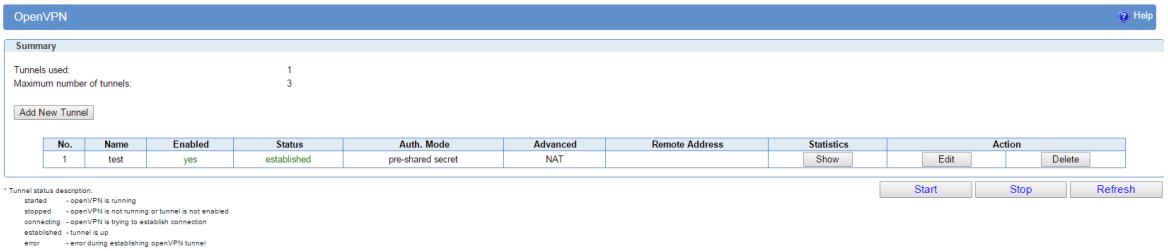
Tunnel Interface Configuration: manual configuration

Local Interface IP Address: 192.168.17.2

Remote Interface IP Address: 192.168.10.20

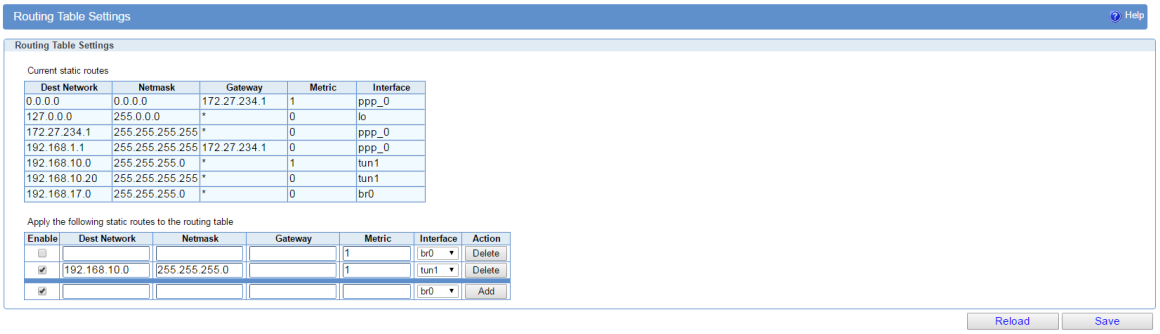
Prenos se vrši preko TCP protokola, a ruter br. 1 predstavlja TCP server. NAT Rule polje je uvek odabrano. Omogućeno je "NATovanje", tj. prevođenje privatnih u javne adrese.

Na slici 4.1.2 je prikazan veb interfejs sa konfigurisanim OpenVPN tunelom za ruter br. 1.



4.1.2 OpenVPN konfiguracija za ruter br. 1

Tabela rutiranja za ruter br.1 prikazana je na slici 4.1.3. Dodata je statička ruta 192.168.10.0, mrežni opseg adresa u kome se nalazi ruter br. 2 i laptop. Odabrani interfejs je tun1, virtuelni mrežni interfejs preko koga se uspostavlja tunel i point-to-point komunikacija.



4.1.3 Tabela rutiranja za ruter br. 1

Konfiguracija tunela na ruteru br. 2:

Add New Tunnel

Tunnel Number: 1

Tunnel Name: test

Enable: true

OpenVPN Settings

Interface Type: TUN

Authenticate Mode: pre-shared secret

Encryption Cipher: AES-128-CBC (128 bit)

Hash Algorithm: RSA-SHA1 (160bit)

Protocol: TCP client

TCP Port: 1194

LZO Compression false

NAT Rules: true

Keep Alive: false

Pre-shared Secret: Generate

Local / Remote Group Settings

Remote Host or IP Address: 172.27.234.2

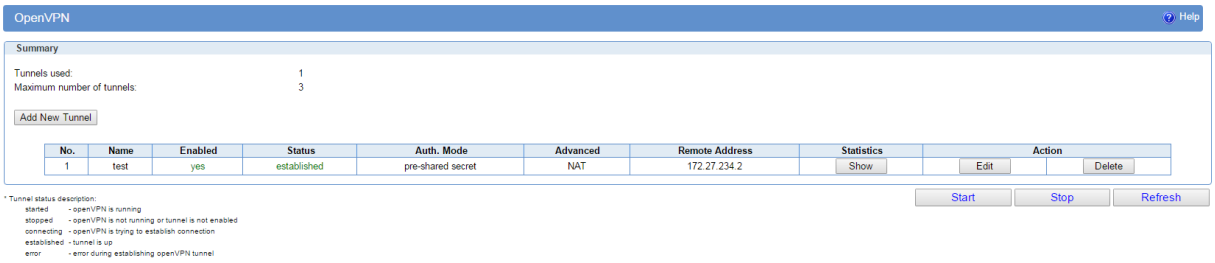
Redirect Gateway: true

Tunnel Interface Configuration: manual configuration

Local Interface IP Address: 192.168.10.20

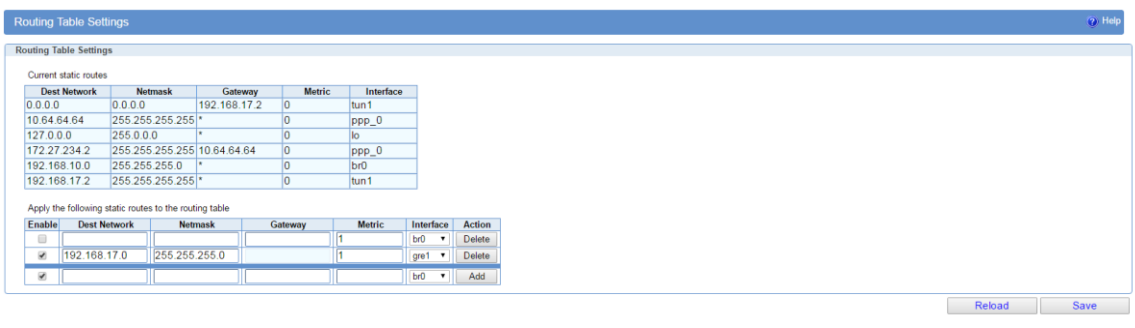
Remote Interface IP Address: 192.168.17.2

Ruter br. 2 predstavlja TCP klijenta, tj. uređaj koji traži uspostavu veze. Na slici 4.1.4 je prikazan veb interfejs sa konfigurisanim OpenVPN tunelom za ruter br. 2.



4.1.4 OpenVPN konfiguracija za ruter br. 2

Tabela rutiranja za ruter br.2 prikazana je na slici 4.1.5. Kako je ruter br 2. TCP klijent, automatski je dodata statička ruta 192.168.17.2, koja predstavlja default gejtvej za ruter br.1. Interfejs je tun1, virtuelni mrežni interfejs preko koga je uspostavljen tunel i point-to-point komunikacija.

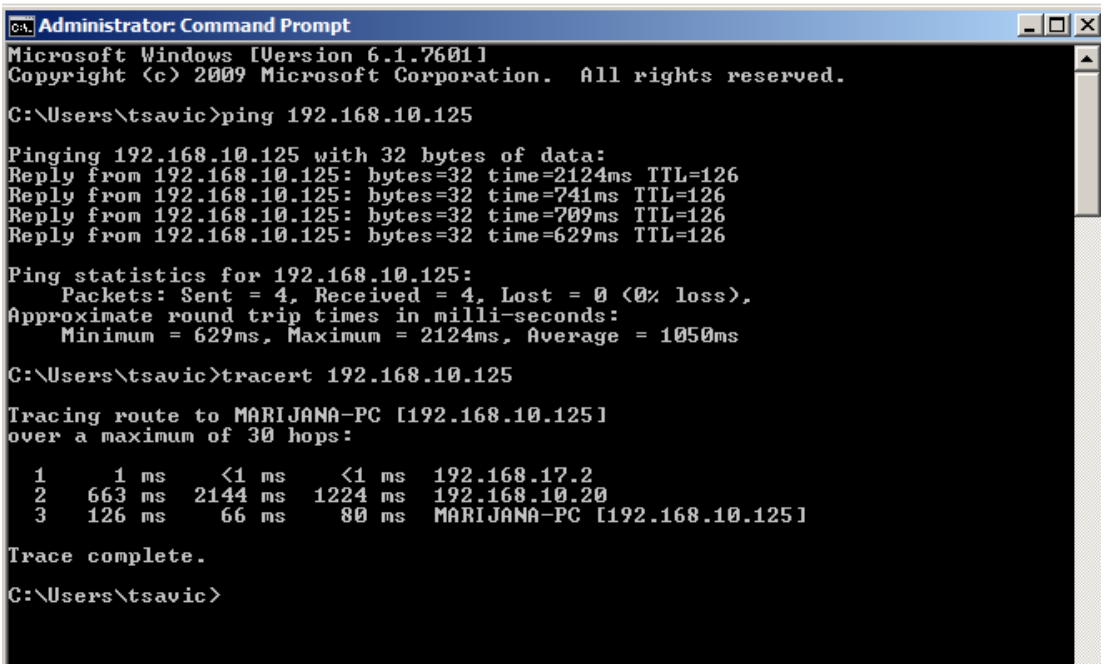


4.1.5 Tabela rutiranja za ruter br. 2

Ping komanda služi za testiranje dostupnosti odredišnog računara na IP mreži i za merenje vremena za koje se vrati poruka poslata od domaćina ka odredišnom računaru. Pušten je ping test sa PC računara, koji ima IP adresu 192.168.17.137 ka laptopu koji je na adresi 192.168.10.125. Dobijanjem odgovora sa laptop-a vidi se da je tunel uspostavljen.

Tracert je komanda koja prikazuje putanju paketa koji nosi informaciju poslatu od izvorišnog ka nekom odredišnom uređaju. Tracert komanda je poslata sa PC računara ka laptopu. Kao rezultat vidi se kojom putanjom prolaze paketi:

Od PC računara stižu do rutera br. 1 (na adresi 192.168.17.2), koji predstavlja default gejtvej za računar. Naredni skok (hop) je ka ruteru br. 2 (na adresi 192.168.10.20), koji predstavlja default gejtvej za ruter br. 2. Poslednji skok (hop) je ka laptopu (na adresi 192.168.10.125). Slika 4.1.6 prikazuje ping test i tracert komandu za uspostavljen OpenVPN tunel.



