HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Firestarter vatrozida

CCERT-PUBDOC-2006-07-161

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.

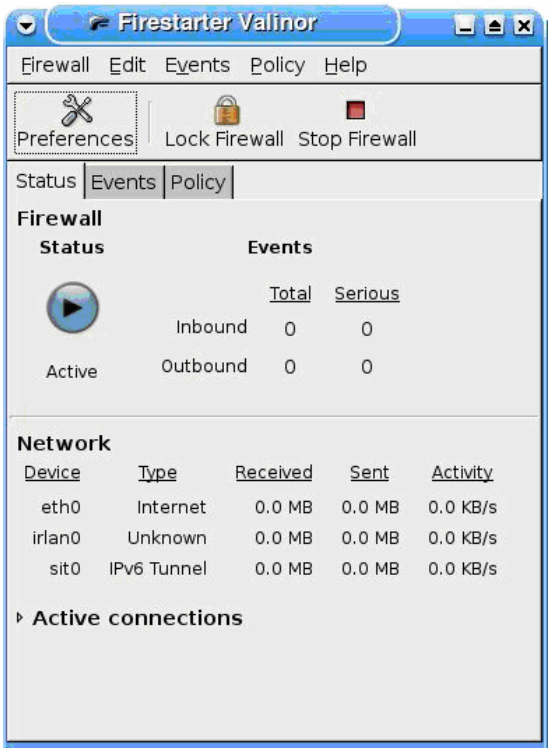
CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

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

Zbog sve veće dostupnosti širokopojasnog Interneta i činjenice da je sve veći broj računala stalno priključen na Internet, sve je veća i potreba za zaštitom računala. Obzirom da prosječni korisnici ne raspolažu dovoljnim znanjem za konfiguraciju složenih vatrozida koji se uobičajeno koriste na poslužiteljskim računalima i većim mrežama, pojavljuje se potreba za jednostavnim, a opet i učinkovitim vatrozidima koji mogu efikasno zaštiti prosječnog korisnika. Posebno su zanimljivi vatrozidi koji ne zahtijevaju nikakve dodatne financijske troškove za krajnjeg korisnika. U takvoj situaciji sve je veći broj vatrozida baziranih na Linux operacijskom sustavu.
Jedan od najzastupljenijih vatrozida u tom segmentu je Firestarter. U ovom dokumentu opisane su glavne karakteristike vatrozida, instalacija te njegova konfiguracija.



Slika 1: Grafičko sučelje Firestarter vatrozida

2. Firestarter vatrozid

Firestarter je grafički vatrozid otvorenog koda namijenjen Linux operacijskim sustavima. Program je razvijen sa ciljem kombiniranja jednostavnosti korištenja te brojnim mogućnostima rada. Firestarter je u osnovi samo grafičko sučelje za konfiguriranje standardnog IP Tables alata koji je sastavni dio jezgre Linux operacijskih sustava (eng. *kernel*).

2.1. Funkcionalnosti Firestarter vatrozida

Pošto je Firestarter zasnovan na korištenju IP Tables alata, Firestarter podržava *Stateful inspection* način filtriranja mrežnih paketa. *Stateful inspection* filtriranje bazira se na kontinuiranom praćenju i analizi pojedinih segmenata paketa koji prolaze kroz vatrozid kako bi se na temelju njih u stvarnom vremenu mogle donositi pravilne odluke o filtriranju paketa. Ovakvim načinom rada vatrozid je u stanju automatski prosljeđivati mrežne pakete koji su dio uspostavljenih konekcija pri čemu se na mrežne pakete koji predstavljaju započinjanje mrežnih konekcija, primjenjuju definirana pravila prosljeđivanja ili odbacivanja mrežnih paketa.

IP Tables alat između ostalog pruža i funkcionalnost NAT (engl. *Network Address Translation*) tehnologije. NAT tehnologija omogućuje istovremeno dijeljene Internet veze između više korisnika pri čemu se lokalnim računalima, koja posjeduju privatne IP adrese, zamjenjuju izvorne IP adrese s vanjskom IP adresom vatrozida preko koje vatrozid komunicira na Internetu. Zahvaljujući ovoj funkcionalnosti, Firestarter se ne mora nužno koristiti samo za zaštitu krajnjeg korisnika već i za zaštitu unutarnjih mreža.

U slučaju da je dijeljena Internet veza *dial-up* tipa, vatrozid će automatski biti konfiguriran s opcijom maskiranja (eng. *Masquearading*) IP adresa računala iz unutarnje mreže. Ta opcija je za *dial-up* konekcije i najpogodnija jer maskiranje zamjenjuje privatne IP adrese s IP adresom koja je pridijeljena mrežnom sučelju, a zbog korištenja *dial-up* veze dodijeljena IP adresa neće uvijek biti ista. Ukoliko je veza ostvarena preko mrežnog sučelja, na vatrozidu će se konfigurirati SNAT (eng. *Source NAT*) koji, nasuprot maskiranju, uvijek zamjenjuje IP adrese računala iz unutarnje mreže s točno definiranom IP adresom. Također, na Firestarter vatrozidu je moguće definirati i DNAT (eng. *Destination NAT*) pravila koja zamjenjuju ciljnu IP adresu u mrežnim paketima s definiranom IP adresom. Funkcionalnost DNAT-a se najčešće koristi u slučajevima kad su poslužitelji pozicionirani u unutarnjoj mreži te koriste privatne IP adrese. U tom slučaju korisnici pristupaju njihovim uslugama na način da iste zahtijevaju od vatrozida. Vatrozid, na temelju definiranih DNAT pravila, prosljeđuje zaprimljene zahtjeve na ciljne poslužitelje. Čim vatrozid primi određeni zahtjev na određeni port, vatrozid automatski prosljeđuje zahtjev na ciljani poslužitelj. Ipak, Firestarter ne podržava DNAT oblik mapiranja IP adresa „jedan na jedan“ gdje se na vanjskom mrežnom sučelju nalazi veći broj IP adresa pri čemu se zahtjevi na točno određenu IP adresu prosljeđuju na ciljani poslužitelj.

