# Primjena Mikrotik vatrozida u lokalnoj mreži

**Kučenjak, Inoslav**



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

**Sveučilišni studij**

# PRIMJENA MIKROTIK VATROZIDA U LOKALNOJ MREŽI

**Završni rad**

**Inoslav Kučenjak**

**Osijek, 2022.**

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

**Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju**

**Osijek, 18.09.2022.**

**Odboru za završne i diplomske ispite**

# Prijedlog ocjene završnog rada na preddiplomskom sveučilišnom studiju

| | |
|---|---|
| **Ime i prezime Pristupnika:** | Inoslav Kučenjak |
| **Studij, smjer:** | Preddiplomski sveučilišni studij Računarstvo |
| **Mat. br. Pristupnika, godina upisa:** | R 4374, 22.07.2019. |
| **OIB Pristupnika:** | 67462946442 |
| **Mentor:** | Izv. prof. dr. sc. Krešimir Grgić |
| **Sumentor:** | Ana Pejković, mag. ing. el. |
| **Sumentor iz tvrtke:** | |
| **Naslov završnog rada:** | Primjena Mikrotik vatrozida u lokalnoj mreži |
| **Znanstvena grana rada:** | **Telekomunikacije i informatika (zn. polje elektrotehnika)** |
| **Zadatak završnog rad:** | Vatrozid predstavlja mrežni sigurnosni uređaj koji nadzire dolazni i odlazni mrežni promet, te odlučuje hoće li propustiti ili blokirati određeni promet na temelju definiranog skupa sigurnosnih pravila. U radu je potrebno analizirati mogućnosti implementacije vatrozida u lokalnu mrežu. Potrebno je implementirati filtriranje mrežnog prometa pomoću Mikrotik-ovog usmjerivača temeljenog na RouterOS operarivnom sustavu, koji će implementirati značajke vatrozida i analizu toka podataka. Sumentor s FERIT-a: Ana Pejković |
| **Prijedlog ocjene završnog rada:** | Izvrstan (5) |
| **Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:** | Primjena znanja stečenih na fakultetu: 3 bod/boda<br>Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda<br>Jasnoća pismenog izražavanja: 2 bod/boda<br>Razina samostalnosti: 3 razina |
| **Datum prijedloga ocjene od strane mentora:** | 18.09.2022. |
| **Datum potvrde ocjene od strane Odbora:** | |

| | |
|---|---|
| Potvrda mentora o predaji konačne verzije rada: | *Mentor elektronički potpisao predaju konačne verzije.* |
| | Datum: |

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

# IZJAVA O ORIGINALNOSTI RADA

**Osijek, 19.09.2022.**

| | |
|---|---|
| **Ime i prezime studenta:** | Inoslav Kučenjak |
| **Studij**: | Preddiplomski sveučilišni studij Računarstvo |
| **Mat. br. studenta, godina upisa:** | R 4374, 22.07.2019. |
| **Turnitin podudaranje [%]:** | 8 |

Ovom izjavom izjavljujem da je rad pod nazivom**: Primjena Mikrotik vatrozida u lokalnoj mreži**

izrađen pod vodstvom mentora Izv. prof. dr. sc. Krešimir Grgić

i sumentora Ana Pejković, mag. ing. el.

moj vlastiti 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, a što je izričito navedeno u radu.

Potpis studenta:

# SADRŽAJ

**1. UVOD ..... 1**

**1.1. Zadatak završnog rada ..... 1**

**2. VATROZID ..... 2**

**2.1. Zašto koristiti vatrozid? ..... 3**

**2.2. Vrste vatrozida ..... 5**

**2.3. Arhitektura vatrozida ..... 8**

**2.4. Problemi i prijetnje vatrozida ..... 11**

**3. MIKROTIK ROUTEROS ..... 15**

**3.1. Konfiguracija RouterOS-a ..... 15**

**4. POSTAVLJANJE VATROZIDA ..... 16**

**4.1. Priprema računala prije spajanja usmjerivača ..... 16**

**4.2. Spajanje usmjerivača na računalo ..... 17**

**5. Filtriranje prometa vatrozida prema adresnoj listi IP adresa, protokolima i portovima. ..... 20**

**5.1. Postavljanje adresne liste IP adresa ..... 20**

**5.2. Blokiranje pristupa klijentima koji se ne nalaze na ranije postavljenoj listi IP adresa .... 22**

**5.3. Filtriranje prometa vatrozida prema portovima i protokolima ..... 23**

5.3.1. Treće pravilo ..... 23

5.3.2. Četvrto pravilo ..... 24

5.3.3. Peto pravilo ..... 25

**5.4. Testiranje ispravnosti postavljenih pravila ..... 26**

**6. ZAKLJUČAK ..... 28**

**LITERATURA ..... 29**

**SAŽETAK ..... 31**

**ABSTRACT ..... 31**

# 1. UVOD

S obzirom da je upotreba Interneta sve češća i budući da kao zajednica postajemo sve ovisniji o njemu, također smo izloženi i raznim opasnostima koje Internet nudi. Jedan od načina zaštite od opasnosti (kao što su gubitak podataka ili neovlaštena izmjena podataka) Interneta je uporabom vatrozida (eng. *firewall*). Vatrozid se koristi nalazi kao veza između lokalnih mreža i vanjskih (neprovjerenih) mreža, a služi za zaštitu mreže računala. Vatrozid se može nalaziti na ulazu lokalne mreže, na izlazu lokalne mreže ili na samom routeru [1]. Vatrozid provjerava sve mrežne pakete po određenom kriteriju i pravilu i na taj način filtrira promet koji se odvija između računalnih mreža. Najčešće se radi o javnoj i privatnoj mreži, ako paketi zadovoljavaju pravila ili kriterije, ti paketi su propušteni. U suprotnom paketi su blokirani i odbijeni. S obzirom da se prilikom korištenja Interneta pojavljuje potreba za sigurnosnim spajanjem na udaljeni terminal usluge, prijenos datoteka (eng. *File Transfer Protocol,* FTP), Usenet (eng. *Network News Transfer* Protocol, NNTP) i uporaba elektroničke pošte (eng. *Simple Mail Transfer Protocol,* SMTP), te se usluge dodaju na listu zahtjeva pristupa. No u slučaju dolaska do promjene, te ako se izrazi potreba za omogućenjem uporabe novog servisa ili usluge, tada je računalna mreža izložena novim načinima napada, te je potrebno omogućiti nove načine zaštite.

## 1.1. Zadatak završnog rada

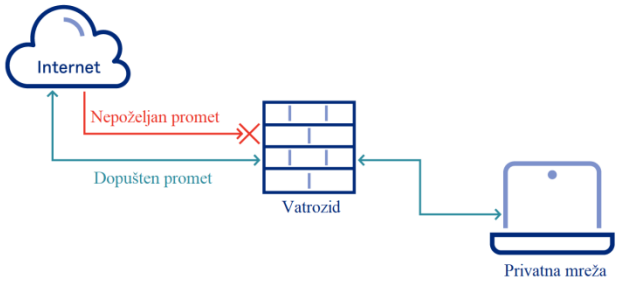
Vatrozid predstavlja mrežni sigurnosni uređaj koji nadzire dolazni i odlazni mrežni promet, te odlučuje hoće li propustiti ili blokirati određeni promet na temelju definiranog skupa sigurnosnih pravila. U radu je potrebno analizirati mogućnosti implementacije vatrozida u lokalnu mrežu. Potrebno je implementirati filtriranje mrežnog prometa pomoću Mikrotik-ovog usmjerivača temeljenog na RouterOS operarivnom sustavu, koji će implementirati značajke vatrozida i analizu toka podataka.

# 2. VATROZID

Vatrozid (*eng. Firewall*) je sustav ili grupa sustava koji provodi kontrolu pristupa između dvije mreže [2]. Stvarni načini na koji se takva kontrola pristupa postiže znatno se razlikuju, no u principu na vatrozid se može gledati kao mehanizam od dva glavna dijela: jedan koji postoji kako bi blokirao promet, te drugi koji propušta promet. Najbitnija karakteristika vatrozida je mogućnost provođenja politike kontrole pristupa.

Ako korisnik nema dobru ideju o tome kakav pristup želi omogućiti ili blokirati, ili ako jednostavno želi dopustiti nekoj osobi ili nekom proizvodu da konfigurira vatrozid na način na koji on ili oni smatraju da bi trebalo, tada radi kontrolu pristupa za cijelu organizaciju.

Drugim riječima vatrozid je mrežna zaštita koja služi kao prepreka između dvaju ili više mrežnih segmenata kao što je prikazano na slici 2.1. Vatrozid je sustav (koji se sastoji od jedne ili više komponenti) koji nudi mogućnost kontrole pristupa između lokalne mreže organizacije i mreže kojom je ta organizacija povezana. Vatrozid također ima mogućnost provjere ili obavijesti (alarma) koja omogućuje vođenje zapisa svih pokušaja pristupa na lokalnu mrežu i sa nje, te pravovremeno obavještavanje o događajima koje korisnik smatra bitnima (provala mreže, napad na mrežu i sl.).




**Slika 2.1: Vatrozid**

Također je potrebno znati da vatrozid nije samo usmjerivač (*eng. Router*), *host system* ili kolekcija sustava koji pružaju mrežnu sigurnost. Vatrozid je pristup sigurnosti mreže; pomaže pri implementaciji veće politike kontrole pristupa koja definira usluge i pristupe koji su dopušteni, te je implementacija unaprijed definirane politike na mrežnoj razini. Glavna zadaća vatrozida je kontroliranje pristupa na zaštićenu mrežu i izvan nje. Implementira politiku mrežnog propusta, tako da je sva komunikacija „prisiljena“ proći kroz vatrozid, gdje je provjerena i uspoređena s unaprijed definiranim kriterijima i pravilima.

## 2.1. Zašto koristiti vatrozid?

Vatrozid se koristi kako bi spriječili napade na korisnikovu lokalnu mrežu [2]. Takvi napadi najčešće mogu biti počinjeni od tri osnovne grupe:

- Ljudi ili korisnici koji na provaljivanje i napadanje informacijskog sustava neke tvrtke gledaju kao na izazov
- Ljudi ili korisnici koji nisu politički ili socijalno okrenuti nego napad na tvrtku i njezine podatke vide kao priliku za visoko tehnološki vandalizam.
- Ljudi ili korisnici koji rade za suparničke tvrtke ili političku stranku, te napad na tvrtku ili političku stranku vide kao legitimnu stratešku metu.

