HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# Analiza Firewall Builder alata

**CCERT-PUBDOC-2005-03-112**

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

**CARNet CERT**, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

**LS&S**, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

# Sadržaj

# 1. Uvod

Korištenje vatrozida pouzdan je i efikasan način zaštite sustava od većine sigurnosnih prijetnji koje dolaze s Interneta, što vatrozid čini neizostavnom komponentom modernih računalnih mreža. Postavljanjem vatrozida unutar računalne mreže, moguće je pojedine dijelove mreže dodatno zaštititi od mogućih prijetnji, kao i spriječiti širenje malicioznih programa sa zaraženih računala na ostatak mreže.

Osim specijaliziranih uređaja i programskih paketa koji filtriraju promet (Checkpoint, Netscreen itd.), vatrozid je moguće implementirati i korištenjem internih mehanizama za filtriranje prometa unutar Linux ili nekog drugog *open source* operacijskog sustava. Ovakav pristup financijski je isplativiji, ali zahtijeva stručno znanje administratora koji mora ispravno podesiti sustav da obavlja željenu funkciju te ponekad ne može ispuniti sve sigurnosne zahtjeve (npr. *stateful inspection*). Budući da je podešavanje vatrozidne zaštite složen postupak, u novije vrijeme sve je više specijaliziranih alata koji administratorima omogućuju da, u nekoliko jednostavnih koraka, podese željene parametre vatrozida, na temelju čega softver generira pravila za podešavanje sustava.

Ovaj dokument opisuje mogućnosti jednog od takvih alata pod nazivom Firewall builder, te izradu jednostavnih vatrozidova korištenjem tog alata.

## 1.1. Mogućnosti alata

Firewall builder je alat za konfiguraciju i upravljanje vatrozidima,s intuitivnim grafičkim sučeljem i mogućnošću izrade pravila za više vrsta vatrozida. Ovaj alat koristi objektno orijentirani pristup, koji administratoru pruža mogućnost da iz definirane baze mrežnih objekata i protokola, jednostavnim "drag-and-drop" operacijama kreira pravila za filtriranje prometa. Trenutno ovaj alat podržava izradu pravila za iptables, ipfilter i OpenBSD PF mehanizme za filtriranje prometa, te konfiguraciju Cisco PIX vatrozida.

Iz pravila podešenih u grafičkom sučelju, Firewall builder je u mogućnosti generirati konfiguracijske datoteke za sve podržane vatrozide, što ga čini idealnim rješenjem za heterogena okruženja. Također, njegovim korištenjem u velikoj mjeri se olakšavaju eventualne buduće migracije na druge operacijske sustave ili mrežnu opremu.

Trenutne mogućnosti alata obuhvaćaju:

- oko stotinu predefiniranih objekata koji obuhvaćaju najpopularnije mrežne protokole i servise,
- mogućnost kreiranja vlastitih objekata temeljenih na IP, ICMP, TCP i UDP protokolima i proizvoljnim servisima,
- mogućnost kreiranja objekata koji opisuju pojedina računala na mreži ili cjelokupne mreže,
- mogućnost kreiranja pravila korištenjem "čarobnjaka" koji sadrže tipične postavke tipične za većinu računalnih mreža, a čiji se izlaz može naknadno uređivati,
- alat za skeniranje mreže koji olakšava kreiranje mrežnih objekata,
- objektno orijentirani pristup upravljanju politika vatrozida, što znači da se promjena u određenom objektu automatski reflektira na sve politike u kojima je taj objekt korišten zato što svi vatrozidi dijele zajedničku bazu objekata,
- jednostavno prevođenje politika vatrozida u konfiguracijsku datoteku ili skriptu koja se lako instalira na ciljani sustav,
- jednostavno grafičko sučelje sa podrškom za *Copy/Paste* operacije sa znakovnim nizovima i svim definiranim objektima,
- podršku za više tipova vatrozidova i drugih sustava za filtriranje prometa,
- podršku za ispis objekata i politika vatrozida na pisač ili njihov *export* u HTML format.

## 1.2. Način Licenciranja

Firewall Builder se distribuira pod tzv. "*dual licensing*" modelom licenciranja. Kao što je već spomenuto, dostupne su inačice ovog alata za Linux, FreeBSD i druge Unix/Linux sustave, kao i za Microsoft Windows i Mac OS X operacijske sustave. Firewall Builder paketi namijenjeni Linux-u, FreeBSD-u i svim ostalim operacijskim sustavima koji se distribuiraju pod uvjetima GPL licence, također su dostupni pod istom licencom. Izvorni kod paketa moguće je dohvatiti sa službenih stranica Firewall Builder projekta (http://www.fwbuilder.org/).

Firewall Builder namijenjen komercijalnim operacijskim sustavima distribuira se pod uvjetima NetCitedel End User License Agreement licence, koju je moguće kupiti na web stranicama projekta.

Pod posebnom licencom distribuiraju se i moduli za izradu pravila za komercijalne vatrozide.

