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 mó[3]*bymchciefiltrowapakiety*? . . . 3

3.2 Jak filtrowaæ pakiety pod Linuksem? . . . 3

3.2.1 Zapisywanie regu[3]*nasta*[3]*e* . . . 4

4 Kim u diab[3]*ajeste¶idlaczegobawiszsimoimkernelem*? **4**

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

6 Jak pakiety podró¿uj±*przezfiltry* **5**

7 U¿ywanie iptables **5**

7.1 Co zobaczysz gdy wystartujesz komputer . . . 6

7.2 Operacje na pojedyñczej regule . . . 6

7.3 Specyfikacja filtrowania . . . 7

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 . . . 8

7.3.5 Fragmenty . . . 8

7.3.6 Rozszerzenia do iptables: Nowe cele i nowe testy . . . 9

7.4 Cel . . . 13

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

7.4.2 Rozszerzenia do iptables: Nowe Cele . . . 14

7.4.3 Specjalne cele wbudowane . . . 15
7.5 Operacje na ca[3]*ym*[3]*acuchu* . . . 15
7.5.1 Tworzenie nowego [3]*acucha* . . . 15
7.5.2 Kasowanie [3]*acucha* . . . 16
7.5.3 Opró¿nianie [3]*acucha* . . . 16
7.5.4 Listowanie zawarto¶ci [3]*acucha* . . . 16
7.5.5 Resetowanie (zerowanie) liczników . . . 16
7.5.6 Okre¶lanie polityki . . . 17

8 U¿ywanie ipchains i ipfwadm 17

9 £±*czenie filtrowania pakietw iNAT* 17

10 Ró¿nice pomiêdzy iptables i ipchains 18

11 Porady w projektowaniu filtra pakietów 18

1 Wprowadzenie

Witam Szanownego czytelnika.

Zak[3]*adam, ewieszcotoadresIP, adressieciowy, maskasieciowa, rutingiDNS.Je¶linie, polecamprzeczytanieHOWTONetw*

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, wstanieparanoiiposzukiwabdziecikiegou*

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¶ci wypowiedziijednocze¶nie zapobi zanywtymHOWTO.*

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

(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'owiWelte*http://netfilter.gnumonks.org

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.takjakbypakiet*

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

3.1 Dlaczego mó g^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}*wekpakietuposiada*
> *dookre¶lonychcz¶cisiecizewntrznej.Innymprzyk*^{3}*ademmoebyto* : *uywamNetscapedoogl* ± *daniaarchiwwDilbert'a.Jesttammasareklampochodz*±*cychzadresudoubleclick.net*, *wicNetscapetraciczasbyje*^{3}*adowa*
> *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.Naprz*
> *cymodrnychz*^{3}*o¶liwychuytkownikwsieci.Innymprzyk*^{3}*ademmoebytwojeyczenie*, *byniezezwalanatelnet'owaniesinaT*
> *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*, *albo*

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'aiinnychdl*
cewprzestrzeniuytkownika'ipfwadm'kontrolowa^3*oregu*^{3}*yfiltruj*±*ce.Wpo*^{3}*owie*1998, *dlaLinuksa*2.2, *zmieni*^{3}*emdosymocn*
Michael'aNeuling'a, *iwprowadzi*^{3}*emnarzdzierwniedzia*^{3}*aj*±*cewprzestrzeniuytkownikanazwane'ipchains'.Ostatecznie*, *w*

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

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

`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(zw*

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

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

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

sprzedaj±*ca¶cianyognioweFirebox, zaoferowa*^{3}*aebdziep*^{3}*acimizanic, wicmog*^{3}*emspdzaswjczaspisz* ± *ctendokumentizajmowasipoprzednimirzeczami.Przewidywa*^{3}*emezajmieto6miesicy, zaj*^{3}*o12, alenakocuczujezosta*^{3}*otozr 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

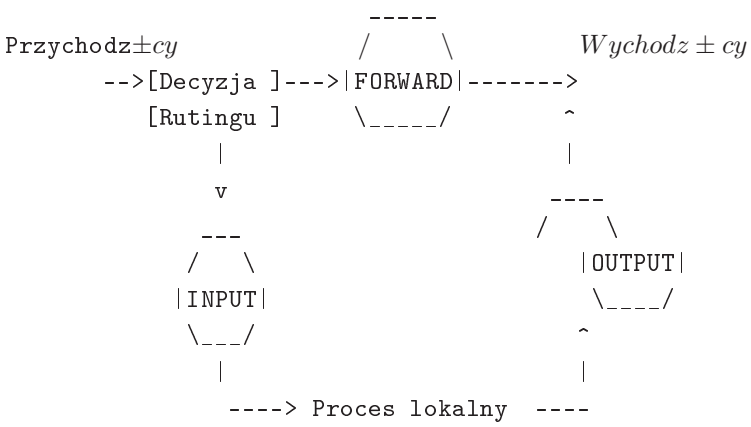
## Stwórz 3acuch blokuj ± cy nowe po3 ± czenia, z wyj ± tkiem tych od ¶rodka
# iptables -N block
# iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT
# iptables -A block -m state --state NEW -i ! ppp0 -j ACCEPT
# iptables -A block -j DROP

