HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza alata Savungan

CCERT-PUBDOC-2004-09-89

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

Povezivanjem privatnih računalnih mreža na Internet, potreba za zaštitom od vanjskih prijetnji postala je iznimno važan aspekt računalne sigurnosti. Iako postoje brojni sigurnosni mehanizmi i kontrole koje omogućuju zaštitu informacijskih resursa od prijetnji s Interneta (antivirus, IDS sustavi i sl.), vatrozidna zaštita najčešće predstavlja prvu liniju obrane. Postavljanjem vatrozida između privatne računalne mreže i Interneta omogućuje se kontrola mrežnog prometa koji se razmjenjuje između ove dvije mreže. Sigurnosnom politikom vatrozida moguće je precizno definirati koje su konekcije dozvoljene, a koje ne, čime se znatno podiže sigurnost resursa na privatnoj računalnoj mreži.

U ovom dokumentu biti će opisan Savungan programski paket, *open source* vatrozid (eng. *firewall*) dizajniran za Microsoft Windows operacijske sustave. Program omogućuje filtriranje mrežnog prometa na drugom (engl. *Data Link*) i trećem (engl. *Network*) sloju OSI modela, a odlikuje se i iznimnom jednostavnošću te brzinom rada. Vatrozid podržava i tzv. *stateful inspection* način filtrirana paketa kojim se dodatno podiže pouzdanost sustava. Prednost *stateful inspection* način rada je što ne ispituje samo zaglavlje paketa, već i njegov sadržaj te stanje pojedinih konekcija.

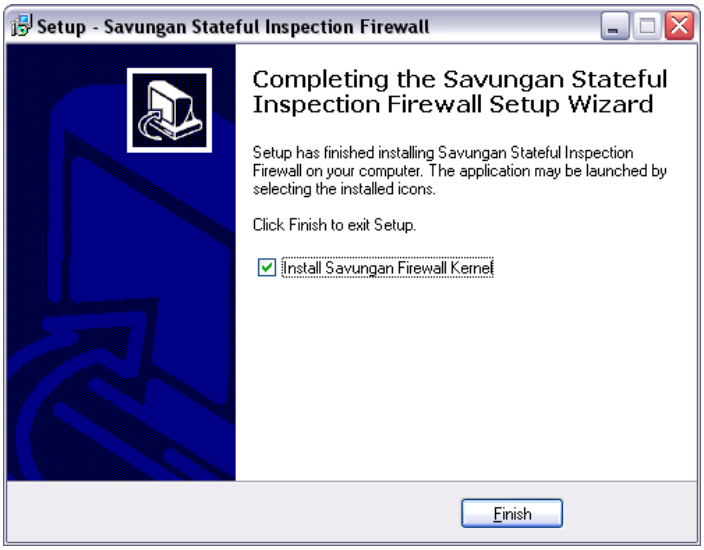
Kao što je već spomenuto program omogućuje filtriranje prometa na drugom mrežnom sloju uključujući *ARP/ RARP* protokole (*Address Resolution Protocol/ Reverse Address Resolution Protocol*), za različita fizička sučelja, a ujedno odvaja primjenu pravila za svaki od njih. Dokument analizira osnovne postupke instalacije Savungan programskog paketa, njegove osnovne karakteristike te mogućnosti primjene u praksi.

2. Instalacija i pokretanje

Za instalaciju osobnog vatrozida Savungan potrebno je dohvatiti izvršnu datoteku na adresi http://www.modemwall.com/Downloads/SAVUNGANBIN2Setup.exe te ju pohraniti na lokalni disk. Datoteka je dostupna u `.exe` formatu pod imenom `SAVUNGANBIN2SETUP.exe`, veličine 1.33 MB. Na referentnoj adresi http://www.modemwall.com/Downloads/Savungan.pdf može se dohvatiti i brošura o samom alatu, u `.pdf` formatu datoteke veličine 674 KB. U trenutku pisanja ovog dokumenta zadnja dostupna inačica alata je `2.0.3`.

