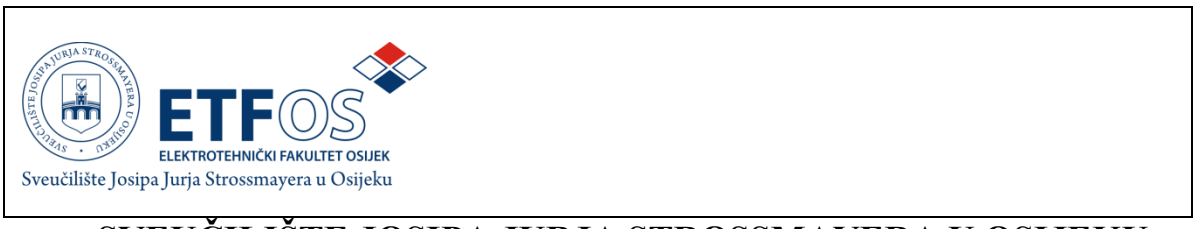
Konfiguriranje hardverskih vatrozida u lokalnim računalnim mrežama

Opačak, Josipa



SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

ELEKTROTEHNIČKI FAKULTET

Sveučilišni studij

KONFIGURIRANJE VATROZIDA U LOKALNIM RAČUNALNIM MREŽAMA

Završni rad

Josipa Opačak

OSIJEK, 2016.

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom studiju	
Osijek, 29.08.2016.	
Odboru za završne i diplomske ispite	
Prijedlog ocjene završnog rada	
Ime i prezime studenta:	**Josipa Opačak**
Studij, smjer:	Preddiplomski studij elektrotehnike, Komunikacije i informatika
Mat. br. studenta, godina upisa:	3771, 2013.
Mentor:	**Prof.dr.sc. Drago Žagar**
Sumentor:	**Dr. sc. Višnja Križanović Čik**
Naslov završnog rada:	**Konfiguracija vatrozida u lokalnim računalnim mrežama**
Primarna znanstvena grana rada:	Telekomunikacije i informatika
Sekundarna znanstvena grana (ili polje) rada:	
Predložena ocjena završnog rada:	
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: Postignuti rezultati u odnosu na Jasnoća pismenog izražavanja: Razina samostalnosti:
Potpis sumentora:	Potpis mentora:
Dostaviti: 1. Studentska služba	
Potpis predsjednika Odbora: _____	
Dostaviti: 1. Studentska služba	

IZJAVA O ORIGINALNOSTI RADA

Osijek,30.8.2016.

Ime i prezime studenta:	**Josipa Opačak**
Studij :	Preddiplomski studij elektrotehnike
Mat. br. studenta, godina upisa:	3771, 2013.

Ovom izjavom izjavljujem da je rad pod nazivom**:**

Konfiguracija vatrozida u lokalnim računalnim mrežama

izrađen pod vodstvom mentora**Prof.dr.sc. Drago Žagar**

i sumentora**Dr.sc. Višnja Križanović Čik**

mojvlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.

Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada,osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, ašto je izričito navedeno u radu.

Potpis studenta:

1. UVOD

U današnje vrijeme kada je Internet posvuda prisutan, kako u različitim poslovnim organizacijama tako i u kućanstvima, javila se sve veća potreba za zaštitom podataka od udaljenih zlonamjernih korisnika . Posebna opasnost javlja se kod računala koja su povezana u mreže i neprestano spojena na Internet. Da bi se zaštitile mreže računala koriste se vatrozidi koji se nalaze kao spona između lokalnih mreža i drugih neprovjerenih mreža. Vatrozidi se nalaze na ulazu odnosno izlazu mreže. Zadatak vatrozida je provjeravati sve mrežne pakete koji ulaze ili izlaze iz mreže po određenim kriterijima i pravilima te filtrirati promet koji se razmjenjuje između računalnih mreža s različitim stupnjevima povjerenja. Najčešće su to javna internetska mreža i neka privatna mreža. Zadaća vatrozida je određene pakete propuštati ili blokirati na njihovom putu, ovisno o postavljenim pravilima. Dolaze u različitim oblicima ovisno o potrebama korisnika. U osnovi, vatrozid je zaštitni mehanizam koji kontrolira mrežne pakete koji se razmjenjuju između mrežnih segmenata i koji iziskuje različite razine sigurnosti.Prilikom korištenja Interneta postoje potrebe za sigurnim spajanjem na udaljene terminale usluga, prijenos datoteka (FTP), elektroničke pošte (SMTP) i Usenet (NNTP). U današnje vrijeme ti servisi su dodani na listu zahtjeva za pristup, ali kako se razvija Internet i dalje se razvija potreba za većim brojem različitih servisa, pa se tako i napadi mijenjaju, kako bi vatrozidi mogli pratiti trendove, nova pravila se moraju kontinuirano ažurirati. Vatrozid (eng.*firewall*) nastao je kasnih 1980-ih godina kada je Internet bio još prilično nova tehnologija u smislu globalnog povezivanja i korištenja.

1.1. Zadatak završnog rada

U ovom radu potrebno je opisati primjenu i vrste vatrozida. Također u primjeru testne mreže potrebno je definirati i postaviti pravila za filtriranje prometa, zaštitu usmjerivača te lokalne računalne mreže. U praktičnom dijelu rada potrebno je kao zaštitni mehanizam koristiti usmjerivač MikroTik RouterOS koji implementira značajke vatrozida koje uključuju analizu i klasifikaciju mrežnog prometa te filtriranje prometa. Provedeno je testiranje konfiguracije usmjerivača MikroTik RoterOS koje je obuhvaćalo određene specifikacije, navedene u radu.

2. SIGURNOST MREŽA, USLUGA I APLIKACIJA

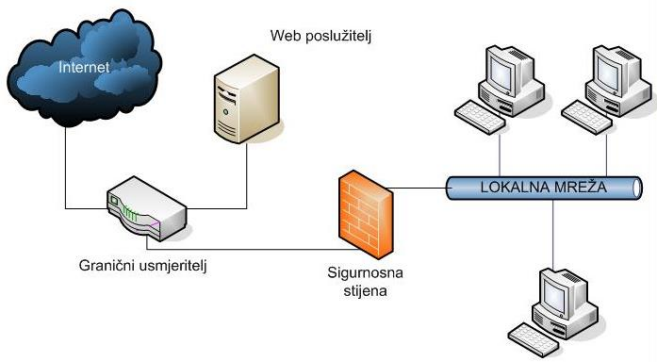
Sigurnost mreža, usluga i aplikacija može se promatrati kao sposobnost mreže ili informacijskog sustava da se suprotstavi neočekivanim slučajnim događajima i neprijateljski usmjerenim aktivnostima [3]. Napadi koji se događaju na informacijski sustav računala mogu narušiti povjerljivost pohranjenih podataka, prenesenih informacija te općenito usluga koje takve mreže nude. Napad na mreže omogućavaju nedostatci u sustavu, odnosno njegove sigurnosne slabosti [16]. Napade je moguće otkloniti uz primjenu odgovarajućih zaštitnih mehanizama čime se smjanjuje ranjivost sustava.

2.1. Vrste računalnih mreža u kojima su potrebni zaštitni mehanizmi

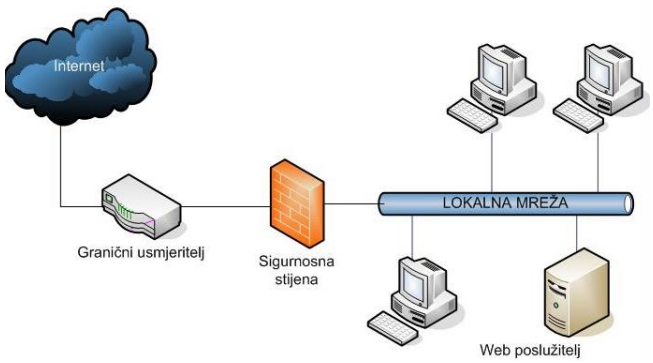
Zaštitni mehanizmi se mogu konfigurirati na različite načine, ovisno o potrebama korisnika i vrstama mreža u koje se postavljaju. Računalne mreže mogu biti privatne mreže koje ne omogućuju pristup vanjskim korisnicima, privatne mreže koje omogućuju pristup vanjskim korisnicima i demilitarizirana zona [3] , opisane u nastavku.