# 2. Instalacija

U svojoj osnovi, Firewall Builder je *open source* projekt (s ograničenjima opisanima u prethodnom poglavlju). Izvorni kod sučelja i modula za prevođenje pravila filtriranja moguće je dohvatiti na službenim stranicama projekta (http://www.fwbuilder.org). Paket je uspješno preveden i radi na sljedećim Open Source sustavima:

- Debian Linux,
- Mandrake Linux,
- RedHat Linux,
- SuSE Linux,
- Gentoo Linux,
- FreeBSD,
- OpenBSD.

Na adresi http://www.fwbuilder.org/archives/cat_installation.html, moguće je pronaći najnovije informacije o inačicama paketa i eventualnim specifičnostima prevođenja i instalacije za pojedine distribucije.

Prije instalacije paketa iz izvornog koda potrebno je osigurati postojanje sljedećih biblioteka i aplikacija na sustavu:

- `libxml2 v2.4.10` ili noviji,
- `libxslt v1.0.7` ili noviji,
- `ucd-snmp` ili `net-snmp`,
- `openssl` – posljednja inačica,
- `QT 3.1.x, 3.2.x, 3.3.x`.

Ukoliko se navedene biblioteke i aplikacije instaliraju iz distribucijskih RPM paketa, uz njih je potrebno instalirati i razvojne (eng. *development*) RPM pakete (npr. `libxml2-devel`). Kod SuSE Linux distribucije dodatno je potrebno instalirati i `elfutils-libelf` i `elfutils-libelf-devel` pakete, kako bi instalacija Firewall Builder-a protekla nesmetano.

Za instalaciju Firewall Builder alata potrebno je dohvatiti dva paketa, `libfwbuilder-2.0.0.tar.gz` i `fwbuilder-2.0.0.tar.gz` i otpakirati ih u proizvoljne direktorije. Nakon toga, u svakom od kreiranih direktorija potrebno je redom izvršiti sljedeće naredbe:

```
#./autogen.sh
#make
#make install
```

Prilikom postupka instalacije, biblioteke se automatski kopiraju u `/usr/local/lib` direktorij, dok se binarne datoteke smještaju unutar `/usr/local/bin` direktorija.

Za ispravno pokretanje programa potrebno je pobrinuti se da je `/usr/local/lib` direktorij naveden unutar `LD_LIBRARY_PATH` varijable okoline ili unutar `/etc/ld.so.conf` datoteke. U protivnom, aplikacija neće biti u mogućnosti učitati dinamičke biblioteke.

Biblioteke i binarne datoteke aplikacije moguće je instalirati i na proizvoljnu lokaciju, specificiranjem prefiksa direktorija prilikom pokretanja konfiguracijske skripte.

```
./autogen.sh --prefix="/opt"
```

U navedenom primjeru, biblioteke će se instalirati u `/opt/lib`, a binarne datoteke u `/opt/bin` direktorij.

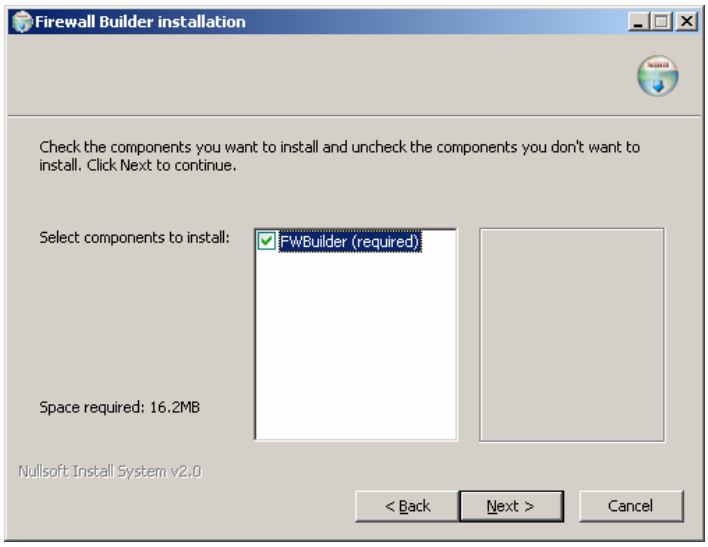
## 2.1. Instalacija RPM paketa

Gotovi RPM paketi dostupni su za SuSE, Mandrake, Fedora i RedHat 9 sustave, dok je paket za Debian Linux uključen u samoj distribuciji. Kao preduvjet za uspješnu instalaciju RPM paketa, također je potrebno instalirati sve gore navedene pakete, osim razvojnih inačica paketa.

## 2.2. Instalacija na Microsoft Windows operacijskim sustavima

Na Windows operacijskim sustavima paket se instalira dvostrukim klikom miša na instalacijsku arhivu, koja pokreće automatski postupak instalacije (Slika 1). Korisniku je na izbor ponuđen odabir

direktorija unutar kojega će se program instalirati. Instalacijska arhiva, koju je moguće dohvatiti s web stranica projekta, namijenjena je evaluaciji, te nakon perioda od 30 dana potrebno kupiti licencu za korištenje ove aplikacije na komercijalnom operacijskom sustavu (1.2).