Nažalost, *Virtual Private Networks* (VPN) tehnologija nije podržana od strane trenutne inačice (1.0) Firestarter vatrozida. VPN je danas neizostavan element većine vatrozida jer omogućava sigurno povezivanje udaljenih korisnika putem nesigurnog medija, kao što je Internet, pri čemu je moguće međusobno povezivanje udaljenih lokalnih računalnih mreža (LAN-to-LAN VPN) te povezivanje udaljenih mobilnih korisnika sa centralnim lokacijama putem *dial-up* ili neke druge veze. Korištenjem VPN tehnologije moguće je kreiranje sigurnog kanala (eng. *tunnel*) između udaljenih lokacija, gdje se kompletni promet enkripcijom štiti od neovlaštenog promatranja. Zbog ovih veoma korisnih mogućnosti koje VPN pruža, proizvođači Firestarter vatrozida opisali su na koji se način spomenuta funkcionalnost ipak može ostvariti u trenutnoj inačici vatrozida. U tu svrhu potrebno je ručno mijenjati `/etc/firestarter/user-pre` datoteku. Detaljnije informacije moguće je pronaći u izvornoj dokumentaciji [2], a potpuna podrška za VPN funkcionalnost najavljena je za inačicu 1.1.

Log zapisi su svakako jedna od važnijih komponenti svakog vatrozida. Oni omogućuju detekciju neovlaštenih radnji te pružaju dodatne mogućnosti za nadzor aktivnosti u mreži. Nažalost, Firestarter nema podršku za logiranje bilo dolaznih bilo odlaznih konekcija već samo pruža mogućnost ispisa blokiranih konekcija na *Events* stranici programskog sučelja. Radi bolje preglednosti taj popis je moguće spremiti u zasebnu tekstualnu datoteku. Također, Firestarter ne pruža podršku za alarmiranje administratora o neuobičajenim aktivnostima, tj. ne postoji način kojim bi se administratora moglo obavijestiti kako se nešto neuobičajeno događa na vatrozidu poput određenih oblika mrežnih napada.

Iako vatrozid ne posjeduje funkcionalnosti logiranja i VPN-a, vatrozid ipak predstavlja dobro programsko rješenje za korisnike. Time pridonose i brojne karakteristike vatrozida od kojih su i sljedeće:

- jednostavno grafičko sučelje za konfiguriranje vatrozida,
- programski čarobnjak (eng. *wizard*) za osnovno podešavanje prilikom prvog pokretanja,
- pregled događaja na vatrozidu u stvarnom vremenu,
- podrška za podešavanje ICMP parametara za sprečavanje DoS napada,
- mogućnost pokretanja korisničkih skripti neposredno prije ili nakon pokretanja vatrozida,
- pregled aktivnih mrežnih konekcija,
- administracijsko sučelje dostupno na velikom broju jezika (preko trideset), itd...

3. Instalacija

Firestarter dolazi u obliku standardnog instalacijskog paketa za većinu popularnih Linux distribucija (Debian, Ubuntu, Fedora Core, Red Hat, SuSE, Gentoo, Mandrake) pa ga većina korisnika može instalirati pomoću programa za upravljanje paketima korištenim u njihovim odabranim Linux distribucijama. Korisnici distribucija za koje ne postoje paketi mogu Firestarter instalirati i iz izvornog koda koji je moguće preuzeti u obliku tar.gz datoteka ili rpm paketa raspoloživih na stranicama proizvođača [1].

Proces instalacije iz izvornog koda ne razlikuje se od uobičajenog postupka. Nakon raspakiravanja koda potrebno je pokrenuti `configure` skriptu u direktoriju u kojem se nalazi izvorni kod. Najčešće nije potrebno dodavati nikakve dodatne opcije konfiguracijskoj skripti, ali za slučaj u kojem je potrebno nešto dodatno izmijeniti, popis svih opcija moguće je dobiti pomoću `configure --help` naredbe. Nakon uspješnog konfiguriranja, programski kod je potrebno prevesti naredbom `make`, a zatim ga i instalirati naredbom `make install`.

Prilikom instalacije iz paketa, program se automatski registrira kao servis pa je vatrozid aktivan i u slučaju kad je grafički dio vatrozida ugašen. Za postizanje iste funkcionalnosti prilikom instaliranja iz izvornog koda, potrebno je instalirati sistemsku `init` skriptu. U direktoriju s izvornim kodom nalazi se primjer jedne `init` skripte koju je potrebno kopirati u `/etc/init.d/` direktorij te ju eventualno dodatno prilagoditi. Nakon instalacije skripte preostaje definiranje sustava na način da isti koristi novu skriptu. Način na koji se to izvodi ovisi o korištenoj distribuciji te izlazi izvan opsega ovog dokumenta.

