KONFIGURACIJA IPSEC-A NA MIKROTIK OPREMI

Perišić, Ivica

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Preddiplomski stručni studij Elektronike

IVICA PERIŠIĆ

Z A V R Š N I R A D

KONFIGURACIJA IPSec-a NA MIKROTIK OPREMI

Split, rujan 2019.

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Preddiplomski stručni studij Elektronike

Predmet: Širokopojasne mreže

Z A V R Š N I R A D

Kandidat: Ivica Perišić

Naslov rada: Konfiguracija IPSec-a na MikroTik opremi

Mentor: Toni Jončić

Split, rujan 2019.

SADRŽAJ

SAŽETAK
Konfiguracija IPSec-a na MikroTik opremi

Projekt Završnog rada bio je ostvarivanje komunikacije na tri lokacije pomoću VPN-a (virtualne privatne mreže). Vodeći protokol za sigurnost bio je IPSec, te se sam rad izvodio na MikroTik opremi. IPSec je skup protokola koji su namjenjeni da zaštite komunikaciju preko Interneta. Kao što je rečeno, funkcioniranje IPSeca na trećem sloju OSI modela pruža jednostavnu i efikasnu zaštitu za TCP i UDP pakete. Za izvedbu projekta korišteni su usmjerivači marke MikroTik, računala i UTP kablove, dok se sam projekt izvodio u prostorijama Sveučilišnog odjela za stručne studije u Splitu, točnije u Laboratoriju P08.

Ključne riječi: VPN, IPSec, MikroTik

SUMMARY
IPSec configuration on MikroTik equipment

The aim of this paper was the communication establishment on three locatios using the VPN (Virtual Private Network). The leading protocol of safety was the IPSec. The practice/practical work was conducted on MikroTik equipment. IPSec is a set of protocols that should protect the communication that is happening over the Internet. As already stated, the functioning of the IPSec in the third layer of the OSI model provides simple but effective protection for both TCP and UDP packages. MikroTik branded routers, computers and UTP cables were used for the project implementation, while the project itself was performed on the premises of the University Department of Professional Studies in Split, more precisely in Laboratory P08.

Keywords: VPN, IPSec, MikroTik

1. UVOD

Osnovna podjela IPSeca, odnosno dvije podskupine protokola su:

- kriptografski protokoli – ESP protokol (eng. *Encapsulating Security Payload*) i AH protokol (eng. *Authentication Header*)
- protokoli za razmjenu ključeva – IKE protokoli (eng. *Internet Key Exchange*)

Također, IPSec ima i dva moda rada; transportni mod i tuneliranje paketa. U prvome modu (transportnom) paketi se šalju između dva krajnja elementa mreže (računala) gdje odredišno računalo prima paket i izvršava sigurnosne provjere prije nego ga proslijedi višim slojevima. U drugom slučaju (tunelu), nekoliko računala se skriva iza jednoga čvora, te su paketi nevidljivi ostatku mreže; samim time i zaštićeni od napada. Osnovna ideja zaštite paketa IPSec protokolima jest mogućnost izgradnje virtualne privatne mreže (VPN). VPN možemo izgraditi u oba moda.

Cilj je bio povezati tri različite točke mreže sa IPSec tunelom koje međusobno nisu bile direktno vezane, već je između njih bio postavljen, uvjetno rečeno, Internet; tri usmjerivača koji su međusobno imali postavljen OSPF protokol i oponašali su javnu mrežu, odnosno pružatlja usluga.

2. OPREMA

2.1. MikroTik

MikroTik je tvrtka koja se bavi područjem razvoja usmjerivača i bežičnih ISP sustava, namjenjena raznim telekom operaterima, tvrtkama koje pružaju IT usluge itd. Središte tvrtke je u Latviji, točnije glavnom gradu Rigi i djeluje od 1996. S vremenom su se proširili na tržište većine zemalja svijeta te nude *PC hardver* (2002. godine su napravili prvi vlastiti *hardver*) i kompletne sustave usmjeravanja.

1. Slika: Logo MikroTik

Osim nekolicine različitih usmjerivača, ponuda MikroTik tvrtke sadrži i preklopnike, bežične sustave (pokućne i uredske), antene, te razne druge proizvode.

U sljedećim stranicama će se pobliže opisati usmjerivači, spomenutog proizvođača, koji su se koristili u izradi ovoga projekta:

- MikroTik hAP ac – usmjerivač je korišten kao vanjski dio, odnosno sudjelovao je u VPN konfiguraciji.
- MikroTik RB2011UiAS – usmjerivač korišten u središtu mreže, odnosno oponašao je javnu mrežu nekog pružatelja usluga.

O korištenim usmjernicima više u nastavku.

2.1.1. MikroTik hAP ac

U kreaciji VPN-ova smo koristili tri servera (računala), UTP kabele, te tri usmjerivača marke „MikroTik hAP ac“, a verzija istih je –RB962UiGS-5HacT2Hnt; to je internacionalna verzija toga usmjerivača (također služi i kao AP i preklopnik). Svaka zemlja ima propise svojih frekvencijskih raspona, pa se on može i ograničavati. Druga verzija je Američka, a razlika im je u tome što Američki usmjerivači imaju fiksne zaključane frekvencije.

2. Slika: Prikaz usmjerivača hAP ac

Korišteni usmjerivač se danas vrlo rasprostranjeno koristi u privatnim kućama ili u uredima, a prednosti koje ga karakteriziraju je to što je dvopojasni uređaj sa Gigabitnim Ethernet priključcima koji omogućuju da se 802.11ac tehnologija u potpunosti iskoristi, bez gubljenja kompatibilnosti sa starijim uređajima koji rade na 2.4GHz (802.11 b/g/n), odnosno 5GHz (802.11 a/n). Tehnologije 802.11 su se prije koristile većinski u LAN mrežama, no u posljednje vrijeme nude i bežični pristup WAN mrežama.

2.1.2 MikroTik RB2011 UiAS-IN

Za unutarnji krug mreže, to jest „Internet uslugu“, koristila su se tri usmjerivača MikroTik RB2011UiAS-IN, UTP kabeli, te računala pomoću kojih smo konfigurirali dotične usmjerivača. Ista računala se nisu koristila u samoj konfiguraciji mreže.

RB2011 pokreće operativni sustav „RouterOS“ koji je i sam proizveden od tvrtke MikroTik. Dinamičko usmjeravanje, MPLS, VPN, vatrozid, konfiguracija u stvarnom vremenu i brojne druge značajke koje su podržane sa usmjerivačkim operativnim sustavom „RouterOS“.

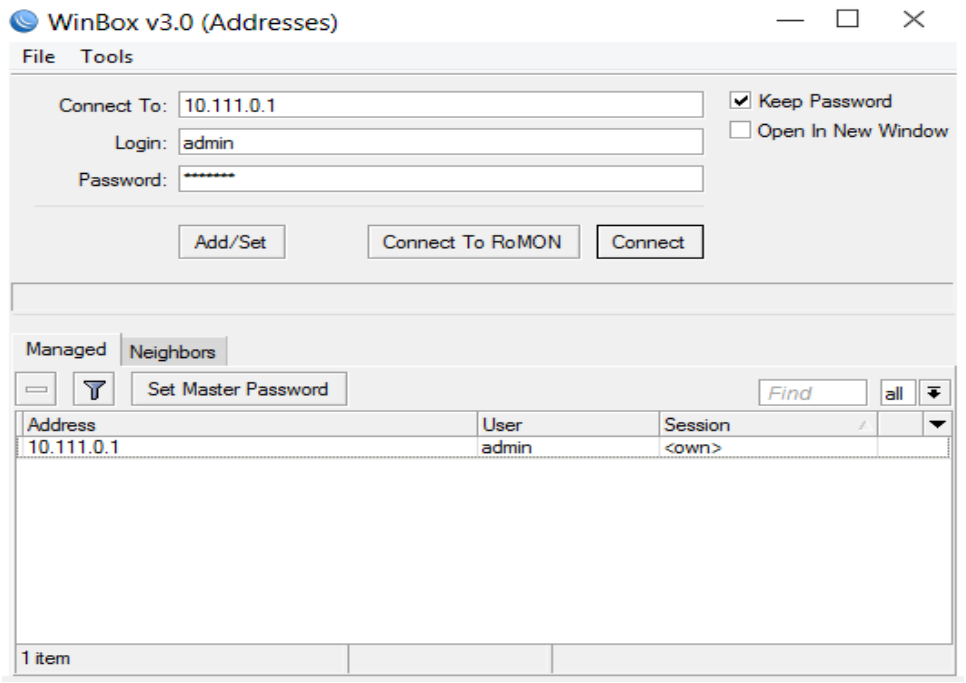
3. Slika: Prikaz usmjerivača RB2011

Kao što se da očitati sa slike, usmjerivač RB2011 ima pet gigabitnih LAN priključaka i pet brzih *Ethernet* LAN port-ova. Osim toga ima i RJ45 serijski ulaz, ima mogućnost USB priključka i više RAM memorije (128MB). Statičke postavke i neke osnovne informacije ovoga usmjernika je lako doznati s obzirom da ima mali LCD zaslon u desnome kutu koji je osjetljiv na dodir.

2.2. Winbox

Winbox je uslužni program kojim se jednostavno omogućuje ulaz u administraciju MikroTik usmjerivača, koristeći grafičko korisničko sučelje. Pomoću njega smo konfigurirali adrese, rute, zaštite, tunel i sve ostalo.

Prilikom pokretanja Winboxa otvara nam se početno sučelje gdje upisujemo potrebne pristupne podatke (korisničko ime, šifru...) u odgovarajuća polja za pristup pojedinom usmjerivaču.



4. Slika: Winbox početno sučelje

Nakon toga slijedi inicijalizacija, dodjela adresa, statičkih ruta itd., o čemu ćemo detaljnije u nastavku.

Winbox, odnosno MikroTik operativni sustav nam omogućuje mnogo mrežnih mogućnosti. Opisivanje svake komponente, odnosno kompletne konfiguracije, premašilo bi svrhu našega zadatka, stoga ćemo se bazirati samo na mogućnostima sustava koje smo koristili u radu.

3. VPN

VPN (eng. Virtual Private Network) je tehnologija koja omogućava sigurno povezivanje mrežnih elemenata (računala) u virtualne privatne mreže preko dijeljene ili javne mrežne infrastrukture. Koristeći VPN omogućeno je povezivanje geografski udaljenih poslovnih partnera, korisnika itd. Pod VPN se podrazumjeva korištenje istih upravljačkih i sigurnosnih pravila koja se primjenjuju unutar mreža. Mogućnosti za uspostavu VPN mreža su različiti komunikacijski kanali, npr. preko Interneta, preko ATM mreža, putem komunikacijske infrastrukture pružatelja usluga itd.

Razlika između privatnih mreža i virtualnih privatnih mreža je ta što privatne mreže prenose podatke iznajmljenom linijom za slanje podataka, dok virtualne mreže stvaraju sigurnosni kanal između dviju (ili više) krajnjih točaka. Prednost korištenja VPN-a je ušteda u odnosu na cijenu iznajmljenih linija. Naravno, iznajmljene mreže imaju pouzdaniji medij za prijenos podatka, s obzirom da Internet može rezuktirati kašnjenjima ili iznenadnim prekidima u komunikaciji.

VPN štiti odaslane podatke automatskim šifriranjem i enkapsuliranjem u IP pakete prilikom slanja podataka između udaljenih mreža, oodnosno automatskim dešifriranjem na prijemnoj strani. Cilj je ograničiti pristup određenim podacima koji su namjenjeni samo određenim korisnicima, odnosno računalima.

Primjena IPSec VPN-a najviše smisla ima u slučajevima kada neka korporacija ima više odvojenih lokacija, a propusnost i kvaliteta usluge komuniciranja nisu od kritičnog značaja.

Upravno spajanje više lokacija će biti opisano u nastavku.

3.1. IPSec

Definiran od strane IETF-a (eng. *Internet Engineering Task Force).* Jedan dio internetskih sigurnosnih sustava (TLS, SSH...) djeluju iznad treće razine OSI modela, no *Internet Protocol Security* se nalazi u trećem sloju OSI modela kao otvoreni standard, odnosno u IPv4 paketu, te je neovisan o aplikacijama. IPSec daje povjerljivost, autentičnost i integritet podatka, a to osigurava autentifikacijom i enkripcijskim protokolima.

IKE (eng. *Internet Key Exchange)* služi za određivanje sigurnosnih parametara i razmjenu ključnih informacija između elemenata koji su sudionici komunikacije. Sigurnosni parametri definiraju vezu među elementima mreže. Sam IPSec to ne bi sam mogao odrediti, odnosno ne posjeduje taj mehanizam, stoga su iz IETF-a odabrali IKE kao standardnu metodu za definiranje sigurnosnih parametara koji su neophodni za rad IPSec-a.

Kao što je već rečeno, radi u dva moda; transportni i tunelski mod.

U prijenosnom modu (transportnom) se šifrira samo podatkovni dio IP paketa, a IP zaglavlja se ostave u prvobitnom obliku. Sloj aplikacije, odnosno aplikacijska zaglavlja su šifrirana. Prednost ovoga načina rada je ta što se svakome IP paketu doda svega par okteta. U prijenosnom načinu rada usmjernici na javnoj mreži mogu vidjeti adrese pošiljateljeve i odredišne strane, što omogućuje potencijalnim napadačima određene informacije, odnosno mogućnosti analize prometa.

U tunelskom modu, koristi se eng. *end-to-end* metoda, odnosno obje strane se dogovaraju oko mehanizama za šifriranje, paketi se kriptiraju, autentificiraju i onda se enkapsuliraju u novi IP paket koji ima i novo IP zaglavlje. Ukoliko IP adresa, protokol i broj porta odgovaraju filtru, taj paket će se obraditi na odgovarajući način. Virtualne privatne mreže se mogu koristiti za komunikaciju između usmjerivača koji povezuju različite mrežne lokacije (*network-to-network),* za komunikaciju udaljenog pristupa korisniku (*host-to-network*), te za privatne komunikacije (*host-to-host*).

Neki od protokola koje IPSec koristi za obavljanje različitih funkcija su:

- Zaglavlja provjere autentičnosti (AH) – osigurava integritet bez veze pomoću *Hash* funkcije, jamči izvor podataka za IP datagrame i pruža zaštitu od napada ponovne reprodukcije.
- Sigurnosno enkapsuliranje tereta (ESP) – osigurava povjerljivost, provjeru identiteta izvora, integritet podataka bez povezivanja, protu-odgovarajuću uslugu i ograničenu povjerljivost protoka prometa.
- Sigurnosna udruženja (SA) – komunicirajuće strane koriste zajedničke sigurnosne atribute (algoritmi i ključevi).

Prilikom slanja paketa kroz tunel, neke karakteristike istoga mogu biti skrivene unutar IPSec tunela, i to onemogućava prepoznavanje klase paketa; ne može se odrediti prioritet paketa i pružatelj usluga će sve jednako prioritizirati, pa **nije moguće provesti kvalitetu usluge (QoS).**

5. Slika: IPSec logo

4. POSTAVLJANJE OSPF-A

4.1. Općenito o OSPF-u

Prilikom konfiguracije rada korišten je i unutarnji protokol usmjeravanja OSPF (eng. *Open Shortest Path First*). Korišteni protokol je bio u središnjem dijelu mreže, odnosno povezivao je usmjernike MikroTik RB2011, koji su kako je navedeno oponašali nekog pružatelja usluga. Za njihovu međusobnu komunikaciju odabran je OSPF protokol jer je jednostavan za konfiguraciju putem Winboxa i vrlo fleksibilno određuje nove putanje paketa ukoliko dođe do nekakvih promjena u autonomnom sustavu (AS). Radi tako što distribuira usmjerivačku informaciju između usmjernika koji pripadaju istome AS.

Ne obrađuje čitav paket, već ga prosljeđuje isključivo na temelju IP adrese koja se nalazi u zaglavlju samoga paketa. Svaki usmjernik koji sudjeluje u jednoj komunikaciji ima istu bazu podataka i svi koriste isti algoritam.

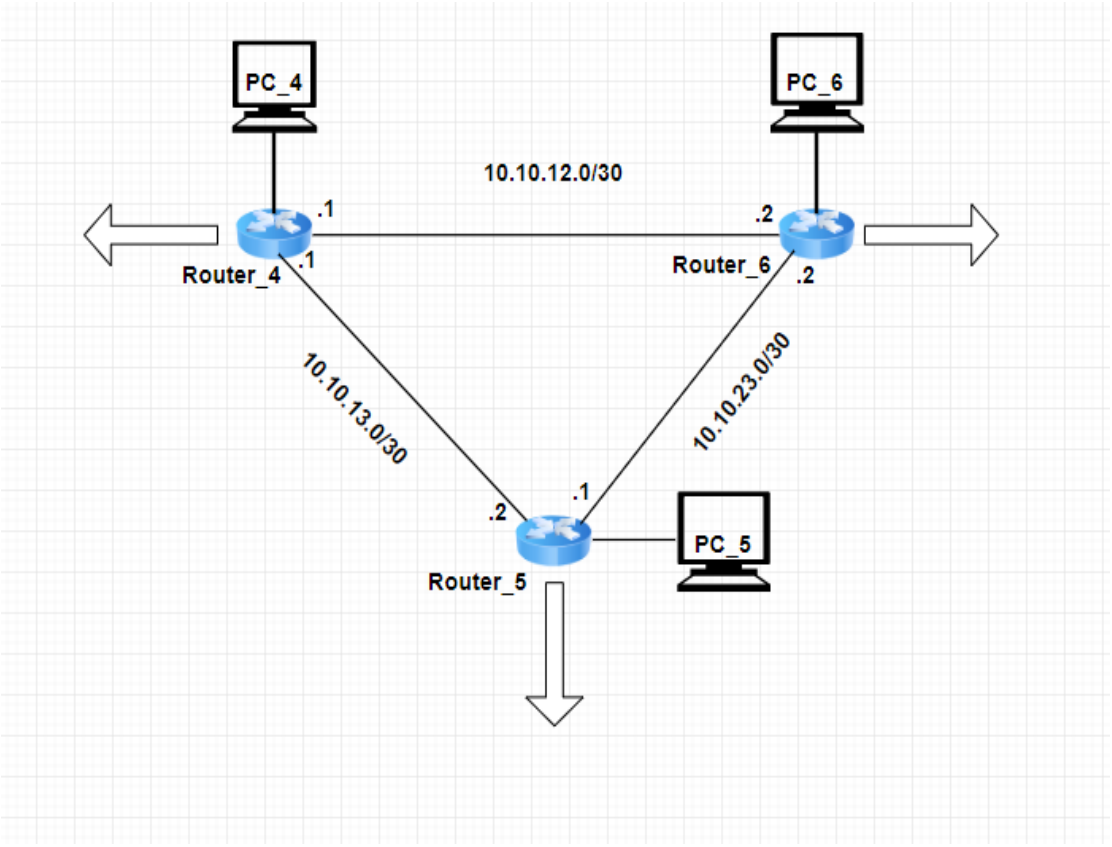
Princip rada OSPF protokola je „stanje veze“ (eng. *link state*). Za izračun i izgradnju najkraće staze koristi se SPF algoritam. Algoritam radi tako da postavlja svaki usmjerivač u korijen stabla i računa najkraće rute za prijenos. Svaki će usmjernik imati svoju vlastitu topologiju najkraćih ruta, iako će svi usmjernici izgraditi stablo korištenjem iste baze podataka stanja veze.

6. Slika: OSPF logo

4.2. Inicijalizacija i adresiranje

Zbog toga što svaki MikroTIk uređaj ima inicijalno podešen isti naziv (MikroTik), IP adresu (192.168.88.1/24) i polje za šifru prazno, radi lakšeg raspoznavanja i konfiguriranja uređaja, poželjno je promijeniti navedene stavke. Inicijalizaciju, odnosno promjena naziva uređaja se vršila tako što se na izborniku konfiguracijskog sučelja odabere stavka „System“, zatim „Identity“ i otvori nam se prozor gdje možemo unijeti željeni naziv uređaja. U našem slučaju smo prvi usmjenik nazvali „Router_4“. Četiri iz razloga što smo prva tri broja dodjelili usmjernicima koji su povezivali servere, odnosno krajnje točke sa središnjom javnom mrežom. Drugi usmjernik iz javne mreže smo nazvali „Router_5“, i treći usmjernik je nazvan „Router_6“.

Zbog lakšeg razumjevanja same konfiguracije na usmjerivačima u nastavku je priložena slika topologije, odnosno shematski prikaz tog dijela mreže.

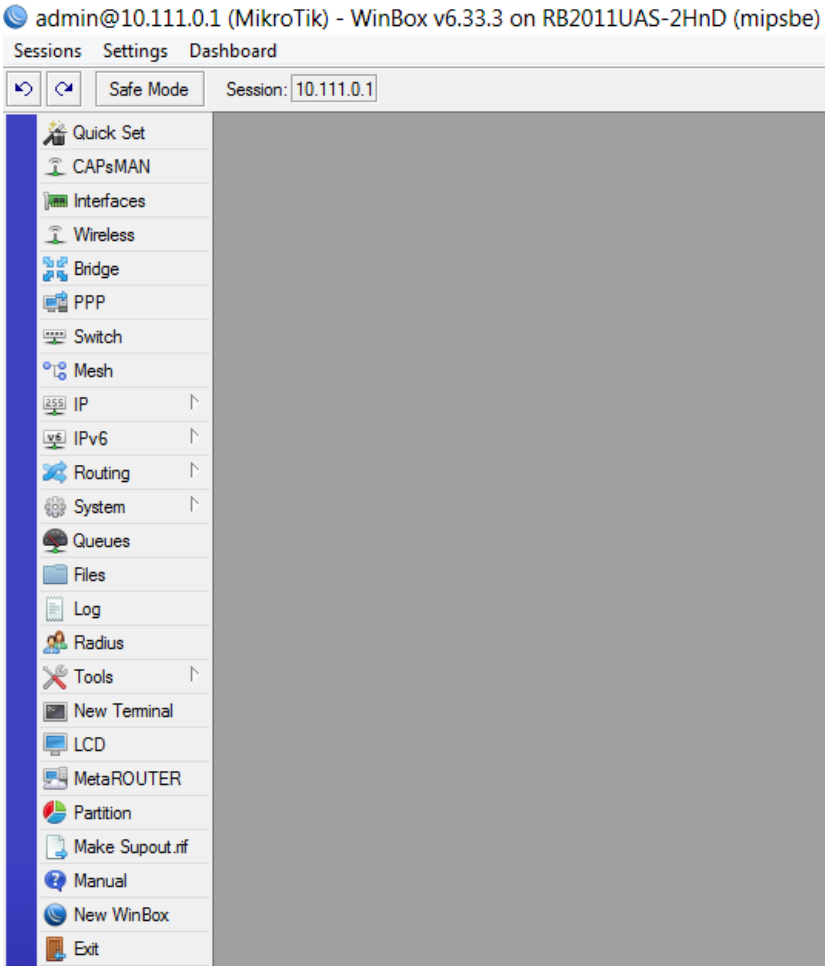


7. Slika: Topologija dijela mreže; Internet

Prvi korak u konfiguraciji OSPF protokola koji je povezivao usmjernike unutarnje mreže bio je inicijalizacija, odnosno promjena naziva usmjernika, zbog jednostavnijeg praćenja mreže. Nakon što se olakšalo snalaženje između usmjernika i smanjila mogućnost nenamjerne greške programera, uslijedila pojedinačna konfiguracija.

4.2.1. Adresiranje usmjernika „Router_4“

Nakon početnih koraka, prije spomenutih, otvori se Winbox konfiguracijsko sučelje.



8. Slika: Winbox konfiguracijsko sučelje

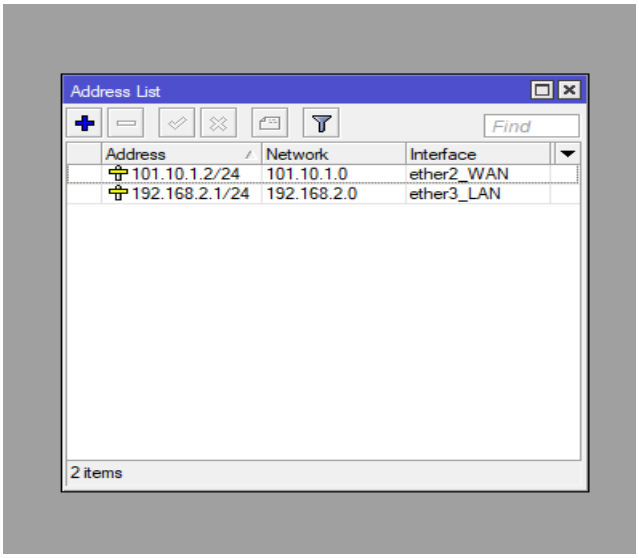
Na priloženoj slici ćemo lakše pratiti daljnje korake koje smo činili prilikom konfiguracije u Winboxu.

Kako bi promijenili adresu pojedinog usmjerivača, to činimo tako što na izbornom stupu izaberemo stavku „IP“, nađemo stavku „Addresses“ i pritiskom na nju otvara nam se prozor „Address List“ s popisom adresa koje usmjerivač trenutno koristi. Iste možemo ili promijeniti ili dodati nove adrese.

Adrese možemo i onemogućiti klikom na „Disable“ i tada red u kojemu se nalazi onemogućena adresa promjeni boju u sivo, a ispred adrese se pojavi „X“ koji označava da je adresa onemogućena. Također, adrese možemo i potpuno ukloniti pritiskom na „Remove“. Za promjenu IP adrese klikne se dva puta na red adrese koju želimo promjeniti, te nam se tada otvori prozor u kojemu je moguće promijeniti adrese, raspon adrese i sučelje na koje želimo da usmjerivač bude spojen.

Adrese koje su vezane za usmjernik „Router_4“, odnosno adrese koje smo dodali na isti su sljedeće:

- 101.10.1.2 – adresa koja veže usmjernik „Router_1“ sa unutarnjom javnom mrežom. *Subnet mask* mreže je 255.255.255.0, odnosno /24.
- 10.10.12.1 – adresa koja povezuje usmjernik „Router_5“. Maska podmreže nije /24, već je /30, što znači da u ovim adresama imamo 30 bita rezerviranih za definiranje mrežnog dijela mreže, a 2 bita za označavanje *host*-ova.
- 10.10.13.1- povezuje usmjernik „Router_4“ sa usmjernikom „Router_6“. Također, podmrežna maska je /30.



9. Slika: Prikaz adresnog prozora

Na priloženoj slici nisu odgovarajuće adrese, već je postavljena figurativno za vizualno dočaravanje izgleda adresnog prozora.

Prvu adresu na usmjenriku „Router_4“, odnosno adresu koja povezuje sa poslužiteljem smo spojili na sučelje broj „4“ (gigabitni priključak). Na sučelje „3“ smo spojili usmjernik „Router_6“, dok je na sučelju „2“ spojen usmjernik „Router_5“. Na sučelju „5“ je bilo povezano računalo „PC_4“, koje nije sudjelovalo u komunikaciji, već smo preko njega samo konfigurirali dotični usmjernik.

4.2.2. Adresiranje usmjernika „Router_5“

Adresiranje usmjernika „Router_5“ se provelo na način da su se dodale sljedeće adrese na određena sučelja:

- Na sučelje „2“ spojen je usmjernik „Router_4“ te smo na to sučelje dodali adresu 10.10.13.2/30.
- Adresa 10.10.23.1/30 je pridodana sučelju „3“ i ono je bilo vezano za usmjernik „Router_6“
- 103.10.1.2/24 je bila veza sa usmjernikom (kojemu je druga strana povezana sa drugim poslužiteljem; „PC_2“) „Router_2“ i to je spojeno preko sučelja „4“.

Kao i kod usmjernika „Router_4“ sučelje „5“ smo iskoristili za povezivanje sa računalom koje nije sudjelovalo u mreži; „PC_5“.

4.2.3. Adresiranje usmjernika „Router_6“

Adresiranje usmjernika „Router_6“ se izvelo tako da su se dodale sljedeće adrese na određena sučelja:

- Sučelju „2“ dodjeljena je adresa 10.10.23.1/30 koja je bila vezana za usmjernik „Router_5“.
- Na sučelje „3“ je postavljena adresa 10.10.12.2/30, odnosno poveznica sa „Router_4“.
- Sučelje „4“ je povezivalo sa usmjernikom „Router_3“ preko adrese 102.10.1.2/24.

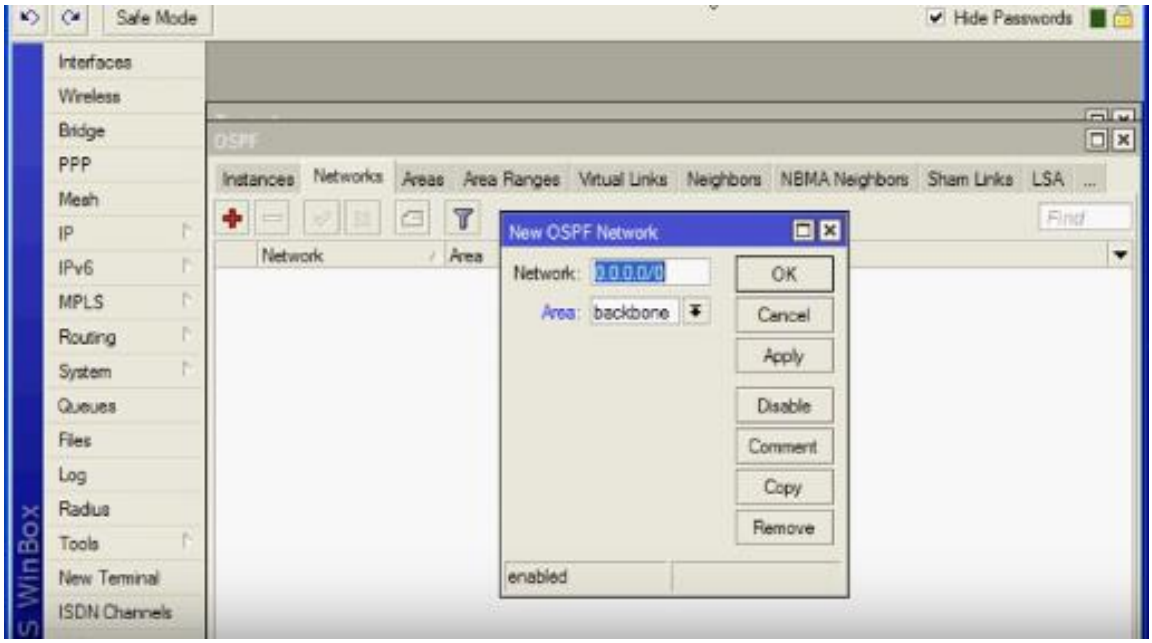
Sučelje „5“ iskorišteno za povezivanje sa računalom „PC_6“ preko kojega smo upravljali dotičnim usmjernikom.