Za instalaciju programa potrebno je pokrenuti spomenutu izvršnu datoteku čime započinje proces instalacije. Tijek instalacije alata izuzetno je jednostavan. Nakon prihvaćanja licenčnog ugovora instalacijski postupak instalira program unutar mape `Program Files` na računalu što korisnik može promijeniti izborom neke druge lokacije za instalaciju.

Nakon uspješne instalacije, pojavit će se dijaloški okvir koji je prikazan na slici 1, a koji korisnika izvješćuje o završenom postupku instalacije te nudi izbor instalacije *Savungan Firewall Kernel* jezgre. Korisnik može isključiti ovu opciju pa provesti ručnu instalaciju navedenog servisa što se svakako preporučuje. Ukoliko ju ostavi uključenu, servis se neće dobro instalirati zbog greške koja je opisana nakon prikazane slike 1.



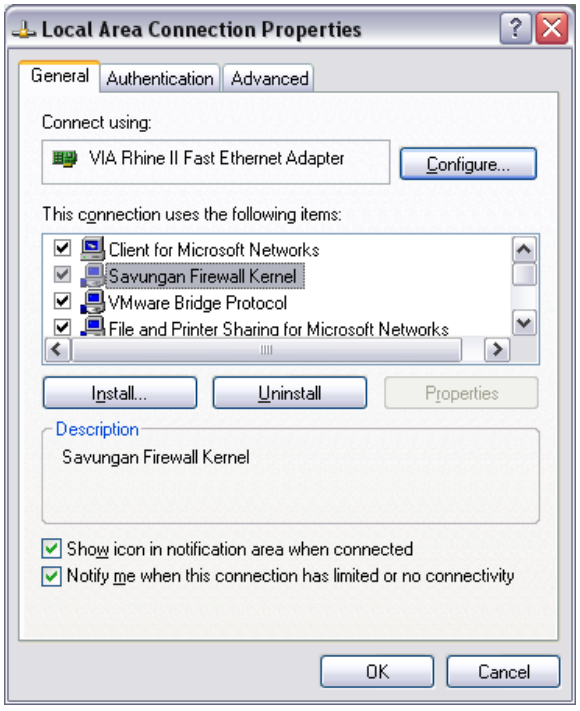
Slika 1: Dijaloški okvir završetka instalacijskog postupka alata Savungan

Prilikom prvog pokretanja alata, javlja se greška prikazana na slici 2.

Slika 2: Greška prilikom pokretanja alata

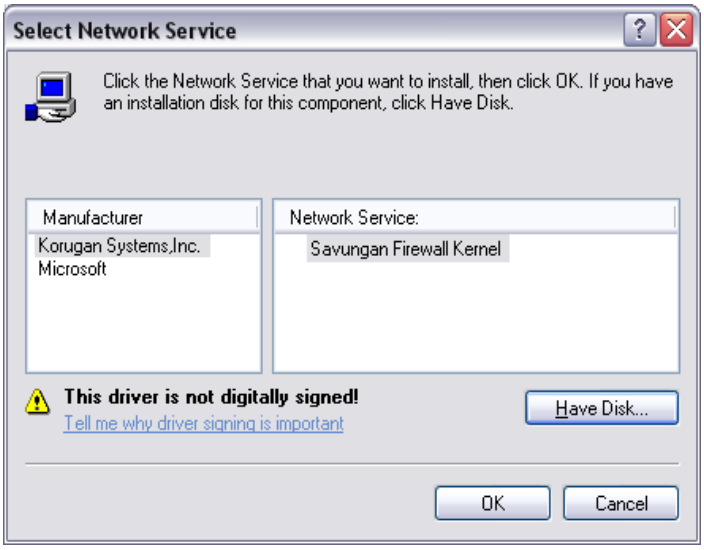
Razlog pojavljivanja greške je greška unutar Microsoftovog *driver installer* programa. Prilikom instalacije, upravljački program se zapravo ne instalira pa je potrebno slijediti navedene korake kako bi se greška ispravila:

1. zatvoriti program Savungan,
2. desnom tipkom miša kliknuti na ikonu *My Network Places* na radnoj površini i odabrati naredbu *Properties*,
3. u otvorenom prozoru, desnom tipkom miša kliknuti na *Local Area Connection* ikonu i odabrati opciju *Properties*,
4. u prozoru svojstava vidljiv je servis *Savungan Firewall Kernel* prikazan na slici 3 koji treba označiti klikom lijeve tipke miša, a potom kliknuti na gumb *Uninstall* kako bi se izvršila deinstalacija servisa,