4. Konfiguracija

Konfiguriranje Firestarter vatrozida se u potpunosti obavlja preko njegovog grafičkog sučelja. Osnovne parametre potrebne za rad definiraju se preko programskog čarobnjaka koji se pokreće kod prvog pokretanja vatrozida. Detaljnija konfiguracija vrši se kroz četiri osnovna dijela grafičkog sučelja:

- *Status* – stranica za prikaz statusnih informacija o vatrozidu, mrežnom prometu i trenutnim vezama,
- *Events* – stranica za prikaz blokiranih veza koje je moguće deblokirati,
- *Policy* – stranica za definiranje pravila propuštanja mrežnih paketa, i
- *Preferences* – stranica koja sadrži dodatne opcije vezane uz ponašanje grafičkog sučelja i vatrozida.

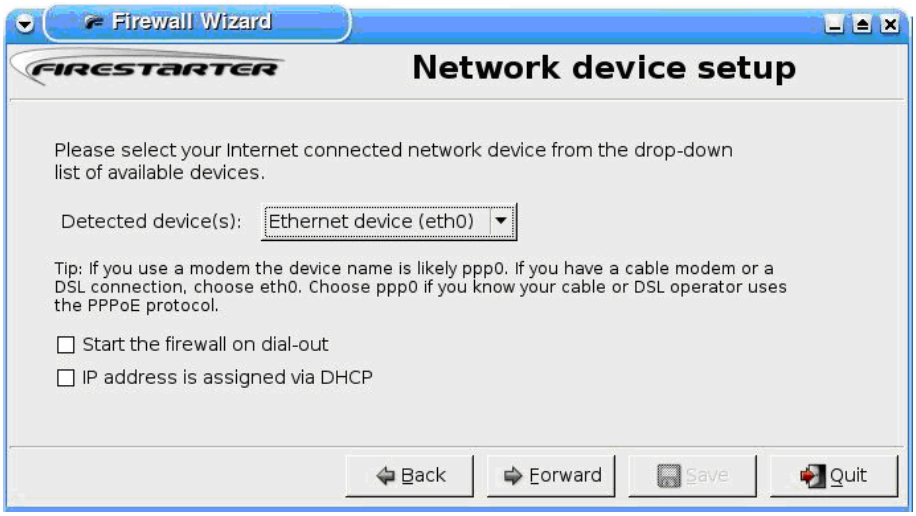
4.1. Konfiguriranje pomoću programskog čarobnjaka

Prilikom prvog pokretanja Firestarter vatrozida automatski se pokreće i programski čarobnjak namijenjen podešavanju osnovnih postavki vatrozida.

U prvom koraku podešavanja potrebno je odabrati mrežni uređaj preko kojeg je računalo spojeno na Internet. Također su dostupne dodatne dvije mogućnosti:

- *Start the Firewall on dial-out* – ukoliko veza prema Internetu nije stalna već ju je potrebno uspostavljati prema potrebi uključivanjem ove opcije Firestarter će ponovo učitati pravila vatrozida prilikom svakog podizanja veze prema Internetu,

- *IP address is assigned via DHCP* – ovu opciju je potrebno uključiti ukoliko mrežno sučelje, koje je povezano na Internet, svoju IP adresu dobiva od strane DHCP servera. Čak i ako se uključi ova opcija, a mrežno sučelje ne dobiva IP adresu preko DHCP servera, vatrozid će i dalje raditi normalno. Ova opcija omogućuje nastavak rada vatrozida i nakon što se promijene mrežne postavke sučelja spojenog na Internet.



Slika 2: Programski čarobnjak za konfiguriranje osnovnih postavki vatrozida

U slijedećem koraku uključivanjem opcije *Enable Internet connection sharing* omogućava se dijeljenje veze na Internet s ostalim računalima. Ovdje je potrebno odabrati mrežno sučelje na kojem se nalazi računalo ili mreža računala kojima je potrebno omogućiti korištenje veze na Internet. Također, moguće je odabrati da računala na privatnoj mreži primaju IP adrese preko DHCP servera na računalu na kojem se nalazi vatrozid. Ukoliko računalo na kojem je instaliran vatrozid posjeduje samo jedno mrežno sučelje ovaj korak u čarobnjaku neće biti prikazan.
U zadnjem koraku čarobnjaka, potrebno je spremiti postavljenu konfiguraciju i pokrenuti vatrozid.

4.2. Konfiguriranje *Status* dijela

Prilikom svakog pokretanja Firestarter vatrozida prvo se otvara *Status* stranica administracijskog sučelja. Na ovoj stranici vidljiv je kratki pregled vatrozida te je moguće promijeniti stanje vatrozida. Postoje tri stanja u kojima se vatrozid može nalaziti:

- aktivan (eng. *Active*) – vatrozid je pokrenut i radi,
- onemogućen (eng. *Disabled*) – vatrozid je ugašen te se sve veze prihvaćaju,
- zatvoren (eng. *Locked*) – nikakav promet se ne propušta kroz vatrozid, ni prema unutra, ni prema van.

