Filtrowanie pakietów w Linuksie 2.4

Rusty Russell, lista pocztowa netfilter@lists.samba.org Wersja oryginalna: $Revision: 495 $ $Date: 2002-02-09 10:47:39 +0100 (Sat, 09 Feb 2002) $

Orygina^3*tegodokumentuznajdujesipodadresem* : http://netfilter.filewatcher.org/

Orygina^3*tegot*^{3}*umaczeniaznajdujesipodadresem* : http://mr0vka.eu.org/tlumaczenia/linux24-pf.html

Spis treści

1 Wprowadzenie **2**

2 Gdzie jest oficjalna strona WWW? Czy jest lista e-mail? **2**

3 To co to jest Filtr Pakietów? **3**

3.1 Dlaczego móg^3*bymchciefiltrowapakiety?* . . . 3

3.2 Jak filtrowaæ pakiety pod Linuksem? . . . 3

3.2.1 Zapisywanie regu^3*nasta*^{3}*e* . . . 3

4 Kim u diab^3*ajeste¶idlaczegobawiszsimoimkernelem?* **4**

5 Bardzo krótki przewodnik Rusty'ego do filtrowania pakietów **4**

6 Jak pakiety podró¿uj±*przezfiltry* **4**

7 U¿ywanie iptables **5**

7.1 Co zobaczysz gdy wystartujesz komputer . . . 5

7.2 Operacje na pojedyñczej regule . . . 6

7.3 Specyfikacja filtrowania . . . 6

7.3.1 Wskazanie adresów IP: $\frac{1}{4}$ród^3*owegoidocelowego* . . . 7

7.3.2 Inwersja . . . 7

7.3.3 Protokó^3 . . . 7

7.3.4 Interfejs . . . 7

7.3.5 Fragmenty . . . 7

7.3.6 Rozszerzenia do iptables: Nowe cele i nowe testy . . . 8

7.4 Cel . . . 12

7.4.1 £añcuchy zdefiniowane przez u¿ytkownika . . . 13

7.4.2 Rozszerzenia do iptables: Nowe Cele . . . 13

7.4.3 Specjalne cele wbudowane . . . 14

7.5 Operacje na ca^3*ym*^{3}*acuchu* . . . 14

7.5.1 Tworzenie nowego ^{3}*acucha* . . . 15
7.5.2 Kasowanie ^{3}*acucha* . . . 15
7.5.3 Opró¿nianie ^{3}*acucha* . . . 15
7.5.4 Listowanie zawarto¶ci ^{3}*acucha* . . . 15
7.5.5 Resetowanie (zerowanie) liczników . . . 15
7.5.6 Okre¶lanie polityki . . . 16

8 U¿ywanie ipchains i ipfwadm 16

9 £±*czeniefiltrowaniapakietwiNAT* 16

10 Ró¿nice pomiêdzy iptables i ipchains 17

11 Porady w projektowaniu filtra pakietów 17

1 Wprowadzenie

Witam Szanownego czytelnika.

Zak^3*adam*, *ewieszcotoadresIP*, *adressieciowy*, *maskasieciowa*, *rutingiDNS.Je¶linie*, *polecamprzeczytanieHOWTON*

To HOWTO oscyluje na granicy delikatnego wprowadzenia (które sprawi, ¿e poczujesz siê zadowolony z siebie, ale niezabezpieczony przed wiatem Rzeczywistym) i surowego, pe^3*negoopisu*(*ktreoszczdzitylkonajwikszychtwardzieli*, *aresztabdziezmieszana*, *wstanieparanoiiposzukiwabdziecikie*

Twoja sieæ nie jest **bezpieczna**. Problem umo¿liwienia szybkiej i wygodnej wymiany informacji a jednocze¶nie ograniczenia jej tylko do w^3*a¶ciwychzastosowa*, *jestporwnywalnydoinnychproblemwtakichjakzapewnieniewolno¶wypowiedziijednocze¶nieza*
zanywtymHOWTO.

Zatem tylko ty mo¿esz zadecydowaæ jak wygl±*dabdziekompromis.Sprbujpoinstruowaciwuytkowaniudostpnychnarzdzi*

(C) 2000 Paul 'Rusty' Russell. Na licencji GNU GPL.

2 Gdzie jest oficjalna strona WWW? Czy jest lista e-mail?

S±*trzyoficjalnestrony* :

Dziêki *Filewatcher* http://netfilter.filewatcher.org/ .

Dziêki *Zespo*^{3}*owiSambaiSGIhttp://netfilter.samba.org/*.*DzikiHarald'owiWeltehttp://netfilter.gnumonks.*

Mo¿esz osi±*gn* ± *jenazasadzierwnowaeniaobci* ± *eniaprzezDNSround* − *robin*, *wybieraj* ± *cadres*http://www.netfilter.org/*i*

http://www.iptables.org .

Oficjalna lista pocztowa znajduje siê na

serwerze list Samba http://www.netfilter.org/contact.html#list .

3 To co to jest Filtr Pakietów?

Filtr pakietów to takie oprogramowanie, które sprawdza **nag**^{3}*wki*(*ang.header*)*pakietwwtrakciejakprzechodz*±
przezmaszynnaktrejdzia^3*aidecydujeoichlosie.Moezdecydowa*, *epakietzostanieodrzucony*(*ang.DROP*, *tzn.takjakbypa*

W Linuksie, filtrowanie pakietów jest wbudowane w kernel (jako modu^3*lubpoprostuwbudowane*)*ijestparjeszczesprytniejszychrzeczyktremoeszzrobi*, *alegeneralnieideapoleganaspraw*

3.1 Dlaczego mó^3*bymchciefiltrowapakiety?*

Kontrola. Bezpieczeñstwo. Czujno¶æ.

Kontrola:

> **kiedy u¿ywasz Linuksa by po**^{3}*aczytwoj* ± *wewntrzn* ± *siezinn* ± *sieci* ± (*powiedzmyzInternetem*)*maszokazjwpu¶citrochrnychtypwruchuiodrzuciinne.Naprzyk*^{3}*ad*, *nag*^{3}*wekpakietupos*
> *dookre¶lonychcz¶cisiecizewntrznej.Innymprzyk*^{3}*ademmoebyto* : *uywamNetscapedoogl* ± *daniaarchiwwDilbert'a.Jesttammasareklampochodz*±*cychzadresudoubleclick.net*, *wicNetscapetraciczasbyje*^{3}*ad*
> *cychdoiztegoadresurozwi*±*zujetenproblem*(*jednakejestparinnychsposobwbyzrobitolepiej*, *sprawd*$\frac{1}{4}$*Junkbuster*).

Bezpieczeñstwo:

> **kiedy Twój linuks jest jedynym komputerem pomiêdzy chaosem Internetu i twoj**±^{3}*adn*±, *uporz*±*dkowan*±*sieci*±, *mi*^{3}*ojestwiedzieemoeszob*^{3}*oyrestrykcjamitoconadchodzidotwychdrzwi.N*
> *cymodrnychz*^{3}*o¶liwychuytkownikwsieci.Innymprzyk*^{3}*ademmoebytwojeyczenie*, *byniezezwalanatelnet'owaniesi*
> *has*^{3}*a*; *prawdopodobniechceszby*(*jakwikszo¶ludzi*)*raczejobserwatoremwInternecieanieserwerem* − *poprostuniedawasinikomudoCiebiedo*^{3} ± *cza*, *poprzezfiltrowanienadchodz* ± *cychpakietws*^{3}*u* ± *cychdoustanawianiapo*^{3} ± *cze*.