- Privatne mreže koje ne omogućuju pristup vanjskim korisnicima obuhvaćaju slučajeve kada privatna lokalna mreža može funkcionirati na način da ne pruža nikakve usluge vanjskim korisnicima te ne podržava virtualne privatne mreže. Zaštitni mehanizam u tom slučaju propušta pakete koji potječu s privatne mreže i odgovarajuće povratne pakete [3]. Zaštitni mehanizam će dakle automatski odbacivati pakete koje korisnik iz vanjske mreže želi poslati privatnoj mreži. Ovakva mreža je sigurnija od ostalih i lako ju je konfigurirati. Međutim, neučinkovita je iz razloga što onemogućava raspodjelu djelatnika određene organizacije na udaljena radna mjesta s obzirom da ne podržava virtualne privatne mreže. Rasprostanjenija je u kućnim uredima, negoli u velikim organizacijama. Privatna mreža ove vrste prikazana je na slici 2.1..
- Privatne mreže koje omogućuju pristup vanjskim korisnicima podrazumijevaju da postoje organizacije koje pružaju usluge vanjskim korisnicima kao što su primjerice web, FTP, DNS i slično, te također omogućavaju konfiguriranje virtualnih privatnih mreža [3]. Privatna mreža ove vrste prikazana je na slici 2.2.. Zaštita za takve organizacije realizira se na više načina:

- Ukoliko se poslužiteljska konfiguracija nalazi izvan lokalne mreže, konfiguracija zaštitnog mehanizma jednaka je kao u prethodnom slučaju, međutim računala izvan lokalne mreže izložena su različitim prijetnjama [3].
- Ukoliko se poslužiteljska konfiguracija nalazi unutar lokalne mreže, a od javne mreže je odvojena zaštitnim mehanizmom tada se dopušta i slanje paketa koji pripadaju odgovarajućim uslugama [3]. Konfiguracija ovakvog zaštitnog mehanizma je prilično osjetljiva jer bilo kakav propust može biti prilika napadaču koji time može doprijeti i do ostalih računala u mreži.
- Ukoliko se koriste dva zaštitna mehanizma, prvi se spaja na javnu mrežu i poslužiteljsku mrežu, a drugi se postavlja između te mreže i privatne lokalne mreže [3]. U ovom slučaju konfiguracijesu različite. Naime zaštitni mehanizam koji je spojen na privatnu lokalnu mrežu propušta samo one pakete koji su dio neke uspostavljene veze, dok zaštitni mehanizam koji je spojen na javnu mrežu osim tih paketa propušta i pakete koji su namijenjeni poslužiteljima.
- Ukoliko koristimo dva zaštitna mehanizma potrebno je iste pakete dva puta provjeravati, zbog čega se smanjuje brzina prijenosa podataka [3]. U ovom slučaju koristi se konfiguracija demilitarizirana zona.

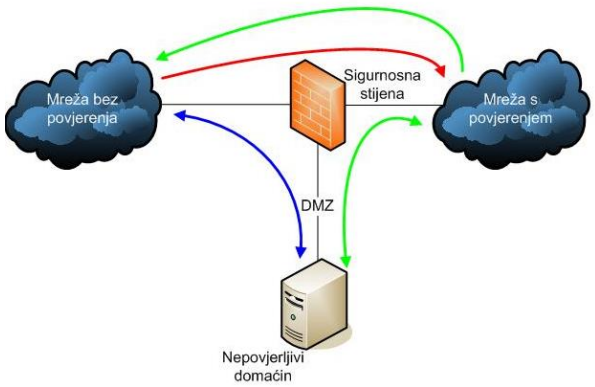


Slika 2.1. Web poslužitelj izvan zaštićenog područja



Slika 2.2. Web poslužitelj unutar zaštićenog područja

- Demilitarizirana zona podrazumijeva da se filtrira promet između javne i privatne mreže. Svaka mreža koristi po jedno mrežno sučelje kojemu dodaje treće sučelje putem kojeg je spojeno na demilitariziranu zonu [3]. Princip konfiguracije mreže je taj da se na sučelje prema privatnoj mreži propuštaju samo paketi koji pripadaju uspostavljenoj vezi, dok se prema poslužiteljima omogućava slanje početnih paketa i s privatne i s javne mreže. Put podataka u demilitariziranoj zoni prikazan je na slici 2.3..



Slika 2.3. Put podataka u demilitariziranoj zoni

2.2. Sigurnosni zahtjevi

Sigurnost mreža, usluga i transakcija bitna je za stvaranja povjerenja u primjenu elektroničkog poslovanja te u svrhu privatne komunikacije. Prijetnja u mrežnoj okolini podrazumijeva događaj koji može naškoditi korisnicima te računalnim sustavima s obzirom na zloupotrebu određenih podataka. Osnovni sigurnosni zahtjevi su [3]:

- autentifikacija - podrazumijeva određene metode provjere autentičnosti korisnika

- cjelovitost - potvrda da su informacije poslane i primljene u nepromijenjenom obliku (samo ovlaštene osobe imaju mogućnost promjene podataka) .
- povjerljivost - podrazumijeva zaštitu povjerljivih informacija od neovlaštenog čitanja
- neporicanje - korisnici ne mogu nijekati komunikaciju u kojoj su sudjelovali
- kontrola pristupa - ograničava pristup informacijama
- raspoloživost - informacije moraju biti raspoložive bez obzira na bilo kakve neočekivane situacije

2.3. Sigurnosne prijetnje

Poznato je nekoliko skupina sigurnosnih prijetnji [3]:

- presretanje - elektronička pošta se može presretati te se informacije mogu kopirati, time se narušava privatnost pojedinca
- prekidanje komunikacije - napadi koji podrazumijevaju prekid uobičajenog tijeka komunikacije
- promjena - pristup bez dozvole, koji podrazumijeva kopiranje, promjenu i uništavanje podataka
- ubacivanje lažnih informacija - podrazumijeva napad na autentičnost zbog ubacivanja zlonamjernih informacija

2.4. Vrste napada

Četiri su glavne vrste napada, a to su [3] :

- presretanje komunikacije - podrazumijeva prisluškivanje i nadzor mrežnog prometa. Ova vrsta napada izvediva je pogotovo kod bežične komunikacije te kod komunikacije koja uključuje višeodredišno ili grupno razašiljanje
- prekidanje komunikacije - moguće je izvršiti uništavanjem uređaja, fizičkim uništavanjem komunikacijskih uređaja, šumovima, brisanjem programa datoteka i slično
- promjene - uključuju promjene u datotekama, zlonamjerno brisanje ili dodavanje informacija

- ubacivanje lažne informacije - podrazumijeva dodavanje novih zapisa, ubacivanje IP datagrama, lažne elektroničke pošte

Potencijalni izvori napada su napadi iznutra i napadi izvana. Napadi iznutra su napadi koji podrazumijevaju da dio prijetnji može doći iz samog sustava i od samih korisnika:

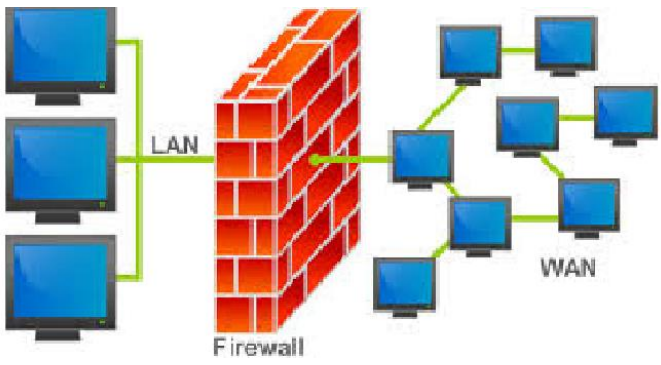
- sami korisnici mogu nenamjerno, radeći određene pogreške uzrokovati štete
- operateri usluga mogu zloupotrijebiti svoj položaj i onemogućiti ili otežati pružanje određenih usluga
- prijetnju predstavljaju i djelatnici koji nisu izravno vezani uz pružanje usluga, ali imaju pristup sustavu

Napadi izvana podrazumijevaju prijetnje koje dolaze izvan sustava [9]:

- vanjski neprijatelji koji imaju pristup javnoj mreži, ali ne i određenim uslugama
- kriminalne ili terorističke organizacije
- obavještajne službe
- komercijalne tvrtke
- hakeri
- istražiteljske agencije.

3. VATROZID

Vatrozid (engl. *firewall*) je sigurnosni, mrežni uređaj, odnosno program koji je smješten između javne mreže i lokalne mreže isprogramiran kako bi zaštitio neovlašteni pristup povjerljivim korisničkim podacima. Princip rada je blokiranje i zabrana prometa po određenim pravilima koja su definirana korisnikovim zahtjevima, odnosno potrebama. Nije nužno da svi korisnici lokalne mreže imaju jednaka prava pristupa Internetu. Postavljaju se između dva ili više korisnika, te se time mogu kontrolirati i prava pristupa korisnika pojedinim dijelovima mreže. Vatrozid ima određene zahtjeve koje prihvaća, dok ostale sve blokira. Vatrozid možemo promatrati i kao virtualni tunel kroz koji putuju kriptirani podaci, idealan je za razmjenu osjetljivih podataka. Može biti softverski ili hardverski. Softverski štiti jedno računalo osim ukoliko štiti cijelu mrežu, postavljen je na određenom računalu koje je spojeno na zaštićenu i nezaštićenu mrežu. U tom slučaju je brzina mrežnog prometa smjanjena jer dolazi do različite provjere podataka. Kod hardverskih vatrozida je pojednostavljena konfiguracija samog vatrozida te je i maksimizirana brzina provjere podataka. Za ispravan rad vatrozida potrebno je precizno odrediti niz pravila koje definiraju kakav mrežni promet je dopušten u pojedinom mrežnom segmentu. Takvom sigurnosnom politikom se određuje nivo zaštite koji se želi postići primjenom vatrozida [2].