Sama status stranica podijeljena je u tri djela:

- *Firewall* - prikazuje stanje vatrozida te ukupni broj blokiranih veza od pokretanja vatrozida.
- *Network* - daje pregled osnovnih informacija za svako mrežno sučelje na računalu. Informacije sadrže: ime sučelja, tip sučelja, količinu primljenog i poslanog prometa te trenutnu aktivnost sučelja izraženu u KB/s.
- *Active connections* - prikazuje sve trenutno uspostavljene veze kroz vatrozid (i ulazne i izlazne). Popis uspostavljenih veza osvježava se u realnom vremenu. Za svaku uspostavljenu vezu prikazuju se:
  - izvor (eng. *source*) - adresa računala koje je uspostavilo vezu,
  - odredište (eng. *destination*) – adresa računala na koje je uspostavljena veza,
  - port – port na kojem je uspostavljena veza,
  - servis (eng. *service*) – mrežni servis koji radi na korištenom portu (http, ftp, ssh i sl.), i
  - program – ime programa koji je uspostavio vezu (ova informacija je dostupna samo za veze koje su uspostavljene s računala na kojem se nalazi vatrozid).

Zapisi u dijelu *Active connections* prikazani su u jednoj od dvije boje:

- crna - trenutno aktivne veze i
- zelena – prekinuta veza koja se briše s liste nakon 10 sekundi.

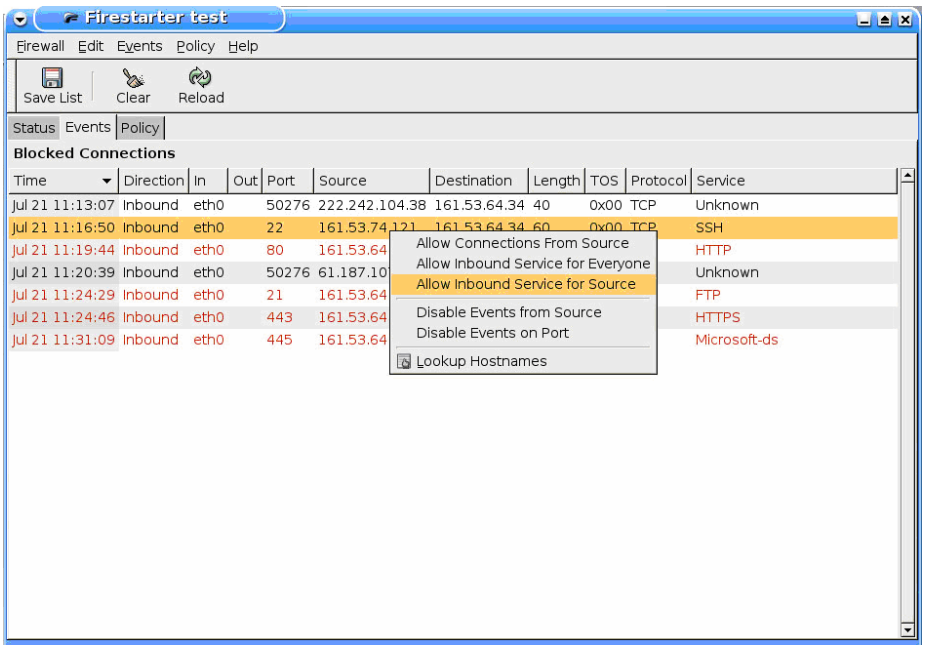
4.3. Konfiguriranje *Events* dijela

Events stranica prikazuje blokirane veze. Za svaku blokiranu vezu moguće je odabrati određenu akciju koja će utjecati na buduće ponašanje vatrozida što omogućuje kreiranje relativno složenih pravila vatrozida na poprilično jednostavan način.
Na popisu blokiranih veza, koje je moguće snimiti u posebnu datoteku, moguće je prikazati slijedeće podatke:

- vrijeme (eng. *time*) – vrijeme blokiranja veze,
- smjer (eng. *direction*) – pokazuje ukoliko je blokirana veza dolazna (iz vanjske mreže prema vatrozidu ili privatnoj mreži) ili odlazna (s vatrozida ili iz privatne mreže prema vanjskoj mreži),
- ulaz (eng. *in*) – dolazno mrežno sučelje,
- izlaz (eng. *out*) – odlazno mrežno sučelje (ukoliko postoji),
- port – korišteni port,
- izvor (eng. *source*) – adresa računala koje je započelo vezu,
- odredište (eng. *destination*) – adresa računala prema kojem je veza uspostavljana,
- duljina (eng. *length*) – veličina blokiranog paketa,
- *TOS* – vrijednost parametra *Type of Service* postavljenog u blokiranom paketu,
- protokol – mrežni protokol kojeg je veza koristila (TCP, UDP...) i
- servis (eng. *service*) – mrežni servis kojem je veza pokušala pristupiti (http, ftp, ssh...).

Desnim klikom na bilo koju blokiranu vezu otvara se izbornik s dodatnim opcijama. Sadržaj dostupnih opcija ovisi o tome je li riječ o dolaznoj ili odlaznoj vezi. Za odlazne veze dostupne opcije su:

- *Allow Connections to Destination* - odabirom ove opcije omogućava se uspostavljanje svih veza prema odredišnoj adresi,
- *Allow Outbound Service for Everyone* – ova opcija omogućit će odlazne veze za blokirani mrežni servis (http, ftp, shh...) sa svih adresa i
- *Allow Outbound Service for Source* – omogućava odlazne veze za blokirani mrežni servis samo za adresu s koje je uspostavljana blokirana veza.