Czujno¶æ:

> **czasami** $\frac{1}{4}$**le skonfigurowana maszyna w sieci lokalnej zadecyduje o skierowaniu paru pakietów do sieci zewnêtrznej.**
> **Mi**^{3}*ojestmcpoinstruowafiltrpakietwbyda*^{3}*Ciznaotakichanormalnychzachowaniach*; *moebdzieszchcia*^{3}*co¶ztymzrobi*, *a*

3.2 Jak filtrowaæ pakiety pod Linuksem?

Kernele Linuksa mia^3*ywbudowanefiltrowaniepakietwodserii*1.1.*Pierwszageneracja*, *bazuj* ± *canaipfwzBSD*, *zosta*^{3}*aprzeniesionaprzezAlanaCox'apodkoniec*1994.*Zosta*^{3}*aonarozbudowanaprzezJos'aVos'aiinnyc*
cewprzestrzeniuytkownika'ipfwadm'kontrolowa^3*oregu*^{3}*yfiltruj*±*ce.Wpo*^{3}*owie*1998, *dlaLinuksa*2.2, *zmieni*^{3}*emdosym*
Michael'aNeuling'a, *iwprowadzi*^{3}*emnarzdzierwniedzia*^{3}*aj*±*cewprzestrzeniuytkownikanazwane'ipchains'.Ostateczn*

Potrzebujesz kernel z infrastruktur±*netfilter* : *netfiltertooglnyszkieletwkerneluLinuksadoktregomog*±
do^3±*czasiinnemodu*^{3}*y*(*takiejakmodu*^{3}*iptables*).*Oznaczatoepotrzebujeszkernelwwersji*2.3.15*lubp*$\frac{1}{4}$*niejszej*, *iwczasiek*

Narzêdzie `iptables` **wstawia i kasuje regu**^{3}*yztabelifiltrowaniapakietwkernela.Oznaczato*, *ecokolwiekdoniejwstawi*

`iptables` **zastêpuje** `ipfwadm` **i** `ipchains`**: zajrzyj do** 8 **(sekcji opisuj**±*cejuywanieipfwadmiipchains*)*poinformacjejakbezbole¶nieuniknprzesiadaniasinaiptablesje¶liuywaszjednegoztychnarzdzi*.

3.2.1 Zapisywanie regu^3*nasta*^{3}*e*

Twoje aktualne ustawienia ¶ciany ogniowej zapisane s±*wkerneluiwzwi* ± *zkuztymznikn* ± *porestarcie.Moeszwyprbowaskryptyiptables* − *saveiiptables* − *restorebyodpowiedniozapisajedoiodtworzyzpliku*.

Innym sposobem mo¿e byæ umieszczenie komend wymaganych by ustawiæ twoje regu^3*ywskrypciewykonywanymwczasiestartu.Upewnijsi, ezrobionco¶inteligentnegowwypadkugdybyco¶posz*^{3}*onietak*

4 Kim u diab^{3}ajeste¶idlaczegobawiszsimoimkernelem?

Jestem Rusty Russell; cz^3*owiekodpowiedzialnyza¶cianogniow±IPLinuksaijeszczejedenkoderktryznalaz*^{3}*siew*^{3}*a coduobytymrazemfiltrowaniepakietwwysz*^{3}*odobrze.Taks ± dz.*

Doskona^3*afirmaWatchGuardWatchGuard*http://www.watchguard.com

sprzedaj±ca¶cianyogniowe*Firebox, zaoferowa*^{3}*aebdziep*^{3}*acimizanic, wicmog*^{3}*emspdzaswjczaspisz ± ctendokumentizajmowasipoprzednimirzeczami.Przewidywa*^{3}*emezajmieto6miesicy, zaj*^{3}*o12, alenakocuczujezosta*^{3}*ot tku, padnitytwardydysk, ukradzionylaptop, paruszkodzonychsystemwplikwijedenzniszczonyekran, alejest.*

Póki jeszcze tu jestem, chcia^3*bymwyklarowamylnewraenianiektrychludzi : niejestemgurukernela.Wiemtowszystko, poniewamojapracaspowodowa*^{3}*aekontaktowa*^{3}*emsizlud*$\frac{1}{4}$*miktrzys± guru : David'emS.Miller'em, Aleksiej'emKuziecow'em, AndiKleen'em, Alan'emCox'em.S ± zajciuprawianiemg*^{3}*bokiejmagii, ajamog*^{3}*empobawisinap*^{3}*ytkichwodach, tamgdziejestbezpiecznie.*

5 Bardzo krótki przewodnik Rusty'ego do filtrowania pakietów

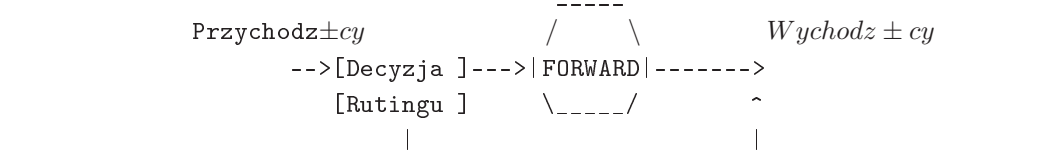
Wiêkszo¶æ ludzi ma pojedyñcze po^3 *± czeniePPPdoInternetu, iniechcebyktokolwiekmg*^{33} *± czysidonich, lubdo¶cianyogniowej :*

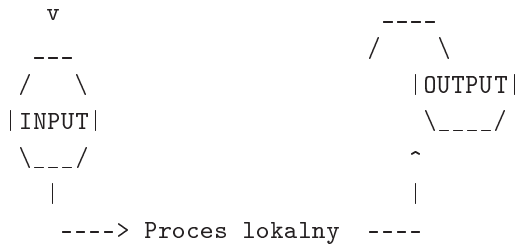
```
## Za3aduj modu3y ¶ledzenia po3 ± cze (niepotrzebne je¶li wbudowane w kernel)
# insmod ip_conntrack
# insmod ip_conntrack_ftp

## Stwórz 3acuch blokuj ± cy nowe po3 ± czenia, z wyj ± tkiem tych od ¶rodka
# iptables -N block
# iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT
# iptables -A block -m state --state NEW -i ! ppp0 -j ACCEPT
# iptables -A block -j DROP

## Do 3acuchw INPUT i FORWARD dodaj skok do tego nowego 3acucha
# iptables -A INPUT -j block
# iptables -A FORWARD -j block
```

6 Jak pakiety podró¿uj±przezfiltry

Kernel rozpoczyna pracê z trzema listami regu^3*wtabelifiltruj ± cej; nazywanesaone*^{3}*acuchami¶cianyogniowej, lubpoprostu*^{3}*acuchami.Tetrzynazwanezosta*^{3}*yINPUT(wej¶ciowy), O*

Dla fanów ASCII-art, ^{3}*acuchyu*^{3}*oones ± wnastpuj ± cysposb :* *(UWAGA : Wygl ± datozupe*^{3}*nieinaczejniwkernelach2.0i2.2!*





Trzy ko^3*areprezentuj±trzy*^{3}*acuchyoktrychwspomnia*^{3}*emwyej.Kiedypakietdocieradoko*^{3}*anadiagramie, sprawdzanyje podrpodiagramie.*

£añcuch to lista regu^3*.Kadaregu*^{3}*amwi′je¶linag*^{3}*wekpakietuwygl ± datak, tozrobimyztympakietemnastpuj±c±rzecz′.Je¶liregu*^{3}*aniepasujedopakietu, sprawdzanajestnastpna.Nakoniec,*

1. **Kiedy pakiet dociera do maszyny (powiedzmy, przez kartê Ethernetow±),** *kernelsprawdzanajpierwadresprzeznaczeniapakietu : nazywasitoroutingiem.Je¶lipakietprzeznaczonyjestdotegokompuera, pakietzostajeprzepuszczonydo*^{3}*acuchaIN*

2. **W innym przypadku, je¶li kernel nie ma w**^{3}*±czonegoprzekazywania(ang.forwarding), lubniewiejakprzekazapak czoneipakietjestprzeznaczonydoinnegointerfejsusieciowego(je¶liwoglemaszjeszczejeden), pakietprzechodziwprawo cego).Je¶lizostajezaakceptowany(ACCEPT), zostaniewys*^{3}*anydalej.Nakoniec, programpracuj ± cynatymkomputerzemoerwniewysy*^{3}*aw*^{3}*asnepakiety.Przejd±oneodrazudo*^{3}*acuchaOUTPUT(wyj¶ciowego) : je¶listwierdzionezaakceptujepakiet(ACCEPT), pakietprzechodzidow*^{3}*a¶ciwegointerfejsusieciowego.*

7 U¿ywanie iptables

`iptables` **ma ca**^{3}*kiemszczeg*^{3}*owypodrcznik(maniptables), doktregowartozajrzeje¶lichodzicioco¶konkretnego.Cizwas ipchainsmog ± poprostuzajrzedo10(rnicpomidzyiptablesiipchains); obanarzdzias ± bardzopodobne.*

Istnieje wiele rzeczy które mo¿esz zrobiæ przy u¿yciu `iptables`**. Zaczynasz z trzema wbudowanymi** ^{3}*acuchamiINPUT, OUTPUTiFORWARD, ktrychniemoeszskasowa.Spjrzmynalistmoliwychoperacjina*

3. **Stworzenie nowego** ^{3}*acucha(−N).Skasowaniepustego*^{3}*acucha(−X).*
2. **Zmiana polityki dla wbudowanego** ^{3}*acucha(−P).Wylistowanieregu*^{3}*w*^{3}*acuchu(−L).*

3. **Wyczyszczenie** ^{3}*acuchazregu*^{3}*(−F).Wyzerowanielicznikwpakietwibajtwewszystkichregu*^{3}*achw*^{3}*acuchu(−Z).*