## 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*), *OUT*

Dla fanów ASCII-art, ^{3}*acuchyu*^{3}*oones* ± *wnastpuj* ± *cysposb* : (*UWAGA* : *Wygl* ± *datozupe*^{3}*nieinaczejniwkernelach*2.0*i*2.2!



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

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

1. **Kiedy pakiet dociera do maszyny (powiedzmy, przez kartê Ethernetow**±), *kernelsprawdzanajpierwadresprzeznaczeniapakietu* : *nazywasitoroutingiem.Je¶lipakietprzeznaczonyjestdotegokompuera*, *pakietzostajeprzepuszczonydo*^{3}*acuchaINPUT*
2. **W innym przypadku, je¶li kernel nie ma w**^{3}±*czonegoprzekazywania*(*ang.forwarding*), *lubniewiejakprzekazapakiet*, *j czoneipakietjestprzeznaczonydoinnegointerfejsusieciowego*(*je¶liwoglemaszjeszczejeden*), *pakietprzechodziwprawonan 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.Cizwasktr ipchainsmog* ± *poprostuzajrzedo*10(*rnicpomidzyiptablesiipchains*); *obanarzdzias* ± *bardzopodobne.*

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

1. **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** $^3acuchazregu^3(-F).Wyzerowanielicznikwpakietwibajtwwewszystkichregu^3achw^3acuchu(-Z).$

   Jest równie¿ parê sposobów na manipulowanie regu$^3amiwobrbie^3acucha$:

   1. **Dodanie nowej regu**$^3ydo^3acucha(-A).Wstawienienowejregu^3ynapewnejpozycjiw^3acuchu(-I).$

2. **Zamiana regu**$^3ynapewnejpozycjiw^3acuchu(-R).Skasowanieregu^3ynapewnejpozycjiw^3acuchu, lubpierwszejktrapasuje($

7.1 Co zobaczysz gdy wystartujesz komputer

iptables mo¿e byæ modu$^3em, ('iptable_filter.o'), ktrypowinienbyautomatycznie^3adowanygdyporazpierwszyuruchomisz$

Zanim nie zostan$\pm wykonanejakie\P komendy(zwruwag, eniektredystrybucjewykonuj \pm juoperacjeziptableswskryptachstartowych)niemaadnychregu^3wewbudowanych^3acuchach('INPUT',' FORWARD'i'OUT$
$domy\P ln\pm politykACCEPT.Moeszzmienidomy\P ln\pm polityk^3acuchaFORWARDprzezpodanieopcji'forward = 0'domodu^3$

7.2 Operacje na pojedyñczej regule

Manipulowanie regu$^3amitobu^3kazmas^3emfiltrowaniapakietw.Najcz\P ciejbdzieszzapewnedodawa^3(-A)ikasowa^3(-D).$
$prostymirozwiniciamitychkoncepcji.$

Ka¿da regu$^3ajestzestawemwarunkwktrepakietmusispe^3niizawierainformacjcozrobije\P litaksista^3o(czylicel, ang.target$
$cezadresuIP127.0.0.1.Wtymprzypadkunaszymiwarunkamis\pm zatem : protoko^3emmusibyICMP, aadresem\frac{1}{4}rd^3owym127.0$

127.0.0.1 to adres pêtli zwrotnej (ang. *loopback*), który posiadasz nawet wtedy gdy nie masz ¿adnego po$^3\pm czeniasieciowego.Moeszuyprogramu'ping'bywygenerowapakietytakiejakpowyej.Poleceniewysy^3apakietyI$
$\pm danieecha(ang.echorequest)naktrewszystkiewsp^3pracuj \pm cehostyodpowiedz \pm pakietemICMPtypu0 -$
$echo.Tosprawia, epolecenietojestwygodnedlatestw.$

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$^3anietylkojednegopakietu).$

Dodajemy teraz (`-A`) do $^3acucha'INPUT'regu^3, ktramwiepakietyz127.0.0.1('-s127.0.0.1')protoko^3uICMP('-picmp')po$

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

Mo¿emy skasowaæ nasz$\pm regu^3nadwasposoby.Popierwsze, poniewawiemyejesttojedynaregu^3aw^3acuchuwej\P ciowym, m$

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

Co spowoduje skasowanie regu³*ynumer*1*w*³*acuchu**INPUT*.