Slika 3: Savungan Firewall Kernel u prozoru svojstava lokalne mreže

5. po završenom postupku deinstalacije, potrebno je kliknuti na gumb *Install* i odabrati opciju *Service*, pa gumb *Add*,
6. u novootvorenom prozoru treba kliknuti gumb *Have disk*, zatim *Browse* kako bi se pronašla odgovarajuća datoteka servisa (slika 4). Ukoliko je alat instaliran u mapu `Program Files` na računalu, putanja do odgovarajuće datoteke je `C:\Program Files\Savungan\Driver`,



Slika 4: Instalacija odgovarajućeg driver-a servisa Savungan Firewall Kernel

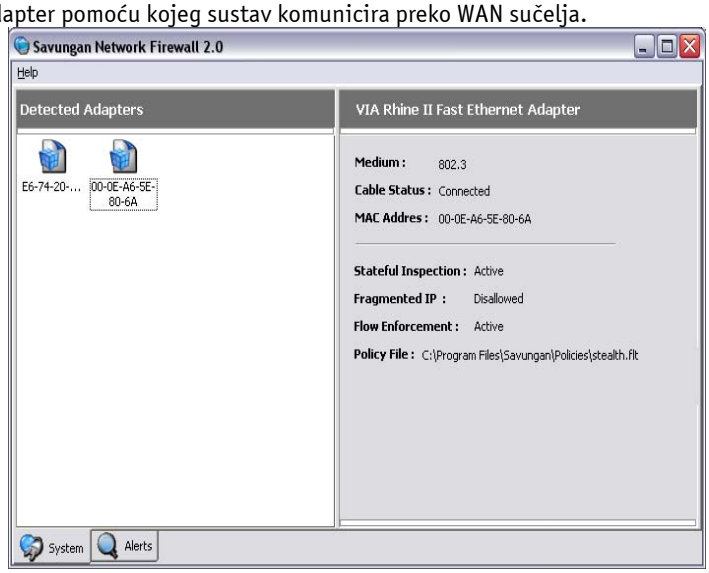
7. navedena putanja sadrži dvije `.inf` datoteke pa je potrebno označiti bilo koju od njih kako bi se instalirao servis,
8. nakon otvaranja `.inf` datoteke korisnik će vidjeti servis *Savungan FireWall Kernel*, označiti ga i kliknuti gumb `OK`. Ukoliko Windows operacijski sustav prikaže dijaloški okvir s porukom o digitalnom potpisu upravljačkog programa, potrebno je kliknuti *Continue Installation* gumb,

9. kada proces instalacije servisa završi, a servis je ponovno prikazan kao na slici 3, potrebno je ponovno pokrenuti program Savungan.

3. Sučelje

Nakon pokretanja alata otvara se sučelje koje je prikazano na slici 5. Sučelje alata vrlo je jednostavno. Sastoji se od izbornika `Help` koji ne sadrži pomoć za rad s programskim alatom, već nudi informacije o programu, što je svakako jedan od nedostataka alata. Ostali elementi sučelja su dvije kartice, `System` i `Alerts`.

Kartica `System` podijeljena je da dva područja. Lijevo područje prikazuje detektirana mrežna sučelja, a desno područje prikazuje osnovna svojstva svakog od njih. `NdisWan` sučelje predstavlja predefinirani adapter pomoću kojeg sustav komunicira preko WAN sučelja.