Jest równie¿ parê sposobów na manipulowanie regu^3*amiwobrbie*^{3}*acucha* :

4. **Dodanie nowej regu**^{3}*ydo*^{3}*acucha(−A).Wstawienienowejregu*^{3}*ynapewnejpozycjiw*^{3}*acuchu(−I).*
2. **Zamiana regu**^{3}*ynapewnejpozycjiw*^{3}*acuchu(−R).Skasowanieregu*^{3}*ynapewnejpozycjiw*^{3}*acuchu, lubpierwszejktrapas*

7.1 Co zobaczysz gdy wystartujesz komputer

iptables mo¿e byæ modu^3*em, (′iptable_filter.o′), ktrypowinienbyautomatycznie*^{3}*adowanygdyporazpierwszyuruchon*

Zanim nie zostan±*wykonanejakie¶komendy(zwruwag, eniektredystrybucjewykonuj ± juoperacjeziptableswskryptachstartowych)niemaadnychregu*^{3}*wewbudowanych*^{3}*acuchach(′INPUT′,′ FORWARD′i′O domy¶ln±politykACCEPT.Moeszzmienidomy¶ln±polityk*^{3}*acuchaFORWARDprzezpodanieopcji′forward = 0′dom*

7.2 Operacje na pojedyñczej regule

Manipulowanie regu^3*amitobu*^{3}*kazmas*^{3}*emfiltrowaniapakietw.Najcz¶ciejbdzieszzapewnedodawa*^{3}*(−A)ikasowa*^{3}*(−*
prostymirozwiniciamitychkoncepcji.

Ka¿da regu^3*ajestzestawemwarunkwktrepakietmusispe*^{3}*niizawierainformacjcozrobije¶litaksista*^{3}*o(czylicel, ang.ta*
*cezadresuIP*127.0.0.1.*Wtymprzypadkunaszymiwarunkamis±zatem : protoko*^{3}*emmusibyICMP, aadresem*$\frac{1}{4}$*rd*^{3}*owym1*

127.0.0.1 to adres pêtli zwrotnej (ang. *loopback*), który posiadasz nawet wtedy gdy nie masz ¿adnego po^3*±czeniasieciowego.Moeszuyprogramu'ping'bywygenerowapakietytakiejakpowyej.Poleceniewysy*^{3}*apakie*
± danieecha(ang.echorequest)naktrewszystkiewsp^3*pracuj ± cehostyodpowiedz ± pakietemICMPtypu*0 −
echo.Tosprawia, epolecenietojestwygodnedlatestw.

```
3. # ping -c 1 127.0.0.1
   PING 127.0.0.1 (127.0.0.1): 56 data bytes
   64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.2 ms

   --- 127.0.0.1 ping statistics ---
   1 packets transmitted, 1 packets received, 0% packet loss
   round-trip min/avg/max = 0.2/0.2/0.2 ms
   # iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP
   # ping -c 1 127.0.0.1
   PING 127.0.0.1 (127.0.0.1): 56 data bytes

   --- 127.0.0.1 ping statistics ---
   1 packets transmitted, 0 packets received, 100% packet loss
   #
```

Widaæ powy¿ej ¿e pierwszy ping dociera (opcje '-c 1' powoduje wys^3*anietylkojednegopakietu).*

Dodajemy teraz (-A) do ^{3}*acucha'INPUT'regu*^{3}*, ktramwiepakietyz*127.0.0.1(*'−s*127.0.0.1*')protoko*^{3}*uICMP('−picmp*

Testujemy nastêpnie dzia^3*anienaszejregu*^{3}*y, wykonuj ± cdrugiping.Nast ± pipauzapoktrejprogramsipodda, pokrtkimoczekiwaniunaodpowied*$\frac{1}{4}$*ktranigdynienadejdzie.*

Mo¿emy skasowaæ nasz±*regu*^{3}*nadwasposoby.Popierwsze, poniewawiemyejesttojedynaregu*^{3}*aw*^{3}*acuchuwej¶ciowyr*

```
# iptables -D INPUT 1
#
```

Co spowoduje skasowanie regu^3*ynumer*1*w*^{3}*acuchuINPUT.*

Drugi sposób to dok^3*adneprzepisaniepolecepoopcji−A, alezamiastopcji−Apodajemyopcj−D.Przydajesitowprzypadku*

```
# iptables -D INPUT -s 127.0.0.1 -p icmp -j DROP
#
```

Sk^3*adniapolecenia−Dmusidok*^{3}*adnieodpowiadaopcjomktrepoda*^{3}*e¶przypoleceniu−A(lub−Iczy−R).Je¶liistniejewiele*
cazostaniaskasowana.

7.3 Specyfikacja filtrowania

Widzieli¶my ju¿ jak u¿ywaæ opcji '-p' by wskazaæ protokó^3*i'−s'bywskazaadres*$\frac{1}{4}$*rd*^{3}*owy, ales ± jeszczeinneopcjektrychmoemyuybyscharakteryzowapakiet.Poniejznajdzieszwyczerpuj ± cekompendium.*

7.3.1 Wskazanie adresów IP: $\frac{1}{4}$ród^{3}owegoidocelowego

Adres IP $\frac{1}{4}$ród^{3}owy('−s','−−source'lub'−−src')idocelowy('−d','−−destination'lub'−−dst')mog ± bypodanenaczterysposoby.Najcz¶ciejrobisitoprzezpodaniepe^{3}nejnazwy,takiejjak'localhost'czy'www.linuxhq.com'.D

Trzeci i czwarty sposób pozwalaj±nawskazaniegrupyadreswIP,takjaknaprzyk^{3}ad'199.95.207.0/24'lub'199.95.207.0/255 nazakresadreswIPod199.95.207.0do199.95.207.255w^3 ± cznie;cyfrypo'/'mwi ± ktracz¶adresuIPmaznaczenie.'/32'czyinaczej'/255.255.255.255'jestdomy¶lne(imwiewszystkieliczbywadresieIPs± wane).Bywskazadowolnyadres,monauy'/0'takjakponiej :

```
[ UWAGA: '-s 0/0' jest tu ca³kowicie zbdne. ]
# iptables -A INPUT -s 0/0 -j DROP
#
```

Ale takich konstrukcji u¿ywa siê rzadko, poniewa¿ efekt jest dok^{3}adnietakisamjakwprzypadkuniepodaniaopcji'−s'wogle.

7.3.2 Inwersja

Wiele flag, w^3±czaj±c'−s'(lub'−−source')i'−d'('−−destination')monapoprzedziznakiem'!'(wymawianym'nie')byws cedotychpodanych.Naprzyk^{3}ad'−s!localhost'bdziepasowadowszystkichpakietwniepochodz ± cychzlocalhost.

7.3.3 Protokó^3

Protokó^{3}podajesipoparametrze'−p'(lub'−−protocol').Protok^{3}moebynumerem(je¶liznaszwarto¶cinumeryczneprotok dla'TCP','UDP'i'ICMP'.Wielko¶literniemaznaczenia,wic'tcp'dzia^{3}ataksamojak'TCP'.

Nazwa protoko^{3}umoebypoprzedzonaprzezznak'!'bywskazanawszystkieoprczwymienionego,takjaknaprzyk^{3}ad'−p!TCP

7.3.4 Interfejs

Opcje '-i' (lub '-in-interface' czyli interfejs wej¶ciowy) i '-o' (lub '-out-interface' czyli interfejs wyj¶ciowy) u¿ywane s±dlawskazaniainterfejsu.Interfejstofizyczneurz ± dzeniedoktregopakietyprzychodz±('−i')izktregos±wysy^{3}ane('−o').Moeszuyprogramuifconfigbywylistowainterfejsy podniesione'(tzn.aktualniepracuj ± ce).

Pakiety podró¿uj±cew^{3}acuchuINPUTniemaj±interfejsuwyj¶ciowego,wicpodanieopcji'−o'wregulewtym^{3}acuchuspo ceprzez^{3}acuchOUTPUTniemaj±interfejsuwej¶ciowego,wicpodanieopcji'−i'wreguletego^{3}acuchaspowodujeeniebdzie

Tylko pakiety podró¿uj±ceprzez^{3}acuchFORWARDmaj ± zarwnointerfejswej¶ciowyiwyj¶ciowy.

Jest ca^{3}kowiciepoprawnewskazanieinterfejsuktryaktualnienieistnieje;regu^{3}aniebdziepasowa^{3}adoniczego,dopkiinter czewdzwanianychPPP(zwykleinterfejsmanazwppp0)ipodobnych.