Drugi sposób to dok³*adneprzepisaniepolecepoopcji*−*A*, *alezamiastopcji*−*Apodajemyopcj*−*D*.*Przydajesitowprzypadkugdy*

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

Sk³*adniapolecenia*−*Dmusidok*³*adnieodpowiadaopcjomktrepoda*³*e*¶*przypoleceniu*−*A*(*lub*−*Iczy*−*R*).*Je*¶*liistniejewieleider cazostaniaskasowana*.

7.3 Specyfikacja filtrowania

Widzieli¶my ju¿ jak u¿ywaæ opcji '-p' by wskazaæ protokó³*i*′−*s*′*bywskazaadres*¼*rd*³*owy*, *ales* ± *jeszczeinneopcjektrychmoemyuybyscharakteryzowapakiet*.*Poniejznajdzieszwyczerpuj* ± *cekompendium*.

7.3.1 Wskazanie adresów IP: ¼ród³*owegoidocelowego*

Adres IP ¼ród³*owy*(′−*s*′,′ − − *source*′*lub*′ − − *src*′)*idocelowy*(′−*d*′,′ − − *destination*′*lub*′ − − *dst*′)*mog* ± *bypodanenaczterysposoby*.*Najcz*¶*ciejrobisitoprzezpodaniepe*³*nejnazwy*, *takiejjak*′*localhost*′*czy*‘*www.linuxhq.com*′.*Drugi*

Trzeci i czwarty sposób pozwalaj±*nawskazaniegrupyadreswIP*, *takjaknaprzyk*³*ad*′199.95.207.0/24′*lub*‘199.95.207.0/255.255 *nazakresadreswIPod*199.95.207.0*do*199.95.207.255*w*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 dok³*adnietakisamjakwprzypadkuniepodaniaopcji*′−*s*′*wogle*.

7.3.2 Inwersja

Wiele flag, w³±*czaj*±*c*′−*s*′(*lub*′ − − *source*′)*i*′−*d*′(′ − − *destination*′)*monapoprzedziznakiem*′!′(*wymawianym*′*nie*′)*bywskaz cedotychpodanych*.*Naprzyk*³*ad*′−*s*!*localhost*′*bdziepasowadowszystkichpakietwniepochodz* ± *cychzlocalhost*.

7.3.3 Protokó³

Protokó³*podajesipoparametrze*′−*p*′(*lub*′ − − *protocol*′).*Protok*³*moebynumerem*(*je*¶*liznaszwarto*¶*cinumeryczneprotoko*³*w dla*′*TCP*′,′ *UDP*′*i*′*ICMP*′.*Wielko*¶*literniemaznaczenia*, *wic*′*tcp*′*dzia*³*ataksamojak*′*TCP*′.

Nazwa protoko³*umoebypoprzedzonaprzezznak*′!′*bywskazanawszystkieoprczwymienionego*, *takjaknaprzyk*³*ad*′−*p*!*TCP*′(*w*

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±wysy3ane('−o').Moeszuyprogramuifconfigbywylistowainterfejsyktr podniesione'(tzn.aktualniepracuj ± ce).

Pakiety podró¿uj±cew3acuchuINPUTniemaj±interfejsuwyj¶ciowego, wicpodanieopcji'−o'wregulewtym3acuchuspowod ceprzez3acuchOUTPUTniemaj±interfejsuwej¶ciowego, wicpodanieopcji'−i'wreguletego3acuchaspowodujeeniebdzieona

Tylko pakiety podró¿uj±ceprzez3acuchFORWARDmaj ± zarwnointerfejswej¶ciowyiwyj¶ciowy.

Jest ca3kowiciepoprawnewskazanieinterfejsuktryaktualnienieistnieje; regu3aniebdziepasowa3adoniczego, dopkiinterfej czewdzwanianychPPP(zwykleinterfejsmanazwppp0)ipodobnych.

Mo¿na równie¿ wskazaæ interfejs koñcz±cjegonazwprzez'+'cospowodujeeregu3abdziepasowa3adowszystkichinterfejswktr guznakw(bezznaczeniaczyinterfejsaktualnieistniejeczynie).Naprzyk3ad, bywskazaregu3ktrapasujedowszystkichinterfe

Interfejs mo¿e byæ poprzedzony przez '!' ze spacjami wokó3, cospowodujeepasowabd ± pakietyktrenies ± powi±zanezewskazanyminterfejsem(tzn.pakietnimniedotar3dosystemu, lubniezamierzanimgoopu¶ci), np.−i!ppp+.