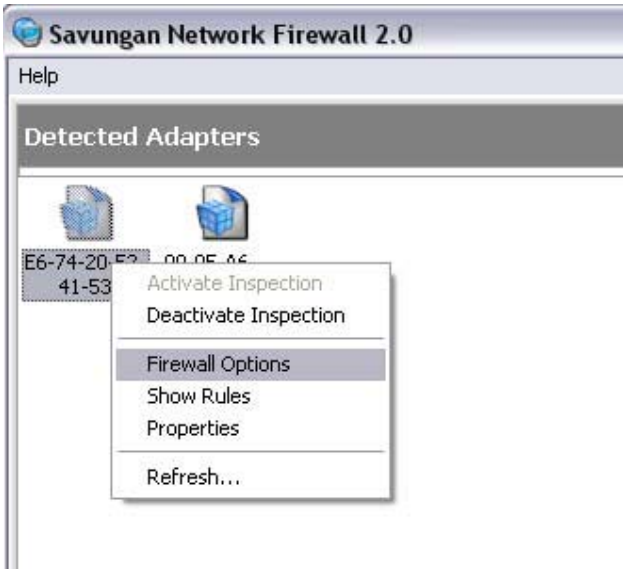
Slika 5: Sučelje alata Savungan

4. Podešavanje alata

Savungan vatrozid, nakon pokretanja, svakako zahtjeva podešavanje opcija filtriranja mrežnog prometa kako bi se prilagodio okruženju u kojem se koristi te nudio optimalan stupanj sigurnosti.

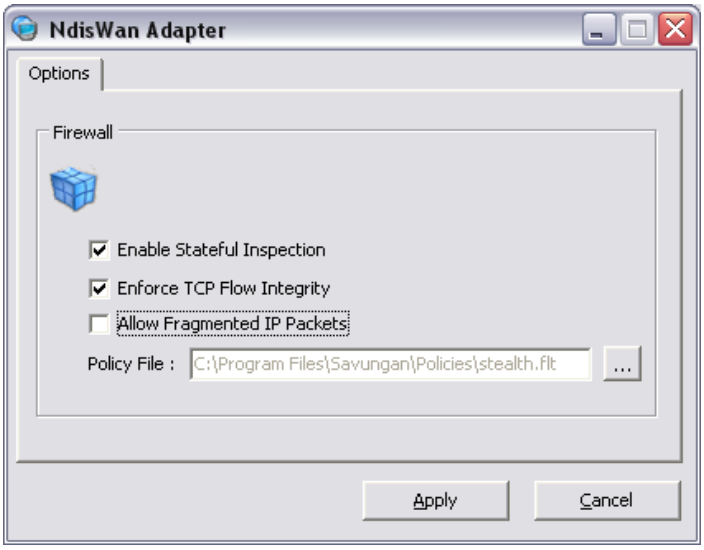
4.1. Opcije vatrozida

Prikaz opcija vatrozida pregledava se tako da se na kartici `System` desnom tipkom miša klikne detektirano mrežno sučelje i odabere opcija *Firewall Options* kao što je prikazano na slici 6.



Slika 6: Izbor sučelja za pregled i podešavanje opcija vatrozida

Nakon izbora navedene opcije, otvara se dijaloški okvir koji prikazuje opcije vatrozida, a prikazan je na slici 7.



Slika 7: Svojstva vatrozida

Za svako mrežno sučelje, vatrozid je moguće podesiti tako da filtrira promet statički i/ili korištenjem *stateful inspection* tehnologije. Samim time moguće je na različitim sučeljima podesiti različite načine filtriranja mrežnog prometa ukoliko za to postoji potreba. Uključivanje opcije `Enable Stateful Inspection` znači da će se istovremeno provoditi filtriranje mrežnog prometa kombinacijom obih metoda. Uključena opcija `Enforce TCP Flow Integrity` osigurava pravilan tijek TCP konekcija kako bi se onemogućilo pregledavanje mrežnih portova korištenjem inteligentnih programa kao što je npr. NMAP kada je aktivan *Savungan* vatrozid.

Opcija `Allow Fragmented IP Packets` definira da li će se dozvoliti fragmentirati paketi (opcija je uključena) ili neće (opcija je isključena). `Policy File` polje označava putanju do datoteke s sigurnosnom politikom vatrozida.