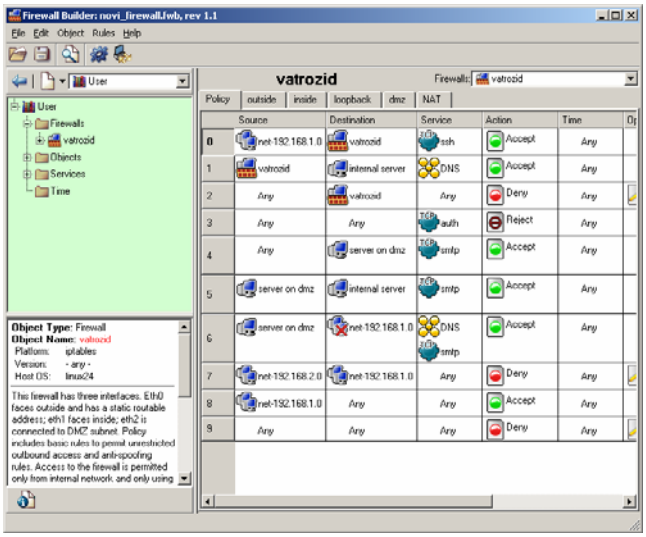



**Slika 1:** Instalacijski prozor Firewall Builder alata

Potrebno je napomenuti da osim vremenskog ograničenja, evaluacijska inačica programa za Windows operacijske sustave ne sadrži nikakva druga ograničenja koja bi se ticala funkcionalnosti programa.

# 3. Sučelje alata

Nakon pokretanja Firewall Builder-a, otvara se glavni prozor aplikacije (Slika 2) koji je podijeljen u dva dijela. U lijevom dijelu prozora nalazi se hijerarhijska struktura objekata, dok se u desnom dijelu prozora prikazuju parametri odabranog vatrozida. Na slici je prikazan izgled objekta pod nazivom "vatrozid", koji predstavlja testni vatrozid izrađen za potrebe pisanja ovog dokumenta. U desnom dijelu prozora vidljiva su sva pravila filtriranja prometa definirana za ovaj vatrozid.




**Slika 2:** Glavni prozor alata

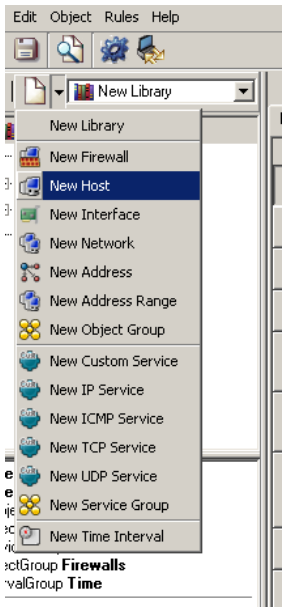
Unutar programa ugrađena je opcija istovremenog rada na konfiguraciji više vatrozidova. U desnom prozoru programa iz padajućeg izbornika *Firewalls*, moguće je odabrati prikaz bilo kojeg od definiranih vatrozidova. Budući da svi vatrozidi koriste zajedničku bazu objekata, promjene na objektu jednog od vatrozida odrazit će se i na ostalima.

## 3.1. Objektno stablo

Objektno stablo koje se nalazi na lijevoj strani prozora, omogućuje grupiranje objekata prema tipu i, na taj način, njegovo svrstavanje u hijerarhiju objekata. U samom vrhu hijerarhije, objekti su grupirani u četiri grupe: *Firewalls*, *Objects*, *Services* i *Time*. Unutar grupe *Firewalls*, nalaze se svi vatrozidovi na kojima se trenutno radi, odnosno čija konfiguracija se nalazi unutar učitane konfiguracijske datoteke. Svi mrežni objekti poput računala, mreža, adresnih prostora, nalaze se u grupi *Objects*, dok se mrežni servisi nalaze unutar grupe *Services*. Grupa *Time* sadrži definicije svih vremenskih intervala kojima je moguće kontrolirati primjenu pojedinih pravila. Novi objekt se prilikom kreiranja automatski svrstava u pripadajuću grupu.

Osim korisničkog stabla, pomoću padajućeg izbornika u lijevom dijelu prozora, moguće je odabrati i stabla objekata pod nazivom *Standard* i *Firewall Templates*. U tim stablima nalaze se predefinirani objekti i predlošci za standardne konfiguracije vatrozida. Unutar ovih stabala nije moguće kreirati objekte niti raditi izmjene nad postojećim objektima, već se objekti definirani u njima koriste kao predložak za izradu vlastite baze objekata ili vatrozida. Kopiranje objekata iz standardnih stabala u korisničko stablo moguće je izvesti pomoću klasičnih "*Copy/Paste*" operacija.