4.1.6. Ping test i traceroute za uspostavljen OpenVPN tunel

Na slici 4.1.7 i 4.1.8 prikazan je log fajl sa rutera, deo uspostave OpenVPN tunela, startovanje skripti i procesa u Linux operativnom sistemu. Kreira se konfiguracioni fajl i startuje tunel. Prikazani su upotrebljeni algoritmi simetrične enkripcije AES-128 (128 dužina ključa) i SHA (heš funkcija za potpisivanje kontrolne sume izvorne poruke i razmena), kao i razmena poruka za obavljenu inicijalizaciju enkripcije.

```
Aug 14 01:44:25 geneko user.info openVPN: starting openvpn_tunnel_1...
Aug 14 01:44:25 geneko daemon.notice openvpn_tunnel_1[7983]: OpenVPN 2.3.2
arm-buildroot-linux-gnueabihf [SSL (OpenSSL)] [LZO] [EPOLL] [eurephia]
[MH] [IPv6] built on Jul  1 2016
Aug 14 01:44:25 geneko daemon.notice openvpn_tunnel_1[7983]: Static
Encrypt: Cipher 'AES-128-CBC' initialized with 128 bit key
Aug 14 01:44:25 geneko daemon.notice openvpn_tunnel_1[7983]: Static
Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Aug 14 01:44:25 geneko daemon.notice openvpn_tunnel_1[7983]: Static
Decrypt: Cipher 'AES-128-CBC' initialized with 128 bit key
Aug 14 01:44:25 geneko daemon.notice openvpn_tunnel_1[7983]: Static
Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Aug 14 01:44:25 geneko daemon.notice openvpn_tunnel_1[7983]: Socket
Buffers: R=[87380->131072] S=[16384->131072]
Aug 14 01:44:25 geneko daemon.notice openvpn_tunnel_1[7983]: TUN/TAP
device tun1 opened
Aug 14 01:44:25 geneko daemon.notice openvpn_tunnel_1[7983]: TUN/TAP TX
queue length set to 100
```

4.1.7. Log fajl sa rutera br.1 (1)

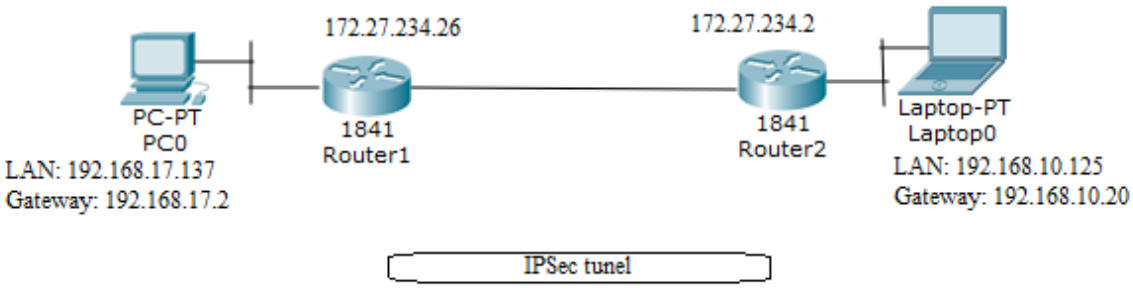
Preko tun1 virtuelnog interfejsa uparuju se ruter br.1 sa ruterom br.2, tj. IP adrese 192.168.17.2 i IP adrese 192.168.10.20. Prikazan je proces upostave TCP konekcije. Nakon uspostavljenog tunela pingovan je ruter 192.168.10.20.

```
Aug 14 01:44:25 geneko daemon.notice openvpn_tunnel_1[7983]: /sbin/ip addr
add dev tun1 local 192.168.17.2 peer 192.168.10.20
Aug 14 01:44:25 geneko daemon.notice openvpn_tunnel_1[7983]:
/home/scripts/proc_openvpn_up.sh tun1 1500 1562 192.168.17.2 192.168.10.20
init
Aug 14 01:44:26 geneko daemon.notice openvpn_tunnel_1[7999]: Listening for
incoming TCP connection on [undef]
Aug 14 01:44:26 geneko user.info openVPN: openvpn_tunnel_1 started = OK
Aug 14 01:44:26 geneko daemon.debug firewall[8001]: (1) Allowing android
access to 169.254.254.254 => 192.168.17.2
Aug 14 01:44:26 geneko daemon.info Firewall[8013]: (3) REFRESH ROUTES...
Aug 14 01:44:30 geneko daemon.notice openvpn_tunnel_1[7999]: TCP
connection established with [AF_INET]172.27.234.54:46869
Aug 14 01:44:30 geneko daemon.notice openvpn_tunnel_1[7999]: TCPv4_SERVER
link local (bound): [undef]
Aug 14 01:44:30 geneko daemon.notice openvpn_tunnel_1[7999]: TCPv4_SERVER
link remote: [AF_INET]172.27.234.54:46869
Aug 14 01:44:37 geneko user.info openVPN: ping[1] to 192.168.10.20
Aug 14 01:44:38 geneko daemon.notice openvpn_tunnel_1[7999]: Peer
Connection Initiated with [AF_INET]172.27.234.54:46869
Aug 14 01:44:40 geneko daemon.notice openvpn_tunnel_1[7999]:
Initialization Sequence Completed
```

4.1.8. Log fajl sa rutera br.1 (2)

4.2. IPSec

IPSec je tip VPN tunela sa sigurnim metodama tunelovanja. Jednostavna mreža sa dva rutera je prikazana na slici 4.2.1.



4.2.1 IPSec tunel (LAN to LAN)

PC računar i ruter na koji je povezan se nalaze u LAN mreži 192.168.17.0/24 (sa maskom podmreže 255.255.255.0). Laptop i ruter na koji je povezan se nalaze u LAN mreži 192.168.10.0/24 (sa maskom podmreže 255.255.255.0). U ruterima su MTS SIM kartice, sa statičkim IP adresama, dodeljenim od mobilnog provajdera. IPSec se uspostavlja preko mobilne mreže. Statičke IP adrese, dodeljenje od mobilnog provajdera su: 172.27.234.26 i 172.27.234.2.

Konfiguracija tunela na ruteru br. 1:

Add New Tunnel

- Tunnel Name: etf,
- Enable: true,
- **Local Group Setup**
- Local Security Gateway Type: IP only
- IP Address: 172.27.234.26
- Local ID Type: IP Address
- Local Security Group Type: Subnet,
- IP Address: 192.168.17.0,
- Subnet Mask: 255.255.255.0.
- **Remote Group Setup**
- Remote Security Gateway Type: IP Only,
- IP Address: 172.27.234.2,
- Remote ID Type: IP Address,
- Remote Security Group Type: Subnet,
- IP Address: 192.168.10.0,
- Subnet Mask: 255.255.255.0.
- **IPSec Setup**
- Key Exchange Mode: IKE with Preshared key,
- Mode: aggressive,
- Phase 1 DH group: Group 2,
- Phase 1 Encryption: AES-128,
- Phase 1 Authentication: SHA1,
- Phase 1 SA Life Time: 28800,
- Perfect Forward Secrecy: false,
- Phase 2 DH group: Group 2,
- Phase 2 Encryption: AES-128,
- Phase 2 Authentication: SHA1,
- Phase 2 SA Life Time: 3600,
- Preshared Key: 0123456789.

- Failover

- Enable IKE Failover: false

- Enable Tunnel Failover: false,

- **Advanced**

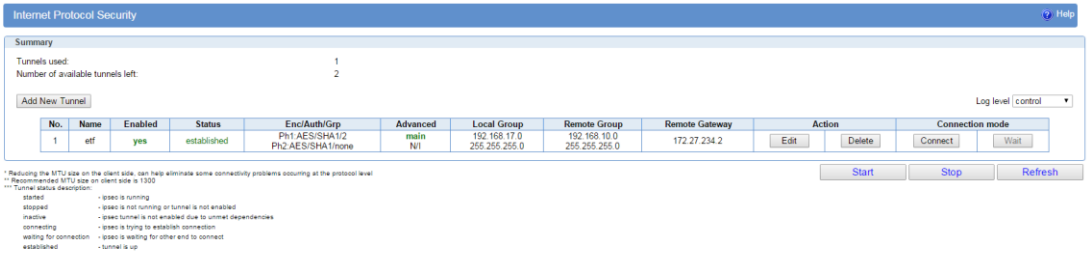
- Compress(Support IP Payload Compression Protocol(IPComp)): false,

- Dead Peer Detection(DPD): false,

- NAT Traversal: true,

- Send Initial Contact: true

Na slici 4.2.2 je prikazan veb interfejs rutera br. 1 na kome je uspostavljen IPSec tunel sa zadatom konfiguracijom.



4.2.2 Uspostavljen IPSec tunel sa zadatom konfiguracijom za ruter br.1

Konfiguracija tunela na ruteru br. 2:

Add New Tunnel

- Tunnel Name: etf,

- Enable: true,

- **Local Group Setup**

- Local Security Gateway Type: IP only

- IP Address: 172.27.234.2

- Local ID Type: IP Address

- Local Security Group Type: Subnet,

- IP Address: 192.168.10.0,

- Subnet Mask: 255.255.255.0.

- **Remote Group Setup**

- Remote Security Gateway Type: IP Only,

- IP Address: 172.27.234.26,

- Remote ID Type: IP Address,

- Remote Security Group Type: Subnet,

- IP Address: 192.168.17.0,

- Subnet Mask: 255.255.255.0

- **IPSec Setup**

- Key Exchange Mode: IKE with Preshared key,

- Mode: aggressive,

- Phase 1 DH group: Group 2,

- Phase 1 Encryption: AES-128,

- Phase 1 Authentication: SHA1,

- Phase 1 SA Life Time: 28800,

- Perfect Forward Secrecy: false,

- Phase 2 DH group: Group 2,

- Phase 2 Encryption: AES-128,

- Phase 2 Authentication: SHA1,

- Phase 2 SA Life Time: 3600,

- Preshared Key: 0123456789.

- Failover

- Enable IKE Failover: false

- Enable Tunnel Failover: false,

- **Advanced**

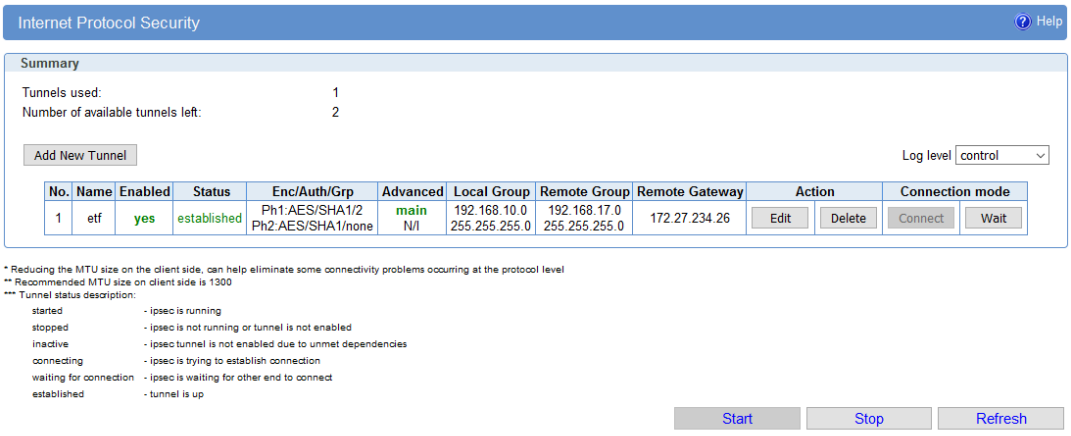
- Compress(Support IP Payload Compression Protocol(IPComp)): false,