Mo¿na równie¿ wskazaæ interfejs koñcz±cjegonazwprzez'+'cospowodujeeregu^{3}abdziepasowa^{3}adowszystkichinterfejsu guznakw(bezznaczeniaczyinterfejsaktualnieistniejeczynie).Naprzyk^{3}ad,bywskazaregu^{3}ktrapasujedowszystkichinte

Interfejs mo¿e byæ poprzedzony przez '!' ze spacjami wokó^3,cospowodujeepasowabd ± pakietyktrenies ± powi±zanezewskazanyminterfejsem(tzn.pakietnimniedotar^{3}dosystemu,lubniezamierzanimgoopu¶ci),np.−i!ppp+.

7.3.5 Fragmenty

Czasami pakiet jest zbyt du¿y by zmie¶ciæ siê ca^{3}ywjednostcetransmisji.Kiedysitakdzieje,jestondzielonynafragment

Problem z fragmentami polega na tym, ¿e pierwszy fragment posiada komplet pól nag^{3}wka(IP + TCP,UDPiICMP)ktrymonasprawdza,alenastpnefragmentymaj ±

tylkopodzbirnag^3*wkw*(*IPbezdodatkowychplspecyficznychdlaprotoko*^{3}*wktreprzenosipakiet*).*Wzwi* ± *zkuztymniemoliwejestanalizowaniepewnychinformacjiznag*^{3}*wkwfragmentw*(*takjakrobisitodlatypowychpakietwTC*

Je¶li prowadzisz ¶ledzenie po^3 ± *czelubNAT*, *towszystkiefragmentyzostan* ± *najpierwz*^{3}*ooneadopierop*$\frac{1}{4}$*niejprzekazanedokodufiltruj*±*cegopakiety*, *wicniepowiniene¶simartwifragmentami*.

W ka¿dym innym przypadku wa¿ne jest by zrozumieæ jak fragmenty traktowane s±*przezregu*^{3}*yfiltruj* ± *ce*.*Kadaregu*^{3}*aktramasprawdziinformacjektrychnieposiadamydladanegopakietu*, *niebdziepasowa*^{3}*a*.*Oznaczato*, *etylk* .*Wzwi*±*zkuztymregu*^{3}*a*$'$−*pTCP* − −*sportwww*$'$(*podaj*±*caport*$\frac{1}{4}$*rd*^{3}*owy*$'$*www*$'$)*nigdyniebdziepasowa*^{3}*adofragmentupak*

Mo¿esz jednak dodaæ regu^3*yspecjalniedladrugiegoinastpnychfragmentw*, *poprzezuycieopcji*$'$−*f*$'$(*lub*$'$− − *fragment*$'$).*I* !$'$.

Zwykle uwa¿a siê za bezpieczne umo¿liwienie drugiemu i nastêpnym fragmentom przej¶æ, poniewa¿ filtrowanie zajmie siê pierwszym fragmentem i w zwi±*zkuztymzapobiegniez*^{3}*oeniupakietunamaszyniedocelowej*; *zdrugiejstronyznaneby*^{3}*ypluskwyktrepowodowa*^{3}*yzaw*

Ma^3*auwagadospecwodsieci* : *pakietyznieksztа*^{3}*cone*(*TCP*, *UDPiICMPktres* ± *zbytkrtkiebykod¶cianyogniowejmg*^{3}*odczytaporty*, *czywprzypadkuICMPkodityp*)*s* ± *rwniewyrzucanegdyprowadzones*±*takieanalizy*.*Dok*^{3}*adnietaksamojestzfragmentamiTCPktrerozpoczynaj*± *siodpozycji*8.

Jako przyk^3*ad*, *poniszaregu*^{3}*awyrzuciwszystkiefragmentyprzeznaczonedla*192.168.1.1 :

```
# iptables -A OUTPUT -f -d 192.168.1.1 -j DROP
#
```

7.3.6 Rozszerzenia do iptables: Nowe cele i nowe testy

`iptables` s±*rozszerzalne*, *cooznaczaefunkcjonalno¶zarwnokernelajakinarzdziaiptablesmoebyrozszerzanabydodano*

Niektóre rozszerzenia s±*standardowe*, *innes* ± *trochbardziejegzotyczne*.*Oczywi¶cie*, *mog* ± *byonedodawaneprzezinnychludziidystrybuowaneniezaleniedlauytkownikwniszowych*.

Fizycznie rozszerzenia znajduj±*sizwyklewpodkatalogumodu*^{3}*wkernela*, *takjaknaprzyk*^{3}*ad*$'$*/lib/modules/*2.4.0 − *test*10/ *na*±*daniegdykernelzosta*^{3}*skompilowanyzopcj*±*CONFIG_KMOD*, *wicniepowinnobypotrzeby*^{3}*adowaniaichrcznie*.

Rozszerzenia do narzêdzia iptables s±*wsp*^{3}*dzielonymibibliotekami*, *ktreznajduj* ± *sizwyklew*$'$*/usr/local/lib/iptables/*$'$, *chodystrybucjemog*±*umie¶cijewkatalogachtakichjak*$'$*/lib/iptables/*$'$*czy*$'$*/usr/lib/*

Rozszerzenia mog±*naleedojednegozdwchtypw* : *nowychcelw*, *lubnowychtestw*(*porozmawiamyonowychcelachzamoment* *automatycznienowetesty* : *aktualnies* ± *nimiTCP*, *UDPiICMPtakjakpokaemytoponiej*.

Mo¿esz dla nich podaæ nowe testy w linii poleceñ po opcji '`-p`', który ^{3}*adujerozszerzenie*.*Dlasamodzielnychnowychtestw*, *uywasiopcji*$'$−*m*$'$*byza*^{3}*adowarozszerzenie*, *poktrejdostpnes*± *noweopcje*.

By uzyskaæ pomoc do rozszerzenia, u¿yj opcji ^{3}*aduj*±*cejgo*($'$−*p*$'$,$'$ −*j*$'$*lub*$'$−*m*$'$)*poktrejpodaj*$'$−*h*$'$*lub*$'$− − *help*$'$, *np*. :

```
# iptables -p tcp --help
#
```

Rozszerzenia TCP Rozszerzenia TCP ^{3}*adowanes* ± *automatyczniegdypodanoopcj*$'$−*ptcp*$'$.*Dodaj* ± *onenastpuj* ± *ceopcje*(*zktrychadnaniepasujedofragmentw*).

–tcp-flags

Po której nastêpuje opcjonalny znak '`!`', a nastêpnie dwa ci±*giflagktrepozwalaj* ± *wskazazestawflagdozbadania*.*Drugici* ± *gmwi*, *ktremaj* ± *byustawione*.*Naprzyk*^{3}*ad* :

```
# iptables -A INPUT --protocol tcp --tcp-flags ALL SYN,ACK -j DROP
```

mówi ¿e sprawdzone powinny zostaæ wszystkie flagi ('ALL' to synonim dla 'SYN,ACK,FIN,RST,URG,PSH'), ale tylko flagi SYN i ACK powinny byæ ustawione. Istnieje równie¿ argument 'NONE' który oznacza ¿e ¿adna flaga nie mo¿e byæ ustawiona.

–syn

opcjonalnie poprzedzona przez '!', jest skrótem dla '-tcp-flags SYN,RST,ACK SYN'.

–source-port

po której nastêpuje opcjonalny '!', a nastêpnie pojedyñczy port lub grupa portów TCP. Porty mog±*bywskazywaneprzeznazwytakiejakw/etc/serviceslubprzeznumery.Grupyportwwskazujesialboprzezdwienazwy*

–sport

to synonim '-source-port'.