7.3.5 Fragmenty

Czasami pakiet jest zbyt du¿y by zmie¶ciæ siê ca3ywjednostcetransmisji.Kiedysitakdzieje, jestondzielonynafragmentyiw

Problem z fragmentami polega na tym, ¿e pierwszy fragment posiada komplet pól nag3wka(IP + TCP, UDPiICMP)ktrymonasprawdza, alenastpnefragmentymaj ± tylkopodzbirnag3wkw(IPbezdodatkowychplspecyficznychdlaprotoko3wktreprzenosipakiet).Wzwi ± zkuztymniemoliwejestanalizowaniepewnychinformacjiznag3wkwfragmentw(takjakrobisitodlatypowychpakietwTCP, U

Je¶li prowadzisz ¶ledzenie po3 ± czelubNAT, towszystkiefragmentyzostan ± najpierwz3ooneadopierop$\frac{1}{4}$niejprzekazanedokodufiltruj±cegopakiety, wicniepowiniene¶simartwifragmentami.

W ka¿dym innym przypadku wa¿ne jest by zrozumieæ jak fragmenty traktowane s±przezregu3yfiltruj ± ce.Kadaregu3aktramasprawdziinformacjektrychnieposiadamydladanegopakietu, niebdziepasowa3a.Oznaczato, etylkopie .Wzwi±zkuztymregu3a'−pTCP − −sportwww'(podaj±caport$\frac{1}{4}$rd3owy'www')nigdyniebdziepasowa3adofragmentupakietu

Mo¿esz jednak dodaæ regu3yspecjalniedladrugiegoinastpnychfragmentw, poprzezuycieopcji'−f'(lub'− − fragment').Popr !'.

Zwykle uwa¿a siê za bezpieczne umo¿liwienie drugiemu i nastêpnym fragmentom przej¶æ, poniewa¿ filtrowanie zajmie siê pierwszym fragmentem i w zwi±zkuztymzapobiegniez3oeniupakietunamaszyniedocelowej; zdrugiejstronyznaneby3ypluskwyktrepowodowa3yzawiesz

Ma3auwagadospecwodsieci : pakietyznieksztа3cone(TCP, UDPiICMPktres ± zbytkrtkiebykod¶cianyogniowejmg3odczytaporty, czywprzypadkuICMPkodityp)s ± rwniewyrzucanegdyprowadzones±takieanalizy.Dok3adnietaksamojestzfragmentamiTCPktrerozpoczynaj± siodpozycji8.