Slika 3.1. Vatrozid

Osnovna funkcija vatrozida je spriječiti neovlašteni pristup s jedne mreže na drugu. Računala koja imaju vatrozid već imaju definirano pravilo o tome što je dozvoljeno, a što ne. Pravila sigurnosti određuju opcije konfiguracije vatrozida. Vatrozid ne pronalazi računalne viruse i crve koji su već na vašem računalu. Protiv ovakvog oblika opasnosti se bore

antivirusni programi. Nadalje, vatrozid neće spriječiti otvaranje opasnih privitaka primljenih elektroničkom poštom niti će blokirat podatke poslane elektroničkom poštom [2].

Glavna uloga vatrozida je ispitivanje IP paketa koji putuju između klijenata i servera, odnosno time se ostvaruje kontrola toka informacija za svaki servis po IP adresi i portu u oba smjera. Zadužen je za više važnih stvari unutar informacijskog sustava :

- mora implementirati politiku sigurnosti što znači da ukoliko određeno svojstvo nije dozvoljeno, mora onemogućiti rad u tom smislu;
- treba bilježiti sumnjive događaje;
- treba upozoriti administratora na pokušaje proboja i kompromiranje sigurnosti;
- u nekim slučajevima vatrozid može onemogućiti statistiku korištenja.

S obzirom na način na koji funkcioniraju postoje tri vrste vatrozida, to su *Packet Filtering, Circut Gateways, Application Gateways:*

- *Packet filtering* je vrsta vatrozida koja filtrira podatkovne pakete ovisno o njihovim IP adresama te o njihovim opcijama paketa. Prate izvorišnu i odredišnu adresu te ovisno o tom donose sigurnosne odluke, propustiti paket ili ne. Opcije kojee proučavaju su izvorišna adresa, odredišna adresa, veličina paketa, ime protokola i slično. *Packet filtering* je dobro rješenje u malim mrežama dok u velikim već gubi na svojoj snazi. Tri podvrste su:
    - statično filtriranje - prisutno je kod većine usmjerivača i pravila za filtriranje mogu se ručno mijenjati.
    - dinamičko filtriranje - dopušta mijenjanje pravila za filtriranje na osnovu vanjskih procesa koji se događaju. Primjerice, dopušta propuštanje FTP paketa iz vanjske mreže ukoliko je netko unutar lokalne mreže zatražio FTP sesiju i traži određen podatak.
    - *Stateful Inspection* - princip rada sličan je kao kod dinamičkog filtriranja s tim da se pozornost više obraća na podatke koji se nalaze u IP paketu.

- *Circuit Gateways* zasniva se na transportnom sloju na kojemu se paketi prihvaćaju ovisno o IP adresama izvora. Ne mogu promatrati protok podataka, ali sprječavaju direktnu vezu između primjerice lokalne i vanjske mreže.
- *Application Gataweys* je jedan od najsloženijih sistema provjere podataka.

Provodi se na sigurnom sustavu domaćina konfigurirans dva mrežna sučelja. Također zahtijeva veću količinu memorije i procesorska sredstva u odnosu na druge tehnologije.

3.1. Filtriranje paketa

Filtriranje paketa podrazumijeva kontroliranje i analizu dolaznih i odlaznih tokova podataka. Analiza se provodi na način da se podatkovni paketi koji se prenose kroz fizički kabel prihvaćaju i analiziraju.

Filter paketa otvara svaki pojedini podatkovni paket i provjerava njegov sadržaj, odnosno odgovara li sadržaj unaprijed određenim pravilima [7]. Pravila su tako postavljena da se dopušta samo minimalno potrebna komunikacija. Primjer bi bilo IP-fragmentiranje. Filtriranjem paketa transparentno se integriraju u mrežu tako da imaju ulazni i izlazni priključak [8] . Točan način rada filtriranja paketa je sljedeći [7]:

- provodi se provjeravanje, s koje strane se paketi prihvaćaju;
- na odredišnom sloju se provjeravaju izvorišna i odredišna MAC adresa;
- u mrežnom sloju se analiziraju izvorišna i odredišna adresa te i zastavice kao i ICMP naredbe;
- na transportnom sloju se provjeravaju brojevi portova UDP/TCP-protokola;
- također se može provjeravati smiju li se podatci slati u određenom vremenskom razdoblju.

Odgovarajuća analiza i provjera podataka i informacija odrađuje se prema unaprijed određenim pravilima i zahtjevima koja su postavljena prilikom programiranja vatrozida. Prilikom utvrđivanja nepravilnosti šalje se obavijest na administratora sustava te ubrzo slijedi odgovarajuća reakcija.

Osnovna pravila filtriranja paketa obuhvaćaju statička filtriranja [7]. Na temelju različitih podataka koje se kod statičkog filtriranja provjeravaju odlučuje se treba li mrežni paket biti proslijeđen na drugu mrežu ili ne. Filtriranje paketa provodi se ovisno o provjeravanju određenih podataka na osnovu kojih se dobiju različite vrste filtriranja, a to su filtriranje paketa ovisno o vrsti protokola, filtriranje paketa u ovisnosti o IP adresama, filtriranje u ovisnosti o portovima, filtriranje paketa u ovisnosti o broju fragmentiranog paketa te filtriranje u ovisnosti o putu usmjeravanja.

Filtriranje paketa ovisno o vrsti protokola, temelji se na principu da je osnovni način rada filtriranje paketa ovisno o sadržaju IP protokolnog polja [6]. Hoće li paket biti proslijeđen ili ne određuje se na osnovu protokola koji se unutar paketa koristi. Najčešći protokoli su:

1. *User Datagram Protocol* (UDP)
2. *TransmissionControl Protocol* (TCP)
3. *Internet Control Message Protocol* (ICMP)
4. *Internet Group Management Protocol* (IGMP)

Vrste filtriranja su sljedeće [7]:

- filtriranje paketa u ovisnosti o IP adresama temelji se na principu da se na osnovu IP adresa računala odnosno mreža omogućava odnosno onemogućava komunikacija. Jedan od načina kako zaštititi mrežu od napadača je onemogućiti promet paketa koji kao odredište imaju određene IP adrese. Najbolji način kako spriječiti neželjene napade je omogućiti pristup mreži samo paketima s određenim IP adresama jer ih napadači lako mogu promijeniti.
- filtriranje paketa u ovisnosti o portovima se temelji na principu rada da se prilikom spajanja računala koriste portovi. Portova ukupno ima 65536 od čega se prvih 1024 koriste samo za određene aplikacije. U ovisnosti o aplikacijama moguće je ograničiti pristup mrežnim paketima. S obzirom da su neki aplikacijski protokoli izuzetno osjetljivi na napade potrebno ih je posebno zaštititi,primjer takvih aplikacijskih portova su Telnet, NetBIOS, POP,... Napadači u takvim portovima imaju izuzetno veliku kontrolu. Također se neki portovi koriste za uništavanje pojedinih informacija, primjer takvog porta je DNS.
- filtriranje paketa u ovisnosti o putu usmjeravanja paketa podrazumijeva točno određivanje puta kojim paket putuje od izvora do odredišta i obrnuto. Način određivanja puta kao zaštite se uobičajeno koristio, međutim počeo se koristiti i u svrhe napada. Određivanjem puta kojim paket mora proći napadaču je omogućeno postaviti svoju vlastitu IP adresu kako bi mu se paket mogao vratiti. Napadač je u mogućnosti odrediti put kojim paket treba proći te i odredišni cilj.
- filtriranje paketa u ovisnosti o veličini fragmentiranog paketa temelji se na procjeni veličine paketa koja je određena maksimalnom veličinom od 1500 okteta. Velike poruke se fragmentiraju u manje pakete, te je svrha početni fragmentirani paket odbaciti kako bi se zaključilo da će i ostali paketi biti beskorisni s obzirom da prvi

paket nosi port aplikacije. Međutim, takvo filtriranje nema svrhu s obzirom da napadači odbačenom paketu mogu pridodati redni broj 1 umjesto 0.

3.2. Vrste sigurnosnih napada na Internet

Potrebno je da vatrozid ima strogu i čvrstu politiku prema dolaznim paketima, jer je u suprotnom podložan raznim vrstama napada. Moguće je konfigurirati vatrozid koji propušta paketa samo sa točno određenih IP adresa, što je izuzetno korisno ukoliko vatrozid ne podržava kreiranje virtualnih privatnih mreža, a želimo omogućiti pristup sa određenih IP adresa lokalnoj mreži [7]. Međutim, to ima i određene nedostatke, naime napadač se može domaći paketa te saznati logičku adresu s koje je dozvoljeno spajanje na lokalnu mrežu. Na taj način napadač može nanijeti štetu lokalnoj mreži jer kreira pakete kojima je izvorišna točka logička adresa s koje je dozvoljeno spajanje.

Vatrozid je potrebno konfigurirati na način da onemogućava različite postojeće napade. Svakodnevno nastaju nove vrste napada, sve razvijeniji i sve kompleksniji te bi bilo dobro kada bi svaki vatrozid bio otporan na poznate napade.