–destination-port

i

–dport

maj±*takiesameopcjejakpowyej, aleokre¶laj ± portprzeznaczenia.*

–tcp-option

po którym nastêpuje opcjonalny znak ! i numer, które wskazuj±*naopcjTCPrwn ± wskazanemunumerowi.Pakietktrynieposiadakompletnegonag*^{3}*wkaTCPjestautomatycznieodrzucanyje¶liwykonanaz*

Parê s^3*wwyja¶nieniaoflagachTCP* Czasami u¿yteczne jest, by zezwoliæ na po^3 ± *czeniaTCPwjednymkierunkualeniewdrugim.Naprzyk*^{3}*ad, moeszchciezezwolinapo*^{3} ± *czeniadozewntrznegoserweraWWW, aleniepo*^{3} ± *czeniaodtegoserwera.*

Naiwnym rozwi±*zaniemby*^{3}*obyblokowaniepakietwTCPnadchodz ± cychztegoserwera.Niestety, po*^{3} ± *czeniaTCPwymagaj ± bypakietymog*^{3}*yporuszasiwjedn ± iwdrug ± stron.*

Rozwi±*zaniemjestblokowanietylkopakietwuywanychdonawi ± zaniapo*^{3} ± *czenia.Nazywasijepakietami SYN(dobrze, technicznierzeczbior ± cs ± topakietyzustawion ± flag ± SYNizgaszonymiflagamiRSTiACK, alenazywamyjepakietamiSYNbyby*^{3}*okrcej).Poprzezzabronienieruchutylkotym czeniomusamegoich*$\frac{1}{4}$*rd*^{3}*a.*

U¿ywa siê do tego opcji '-syn': która jest dozwolona tylko dla regu^3*ktrewskazuj ± naprotok*^{3}*TCP.Naprzyk*^{3}*ad, bywskazapo*^{3} ± *czeniaTCPz*192.168.1.1 :

```
-p TCP -s 192.168.1.1 --syn
```

Dzia^3*nieflagimonaodwrcipoprzedzaj±cj±'!', cooznacza, echodzinamopakietyrneodtychktreinicjuj±po*^{3}*± czenie.*

Rozszerzenia UDP S±*one*^{3}*adowaneautomatyczniepopodaniu'–pudp'.Udostpniaj ± opcj'– – source – port','– – sport','– – destination – port'i'– – dport', dok*^{3}*adnietakiesamejakdlaTCPpowyej.*

Rozszerzenia ICMP £adowane automatycznie po podaniu '`-p icmp`'. Udostêpniaj±*onetylkojedn* ± *now* ± *opcj* :

–icmp-type

po której nastêpuje opcjonalny znak '`!`', a nastêpnie albo nazwa typu pakietu ICMP (np. '`host-unreachable`', czyli *komputer nieosi±galny*), *lubnumertypu*(*np.*′3′), *lubnumertypuikododdzieloneprzez*′/′(*np.*′3/3′).*Listadostpnychnazwtypw IC*

Inne rozszerzenia testowe Inne rozszerzenia w paczce netfiltera s±*rozszerzeniamidemonstracyjnymi*, *ktre*(*je¶lijezainstalowano*)*mog* ± *bywywo*[3]*anepoprzezopcj*′−*m*′.

mac

Modu[3]*tenmusibywskazanyprzez*′−*mmac*′*lub*′− − *matchmac*′.*Uywasigodosprawdzania*$\frac{1}{4}$*rd*[3]*aEthernetowego*(*tzw cegopakietuiwzwi±zkuztymdzia*[3]*atylkow*[3]*acuchachPREROUTINGiINPUT.Udostpniaontylkojedn*± *opcj* :

–mac-source

po którym nastêpuje opcjonalny '`!`' a nastêpnie adres ethernetowy w formacie heksdecymalnym oddzielanym dwukropkami, np. '`-mac-source 00:60:08:91:CC:B7`'.

limit

Modu[3]*tenmusibywskazanyprzez*′−*mlimit*′*lub*′− − *matchlimit*′.*Uywasigodoograniczaniaczstotliwo¶cipasowania pasowaztak±czstotliwo¶ci±jakpodanawtejopcjiwczasiejedensekundy*(*domy¶lnie*3*krotnienagodzin*, *zseri*± 5).*Modu*[3]*umoliwiapodaniedwchargumentwopcjonalnych* :

–limit

po którym nastêpuje numer; okre¶la maksymalny ¶redni numer testów pozytywnych na sekundê. Numer mo¿e równie¿ wskazywaæ wprost jednostki, przez u¿ycie '`/second`', '`/minute`', '`/hour`' lub '`/day`', albo ich skrótów (np. '`5/second`' to to samo co '`5/s`').

–limit-burst

po którym nastêpuje numer, okre¶laj±*cymaksymaln* ± *seripoktrejpowyszylimitsiw*[3] ± *cza.*

U¿ywa siê tego testu zwykle w po[3]±*czeniuzcelemLOGbyzrealizowaograniczonelogowanie.Byzrozumiejaktodzia*[3] *caregu*[3]*a*, *ktralogujepakietyzdomy¶lnymilimitami* :

```
# iptables -A FORWARD -m limit -j LOG
```

Gdy pierwszy raz dochodzimy do regu[3]*y*, *pakietjestlogowany*; *taknaprawd*, *poniewadomy¶ln* ± *seri* ± *jest*5, *pierwszepipakietwzostaniezalogowane.Nastpnie*, *miniedwadzie¶ciaminutzanimzalogowanyzostanienastp cydotejregu*[3]*y*, *niezalenieodtegoilepakietwdoniejdotrze.Jednocze¶nie*, *kadedwadzie¶ciaminutktreminiebezpakie gu*100*minut*, *seriazostaniewpe*[3]*niodnowiona*; *do*5*sztuk*, *takjakzaczli¶my.*

Nota: nie mo¿esz aktualnie stworzyæ regu[3]*yktremaczasodnawianiasipowyej*59*godzin*, *wicje¶liustawisz¶redni*± *czstotliwo¶najedenpakietnadzie*, *numerseriimusibymniejszyni*3.

Mo¿esz równie¿ u¿yæ tego modu[3]*ubyzapobiecrozmaitymatakomOdmowyUs*[3]*ugi*(*ang.DenialofService*), *zwikszym*

Zabezpieczenie przed powodzi±*pakietwSYN*(*ang.Syn* − *flood*) :

```
# iptables -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT
```

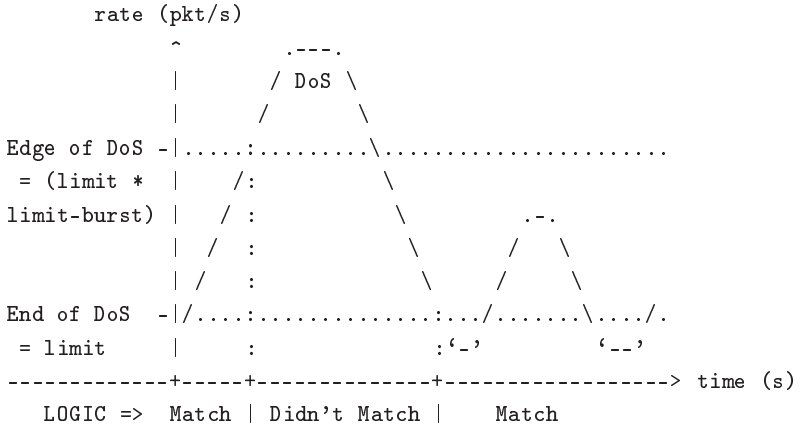
Skaner portó[3]*Furtive* :

```
# iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j ACCEPT
```

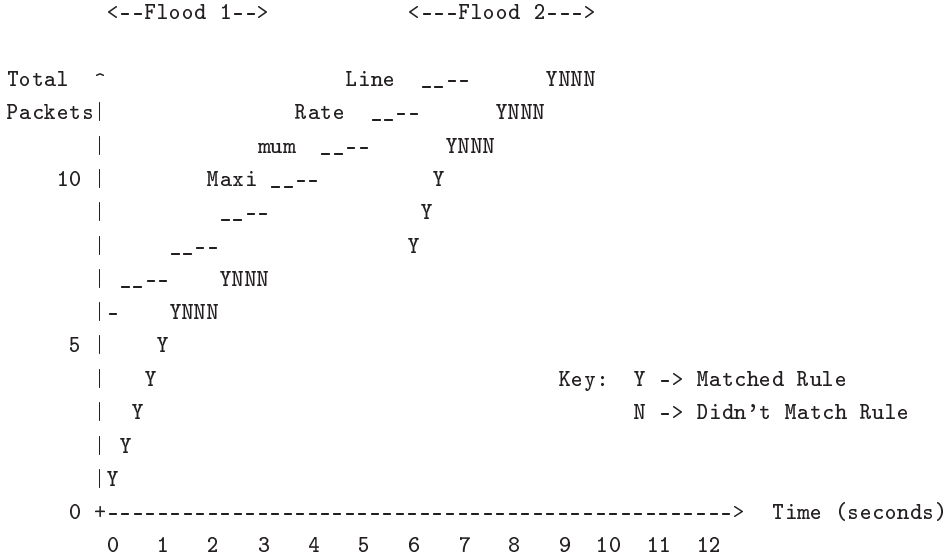
Ping of death:

```
# iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
```

Modu³*tendzia*³*ajak*"*drzwihisterii*", *takjakpokazanotonadiagramieponiej.*



Powiedzmy ¿e pasuje jeden pakiet na sekundê z seri±*piciupakietw*, *alepakietyzaczynaj* ± *dochodziwilo*¶*ciczterechnasekundprzeztrzysekundy*, *anastpnieznowupotrzechsekundach.*



Widaæ, ¿e pierwsze piêæ pakietów przekracza limit jednego pakietu na sekundê, a nastêpnie w³ ± *czasiograniczanie*(*limit*).*Je*¶*linast* ± *pipauza*, *kolejnaseriazostaniewpuszczonaaleniepowyejmaksymalnejczstotliwo*¶*ciokre*¶*lonejprzezregu*³(1*pakietnase*

Ten modu³*starasiustalipewnecharakterystykitwrcypakietu*, *dlapakietwgenerowanychlokalnie*.*Jegouyciejestmoliwety niemiew*³*a*¶*ciciela*, *awzwi* ± *zkuztymniebd* ± *pasowa*³*y.*

–uid-owner userid

Pasuje dla pakietów stworzonych przez proces ze wskazanym efektywnym (numerycznym) identyfikatorem u¿ytkownika.