Jako przyk3ad, poniszaregu3awyrzuciwszystkiefragmentyprzeznaczonedla192.168.1.1 :

```
# 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, cooznaczae funkcjonalno¶zarwnokernelajakinarzdziaiptablesmoebyrozszerzanabydodanoweo*

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/*ker*
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/ipt*

Rozszerzenia mog±*naleedojednegozdwchtypw* : *nowychcelw, lubnowychtestw*(*porozmawiamyonowychcelachzamoment*).*N*
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.Grupyportwwskazujesialboprzezdwienazwyport*

−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.Pakietktryniepos iadakompletnegonag*^{3}*wkaTCPjestautomatycznieodrzucanyje¶liwykonanazosta*

Parê s^3*wyja¶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).Poprzezzabronienieruchutylkotympak 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.*$'3/3'$).*ListadostpnychnazwtypwICMP*

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.adr 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¶cipasowaniareg pasowaztak±czstotliwo¶ci±jakpodanawtejopcjiwczasiejedensekundy(domy¶lnie3krotnienagodzin, 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]*a, p 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¶ciaminutzanimzalogowanyzostanienastpny cydotejregu*[3]*y, niezalenieodtegoilepakietwdoniejdotrze.Jednocze¶nie, kadedwadzie¶ciaminutktreminiebezpakietuk 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*), *zwikszymws*

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

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

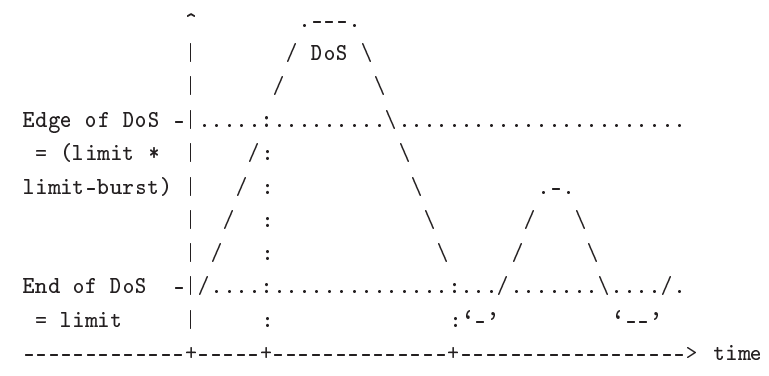
Skaner portó[3]*Furtive* :

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

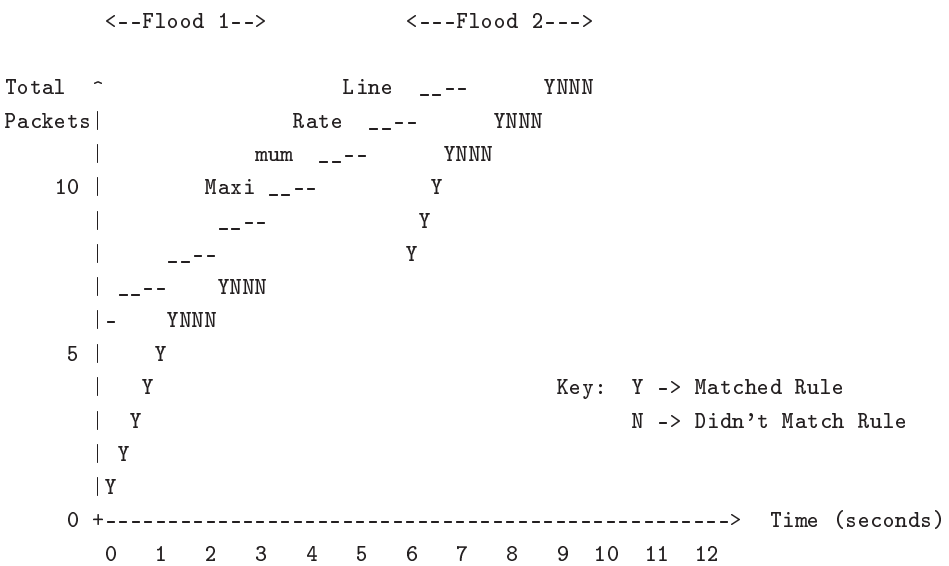
Ping of death:

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

Modu[3]*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 w[3] ± *czasiograniczanie*(*limit*).*Je¶linast* ± *pipauza*, *kolejnaseriazostaniewpuszczonaaleniepowyejmaksymalnejczstotliwo¶ciokre¶lonejprzezregu*[3](1*pakietnasekun*

Ten modu[3]*starasiustalipewnecharakterystykitwrcypakietu*, *dlapakietwgenerowanychlokalnie*.*Jegouyciejestmoliwetylkou 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*′.*Wykonujernelosowetestysp cenapakiecie*.*Modu*[3]*tennieby*[3]*sprawdzanyiniepowinienbyuywanyjakotestzwi* ± *zanyzbezpieczestwem*(*prawdopodobniesprawiaewszystkowygl*±*dajeszczegorzej*, *poniewasammoemiepluskwy*).*Nieudostp*

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

Podanie w regule opcji '`-m state`' udostêpnia dodatkow±*opcj*′ − − *state*′, *ktrajestlist* ± *oddzielonychstanwdoprzetestowania*(*opcja*′!′*wskazujenapakietyniepasuj* ± *cedowskazanychstanw*).*Stanamiktremonaspr*

NEW (NOWY)

Pakiet który tworzy nowe po^3 ± *czenie.*

ESTABLISHED (NAWI¡ZANY)

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

RELATED (POWI¡ZANY)

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

INVALID (B£ÊDNY)

Pakiet który nie mo¿e byæ zidentyfikowany z jaki¶ powodów: mog±*tobywyczerpaniesipamici*, *lubb*^{3}*dyICMPktrenienale*± *doadnegoznanegopo*^{3} ± *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±*donaszychtestw.Nazywasitocelem*(*ang.target*)*regu*^{3}*y.*