4.2. Definiranje pravila vatrozida

Savungan vatrozid ima vrlo fleksibilnu i jednostavnu sintaksu pisanja pravila što je svakako jedna od njegovih kvaliteta. Na ovaj način smanjuje se mogućnost pogreške prilikom pisanja samih pravila filtriranja.
Pisanje pravila filtriranja mrežnog prometa omogućeno je za Ethernet, IP, TCP, UDP i ICMP protokole, čime se omogućuje filtriranja prometa na drugom i trećem sloju OSI modela.
Struktura pravila za filtriranje na drugom sloju (Ethernet) je slijedeća:

```
PASS|DROP ETH IN|OUT|BOTH FROM <addr> TO <addr> [ETHERTYPE
<ethertype>] [NOLOG]
```

gdje oznaka `<addr>` može poprimiti 12-to znamenkastu MAC adresu oblika `000000000000` ili vrijednost "`ANY`". Oznaka `<ethertype>` predstavlja naziv protokola sloja 2. Podržani protokoli sloja 2 su:

- EIP - IP protokol,
- EIP6 - IPv6 protokol,
- EPUP - PUP protokol,
- ENS - NS protokol,
- EARP - ARP protokol,
- EDN - DN protokol,
- ELAT - LAT protokol,
- EATALK - ATALK protokol,
- EAARP - AARP protokol,
- ERARP - RARP protokol,
- ELOOP - LOOP protokol,
- ERC - RC protokol,
- ANY - bilo koji protokol sloja 2.

Konkretni primjer pravila priložen je u nastavku:

```
PASS ETH OUT FROM 001122334455 TO 112233445566
```

Struktura pravila za filtriranje paketa na mrežnom sloju je sljedeća:

```
PASS|DROP IP IN|OUT|BOTH FROM <addr> TO <addr> [IPPROTO <ipproto>]
[NOLOG]
```

gdje oznaka `<addr>` predstavlja IP adresu ili područje adresa u CIDR formatu (npr. `192.168.0.0/24`) ili vrijednost "`ANY`". Oznaka `<ipproto>` predstavlja broj IP protokola.
Primjer pravila za filtriranje paketa na mrežnom sloju:

```
DROP IP IN FROM ANY TO 127.0.0.1
```

Struktura pravila za filtriranja paketa na transportnom sloju (TCP/UDP) je slijedeća:

```
PASS|DROP TCP IN|OUT|BOTH FROM <addr> TO <addr> [FLAGS <flags>]
[NOLOG]
```

gdje oznaka `<addr>` predstavlja IP adresu ili područje adresa u CIDR formatu te područje portova na koje se pravilo odnosi, a oznaka `<flags>` predstavlja TCP zastavice na temelju kojih je također moguće provoditi filtriranje. Znaka '+' ili '–' koji slijedi iza TCP zastavice označava da je određena zastavica postavljena ili nije. TCP zastavice koje je moguće navesti su:

- `A – ACK` – potvrda primljenih podataka,
- `P – PSH` – dostavljanje podataka primatelju,
- `S – SYN` – inicijacija spoja,
- `R – RST` – resetiranje spoja,
- `F – FIN` – terminiranje spoja,
- `U – URG` – hitan paket.

Primjer TCP pravila:

```
DROP TCP IN FROM 192.168.5.0/24 TO 0.0.0.0/0:1-1024 FLAGS S+A-
```

Struktura UDP pravila je slijedeća:

```
PASS|DROP UDP IN|OUT|BOTH FROM <addr> TO <addr> [NOLOG]
```

gdje oznaka `<addr>` predstavlja IP adresu ili područje adresa u CIDR formatu te područje portova na koje se pravilo odnosi.
Primjer UDP pravila:

```
PASS UDP IN FROM 0.0.0.0/0:53 TO ANY
```

Struktura ICMP pravila je slijedeća:

```
PASS|DROP   ICMP   IN|OUT|BOTH   FROM   <addr>   TO   <addr>   [TYPE
<type>.<code>] [NOLOG]
```

gdje oznaka `<addr>` predstavlja IP adresu ili područje adresa u CIDR formatu. Oznaka `<type>` predstavlja tip ICMP paketa, a `<code>` polje predstavlja kod ICMP paketa.

Primjer ICMP pravila:

```
PASS ICMP IN FROM 212.23.32.45/25 TO ANY TYPE 0.0
```

4.3. Predefinirane politike

Prilikom prvog pokretanja vatrozida, Savungan koristi predefinirane politike tj. inicijalni skup pravila koji su zapisani u tekstualnoj datoteci. Za svako fizičko sučelje, vatrozid sadrži različit skup pravila. Predefinirane politike nalaze se u mapi `Policies` unutar instalacijske putanje alata (`C:\Program Files\Savungan\Policies`).

To su datoteke `only_http_in.flt`, `only_http_out.flt`, `pass_all_activity.flt`, `stealth.flt` i `stop_all_activity.flt`. Datoteka `rules_manifesto.flt` sadrži primjere i način pisanja pravila filtriranja. Datoteke se otvaraju pomoću bilo kojeg tekstualnog editora.

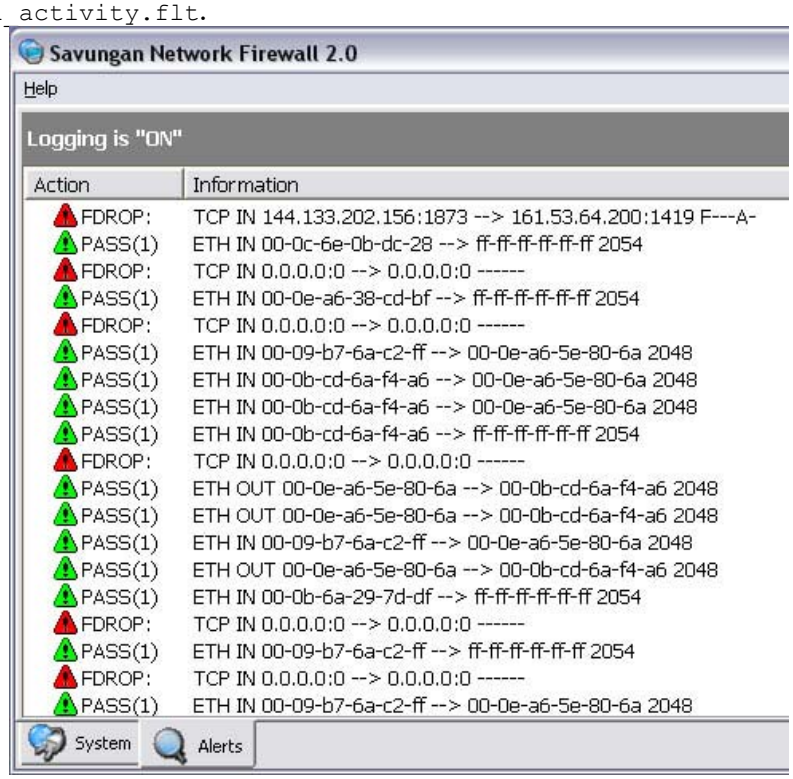
Dio datoteke `rules_manifesto.flt` prikazan je u nastavku dokumenta:

```
# ------------------------------------------------------------------
#
# Rules format: Stateful Inspection is only supported for TCP
# protocol for now.
# As of Kernel version 2.5 it will be available for all
# protocols supported.
# Rules are applied from TOP to BOTTOM! All reserved words
# must be in uppercase!
# WARNING : THIS IS A SAMPLE FILTER AND MUST NOT BE
# APPLIED TO FIREWALL BECAUSE
# IT MAY NEGATIVELY AFFECT NETWORK PEFORMANCE AND SECURITY!
# ------------------------------------------------------------------#
# Ethernet rules:
#
# PASS|DROP ETH IN|OUT|BOTH FROM <addr> TO <addr> [ETHERTYPE <ethertype>]
[NOLOG]
#
#
# Where <addr> is 12 digit MAC-address or "ANY"
#  <addr> ::== ANY (No IP address support for ETH rules)
#   is equal to 000000000000
#
# And <ethertype> is Layer 2 protocol name.
# Supported layer 2 protocols are as follows:
# <ethertype> :== "EIP",          IP protocol,
#                  "EIP6",              IPV6 protocol,
#                  "EPUP",             PUP    protocol,
#                  "ENS",       NS     protocol,
#                  "EARP",              ARP    protocol,
#                  "EDN",       DN     protocol,
#                  "ELAT",              LAT    protocol,
#                  "EATALK",            ATALK protocol,
#                  "EAARP",             AARP  protocol,
#                  "ERARP",             RARP  protocol,
#                  "ELOOP",             LOOP  protocol,
#                  "ERC",       RC    protocol,
#                  "ANY",       ANY Layer 2 protocol.
# Example:
#
# PASS ETH IN FROM ANY TO 001122334455 ETHERTYPE EARP NOLOG
# PASS ETH BOTH FROM ANY TO ANY ETHERTYPE EIP NOLOG
# DROP ETH OUT FROM FFEE4433FFEE TO 223344556699 ETHERTYPE ANY
```

```
# PASS ETH OUT FROM 001122334455 TO 112233445566
#
# ------------------------------------------------------------------------
```