–gid-owner groupid

Pasuje dla pakietów stworzonych przez proces ze wskazanym efektywnym (numerycznym) identyfikatorem grupy.

–pid-owner processid

Pasuje dla pakietów stworzonych przez proces ze wskazanym efektywnym (numerycznym) identyfikatorem procesu.

–sid-owner sessionid

Pasuje dla pakietów stworzonych przez proces we wskazanej grupie sesji.

Jest to eksperymentalny modu^3*ktregouywasiprzezpodanie*$'-munclean'lub'--matchunclean'.Wykonujernelosowetest$
cenapakiecie.Modu^3*tennieby*^{3}*sprawdzanyiniepowinienbyuywanyjakotestzwi* $\pm$
zanyzbezpieczestwem(prawdopodobniesprawiaewszystkowygl$\pm$*dajeszczegorzej, poniewasammoemiepluskwy).Nieud*a

Test Stanu Najbardziej u¿ytecznym testem jest ten dostarczany przez rozszerzenie '`state`', który interpretuje analizê ¶ledzenia po$^3 \pm$ *czemodu*^{3}*u'ip_conntrack'.Generalniebardzozalecasijegowykorzystanie.*

Podanie w regule opcji '`-m state`' udostêpnia dodatkow$\pm$*opcj*$'--state', ktrajestlist$ $\pm$
oddzielonychstanwdoprzetestowania(opcja'!'wskazujenapakietyniepasuj $\pm$ *cedowskazanychstanw).Stanamiktremon*e

NEW (NOWY)

Pakiet który tworzy nowe po$^3 \pm$ *czenie.*

ESTABLISHED (NAWI¿ZANY)

Pakiet który nale¿y do istniej$\pm$*cegopo*$^3 \pm$ *czenia(np.pakietodpowiedzi, lubpakietwychodz* $\pm$ *cywpo*$^3 \pm$ *czeniuktreotrzyma*^{3}*ojuodpowiedzi).*

RELATED (POWI¿ZANY)

Pakiet który jest powi$\pm$*zanyzistniej*$\pm$*cympo*$^3\pm$*czeniem, aleniejestjegocz¶ci*$\pm$*, tj.nppakietzb*^{3}*demICMP, lub(je¶liza*^3a
cypo$^3 \pm$ *czenieftpdladanych.*

INVALID (B£ÊDNY)

Pakiet który nie mo¿e byæ zidentyfikowany z jaki¶ powodów: mog$\pm$*tobywyczerpaniesipamici, lubb*^{3}*dyICMPktrenienale*$:$
doadnegoznanegopo$^3 \pm$ *czenia.Generalnie, pakietytegotypupowinnosiodrzuca.*

Przyk^3*ademwykorzystaniategopotnegorozszerzeniamog*^{3}*obyby* :

```
# iptables -A FORWARD -i ppp0 -m state ! --state NEW -j DROP
```

7.4 Cel

Znamy ju¿ testy które mo¿emy przeprowadziæ na pakiecie, potrzebujemy zatem sposobu by wskazaæ co robiæ z pakietami które pasuj$\pm$*donaszychtestw.Nazywasitocelem(ang.target)regu*^{3}*y.*

S$\pm$*dwaprostewbudowanecele* : *DROP(wyrzuci)iACCEPT(zaakceptowa).Jujewidzieli¶my.Je¶liregu*^{3}*apasujedopakie*
lospakietuzosta^3*juokre¶lony.*

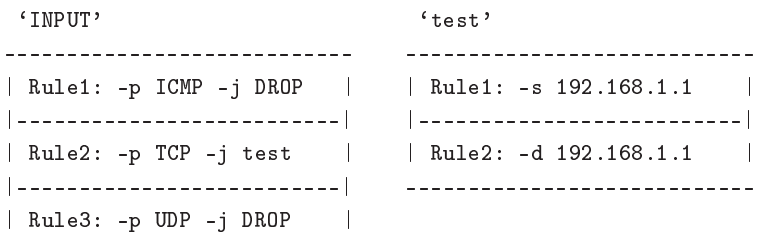
Istniej$\pm$*jeszczedwainnetypycelw* : *rozszerzeniai*^{3}*acuchyzdefiniowaneprzezuytkownika.*

7.4.1 £añcuchy zdefiniowane przez u¿ytkownika

Bardzo potê¿n±w^{3}asno¶ci±ktr±iptablesdziedziczyzipchainsjestmoliwo¶tworzeniaprzezuytkownikanowych^{3}acuchw, konwencj±, wszystkie^{3}acuchygenerowaneprzezuytkownikapisanes±ma^{3}ymiliteramibyodrnijeodwbudowanych(opisze

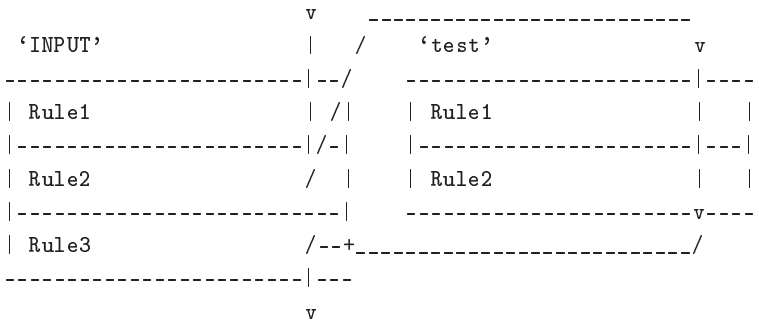
Kiedy do regu^{3}ydocierapakietktrypasuje, aceltejregu^{3}yzdefiniowanyjestjako^{3}acuchzdefiniowanyprzezuytkownika, r

Czas na trochê rysunków ASCII. Rozwa¿my dwa (¶miesznie proste) ^{3}acuchy : $INPUT$(^{3}acuchwbudowany)itest(^{3}acuchzdefiniowanyprzezuytkownika).



Rozwa¿my pakiet TCP nadchodz±cyz192.168.1.1iwys^{3}anydo1.2.3.4.Wchodziondo^{3}acuchaINPUTirozpoczynasisprawd ganyjestkoniec^{3}acucha'test'.Wracamydo^{3}acuchaINPUT, wktrymostatniosprawdzali¶myregu^{3}drug±, terazwicspraw ktrarwnieniepasuje.

Zatem droga pakietu wygl±dawsposbnastpuj ± cy :



£añcuchy zdefiniowane przez u¿ytkownika mog±jakocelwskazywainne^{3}acuchyrwniezdefiniowaneprzezuytkownika(ale tworzyptli : twjpakietzostaniewyrzuconyje¶liokaesiejestsprawdzanywptli).

7.4.2 Rozszerzenia do iptables: Nowe Cele

Innym typem rozszerzenia jest cel. Cel sk^{3}adasizmodu^{3}ukernelaiopcjonalnychrozszerzeiptables, ktrezapewniaj± opcjedlaliniipolece.Jestkilkatakichrozszerzewstandardowejdystrybucjinetfilter :

LOG

Modu^{3}tenzapewnialogowaniewkernelupasuj ± cychpakietw.Udostpnianastpuj ± ceopcje :

–log-level

Po którym nastêpuje nazwa poziomu logowania lub odpowiednik numeryczny. Prawid^{3}owyminazwamis±(wielko¶literniejestwana)'debug',' info',' notice',' warning',' err',' crit',' alert'i'e cyfryod7do0.Sprawd$\frac{1}{4}$stronpodrcznikasyslog.confbydowiedziesicooznaczaj ± poszczeglnepoziomy.Domy¶lnymjest'warning'.

–log-prefix

po którym nastêpuje ci±gdo29znakw, ktrydodawanyjestdologowanejinformacjibyumoliwijejjednoznaczn identyfikacj.