Novi objekt moguće je kreirati unutar izbornika *Object -> New Object*, nakon čeka se otvara padajući izbornik koji nudi izbor tipa objekta koji se želi kreirati (Slika 3). Osim objekta, korisnik je u mogućnosti kreirati i novo stablo objekata (opcija *New Library*), koje se po potrebi može spremiti u datoteku i učitati u bilo kojem aktivnom projektu. Stabla se spremaju i učitavaju pomoću opcija *Import Library* i *Export Library* iz *File* izbornika.




**Slika 3:** Kreiranje novog objekta ili stabla objekata

## 3.2. Opcije za podešavanje sučelja

Parametri koji određuju ponašanje sučelja nalaze se unutar *Edit->Preferences* izbornika. Kao važnije parametre treba izdvojiti sljedeće:

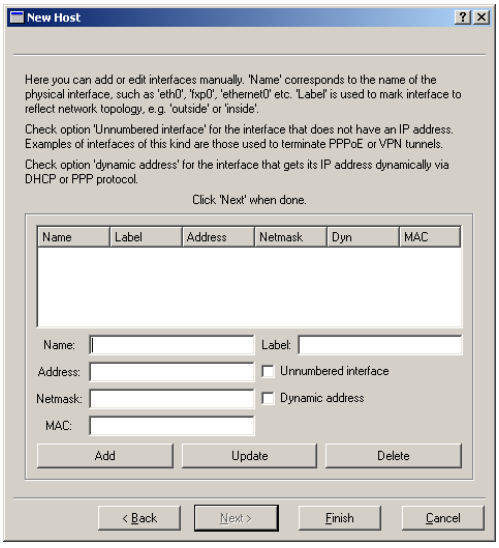
- *General -> Working Directory* – ova opcija određuje radni direktorij programa. Unutar ovog direktorija pohranjuje datoteka koja definira vatrozid ("*data file*") i sve datoteke koje nastaju postupkom prevođenja pravila. Ukoliko je parametar ostavljen prazan, program će koristiti `/home` direktorij korisnika ili direktorij iz kojega je učitana trenutno aktivna konfiguracija vatrozida.
- *General -> Automatically save data in dialogs while switching between objects* – svaki otvoreni objekt prikazan je u desnoj strani glavnog prozora. Prilikom otvaranja novog objekta, program automatski pita korisnika da li želi snimiti eventualne izmjene načinjene na prethodno korištenom objektu. Uključivanjem ove opcije, program prilikom promjene objekta automatski snima sve načinjene promjene, bez potrebe za interakcijom korisnika.
- *SSH* – unutar ovog izbornika upisuju se lokacije "*Secure Shell*" i "*Secure Copy*" aplikacija na sustavu, pomoću kojih Firewall Builder kopira gotovu konfiguraciju vatrozida na udaljeno računalo.
- *Libraries* – ranije spomenuta stabla s hijerarhijskom strukturom objekata, u ovom alatu nazivaju se *Libraries*. Korisnički definirana stabla moguće je pomoću ovog izbornika automatski učitati prilikom pokretanja programa.

# 4. Rad s objektima

Kao što je u uvodu spomenuto, Firewall Builder koristi objektni pristup kreiranju vatrozida. Zbog toga je prije kreiranja vatrozida potrebno kreirati objekte koji predstavljaju računala na mreži, samu mrežu, kao i objekte koji predstavljaju pojedine mrežne servise. Tipovi objekata koje je u ovoj aplikaciji moguće definirati i njihove osnovne karakteristike opisani su u nastavku.

## 4.1. *Host* objekt

Ovaj objekt predstavlja računala spojena na mrežu, točnije bilo koje desktop računalo, poslužitelj ili mrežni uređaj. Općenito, *host* objektom podrazumijeva se bilo koji element računalne mreže koji posjeduje mrežno sučelje i IP adresu. Naravno, svaki *host* objekt može imati više mrežnih sučelja koja ne moraju nužno fizički postojati na računalu (npr. virtualna sučelja).
Proces dodavanja novog *host* objekta izveden je pomoću "čarobnjaka", koji od korisnika prikuplja sve podatke potrebne za kreiranje novog objekta.
Osnovni podaci koje korisnik treba unijeti su ime objekta (ne mora odgovarati FQDN imenu računala), IP adresu mrežnog sučelja i opcionalno je moguće navesti MAC adresu mrežnog sučelja (Slika 4). Broj mrežnih sučelja nije ograničen, tako da je moguće dodati proizvoljno mnogo sučelja jednom *host* objektu. Ovdje je potrebno napomenuti da *host* objekt ne može sadržavati nikakva pravila za filtriranje prometa ili NAT (eng. *network address translation*), već je to isključivo svojstvo *firewall* objekta.