Slika 3: Prikaz blokiranih veza

Za dolazne veze raspoložive opcije su:

- *Allow Connections from Source* – dozvoljava sve dolazne veze s adrese s koje je uspostavljana blokirana veza,
- *Allow Inbound Service for everyone* – dozvoljava sve dolazne veze za blokirani mrežni servis i
- *Allow Inbound Service for Source* – dozvoljava dolazne veze za blokirani mrežni servis samo s adrese s koje je uspostavljana blokirana veza.

Osim opcija kojima se mijenjaju pravila rada vatrozida, u izborniku su također dostupne i opcije za filtriranje sigurnosnih događaja. Radi se o dvije opcije:

- *Disable Events from Source* – sve blokirane konekcije s izvorišne adrese više neće biti prikazane, ali će i dalje biti blokirane, te
- *Disable Events from Port* – blokirane veze na određenom portu više neće biti prikazane.

Svi zapisi na Events stranici prikazani su jednom od sljedećih boja:

- crna – veza na slučajnom portu blokirana od strane vatrozida,
- crvena – pokušaj pristupa servisu koji nije javno dostupan i
- siva – veze koje su klasificirane kao bezopasne pri čemu se najčešće radi o prometu odaslanom cijeloj mreži (eng. *broadcast traffic*).

4.4. Konfiguriranje *Policy* dijela

Na *Policy* stranici administracijskog sučelja moguće je izravno definirati pravila filtriranja mrežnog prometa. Pravila se mogu podijeliti u dva osnovna dijela: pravila za dolazni promet i pravila za odlazni promet. Unutar svaka od ta dva dijela nalaze se tri grupe pravila. Za dodavanje pravila u bilo koju od tri grupe potrebno je prvo odabrati grupu, a zatim na traci s alatima odabrati *Add rule* ili desno kliknuti unutar grupe i na izborniku koji se pojavi odabrati *Add rule*. Pravila se uklanjaju na način da ih se označi i zatim se odabere *Remove rule* na traci s alatima ili u izborniku dostupnom nakon desnog klika. Analogno tome moguće je i mijenjati već postojeća pravila odabirom *Edit rule*.

Da bi se pravila počela primjenjivati potrebno je odabrati *Apply Policy*. Alternativno je moguće u *Preferences* dijelu odabrati opciju prema kojoj se sve promjene pravila automatski primjenjuju.

4.4.1. Početna pravila

Početna pravila Firestarter vatrozida postavljena su sa ciljem osiguravanja sigurnosti, kako samog vatrozida tako i računala u privatnoj mreži iza vatrozida. Početna pravila su slijedeća:

- nove dolazne veze prema vatrozidu ili privatnoj mreži iz javne mreže se blokiraju,
- računalo na kojem se nalazi vatrozid može slobodno uspostavljati veze prema svim ostalim računalima,
- računala u privatnoj mreži mogu uspostavljati veze prema vanjskoj mreži, ali ne i prema vatrozidu te
- promet s javne mreže, koji je odgovor na zahtjeve za uspostavom veza od strane vatrozida ili računala na privatnoj mreži, propušta se kroz vatrozid.

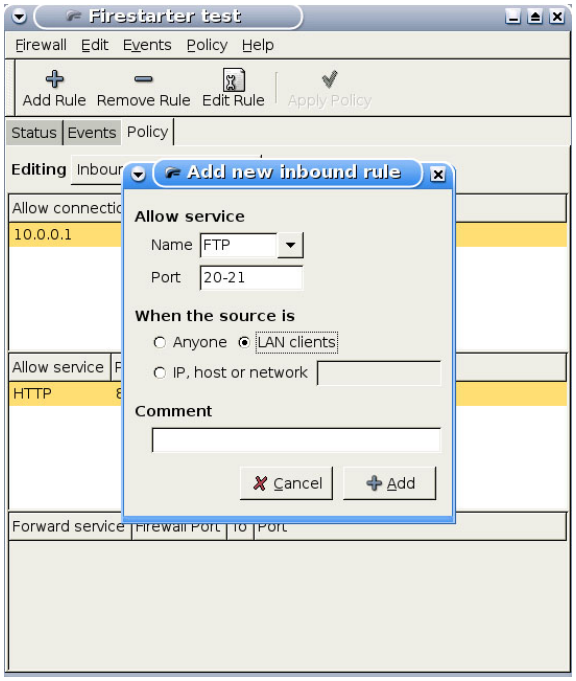
4.4.2. Pravila za dolazne veze

Pravila za dolazne veze kontroliraju sav dolazni promet s Interneta i lokalne mreže prema vatrozidu. Početne postavke u potpunosti blokiraju sav promet. Pravila koja se dodaju kreiraju iznimke u vatrozidu i propuštaju određene oblike mrežnog prometa. Grupe pravila za dolazni promet su:

- *Allow Connections from Host* – kod dodavanja pravila u ovoj grupi, jedini parametar koji je moguće zadati je adresa ili ime računala. Dodavanjem računala u ovu grupu dozvoljava se sav dolazni promet s tog računala.
- *Allow Service* – ovom grupom pravila moguće je postići puno detaljniju kontrolu prometa. Pravila u ovoj grupi imaju dva parametra: mrežni servis i izvor. Mrežni servis je moguće odabrati ili iz padajućeg izbornika ili ručnim unosom porta ili portova koje servis koristi. Kod odabira izvora ponuđena su tri moguća odabira:
  - svi (eng. *Anyone*) - pristup odabranom servisu se omogućava svim korisnicima.
  - lokalni klijenti (eng. *LAN clients*) - servis je dostupan samo računalima na lokalnoj mreži i

- zahtjevi s definiranih IP adresa, imena računala ili mreža - omogućuje unos IP adrese, imena računala ili mreže kojima će servis biti dostupan. Dodavanje ovakvog pravila prikazano je na slici *Slika 4*.