Modu³*tenuywanyjestnajcz¶ciejztestemlimit, dzikiczemunieza¶miecaszsobielogw.*

Modu³*tenmatakiesamodzia³aniejak'DROP', pozatymetonadawcypakietuodsy³anyjestpakietICMP'portunreachable'. dICMPniezostanieodes³anyje¶li(sprawd¼RFC*1122) :

- Pakiet którego dotyczy ta regu³*ajestwiadomo¶ci±ICMPob³dzie, lubnieznanymtypemwiadomo¶ciICMPPakietkt*

- Wys³*ali¶myjuostatniozbytduowiadomo¶ciob³dachICMPdotegonadawcy(zajrzyjdo/proc/sys/net/ipv4/icmp_ratelim*

  Do REJECT mo¿na równie¿ dodaæ opcjonalny argument '`-reject-with`' który pozwala na zadeklarowanie jaki dok³*adniepakietICMPmazostaodes³anyzamiastdomy¶lnego'portunreachable'.Sprawd¼stronpodrcznika.*

7.4.3 Specjalne cele wbudowane

S±*dwawbudowanespecjalnecele* : *RETURN*(*POWRT*)*iQUEUE*(*KOLEJKA*).

`RETURN` ma dok³*adnietensamefektjakzakoczeniesprawdzania³acucha* : *dlaregu³yw³acuchuwbudowanymsprawdzanajestwtedypolityka.Dlaregu³ywzdefiniowanymprzezuytkownika³acuchu,*

`QUEUE` to cel który kolejkuje pakiety dla przetwarzania w przestrzeni u¿ytkownika. ¯eby mo¿na by³*otencelzastosowa, potrzebnes* ± *jeszczedwask³adniki* :

- program **obs**³*uguj* ± *cykolejk*(*ang.queuehandler*), *ktryzajmiesimechanik* ± *przekazywaniapakietwpomidzykernelemiprzestrzeni* ± *uytkownika*(*ang.userspace*); *orazaplikacjadzia³aj*± *cawprzestrzeniuytkownikaktrabdziepotrafi³aobs³uyprzyjcie, ewentualn*±*modyfikacjiopcjonalnewydaniewerdyktuw*

  Standardowym programem obs³*uguj*±*cymkolejkidlaIPv4jestwiptablesmodu³ip_queue, ktrydystrybuowanyjestzkernel*

  Poni¿ej przedstawiono krótki przyk³*adjakuyiptableszkolejk*±*pakietwdoprzetwarzaniawprzestrzeniuytkownika* :

  ```
  # modprobe iptable_filter
  # modprobe ip_queue
  # iptables -A OUTPUT -p icmp -j QUEUE
  ```

  W powy¿szych regu³*ach, pakietyICMPgenerowanelokalnie*(*takjaknaprzyk³adprzyuyciupoleceniaping*)*przekazywanes domodu³uip_queue, ktrystarasidostarczypakietydoaplikacjidzia³aj*±*cejwprzestrzeniuytkownika.Je¶liniematakiejap wyrzucane.*

  By napisaæ tak±*aplikacj, naleyuyAPIlibipq.Dystrybuowanajestonarazemziptables.Kodprzyk³adowyznajdujesiwnar*

  Status modu³*uip_queuemoebysprawdzonyprzezwywo³anie* :

  ```
  /proc/net/ip_queue
  ```

  Maksymalna d³*ugo¶kolejki*(*tzn.ilo¶pakietwdostarczonychdoprzestrzeniuytkownikabezodpowiedzi*)*moebykontrolowan*

  ```
  /proc/sys/net/ipv4/ip_queue_maxlen
  ```

  Domy¶ln±*warto¶ci* ± *jest*1024.*Kiedyzostajeosi* ± *gnitylimit, nowepakietybd* ± *wyrzucanedopkid³ugo¶kolejkiniespadnieponiejwarto¶cimaksymalnej.Dobreprotoko³ytakiejakTCPinterpretuj*± *wyrzucanepakietyjakot³okiprawdopodobniedadz*±*sobiespokjgdykolejkasiwype³ni.Monaoczywi¶cietrochpoeksperyme maksymaln* ± *d³ugo¶kolejkidlaokre¶lonejsytuacji, je¶lidomy¶lnawarto¶jestzbytma³a.*

7.5 Operacje na ca³ym³acuchu

Bardzo przydatn±*opcj*±*wiptablesjestmoliwo¶grupowaniaregu³w³acuchy.Moeszjenazwajakchcesz, alezalecamraczej do*31*liter.*

7.5.1 Tworzenie nowego ^3acucha

Stwórzmy nowy $^3acuch.Poniewajestemkolesiemzwyobra\frac{1}{4}ni\pm, nazwijmygo'test'.Moemyuyalbo'-N'albo'--new-ch$

```
# iptables -N test
#
```

Proste. Mo¿esz teraz dodaæ do niego swoje regu$^3ytakjaktojuopisano.$

7.5.2 Kasowanie ^3acucha

Kasowanie $^3acucharwniejestproste, uywasidotegoopcji'-X'lub'--delete-chain'.Adlaczego'-X'?C, wszystkiedobrel$

```
# iptables -X test
#
```

Jest jednak parê ograniczeñ dotycz±$cychkasowania^3acuchw$: $musz \pm bypuste(sprawd\frac{1}{4}sekcj7.5.3(Oprnianie^3acucha)poniej)iniemog\pm bywskazywanejakocelwinnejregule.Niemoeszrwnies$

Je¶li nie podasz nazwy $^3acucha, skasowanezostan\pm wmiarmoliwo¶ciwszystkie^3acuchyzdefiniowaneprzezuytkownika.$

7.5.3 Opró¿nianie ^3acucha

Istnieje oczywi¶cie równie¿ sposób by wykasowaæ wszystkie regu$^3yz^3acucha.Uywasidotegoopcji'-F'(lub'--flush').$

```
# iptables -F FORWARD
#
```

Je¶li nie wska¿esz konkretnego $^3acucha, oprnionezostan \pm wszystkie.$

7.5.4 Listowanie zawarto¶ci ^3acucha

Mo¿esz wylistowaæ regu$^3yw^3acuchu, uywaj \pm copcji'-L'(lub'--list').$

Pozycja '`refcnt`' przy ka¿dym $^3acuchuzdefiniowanymprzezuytkownikapodajenumerregu^3ktreodwo^3uj \pm sidotego^3acucha.Warto¶tamusibyrwnazero(a^3acuchmusibypusty), bytaki^3acuchmonaby^3oskasowa.$

Je¶li pominiêto nazwê $^3acucha, wylistowanezostan \pm wszystkie^3acuchy, nawettepuste.$

Istniej±$trzyopcjektremog\pm towarzyszyopcji'-L'.Opcja'-n'(numerycznie)jestotyleprzydatna, ezapobiegasprawdzaniu cymadresomIPprzeziptables, comoespowodowaduezw^3okije¶litwjDNS(azak^3adamyeuywaszDNSjakwikszo¶ludzi)n$

Opcja '`-v`' pokazuje wszystkie detale regu$^3, takiejaklicznikipakietwibajtw, porwnaniaTOS(TypuUs^3ugi, ang.TypeofSe pominite.$

Zwróæ uwagê ¿e liczniki pakietów i bajtów drukowane s±$przyuyciusuffiksw'K','M'lub'G', dlaodpowiednio1000, 1,000,0 due.$

7.5.5 Resetowanie (zerowanie) liczników

Czasami przydatne jest móc wyzerowaæ liczniki. Wykonuje siê to przez u¿ycie opcji '`-Z`' (lub '`-zero`').

Rozwa¿ poni¿szy przyk^3ad :

```
# iptables -L FORWARD
# iptables -Z FORWARD
#
```

Pewna liczba pakietów mog^3*abyprzej¶pomidzywydaniempoleceniazopcj* ±′ −*L*′*a*′−*Z*′.*Wzwi* ± *zkuztym*, *moesztychopcjiuywarazem*, *bywyzerowalicznikidok*^{3}*adniewmomencieichwy¶wietlenia*.

7.5.6 Okre¶lanie polityki

Wspomnieli¶my ju¿ co dzieje siê gdy pakiet dociera do koñca wbudowanego ^{3}*acucha*, *kiedyrozmawiali¶myotymjakpakietpodrujeprzez*^{3}*acuchy.Wtymprzypadkuolosiepakietudecydujepolitykadla*^{3} *przypisan*±*polityk*, *poniewaje¶lipakietdocieradokoca*^{3}*acuchazdefiniowanegoprzezuytkownika*, *sprawdzaniewracadop*

Polityk±*moebyACCEPTlubDROP*, *naprzyk*^{3}*ad* :

```
# iptables -P FORWARD DROP
#
```

8 U¿ywanie ipchains i ipfwadm

W dystrybucji netfilter znajduj±*simodu*^{3}*yipchains.oiipfwadm.o.Monaza*^{3}*adowajedokernela*(*UWAGA* : *s* ± *niekompatybilnezmodu*^{3}*emip_tables.o*!).*Moesznastpnieuywaichtakjakzastarychdobrychczasw*.