- Dead Peer Detection(DPD): false,

- NAT Traversal: true,

- Send Initial Contact: true

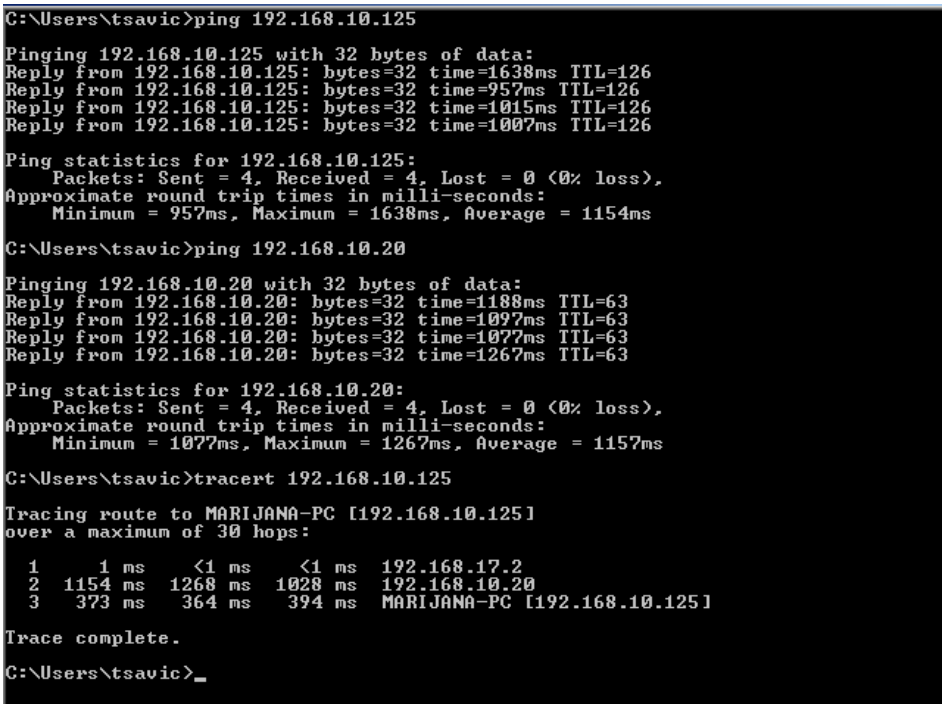
Na slici 4.2.3 je prikazan veb interfejs rutera br. 2 na kome je uspostavljen IPSec tunel sa zadatom konfiguracijom.



4.2.3 Uspostavljen IPSec tunel sa zadatom konfiguracijom za ruter br. 2

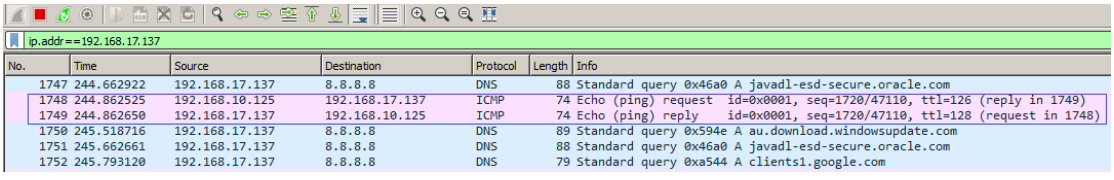
Pušten je ping test sa PC računara , koji ima IP adresu 192.168.17.137 ka laptopu koji je na adresi 192.168.10.125. Dobijanjem odgovora sa laptop-a vidi se da je tunel uspostavljen. Pušten je ping test ka ruteru koji je na adresi 192.168.10.20. Tracert komanda je poslata sa PC računara ka laptopu. Kao rezultat vidi se kojom putanjom prolaze paketi:

Sa PC računara koji je na adresi 192.168.17.137, prelaze na ruter, koji predstavlja uređaj za izlaz računara na mobilnu mrežu (*Default Gateway).* Ruter je na adresi 192.168.17.2. Zatim, ulaze u tunel koji se ostvaruje preko statičkih IP adresa, dobijenih od provajdera. (172.27.234.26 i 172.27.234.2). Naredni skok *(hop)* je ruter koji je ima IP adresu 192.168.10.20 i on za laptop predstavlja uređaj za izlaz na mobilnu mrežu. Odredište je laptop na adresi 192.168.10.125. Na slici 4.2.4 su prikazane ping i tracert komanda.



4.2.4 Ping test i traceroute za uspostavljen IPSec tunel

Slika 4.2.5 prikazuje uhvaćene pakete u wiresharku, puštanjem pinga sa laptop-a (sa adrese 192.168.10.125 na PC računar koji je na adresi 192.168.17.137.



4.2.5 Poslati paketi sa laptopa, prikazani u Wiresharku

IPSec uključuje mnoge komponente tehnologije i metode enkripcije. IPSec proces se može podeliti u pet glavnih koraka:

- "**Zanimljivi saobraćaj**" pokreće IPSec proces. Saobraćaj se smatra interesantnim kada je bezbednosna "politika" IPSeca-a konfigurisana i među IPSec parovima počinje IKE proces.

- **IKE phase 1**. IKE autentifikuje IPSec parove i pregovara IKE SAs (*IPSec Security Associations*) tokom ove faze, formirajući siguran kanal za pregovore IPSec SAs u fazi 2. Osnovna svrha IKE faze 1 je da autentifikuje IPSec parove i da uspostavi siguran kanal između njih omogućujući IKE razmenu. IKE faza 1 obavlja sledeće funkcije:

  - Potvrđuje verodostojnost i štiti identitet IPSec parova

  - Pregovara o poklapanju IKE SA pravila između parova da zaštiti IKE razmenu.

  - Obavlja autentifikovanu Diffie-Hellman razmenu sa krajnjim rezultatom poklapanja deljenih tajnih ključeva (*shared secret keys*).

  - Uspostavlja siguran tunel za pregovaranje IKE faze 2 parametara.

  - IKE faza 1 se javlja u dva moda: *main* i *aggressive*.

  ***Main* mod** ima tri dvosmerne razmene između inicijatora i prijemnika.

  Prva razmena: Algoritmi i heševi se koriste da osiguraju IKE komunikaciju i obezbede IKE SAs usklađivanje u svakom paru.

  Druga razmena: Koristi Diffie-Hellman razmenu da generiše materijal koji se koristi da generiše deljeni, tajne ključeve i da prođe proveru slučajnih brojeva poslatih na drugoj strani, a zatim i potpisom da dokažu svoj identitet.

  Treća razmena: Proverava identitet druge strane. Identitet vrednost je IP adresa IPSec para u šifrovanom obliku. Rezultat u *main* modu je poklapanje IKE SAs između parova da obezbede zaštitni tunel za naredne zaštićene ISAKMP (*Internet Security Association and Key Management Protocol)* razmene između IKE parova. IKE SA specificira vrednost za IKE razmenu: koji metod autentifikacije se koristi, enkripcija i heš algoritmi, koja Diffie-Hellman grupa je u upotrebi, vreme života IKE SA u sekundama i kilobajtima i vrednost deljenog, tajnog ključa za enkripciju algoritama. IKE SA u svakom paru je dvosmerna.

  Aggressive mod služi za manje razmene i manje pakete. Pri prvoj razmeni, gotovo sve je smešteno u predložene IKE SA vrednosti: Diffie-Helman javni ključ, paket koji nosi identitet i koji se može koristiti da verifikuje identitet preko nekog trećeg segmenta. Primalac šalje sve nazad, što je potrebno da se kompletira razmena. Jedino što ostaje za inicijatora je da potvrdi razmenu. Slabost upotrebe *aggressive* moda je što obe strane imaju razmenjene informacije pre nego što je uspostavljen siguran kanal. Moguće je da se dogodi ”snifovanje” (*sniff*) i otkrije ko je formirao SA.

- **IKE phase 2.** IKE pregovara IPSec SA parametre i uspostavlja poklapanje IPSec SAs u parove, tj omogućava uspostavljanje IPSec tunela. IKE faza 2 obavlja seledeće funkcije:

  - Pregovara IPSec SA parametre zaštićene postojećim IKE SA

  - Periodično pregovara IPSec SAs da osigura bezbednost

  - Opciono vrši dodatnu Diffie-Hellman razmenu

  IKE phase 2 ima jedan mod, koji se naziva *quick* mod. Quick mod se javlja nakon što je IKE uspostavio siguran tunel u fazi 1. Pregovara u razmeni ključeva ’’*shared IPSec policy*’’, stvara deljene, tajne ključeve koji se koriste za bezbednosne algoritme i uspostavlja IPSec SAs.

Quick mod se takođe koristi za ponovne pregovore sa novim IPSec SA, kada vreme života IPSec SA istekne. Osnovni quick mod se koristi da osveži ključeve koji se koriste da kreiraju deljene, tajne ključeve bazirane na ključevima koji su nastali u Diffie-Helman razmeni u fazi 1.

- **Prenos podataka.** Podaci se prenose između IPSec parova na osnovu IPSec parametara i ključeva čuvanih u SA bazi podataka.

  Kada je faza 2 potpuna i quick mod je uspostavio IPSec SAs, informacije se razmenjuju u IPSec tunelu. Paketi se enkriptuju i dekriptuju koristeći enkripciju definisanu u IPSec SA.

- **Prekid IPSec tunela.** IPSec SAs prekida tunel brisanjem ili isticanjem vremenskog intervala.

  -SA može isteći kada je određeni broj sekundi proteklo ili kada je je prošao određen broj bajtova kroz tunel. Kada je potreban sledeći SAs za protok, IKE obavlja novu fazu 2 i, ako je potrebno novu fazu 1 pregovaranja. Uspešno pregovaranje rezultira novim SAs i novim ključevima. Novi SAs može biti uspostavljen pre nego što stari istekne, tako da se protok nastavlja bez prekida [7].