4.3. Konfiguracija OSPF-a u Winboxu

Nakon adresiranja usmjernika, odnosno sučelja koja ih povezuju sa ostatkom mreže, usmjernici međusobno još nisu mogli komunicirati, stoga se morao postaviti neki komunikacijski protokol (OSPF, RIP, statičke rute itd.) koji bi omogućio njihvou međusobnu komunikaciju unutar njihovog trokuta, odnosno unutarnje mreže (podsjetnik; unutarnja mreža oponaša Internet).

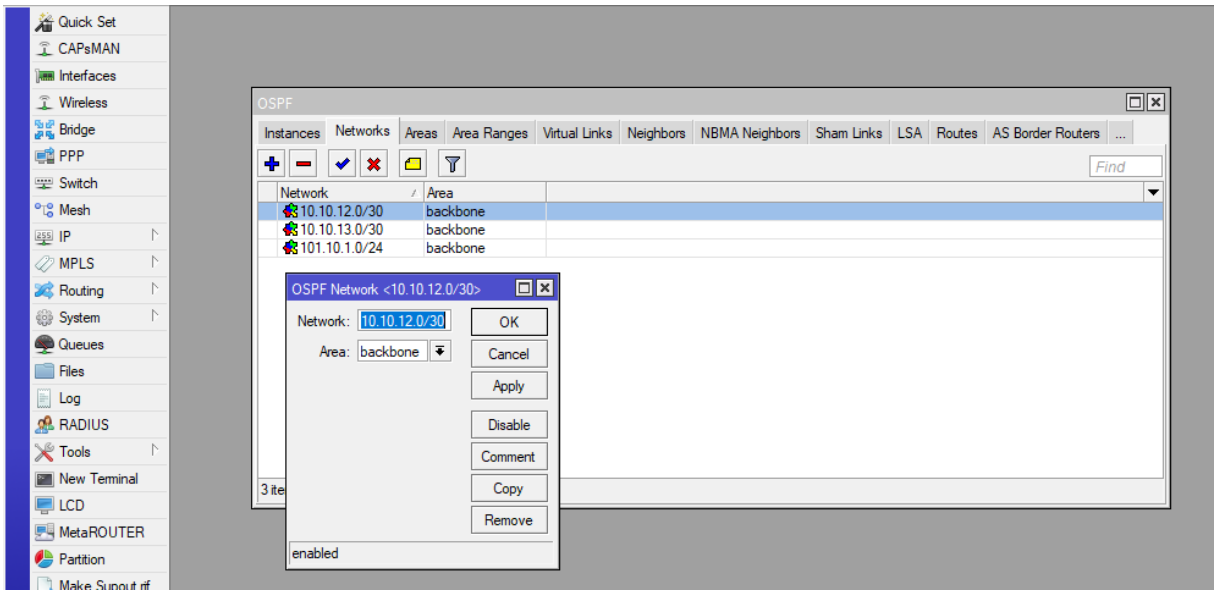
4.3.1. Postavljanje OSPF-a na „Router_4“

Na izbornoj traci konfiguracijskog sučelja izabere se stavka „Routing“, otovri se novi izbornik raznih protokola gdje se odabire „OSPF“. Nakon toga se otvori prozor koji ima vodoravnu izbornu traku (*Interfaces, Intances, Networks, Areas, Area Ranges, Virtual Links, Neighbors,Sham Links, LSA, Routes...*) i od ponuđenog se odabere „Networks“. Sljedeći korak nakon ulaska u prozor „Networks“ je klik na „+“ nakon čega se otvori novi prozor gdje se upisuju adrese raspona mreže na kojoj želimo da OSPF bude ostvaren.



10. Slika: Dodavanje OSPF-a

Na priloženoj slici se može vidjeti polje označeno plavom bojom gdje se upisuju mreže. Za svako sučelje mora se ponovno ići na „+“. Kod usmjernika „Router_4“ se ta radnja ponovila tri puta; prvi put se upisala adresa mreže sa sučelja „2“ (10.10.13.0/30), drugi put adresa mreže sa sučelja „3“ (10.10.12.0/30), te u trećem navratu adresu koja komunicira sa usmjernikom sa sučelja „4“ (101.10.1.0/24).



11. Slika: Prikaz konfiguriranog OSPF-a

4.3.2. Postavljanje OSPF-a na „Router_5“ i „Router_6“

Kako je opisano u poglavlju 4.3.1., postupke ponovimo i kod ostala dva usmjernika.

Kod usmjernika „Router_5“ dodamo tri adrese: 10.10.13.0/30, 10.10.23.0/30 i naravno adresu mreže 103.10.1.0/24. Navedene tri adrese su sa sučelja „2“, „3“ i „4“.

Nakon što su se usmjernici „Router_1“, „Router_2“, „Router_4“ i „Router_5“ povezali, nedostaje još samo konfiguracija „Router_6“ da bi se ostvarila međusobna komunikacija.

„Router_6“ se konfigurirao tako što su mu se u OSPF povezala sučelja „2“, „3“ i „4“ sa odgovarajućim adresama (10.10.12.0/30, 10.10.23.0/30 i 102.10.1.0/24).

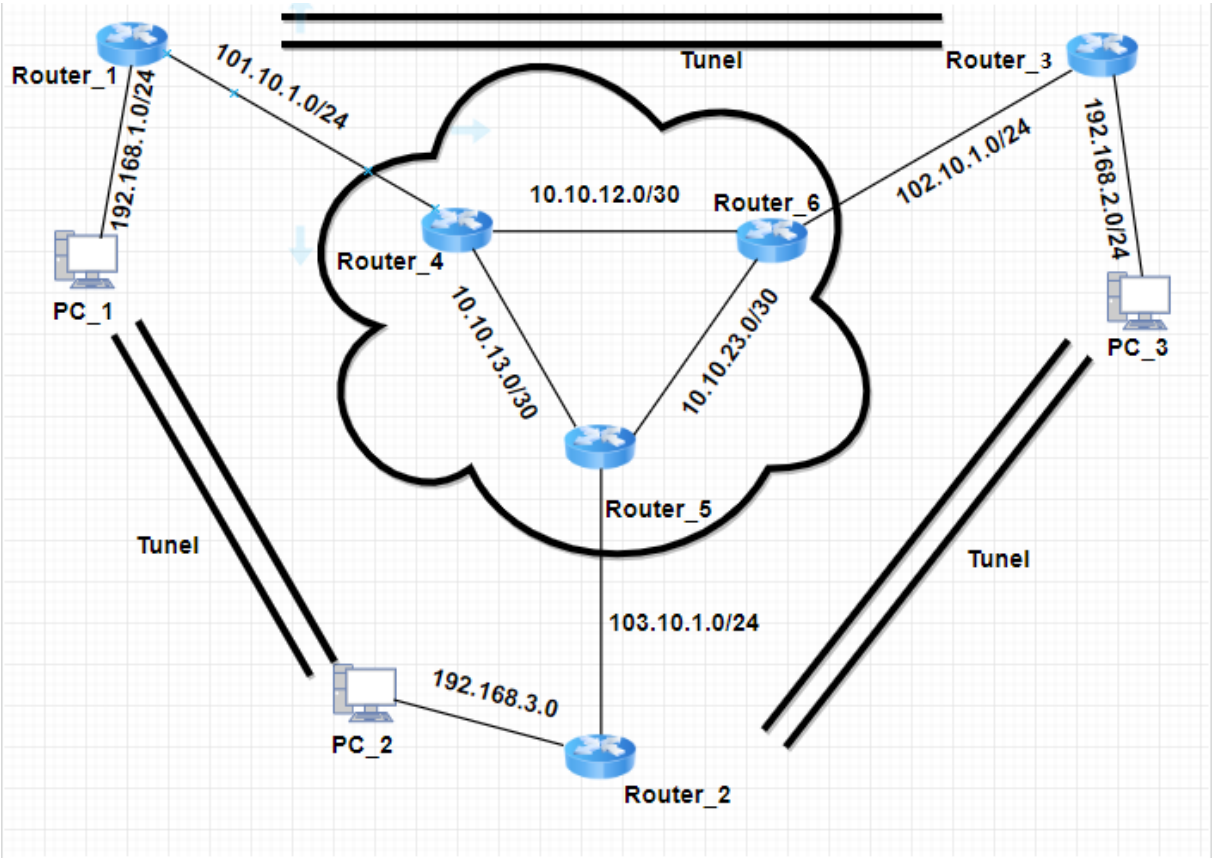
Nakon postavljanja OSPF-a na sva tri usmjernika, proradila im je međusobna komunikacija i komunikacija sa granama koje vode ka VPN-u, te smo imali podlogu za daljnju konfiguraciju i realističan dojam javne mreže od nekog pružatelja usluga.

5. PRAKTIČNI DIO KONFIGURACIJE

Prilikom konfiguracije mreže koristili smo tri računala koja su aktivno sudjelovala u mreži, odnosno poslužitelja; svako od njih je trebalo povezati tako da sigurno mogu komunicirati sa međusobno, iako nisu bili direktno povezani već je njih bila druga javna mreža.

12. Slika: Izvedba projekta u laboratoriju P08

Na priloženoj slici nam je prikazana praktična izvedba projekta gdje se može vidjeti na koji način smo spojili samu mrežu, te je slika pogodna za daljnje shvaćanje.



13. Slika: Topologija mreže

Na slici je prikazana topologija mrežnih elemenata, te IP adrese koje su dodjeljene pojedinom elementu. Na relacijama Računalo – Usmjerivač uspostavljali smo LAN (lokalna mreža) veze sa privatnim IP adresama, dok smo na relacijama Usmjerivač – Usmjerivač uspostavljali WAN (globalna mreža) veze s javnim IP adresama.

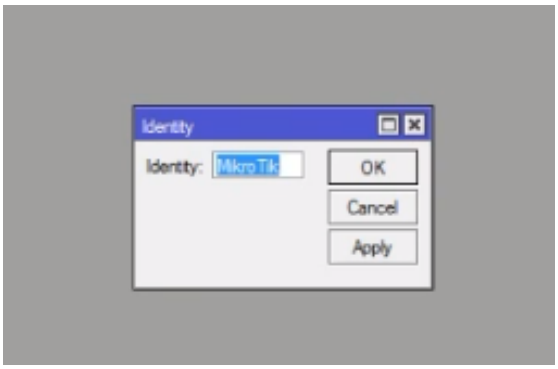
Na slici se se vizualno dočarala dodjela adresa te samo postavljanje svakoga elementa. Također, vizualno se može dobiti ideja na koji način su se tunelima spajala računala iz VPN mreža.

Za povezivanje svih elemenata korišteno je devet UTP kabela.

6. LOGISTIČKI DIO KONFIGURACIJE; RAD U WINBOXU

6.1. Promjena identiteta usmjernika

Naziv uređaja se mijenja tako što se na izborniku konfiguracijskog sučelja odabere stavka „System“, zatim „Identity“ i otvori se prozor gdje je omogućeno unošenje željenog naziva pojedinog uređaja. Unutrašnji dio mreže, tzv. Internet, je već prije objašnjen, stoga će u daljnjem razlučivanju koraka biti isključen. Računalima sam programer zadaje nazive, no to nigdje ne zapisuje (osim shemi mreže), dok se promjena naziva usmjernika vidi na rubu glavnog prozora Winboxa.



14. Slika: Prikaz prozora za promjenu naziva

Računalu, odnosno prvome poslužitelju (gledajući topologiju; s lijeva na desno), kojega smo na topologiji mreže nazvali „PC_1“, usmjernik na koji je vezan je usmjernik koju povezuje upravo njega sa unutrašnjom mrežom, te se tom usmjerniku dodjelio naziv „Router_1“.

Gledajući sliku topologije mreže odozdo prema gore, računalu (poslužitelju) se dodjelio naziv „PC_2“, a usmjernik koji ga povezuje, odnosno dovodi do Interneta, nazvan je „Router_2“.

Računalo na desnoj strani slike topologije mreže na unutrašnju mrežu je vezano sa usmjernikom kojemu se promjenio naziv u „Router_3“.

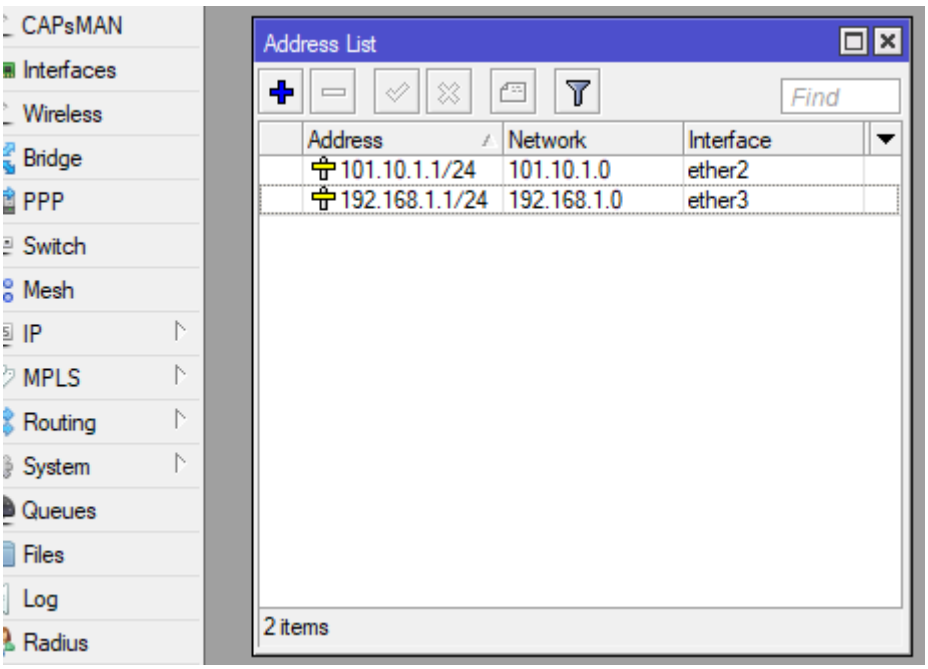
Klikom na „Interfaces“ u glavnom konfiguraciskoj sučelju, otvori se tablica svih sučelja na tome uređaju gdje možemo promijeniti naziv sučelja, uključiti i isključiti ARP tabele, onemogućiti pojedino sučelje, dodati komentar itd.

6.2. Dodjela IP adresa

6.2.1. Dodjela adresa na „Router_1“

Kako bi promijenili adresu pojedinog usmjerivača, to činimo tako što na izbornom stupu izaberemo stavku „IP“, nađemo stavku „Addresses“ i pritiskom na nju otvara nam se prozor „Address List“ s popisom adresa koje usmjerivač trenutno koristi. Iste možemo ili promijeniti ili dodati nove adrese

Adrese možemo i onemogućiti klikom na „Disable“ i tada red u kojemu se nalazi onemogućena adresa promjeni boju u sivo, a ispred adrese se pojavi „X“ koji označava da je adresa onemogućena. Također, adrese možemo i potpuno ukloniti pritiskom na „Remove“. Za promjenu IP adrese klikne se dva puta na red adrese koju želimo promjeniti, te nam se tada otvori prozor u kojemu je moguće promijeniti adrese, raspon adrese i sučelje na koje želimo da usmjerivač bude spojen.



15. Slika: Prikaz adresnog prozora

Slika nam prikazuje što smo sve izmjenili, te kako nam izgleda adresni prozor nakon izmjena. Stare adrese, zadane od prije, smo uklonili te smo dodali nove adrese pritiskom na „+“. Isto tako može se vidjeti i raspon mreža dodanih adresa, te odgovarajuća sučelja.

Dodjeljene adrese na usmjerniku „Router_1“:

- 101.10.1.1/24 – adresa koja omogućava povezivanje sa unutrašnjom mrežom, te se ona dodjelila ulaznom sučelju „2“.
- 192.168.1.1/24 – veza prema poslužitelju koji treba stupiti u komunikaciju sa ostalim privatnim poslužiteljima, spojena na sučelje „3“.

6.2.2. Dodjela adresa na „Router_2“

Na usmjerniku „Router_2“ gdje su također praćeni koraci („IP“, zatim „Addresses“), dodjeljujemo adrese koje usmjernik koristi u konfiguraciji. Korištene adrese:

- 103.10.1.1/24 – adresa zadužena za povezivanje sa unutrašnjom mrežom, spojena na sučelje „2“.
- 192.168.3.1/24 – veza prema poslužitelju, odnosno računalu „PC_3“ i spojena je na sučelje „3“.

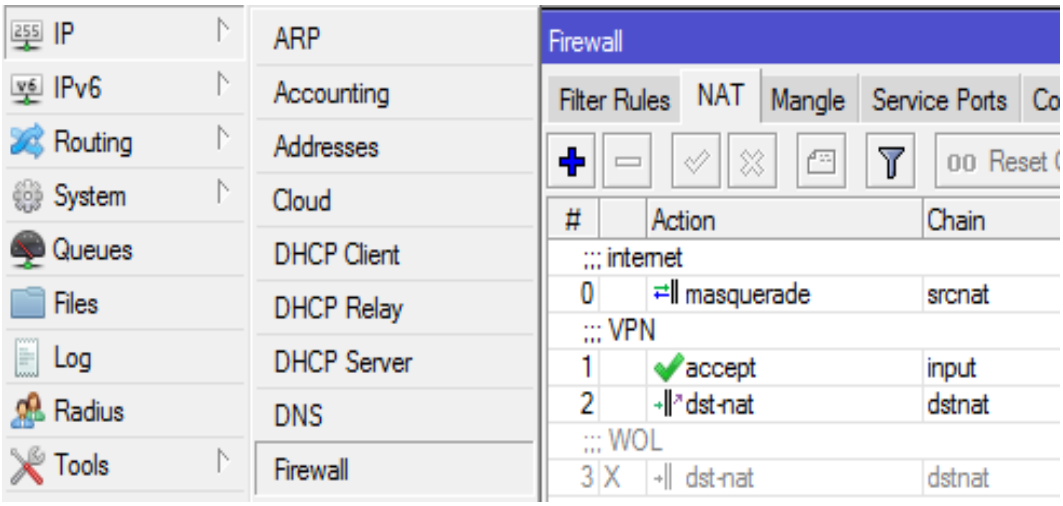
6.2.3. Dodjela adresa na „Router_3“

Primjenjujući objašnjene dosadašnje korake, adrese dodjeljene usmjerniku „Router_3“ su sljedeće:

- 102.10.1.1/24 – veza s „Internetom“, sučelje „2“.
- 192.168.2.1/24 – veza sa poslužiteljem, sučelje „3“.

6.3. Vatrozid

Firewall ili Vatrozid je sigurnost, odnosno nadzor mreže koji nam pomaže u pravovremenom izbjegavanju potencijalnih sigurnosnih problema ili poteškoća s korištenjem u slučaju prevelikog opterećenja koje nastane uslijed zauzeća dostupnog kapaciteta mreže. Vatrozid radi na način da neće propustiti ništa iz vanjske mreže u našu lokalnu mrežu ukoliko mi sami ne otvorimo ulaze (port-ove) za prosljeđivanje prometa i regulaciju propusnosti. Pomoću regulacije propusnosti može se ograničiti propusnost za jednoga ili više korisnika i također se može ograničiti raspon uređaja.



16. Slika: Otvaranje Vatrozida i prikaz otvorenih port-ova

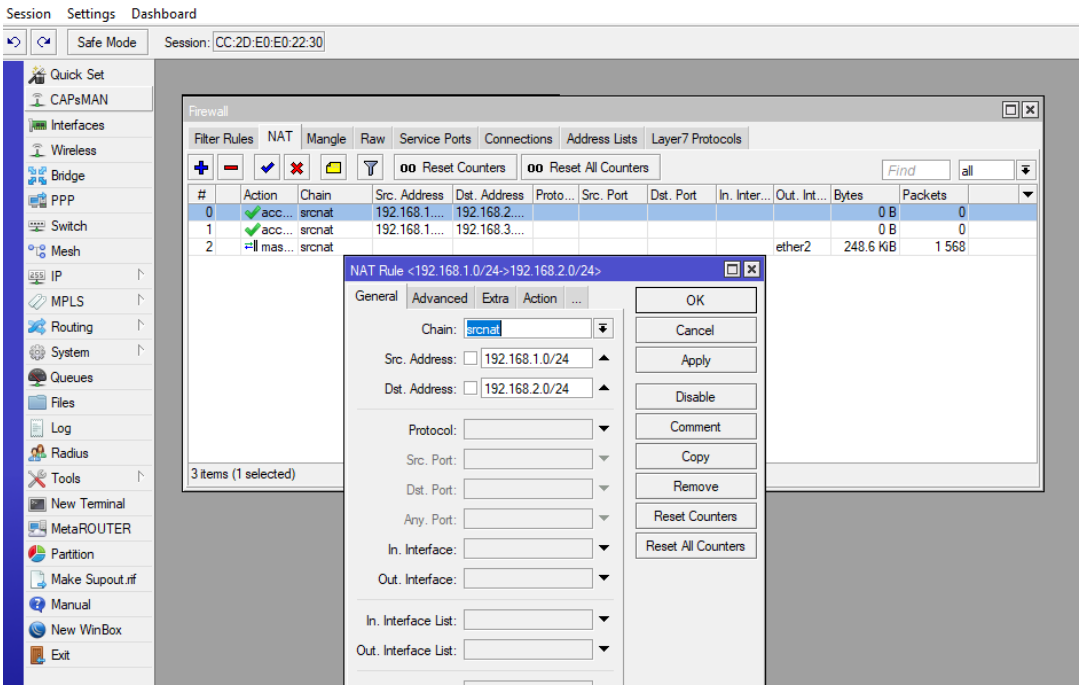
Kako bi se otvorili ulazi, potrebno je izabrati stavku „IP“, te „Firewall“. Potom nam se otvori prozor gdje na horizontalnoj traci se traži „NAT“ (*Network Address Translation*). *NAT* je proces pretvaranja pojedine IP adrese koja se koristi u jednoj mreži u IP adresu druge mreže. Nakon NAT se klikne na „+“ koji otvara novi prozor gdje se na izbornoj traci odabere „General“ i tu se između ostalog može upisati, odnosno upisuje izvorišna adresa mreže, te odredišna. Klikom na „Apply“ se potvrdi otvaranje određenog ulaza.

6.3.1. Postavljanje Vatrozida na „Router_1“

Za postavljanje „NAT“ na „Router_1“ dva puta se postavljaju odredišne adrese, odnosno otvaraju se rute prema ostalim („Router_2“ i „Router_3“) poslužiteljima. Izvorišna adresa mreže je ovom slučaju adresa usmjernika prema kojemu se prolazi otvaraju; izvorišna adresa je: 192.168.1.0/24.

Otvaranje ruta vrši se prema gore navedenim koracima, odnosno dva puta se mora ponoviti postupak „IP“, pa „Firewall“, zatim tražimo „NAT“, i u konačnici „+“. U oba pristupa je izvorišna adresa ista, a mjenjamo odredišnu. Redoslijed je nebitan, pa nije bitno koja se adresa za odredišnu stavlja prva, a koja druga.

Korištene odredišne adrese za konfiguraciju Vatrozida na „Router_1“ su: 192.168.2.0/24 (adresa koja vodi od „Router_3“ do poslužitelja, odnosno računala „PC_3“) i adresa 192.168.3.0/24 (adresa koja povezuje „Router_2“ i poslužitelja, to jest računalo „PC-2“).



17. Slika: Prikaz otvaranja i već otvorenih port-ova

Nakon postavljenih adresa, klikne se „Apply“ i zatim „OK“.

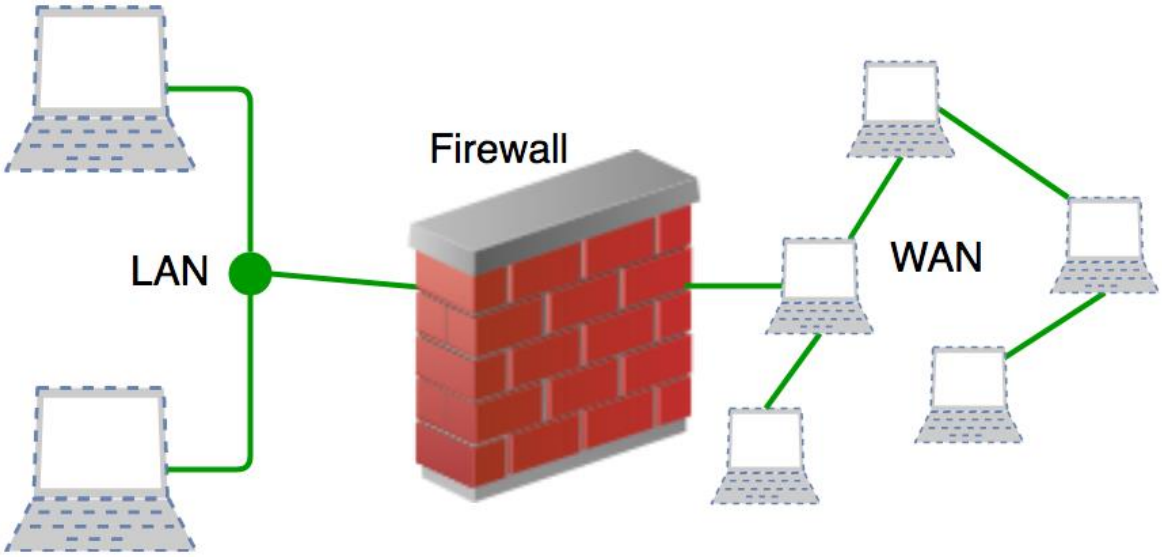
Nakon što se dva puta ponovi isti postupak (samo se promijeni odredišna adresa), ponovno se ide na „+“, te se u „General“ ode na polje „Out. Interface“ gdje se postavi izlazno sučelje (Ether_2). Zatim se u istom prozoru ode na „Action“ i odabere se „Masquerade“.

6.3.2. Postavljanje Vatrozida na „Router_2“ i „Router_3“

Da bi konfiguracija cijela uspješno radila, odnosno da bi fizički odvojeni poslužitelji mogli međusobno komunicirati, potrebno je u svakoj VPN mreži ponoviti prethodno opisane korake. Pa tako moramo konfigurirati i na usmjernicima „Router_2“ i „Router_3“.

Na usmjerniku „Router_2“ postavlja se njegova izvorišna adresa, odnosno 192.168.3.0/24, dok su odredišne adrese 192.168.1.0/24 i 192.168.2.0/24.

Izvorišna adresa od usmjernika „Router_3“ je 192.168.2.0/24, aodredišne su 192.168.1.0/24 i 192.168.3.0/24.



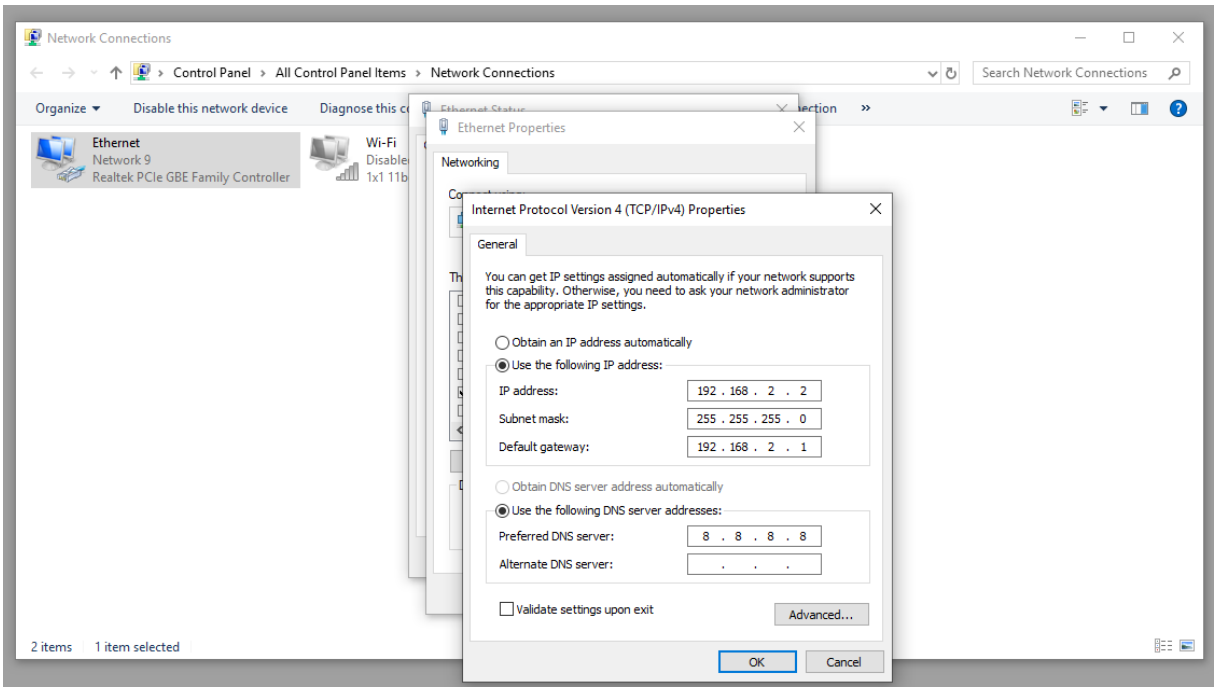
18. Slika: Firewall

Slikoviti prikaz položaja gdje Vatrozid djeluje, odnosno gdje se postavlja.

7. POSTAVLJANJE IPSEC TUNELA

7.1. Postavljanje adresa na PC-eve

Konačno, nakon svih navedenih i opisanih postupaka, na kraju se postavlja IPSec. Prije postavljanja IPSec-a, provjerio sepostav statičkih ruta tako što su se pingali elemente mreže međusobno. Prije toga su se na PC-jevima morale promjeniti njihove adrese, odnosno ručno ih postavili na odgovarajuće.



19. Slika: Promjena IP adrese na računalu

Krajnja računala su mogla komunicirati samo sa svojim usmjernikom, to jest, paket nije prolazio u WAN mrežu.

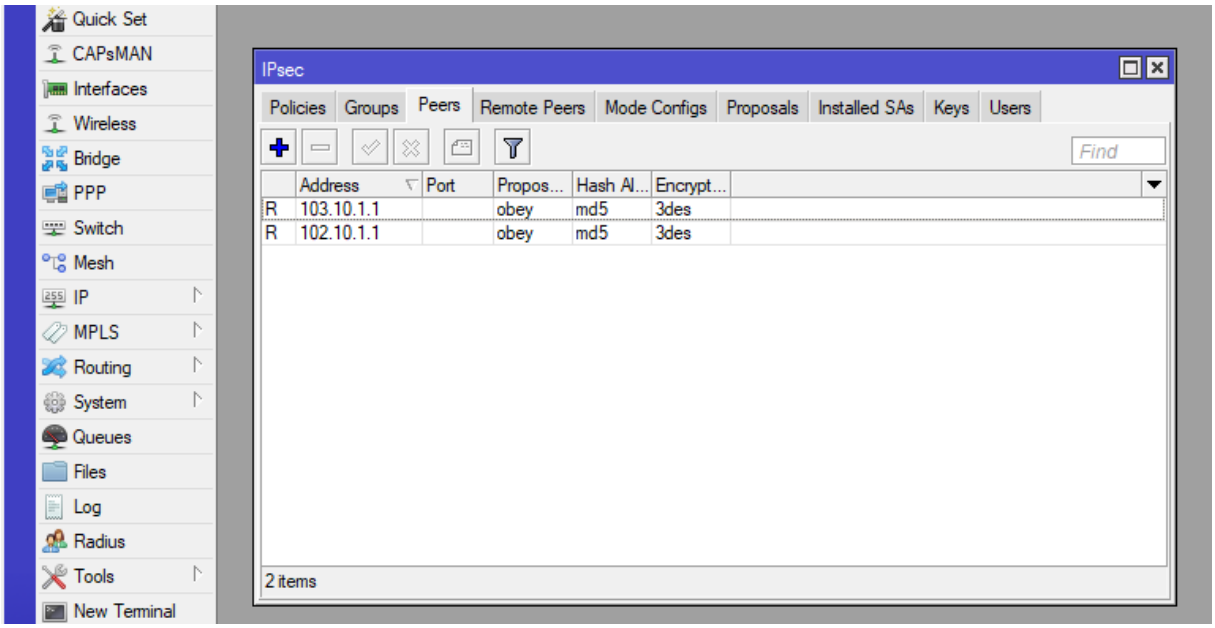
Postavljanje IPSec tunela je omogućilo prolazak paketa od računala „PC-1“ do računala „PC-2“ i „PC_3“, te obratno, što je u globalu i bio cilj zadatka.

Postavljene adrese poslužitelja:

- PC_1 – 192.168.1.2, podmrežna maska je 255.255.255.0
- PC_2 – 192.168.3.2, podmrežna maska je 255.255.255.0
- PC_3 – 192.168.2.2, podmrežna maska je 255.255.255.0

7.2. Postavljanje „Peers-a“

U „Peers-u“ se popunjavaju polja adrese mreže na koju nam paket treba doći, bira se autentifikacijsku metoda i vrlo značajno polje „Secret“ u koje se upisuje šifra koja se također mora poklopiti s obje strane mreže.



20. Slika: Izgled prozora „Peers“

Na svakome usmjerniku se ponove ovi koraci, te se za adrese postavljaju adrese koje su između usmjernika i unutarnje mreže, odnosno adrese koje provode pakete prema unutarnjoj mreži, odnosno Internetu. Na svakoj strani se moraju postaviti dvije „Peers“ kolone, a stavljaju se nasuprotne adrese od dotičnog usmjernika.

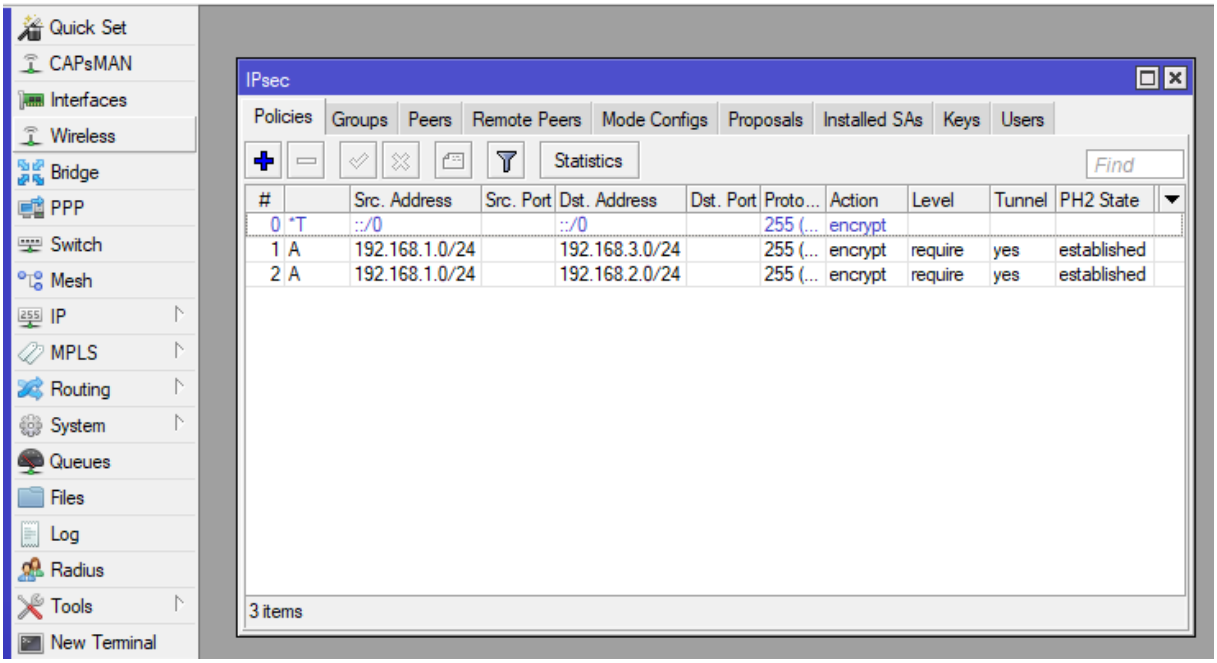
Pa tako:

- Za usmjernik „Router_1“ se postave dvije kolone; jedna sa adresom 102.10.1.1 i druga 103.10.1.1.
- Za usmjernik „Router_2“ se postavljaju adrese 101.10.1.1 i 102.10.1.1.
- Za usmjernik „Router_3“ su adrese 101.10.1.1 i 103.10.1.1.

Od velikog značaja je polje „Secret“ gdje se nalazi šifra koja se mora poklopiti od svih strana koje žele međusobno komunicirati. Korištena zaporka u tome polju bila je „12345“. Korištena šifra je vrlo jednostavna, no ozbiljnije korporacije koje koriste VPN metodu sa IPSec protokolom koriste kompliciranije.

7.3. Postavljanje pravila (*eng. Policies*)

Dok je otvoren prozor IPSec-a, ide se na „Policies“ (Pravila). Ulaskom u to polje otvori se prozor gdje je na izbor dato „General“ ili „Action“. Klikom na „Action“ moguće je opet izabrati protokol koji je već prije određen da će se koristiti, stavi se kvačica u polje gdje piše „Tunnel“ te se zatim upišu izvorišne i odredišne adrese. Također, u desnome stupcu se vidi uspješna uspostava veze (eng. *Established*).



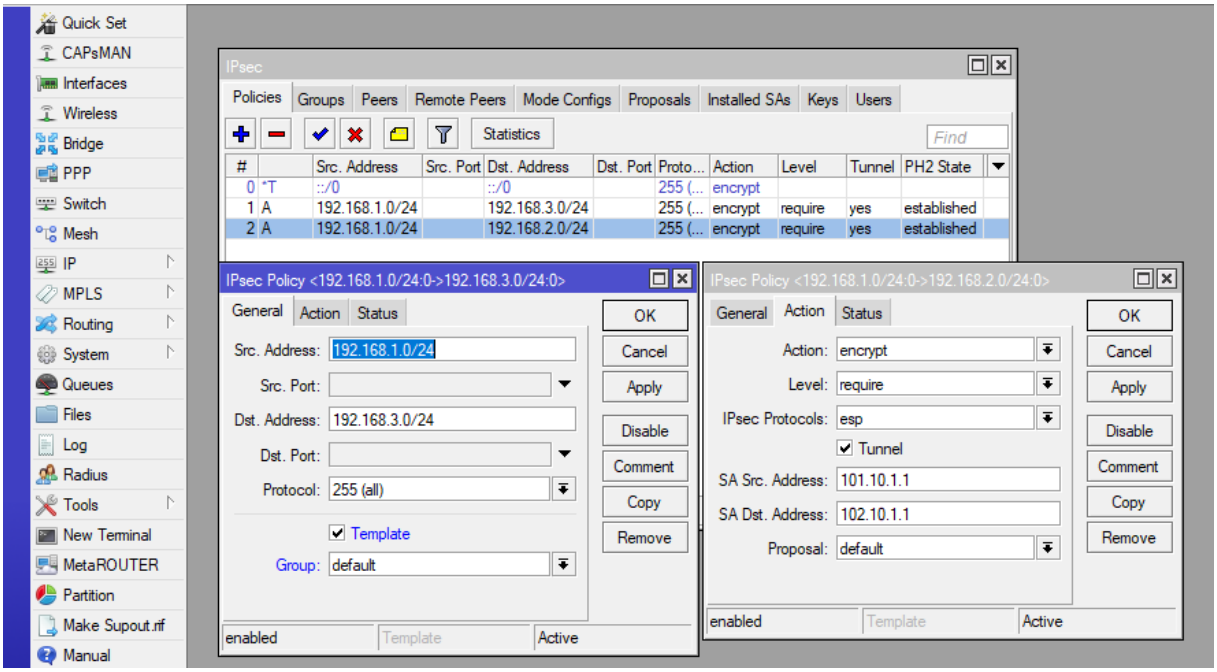
21. Slika: Prikaz polja „Policies“

U „General“:

- Za „Router_1“ na mjesto izvorišne adrese upisuje adresa LAN mreže, odnosno upisuje se strana koja gleda prema poslužitelju, a ta adresa je 192.168.1.0/24, dok su odredišne adrese usmjernik „Router_1“ su 192.168.2.0/24 i 192.168.3.0/24.
- Za „Router_2“ izvorišna adresa je192.168.3.0/24, dok su odredišne 192.168.1.0/24 i 192.168.2.0/24.
- Kod „Router_3“ izvorišna adresa je 192.168.2.0/24, a odredišne su 192.168.1.0/24 i 192.168.3.0/24

U „Action“:

- „Router_1 “ koristi 101.10.1.1 kao izvorišnu, te 102.10.1.1 i 103.10.1.1 kao odoredišne adrese.
- „Router_2“ koristi 103.10.1.1 kao izvorišnu, te 101.10.1.1 i 102.10.1.1 kao odredišne adrese.
- „Router_3“ koristi 102.10.1.1 kao izvorišnu, te 101.10.1.1 i 103.10.1.1 kao odredišne adrese.



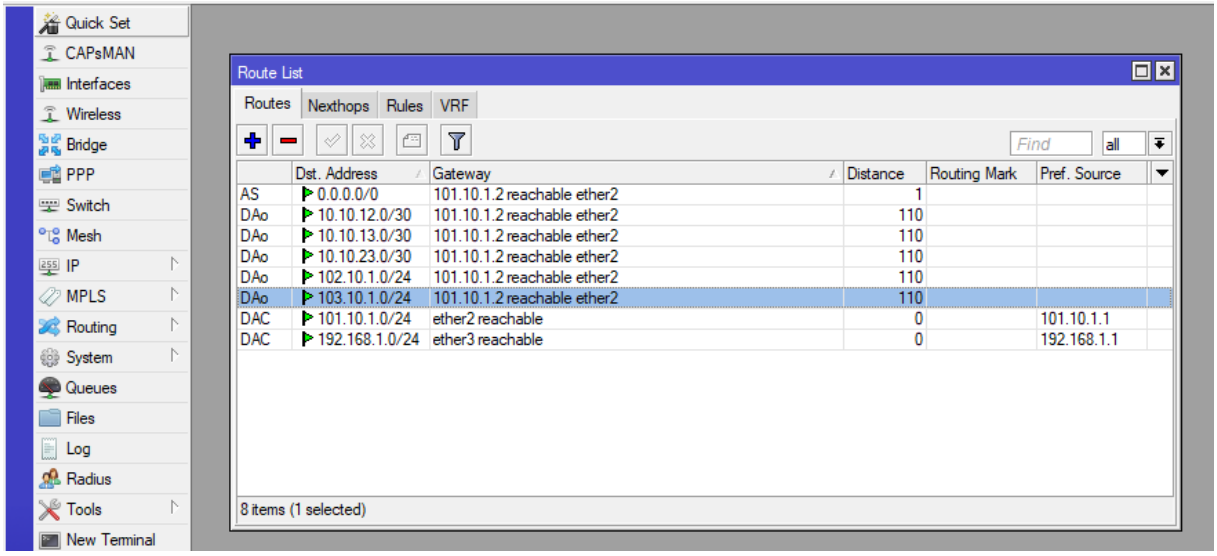
22. Slika: Prikaz „General“ i „Action“

Na priloženoj slici može se vidjeti otovreni prozor „General“ koji je poveznica sa „Router_2“, te kako se ne može ista konfiguracija pravila otvoriti u dva prozora, za prikaz „Action“ se otvorila poveznica sa „Router_3“.

„Policies“ su radili po „default“, odnosno zadanim prijedlozima (eng. *Proposals).*

7.4. Pregled ruta

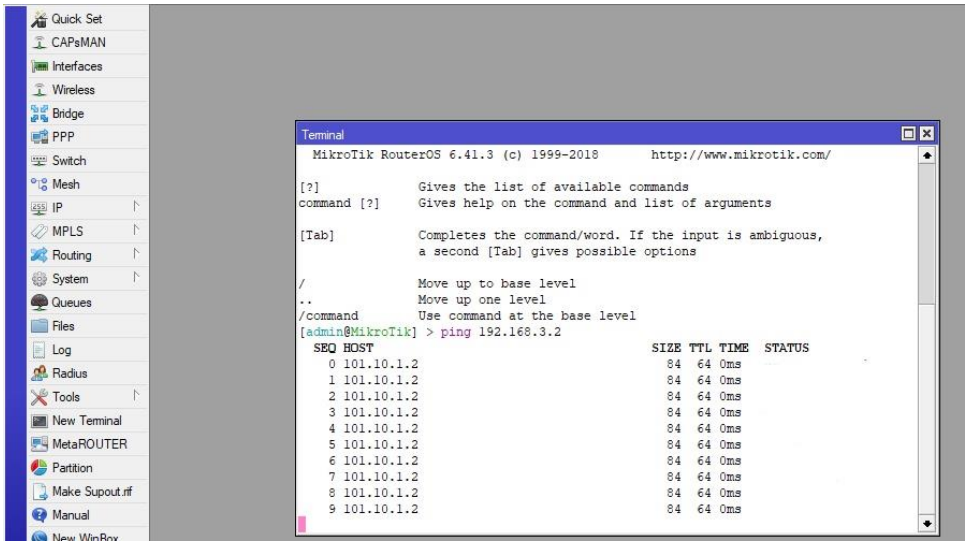
Nisu se postavljale statičke rute, no klikom na „IP“, zatim „Routes“ prikaže se izlist svih trenutnih ruta spojenih na pojedini usmjernik.



23. Slika: Prikaz ruta

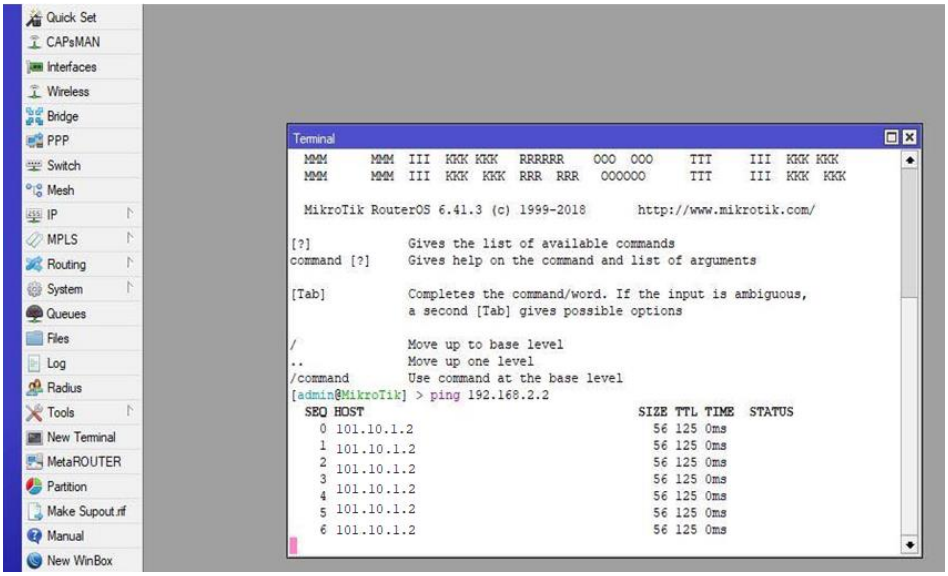
8. REZULTAT

Kao dokaz uspješno provedenog projekta u nastavku će se staviti slika. Provjera ispravnosti konfiguracije se vršila tako što se na glavnom konfiguracijskom sučelju odabere stavka „New Terminal“ i otvori nam se prozor koji oponaša Naredbeni Redak (*eng. Command Prompt*) u koji upisujemo adrese koje nas zanimaju za provjeru komunikacije.



24. Slika: Prikaz komunikacije PC_1 sa PC_2

Na slici se može vidjeti prolaz „Pinga“ od prvog poslužitelja prema drugome. „Pinganje“ se provelo sa svih računala u Winboxu.



25. Slika: Prikaz komunikacije PC_1 sa PC_3

9. ZAKLJUČAK

IPSec protokol je osmišljen tako da zaštiti pojedinačne TCP/IP pakete koji putuju mrežom pomoću enkripcije javnih ključeva. Tijekom godina se razvilo niz metoda kako se osigurava sigurnost preko interneta, no IPSec je prvi koji štiti paket na IP sloju. Paketi koji su pod zaštitom IPSeca su sporiji od uobičajenih IP paketa zbog veličine paketa i popratnnih stvari koji su potrebni za šifriranje, odnosno dešifriranje. Pošto je paket veći, to utječe i na potrošnju mrežnog pojasa.

VPN (*Virtual Private Network*) je tehnologija kojom je omogućeno sigurno povezivanje mrežnih elemenata preko javne mrežne infrastrukture u virtualne privatne mreže, gdje se IPSec često koristi kao protokol. Ovaj način zaštite je i dokaz kako nije nužno da se kupuju ili implementiraju razni sustavi, već je potrebno poznavati sustav i iskoristiti sve funkcionalnosti koje su već u njemu implementirane.

POPIS LITERATURE

Internet izvori:

http://rajco.me/blog/2012/08/mikrotik-vpn/?fbclid=IwAR1wFYamj3hJWU-sVuQEWCJvb0sh-tbUvbUcVcVvpnR05R6fLVUQH5s2yeM

https://mikrotik.com/product/RB962UiGS-5HacT2HnT?fbclid=IwAR3KoHe60yijpvmaQhD0v-3VNuGh3q1YD0NcFqg3h0k97BYPNelsFjMoL2I

https://www.petri.com/what_are_ipsec_policies?fbclid=IwAR1pC9z_JXSIb3zcsTGOyWo4Lf4N9xAEosnVd52Hz2YhsOX7tfEetYsokb8

https://www.thesecuritybuddy.com/vpn/what-is-ipsec-protocol-and-how-does-it-work/?fbclid=IwAR3KoHe60yijpvmaQhD0v-3VNuGh3q1YD0NcFqg3h0k97BYPNelsFjMoL2I

http://spvp.zesoi.fer.hr/seminari/2006/ZivkovicGoran_IPsec.pdf

POPIS SLIKA