- *Forward Service* – ova skupina pravila je aktivna jedino kad je uključeno dijeljenje Internet veze između većeg broja računala. Kod dijeljenja Internet veze, skupina računala je s Interneta vidljiva kao jedna cjelina, tj. kao jedna IP adresa - vatrozidova. Obzirom da sva računala dijele jednu javnu IP adresu, kako bi se osigurala javnu dostupnost određenih servisa na lokalnoj mreži, vatrozid mora prosljeđivati promet između javne i lokalne mreže. U ovoj skupini pravila također postoje dva parametra: mrežni servis i odredište. Servis se odabire ili iz padajućeg izbornika ili unosom portova na kojima će vatrozid slušati. Kad vatrozid primi zahtjev na odabranom portu prosljeđuje ga računalu na lokalnoj mreži koje je specificirano u pravilu.



Slika 4: Novo dolazno pravilo

4.4.3. Pravila za odlazne veze

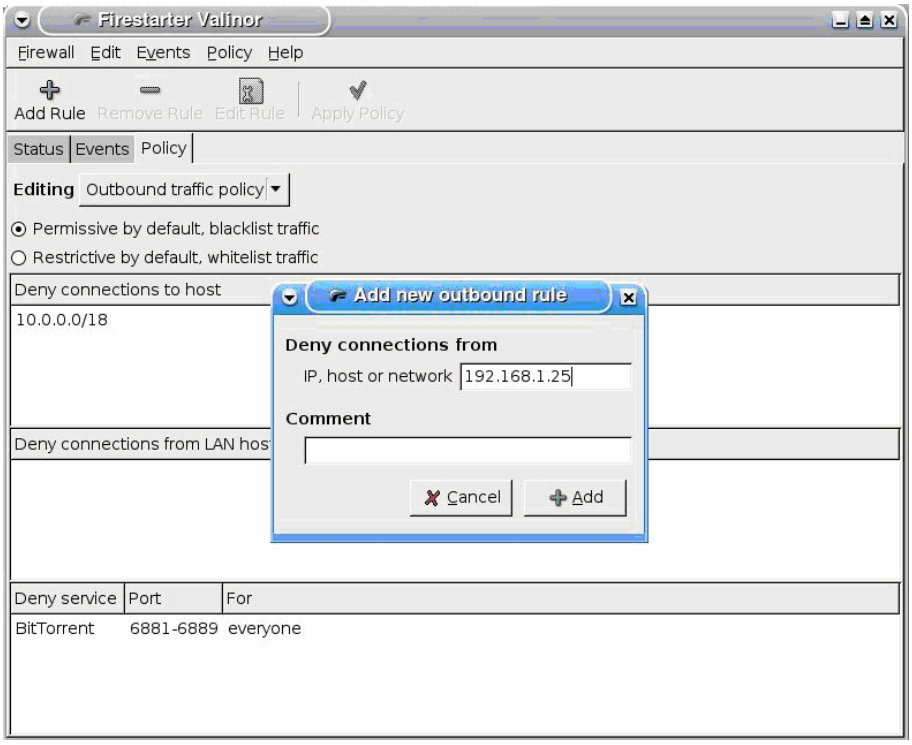
Pravila za odlazne veze kontroliraju sav odlazni promet s vatrozida i lokalne mreže prema javnoj mreži. Po početnim postavkama sav odlazni promet je dozvoljen (dopuštajući modus). Također, naknadno je moguće promijeniti početne postavke kako bi sav odlazni promet bio blokiran (ograničavajući modus).

4.4.3.1. Dopuštajući modus

U ovom modusu se vatrozid nalazi nakon instalacije i u njemu nema ograničenja na odlazni promet. Pravila, koja se naknadno dodaju u ovom modusu, zabranjuju odlazni promet.
Razlikuju se tri grupe pravila:

- *Deny connections to host* - pravila u ovoj grupi primaju samo jedan parametar: IP adresu ili ime računala prema kojem se blokiraju sve konekcije.
- *Deny connections from LAN host* – ovim pravilima onemogućuje se pojedinim računalima iz privatne mreže izlazak na javnu mrežu.
- *Deny service* – pravila u ovoj grupi pružaju detaljniju kontrolu prometa. Pravila primaju dva parametra: mrežni servis i izvor. Servis se bira kao i u ostalim slučajevima dok se za izvor mogu odabrati svi, vatrozid, klijenti iz lokalne mreže ili određene IP adrese, poslužitelji ili mreže. Dodavanje pravila u ovoj grupi zabranjuje definiranom izvoru korištenje određenog

mrežnog servisa. Odabir izvora obavlja se na identičan način kao i kod *Allow service* pravila za dolazne veze.