Bêd±*onewspieranejeszczeprzezjaki¶czas.Wydajemisiesensownymwzoremjest*2 ∗ [*notkaozast* ± *pieniu* − *pierwszastabilnadystrybucja*], *poktrymtoczasiedostpnajeststabilnawersjanowegoodpowiednika.Oznaczatoewsparcied*

9 £±*czeniefiltrowaniapakietwiNAT*

Zwykle u¿ywa siê jednocze¶nie Translacji Adresów Sieciowych (NAT, zajrzyj do NAT HOWTO) i filtrowania pakietów. Dobra wiadomo¶æ jest taka ¿e ^{3} ± *czysijebardzodobrze*.

Projektujesz swój filtr pakietów kompletnie ignoruj±*cNAT.Adresy*$\frac{1}{4}$*rd*^{3}*oweiprzeznaczeniaktrebdziesprawdza*^{3}*filtrpaki* *prawdziwymi*′*adresami.Naprzyk*^{3}*ad*, *je¶liprowadziszDNATiwysy*^{3}*aszpo*^{3} ± *czeniado*1.2.3.4*naport*80*przez*10.1.1.1*port*8080, *filtrpakietwzobaczypakietypodruj* ± *cedo*10.1.1.1*naport*8080(*prawdziwyadresprzeznaczenia*), *anie*1.2.3.4*naport*80.*Podobnie*, *moeszzignorowamasquerading zpunktuwidzeniafiltrapakietwpakietybd*±*nadchodzi*^{3}*yzprawdziwychwewntrznychadreswIP*(*powiedzmy*10.1.1.1)*aodp*

Mo¿esz u¿ywaæ testu stanu ('state') bez dostarczania dodatkowej pracy filtrowi pakietów, poniewa¿ NAT wymaga i tak ¶ledzenia po^3 ± *cze*(*ang.connectiontracking*).*Byrozszerzyprostyprzyk*^{3}*admaskaradyzNATHOWTOozabronieniekreowaniunowychpo czezinterfejsuppp*0, *zrobi*^{3}*by¶tak* :

```
# Masquerade out ppp0
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE

# Disallow NEW and INVALID incoming or forwarded packets from ppp0.
iptables -A INPUT -i ppp0 -m state --state NEW,INVALID -j DROP
iptables -A FORWARD -i ppp0 -m state --state NEW,INVALID -j DROP

# Turn on IP forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward
```

10 Ró¿nice pomiêdzy iptables i ipchains

- Po pierwsze, nazwy wbudowanych $^3acuchwzosta^3yzmienionezma^3ychnaDU\Psi Elitery, poniewa^3acuchyINPUTiOU$
- Porty TCP i UDP podaje siê teraz przez opcje `-source-port` lub `-sport` (czy te¿ `-destination-port`/`-dport`) i zapisuje po wskazaniu protoko$^3u('-ptcp'lub'-pudp')poniewadopieroone^3aduj\pm rozszerzeniaodpowiednioTCPiUDPOpcjTCP'-y'zmie$ $zapisapo'-ptcp'.$
- Cel DENY w koñcu nazywa siê DROP (WYRZUCIÆ).
- Dzia$^3azerowaniepojedyczych^3acuchwzjednoczesnymwylistowaniemichzawarto\P ci.Dzia^3azerowaniewbudowany$ $czniezkasowaniemlicznikwwywo^3aniapolitykidladanego^3acucha$
- Listowanie $^3acuchwdostarczaci'atomowego'zdjcia(ang.snapshot)licznikw.REJECTiLOGs \pm terazcelamirozszerzonymi, cooznaczaes \pm osobnymimodu^3amikernela.$
- Nazwy $^3acuchwmog\pm miedo31znakw.OpcjaMASQnazywasiwkocuMASQUERADEiuywainnejsk^3adni.REDIR$ $HOWTObyuzyskawicejinformacjijakuytychopcji.$

- Opcja '`-o`' nie jest ju¿ u¿ywana by kierowaæ pakiety do urz$\pm dzeniazprzestrzeniuytkownika(sprawd\frac{1}{4}opcj'-i'powyej).W$

11 Porady w projektowaniu filtra pakietów

W dziedzinie bezpieczeñstwa komputerowego zwykle za powszechn$\pm m \pm$ $dro\P uwaasiblokowaniewszystkiegoadopieropotemotwieraniuodpowiednichportwwmiarjakstaj \pm$ $siepotrzebne.Mwisiotymzwykle'toconiejestwyra\frac{1}{4}niedozwolone, jestzabronione'.Zalecamtopodej\P cie, je\P libezpieczes$

Nie uruchamiaj ¿adnych us$^3ugktrychniemusiszmie, nawetje\P liwydajecisiezablokowa^3e\P donichdostp.$

Je¶li budujesz dedykowan$\pm\P cianogniow\pm, rozpocznijodzerazblokowaniemwszystkichpakietw, potemdodawajus^3ugiire$ $imdzia^3a.$

Zalecam równie¿ bezpieczeñstwo 'warstwowe': po$^3 \pm cztcp - wrappers(dlapo^3 \pm$ $czedofiltrapakietw), proxy(dlapo^3\pm czeprzechodz\pm cychprzezfiltrpakietw), weryfikacjdrogi(ang.routeverification)if$ $naprzyk^3ad, twojasiewewntrznamaadresy10.1.1.0/24, apakietztakimadresemdocieradofiltrapakietwprzezinterfejsze$ $powinienzostaodrzucony.Moetozostaw^3 \pm czonedlajednegointerfejsu(ppp0)takjakniej$:

```
# echo 1 > /proc/sys/net/ipv4/conf/ppp0/rp_filter
#
```

Lub dla wszystkich istniej$\pm cychiprzysz^3ychinterfejswtakjakniej$:

```
# for f in /proc/sys/net/ipv4/conf/*/rp_filter; do
#     echo 1 > $f
# done
#
```

Debian robi to domy¶lnie je¶li jest to mo¿liwe. Je¶li masz routing asymetryczny (tzn. spodziewasz siê pakietów nadchodz$\pm cychzdziwnychkierunkw), bdzieszprawdopodobniemusia^3wy^3 \pm$ $czytakiefiltrowanienatychinterfejsach.$

Logowanie jest u¿yteczne w trakcie konfigurowania ¶ciany ogniowej, gdy co¶ nie dzia$^3a, alenadzia^3aj \pm$ $cej\P cianieogniowejzawszepo^3 \pm czlogowaniezopcj \pm' limit', byzapobieczape^3nieniutwoichlogw.$

Zalecam równie¿ ¶ledzenie po^3 ± *czedlasystemwwktrychbezpieczestwojestspraw* ± *priorytetow*± : *wprowadzapewneop*$\frac{1}{4}$*nienia, poniewa¶ledzones* ± *wszystkiepo*^{3} ± *czenia, alejesttobardzoprzydatnewkontrolowaniudostpudotwoichsieci.Bymoebdzieszmusia*^{3}*za*^{3}*adowamodu*^{3}$'$*ip_conntr*
cy(*np.*$'$*ip_conntrack_ftp.o*$'$).

```
# iptables -N no-conns-from-ppp0
# iptables -A no-conns-from-ppp0 -m state --state ESTABLISHED,RELATED -j ACCEPT
# iptables -A no-conns-from-ppp0 -m state --state NEW -i ! ppp0 -j ACCEPT
# iptables -A no-conns-from-ppp0 -i ppp0 -m limit -j LOG --log-prefix "Bad packet from ppp0:"
# iptables -A no-conns-from-ppp0 -i ! ppp0 -m limit -j LOG --log-prefix "Bad packet not from ppp0:"
# iptables -A no-conns-from-ppp0 -j DROP

# iptables -A INPUT -j no-conns-from-ppp0
# iptables -A FORWARD -j no-conns-from-ppp0
```

Budowanie dobrej ¶ciany ogniowej jest poza tematem tego HOWTO, ale moj±*rad*±*jest*$'$*b*±*d*$\frac{1}{4}$*minimalist*±$'$
.ZajrzyjdoSecurityHOWTOpowicejinformacjiotestowaniuisprawdzaniutwojejmaszyny.