S±*dwaprostewbudowanecele* : *DROP*(*wyrzuci*)*iACCEPT*(*zaakceptowa*).*Jujewidzieli¶my.Je¶liregu*^{3}*apasujedopakietua*
lospakietuzosta^3*juokre¶lony.*

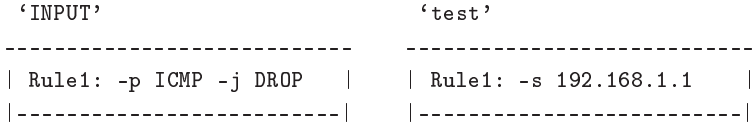
Istniej±*jeszczedwainnetypycelw* : *rozszerzeniai*^{3}*acuchyzdefiniowaneprzezuytkownika.*

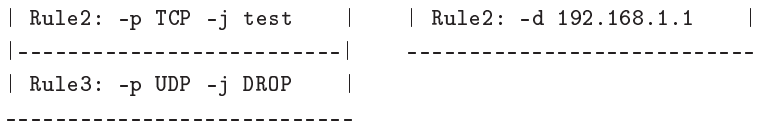
7.4.1 £añcuchy zdefiniowane przez u¿ytkownika

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

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

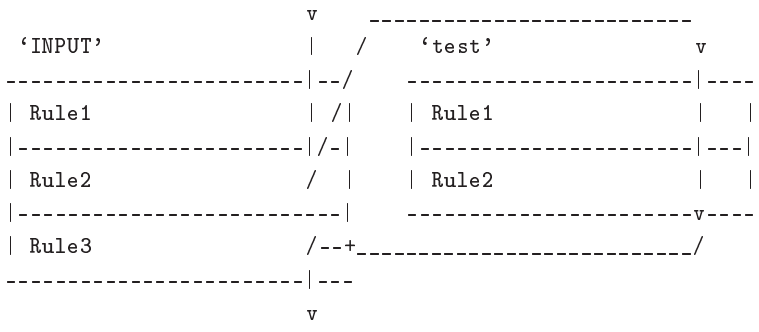
Czas na trochê rysunków ASCII. Rozwa¿my dwa (¶miesznie proste) ^{3}*acuchy* : *INPUT*(^{3}*acuchwbudowany*)*itest*(^{3}*acuchzdefiniowanyprzezuytkownika*).





Rozwa¿my pakiet TCP nadchodz±*cyz*192.168.1.1*iwys*[3]*anydo*1.2.3.4.*Wchodziondo*[3]*acuchaINPUTirozpoczynasisprawdzana ganyjestkoniec*[3]*acucha′test′.Wracamydo*[3]*acuchaINPUT, wktrymostatniosprawdzali¶myregu*[3]*drug±, terazwicsprawdzan ktrarwnieniepasuje.*

Zatem droga pakietu wygl±*dawsposbnastpuj ± cy* :



£añcuchy zdefiniowane przez u¿ytkownika mog±*jakocelwskazywainne*[3]*acuchyrwniezdefiniowaneprzezuytkownika(alenie 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′eme cyfryod*7*do*0.*Sprawd*$\frac{1}{4}$*stronpodrcznikasyslog.conf bydowiedziesicooznaczaj ± poszczeglnepoziomy.Domy¶lnymjest'warning'.*

–log-prefix

po którym nastêpuje ci±*gdo*29*znakw, ktrydodawanyjestdologowanejinformacjibyumoliwijejjednoznaczn± identyfikacj.*

Modu[3]*tenuywanyjestnajcz¶ciejztestemlimit, dzikiczemunieza¶miecaszsobielogw.*

Modu[3]*tenmatakiesamodzia*[3]*aniejak′DROP′, pozatymetonadawcypakietuodsy*[3]*anyjestpakietICMP′portunreachable′.We dICMPniezostanieodes*[3]*anyje¶li(sprawd*$\frac{1}{4}$*RFC*1122) :

- Pakiet którego dotyczy ta regu^3*ajestwiadomo¶ci±ICMPob^{3}dzie, lubnieznanymtypemwiadomo¶ciICMPPakietktreg*
- Wys^3*ali¶myjuostatniozbytduowiadomo¶ciob^{3}dachICMPdotegonadawcy(zajrzyjdo/proc/sys/net/ipv4/icmp_ratelimit).*

Do REJECT mo¿na równie¿ dodaæ opcjonalny argument '`-reject-with`' który pozwala na zadeklarowanie jaki dok^3*adniepakietICMPmazostaodes^{3}anyzamiastdomy¶lnego'portunreachable'.Sprawd$\frac{1}{4}$stronpodrcznika.*

7.4.3 Specjalne cele wbudowane

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

`RETURN` ma dok^3*adnietensamefektjakzakoczeniesprawdzania^{3}acucha* : *dlaregu^{3}yw^{3}acuchuwbudowanymsprawdzanajestwtedypolityka.Dlaregu^{3}ywzdefiniowanymprzezuytkownika^{3}acuchu, ozn*

`QUEUE` to cel który kolejkuje pakiety dla przetwarzania w przestrzeni u¿ytkownika. ¯eby mo¿na by^3*otencelzastosowa, potrzebnes ± jeszczedwask^{3}adniki* :

- program **obs**^{3}*uguj ± cykolejk*(*ang.queuehandler*), *ktryzajmiesimechanik ± przekazywaniapakietwpomidzykernelemiprzestrzeni ± uytkownika*(*ang.userspace*); *orazaplikacjadzia^{3}aj± cawprzestrzeniuytkownikaktrabdziepotrafi^{3}aobs^{3}uyprzyjcie, ewentualn±modyfikacjiopcjonalnewydaniewerdyktuwspra*

Standardowym programem obs^3*uguj±cymkolejkidlaIPv4jestwiptablesmodu^{3}ip_queue, ktrydystrybuowanyjestzkernelemi*

Poni¿ej przedstawiono krótki przyk^3*adjakuyiptableszkolejk±pakietwdoprzetwarzaniawprzestrzeniuytkownika* :