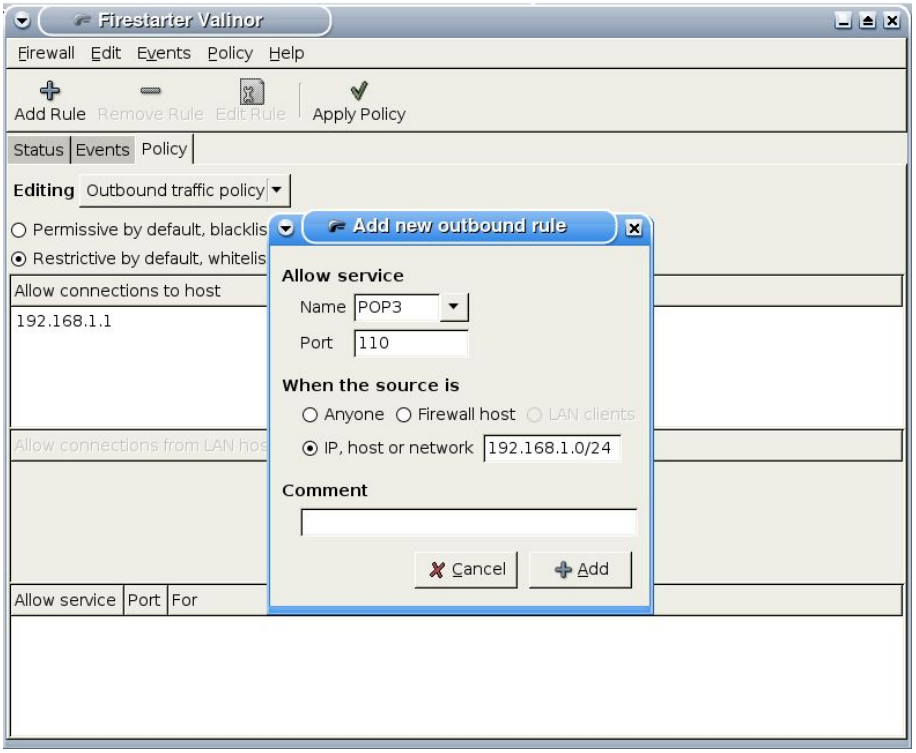
Slika 5: Dodavanje pravila za odlazni promet u dopuštajućem modusu

4.4.3.2. Ograničavajući modus

U ograničavajućem modusu nije dozvoljen nikakav odlazni promet sve dok ga se pravilom eksplicitno ne propusti. Ovaj modus pruža potpuniju zaštitu od prethodno opisanog. Nedostatak ovog modusa je u tome što nijedna mrežna aplikacija neće raditi dok se ne kreiraju pravila koja će joj omogućiti nesmetanu komunikaciju.

I ovom modusu, kao i u prethodnom, postoje tri grupe pravila:

- *Allow connections to host* – ova pravila predstavljaju tzv. legitimnu listu (eng. *whitelist*) dozvoljenih odredišta i njima je moguće dozvoliti pristup određenim poslužiteljima.
- *Allow connections from LAN host* – pravila u ovoj grupi dozvoljavaju pojedinim računalima na lokalnoj mreži neograničen pristup javnoj mreži.
- *Allow service* – ova grupa omogućuje preciznu kontrolu prometa. Pravila iz ove grupe su logički suprotna onima iz *Deny service* grupe iz dopuštajućeg modusa, a parametri su identični. Korištenjem ovih pravila moguće je primjerice određenom računalu dozvoliti upotrebu mrežnog servisa koji je zabranjen svim ostalima.



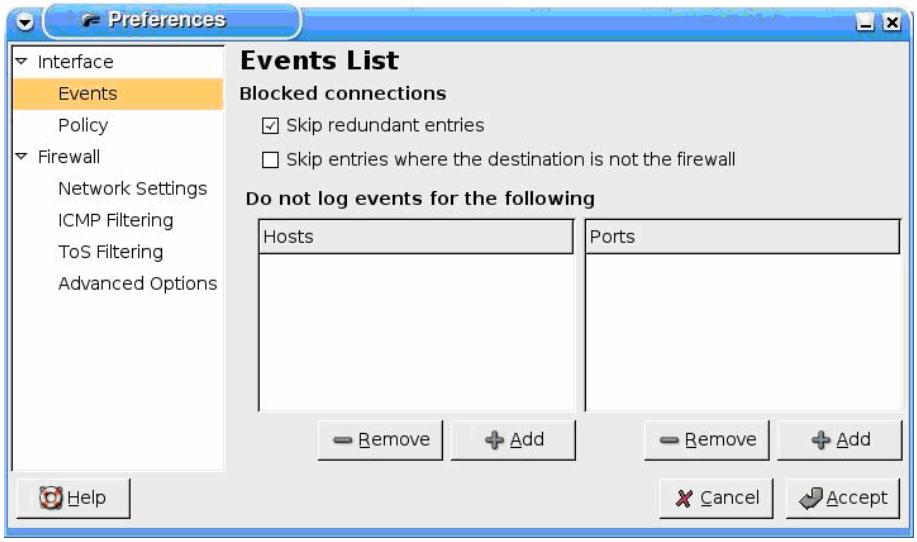
Slika 6: Dopuštanje korištenja mrežnog servisa u ograničavajućem modusu

4.5. Konfiguriranje *Preferences* dijela

Preferences dijalog Firestarter vatrozida sadrži mnoge opcije koje kontroliraju ponašanje grafičkog sučelja, ali i samog vatrozida. Dijalog je dostupan odabirom *Preferences* opcije na traci s alatima ili odabirom iz izbornika *Edit*. Raspoložive opcije su podijeljene u dva dijela: opcije grafičkog sučelja i opcije vatrozida.