Najčešće vrste napada kojima se vatrozidi bave su *IP Address Spoofing, Smurf, Syn Flooding, Ping of death* i *Port scanning:*

- *IP Address Spoofing* se temelji na zlonamjernom lažiranju IP adrese kojim je moguće zaobići zaštitne mehanizme koji se temelje na filtriranju prometa prema IP adresama. Omogućava prolazak paketa s vanjskog okruženja na unutarnje. Napadač kao izvorišnu adresu koristi neku od adresa unutar lokalne mreže. Vatrozid je konfiguriran na način da omogućava prolazak paketa. Napad ove vrste može se spriječiti na način da se onemogući prosljeđivanje paketa koji kao izvorišnu adresu ima neku od lokanih adresa, a kao ulazno okruženje okruženje koje je spojeno na internet.
- *Smurf* napad podrazumijevaju oštećenja koja za cilj imaju onemogućavanje rada pojedinih servera i računala. Napadač odašilje*ICMP* echo zahtjev paket na *broadcast* adresu cijele lokalne mreže. Kao odredišno računalo navodi se ono koje se želi onesposobiti velikim brojem odgovora. Kao bismo se obranili od ovakve vrste napada dovoljno je u konfiguraciji vatrozida onemogućiti *broadcast* paket.
- *Syn flooding* podrazumijeva slanje velikog broja TCP podataka koji su označeni *SYN* zastavicom. Zloupotrebljava mehanizam uspostave TCP konekcije, uspostavlja velik

broj poluotvorenih konekcija. Server može primiti samo ograničeni broj istovremenih konekcija te se iz tog razloga legitimni korisnici neće moći spojiti na server. Problem ove vrste rješava se ograničavanjem broja dolazećih paketa.

- Ping of death podrazumijeva mogućnost rušenja operacijskog sustava zbog velikog broja *ICMP echo* zahtjeva. Problem ove vrste rješava se ograničavanjem broja *ICMP echo* zahtjeva.
- *Port scanning* se temelji na skeniranju portova odredišnog računala koje se provodi pomoću programa koji osluškujući portove detektira koju su od njih otvoreni, tj. pokrenuti. Na taj način detektiraju procese koje bi mogli iskoristiti za provalu u sustav.

3.3. Konfiguracija vatrozida

Postoji više različitih načina konfiguracije vatrozida u mreži, najpoznatiji su *Screening router, Bastion host, Dual-homed host, Sreened host i Screened subnet* [10]:

- *Screening router* podrazumijeva jednu od najjednostavnijih konfiguracija vatrozida. Princip rada podrazumijeva usmjerivać koji analizira dolazni i odlazni promet, te propušta odnosno odbacuje određene pakete u ovisnosti o pravilima koja su unaprijed postavljena.
- *Bastion host* podrazumijeva složeniji stupanj zaštite od *Screening ruter* konfiguracije. Za zaštitu je poslužitelj postavljen u mreži koja je od interneta odvojena vatrozidom. Takva mreža zove se demilitarizirana zona. Izravan pristup iz interne mreže prema vanjskoj moguć je samo preko *Bastion hosta*.
- *Dual homed host* konfiguracija slična je *Bastion host* konfiguraciji, međutim razlika je u tom što host u ovom slučaju ima dva odvojena sučelja, odnosno prema unutrašnjoj i prema vanjskoj mreži.
- Kombinacija *Screening routera* i *Bastion host* konfiguracije čini *Sreened host* konfiguraciju. U ovom slučaju se između *screening rutera* i *bastion hosta* nalazi demilitarizirana zona.
- Razina sigurnosti povećana je dodavanjem još jednog unutrašnjeg *screening rutera*. Princip rada temelji se na tome da unutrašnji i vanjski usmjerivač komuniciraju preko *bastion hosta*, nikad izravno.

4. MIKROTIK ROUTEROS

MikroTik RouterOS poznatiji je kao operacijski sustav MikroTik RouterBOARD hardvera. Operacijski sustav RouterOS je glavni proizvod kompanije MikroTik [12]. Baziran je na Linux v2.6 kernelu, te u skladu s tim podržava sve hardverske komponente koje podržavaju te verzije kernela. Njegova glavna značajka je da može biti instaliran i na računalu kao usmjerivač s odgovarajućim značajkama usmjeravanja, vatrozida, bežične pristupne točke, virtualne privatne mreže, upravljanje propusnim opsegom,*hotspot gateway*-om i slično. Mogućnosti koje će imati RouterOS ovise o instaliranim paketima koji se mogu dodavati i uklanjati ovisno o potrebama. Flash memorija služi za pohranjivanje paketa prilikom instaliranja. Nakon pohranjivanja paketa, potrebno je resetirati uređaj kako bi operacijski sustav mogao provjeravati jesu li dodani novi paketi i instalirati ih. Pakete je jednostavno i ukloniti što je vrlo važno s obzirom da RouterOS pruža bezbroj mogućnosti.

4.1. Konfiguracija

RouterOS podržava razne metode konfiguracije: lokalni pristup s tipkovnicom i monitorom, Telnet i siguran pristup SSH preko mreža, prilagođeni GUI konfiguracijski uređaj koji se zove *Winbox*, te API sučelje za programiranje za izgradnju vlastite kontrole prijave [12]. U slučaju da ne postoji lokalni pristup i imamo problem s IP komunikacijskom razinom, RouterOS također podržava MAC razinu. MikroTik RouterOS postavljen je između mrežne kompanije i javne mreže te uspješno štiti računala od zlonamjernih aktivnosti. RouterOS ima snažno i ujedno jednostavno konfiguracijsko sučelje.

- Winbox GUI preko IP i MAC
- CLI s Telnetom, SSH, Lokalnim konzolama i Serijskim konzolama
- API za programiranje vlastitih alata
- Web sučelje

4.2. Općenita pravila filtriranja MikroTikom

Mrežni vatrozidi čuvaju osjetljive pakete unutar mreže od prijetnji koje se nalaze izvan mreže. Prilikom spajanja različitih mreža uvijek postoji opasnost od napada izvana. Napadi mogu uzrokovati krađu osobnih podataka, promjenu ili uništenje bitnih podataka ili uništenje *hard* diska [15]. Vatrozidi se koriste kako bi smanjili navedene rizike prilikom spajanja različitih mreža. Međutim ključno rješenje je ispravno konfiguriranje vatrozida.

MikroTik RouterOS ima bitne značajke vezane uz provedbu vatrozida [13]:

- *Stateful* pregled paketa
- *Layer-7protocol detection*
- *Peer- to- peer* filtriranje protokola
- Klasifikacija prometa pri kojoj se razmatra:
    - Izvorišna MAC adresa
    - IP adresa i tipovi adresa
    - Portovi
    - IP protokoli
    - Opcije protokola
    - DSCP bajtovi
    - Sadržaj paketa
    - Veličini paketa
    - Redoslijed paketa
    - Vrijeme dolaska paketa

Vatrozid djeluje prema određenim pravilima. Pravila odlučuju hoće li usmjerivač prihvatiti određene IP pakete i što će s njima učiniti. Pravila su organizirana u lance za bolje upravljanje za obradu paketa koji izlaze iz usmjerivača i napuštaju ga kroz jedno od sučelja.. Lanci su ulaz (eng. *Input*) , proslijeđivanje (eng. *forward*) i izlaz (eng.*output*) . Odgovorni su za sav promet koji ide od, kroz i na usmjerivač. Novi lanci se mogu i dodavati ovisno o potrebama. *Input,* odnosno ulaz se koristi za obradu paketa koji ulaze u usmjerivač preko jednog od sučelja s odredišnom IP adresom koja je jedna od adresa usmjerivača. *F*orward se koristi za obradu paketa koji prolaze kroz usmjerivač, a *output* odnosno izlaz se koristi za obradu podataka koji idu na izlaz usmjerivača.

4.3. Struktura Firewall Filtera

Firewall filter je alat koji služi za filtriranje paketa čime pruža sigurnosne funkcije kojima se upravlja tokom podataka u iz i kroz usmjerivač [13]. *Firewall filter* se sastoji iz pravila IF <*condition*>THEN < ac*tion*> . Prilikom obrade podataka ovi filteri obrađuju pakete redom kroz pravila kako su navedena. Ukoliko paket odgovara određenim pravilima izvršavaju se određene akcije na ta pravila, inače paket prelazi na iduće pravilo. *Firewall filter* pravila su organizirana u određene lance, vrste lanaca su:

1. ulaz (eng. *input*) – obrađeni paketi se šalju na usmjerivač
2. izlaz (eng. *output)* – obrađeni paketi se šalju preko usmjerivač
3. naprijed (eng. *forward*) – obrađeni paketi se šalju kroz usmjerivač

Lanci se koriste u svrhu smanjenja procječnog broja pravila kroz koja paketi prolaze, kako bi vatrozid bio brži te kako bi se lakše upravljalo strukturom vatrozida.