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

W powy¿szych regu^3*ach, pakietyICMPgenerowanelokalnie*(*takjaknaprzyk^{3}adprzyuyciupoleceniaping*)*przekazywanes± domodu^{3}uip_queue, ktrystarasidostarczypakietydoaplikacjidzia^{3}aj±cejwprzestrzeniuytkownika.Je¶liniematakiejaplika wyrzucane.*

By napisaæ tak±*aplikacj, naleyuyAPIlibipq.Dystrybuowanajestonarazemziptables.Kodprzyk^{3}adowyznajdujesiwnarzdzi*

Status modu^3*uip_queuemoebysprawdzonyprzezwywo^{3}anie* :

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

Maksymalna d^3*ugo¶kolejki*(*tzn.ilo¶pakietwdostarczonychdoprzestrzeniuytkownikabezodpowiedzi*)*moebykontrolowanapr*

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

Domy¶ln±*warto¶ci ± jest*1024.*Kiedyzostajeosi ± gnitylimit, nowepakietybd ± wyrzucanedopkid^{3}ugo¶kolejkiniespadnieponiejwarto¶cimaksymalnej.Dobreprotoko^{3}ytakiejakTCPinterpretuj± wyrzucanepakietyjakot^{3}okiprawdopodobniedadz±sobiespokjgdykolejkasiwype^{3}ni.Monaoczywi¶cietrochpoeksperymento maksymaln ± d^{3}ugo¶kolejkidlaokre¶lonejsytuacji, je¶lidomy¶lnawarto¶cijestzbytma^{3}a.*

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

Bardzo przydatn±*opcj±wiptablesjestmoliwo¶ciagrupowaniaregu^{3}w^{3}acuchy.Moeszjenazwajakchcesz, alezalecamraczejuyw do*31*liter.*

7.5.1 Tworzenie nowego ^{3}*acucha*

Stwórzmy nowy ^{3}*acuch.Poniewajestemkolesiemzwyobra$\frac{1}{4}$ni±, nazwijmygo'test'.Moemyuyalbo'−N'albo'− − new − chain'*

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

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

7.5.2 Kasowanie ^{3}*acucha*

Kasowanie^3*acucharwniejestproste*, *uywasidotegoopcji'−X'lub'− − delete − chain'.Adlaczego'−X'?C*, *wszystkiedobreliter*

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

Jest jednak parê ograniczeñ dotycz±*cychkasowania*^{3}*acuchw* : *musz* ± *bypuste*(*sprawd*$\frac{1}{4}$*sekcj*7.5.3(*Oprnianie*^{3}*acucha*)*poniej*)*iniemog*±*bywskazywanejakocelwinnejregule.Niemoeszrwnieskas*

Je¶li nie podasz nazwy ^{3}*acucha*, *skasowanezostan*±*wmiarmoliwo¶ciwszystkie*^{3}*acuchyzdefiniowaneprzezuytkownika.*

7.5.3 Opró¿nianie ^{3}*acucha*

Istnieje oczywi¶cie równie¿ sposób by wykasowaæ wszystkie regu^3*yz*^{3}*acucha.Uywasidotegoopcji'−F'*(*lub'− − flush'*).

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

Je¶li nie wska¿esz konkretnego ^{3}*acucha*, *oprnionezostan* ± *wszystkie.*

7.5.4 Listowanie zawarto¶ci ^{3}*acucha*

Mo¿esz wylistowaæ regu^3*yw*^{3}*acuchu*, *uywaj* ± *copcji'−L'*(*lub'− − list'*).

Pozycja '`refcnt`' przy ka¿dym ^{3}*acuchuzdefiniowanymprzezuytkownikapodajenumerregu*^{3}*ktreodwo*^{3}*uj* ± *sidotego*^{3}*acucha.Warto¶tamusibyrwnazero*(*a*^{3}*acuchmusibypusty*), *bytaki*^{3}*acuchmonaby*^{3}*oskasowa.*

Je¶li pominiêto nazwê ^{3}*acucha*, *wylistowanezostan* ± *wszystkie*^{3}*acuchy*, *nawettepuste.*

Istniej±*trzyopcjektremog*±*towarzyszyopcji'−L'.Opcja'−n'*(*numerycznie*)*jestotyleprzydatna*, *ezapobiegasprawdzaniunaz*
cymadresomIPprzeziptables, *comoespowodowaduezw*^{3}*okije¶litwjDNS*(*azak*^{3}*adamyeuywaszDNSjakwikszo¶ludzi*)*nieje*