  U našem slučaju odabrano je:

IPSec Setup

- Key Exchange Mode: IKE with Preshared key,
- Mode: aggressive,
- Phase 1 DH group: Group 2,
- Phase 1 Encryption: AES-128,
- Phase 1 Authentication: SHA1,
- Phase 1 SA Life Time: 28800,
- Perfect Forward Secrecy: false,
- Phase 2 DH group: Group 2,
- Phase 2 Encryption: AES-128,
- Phase 2 Authentication: SHA1,
- Phase 2 SA Life Time: 3600,
- Preshared Key: 0123456789

Na slikama 4.2.6 i 4.2.7 prikazan je log fajl sa rutera, deo uspostave IPSec tunela, startovanje skripti i procesa u Linux operativnom sistemu. Prikazana je IKE faza 2 i quick mod, slanje paketa između statičkih IP adresa dodeljenih od provajdera (172.27.234.2 i 172.27.234.26). Startuje se IPSec servis i kreira konfiguracioni fajl. Startuje se strongswan. Strongswan je implementacija IPSec-a, za Linux operativni sistem. Fokus je na snažnim mehanizmima autentifikacije koristeći X.509 verzije sertifikata ključeva. Startovanjem strongswan-a svi tuneli su aktivni i prenos može da se vrši.

```
Aug 19 14:52:25 geneko daemon.info charon: 24[ENC] parsed QUICK_MODE
request 1086614877 [ HASH ]
Aug 19 14:52:25 geneko daemon.info charon: 24[IKE] CHILD_SA ipsec1{1}
established with SPIs c1f0ce6e_i cff55a5b_o and TS 192.168.17.0/24 ===
192.168.10.0/24
Aug 19 14:52:25 geneko authpriv.info charon: 24[IKE] CHILD_SA ipsec1{1}
established with SPIs c1f0ce6e_i cff55a5b_o and TS 192.168.17.0/24 ===
192.168.10.0/24
Aug 19 14:52:25 geneko daemon.info charon: 25[NET] received packet: from
172.27.234.2[500] to 172.27.234.26[500] (196 bytes)
Aug 19 14:52:25 geneko daemon.info charon: 25[ENC] parsed QUICK_MODE
request 975300086 [ HASH SA No ID ID ]
Aug 19 14:52:25 geneko daemon.info charon: 25[IKE] detected rekeying of
CHILD_SA ipsec1{1}
Aug 19 14:52:25 geneko daemon.info charon: 25[ENC] generating QUICK_MODE
response 975300086 [ HASH SA No ID ID ]
Aug 19 14:52:25 geneko daemon.info charon: 25[NET] sending packet: from
172.27.234.26[500] to 172.27.234.2[500] (172 bytes)
Aug 19 14:52:25 geneko daemon.info charon: 26[NET] received packet: from
172.27.234.2[500] to 172.27.234.26[500] (68 bytes)
Aug 19 14:52:25 geneko daemon.info charon: 26[ENC] parsed INFORMATIONAL_V1
request 3256836227 [ HASH N(NO PROP) ]
```

4.2.6 Log fajl sa rutera br.1 (1)

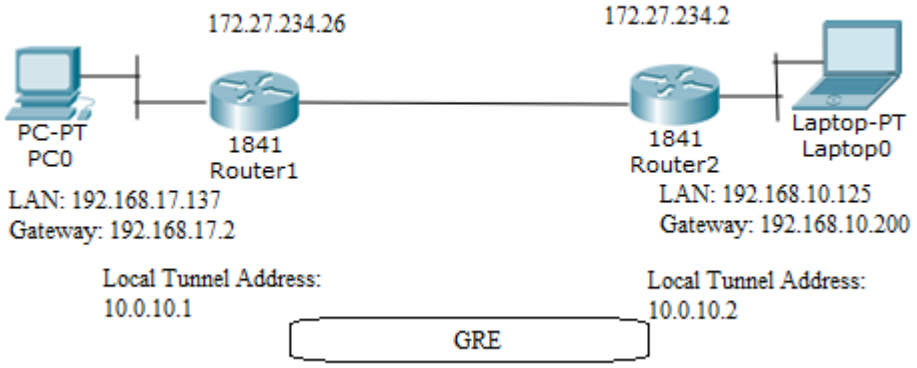
```
Aug 19 14:55:04 geneko user.info IPSec[3949]: Starting IPSec service
Aug 19 14:55:04 geneko user.info IPSec: ipsec start...
Aug 19 14:55:05 geneko user.info IPSec[3949]: creating secrets file...
Aug 19 14:55:05 geneko user.info IPSec[3949]: secrets file created = OK
Aug 19 14:55:05 geneko user.info IPSec[3949]: creating conf file...
Aug 19 14:55:06 geneko user.info IPSec[3949]: conf file created = OK
Aug 19 14:55:06 geneko daemon.debug firewall[4021]: (1) Allowing android
access to 169.254.254.254 => 192.168.17.2

Aug 19 14:55:07 geneko user.info IPSec[3949]: starting strongswan...
Aug 19 14:55:07 geneko authpriv.info ipsec_starter[4056]: Starting
strongSwan 5.1.1 IPsec [starter]...
Aug 19 14:55:12 geneko user.info IPSec[3949]: strongswan started = OK
Aug 19 14:55:14 geneko user.info IPSec[3949]: all tunnels up...
Aug 19 14:55:14 geneko daemon.info charon: 24[NET] received packet: from
172.27.234.2[500] to 172.27.234.26[500] (156 bytes)
```

4.2.7 Log fajl sa rutera br.1 (2)

Zbog toga što ima enkripciju, autentifikaciju, integritet i upravljanje ključevima IPSec se smatra najboljim VPN rešenjem kada je siguran prenos u pitanju.

4.3. GRE

GRE je tip VPN tunela, ali ne predstavlja sigurnu metodu tunelovanja. Jednostavna mreža sa dva rutera je prikazana na slici 4.3.1.



4.3.1 GRE konfiguracija

PC računar i ruter na koji je povezan se nalaze u LAN mreži 192.168.17.0/24 (sa maskom podmreže 255.255.255.0). Laptop i ruter na koji je povezan se nalaze u LAN mreži 192.168.10.0/24 (sa maskom podmreže 255.255.255.0). U ruterima su MTS SIM kartice, sa statičkim IP adresama, dodeljenim od mobilnog provajdera. GRE tunel se uspostavlja na nivou rutera. Statičke IP adrese, dodeljene od mobilnog provajdera su: 172.27.234.26 i 172.27.234.2.

Konfiguracija rutera br. 1:

-Enable: true

-Local Tunnel Address:10.0.10.1

-Local Tunnel Network: 255.255.255.2

-Tunnel Source: IP

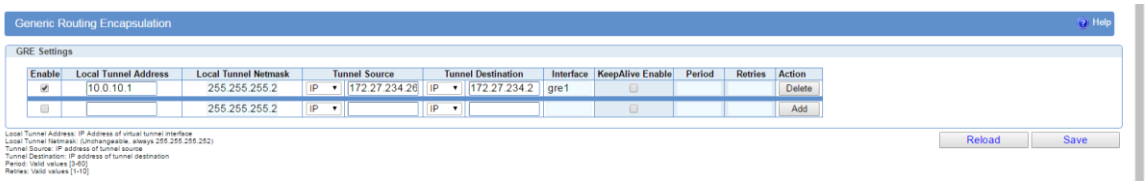
-Tunnel Source: 172.27.234.26

-Tunnel Destination: IP

-Tunnel Destination: 172.27.234.2

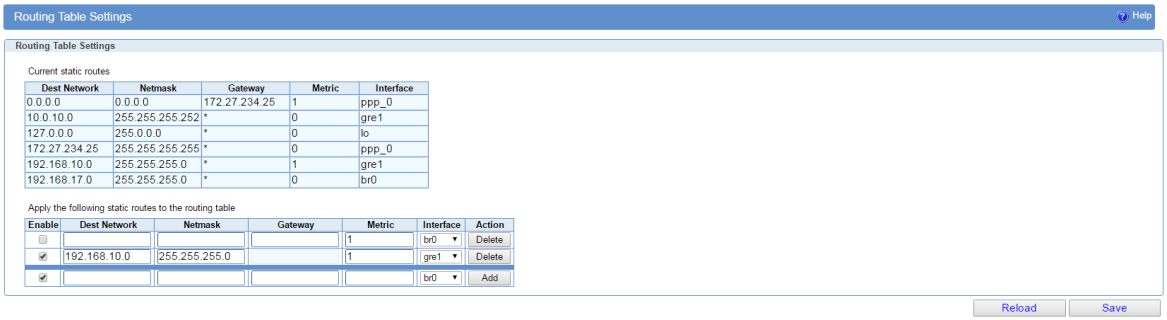
-Interface: gre1

Za Local Tunnel Address biraju se dve IP adrese. Na jednoj strani dodeljena je IP adresa 10.0.10.1, a na drugoj 10.0.10.2., sa maskom podmreže 255.255.255.2, na kojima se formira GRE tunel na virtuelnom interfejsu gre1. Na slici 4.3.2 je prikazan veb interfejs sa konfiguracijom GRE tunela na ruteru br. 1.



4.3.2 Konfiguracija GRE tunela za ruter br. 1

U tabelu rutiranja rutera br. 1 dodaje se mrežni opseg adresa (192.168.10.0) na kojim se nalaze ruter br. 2 i laptop. Za ruter br.1 veb interfejs sa tabelom rutiranja prikazan je na slici 4.3.3.



4.3.3 Tabela rutiranja za ruter br. 1

Konfiguracija rutera br. 2:

-Enable: true

-Local Tunnel Address:10.0.10.2

-Local Tunnel Network: 255.255.255.2

-Tunnel Source: IP

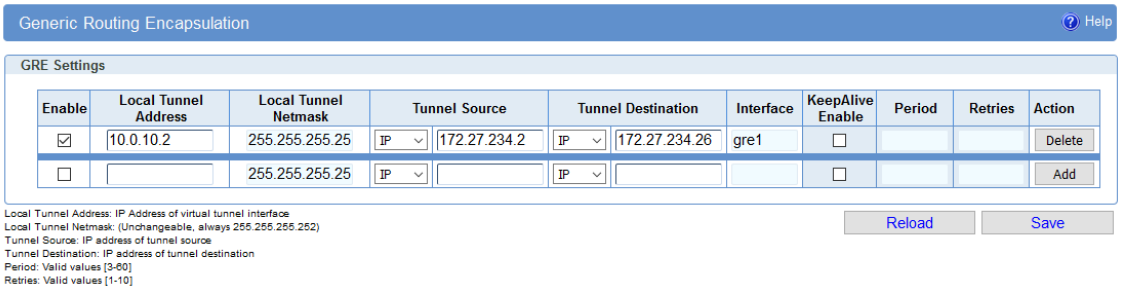
-Tunnel Source: 172.27.234.2

-Tunnel Destination: IP

-Tunnel Destination: 172.27.234.26

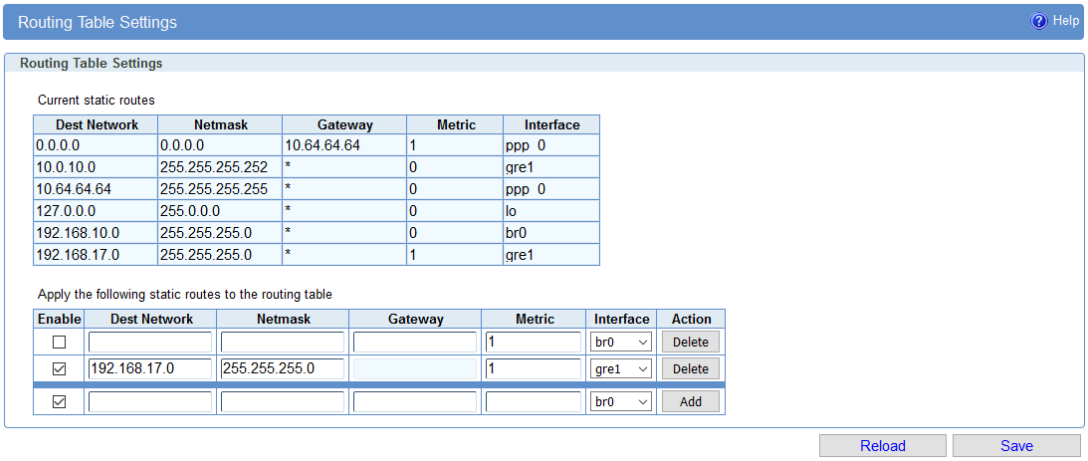
-Interface: gre1

Na slici 4.3.4 je prikazan veb interfejs sa konfiguracijom GRE tunela na ruteru br. 2.