**Slika 4:** Definiranje mrežnih sučelja host objekta

Jednom kreirani *host* objekt može se naknadno uređivati tako da se dvostrukim klikom miša na objekt uključi prozor za izmjenu objekta. Parametri koje je moguće mijenjati su:

- *Name* – ime *host* objekta.
- *MAC matching* – ukoliko je ova opcija omogućena, prevodilac koji kreira pravila za vatrozid, prilikom prevođenja će koristiti MAC adrese sučelja umjesto IP adresa.
- *SNMP community* – ime SNMP zajednice koje se, u slučaju da je na računalu pokrenut SNMP agent, koristi za prikupljanje dodatnih podataka o sustavu. Ukoliko na udaljenom računalu nije instaliran SNMP agent, ovo polje može biti prazno.
- *Comment* – u ovo polje moguće je unijeti proizvoljni tekst koji pobliže opisuje objekt.

### 4.1.1. *Interface* objekt

Sva mrežna sučelja koja su definirana za pojedini *host* objekt definirana su kao posebni *interface* objekti koji se u hijerarhiji nalaze jednu razinu niže od *host* objekta. Adrese pojedinih sučelja tretiraju se kao *address* objekti i smještaju razinu niže u odnosu na *interface* objekte. *Interface* objekti, isto kao i *host* objekti, sadrže ime, komentar koji ih pobliže opisuje i oznaku objekta. Uz te podatke, moguće je birati između četiri opcije koje pobliže opisuju tip objekta, a tipovi *interface* objekata su: *regular*, *dynamic*, *unnumbered* i *management*.

*Regular interface* predstavlja klasično mrežno sučelje sa statički definiranom IP adresom, koja se ne planira mijenjati tokom vremena. Takvu adresu Firewall builder može izravno koristiti prilikom kreiranja pravila vatrozida.

*Dynamic interface* posjeduje dinamički dodijeljenu IP adresu (npr. DHCP ili PPP protokolom), što podrazumijeva da ta adresa nije poznata prilikom kreiranja pravila vatrozida i ona se ne koristi od strane prevodioca. Ipak, određeni vatrozidi, poput OpenBSD PF i Netfilter-a dozvoljavaju definiranje dinamičkih sučelja, čije se adrese definiraju prilikom učitavanja politike vatrozida ili čak tijekom njegovog rada.

Pod *Unnumbered* sučeljima smatraju se ona koja u pravilu nikada ne posjeduju IP adresu. Kao primjeri takvih sučelja mogu se navesti krajnje točke kod protokola za tuneliranje (npr. GRE, PPPoE, ...) ili sučelja na premosnicima (eng, *bridge*).. Firewall Builder takva sučelja ignorira i nikada ih ne uključuje u politiku vatrozida.

Ukoliko se sučelje dodatno označi kao *Management* sučelje, Firewall Builder će ga koristiti za komunikaciju s računalom. Trenutno je ta komunikacija ograničena na SNMP protokol kojim se dohvaćaju informacije o udaljenom računalu.

### 4.1.2. *Address* objekt

*Address* objekt, koji se u hijerarhiji nalazi ispod *Interface* objekta, opisuje IP adresu sučelja. Ovaj objekt sadrži ime sučelja, njegovu IP adresu i kratak opis objekta. Trenutno je podržano isključivo IPv4 adresiranje, iako se u budućnosti planira podrška za IPv6 adrese. *Address* objekt može biti i fizički, npr. može sadržavati MAC adresu sučelja, ali u tom slučaju potrebno je znati da samo ograničen broj vatrozida podržava filtriranje prema fizičkim adresama sučelja. Konkretno, od platformi koje podržava Firewall Builder, jedino je Netfilter vatrozid sposoban provoditi filtriranje prema fizičkim adresama sučelja.

## 4.2. *Network* objekt

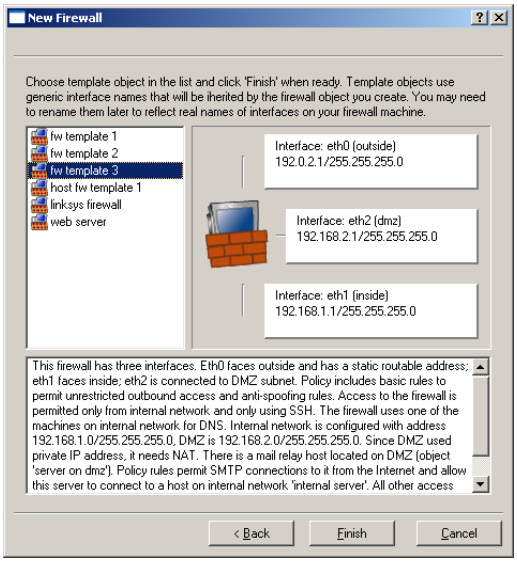
*Network* objekt opisuje raspon adresa određene računalne mreže, koji će se kasnije koristiti prilikom kreiranja pravila za filtriranje mrežnih paketa. Ovaj objekt sadrži adresu mreže i mrežnu masku pomoću koje se automatski računa raspon IP adresa koji zadana mreža obuhvaća.

## 4.3. *Address Range* objekt

Ukoliko se, umjesto cijele računalne mreže, želi definirati samo određeni raspon adresa koji definira računala nad kojima će se provoditi identična pravila filtriranja mrežnog prometa, koristi se *Address Range* objekt. U polja ovog objekta upisuju se početna i završna adresa adresnog raspona, s time da su i te adrese uključene u isti.