4.5.1. Opcije grafičkog sučelja

Ovaj dio podijeljen je na tri dijela za općenito podešavanje grafičkog sučelja i podešavanje *Events* i *Policy* stranica. Kod opcija za podešavanje grafičkog sučelja moguće je uključiti ikonu koja pokazuje informacije o statusu vatrozida koje su inače dostupne na *Status* stranici grafičkog sučelja. Od opcija vezanih uz *Events* stranicu potrebno je napomenuti da se na tom dijelu nalazi popis filtriranih sigurnosnih događaja koji se ne prikazuju na stranici *Events*.

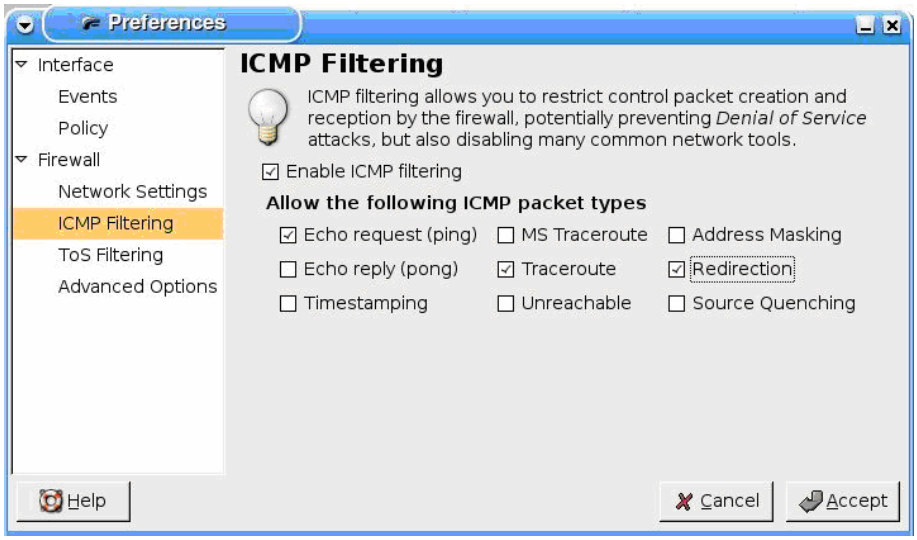


Slika 7: Podešavanje filtera za prikazivanje blokiranih veza na *Events* stranici

4.5.2. Opcije vatrozida

U *Firewall* dijelu je moguće podesiti neke naprednije mogućnosti vatrozida, ali također i promijeniti opcije postavljene korištenjem programskog čarobnjaka prilikom prvog pokretanja. U dijelu *Network Settings* moguće je podesiti dijeljenje Internet veze na više računala te na jednostavan način osposobiti DHCP.

Među naprednijim opcijama vatrozida nalaze se i one za filtriranje ICMP paketa koji čine posebnu klasu prometa koju koriste mnogi mrežni alati (npr. ping, traceroute, ...). Firestarter će prema ugrađenim pravilima dopuštati ICMP pakete, ali će donekle kontrolirati njihovu količinu kako bi se spriječili DoS napadi.



Slika 8: Podešavanje filtriranja ICMP paketa

Osim navedenih opcija moguće je dodatno podesiti i ToS (eng. *Type of Service*) filtriranje pri čemu se definira ukoliko paketi trebaju biti odbijeni uz obavijest ili odbačeni bez obavijesti.

5. Zaključak

Iako Firestarter vatrozid ne posjeduje neke osnovne funkcionalnosti uobičajene na vatrozidima poput logiranja mrežnog prometa, alarmiranja administratora i mogućnosti za VPN konekcije, vatrozid je ipak opravdao svoj status jednog od najzastupljenijih vatrozida namijenjenih neiskusnim korisnicima i kućnim računalima. Ističe se svojom jednostavnošću i brzinom podešavanja. Čak je i najsloženija pravila moguće podesiti u samo nekoliko minuta i to korištenjem isključivo grafičkog sučelja.

Posebno je potrebno istaknuti mogućnost jednostavnog kreiranja pravila na temelju stvarnih situacija, tj. na temelju blokiranih veza. Na taj način omogućeno je kreiranje pravila filtriranja koja su po potrebi prilagođena svakom računalu koje se nalazi iza njega, a sam administrator vatrozida neće se morati upuštati u pisanje kompliciranih skripti ili uređivanje sistemskih datoteka već će cijelu konfiguraciju moći izvršiti korištenjem grafičkog okruženja.

Vodeći računa o svim prednostima i nedostacima Firestarter vatrozida nameće se zaključak kako je Firestarter odlično rješenje za zaštitu kućnih računala te manjih kućnih i uredskih mreža. U takvom relativno maje zahtjevnom okruženju, prednosti Firestarter vatrozida dolaze do punog izražaja dok nedostaci nisu toliko uočljivi i bitni.

6. Reference

[1] Web stranice Firestarter vatrozida, http://www.fs-security.com/, srpanj, 2006.
[2] Firestarter 1.0 korisnički priručnik, http://www.fs-security.com/docs.php, srpanj, 2006.