Kako bi se smanjila opasnost od takvih napada i povećala razina sigurnosti lokalne mreže i/ili Internetske stranice, postoje određene strateške mjere koje su razvijene, te se kontinuirano moraju ažurirati i unaprijeđivati. Sigurnosne strategije koje su važne i koje se koriste za zaštitu podataka i informacija određene tvrtke su:

- *Data integrity*: Sigurnost i potvrda da podatci nisu izmijenjeni
- *Confidentiality*: Privatnost omogućena enkripcijom
- *Authentication*: Provjera inicijatora ugovora
- *Nonrepuditation*: Nepobitan dokaz sudjelovanja
- *Availability*: Osiguranje potražnje usluge

Kako je već ranije navedeno, vatrozid se postavlja na vezu između lokalne mreže i javne mreže na koju je računalo ili organizacija spojeno/spojena. Koristi se radi osobne sigurnosti, to jest kako bi se osigurao prijenos paketa kroz vezu na siguran način. No postoje i druge prednosti uporabe vatrozida, kao što su:

- Zaštita od ranjivih usluga koje se pokreću na serveru koje mogu povećati vjerojatnost napada
- Kontrolirani pristup stranici sustava
- Koncentrirana sigurnost
- Ojačana privatnost
- Bilježenje i statistika korištenja mreže ili zlouporaba mreže
- VPN (*Virtual Private Network*)

- DMZ (*Demilitarized Zone*)

No vatrozid ne može biti korišten kao zaštita protiv napada koji ne prolaze kroz njega. Također vatrozid je beskoristan kada je riječ o izdaji ili prodaji informacija od strane zaposlenika organizacije. Vatrozid je približno beskoristan kao zaštita protiv virusa, jer postoji previše načina kodiranja binarnih podataka i previše arhitektura i različitih virusa, te nije moguće raditi provjeru za sve njih. Drugim riječima zdrav razum korisnika je i dalje najbolja zaštita od virusa i provala u sustav (osim ako je riječ o slanju programa e-poštom koji korisnik slučajno pokrene).

Ovisno o tvrtci i njezinim potrebama postoje i različiti tipovi vatrozida, gdje svaki nudi neku prednost. Tvrtka može inkorporirati sve tipove ili samo one koji su joj potrebni, a tipovi vatrozida su[3]:

- „*Application Layer 7*“: Sortiranje prometa po sadržaju i destinaciji; blokiranje bilo kojeg prometa koji ne odgovara unaprijed definiranim pravilima.
- „*Connection tracking*“: Proučavanje razgovora između dva izvora koristeći znanje o prije korištenoj IP adresi.
- „*Endpoint*“: Uspoređivanje paketa podataka s pravilima koje je korisnik kreirao.
- „*Network address translation (NAT)*“: NAT može sakriti IP adresu pojedinca, time se neovlaštenim osobama onemogućuje razumijevanje rada servera; tehnički nije vatrozid, ali se ponaša kao vatrozid.
- „*Next-generation*“: Uporabom jednog proizvoda omogućuje se spriječavanje provale i analiza prijetnje.
- „*Packet filtering*“: Pravila definiraju koji paketi moraju biti provjereni i što se dogodi ako dođe do podudaranja s određenim pravilom (uljez, odbijanje prihvaćanja paketa, „problem“).
- „*Web application proxy*“: Pravila diktiraju kako promet jedne specifične aplikacije funkcionira.
- „*Stateful inspection*“: Sva aktivnost otvorene veze se nadzire, a pravila za filtriranje diktiraju što se poduzima s informacijama ili paketima.
- „*Unified threat managment*“: Sva aktivnost otvorenih veza se nadzire, te sustav čini čestu provjeru je li došlo do napada.
- „*Virtual*“: Promet koji se odvija između fizičke i virtualne mreže se nadzire.

## 2.2. Vrste vatrozida

Postoje brojne vrste vatrozida, no proizvoljno se može reći da postoji pet ključnih vrsta vatrozida koji koriste različite mehanizme za prepoznavanje i filtriranje zlonamjernog prometa. Budući da svaki vatrozid može biti konfiguriran na različite načine od veće važnosti je čemu određeni vatrozid služi. Dodatno, tvrtkama je možda potrebno više od jednog vatrozida kako bi osigurali svoje vatrozide, a postoje tri različite mogućnosti postavljanja vatrozida koje je potrebno razmotriti [5].

Vrste vatrozida su:

1. Vatrozid za filtriranje paketa
2. *Circuit–level gateway*
3. *Proxy* vatrozid
4. Vatrozid za inspekciju stanja
5. Vatrozid sljedeće generacije (eng. *Next-Generation Firewall,* NGFW)

1. Vatrozid za filtriranje paketa

Vatrozidi za filtriranje paketa rade *online* na spojnim točkama gdje uređaji poput usmjerivača i preklopnika obavljaju svoj posao. Međutim, ti vatrozidi ne usmjeravaju pakete, nego uspoređuju svaki primljeni paket sa skupinom utvrđenih kriterija, kao što su dopuštene IP adrese, vrsta paketa, broj porta i drugi aspekti zaglavlja paketnog protokola. Paketi koji su označeni kao problematični ne prosljeđuju se i stoga prestaju postojati [5].

Prednosti filtriranja paketa vatrozidom

- Jedan uređaj može filtrirati promet za cijelu mrežu
- Iznimno brz i učinkovit u skeniranju prometa
- Niska cijena
- Minimalni učinak na druge resurse, performanse mreže i iskustvo krajnjeg korisnika

Nedostatci filtriranja paketa vatrozidom

- Budući da se filtriranje prometa u potpunosti temelji na informacijama o IP adresi ili portu, filtriranju paketa nedostaje širi kontekst koji informira druge vrste vatrozida
- Ne provjerava nosivost i može se lako krivotvoriti
- Nije idealna opcija za svaku mrežu
- Liste kontrole pristupa mogu biti teške za postavljanje i upravljanje

2. *Circuit-level gateway*

Koristeći još jedan relativno brz način identificiranja zlonamjernog sadržaja, pristupnici na razini kruga nadziru TCP rukovanje i druge poruke pokretanja veze mrežnog protokola diljem mreže dok se uspostavljaju između lokalnih i udaljenih računala kako bi utvrdili je li veza koja se pokreće legitimna (je li udaljeni sustav pouzdan). Međutim, sami ne pregledavaju pakete.

Prednosti *circuit-level gatewayja*

- Obrađuje samo tražene transakcije, sav ostali promet se odbija
- Jednostavan za postavljanje i upravljanje
- Niska cijena i minimalan utjecaj na iskustvo krajnjeg korisnika

Nedostatci *circuit-level gatewayja*

- Ako se ne koristi u kombinaciji s drugom sigurnosnom tehnologijom, c*ircuit-level gateway* ne nudi zaštitu od povrede sigurnosti podataka s uređaja unutar vatrozida
- Nema praćenja aplikacijskog sloja
- Zahtijeva stalna ažuriranja kako bi pravila bila aktualna

3. *Proxy* vatrozid

*Proxy* vatrozid - funkcionira kao jedina ulazna i izlazna točka s mreže. *Proxy* vatrozid filtrira pakete, ne samo prema usluzi za koju je namijenjen (kako je određeno odredišnim portom), već i prema drugim karakteristikama, kao što je niz HTTP (eng. *Hypertext Transfer Protocol*) zahtjeva.

Prednosti *proxy* vatrozida

- Ispituje svu komunikaciju između vanjskih izvora i uređaja iza vatrozida, provjeravajući ne samo informacije o adresi, portu i TCP zaglavlju, već i sam sadržaj prije nego što dopusti da bilo kakav promet prođe kroz *proxy*
- Pruža precizne sigurnosne kontrole koje mogu, na primjer, dopustiti pristup web stranici, ali ograničiti koje stranice na toj stranici korisnik može otvoriti
- Štiti anonimnost korisnika

Nedostatci *proxy* vatrozida

- Može spriječiti rad mreže
- Skuplji od nekih drugih opcija vatrozida
- Zahtijeva visok stupanj napora kako bi se izvukla maksimalna korist od pristupnika
- Ne radi sa svim mrežnim protokolima

4. Vatrozid za inspekciju stanja

Uređaji svjesni stanja ne samo da ispituju svaki paket, već isto tako prate je li taj paket dio uspostavljenog TCP-a ili druge mrežne veze. To nudi veću sigurnost nego samo filtriranje paketa ili *circuit monitoring*, ali ima veći utjecaj na performanse mreže. Daljnja varijanta inspekcije s praćenjem stanja je višeslojni inspekcijski vatrozid, koji razmatra tijek transakcija u procesu preko višestrukih slojeva protokola sedmoslojnog modela međusobnog povezivanja otvorenih sustava (eng. *Open Systems Interconnection*, OSI).

Prednosti vatrozida za inspekciju stanja

- Nadzire cijeli tijek stanja veze, dok također provjerava IP adrese i korisni sadržaj za temeljitiju sigurnost
- Nudi visok stupanj kontrole nad sadržajem koji se pušta u mrežu ili iz nje
- Ne treba otvarati brojne priključke da bi se omogućio ulaz ili izlaz prometa

Nedostatci vatrozida za inspekciju stanja

- Zahtijeva mnogo resursa i ometa brzinu mrežne komunikacije
- Ne pruža mogućnosti provjere autentičnosti za potvrdu da izvori prometa nisu krivotvoreni

5. Vatrozid sljedeće generacije (eng. *Next-Generation Firewall*, NGFW)

Tipični vatrozid sljedeće generacije kombinira inspekciju paketa s inspekcijom stanja i također uključuje razne vrste duboke inspekcije paketa (eng. *Deep Packet Inspection*, DPI), kao i druge mrežne sigurnosne sustave, kao što su IDS (eng. *Intrusion Detection System*) i IPS (eng. *Intrusion Prevention System*), tj. filtriranje zlonamjernog softvera. Dok inspekcija paketa u tradicionalnim vatrozidima gleda isključivo na zaglavlje protokola paketa, DPI gleda na stvarne podatke koje paket nosi.

Prednosti vatrozida sljedeće generacije

- Kombinira DPI s filtriranjem zlonamjernog softvera i drugim kontrolama za pružanje optimalne razine filtriranja
- Može se automatski ažurirati kako bi se pružio trenutni kontekst

Nedostatci vatrozida sljedeće generacije

- Kako bi izvukle najveću korist, tvrtke moraju integrirati NGFW s drugim sigurnosnim sustavima, što može biti složen proces; skuplji od ostalih vrsta vatrozida

## 2.3. Arhitektura vatrozida

Vatrozidi se mogu konfigurirati u više različitih arhitektura, pružajući različite razine sigurnosti uz različite troškove instalacije i operacija. Tvrtke bi trebale uskladiti svoj profil rizika s vrstom odabrane arhitekture vatrozida [2]. Neke od arhitektura vatrozida su:

- *Multi-homed host*
- Provjereni poslužitelj
- Zaštićena podmreža

*Multi-homed host*

Ova je arhitektura složenija implementacija vatrozida provjerenih poslužitelja. U ovom arhitektonskom pristupu, *bastion* poslužitelj prima dvije NIC (eng. *Network Interface Cards)* u konfiguraciji *bastion* poslužitelja. Jedan od NIC-a je spojen na vanjsku mrežu, a drugi je spojen na internu mrežu čime se pruža dodatni sloj zaštite [6]. (Usmjeravanje pomoću vatrozida obično je onemogućeno za vatrozid s dvostrukom matičnom mrežom tako da se internetski protokol paketi iz jedne mreže ne usmjeravaju izravno s jedne mreže na drugu [2].)