Opcja '`-v`' pokazuje wszystkie detale regu^3, *takiejakliczniki*i*pakietwibajtw*, *porwnaniaTOS*(*TypuUs*^{3}*ugi*, *ang.TypeofServic*
pominite.

Zwróæ uwagê ¿e liczniki pakietów i bajtów drukowane s±*przyuyciusuffiksw'K'*,*' M'lub'G'*, *dlaodpowiednio*1000, 1, 000, 000*i*
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^3*ad* :

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

Pewna liczba pakietów mog^3*abyprzej¶pomidzywydaniempoleceniazopcj* $\pm'$ $-L'a'-Z'.Wzwi$ $\pm$ *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}*acu przypisan±polityk, poniewaje¶lipakietdocieradokoca*^{3}*acuchazdefiniowanegoprzezuytkownika, sprawdzaniewracadopopr*

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* $\pm$ *niekompatybilnezmodu*^{3}*emip_tables.o*!).*Moesznastpnieuywaichtakjakzastarychdobrychczasw.*

Bêd±*onewspieranejeszczeprzezjaki¶czas.Wydajemisiesensownymwzoremjest*$2*[notkaozast \pm pieniu-$ *pierwszastabilnadystrybucja], poktrymtoczasiedostpnajeststabilnawersjanowegoodpowiednika.Oznaczatoewsparciedlaty*

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} $\pm$ *czysijebardzodobrze.*

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

Mo¿esz u¿ywaæ testu stanu ('state') bez dostarczania dodatkowej pracy filtrowi pakietów, poniewa¿ NAT wymaga i tak ¶ledzenia po^3 $\pm$ *cze*(*ang.connectiontracking*).*Byrozszerzyprostyprzyk*^{3}*admaskaradyzNATHOWTOozabronieniekreowaniunowychpo*^{3}$\pm$ *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 $^3acuchwzosta^3yzmienionezma^3ychnaDU\text{Æ}Elitery, poniewa^3acuchyINPUTiOUTPU$
- Porty TCP i UDP podaje siê teraz przez opcje `-source-port` lub `-sport` (czy te¿ `-destination-port`/`-dport`) i zapisuje po wskazaniu protoko$^3u('-ptcp'lub'-pudp')poniewadopieroone^3aduj\pm rozszerzeniaodpowiednioTCPiUDPOpcjTCP'-y'zmienion$ $zapisapo'-ptcp'.$
- Cel DENY w koñcu nazywa siê DROP (WYRZUCIÆ).
- Dzia$^3azerowaniepojedyczych^3acuchwzjednoczesnymwylistowaniemichzawarto\P ci.Dzia^3azerowaniewbudowanych^3a$ $czniezkasowaniemlicznikwwywo^3aniapolitykidladanego^3acucha$
- Listowanie $^3acuchwdostarczaci'atomowego'zdjcia(ang.snapshot)licznikw.REJECTiLOGs \pm terazcelamirozszerzonymi, cooznaczaes \pm osobnymimodu^3amikernela.$
- Nazwy $^3acuchwmog\pm miedo31znakw.OpcjaMASQnazywasiwkocuMASQUERADEiuywainnejsk^3adni.REDIREC$ $HOWTObyuzyskawicejinformacjijakuytychopcji.$

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

11 Porady w projektowaniu filtra pakietów

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

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

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

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

- ```
  # 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±$cychzdziwnychkierunkw), bdzieszprawdopodobniemusia^3wy^3 \pm czytakiefiltrowanienatychinterfejsach.$

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

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

```
# 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$\pm rad\pm jest'b\pm d\frac{1}{4}minimalist\pm'$ $.ZajrzyjdoSecurityHOWTOpowicejinformacjiotestowaniuisprawdzaniutwojejmaszyny.$