4.3.4 Konfiguracija GRE tunela za ruter br.2

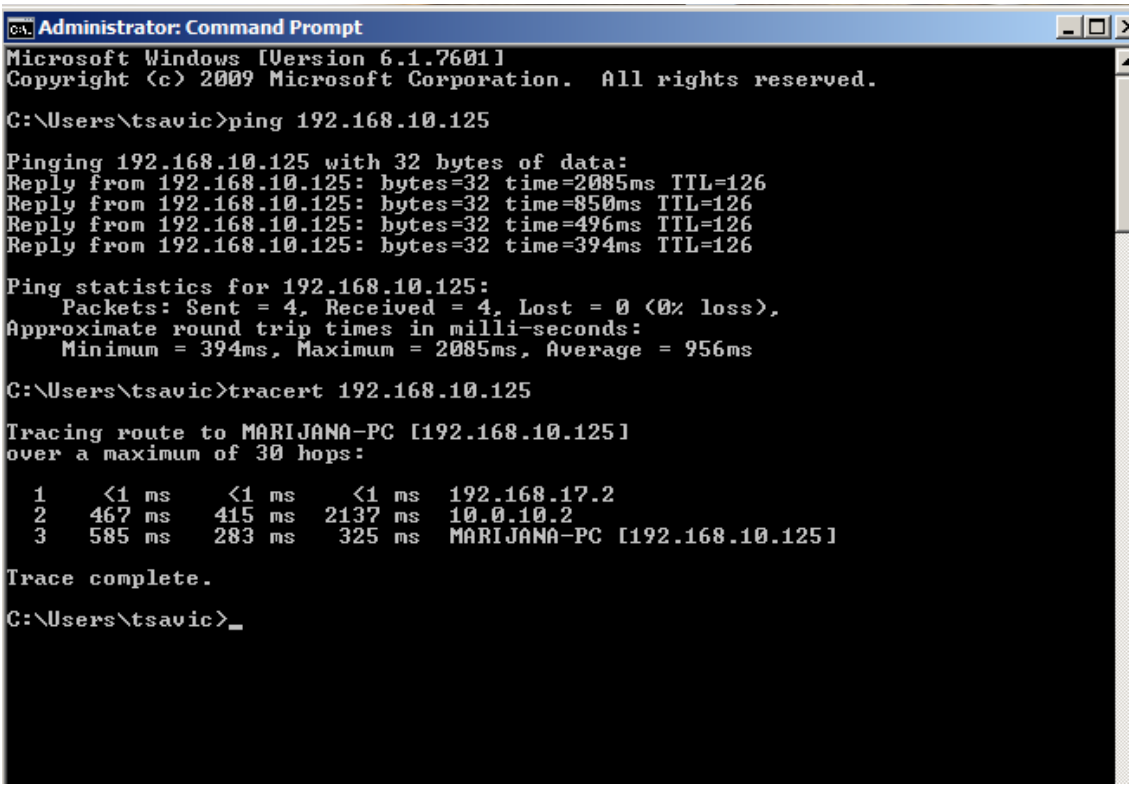
U tabelu rutiranja rutera br. 2 dodaje se mrežni opseg adresa (192.168.17.0) na kojim se nalaze ruter br. 1 i PC računar. Za ruter br.2 veb interfejs sa tabelom rutiranja prikazan je na slici 4.3.5.



4.3.5 Tabela rutiranja za ruter br. 2

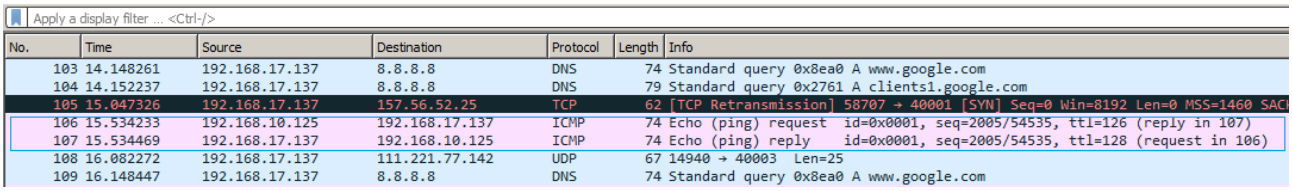
Pušten je ping test sa PC računara, koji se nalazi na adresi 192.168.17.137, ka laptopu koji se nalazi na adresi 192.168.10.125. Dobijanjem odziva sa laptopa, vidi se da je tunel uspostavljen.

Komandom tracert prikazana je putanja paketa kroz tunel, sa računara ka laptopu. Prvi skok (hop) je ka ruteru br. 1 koji je na adresi 192.168.17.2, zatim ka ruteru br. 2 koji sada ima adresu 10.0.10.2 i poslednji skok ka odredištu, tj. ka laptop-u kome je dodeljena adresa 192.168.10.125.



4.3.6 Ping test i traceroute za uspostavljen GRE tunel

Na slici 4.3.7 vide se paketi uhvaćeni u wiresharku, puštanjem ping testa sa laptopa (IP adresa 192.168.10.125), ka računaru (IP adresa 192.168.17.137).



No.	Time	Source	Destination	Protocol	Length	Info
103	14.148261	192.168.17.137	8.8.8.8	DNS	74	Standard query 0x8ea0 A www.google.com
104	14.152237	192.168.17.137	8.8.8.8	DNS	79	Standard query 0x2761 A clients1.google.com
105	15.047326	192.168.17.137	157.56.52.25	TCP	62	[TCP Retransmission] 58707 → 40001 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SAC
106	15.534233	192.168.10.125	192.168.17.137	ICMP	74	Echo (ping) request id=0x0001, seq=2005/54535, ttl=126 (reply in 107)
107	15.534469	192.168.17.137	192.168.10.125	ICMP	74	Echo (ping) reply id=0x0001, seq=2005/54535, ttl=128 (request in 106)
108	16.082272	192.168.17.137	111.221.77.142	UDP	67	14940 → 40003 Len=25
109	16.148447	192.168.17.137	8.8.8.8	DNS	74	Standard query 0x8ea0 A www.google.com

4.3.7 Poslati paketi sa laptopa, prikazani u Wiresharku

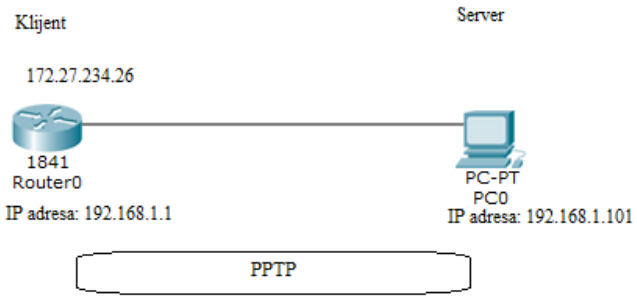
```
Aug 19 15:41:56 geneko user.notice udev[8817]: gre1 [] remove
Aug 19 15:41:57 geneko user.notice udev[8828]: gre1 [ac:1b:ea:1a] add
Aug 19 15:41:57 geneko daemon.info gre[8823]: (1) gre tunnel gre1 created
Aug 19 15:41:57 geneko daemon.info Firewall[8823]: (3) REFRESH ROUTES...
Aug 19 15:41:57 geneko daemon.debug firewall[8823]: (1) Allowing android
access to 169.254.254.254 => 192.168.17.2
```

4.3.8 Log fajl sa rutera br. 2

Iz log fajla se vidi kreiranje GRE tunela i da ne koristi nikakve metode zaštite, tj krajnje tačke ne koordiniraju parametre pre slanja saobraćaja kroz tunel. Dokle god je destinacija u tabeli rutiranja saobraćaj može da ide tom putanjom. GRE ne obezbeđuje pouzdanost ili redosled. GRE tuneli nude minimalnu bezbednost u odnosu na IPSec koji obezbeđuje pouzdanost, autentifikaciju podataka i integritet. GRE ima osnovne mehanizme enkripcije, ali se ključ nosi zajedno sa paketom, što donekle smanjuje svrhu. GRE je jednostavan, ali moćan alat za tunelovanje. Podržava bilo koji OSI protokol sloja 3 preko IP-a, što u osnovi predstavlja point-to-point privatnu vezu. Privatna veza između dve krajnje tačke je osnovna definicija VPN-a [8].

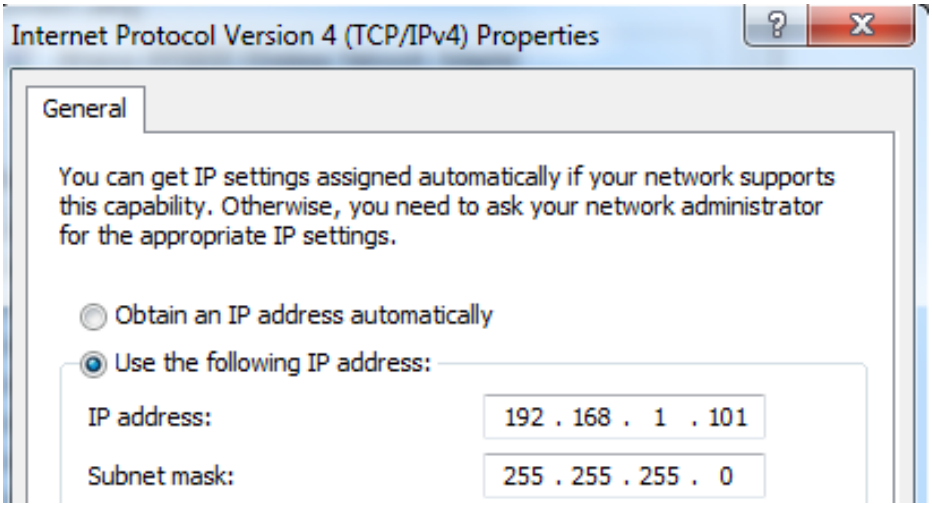
4.4. PPTP

Konfiguracija PPTP tunela je prikazana na slici 4.4.1.