Provjereni poslužitelj

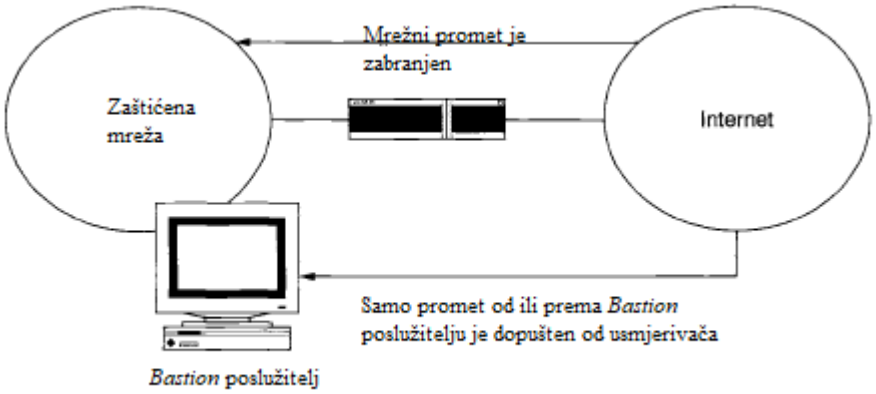
Slika 2.2 prikazuje vatrozid koji kombinira usmjerivač za filtriranje paketa s diskretnim vatrozidom kao što je aplikacijski *proxy* poslužitelj. U ovom pristupu, usmjerivač pregledava paket prije ulaska u internu mrežu i smanjuje promet i opterećenje mreže na internom *proxyju*. Aplikacijski *proxy* provjerava protokol aplikacijskog sloja kao što je HTTP ili HTTPS (eng. *Hypertext Transfer Protocol Secure*) i izvodi *proxy* usluge. Ovaj odvojeni poslužitelj naziva se *bastion* poslužitelj i može biti dobra meta za vanjske napade, stoga ga treba temeljito osigurati. *Bastion* poslužitelj pohranjuje kopije internih dokumenata, što ga čini obećavajućom metom za napadače. *Bastion* poslužitelj također se neformalno naziva i 'žrtveni poslužitelj'.

Prednosti

Ova konfiguracija zahtijeva od napadača 'hakiranje' i ugrožavanje dva odvojena sustava prije pristupa internim podacima. Na taj način *bastion* poslužitelj i usmjerivač štite podatke i imaju učinkovitiju i sigurniju implementaciju [6]. (Ako se treba postaviti pristupnik za filtriranje paketa, tada bi *bastion* poslužitelj trebao biti postavljen tako da sve veze iz vanjske mreže

prolaze kroz *bastion* poslužitelja kako bi se spriječila izravna internetska veza između mreže tvrtke i vanjskog svijeta [2].)

Arhitektura povjerenog poslužitelja prikladna je kada: malo veza dolazi s Interneta (osobito nije odgovarajuća arhitektura ako je odabrani glavni poslužitelj javni web poslužitelj). mreža koja se štiti ima relativno visoku razinu sigurnosti poslužitelja.




**Slika 2.2: Primjer arhitkture povjerenog poslužitelja**

Zaštićena podmreža

Od svih dostupnih arhitektura, *Screened Subnet* vatrozid široko se koristi i implementira u korporativnim mrežama, prikazan na slici 2.3. Vatrozid zaštićene podmreže, kao što ime sugerira, koristi DMZ i kombinacija je *multi-homed gatewayja* i vatrozida provjerenog poslužitelja. U postavkama zaštićenog podmrežnog vatrozida, mrežna arhitektura ima tri komponente, a postava je sljedeća:

1. komponenta: Ova komponenta djeluje kao javno sučelje i povezuje se na Internet.

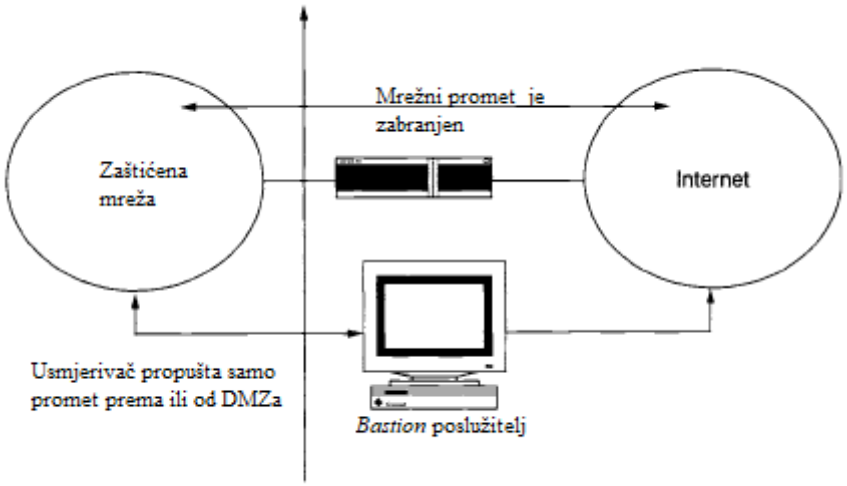
2. komponenta: Ova komponenta je srednja zona koja se naziva demilitarizirana zona. Djeluje kao međuspremnik između 1. i 3. komponente.

3. komponenta: Sustav u ovoj komponenti povezuje se s intranetom ili drugom lokalnom arhitekturom.

Prednosti

Korištenje dodatnog "sloja" i drugih aspekata zaštićenog vatrozida podmreže čini ga održivim izborom za mnoga mjesta s velikim ili brzim prometom. Zaštićeni vatrozid podmreže također pomaže u propusnosti i fleksibilnosti [6]. (Zaštićenu podmrežu treba postaviti dodavanjem perimetarske mreže za odvajanje unutarnje mreže od vanjske. Ovo osigurava da ako dođe do uspješnog napada na *bastion* poslužitelja, napadač je ograničen na perimetarsku mrežu usmjerivačem za zaštitu koji je povezan između interne i perimetarske mreže [2].)

Dok zaštićeni vatrozid podmreže koristi dva zaštićena usmjerivača za stvaranje tri podmreže, vatrozid provjerenog poslužitelja koristi samo jedan zaštićeni usmjerivač da definira dvije podmreže: vanjsku mrežu i internu mrežu. Zaštićeni vatrozid podmreže je sigurniji jer uljez mora prijeći dvije filtrirane rute da bi došao do interne mreže. Ako je *bastion* / DMZ (eng. *Demilitarized Zone*) poslužitelj ugrožen, uljez i dalje mora zaobići drugu filtriranu rutu kako bi došao do internih mrežnih poslužitelja [14].




**Slika 2.3: Primjer arhitkture zaštićene podmreže**

## 2.4. Problemi i prijetnje vatrozida

Sami vatrozidi se nikad ne bi trebali smatrati sveobuhvatnim rješenjem za potrebe kibernetičke sigurnosti tvrtke. Korisni su, ali postoji nekoliko problema s vatrozidima zbog kojih bi bilo loše oslanjati se samo na ovaj jedini sigurnosni alat za zaštitu poslovanja. Neke od opasnosti su: unutarnji napadi, propuštene sigurnosne zakrpe, greške u konfiguraciji, nedostatak duboke inspekcije paketa, DDoS napadi, jednostavna lozinka, protokoli inspekcije su jednostavni, *Smurf* napadi, *IP spoofing, SYN flood* napad, *Ping of Death, Port Scan*

- Unutarnji napadi

Vatrozid perimetra namijenjen je zaštiti od napada koji potječu izvan mreže korisnika. Tipično, perimetarski vatrozid postaje beskoristan—uostalom, napadač je već na sustavu. Međutim, čak i kada napad potječe iz mreže korisnika, vatrozidi mogu učiniti nešto dobro, ako postoje unutarnji vatrozidi povrh perimetarskih vatrozida korisnika. Unutarnji vatrozidi pomažu u razdjeljivanju pojedinačnih sredstava na mreži korisnika tako da se napadači moraju znatnije potruditi da prijeđu s jednog sustava na drugi. To pomaže produžiti napadačevo vrijeme proboja tako da korisniku nudi više vremena za odgovor na napad [7].

- Propuštene sigurnosne zakrpe

Ovo je problem koji nastaje kada se softverom mrežnog vatrozida ne upravlja ispravno. U svakom softverskom programu postoje ranjivosti koje napadači mogu iskoristiti—to vrijedi i za vatrozidne programe, kao i za bilo koji drugi softver. Kada dobavljači vatrozida otkriju te ranjivosti, uglavnom rade na stvaranju zakrpe koja rješava problem što je prije moguće.

Međutim, samo postojanje zakrpe ne znači da će se automatski primijeniti na vatrozidni program tvrtke. Sve dok se ta zakrpa stvarno ne primijeni na softver vatrozida, ranjivost je još uvijek prisutna, samo je pitanje trenutka kada će je iskoristiti nasumični napadač.

Najbolje rješenje za ovaj problem je stvoriti i pridržavati se strogog rasporeda upravljanja zakrpama. Prema takvom rasporedu, potrebno je provjeravati sva sigurnosna ažuriranja za softver vatrozida i svakako ih primijeniti što je prije moguće [7].

- Greške u konfiguraciji

Čak i kada je vatrozid postavljen na mreži i ima sve najnovije zakrpe ranjivosti, još uvijek može uzrokovati probleme ako konfiguracijske postavke vatrozida stvaraju sukobe. To može dovesti do gubitka performansi na mreži tvrtke u nekim slučajevima, a vatrozid ne uspijeva potpuno pružiti zaštitu u drugima.

Na primjer, dinamičko usmjeravanje je postavka za koju se davno smatralo da nije loša ideja jer rezultira gubitkom kontrole koji smanjuje sigurnost. Ipak, neke tvrtke ga ostavljaju uključenim, stvarajući ranjivost u zaštiti vatrozida [7].

- Nedostatak duboke inspekcije paketa

Inspekcija sloja 7 (ili "dubokog paketa") je rigorozan način inspekcije koji koriste vatrozidi sljedeće generacije za ispitivanje sadržaja informacijskog paketa prije nego što se odobri ili zabrani prolaz tog paketa u sustav ili iz njega.

Manje napredni vatrozidi mogu jednostavno provjeriti točku podrijetla i odredište podatkovnog paketa prije nego što odobre ili odbiju zahtjev, odnosno informacije koje napadač može lako krivotvoriti kako bi prevario vatrozid mreže.

Najbolje rješenje za ovaj problem je korištenje vatrozida koji može izvršiti duboku inspekciju paketa kako bi provjerio informacijske pakete za poznati zlonamjerni softver da bi se mogao odbiti [7].

- DDoS napad (eng. *Distributed Denial-of-Service Attack, DDoS Attack*)

Distribuirani napadi uskraćivanja usluge (DDoS) često su korištena strategija napada, poznata po tome što je vrlo učinkovita i relativno jeftina za izvođenje. Osnovni cilj je nadjačati resurse branitelja i uzrokovati gašenje ili produljenu nemogućnost pružanja usluga. Jedna kategorija napada (napadi na protokol) osmišljena je da iscrpi resurse vatrozida i upravitelja opterećenja kako bi ih spriječili u obradi legitimnog prometa.

Iako vatrozidi mogu ublažiti neke vrste DDoS napada, još uvijek mogu biti preopterećeni napadima na protokol.

Ne postoji jednostavno rješenje za DDoS napade, budući da postoje brojne strategije napada koje mogu iskoristiti različite slabosti u mrežnoj arhitekturi vaše tvrtke. Neki pružatelji usluga kibernetičke sigurnosti nude usluge "čišćenja", pri čemu preusmjeravaju dolazni promet s mreže i odvajaju legitimne pokušaje pristupa od DDoS prometa. Taj se legitimni promet zatim šalje mreži radi nastavka s normalnim radom [7].