4.4. Uporaba politika

Kao što je već spomenuto, Savungan vatrozid omogućuje pisanje proizvoljnih politika filtriranja prometa. Politike se sastavljaju u bilo kojem tekst editoru i spremaju u formatu `.flt`. Datoteke je moguće pohraniti bilo gdje na lokalnom disku, ukoliko se ne želi koristiti mapa u kojoj su spremljene predefinirane politike. Kada je politika pohranjena na lokalnom disku, u svojstvima vatrozida (Slika 7) potrebno je definirati polje `Policy File` koje označava putanju do datoteke s pravilima filtriranja. Slika 8 prikazuje log zapise vatrozida kada se koristi predefinirana politika `pass_all_activity.flt`.

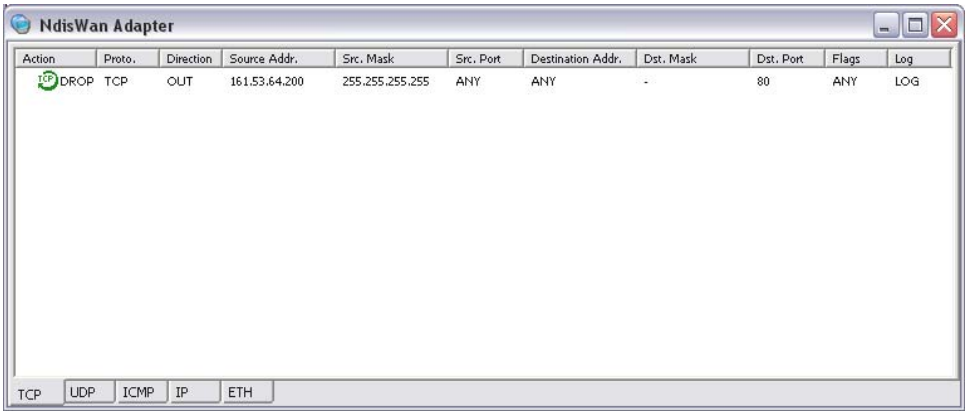


Slika 8: Filtriranje prometa

Politika pod imenom `tcp80.flt` primjer je politike filtriranja HTTP prometa. Primjera pravila dan je u nastavku:

```
DROP TCP OUT FROM 161.53.64.200 TO ANY:80
```

Prikazanim pravilom blokira se HTTP promet sa adrese 161.53.64.200 prema svim ostalim računala, odnosno korisniku se onemogućava korištenje Web servisa. Sigurnosna politika je primijenjena nad oba adaptera. Dvostrukim klikom na adapter otvara se prozor prikazan na slici 9 koji prikazuje korišteno pravilo filtriranja.



Slika 9: Korištenje politike tcp80.flt

5. Zaključak

Savungan alat može se opisati kao jednostavan program namijenjen filtriranju mrežnog prometa unutar mreža temeljenih na TCP/IP protokolu. Filtriranje paketa moguće je na drugom i trećem sloju OSI modela, a podržan je i *stateful inspection* način rada. Program se odlikuje iznimnom fleksibilnošću i jednostavnošću, a ujedno je i potpuno besplatan.

No, bez obzira na jednostavnost samog alata, njegova primjena od korisnika zahtjeva određeno poznavanje mrežnih protokola i načina komunikacije s obzirom da se pravila definiraju ručno korištenjem odgovarajuće sintakse. Ovakav način kreiranja pravila podložan je greškama i propustima, pogotovo kod manje iskusnih korisnika.