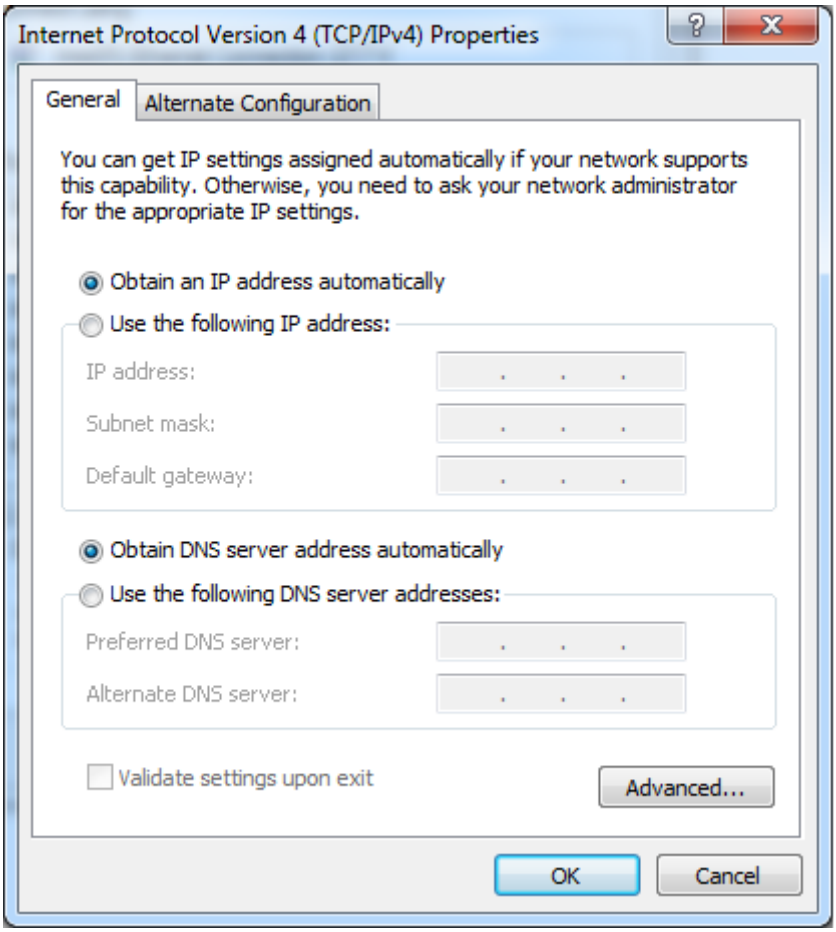
Akcije [13]:

- *Accept* – paket se prihvaća bez poduzimanja bilo kakvih akcija, paket je prolazi i niti jejdno pravilo se na njemu više ne primjenjuje
- *Add-dst-to-address-list* - dodaje odredišnu adresu IP paketa na popis adresa određen address list parametrom
- *Add-src-to-address-list* - dodaje izvorišnu adresu IP paketa na popis određen address list parametrom
- *Drop* - ispušta pakete
- *Jump* - predstavlja skok na lancu određen vrijednošću jump- target parametra
- *Log* - bilo koje slaganje s ovom akcijom dodaje poruku sistemskom logu
- Pas*sthrough* - ignorira ovo pravilo i prelazi na sljedeće
- *Reject* - odbacuje se paket i šalje ICMP reject poruku
- *Return* - ponovno se prolazi kroz kontrolu u lancu
- *Tarpit* - hvata i čuva dolazne TCP veze

5. FILTRIRANJE PAKETA PREMA IP ADRESAMA,PORTOVIMA I PROTOKOLIMA

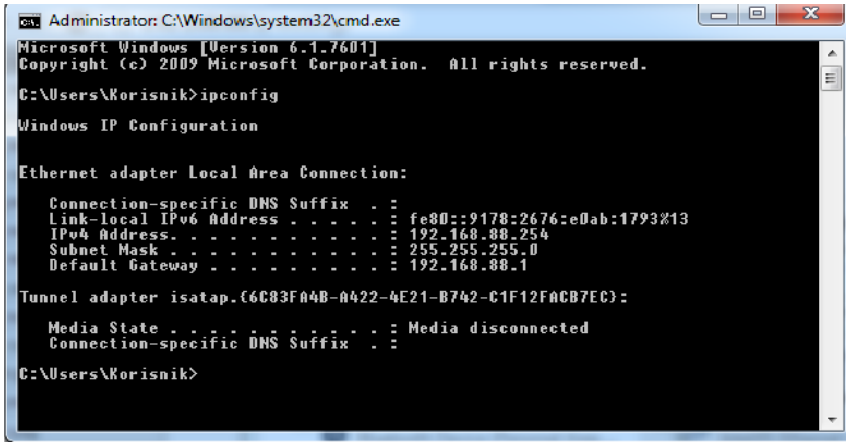
5.1. Blokiranje IP adrese pomoću MikroTika

U prvom koraku potrebno je isključiti vatrozid na računalu ukoliko je pokrenut. Zatim je potrebno deaktivirati sve mrežne konekcije na računalima osim lokalne mreže. U idućem koraku postavlja se IP adresa računala, što je učinjeno automatskim odabirom kako je prikazano na slici 7.1.. Postavljanjem IP adrese pristupa se MikroTik Routeru.



Slika 7.1. Automatski odabir IP adrese

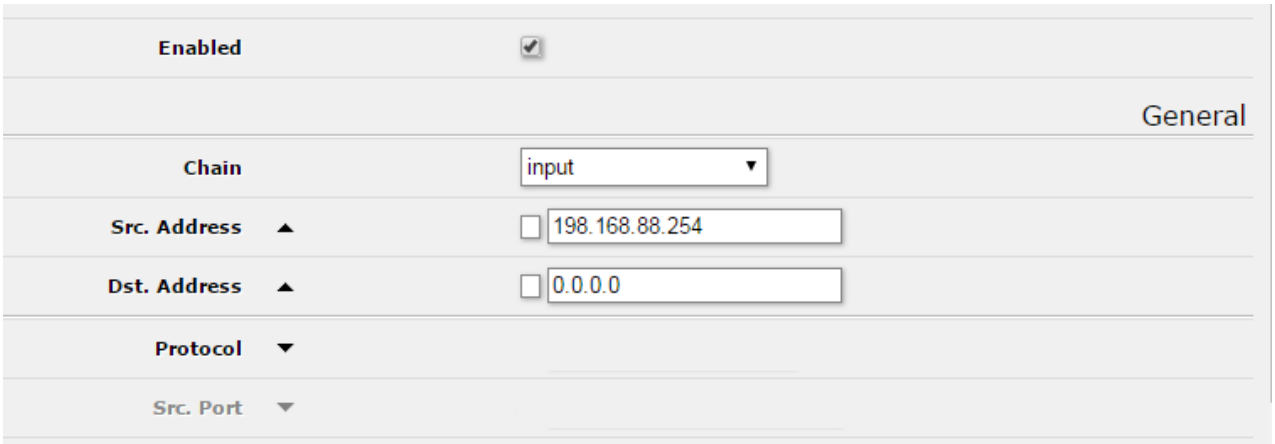
Također je potrebno provjeriti postoji li konekcija između računala i usmjerivača upisivanjem naredbe *ping* na otvorenoj konzoli računala. Upisivanjem naredbe *ping* uviđamo da postoji konekcija između računala i usmjerivača što je vidljivo na slici 7.2..



Slika 7.2. Konekcija računala i usmjerivača

Zatim se otvara internetski preglednik te pristupamo konfiguraciji usmjerivača.

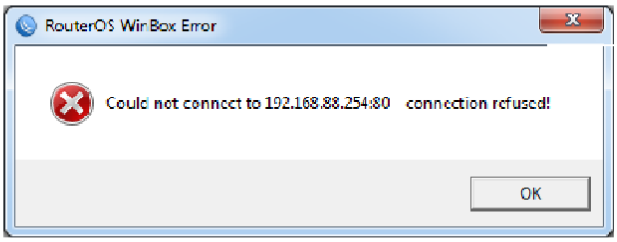
Svrha ovog zadatka je blokirati vlastitu IP adresu, te se započinje postavljanje pravila. U izborniku *Firewall Filter Rules* biramo određene akcije. Lanac koji biramo je *input*, što podrazumijeva da će se obrađivati podatci koji ulaze na usmjerivač preko jednog od sučelja s odredišnom IP adresom koja je adresa usmjerivača, također unosimo adresu koju želimo blokirati dodavajući izvorišnu IP adresu, te biramo akciju *drop* što podrazumijeva ispuštanje paketa prikazano na slici 7.4... Ovom konfiguracijom smo podesili ispuštanje paketa koji ulaze na usmjerivač pod izvorišnom adresom samog usmjerivača. Odabir odgovarajućeg lanca i adrese vidljiv je na slici 7.3.



Slika 7.3. Odabir izvorišne adrese

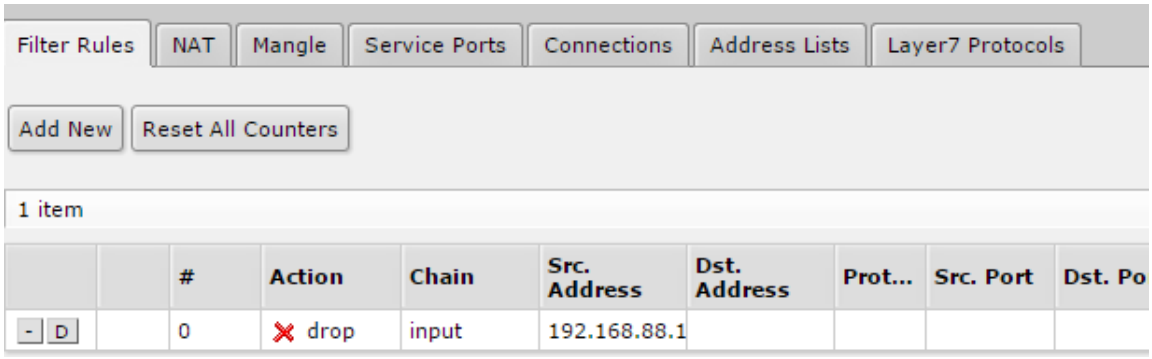
Slika 7.4. Ispuštanje paketa

Nakon pravila filtriranja korištenjem izbornika *Mikrotik WinBox Loader* provjerava se može li se odgovarajućom adresom pristupiti MikroTik usmjerivaču, te se uviđa da nije moguće pristupiti MikroTiku adresom koja je prethodno blokirana, što je bila svrha zadatka. Onemogućen pristup usmjerivaču prikazan je na slici 7.5.