## 4.4. *Firewall* objekt

*Firewall* objekt predstavlja sam vatrozid te se, slično kao i *host* objekt, kreira se pomoću čarobnjaka. Korisniku je nakon unosa imena vatrozida i platforme za koju se vatrozid kreira (Iptables, PF, Ipfilter, PIX), na izbor ponuđeno nekoliko najčešće korištenih konfiguracija vatrozida (Slika 5). U većini slučajeva ponuđene konfiguracije, uz manje izmjene, u potpunosti zadovoljavaju potrebe filtriranja prometa za tipične računalne mreže. Naravno, ukoliko se korisnik na to odluči, ostavljena je i mogućnost proizvoljne konfiguracije vatrozida.

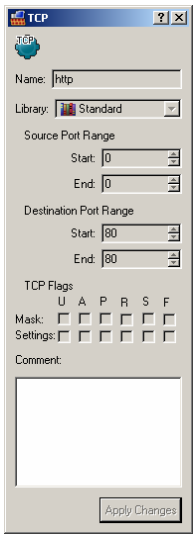



**Slika 5:** Odabir uobičajenih konfiguracija vatrozida

Slika 5 prikazuje gotovu konfiguraciju vatrozida pod nazivom "*fw template 3*", koja ima definirana tri mrežna sučelja. Prvo sučelje (`eth0`) koristi se za spajanje na javnu mrežu (Internet), sučelje `eth1` povezuje vatrozid s internom mrežom, dok je sučelje `eth2` spojeno na DMZ podmrežu na kojoj se nalaze poslužitelji koji moraju biti dostupni s javne mreže.
Inicijalne politike ovog vatrozida podešene su tako da ne propuštaju promet s Interneta na internu mrežu, već da isključivo dopuštaju pristup e-mail poslužitelju u DMZ podmreži. Konfiguracijskom sučelju vatrozida (SSH protokol) pristup je dozvoljen isključivo s interne mreže.

## 4.5. *Service* objekti

Kako bi se filtriranje prometa moglo provoditi prema pojedinim servisima, definiraju se *Service* objekti. Firewall Builder inicijalno nudi standardne tipove objekata za najčešće korištene protokole, kao što su ICMP, UDP i TCP protokoli.
Za svaki od navedenih protokola, moguće je definirati objekte koji predstavljaju pojedine računalne servise koji koriste navedene protokole. Tako bi se na primjer web servis definirao kao TCP Service objekt koji dozvoljava promet na dolazni port 80 (Slika 6).




**Slika 6:** Parametri TCP Service objekta za web poslužitelj

Velik broj unaprijed definiranih objekata (oko stotinjak) već se nalazi unutar Firewall Builder-a i u potpunosti zadovoljava većinu potreba koje mogu imati administratori malih i srednjih računalnih

mreža. U slučaju da potrebni servis nije unaprijed definiran, uvijek postoji mogućnost ručnog definiranja parametara istog.

### 4.6. *Time interval* objekt

Osim objekata koji definiraju računala koja se nalaze na mreži, samih vatrozida i objekata koji predstavljaju mrežne servise, Firewall Builder dozvoljava i definiciju posebnih objekata koji definiraju vremenske intervale.
Ovi objekti koriste se za uključivanje i isključivanje pravila za filtriranje mrežnog prometa, ovisno o definiranim vremenskim intervalima. Tako je na primjer određena pravila za filtriranje prometa moguće primijeniti isključivo npr. za vrijeme radnog vremena ili vikendima.

## 5. Kreiranje vatrozida

Nakon kreiranja svih potrebnih objekata, potrebno je detaljnije podesiti *firewall* objekte, odnosno definirati pravila filtriranja prometa, nakon čega modul za prevođenje transformira pravila u oblik pogodan za instalaciju vatrozida na sustav.

### 5.1. Kreiranje politika

Uz svaki *firewall* objekt, koji predstavlja stvaran vatrozid, povezan je niz politika koje definiraju način na koji se paketi usmjeravaju. Kada se u hijerarhijskom stablu odabere *firewall* objekt, u desnom dijelu ekrana mogu se vidjeti politike vatrozida, tj. pojedina pravila. Paketi se analiziraju tako da se uspoređuju s pravilima politike i ukoliko paket odgovara nekom od pravila, to pravilo se primjenjuje. Važno je napomenuti da se uspoređivanje provodi onim redoslijedom kojim su pravila definirana, te da se kao važeće uzima prvo pravilo kojem paket odgovara. Politike za usmjeravanje se općenito mogu svrstati u tri grupe:

- **Globalna politika** (eng. *global policy*) – upravlja prometom na svim mrežnim sučeljima i definira način na koji se pristupa računalima iza vatrozida.
- **Politike sučelja** (eng. *interface policies*) – jednako kao i globalna politika, politike sučelja definiraju način na koji se pristupa računalima iza vatrozida, ali na razini pojedinih sučelja.
- **NAT pravila** (eng. *network address translation rules*) – NAT pravila opisuju način na koji se na vatrozidu transformiraju adrese i mrežni portovi paketa koji prolaze sa interne mreže na vanjsku i obratno.

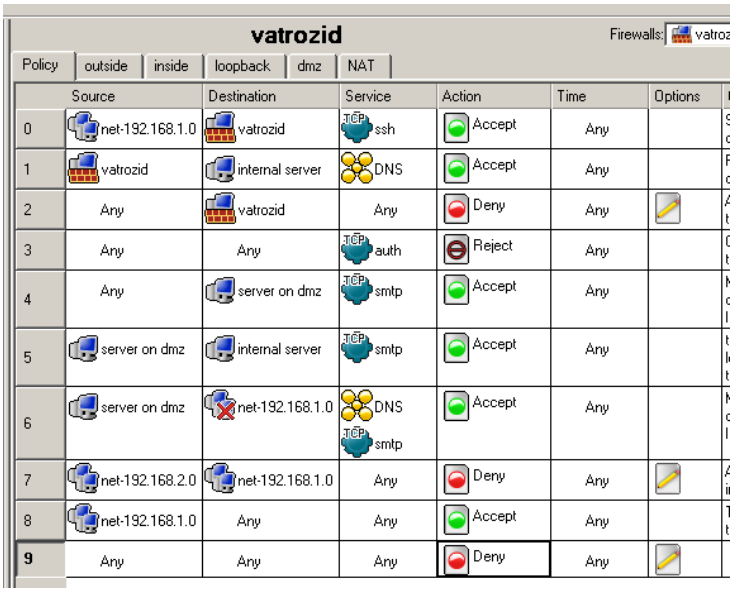
Slika 7 prikazuje logički slijed na koji se definirana pravila primjenjuju nad paketima koji dolaze na vatrozid. Konačna pravila koja prevodilac generira mogu se razlikovati u odnosu na ovaj redoslijed, ovisno o platformi na kojoj se vatrozid implementira. Bez obzira na to, vatrozid u Fireall Builderu treba kreirati u skladu s navedenim redoslijedom pravila.


**Slika 7:** Redoslijed primjene pravila za filtriranje paketa

Svako pravilo ima definiran objekt koji je izvor paketa (eng. *source*), odredišni objekt (eng. *destination*) i pripadajući servis (eng. *service*). Izraz Any u bilo kojem od ovih parametara pravila definira bilo koji objekt. Kao rezultat primjene pravila slijede sljedeće akcije od strane vatrozida:

- *Accept* – paket koji sadrži izvornu, odredišnu adresu koja odgovara pravilu i namijenjen je mrežnom servisu koji je također definiran u pravilu, propušta se kroz vatrozid.
- *Deny* – ukoliko se sadržaj paketa odgovara pravilu za koje je definirana *Deny* akcija vatrozida, paket se jednostavno ispušta i ne dolazi na krajnju destinaciju.
- *Reject* – ova akcija slična je *Deny* akciji ali se, uz odbacivanje paketa, pošiljaocu šalje odgovarajući ICMP paket koji ga obavještava da je paket odbijen.

Smjer dolaska i odlaska paketa definira se iz perspektive računala na kojem je instaliran vatrozid. Tako se na primjer paketi koji s interne mreže dolaze na interno mrežno sučelje vatrozida smatraju ulaznima, a paketi koji dolaze s vanjske mreže (Internet) na internom sučelju smatraju izlaznim paketima. Obrnuta situacija je na vanjskom sučelju vatrozida, gdje se paketi s interne mreže smatraju izlaznima, a paketi s vanjske mreže ulaznima.

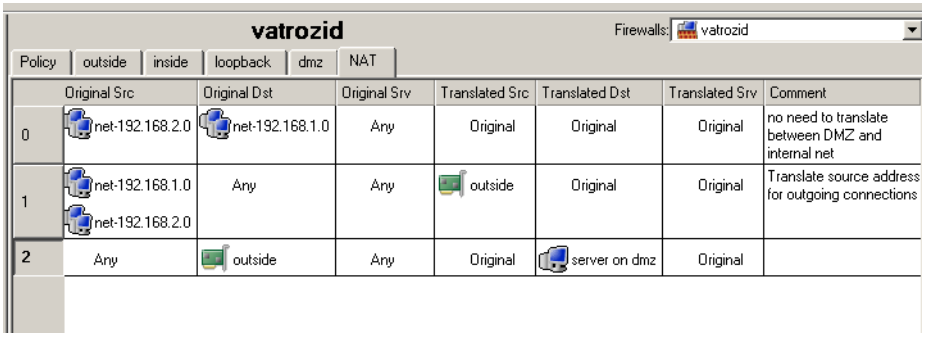



**Slika 8:** Pravila za filtriranje paketa

Na Slici 8 prikazana su pravila filtriranja mrežnog prometa za *firewall* objekt opisan u prethodnom poglavlju. Potrebno je primijetiti da je posljednje pravilo izvedeno tako da odbacuje sve pakete tj. bilo koji paket koji ne odgovara gornjim pravilima automatski se odbacuje. Na taj način, u slučaju krivo podešenih pravila, ne može se dogoditi da vatrozid propušta pakete koji ne odgovaraju niti jednom od pravila.