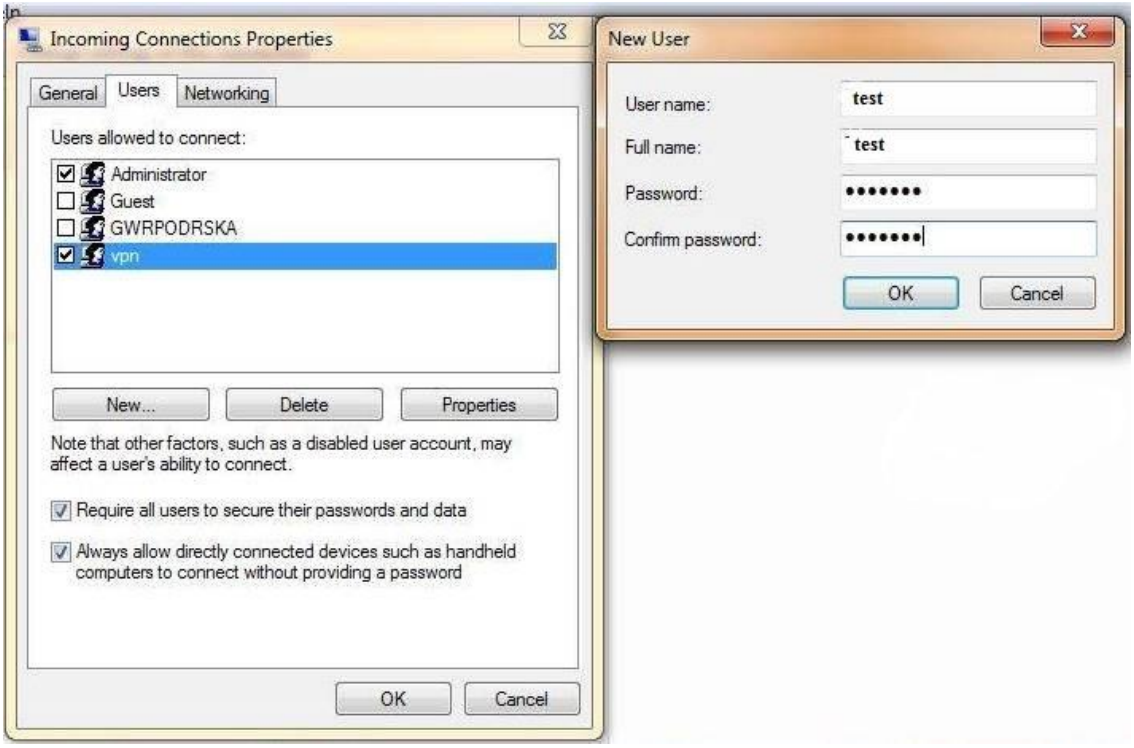
4.4.1 PPTP konfiguracija

Na Windows 7 potrebno je podići server za PPTP, koji se nalazi na adresi 192.168.1.101. Na mrežnoj kartici dodata je IP adresa 192.168.1.101, sa maskom podmreže 255.255.255.0.



4.4.2 Dodavanje IP adrese

Kreirana je nova VPN konekcija, tj konfiguracija koja omogućava da kompjuter prihvati VPN konekciju i podešavanja sa rutera za Point-to-Point Protocol (PPTP), na Windows 7. U Network and Sharing Center podešavanju, kliknuti na Change adapter settings, zatim na New Incoming Connection. Dodati novog korisnika (user) i šifru, koji će se upisati pri konfigurisanju tunela na ruteru.



4.4.3 Kreiranje nove konekcije

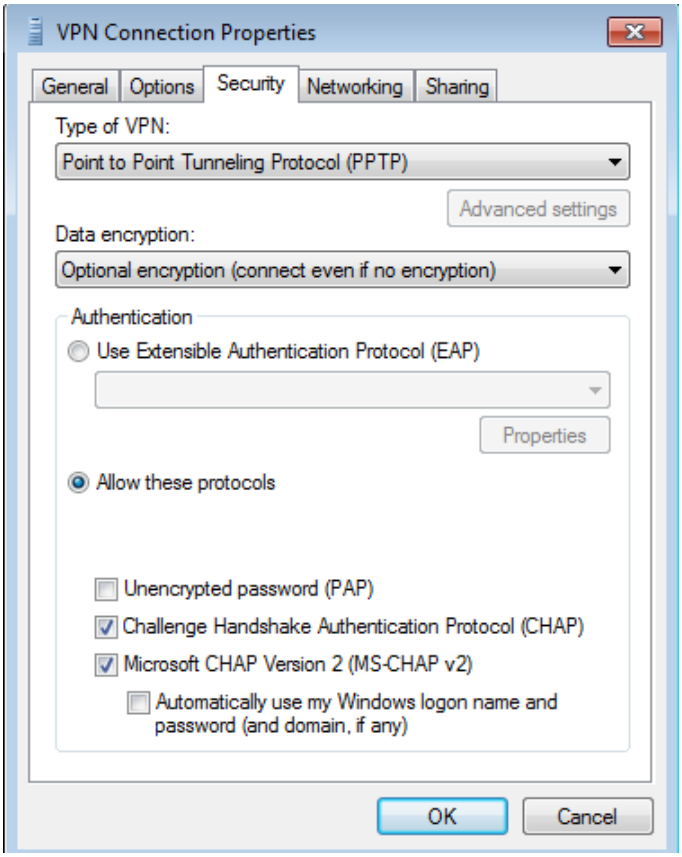
Podešavanje test(test) WAN Miniport (PPTP) prikazano je na slici 4.4.3. Upisuje se u polje User name: test, a u polje Password šifra koju smo odabrali pri kreiranju VPN konekcije.

4.4.3 Podešavanje VPN konekcije (1)

U polju Security, za tip VPN konekcije odabrano je Point to Point Tunneling Protocol (PPTP), tip autentifikacije Challenge Handshake Authentication Protocol (CHAP).

PPTP protokol vrši enkapsulaciju PPP paketa od polazne tačke, preko Interneta, do odredišta. Za autentifikaciju korisnika koristi PPP protokole PAP (*Password Authentication Protocol*) ili CHAP (*Challenge Handshake Authentication Protocol*). PAP protokol predstavlja standardnu proceduru logovanja klijenta kod servera sa korisničkim imenom i lozinkom. CHAP protokol koristi periodično generisani string koji server šalje klijentu. Ovaj primenjuje heš funkciju na taj string i otisak kao rezultat vraća serveru. Server obavlja istu heš operaciju i autentifikuje klijenta ako je rezultat isti sa onim dobijenim od klijenta. Za tunelovanje PPP paketa preko Interneta PPTP koristi GRE protokol. Kriptovanje tunelovanih PPP paketa u PPTP protokolu vrši MPPE (*Microsoft Point-to-Point Encryption*) protokol. MPPE protokol koristi za kriptovanje RSA RC4 algoritam, sa ključevima dužine 40 ili 128 bita koji se menjaju periodično [9].

Na slici 4.4.4 prikazana su podešavanja VPN konekcije u polju Security.



4.4.4 Podešavanje VPN konekcije (2)

Konfiguracija na ruteru:

PPTP Tunnel Settings

Number: 1

Enabled: true

Tunnel name: test

PPTP server IP address or hostname: 192.168.1.101

Remote network: 192.168.1.0

Remote netmask: 255.255.255.0

Username: test

Password:

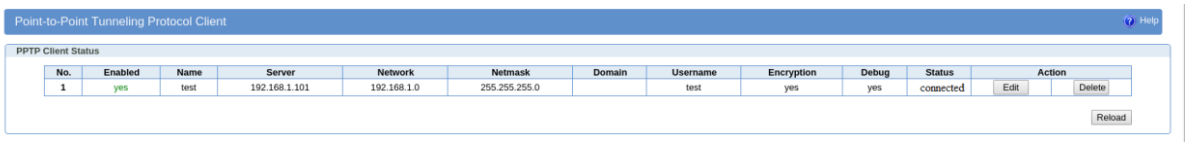
Encryption: true

Persist: true

Maxfail: 10

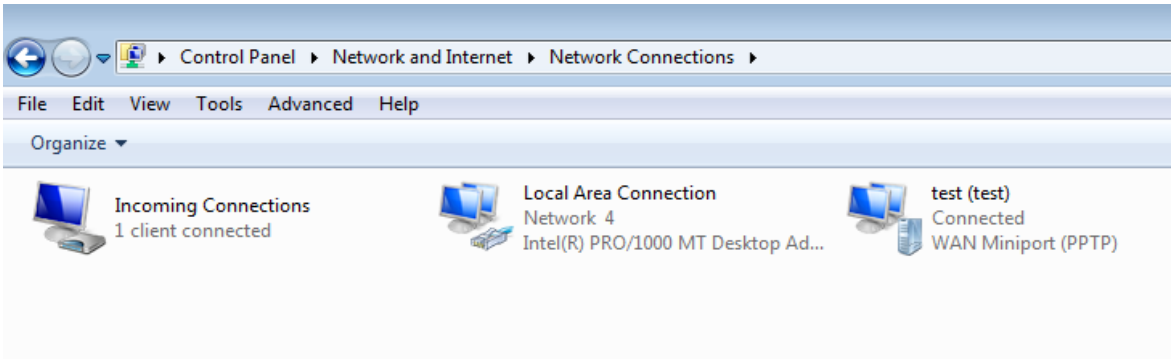
Debug: true

Tunel name, username i šifra su proizvoljni. Veb interfejs rutera sa konfigurisanim i uspostavljenim tunelom prikazan je na slici 4.4.5.



4.4.5 PPTP konfiguracija na ruteru

Na test kartici vidimo da je uspostavljena konekcija, što se vidi na slici 4.4.6.



4.4.6 Uspostavljena PPTP konekcija

Na slici 4.4.7 prikazan je log fajl sa rutera, deo uspostave PPTP tunela, startovanje skripti i procesa u Linux operativnom sistemu, razmena poruka za CHAP autentifikaciju.

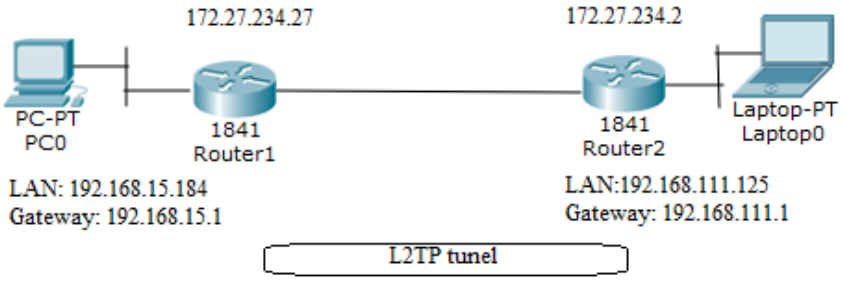
```
Aug 14 03:38:34 geneko daemon.info pppd[16923]: Using interface pptp1
Aug 14 03:38:34 geneko daemon.notice pppd[16923]: Connect: pptp1 <-->
/dev/pts/0
Aug 14 03:38:35 geneko daemon.notice pptp[2752]: anon
log[ctrlp_rep:pptp_ctrl.c:258]: Sent control packet type is 1 'Start-
Control-Connection-Request'
Aug 14 03:38:35 geneko daemon.notice pptp[16938]: anon
log[ctrlp_disp:pptp_ctrl.c:758]: Received Start Control Connection Reply
Aug 14 03:38:35 geneko daemon.notice pptp[16938]: anon
log[ctrlp_disp:pptp_ctrl.c:792]: Client connection established
Aug 14 03:38:35 geneko daemon.debug pppd[16923]: sent [LCP ConfReq id=0x1
<mru 1450> <asyncmap 0x0> <magic 0xfe9a78a2> <pcomp> <accomp>]
Aug 14 03:38:36 geneko daemon.notice pptp[16938]: anon
log[ctrlp_rep:pptp_ctrl.c:258]: Sent control packet type is 7 'Outgoing-
Call-Request'
Aug 14 03:38:36 geneko daemon.notice pptp[16938]: anon
log[ctrlp_disp:pptp_ctrl.c:877]: Received Outgoing Call Reply.
Aug 14 03:38:36 geneko daemon.notice pptp[16938]: anon
log[ctrlp_disp:pptp_ctrl.c:916]: Outgoing call established (call ID 0,
peer's call ID 50966)
[local:b2.eb.67.b1.37.89.45.09.bf.7b.94.a9.87.db.f4.30.00.00.00.00]>]
Aug 14 03:38:38 geneko daemon.debug pppd[16923]: sent [LCP ConfAck id=0x1
<mru 1400> <auth chap MS-v2> <magic 0x5d245336> <pcomp> <accomp> <endpoint
Aug 14 03:38:38 geneko daemon.debug pppd[16923]: rcvd [CHAP Challenge
id=0x0 <fb60e6058f20fcfc7beb533aa9cf6093>, name = "VM-DEVEL01-PC"]
Aug 14 03:38:38 geneko daemon.debug pppd[16923]: sent [CHAP Response
id=0x0
<29f75a5fa1ab605c51166e50889c18ee0000000000000000c339e2a17030faad4ea169ef3
cb9bf0a05807f7c43a386fb00>, name = "test"]
Aug 14 03:38:38 geneko daemon.debug pppd[16923]: rcvd [LCP EchoRep id=0x0
magic=0x5d245336]
Aug 14 03:38:38 geneko daemon.debug pppd[16923]: rcvd [CHAP Success id=0x0
"S=A43F271A9BAF4137EC4A0C75F412F61EB1F2831F"]
Aug 14 03:38:38 geneko daemon.notice pppd[16923]: CHAP authentication
succeeded
```

4.4.7 Log fajl PPTP tunela na ruteru

PPTP prenosi podatke preko TCP-a. Mogu se javiti problemi sa firewall-om jer firewall ne prepoznaje GRE. PPTP za razliku od L2TP-a odvojeno šalje kontrolne informacije i podatke – prve putem TCP-a, a druge putem GRE-a (manje popularan Internet standard).

4.5. L2TP

L2TP je tip VPN tunela koji ne obezbeđuje enkripciju ili pouzdanost. On se oslanja na protokol za šifrovanje koji je u sklopu tunela i obezbeđuje privatnost. Jednostavna mreža sa dva rutera je prikazana na slici 4.5.1.



4.5.1 L2TP konfiguracija

PC i ruter na koji je povezan se nalaze u LAN mreži 192.168.15.0/24 (sa maskom podmreže 255.255.255.0). Laptop i ruter na koji je povezan se nalaze u LAN mreži 192.168.111.0/24 (sa maskom podmreže 255.255.255.0). U ruterima su MTS SIM kartice, sa statičkim IP adresama, dodeljenim od mobilnog provajdera. Statičke IP adrese, dodeljenje od mobilnog provajdera su: 172.27.234.27 i 172.27.234.2.

Konfiguracija rutera br. 1:

-Enabled: true

-Name: test

-Local IP address: 172.27.234.27

-Tunnel ID: 1

-UDP Source Port: 80

-Session ID: 80

-Peer IP address: 172.27.234.2

-Peer Tunnel ID: 2

-UDP Destination Port: 81

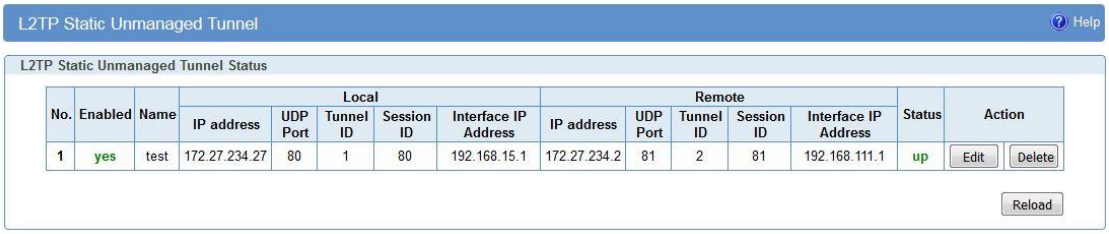
-Peer Session ID: 81

-Interface IP Address: 192.168.15.1

-Peer Interface IP Address: 192.168.111.1

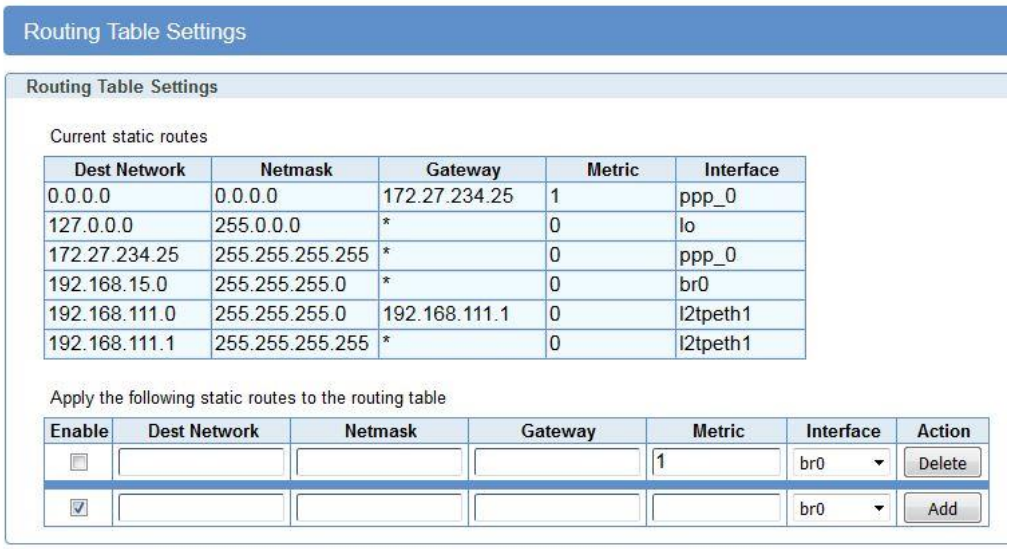
-MTU 1488

Veb interfejs rutera br. 1 sa konfigurisanim i uspostavljenim tunelom prikazan je na slici 4.5.2.



4.5.2 L2TP konfiguracija tunela na ruteru br. 1

U tabelu rutiranja rutera br. 1 dodaje se mrežni opseg adresa na kome se nalaze ruter br. 2 i PC računar, IP adresa na kojoj se nalazi ruter br. 2 (192.168.111.1), obe na l2tpeth1 virtuelnom mrežnom interfejsu na kome se uspostavlja L2TP tunel. Kada je L2TP sesija uspostavljena kreira se virtuelni mrežni interfejs za tu sesiju, koji je konfigurisan i upostavljen kao bilo koji drugi mrežni interfejs. Kada podaci prođu kroz interfejs, prenose se kroz L2TP tunel do svoga para. Konfigurisanjem tabele rutiranja i dodavanjem interfejsa, L2TP interfejs postaje virtuelna povezanost do para, na drugom kraju. U primeru ovih konfiguracija, to predstavlja l2tpeth1 virtuelni interfejs. Adresa 192.168.111.1 predstavlja gejtvej za PC računar, tj za mrežu 192.168.111.0 (sa maskom podmreže 255.255.255.0). Za ruter br.2 veb interfejs sa tabelom rutiranja prikazan je na slici 4.5.3.



4.5.3 Tabela rutiranja za ruter br. 1

Konfiguracija rutera br. 2:

-Enabled: true

-Name: test

-Local IP address: 172.27.234.2

-Tunnel ID: 2

-UDP Source Port: 81

-Session ID: 81

-Peer IP address: 172.27.234.27

-Peer Tunnel ID: 1

-UDP Destination Port: 80

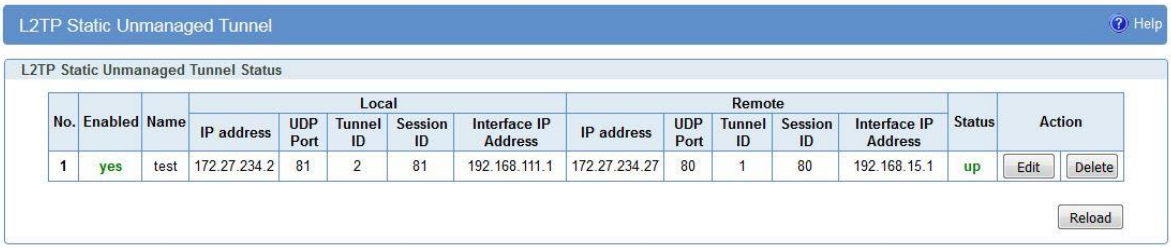
-Peer Session ID: 80

-Interface IP Address: 192.168.111.1

-Peer Interface IP Address: 192.168.15.1

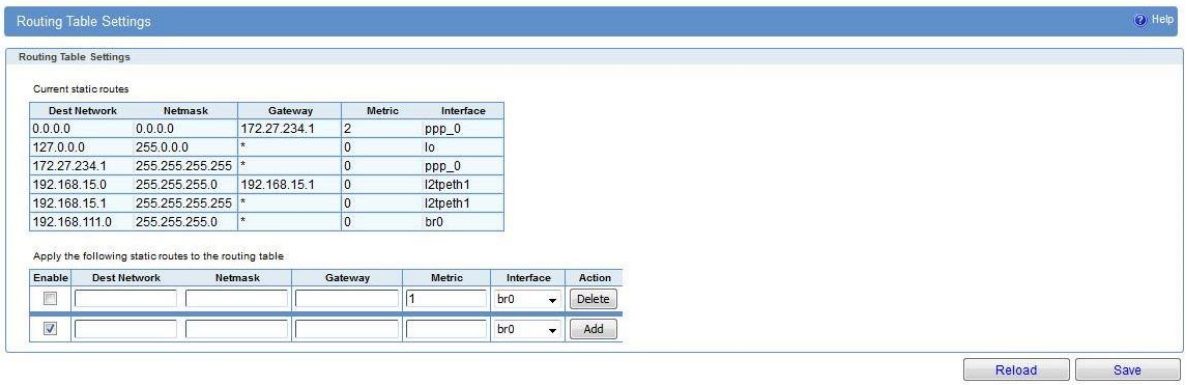
-MTU 1488

Veb interfejs rutera br. 2 sa konfigurisanim i uspostavljenim tunelom prikazan je na slici 4.5.4.



4.5.4 L2TP konfiguracija na ruteru br. 2

U tabelu rutiranja rutera br. 2 dodaje se mrežni opseg adresa na kome se nalaze ruter br. 1 i PC računar, IP adresa na kojoj se nalazi ruter br. 1 (192.168.15.1), obe na l2tpeth1 virtuelnom mrežnom interfejsu na kome se uspostavlja L2TP tunel. Adresa 192.168.15.1 predstavlja gejtvej za PC računar, tj za mrežu 192.168.15.0 (sa maskom podmreže 255.255.255.0). Za ruter br.2 veb interfejs sa tabelom rutiranja prikazan je na slici 4.5.5.

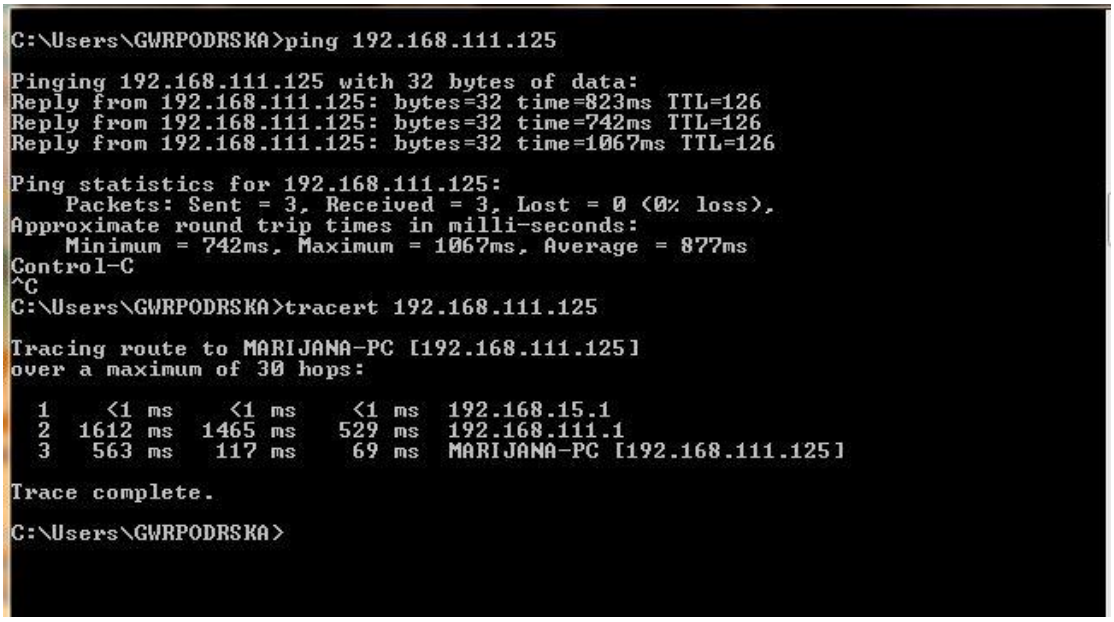


4.5.5 Tabela rutiranja za ruter br. 2

Pušten je ping test sa PC računara, koji se nalazi na adresi 192.168.15.184, ka laptopu koji se nalazi na adresi 192.168.111.125. Dobijanjem odziva sa laptopa, vidi se da je tunel uspostavljen.

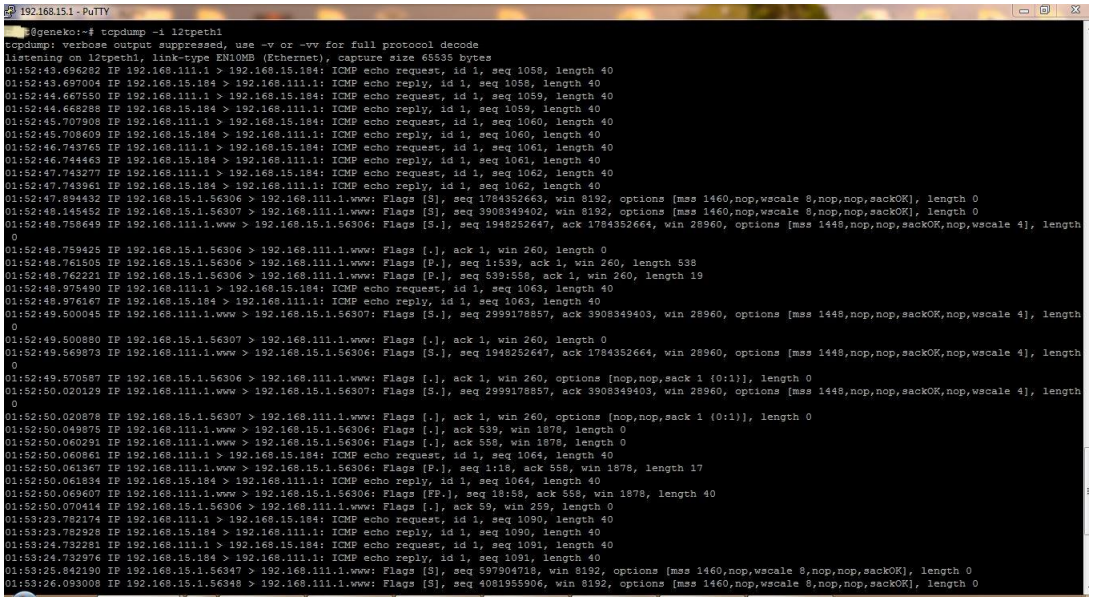
Komandom tracert prikazana je putanja paketa kroz tunel, sa računara ka laptopu. Prvi skok (hop) je ka ruteru br. 1 koji je na adresi 192.168.15.1, zatim ka ruteru br. 2 koji ima adresu

192.168.111.1 i poslednji skok ka odredištu, tj ka laptop-u kome je dodeljena adresa 192.168.111.125. Na slici 4.5.6 prikazane su ping i tracert komanda.



4.5.6 Ping i tracert komanda

Tcpdump komanda se drugačije naziva analizator paketa (*packet analyzer*). Prikazuje opis sadržaja paketa sa određenog mrežnog interfejsa. Tcpdump komanda u ovom slučaju prikazuje pakete na l2tpeth1 interfejsu, na kome je uspostavljen L2TP tunel. Komanda je puštena sa rutera br. 1 koji se nalazi na adresi 192.168.15.1, što je prikazano na slici 4.5.7.



4.5.7 Tcpdump komanda

L2TP prenosi podatke preko UDP-a. UDP je manje siguran, jer ne vrši ponovno slanje izgubljenih podataka, ali je brži protokol od TCP-a. Preporuka je da se sa njim koristi IPSec koji obavlja šifriranje i upravljanje ključevima u IP okruženju. L2TP protokol ima pored poruka

podataka i kontrolne poruke za održavanje tunela, a i mogućnost kompresije zaglavlja čime se povećava propusna moć veze. Za autentifikaciju korisnika L2TP protokol se oslanja na PPP protokole PAP i CHAP. Protokol L2TP nema mogućnost enkripcije pri korišćenju preko Interneta za to koristi protokol IPSec.

5. ANALIZA VPN PROTOKOLA

Prilikom uspostave konfiguracija, brzina uspostave zavisi od složenosti algoritama, tačnije od kompleksnosti metoda u odnosu na nivo sigurnosti koji obezbeđuju.

L2TP prenosi poruke preko UDP protokola, a PPTP preko TCP protokola. UDP je brži, ali manje pouzdan protokol jer ne vrši ponovno slanje izgubljenih paketa. Prilikom uspostave komunikacije preko TCP protokola potrebno je da se između predajne i prijemne strane razmene kontrolne poruke sa podešenim parametrima. Ukoliko se OpenVPN uspostavlja preko UDP protokola brže ce se uspostaviti, nego preko TCP protokola. Prednost L2TP-a je što može da se integriše sa IPsec protokolom i koristi njegove zaštitne mehanizme. PAP i CHAP protokol autentifikuju korisnika, a ne mašinu (server), niti paket. S obzirom da L2TP protokol za autentifikaciju koristi PPP mehanizme PAP i CHAP, L2TP tunel je kao i PPTP ranjiv na napade.

GRE tunel ne koristi mehanizme zaštite i uspostavlja se odmah posle komande za startovanje tunela na ruteru, sa obe strane. Firewall ne prepoznaje GRE tunel, pa je potrebno podesiti da propušta GRE pakete. U primeru konfiguracija iz poglavlja četiri, firewall je bio isključen.

IPSec se smatra najboljim resenjem jer obezbeđuje autentifikaciju, enkripciju i integritet podataka. Međutim, razmena poruka prilikom uspostave traje duže u odnosu na tunele koji ne obezbeđuju zaštitu i samim tim zbog složenosti konfiguracije IPSec troši više resursa procesora, uređaja na kome se konfiguriše. Za konfiguraciju IPSeca na računaru potrebno je instalirati neku vrstu programa, primer Strongswan (implementacija za Linux operativni sistem). Ukoliko je potrebno omogućiti pristup i prenos poverljivim podacima sa velikim stepenom zaštite IPSec je pravo rešenje.

6. ZAKLJUČAK

Virtuelna privatna mreža pruža zaštitu nad informacijama i podacima koji se prenose Internetom tako što omogućava uspostavu virtuelnog tunela. Pristup tunelu je moguće ostvariti sa bilo koje lokacije koja ima vezu sa Internetom. Prednosti ovih protokola su dugogodišnja prisutnost, jednostavna primena i dostupnost na različitim platformama i uređajima.

Ovaj rad sadrži teorijska objašnjenja i praktične primere konfiguracija VPN-a. Objašnjena je terminologija, prikazana klasifikacija i opisani standardizovani referentni modeli. Prikazano je kako se one realizuju u stvarnim uslovima. Teorijska objašnjenja ističu prednosti i mane, osnovne osobine, bezbednost. Podaci koji se prenose preko bilo koje javne mreže su nezaštičeni, zbog čega postoji opasnost od prisluškivanja podataka od strane neovlašćenih lica. Razmatrana je mera bezbednosti Virtuelnih privatnih mreža u zavisnosti od protokola koji koriste, da bi se ostvarili poverljivost, integritet i autentičnost podataka. U realnim situacijama ne može se obezbediti interoperabilnost različitih implementacija VPN-a. Međutim, iako postoje ti nedostaci, planiranjem i adekvatnim implementiranjem, VPN služi kao efikasno rešenje za uspostavu sigurne host-to-host komunikacije ili uspostavu kanala između udaljenih lokacija.

LITERATURA

[1] http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf

[2] Todd Lammle – CCNA Routing and Switching Study Guide

[3] http://whatismyipaddress.com/vpn

[4] http://security.lss.hr/images/dokumenti/lss-pubdoc-2011-06-016.pdf

[5] http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-11-246.pdf

[6] http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-04-298.pdf

[7] http://www.ciscopress.com/articles/article.asp?p=25474&seqNum=7

[8] http://ptgmedia.pearsoncmg.com/images/9781587201509/samplechapter/158720150X_CH14.pdf

[9] https://www.academia.edu/934414/Bezbednost_podataka_u_VPNu_na_javnoj_globalnoj_mre%C5%BEi

[10] Odom Wendell Cisco CCNA Routing and switching ICND2 200-101

[11] https://technet.microsoft.com/en-us/library/cc958045.aspx

[12] https://technet.microsoft.com/en-us/library/cc958047.aspx