Slika 7.5. Onemogućena konekcija računala i MikroTik usmjerivača

Promjenom IP adrese na način koji je prethodno opisan prilikom postavljanja prve IP adrese, ponovno je moguće pristupiti MikroTik Routeru. Svrha zadatka je ovime ispunjena.



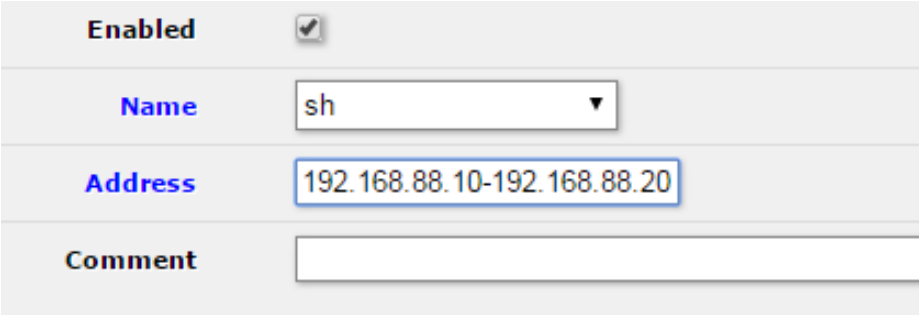
Slika 7.6. Pristup MikroTik usmjerivaču

5.2. Filtriranje paketa prema opsegu IP adresa

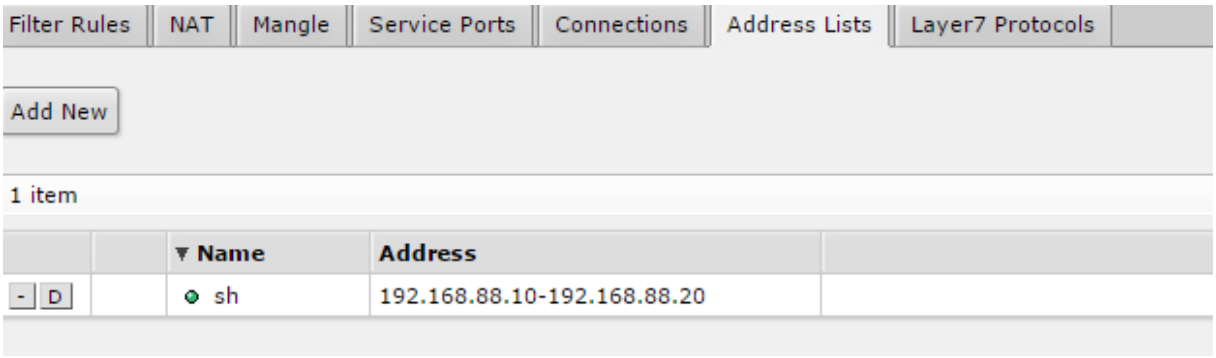
U ovom praktičnom primjeru promet se filtrira prema IP adresama, portovima i protokolima [11]. Nakon postavljanja IP adrese računalu i nakon pristupa MikroTik usmjerivaču promet filtriramo koristeći izbornik *Firewall Filter Rules*.

U prvom koraku je potrebno kreirati listu adresa pod imenom sh u kojoj se nalazi određeni raspon IP adresa koje će imati pristup MikroTik usmjerivaču.

Koristeći izbornik *New Firewall Address List* dodajemo ime listi adresa i raspon što je vidljivo na slici 7.7. . Prema pravilima, pristup usmjerivaču dopušta se isključivo IP adresama koje se nalaze u određenom rasponu 192.168.88.10 – 192.168.88.20 koje se nalaze u kreiranoj listi pod imenom *sh* što je prikazano na slici 7.8..

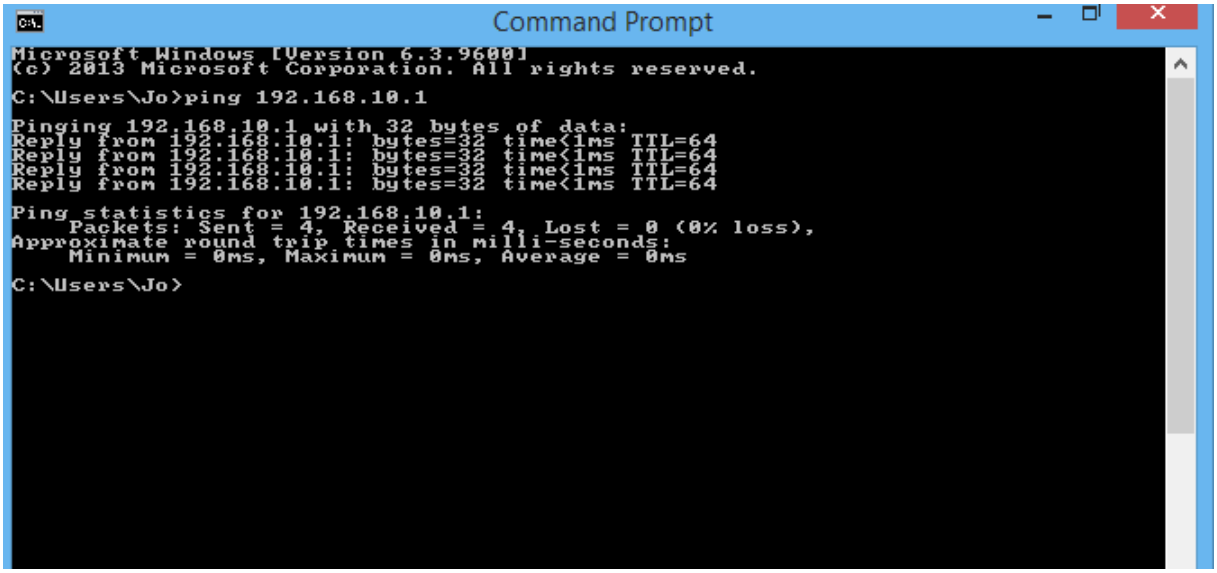


Slika 7.7. Odabir imena i raspona liste adresa



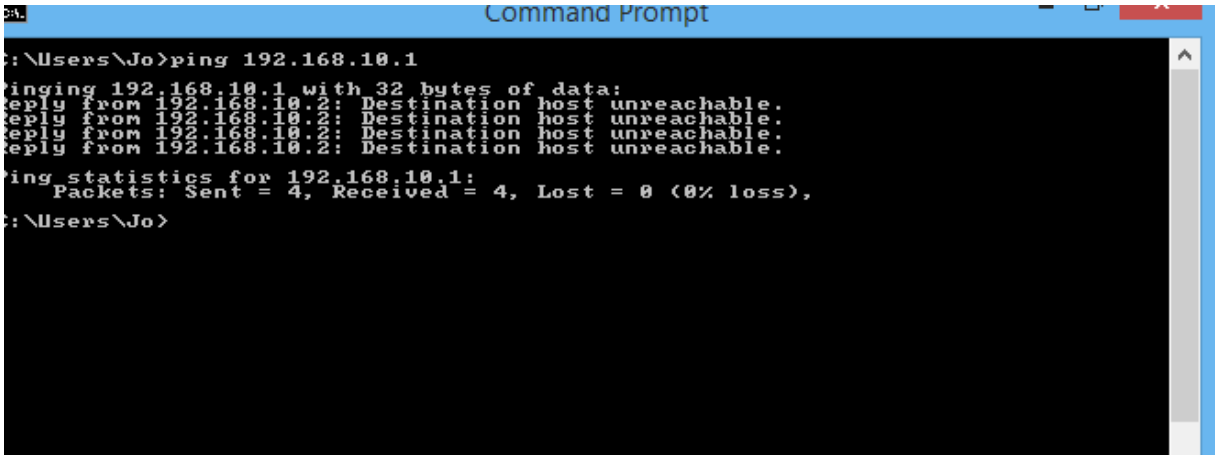
Slika 7.8. Kreirana lista adresa sh

Nakon definiranja raspona IP adresa koji može pristupiti usmjerivaču provjereno je je li konfiguracija uistinu uspjela. U izborniku *Command Prompt* upisivanjem naredbe *ping* i IP adrese usmjerivača koja je u zadanom rasponu utvrđeno je da je moguć pristup MikroTik usmjerivaču što je vidljivo na slici 7.9.



Slika 7.9. Pristup MikroTiku IP adresom 192.168.10.15.