- Jednostavna lozinka

Poznato je da je lozinke teško zapamtiti, što dovodi u iskušenje da se postave jednostavne ili, još gore, zadane tvorničke postavke. Ako je dopušteno da se to dogodi na sustavu, podatci sustava izloženi su svim mogućim vrstama napada i iskorištavanja. Ovo posebno vrijedi za SQL poslužitelje ako krajnji korisnik nije uspio ojačati svoje vjerodajnice za provjeru autentičnosti. Pad jednog servera ugrožava sva računala koja su na njega povezana [8].

- *Smurf* napad

*Smurf* napad je napad distribuiranog uskraćivanja usluge (DDoS) na mrežnom sloju, nazvan po zlonamjernom softveru *'DDoS.Smurf'* koji omogućuje njegovo izvršenje. *Smurf* napadi donekle su slični *ping flodingu,* jer se oba izvode slanjem niza ICMP Echo paketa zahtjeva. Međutim, za razliku od običnog *ping floodinga, Smurf* služi za pojačanje napada povećavajući svoj potencijal štete iskorištavanjem karakteristika mreža za emitiranje [9].

- *IP Spoofing*

*IP spoofing* je stvaranje paketa internetskog protokola (IP) koji imaju modificiranu izvornu adresu kako bi se sakrio identitet pošiljatelja, oponašao drugi računalni sustav ili oboje. To je tehnika koju zlonamjerne osobe često koriste za izazivanje DDoS napada na ciljni uređaj ili okolnu infrastrukturu.

Slanje i primanje IP paketa primarni je način na koji umrežena računala i drugi uređaji komuniciraju i to čini osnovu modernog interneta. Svi IP paketi sadrže zaglavlje koje prethodi tijelu paketa i sadrži važne informacije o usmjeravanju, uključujući adresu izvora. U normalnom paketu izvorna IP adresa je adresa pošiljatelja paketa. Ako je paket krivotvoren, izvorna adresa će biti krivotvorena [10].

- *SYN Flooding* napad

*SYN Flooding* je uobičajeni oblik napada uskraćivanjem usluge (DDoS) koji može ciljati bilo koji sustav povezan s internetom i koji pruža uslugu TCP-a (eng. *Transmission Control Protocol*), npr. web poslužitelj, poslužitelj e-pošte, prijenos datoteka. *SYN flooding* je vrsta TCP *State-Exhaustion Attacka* koji pokušava iskoristiti tablice stanja veze prisutne u mnogim infrastrukturnim komponentama, kao što su upravitelji opterećenja, vatrozidi, sustavi za sprječavanje upada (eng. *Intrusion Prevention System*, IPS) i sami aplikacijski poslužitelji. Ova vrsta DDoS napada može srušiti i uređaje velikog kapaciteta koji mogu održavati milijune veza [11].

- *Ping of Death* napad

Ping smrti (poznat i kao PoD) vrsta je napada uskraćivanja usluge (DoS) u kojem napadač pokušava srušiti, destabilizirati ili zamrznuti ciljano računalo ili uslugu slanjem neispravnih ili prevelikih paketa pomoću jednostavne naredbe 'ping'. Dok PoD napadi iskorištavaju naslijeđene slabosti koje su možda zakrpane u ciljanim sustavima. Međutim, u sustavima bez zakrpa, napad je i dalje relevantan i opasan. Nedavno je postala popularna nova vrsta PoD napada. Ovaj napad, obično poznat kao *Ping flood*, vrsta je napada gdje je ciljani sustav pogođen ICMP paketima koji se brzo šalju putem pinga bez čekanja odgovora [12].

- *Port scanning*

Skeniranje priključaka uobičajena je tehnika koju 'hakeri' koriste za otkrivanje otvorenih vrata ili slabih točaka u mreži. Napad skeniranjem porta pomaže *cyber* kriminalcima da pronađu otvorene portove i otkriju primaju li ili šalju podatke. Također može otkriti koristi li tvrtka aktivne sigurnosne uređaje poput vatrozida. Kada 'hakeri' pošalju poruku portu, odgovor koji dobiju određuje koristi li se port i postoje li potencijalne slabosti koje sbi se mogle iskoristiti [13].

# 3. MIKROTIK ROUTEROS

MikroTik RouterOS je operacijski sustav MikroTik RouterBOARD uređaja koje proizvodi tvrtka MikroTik. MikroTik je latvijska tvrtka koja se bavi razvojem routera i bežičnih ISP (eng. *Internet Service Provider*) sustava, također nude hardvere i softvere za pristup Internetu u većini država svijeta. MikroTik RouterOS također može biti instaliran na računalu te će to računalo imati sve mogućnosti koje nudi i usmjerivač (kao što su usmjeravanje prometa, vatrozid, upravljanje propustom prometa, bežična pristupna točka, *hotspot gateway*, VPN server i dr.). Operacijski sustav se bazira na Linux v2.6 *kernelu* i podržava sve mogućnosti koje nudi ta verzija *kernela*. Sposobnosti koje nudi RouterOS ovise o instaliranim paketima. Nakon dodavanja paketa potrebno je resetirati uređaj kako bi sustav ažurirao listu paketa i instalirao ih [4].

## 3.1. Konfiguracija RouterOS-a

RouterOS podržava različite načine konfiguracije kao što su lokalni pristup uporabom tipkovnice i monitora, uporabom terminala serijske konzole, Telnet i sigurni SSH (eng. *Secure Shell*) pristup preko mreže, jednostavno Web konfiguracijsko sučelje i API programsko sučelje za izgradnju vlastite kontrolne aplikacije. U slučaju da je lokalni pristup onemogućen, te postoji problem s IP komunikacijskim slojem, također podržava vezu preko MAC sloja s prilagođenim Mac-Telnet i Winbox alatima. U ostalom RouterOS pruža snažne i jednostavne linijske naredbe za konfiguraciju preko sučelja s ugrađenom mogućnošću pisanja skripti [4].

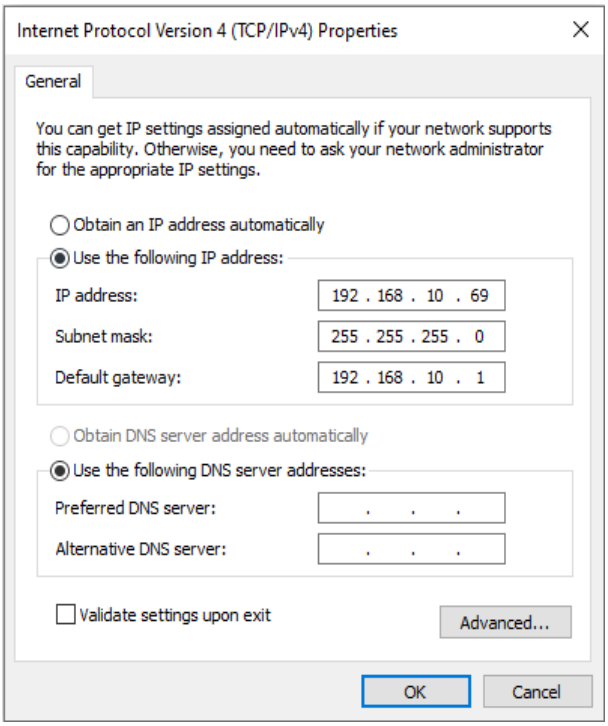
- Winbox GUI uporabom IP-a i MAC-a
- CLI (eng. *Command-line Interface*) s Telnetom, SSH, Lokalne konzole i Serijske konzole
- API koji služi za programiranje i stvaranje vlastitih alata
- Web sučelje

# 4. POSTAVLJANJE VATROZIDA

## 4.1. Priprema računala prije spajanja usmjerivača

Prije samog postavljanja pravila vatrozida potrebno je isključiti vatrozid (eng. *firewall*) računala koje koristimo i onemogućiti sve mrežne konekcije osim LAN-a ili Etherneta (ovisi o računalu). To je učinjeno na način da odemo na 'kontrolnu ploču' (eng. *Control Panel*) računala zatim odaberemo 'mreža i Internet' (eng. *Network and Internet*) → 'centar za mrežu i dijeljenje' (eng. *Network and Sharing Centre*). Nakon toga odabrana je opcija 'promijenite postavke adaptera' (eng. *Change Adapter Settings*), potrebno je onemogućiti sve mrežne veze na računalima osim veze lokalnog područja (eng. *Local Area Connection, LAN*). Nakon toga potrebno je isključiti vatrozid (eng. *firewall*), ukoliko je pokrenut na računalu. To je učinjeno vraćanjem na 'centar za mrežu i dijeljenje' (eng. *Network and Sharing Centre*) → te je odabrana opcija 'Windows vatrozid' (eng. *Windows Defender Firewall*) → odabrana je opcija 'uključi ili isključi Windows vatrozid' (eng. *Turn Windows Defender Firewall on or off*) → te je isključen vatrozid za privatne i javne mreže.

Zadnji korak koji je potrebno izvršiti na računalu prije spajanja i konfiguriranja usmjerivača potrebno je vratiti se na 'centar za mrežu i dijeljenje' (eng. *Network and Sharing Centre*) → odabrati 'promijenite postavke adaptera' (eng. *Change Adapter Settings*) → zatim dva puta lijevim klikom miša kliknuti na 'veza lokalnog područja' (eng. *Local Area Connection, LAN*) → odabrana je opcija *Internet Protocol Version4 (TCP/Ipv4*) i namještene su postavke kao na slici 4.1. Time je računalu dodijeljena određena IP adresa kojom namjeravamo pristupiti konfiguratoru usmjerivača.



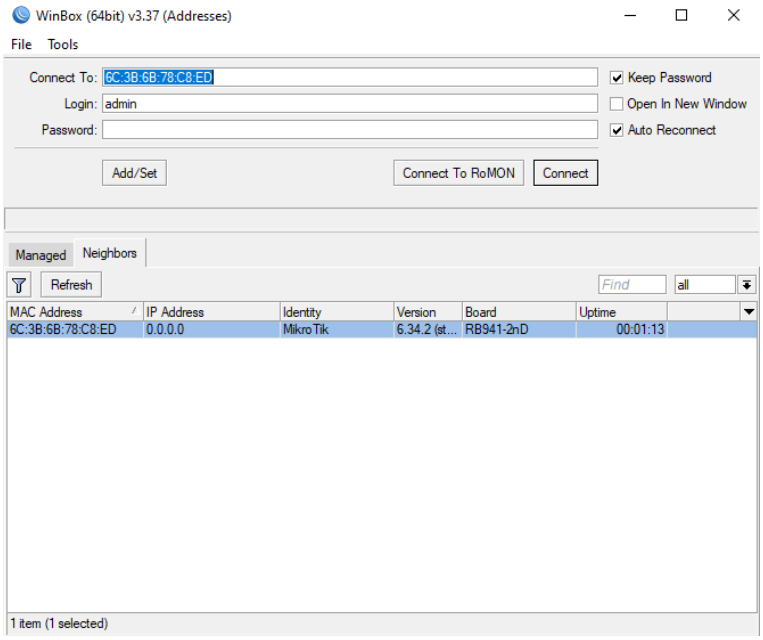

**Slika 4.1: Postavke IP adrese, podmaske i zadanog pristupa korištenog računala.**

## 4.2. Spajanje usmjerivača na računalo

Usmjerivač koji je korišten zove se *routerboard hAP lite* te je potrebno resetirati uređaj prilikom samog paljenja i unutar konfiguratora usmjerivača.

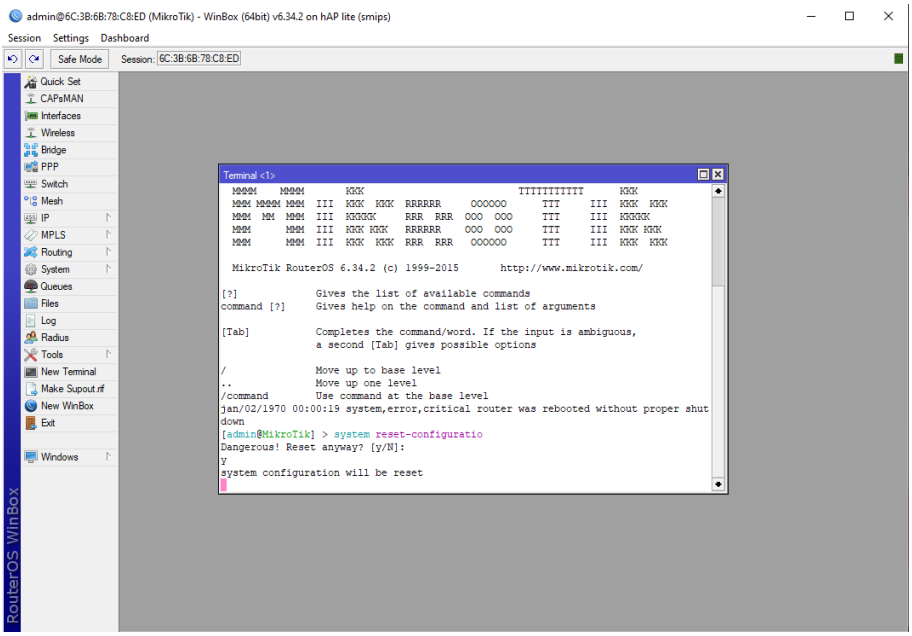
Resetiranje usmjerivača prilikom uključivanja vrši se prilikom samog paljenja držanjem tipke *res/wps* (potrebno je primjetiti da svjetleća dioda (LED) pored koje piše *usr* počne treperiti, tipku je potrebno držati pritisnutom sve dok dioda ne prestane treperiti).

Nakon tog potrebno je spojiti računalo pomoću *patch* kabela na port *ether2* sučelje usmjerivača. Zatim je potrebno pokrenuti *WinBox* aplikaciju i odabrati MAC adresu (eng. *MAC Address*) usmjerivača s popisa unutar aplikacije, te kliknuti na *Connect*, prikazano na slici 4.2.



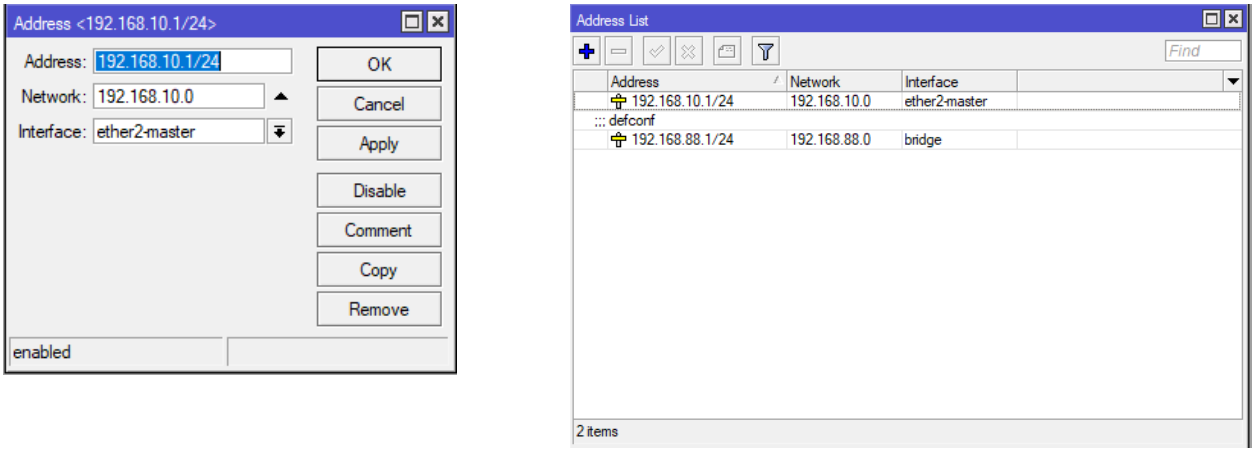

**Slika 4.2: Odabir korištenog usmjerivača unutar *WinBox* aplikacije.**

Nakon što se otvori konfigurator usmjerivača potrebno je otvoriti novi terminal (eng. *New Terminal*) te unutar terminala, prikazano na slici 4.3 upisati naredbu *system reset-configuration* i pritisnuti slovo *y*. Time je usmjerivač postavljen na tvorničke postavke.




**Slika 4.3: Postavljanje usmjerivača na tvorničke postavke unutar konfiguratora.**

Nakon uspješnog izvršenja naredbe trebao bi se ponovno otvoriti konfigurator usmjerivača. Potrebno je sučelju *ether2* dodijeliti IP adresu. Unutara izbornika *IP* potrebno je odabrati opciju *Addresses* i unutar izbornika *Address List* odabrati oznaku '+', te dodijeliti sučelju *ether2* adresu 192.168.10.1/24 i postaviti adresu mreže na 192.168.10.0. Nakon toga unutar izbornika *IP* potrebno je odabrati opciju *Firewall* (uporabom izbornika se postavljaju pravila korištenog vatrozida), prikazano na slici 4.4.



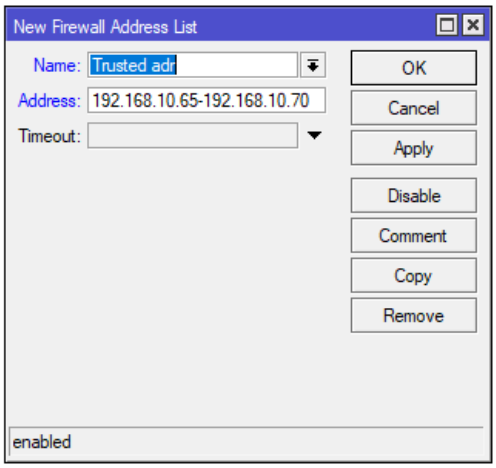

**Slika 4.4: Dodjeljivanje IP adrese i mrežne adrese sučelju *ether2*.**

# 5. Filtriranje prometa vatrozida prema adresnoj listi IP adresa, protokolima i portovima.

## 5.1. Postavljanje adresne liste IP adresa

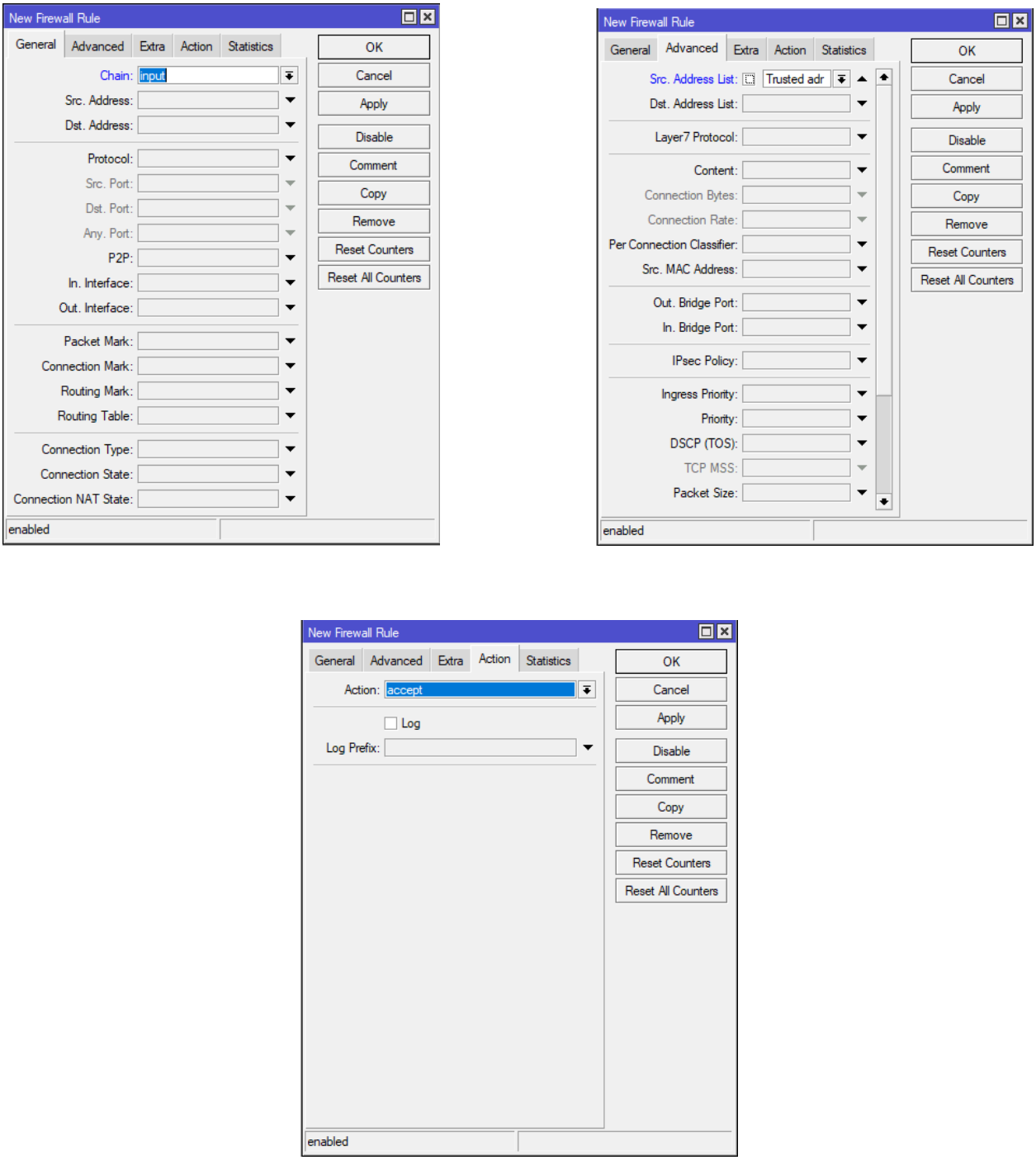
Kao prvo pravilo postavljeno je pravilo koje uvijek propušta klijente čija se IP adresa nalazi unutar određenog raspona (u ovom slučaju to će biti svi klijenti čija se IP adresa nalazi unutar sljedećeg raspona: 192.168.10.65 – 192.168.10.70). Te IP adrese su spremljene kao lista te ih usmjerivač uvijek propušta kada klijent s odgovarajućom IP adresom zatraži pristup.

Unutar izbornika *Firewall* odabrana je opcija *Address Lists* te klikom na oznaku '+', dodana je nova lista adresa pod nazivom *'Trusted adr'*, prikazano na slici 5.1.




**Slika 5.1: Kreiranje liste adresa.**

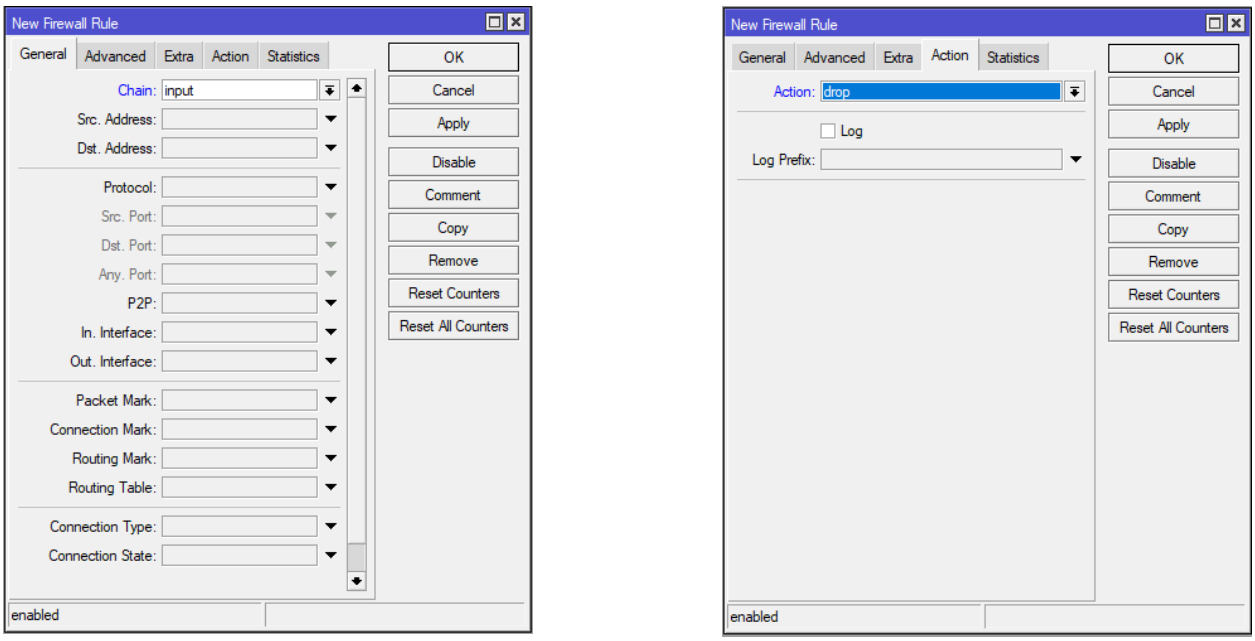
Zatim unutar izbornika *Firewall* odabran je izbornik *Filter Rules*, te klikom na oznaku '+' omogućeno je kreiranje novog pravila za vatrozid. Unutar prozora *New Firewall Rule* potrebne opcije su *General* (unutar *General* kao lanac odabran je *input* što podrazumijeva da se obrađuju svi podatci koji ulaze na usmjerivač uporabom jednog od njegovih sučelja s odredišnom IP adresom koja je adresa usmjerivača), *Advanced* (unutar opcije *Advanced*, od ponuđenih postavki u izborniku *Src. Address List* odabrana je ranije kreirana lista adresa '*Trusted adr*') i *Action* (unutar opcije *Action* kao akciju koju će usmjerivač poduzeti odabrana je opcija *accept*), prikazano na slici 5.2.




**Slika 5.2: Postavke izbornika *General, Advanced* i *Action* za prvo pravilo.**

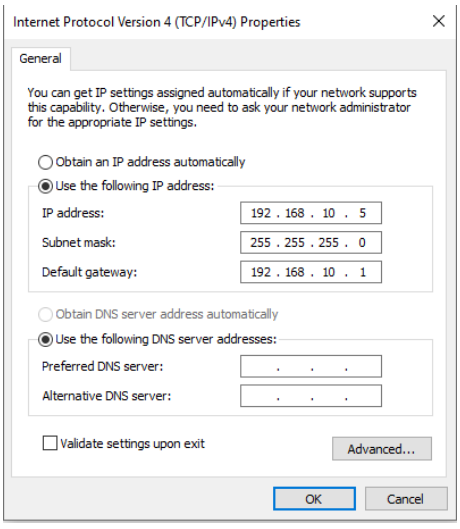
## 5.2. Blokiranje pristupa klijentima koji se ne nalaze na ranije postavljenoj listi IP adresa

Za postavljanje ovog pravila unutar *New Firewall Rule* prozora potreban je izbornik *General* (unutar izbornika *General* kao lanac ili *Chain* postavljen je *input*) i izbornik *Action* (unutar izbornika *Action*, kao akciju koju je željno poduzeti odabrana je opcija *drop*), prikazano na slici 5.3. Ovim i prethodno postavljenim pravilom usmjerivač će propuštati samo promet klijenata čija se IP adresa nalazi unutar adresne liste '*Trusted adr*' dok će sve ostale klijente blokirati.

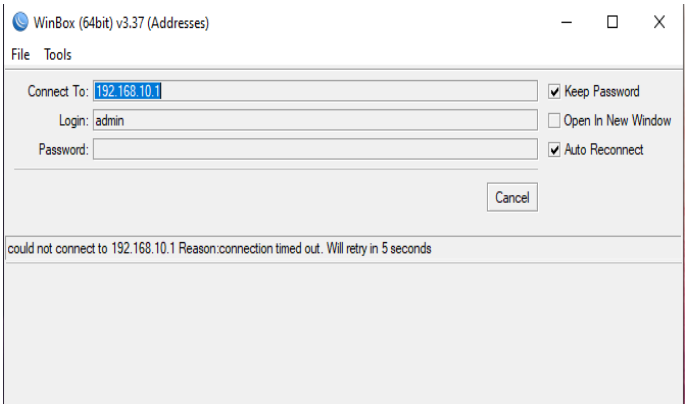



**Slika 5.3: Postavke *General* i *Action* drugog pravila.**

Nadalje, postavljanjem IP adrese klijenta, prikazano na slici 5.4 usmjerivač će blokirati pristup korisniku, prikazano na slici 5.5, te je potrebno pristupiti koristeći odgovarajuću IP adresu.




**Slika 5.4: Testna adresa korištenog računala**



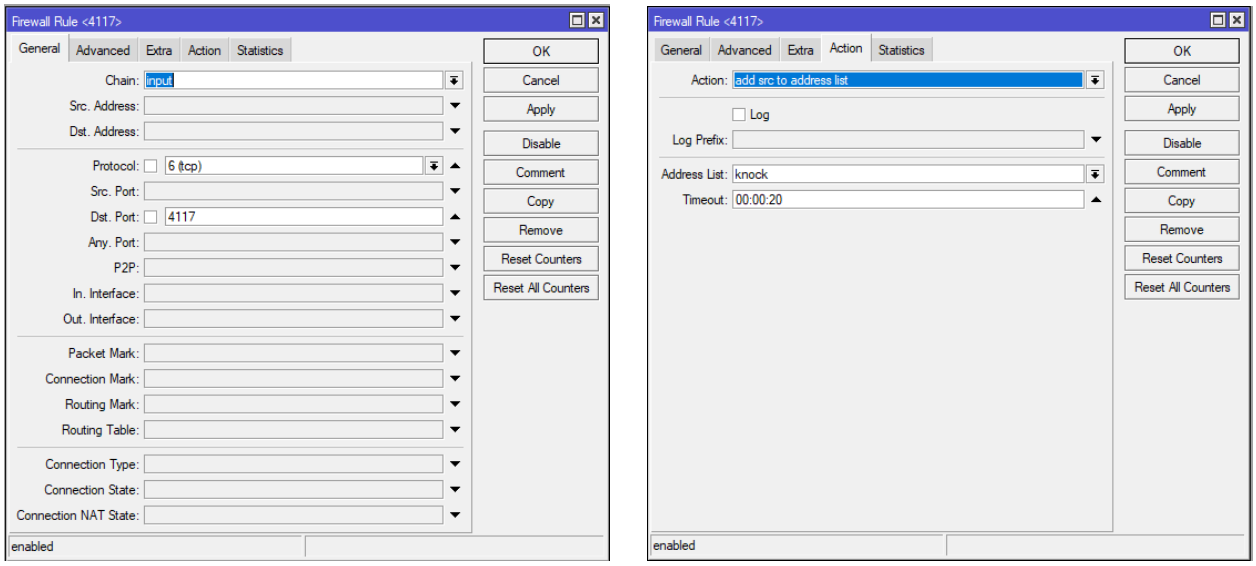

**Slika 5.5: Blokiran pristup usmjerivaču, radi uporabe neodgovarajuće IP adrese računala**

## 5.3. Filtriranje prometa vatrozida prema portovima i protokolima

Zadnja pravila koja je potrebno dodati služe za filtriranje paketa prema definiranim portovima i protokolima. Usmjerivač je konfiguriran na način da dinamički dodaje zapis o IP adresama u adresnu listu, te taj zapis vrijedi unutar ograničenog perioda (takav način pristupa naziva se *port knocking*).

### 5.3.1. Treće pravilo

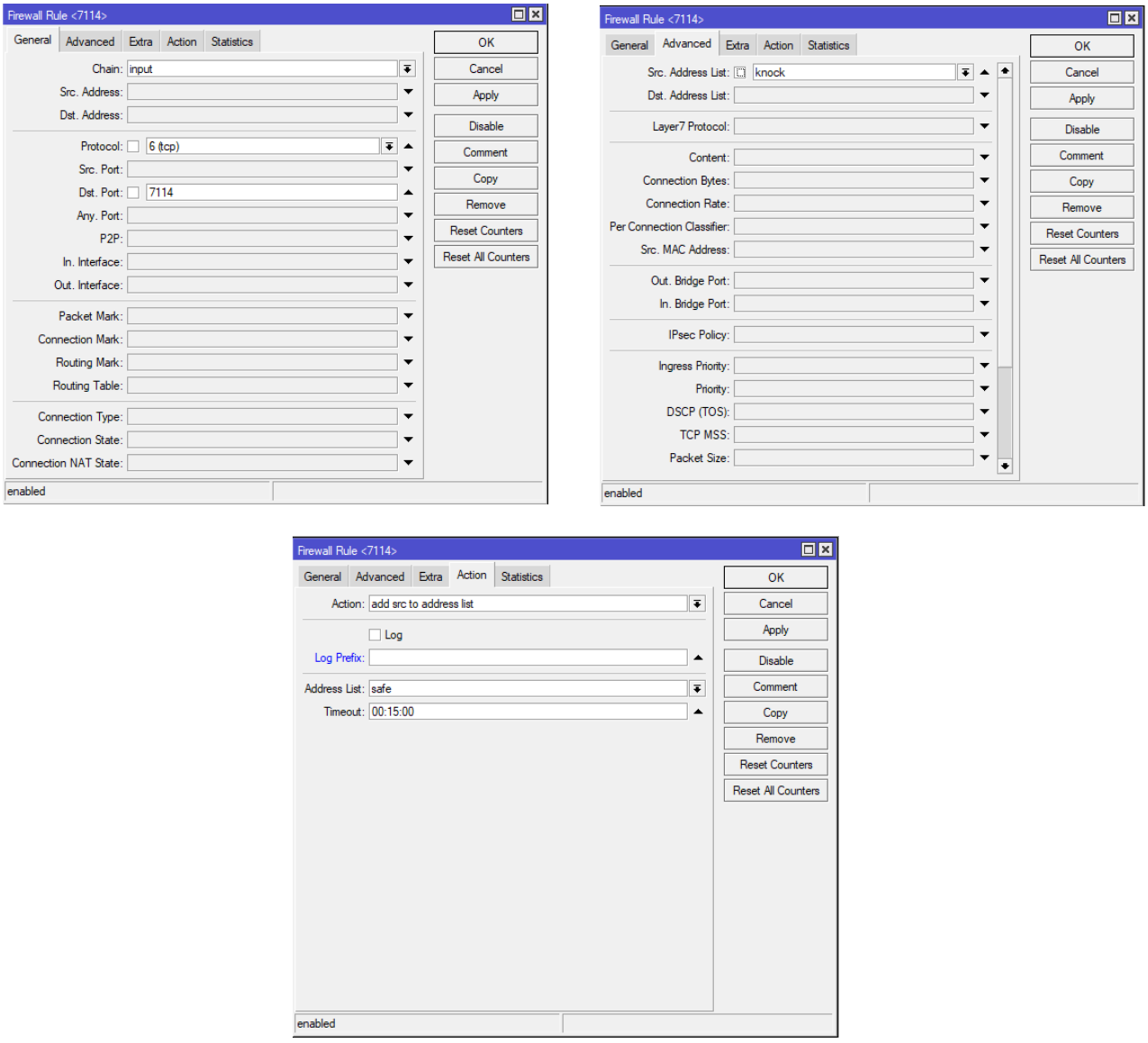
Klikom na *New Firewall Rule* kreirano je novo pravilo koristeći opcije *General* (unutar izbornika *General* kao lanac postavljen je *input*, protokol koji je korišten je *6 (tcp)*, a *Dst. Port* je 4117) i *Action* (unutar izbornika *Action*, kao akciju odabrana je opcija *add src to address list*, ime adresne liste na koju se dodaje zapis IP adrese klijenta je *'knock'*, te je *timeout* postavljen na 20 sekundi), prikazano na slici 5.6. Ovim pravilom omogućeno je dodavanje klijenta koji šalje paket usmjerivaču na port 4117 na listu pod nazivom *'knock'*, postavljen je *timeout* od 20 sekundi i blokiran je sav promet osim prometa na portu 4117.




**Slika 5.6: Postavke izbornika *General* i *Action* trećeg pravila.**

### 5.3.2. Četvrto pravilo

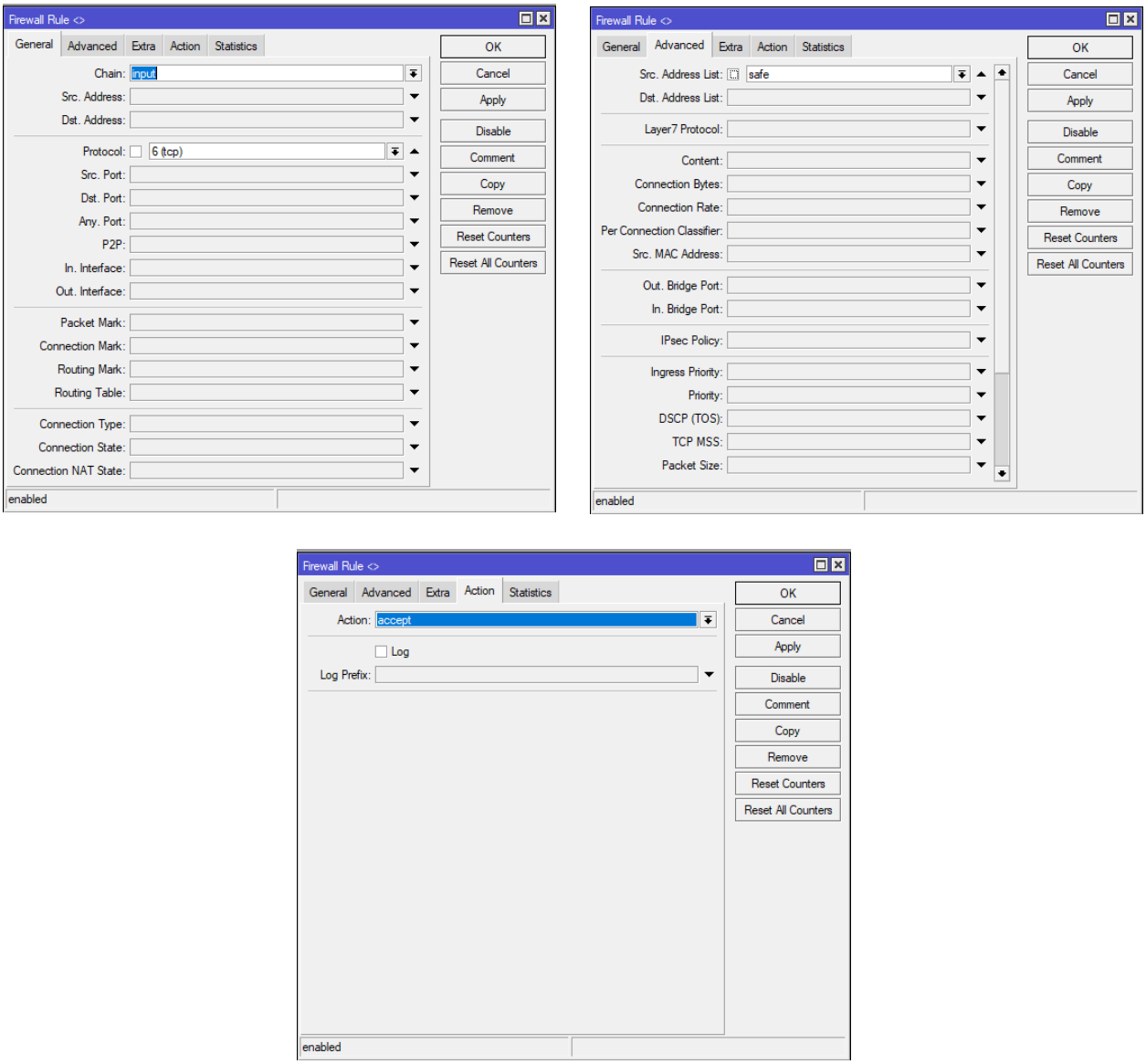
Četvrto pravilo konfigurirano je koristeći izbornike *General* (*Chain* će biti postavljen kao *input*, jer će pravilo vršiti provjeru podataka koji se šalju na usmjerivač, zatim je odabran 6 (tcp) protokol, a *Dst. Port* je 7114), *Advanced* (u ovom izborniku kao izvorna lista adresa odabrana je lista pod nazivom *'knock'*) i *Action* (izbornik je konfiguriran tako da kao akciju, pravilo kreira listu i zapis IP adrese dodaje na dinamičku listu pod nazivom *'safe'* uz *timeout* od 15 minuta), prikazano na slici 5.7. Ako raniji klijent sa liste *'knock'* pošalje paket usmjerivaču na port 7114, usmjerivač provjerava nalazi li se klijent na listi *'knock'*, ako se nalazi, dodaje IP adresu klijenta u adresnu listu *'safe'* uz postavljeni *timeout* od 15 minuta.




**Slika 5.7: Postavke izbornika *General*, *Advanced* i *Action* četvrtog pravila.**

### 5.3.3. Peto pravilo

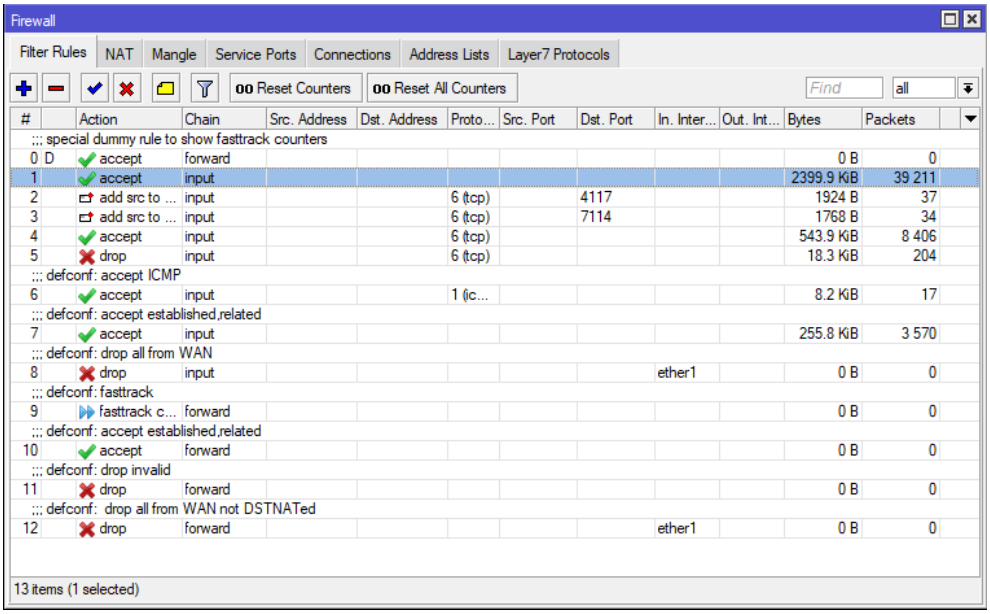
Petim pravilom omogućeno je svim klijentima koji se nalaze unutar adresne liste *'safe'* pristup konfiguratoru usmjerivača. Pravilo će biti konfigurirano koristeći izbornike *General* (odabrani lanac je *input*, time vršimo obradu podataka koji se šalju na usmjerivač i korišteni protokol je 6 (tcp), *Advanced* (unutar izbornika *Advanced* kao *Src. Address List* odabrana je lista adresa *'safe'*) i *Action* (unutar izbornika *Action* kao akcija koju pravilo poduzima odabrana je akcija *accept*), prikazano na slici 5.8. Pravilo dopušta pristup konfiguratoru usmjerivača jedino IP adresama klijenata koji se nalaze unutar liste *'safe'*.



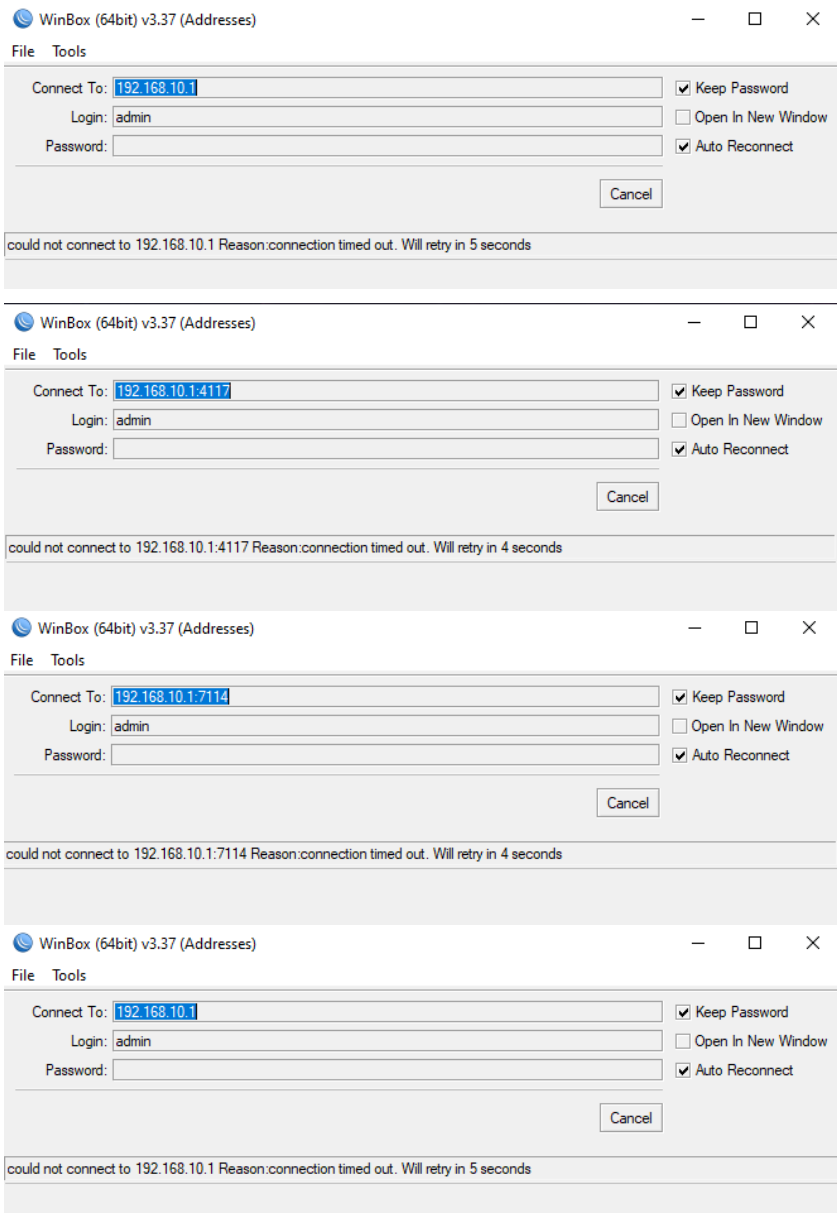

**Slika 5.8: Postavke izbornika *General*, *Advanced* i *Action* petog pravila.**

## 5.4. Testiranje ispravnosti postavljenih pravila

Za kraj je potrebno testirati funkcioniraju li pravila kako je predviđeno. Uvjet za prvo pravilo je da se IP adresa klijenta nalazi u rasponu od 192.168.10.65 – 192.168.10.70, tada je klijentu pristup uvijek odobren. Za pravila od 3 do 5 potrebno je zatražiti pristup usmjerivaču određenim redoslijedom. Također je potrebno postaviti pravila određenim redoslijedom unutar konfiguratora usmjerivača kako bi sve funkcioniralo ispravno, prikazano na slici 5.9. Unutar aplikacije *WinBox* prvo je potrebno pristupiti usmjerivaču uporabom porta 4117 (pristup će biti onemogućen, ali će zapis IP adrese biti dodan na listu adresa *'knock'*), zatim je potrebno pristupiti usmjerivaču uporabom porta 7114 (time je zapis IP adrese dodan sa liste *'knock'* na listu adresa 'safe' i omogućen nam je pristup usmjerivaču), a za kraj je potrebno pristupiti usmjerivaču uporabom njegove adrese (192.168.10.1), prikazano na slici 5.10. Pokušaj pristupa takvim redoslijedom vatrozid je odredio da je klijent povjerljiv i omogućuje mu pristup.




**Slika 5.9: Redoslijed pravila unutar vatrozida, pravila kreirana u radu nalaze se od broja 1 do 5.**




**Slika 5.10: Postupak prijave uporabom trećeg, četvrtog i petog pravila.**

# 6. ZAKLJUČAK

S obzirom da smo u današnje vrijeme sve više okruženi tehnologijom i da je velika količina te tehnologije spojena na Internet, također postoje opasnosti za nas kao korisnike te tehnologije, ali i rizik oštećenja uređaja od zlonamjernih korisnika. Štete mogu biti bezazlene od primanja i slanja velikog broja nepoželjnih reklama (eng. *spam mail*), do neovlaštenog pristupa uređajima i informacijama, do krađe tih informacija, pa sve do primanja virusa koji imaju potencijala biti izuzetno štetni. Prilikom korištenja Interneta sigurnost računala od velike je važnosti za privatnu uporabu, ali isto tako i za uporabu unutar organizacije ili tvrtke. Jedna od efikasnijih sigurnosnih mjera zaštite je uporaba vatrozida. Vatrozid je koristan jer ga se može konfigurirati na različite načine koji odgovaraju klijentu (pojedincu ili organizaciji) za njegovu uporabu u svakodnevnom životu. Vatrozid funkcionira na način da analizira i filtrira pakete koji dolaze u komunikaciju između dvaju ili više čvorova u mreži, a to čini tako da blokira ili propusti promet (ovisi o načinu na koji je konfiguriran).

MikroTik RouterOS jedan je od operacijskih sustava koji se može koristiti za konfiguriranje vatrozida, omogućava analizu toka podataka i evidentiranje stanja mreže. MikroTik nudi korisniku kreiranje i podešavanje raznih pravila filtriranja podatkovnog prometa kroz usmjerivač, što nudi visoku razinu fleksibilnosti prilikom dizajna vatrozida. Operacijski sustav MikroTik RouterOS pogodan je radi mogućnosti pretvorbe osobnog računala u *softverski* usmjerivač koji je pogodan za rad s usmjerivačima i konfiguratorima usmjerivača.

Korištena konfiguracija vatrozida omogućila je filtriranje paketa prema IP adresama unutar adresne liste, prema protokolima i portovima računala. Nakon uspješno i pravilno postavljenih pravila vatrozida, vatrozid je svim neovlaštenim korisnicima zabranio pristup usmjerivaču, te je time postignuta zaštita računala i korisnika mreže.

# LITERATURA


[1] N. Gupta, V. Naik and S. Sengupta, "A firewall for Internet of Things," 2017 9th International Conference on Communication Systems and Networks (COMSNETS), 2017, pp. 411-412, doi: 10.1109/COMSNETS.2017.7945418.

[2] Vacca, John R, and Scott Ellis. Firewalls: Jumpstart for Network and Systems Administrators. Burlington, MA: Elsevier Digital Press, 2005. Internet resource.

[3] *Firewall: Definition, how they work & why you need one*. Okta. (n.d.). Retrieved June 28, 2022, from https://www.okta.com/identity-101/firewall/

[4] *Mikrotik routeros - about Routeros*. Mikrotik RouterOS Licences. (n.d.). Retrieved June 29, 2022, from http://www.mikrotik-routeros.net/routeros.aspx

[5] Amy Larsen DeCarlo; Robert G. Ferrell. (2021, January 19). *The 5 different types of firewalls explained*. SearchSecurity. Retrieved September 17, 2022, from https://www.techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls

[6] 21, M., 7, M., 4, M., & 28, F. (2021, August 24). *Firewall types and architecture*. Infosec Resources. Retrieved September 17, 2022, from https://resources.infosecinstitute.com/topic/firewall-types-and-architecture/

[7] Eric Dosal April 12, Dosal, E., & 12, A. (2018, April 12). *5 firewall threats and vulnerabilities to look out for*. Cybersecurity Solutions. Retrieved September 17, 2022, from https://www.compuquip.com/blog/firewall-threats-vulnerabilities

[8] Kaplanskiy, A. (2021, September 27). *Top firewall vulnerabilities and threats*. TrustNet Cybersecurity Solutions. Retrieved September 17, 2022, from https://www.trustnetinc.com/firewall-vulnerabilities/

[9] *What is a Smurf attack: Ddos attack glossary: Imperva*. Learning Center. (2020, September 30). Retrieved September 17, 2022, from https://www.imperva.com/learn/ddos/smurf-attack-ddos/

[10] *What is IP spoofing? | cloudflare*. (n.d.). Retrieved September 17, 2022, from https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

[11] *What is a SYN flood ddos attack and how do you to prevent it?* NETSCOUT. (n.d.). Retrieved September 17, 2022, from https://www.netscout.com/what-is-ddos/syn-flood-attacks

[12] *What is ping of death (pod): Ddos attack glossary: Imperva*. Learning Center. (2020, September 30). Retrieved September 17, 2022, from https://www.imperva.com/learn/ddos/ping-of-death/

[13] *What is a port scan? how to prevent port scan attacks?* Fortinet. (n.d.). Retrieved September 17, 2022, from https://www.fortinet.com/resources/cyberglossary/what-is-port-scan

[14] Wikimedia Foundation. (2022, August 28). *Screened subnet*. Wikipedia. Retrieved September 18, 2022, from https://en.wikipedia.org/wiki/Screened_subnet

Slika [2.1] https://www.okta.com/identity-101/firewall/.

Slika [2.2] Vacca, John R, and Scott Ellis. Firewalls: Jumpstart for Network and Systems Administrators. Burlington, MA: Elsevier Digital Press, 2005. Internet resource.

Slika [2.3] Vacca, John R, and Scott Ellis. Firewalls: Jumpstart for Network and Systems Administrators. Burlington, MA: Elsevier Digital Press, 2005. Internet resource.

## SAŽETAK

Kako Internet postaje sve bitniji dio svakodnevnog života, ali isto tako i života raznih organizacija, bitno je znati kakvim se opasnostima izlažemo, te kako se možemo zaštititi i osigurati od raznih prijetnji kojima se izlažemo korištenjem Interneta. Unutar organizacije veliku ulogu sigurnosti čini ograničenje pristupa neovlaštenim korisnicima mreže organizacije, radi zaštite podataka i uređaja koji su pod tom organizacijom. Vatrozid pruža mogućnost kontrole toka prometa mreže i pristup mreži organizacije. Mogućnosti vatrozida i neke od sposobnosti prikazane su korištenjem usmjerivača MikroTik RouterOS. Cilj rada je prikazati te mogućnosti u uporabi, te na koji način vatrozid može pomoći pri održavanju prometa mreže sigurnim. Usmjerivačem su provedena pravila koja obuhvaćaju filtriranje paketa prema listi IP adresa, protokolima i portovima. Uporabom postavljenih pravila korištenja mreže omogućeno je korištenje mreže samo određenim korisnicima, čime je postignuta sigurnost mreže.



Ključne riječi: vatrozid, MikroTik RouterOS, zaštita mreže, filtriranje prometa, prijetnje na Internetu.



## ABSTRACT

As the Internet is becoming an increasingly important part of everyday life, but also the life of various organizations, it is important to know what dangers we are exposed to and how we can protect ourselves and insure ourselves against various threats to which we are exposed using the Internet. Within the organization, security plays a major role in restricting access to unauthorized users of the organization's network, in order to protect data and devices under that organization. A firewall provides the ability to control the flow of network traffic and access to an organization's network. The firewall possibilities and some of the capabilities are demonstrated using the MikroTik RouterOS router. The goal of this thesis is to show these possibilities in use and how a firewall can help keep network traffic safe. The router implements rules that include packet filtering according to the list of IP addresses, protocols and ports. By using the set network usage rules, it is possible to use the network only for certain users, thus achieving network security.



Key words: firewall, MikroTik RouterOS, network protection, traffic filtering, Internet threats.