## 5.2. NAT

Jednako kao i kod politika za filtriranje paketa, pravila za prevođenje adresa pregledavaju se redoslijedom kojim su definirana u NAT politici. Prvo pravilo kojem paket odgovara, primijeniti će se za transformaciju adrese. NAT pravila je moguće pregledavati pomoću kartice NAT u desnom dijelu ekrana (Slika 9).




**Slika 9:** NAT pravila vatrozida

Novo pravilo dodaje se desnim klikom miša na traku na kojoj se nalaze redni brojevi pravila i odabirom opcije *Insert Rule*. Elementi svakog pravila su sljedeći:

- *Original Source* – objekt koji sadrži izvorišnu adresu paketa,
- *Original Destination* – objekt koji sadrži originalnu odredišnu adresu (prije translacije) paketa,
- *Original Service* – *service* objekt čijem portu odgovara originalni paket,
- *Translated Source* – ovaj objekt definira izvorišnu adresu koju će paket imati nakon postupka transformacije adrese,
- *Translated Destination* – definira odredišnu adresu transformiranog paketa,
- *Translated Service* – definira protokol i brojeve portova kojima će se zamijeniti isti parametri u originalnom paketu.

Kao primjer mogu se uzeti pravila sa slike 8. Prvo pravilo odnosi se na pakete kojima je izvor DMZ sučelje, a odredište interna mreža, s time da se u obzir uzimaju svi portovi i svi servisi. Budući da obje mreže koriste privatnu klasu IP adresa, nema potrebe za transformacijom adresa, odnosno transformirani paket biti će identičan originalnom. Drugo pravilo transformira sve pakete koji sa internih i DMZ sučelja idu prema Internetu, na taj način da se izvorišne adrese mijenjaju s adresom vanjskog mrežnog sučelja. Treće pravilo prosljeđuje sve pakete koji dolaze sa Interneta, na poslužitelj koji se nalazi u DMZ mreži.

## 5.3. Prevođenje pravila i instalacija vatrozida

Ispravno konfiguriran vatrozid se, pomoću posebnih modula, prevodi u oblik pogodan za instalaciju na sustav na kojem se vatrozid fizički nalazi. Modul za prevođenje aktivira se unutar izbornika *Rules*, odabirom opcije *Compile*. Kao rezultat, u `/home` direktoriju korisnika (ukoliko drugačije nije definirano) kreirati će se *shell* skripta s pravilima za konfiguraciju vatrozida. Skriptu je potrebno pokrenuti na operacijskom sustavu na kojem se nalazi vatrozid, kako bi se pravila učitala u mehanizam za filtriranje prometa.

Ukoliko na računalu na kojem je pokrenut Firewall Builder postoje *Secure Shell* i *Secure File Copy* klijenti, odabirom opcije *Rules->Install*, moguće je skriptu automatski instalirati na udaljeno računalo. Podešavanje Firewall Builder-a za rad sa *Secure Shell* i *Secure File Copy* klijentima opisano je u poglavlju 3.2.

# 6. Zaključak

Firewall Builder predstavlja vrlo dobar grafički alat za izradu pravila filtriranja prometa koji administratorima u velikoj mjeri olakšava izradu i održavanje vatrozidova temeljenih na Linux i FreeBSD operacijskim sustavima. Mnoštvo naprednih opcija i "čarobnjaka" omogućavaju brzo kreiranje jednostavnih vatrozidnih pravila, bez potrebe za dubljim razumijevanjem alata za filtriranje prometa (iptebles, pf i sl.) i učenjem pravila za njihovu konfiguraciju. Objektni pristup izradi pravila vatrozida do punog izražaja dolazi kod upotrebe ovog alata na velikim računalnim mrežama s višestrukim vatrozidovima, gdje je u slučaju promjena konfiguracije mreže dovoljno promijeniti parametre odgovarajućih objekata i generirati nova pravila za sve vatrozide.

Podrška za više tipova vatrozida, čini ovaj alat idealnim za upotrebu u heterogenim mrežama, budući da je sve karakteristike vatrozida kreiranog u grafičkom sučelju u potpunosti moguće prenijeti na bilo koji od podržanih operacijskih sustava ili uređaja.

Ipak, bez obzira na sve prednosti koje ovakav pristup izradi vatrozida nudi, u kritičnim primjenama potrebno je ručno pregledati pravila koje alat generira i uočiti eventualne propuste. Također, potrebno je redovito pratiti službene web stranice ovog projekta i u slučaju otkrivenih propusta u programskom kodu zaduženom za generiranje pravila, nadograditi alat ispravljenom inačicom.