Zatim upisivanjem u izborniku *Command Prompt* naredbe *ping* i IP adrese usmjerivača koja se nalazi izvan zadanog raspona utvrđeno je da pristup MikroTiku nije moguć, što je vidljivo na slici 7.10. te je konfiguracijom i postavljeno.

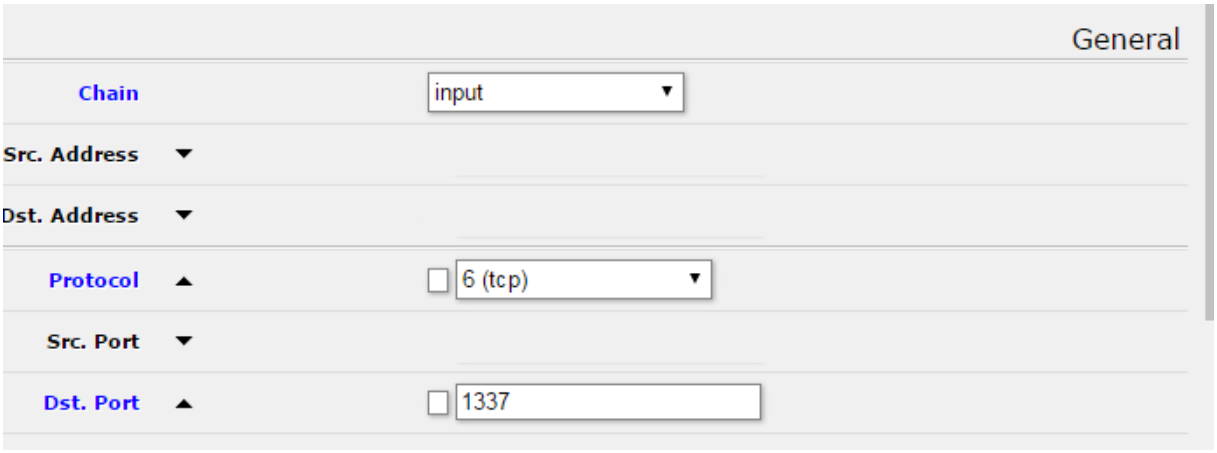


Slika 7.10. Onemogućen pristup IP adresom 192.168.10.2.

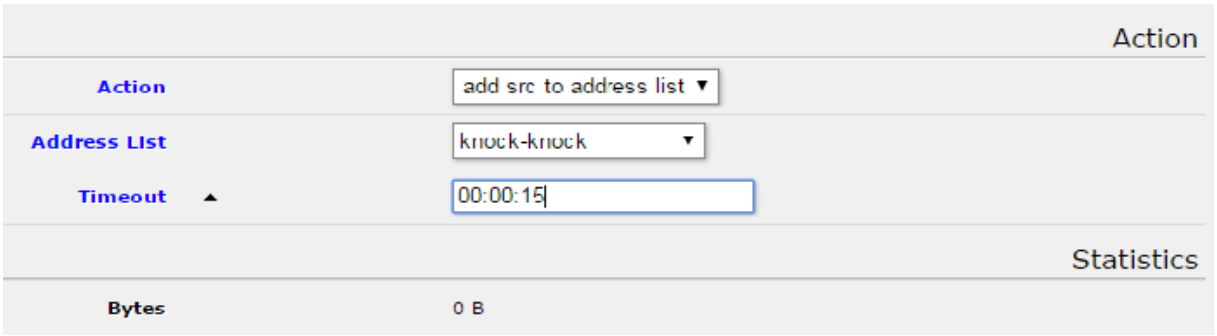
5.3. Filtriranje paketa prema portovima i protokolima

Koristeći izbornik *New Firewall Rule* zadajemo određeni protokol i broj porta, odnosno blokira se sav promet paketa osim onog na portu 1337, lanac koji odabiremo je *input*

što podrazumijeva obradu podataka koji se šalju na usmjerivač, biramo određeni protokol birajući njegovo ime i broj, te port na koji je predodređeno slanje paketa, u ovom slučaju je to port 1337 [11]. Konfiguracija je vidljiva na slikama 7.11. i 7.12.. U izborniku *action* bira se da se svi paketi bilježe samo s određene izvorišne adrese. Izbornik *timeout* određuje vremenski interval u kojemu se mjeri brzina paketa.

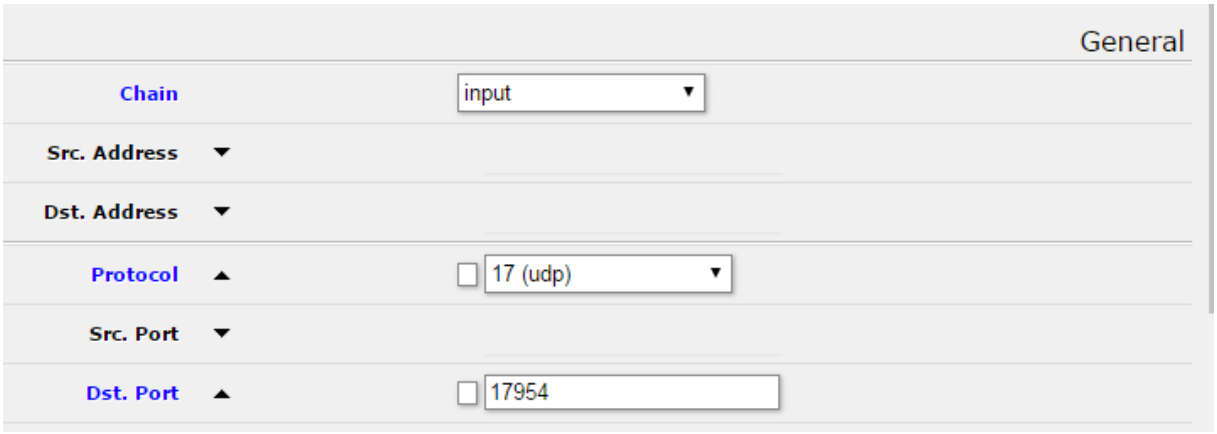


Slika 7.11. Odabir protokola i porta

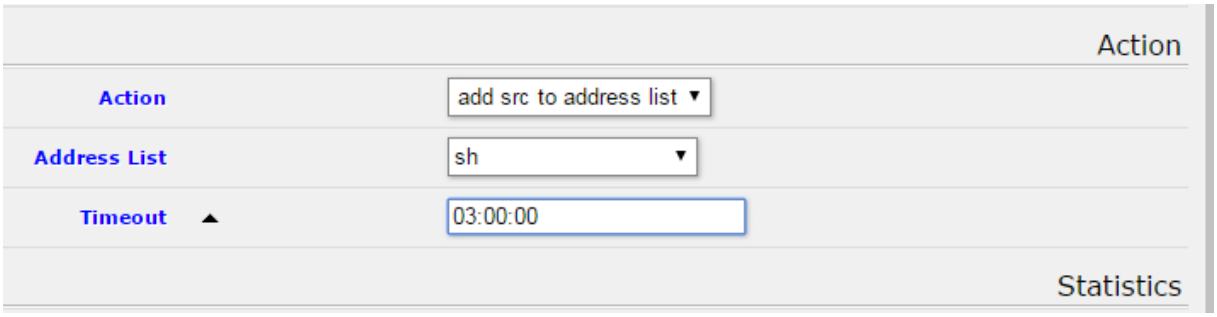


Slika 7.12. Odabir akcije, liste adresa i vremenskog intervala

U drugom pravilu vatrozida također zadajemo određeni protokol i port, lanac koji obrađujemo je također *input*, protokol se određuje izborom imena i broja te se blokira sav promet paketa osim onog koji predviđa slanje paketa na portu 17954. Također zadajemo izvorišnu adresu paketa, te biramo vremenski interval u kojemu se mjeri brzina paketa. Odabir pravila vidljiv je na slikama 7.13. i 7.14.

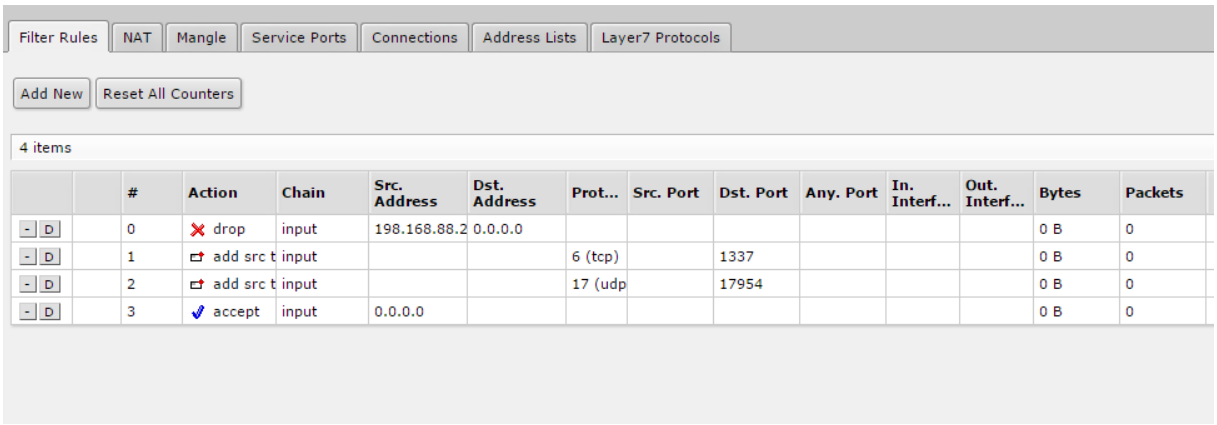


Slika 7.13. Odabir protocola i porta



Slika 7.14. Odabir akcije, liste adresa i vremenskog intervala

U trećem koraku dopuštamo jedino listi adresa *sh* pristup usmjerivaču, te u četvrtom koraku onemogućavamo pristup svemu što nije u sklopu zadanog, te dolazimo do konfiguracije u kojoj je navedeno sve prethodno konfigurirano što je vidljivo na slici 7.15..



Slika 7.15. Konfiguracija vatrozida

6. ZAKLJUČAK

Problemi sigurnosti i privatnosti u radu su najveći problem pri korištenju Interneta . Iz dana u dan sve je veći broj korisnika Interneta, te se također povećava moć njegove zlouporabe. Problemi koji se mogu pojaviti pri zlouporabi Interneta su raznovrsni: od bezazlenih kao što su slanje velikog broja reklamnim materijala, do neovlaštenog pristupa podacima sa računala, krađe informacija, pa do slanja virusa koji mogu nanijeti izuzetnu štetu . Sigurnost računala pri korištenju interneta je od velike važnosti, kako za pojedinca koji koristi Internet tako i za velike organizacije. Kako bi se spriječila zlouporaba povjerljivih podataka jedno od rješenja je korištenje vatrozida. Vatrozid je od velike koristi ukoliko se na ispravan način konfigurira u skladu s potrebama korisnika. Glavna uloga vatrozida je analiza i filtriranje paketa koji su u komunikaciji između dvaju ili više čvorova u mreži.

MikroTik RouterOS omogućava konfiguraciju inteligentnog vatrozida, što podrazumijeva provedbu inteligentne analize toka podataka, te evidentiranje stanja mrežnih konekcija koje prolaze kroz njega. Pomoću MikroTik usmjerivača moguće je podesiti razna pravila filtriranja paketa, što je od izuzetne važnosti za sigurnost prometa paketa. MikroTik RouterOS je operacijski sustav koji je izuzetno pogodan jer bilo koje osobno računalo može pretvoriti u softwarski usmjerivač koji ima osnovne pogodnosti za rad svakog usmjerivača.

Načinjena je konfiguracija vatrozida pri čemu se filtriranje paketa provodilo prema IP adresama, rasponu IP adresa, protokolima i portovima. Nakon ispravne konfiguracije vatrozida, svaki puta kada je računalo zaprimilo neovlašteni zahtjev, vatrozid je blokirao spajanje čime je omogućena zaštita računala te time i korisnika.

7. LITERATURA

[1] Belošević, Anđelko. *Zaštita računalnih sustava vatrozidom*, pristup stranici:

15.travnja2016.http://www.scribd.com/doc/76941838/3/Povijest-vatrozida#page=6.

[2] Conry-Murray, Andrew; Weafer, Vincent, 2005. *Sigurni na Internetu*, Tiskara Zelina.

[3] Gledec, Gordan; Mikuc, Miljenko; Kos, Mladen, 2002. Sigurnost u privatnim komunikacijskim mrežama, Zagreb: FER. Pristup stranici: 25.svibnja 2016. https://www.fer.unizg.hr/_download/repository/Sigurnost_u_privatnim_komunikacijskim_mrezama.pdf

[4] Franjić, Marko, 1999. *Digitalna ekonomija*, Digimark d.o.o, Zagreb.

[5] Kiš, Miroslav, 2002. *Informatički rječnik*, drugo izdanje, naklada Ljevak, Zagreb.

[6] Kurose, James F.; Ross, Keith W., 2001. *Computer Networking: A Top-Down Approach Featuring the Internet*, Addison Weslez.

[7] Pohlmann, Norbert, 2003. *Firewall-Systeme*, Media-Print, Paderborn. Pristup stranici: 21. svibnja 2016.http://norbert-pohlmann.com/app/uploads/2015/08/Firewall-Systeme.pdf.

[8] Stepken, Guido, 1999. *Firewall Handbuch für LINUX 2.0 und 2.2*.

Pristup stranici: 20.svibnja 2016. http://ip-klaeden.selfhost.eu/webseiten/linux-firewall-handbuch/FirewalhandbuchLINUX.pdf.

[9] Tanenbaum, Andrew S., 1996. *Computer Networks*, Third edition, Prentice-Hall, Inc.

[10] Žagar, Drago; Grgić, Krešimir. *Komunikacijske mreže: Sigurnost u računalnim mrežama*. Pristup stranici Loomen: 20. svibnja 2016.

[11] *Mikrotik Firewall: Securing Your Router With Port Knocking*, pristup stranici:10. lipnja 2016. http://mum.mikrotik.com/presentations/ID08/portknock.pdf.

[12] *RouterOS*, pristup stranici: 21. svibnja 2016. http://www.mikrotik-routeros.net/routeros.aspx

[13] *Firewall Filter*, pristup stranici: 21. svibnja 2016. http://www.mikrotik.com/testdocs/ros/3.0/qos/filter.php

[14] *Internet*, pristup stranici: 20. svibnja 2016. http://hr.wikipedia.org/wiki/Internet.

[15] *Krađa identiteta*, pristup stranici: 20. svibnja 2016. http://hr.wikipedia.org/wiki/Hakeri.

[16] *Sigurnost i zaštita na internetu*, pristup stranici: 20. svibnja 2016. http://sigurnost.tvz.hr/.

Slika [2.1.] http://sigurnost.zemris.fer.hr/ns/firewall/2006_zeman/.

Slika [2.2.] http://sigurnost.zemris.fer.hr/ns/firewall/2006_zeman/.

Slika [2.3.] http://sigurnost.zemris.fer.hr/ns/firewall/2006_zeman/.

Slika [3.1.] https://en.wikipedia.org/wiki/Firewall_(computing)

SAŽETAK

S obzirom da je u današnje vrijeme Internet od izuzetne važnosti, te je neizostavan segment bilo koje društvene grane izuzetno je bitno posvetiti se njegovoj sigurnosti. Razno razne su prijetnje koje se nalaze na internetu, te ih je sve više. Kako bi Internet bio što sigurniji od izuzetne važnosti je ograničiti pristup pojedinih korisnika određenim dijelovima mreže. Svi korisnici u LAN-u ne moraju imati ista prava pristupa Internet mreži. Jedan od načina kontroliranja prava pristupa je korištenje vatrozida. Mogućnosti vatrozida predstavljene su pomoću posebnog usmjerivača, odnosno MikroTik RouteraOS.Svrha ovog rada bila je opisati način sigurnosti koji obuhvaća filtriranje paketa. Pomoću usmjerivača MikroTik RouteraOS provedeno je filtriranje paketa prema IP adresama, portovima i protokolima. Uz pomoć provedenih pravila, pristup mreži nije omogućen svim korisnicima što je svrha zaštitnog mehanizma.

Ključne riječi: prijetnje na internetu, korisnici u LAN-u, mogućnosti vatrozida, MikroTik RouterOS, filtriranje paketa, zaštitan mehanizam.

ABSTRACT

Given that nowadays the Internet is of the utmost importance and it is an integral part of any social branch, it is extremely important to dedicate ourselves to its security. There are various kinds of threats found on the Internet, and every day there can be found even more of these. In order to make the Internet as secure as possible, it is vital to limit some users the access to certain parts of the network. Not all LAN users have to have the same access rights to the Internet network. One way of controlling these access rights is using the firewall. Its possibilities are presented using special router, namely MikroTikRouterOS. The concept of this work is to describe manner of security that packet filtering includes. Packet filtering categorised by IP addresses, ports and protocols is here performed using the router MikroTikRouterOS. With the help of the implemented rights, the network access is not enabled to all users which is the purpose of a defence mechanism.

Keywords: threats on the Internet, LAN users, firewall possibilities, MikroTik RouterOS, packet filtering, defence mechanism.

ŽIVOTOPIS

JOSIPA OPAČAK

Rođena 12.07.1994. u Stuttgartu, Njemačka. Osnovnu školu „Bogoslav Šulek“ završila je s odličnim uspjehom u Slavonskom Brodu gdje 2009. godine upisuje opću gimnaziju „Matija Mesić“ koju završava 2013. godine, također s odličnim uspjehom.

2013. godine upisuje preddiplomski sveučilišni studij elektrotehnike na Elektrotehničkom fakultetu u Osijeku, te nakon prve godine opredjeljuje se za smjer „Komunikacije i informatika“ .

Članica je Studentskog zbora od 2015. godine te sudjeluje u različitim fakultetskim projektima .

U slobodno vrijeme aktivno se bavi sportom, predstavlja fakultet u rukometu te ekipno osvaja prve medalje u povijesti ženskog sporta na fakultetu. Također je zaposlena preko Studentskog servisa.

Tečno govori engleski jezik, njemački jezik te je informatički pismena.

U Osijeku, 27. kolovoza 2016. Josipa Opačak

Potpis: