Linux 2.4 NAT HOWTO

Rusty Russell, lista pocztowa netfilter@lists.samba.org Wersja oryginalna: $Revision: 487 $ $Date: 2002-01-14 10:35:13 +0100 (Mon, 14 Jan 2002) $

Orygina^3*tegodokumentuznajdujesipodadresem* : http://www.netfilter.org/documentation/HOWTO/NAT-HOWTO.html

T^3*umaczenie* : *£ukaszBromirski*, *l.bromirski@mr0vka.eu.org*

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

Spis treści

1 Wprowadzenie **2**

2 Gdzie znajduje siê oficjalna strona WWW i lista? **2**

2.1 Co to jest Translacja Adresów Sieciowych (NAT)? . . . 2

2.2 Po co mia^3*bymstosowaNAT*? . . . 3

3 Dwa typy NAT **3**

4 Szybkie przej¶cie z kerneli 2.0 i 2.2 **3**

4.1 Ja chcê tylko maskarady! Ratunku! . . . 4

4.2 A co z ipmasqadm? . . . 5

5 Kontrolowanie tego, co poddawaæ NAT **5**

5.1 Proste przyk^3*adyzuyciemiptables* . . . 6

5.2 Dok^3*adniejszeinformacjeowyborzepakietwdomodyfikowania* . . . 6

6 Okre¶lanie jak zmieniaæ pakiety **6**

6.1 ¬*rd*^{3}*owyNAT* . . . 6

6.1.1 Maskarada . . . 7

6.2 Docelowy NAT . . . 7

6.2.1 Przekierowywanie (ang. *redirection*) . . . 7

6.3 Wiêcej o mapowaniach . . . 8

6.3.1 Wybór wielu adresów z zakresu . . . 8

6.3.2 Wykonywanie pustych mapowañ NAT . . . 8

6.3.3 Standardowe zachowanie NAT . . . 8

6.3.4 Mapowanie portów $\frac{1}{4}$ród^3*owychwynikaj* $\pm$ *cezinnychpo*^{3} $\pm$ *cze* . . . 8

6.3.5 Co dzieje siê gdy NAT zawiedzie 8
6.3.6 Wiele mapowañ, nak^3*adaniesiikonflikty* 9
6.3.7 Zmiana adresu docelowego dla lokalnie generowanych po^3 ± *cze* 9

7 Protoko^3*yspecjalne* **9**

8 Problemy z NAT **9**

9 $\neg rd^3owyNAT(SNAT)irouting$ **10**

10 Docelowy NAT (DNAT) do tej samej sieci **10**

11 Podziêkowania **11**

1 Wprowadzenie

Witam, szanowny czytelniku.

W^3a¶*niezanurzaszsiwfascynuj* ± *cy*(*choczasamikoszmarny*)¶*wiatNAT* : *TranslacjiAdreswSieciowych*, *atendokumentHOWTObdziedlaCiebiewmiardok*^{3}*adnymprzewodnikiem*, *dotegoinietylko*, *te*

W linuksie 2.4 dodano infrastrukturê do manipulowania pakietami nazwan±*'netfilter'*.*Warstwazbudowananajejfundamentachzapewnia NAT*, *kompletnieprzepisanywporwnaniudopoprzed*

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

2 Gdzie znajduje siê oficjalna strona WWW i lista?

S±*trzyoficjalnestrony* :

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

Dziêki *Zespo*^{3}*owiSambaiSGI**http://netfilter.samba.org/*.*DzikiHarald'owiWelte**http://netfilter.gnumonks.org*

By odnale$\frac{1}{4}$æ oficjaln±*listpocztow* ± *netfilter*, *zajrzyjna*

Netfilter List http://www.netfilter.org/contact.html#list .

2.1 Co to jest Translacja Adresów Sieciowych (NAT)?

Zwykle, pakiety podró¿uj±*od*$\frac{1}{4}rd^3a$(*takiegojaktwjkomputer*)*doswojegoprzeznaczenia*(*takiegojakwww.gnumonks.org*)*prze*
cze : *oko*^{3}*o*19*st*±*dgdziejestem*, *wAustralii*Ł*adenztychwz*^{3}*wniezmieniatwojegopakietu* : *poprostuprzesy*^{3}*agodalej*.

Je¶li jeden z tych wêz^3*wmia*^{3}*bywykonaNAT*, *zmieni*^{3}*byadres*$\frac{1}{4}rd^3$*owylubprzeznaczeniawtrakciejakpakietprzechodzi*^{3}*byprz*
zkuztymuywanieNATjestzawszetrochryzykowne.*Zwyklewze*^{3}*ktrywykonujeNATzapamitasposbwjakizmieni*^{3}*pakietikie*

2.2 Po co mia^3*bymstosowaNAT*?

W idealnym ¶wiecie, nie by^3*obypowodu.Ale*, *g*^{3}*wnymipowodamis*± :

Modemowe po^3 ± *czeniedoInternetu*

Wiêkszo¶æ ISP (dostawców internetowych) daje ci jeden IP gdy siê do nich wdzwaniasz. Mo¿esz wysy^3*apakietyzdowolnymadresem*$\frac{1}{4}$*rd*^{3}*owym*, *aletylkoodpowiedziprzeznaczonedotegokonkretnegoIPktryzosta*^{3}*Cipr zpowrotemdoCiebie.Je¶lichceszuywawielukomputerw*(*je¶liposiadasznaprzyk*^{3}*adsiewdomu*)*izapewniimdostpdoInte*

Aktualnie jest to najczêstsze zastosowanie NAT, znane pod nazw±'*masquerading'w¶wiecielinuksa.NazywamtoSNAT przypomnieniet*^{3}*um.*).

Wiele serwerów

Czasami chcesz zmieniæ sposób w jaki pakiety rozprowadzane s±*wtwojejsieci.Zwykledziejesitakponiewamaszjedenadres*I *cychpakietw*, *moesztoosi*±*gn*±.*TentypNATnazywanyby*^{3}*wdotychczasowychwersjachLinuksaprzekazywaniemportw*(*ang.*

Najczêstszym rodzajem tego sposobu jest **rozk**^{3}*adanieobci*±*enia*(*ang.load* − *sharing*), *mapowaniewskazujewtedynalistmas sinadchodz* ± *cymiwywo*^{3}*aniami.Je¶lizamierzaszrobico¶takiegonapowanie*, *wartozajrzepodadres*

linuksowego wirtualnego serwera http://linuxvirtualserver.org/ **.**

Transparentne Proxy

Czasami chcesz udawaæ ¿e ka¿dy pakiet który przechodzi przez twój komputer z Linuksem, przeznaczony jest do jakiej¶ aplikacji uruchomionej w^3*a¶nienanim.Uywasitegodotworzeniatransparentnychproxy* : *proxytoprogramktrypo¶redniczywwymianieinformacjimidzytwoj* ± *sieci* ± *a¶wiatemzewntrznym.Transparentnychdlatego*, *etwojasieniewienaweterozmawiazproxy*, *dopkioczywi¶cieproxydzia*^{3}*a.*

Mo¿na tak skonfigurowaæ Squida, i nazywa siê to przekierowywaniem (ang. *redirection*) lub transparentnym proxy we wcze¶niejszych wersjach Linuksa.

3 Dwa typy NAT

Dzielê NAT na dwa rodzaje: ¬*rd*^{3}*owyNAT*(*SNAT*)*iDocelowyNAT*(*DNAT*).

SNAT ma miejsce wtedy, gdy zmieniasz adres $\frac{1}{4}$**ród**^{3}*owypierwszegopakietu* : *tzn.kiedyzmieniaszadresmaszynyzktrejinicjowanejestpo*^{3}±*czenie.SNATwykonywanyjestzawszeporoutingu*(*ang.post* − *form* ± *SNAT.*

DNAT ma miejsce wtedy, gdy zmieniasz adres docelowy pierwszego pakietu: tzn. kiedy zmieniasz adres maszyny do której ma dotrzeæ po^3 ± *czenia.DNATwykonywanyjestzawszeprzedroutingiem*(*ang.pre* − *routing*), *kiedypakietw*^{3}*a¶niezosta*^{3}*odebranyzkabla.Pr eniaitransparentneproxytowszystkornerodzajeDNAT.*

4 Szybkie przej¶cie z kerneli 2.0 i 2.2

Przepraszam wszystkich nadal zszokowanych po przej¶ciu z 2.0 (ipfwadm) do 2.2 (ipchains).
S±*dobreiz*^{3}*ewiadomo¶ci*

Przede wszystkim, mo¿esz u¿ywaæ dalej ipchains i ipfwadm tak jak kiedy¶. By to zrobiæ, musisz w^3 ± *czydokernela*(*insmod*)*modu*^{3}*y*′*ipchains.o*′*lub*′*ipfwadm.o*′*ktreznajduj* ± *siwnajnowszejdystrybucjipakietunetfilter.Modu*^{3}*ymog* ± *byza*^{3}*adowanetylkoroz*^{3} ± *cznie*(*zosta*^{3}*e¶ostrzeony*)*iniepowinnyby*^{3} ± *czonezinnymimodu*^{3}*aminetfilter.*

Kiedy ju¿ zainstalujesz jeden z tych modu^3*w, moeszuywaipchainsiipfwadmtakjakdotejpory, znastpuj*± *cymirnicami* :

- **Ustawienie czasu wyga¶niêcia dla po**^{3}±*czemaskaradowanychopcjamiipchains* − *M* − *Slubipfwadm* − *M* − *snic duod*^{3}*usze, niepowinnomietoznaczenia.Polainit_seq, deltaiprevious_deltawlistinguszczeg*^{3}*owymmaskaradys*± *zawszeustawionenazero.*

- **Zerowanie i listowanie liczników w tym samym momencie '`-Z -L`' nie dzia**^{3}*a* : *licznikiniezostan* ± *wyzerowane.Warstwazapewniaj* ± *cakompatybilno¶wstecznieskalujesizbytdobrzedladuychilo¶cipo*^{3} ± *cze* : *nieuywajjejnafirmowejbramie*!

  Hakerzey mog±*rwniezauway, e* :

  - **Mo¿esz siê teraz bindowaæ do portów 61000-65095 nawet je¶li dzia**^{3}*amaskarada.Jejkodzak*^{3}*ada*^{3}*dotejporyewtymzakresieportwmg*^{3}*sirz* ± *dzi, wicprogramyniemog*^{3}*ygouywa.*(*Nieudokumentowana*)*opcja*′*getsockname*′, *ktrejprogramypracuj*± *cejakotransparentneproxymog*^{3}*yuybyuzyskaprawdziweadresyprzeznaczeniapo*^{3} ± *czejuniedzia*^{3}*a.*

- **(Nieudokumentowana) opcja '`bind-to-foreign-address`' równie¿ nie zosta**^{3}*azaimplementowana; by*^{3}*auywanatostworzeniakompletnejiluzjitransparentnegoproxy.*

4.1 Ja chcê tylko maskarady! Ratunku!

Wiêkszo¶æ ludzi chce. Je¶li masz dynamicznie przydzielany IP podczas wdzwaniania siê po PPP (je¶li nie wiesz o co chodzi to zapewne tak w^3*a¶niejest*), *moeszpoprostupowiedzieswojejmaszynieewszystkiepakietywychodz* ± *ceztwojejsieciwewntrznejpowinnybyzmienianetak, bywygl* ± *da*^{3}*yjakpakietywychodz* ± *cezkomputerawdzwaniaj* ± *cegosi.*

```
# Za³aduj modu³ NAT (usuwa inne).
modprobe iptable_nat

# W tabeli NAT (-t nat), dodaj regu³ (-A) po routingu
# (POSTROUTING) dla wszystkich pakietów wychodz±cych przez ppp0 (-o ppp0)
# która mówi by prowadziæ maskaradowanie po³±czenia (-j MASQUERADE).
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE

# W³±cz przekazywanie IP
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Zauwa¿ ¿e nie prowadzimy tutaj ¿adnego filtrowania pakietów: je¶li chcesz je zastosowaæ, przeczytaj Filtrowanie Pakietów HOWTO a w szczególno¶ci sekcjê: '£±*czenieNATifiltrowaniapakietw*′.

4.2 A co z ipmasqadm?

Istnieje du¿o mniejsza liczba u¿ytkowników, wiêc specjalnie nie przejmowa^3*emsiwsteczn* $\pm$ *kompatybilno¶ci*$\pm$.*Moeszpoprostuwy'iptables* $-$ *tnat'bywykonywaprzekazywanieportw.Naprzyk*^{3}*ad, dlaLinuksa*2.2*mg*^{3}*by¶*

```
# Linux 2.2
# Przeka¿ pakiety TCP kierowane do portu 8080 na 1.2.3.4 do 192.168.1.1 na port 80
ipmasqadm portfw -a -P tcp -L 1.2.3.4 8080 -R 192.168.1.1 80
```

A teraz zrobisz:

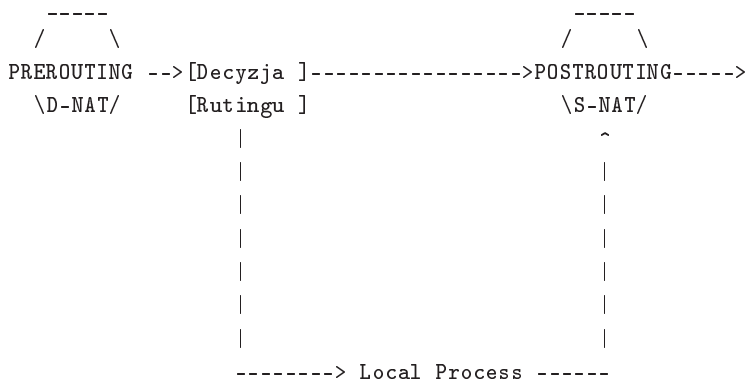
```
# Linux 2.4
# Dodaj regu$^3$ przed routingiem (-A PREROUTING) do tabeli NAT (-t nat) mwi±c±, e
# pakiety TCP (-p tcp) kierowane do 1.2.3.4 (-d 1.2.3.4) na port 8080 (--dport 8080)
# maj± by zmapowane (-j DNAT) na 192.168.1.1, port 80 (-- to 192.168.1.1 : 80).
iptables -A PREROUTING -t nat -p tcp -d 1.2.3.4 --dport 8080 \
        -j DNAT --to 192.168.1.1:80
```

5 Kontrolowanie tego, co poddawaæ NAT

Musisz stworzyæ takie regu^3*yNAT, bykernelwiedzia*^{3}*ktrepo*^{3}$\pm$*czeniapoddawamodyfikacjomijaktorobi.Bytegodokona,*

Tabela NAT zawiera dwie listy zwane '^{3}*acuchami'*(*ang.chains*) : *kadaregu*^{3}*awtakiejli¶ciejestsprawdzanadopkiktra¶niepasuje.Tedwa*^{3}*acuchynazywaj* $\pm$ *si* : *PREROUTING*(*dlaDNAT, poniewapakietynajpierwdonasdocieraj*$\pm$), *POSTROUTING*(*dlaSNAT, poktrympakietyopu naszsystem*)*iOUTPUT*(*dlaDNAT, dlapakietwgenerowanychlokalnie*).

Poni¿szy rysunek ilustrowa^3*bytodosydobrzegdybymmia*^{3}*chotrochtalentuartystycznego* :



W ka¿dym z wêz^3*wpowyej, gdydocieradoniegopakiet, sprawdzanejestzjakimpo*^{3} $\pm$ *czeniemjestskojarzony.Je¶lijesttonowepo*^{3}$\pm$*czenie, sprawdzamyodpowiedni*^{3}*acuchwtabeliNATbysprawdzicomamyznim czenia.*

5.1 Proste przyk^3*adyzuyciemiptables*

`iptables` **pobiera pewn**±*liczbstandardowychopcjitakjakpodanotoniej.Wszystkieopcjezpodwjnymznakiemminusmog*± *byskrcone,takd*^{3}*ugojakiptablesmoejerozrniodinnychmoliwychznacze.Je¶litwjkernelmawkompilowan* ± *obs*^{3}*ugiptablesjakomodu*^{3}*,musiszgonajpierwza*^{3}*adowa :' insmodip_tables'.*

Najwa¿niejsz±*opcj* ± *jestwybieraj* ± *catabel,'−t'.Dlawszystkichoperacjiktredotycz* ± *NAT,uywabdzieszopcji'−tnat'.Drug*±*wan*±*opcj*±*jest'−A',ktras*^{3}*uydododawanianowejregu*^{3}*ynakoniec*^{3}*acucha(np.'−AP tku(np.'−IPREROUTING').*

Mo¿esz podawaæ adresy $\frac{1}{4}$**ród**^{3}*owe('−s'lub'−−source')idocelowe('−d'lub'−−destination')pakietwktrychmadotyczyN*

Mo¿esz równie¿ wskazaæ interfejs wej¶ciowy ('-i' lub '`-in-interface`') lub wyj¶ciowy ('-o' lub '`-out-interface`'), ale który konkretnie zale¿y równie¿ od tego który ^{3}*acuchwskaesz : w*^{3}*acuchuPREROUTINGmoeszwskazatylkointerfejswej¶ciowy,aw*^{3}*acuchuPOSTROUTINGmoeszwskazatylkointerf b*^{3} ± *d.*

5.2 Dok^3*adniejszeinformacjeowyborzepakietwdomodyfikowania*

Powiedzia^3*emwyej,emoeszwskazaadresy*$\frac{1}{4}$*rd*^{3}*oweidocelowe.Je¶liominieszadres*$\frac{1}{4}$*rd*^{3}*owy,pasowabdziekadyadres*$\frac{1}{4}$*rd*^{3}*ow*

Mo¿esz równie¿ wskazaæ konkretny protokó^3*('−p'lub'−−protocol'),takijakTCPczyUDP;pasowabd*± *pakietytylkoztegoprotoko*^{3}*u.G*^{3}*wnympowodemdlaktregochcia*^{3}*by¶wskazakonkretnyprotok*^{3}*jestto,ezkadymznichskojarzo dodatkoweopcje : wszczeglno¶ci'−−source−port'i'−−destination−port'(ktremonaskrcido'−−sport'i'−−dport').*

Opcje te pozwalaj±*ciokre¶liojakiepakietychodzizdok*^{3}*adno¶ci*±*doportu*$\frac{1}{4}$*rd*^{3}*owegoidocelowego.Jesttouytecznewprzekaz*

Opcjom tym musi towarzyszyæ opcja '-p' (która ma ten skutek uboczny, ¿e do^3*adowywujewsp*^{3}*dzielonerozszerzeniebibliotecznedlakonkretnegoprotoko*^{3}*u).Dowskazanianumeruportumoeszuywanu*

Wszystkie sposoby na które mo¿esz wskazaæ okre¶lony typ pakietów wyszczególnione zosta^3*ywpodrczniku(maniptables).*

6 Okre¶lanie jak zmieniaæ pakiety

Wiesz ju¿ jak wybraæ pakiety do modyfikacji. By skompletowaæ nasz±*regu*^{3}*,musimypoinformowajeszczekernelcozrobizpasuj* ± *cymipakietami.*

6.1 ¬*rd*^{3}*owyNAT*

Chcesz prowadziæ ¬*rd*^{3}*owyNAT,czylizmieniaadresy*$\frac{1}{4}$*rd*^{3}*owepo*^{3}±*czenaco¶innego.Dziejesitow*^{3}*acuchuPOSTROUTIN wys*^{3}*ane;jesttobardzowanyszczeg*^{3}*,poniewaoznaczaecokolwiekinnegonatejmaszynieogl* ± *daj* ± *ctenpakiet(routing,filtrowaniepakietw)bdziewidzia*^{3}*ogowstaniejeszczeniezmienionym.Oznaczato,emonarwnieuywaopc*

¬*rd*^{3}*owyNATwykonujesiprzezwpisanie'−jSNAT',idodanieopcji'−−to−source',ktraokre¶laadreslubgrupdocelowychad*

```
## Zmieñ adres ¼ród³owy na 1.2.3.4.
# iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4

## Zmieñ adres ¼ród³owy na 1.2.3.4, 1.2.3.5 lub 1.2.3.6
```

```
# iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4-1.2.3.6

## Zmieñ adresy ¼ród³owy 1.2.3.4, porty z zakresu 1 - 1023
# iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT --to 1.2.3.4:1-1023
```

6.1.1 Maskarada

Jest to specjalizowana odmiana $\neg rd^3owegoNATu : powinnabyuywanatylkoje¶limaszdynamicznieprzydzielanyadresI$

Nie musisz podawaæ adresów $\frac{1}{4}$**ród**$^3owychbywykonamaskarad$: $uyjeonaadresu\frac{1}{4}rd^3owegointerfejsuprzezktrypakietybd \pm opuszcza^3ymaszyn.Alecowaniejsze, je¶lipo^3 \pm czeniewdzwanianezostaniezamknite, po^3 \pm czenia(ktreitakjuzosta^3yzerwane)zostan \pm zapomniane, cooznaczamniejzgrzytwwmomenciegdyponowniesiwdzwoniszznowymIP.$

```
## Maskaraduj wszystko wychodz±ce przez ppp0.
# iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

6.2 Docelowy NAT

Wykonywany jest w $^3acuchuPREROUTING, zarazpotymjakpakietzostajeodebrany, cooznaczaecokolwiekinnegonatejr$

Docelowy NAT wskazuje siê przez podanie opcji '`-j DNAT`' i '`-to-destination`' która okre¶la pojedyñczy adres lub zakres adresów IP; opcjonalnie mo¿na wskazaæ port lub zakres portów (ale tylko dla protoko$^3wTCPiUDP$).

```
## Zmieñ adresy docelowe na 5.6.7.8
# iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 5.6.7.8

## Zmieñ adresy docelowe 5.6.7.8, 5.6.7.9 lub 5.6.7.10
# iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 5.6.7.8-5.6.7.10

## Zmieñ adresy docelowe ruchu WWW na 5.6.7.8, port 8080
# iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth0 \
        -j DNAT --to 5.6.7.8:8080
```

6.2.1 Przekierowywanie (ang. *redirection*)

Jest to specjalizowany przypadek DNAT: dodano go dla wygodny, poniewa¿ jest to dok$^3adnietosamocowykonanieDNATnaadresinterfejsuwej¶ciowego.$

```
## Wy¶lij przychodz±cy ruch WWW na port 80 do naszego transparentnego proxy (squida)
# iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 \
        -j REDIRECT --to-port 3128
```

Zwróæ uwagê na to, ¿e squid musi zostaæ skonfigurowany tak by wiedzia$^3ejesttransparentnymproxy$!

6.3 Wiêcej o mapowaniach

Jest trochê ró¿nych subtelno¶ci w NAT z którymi wiêkszo¶æ u¿ytkowników nigdy nie bêdzie mia^3*adoczynienia.S* ± *onetuudokumentowanedlaciekawskich.*

6.3.1 Wybór wielu adresów z zakresu

W momencie gdy poda siê zakres adresów IP, s±*onewybieranenapodstawieostatniouywanegoIPdlapo*^{3}± *czeoktrychkodwie.Dajetoco¶nakszta*^{3}*tprymitywnegorozk*^{3}*adaniaobci* ± *enia.*

6.3.2 Wykonywanie pustych mapowañ NAT

Mo¿esz u¿yæ celu '`-j ACCEPT`' by pozwoliæ na przej¶cie po^3 ± *czeniabezwykonaniaNAT.*

6.3.3 Standardowe zachowanie NAT

Domy¶lnym zachowaniem jest zmiana po^3±*czeniatylkonatyleilepotrzeba, wgranicachregu*^{3}*ypodanejprzezuytkownika dano, chybaebdzietokonieczne.*

6.3.4 Mapowanie portów $\frac{1}{4}$**ród**^{3}*owychwynikaj* ± *cezinnychpo*^{3} ± *cze*

Nawet gdy dla danego po^3±*czenianiewykonujesiNAT, moesiokazaezostaniewykonanatranslacjaadresu*$\frac{1}{4}$*rd*^{3}*owego, wz zkuztymejestjujakie¶po*^{3} ± *czenieuywaj* ± *cetegoportu.Rozwamynastpuj* ± *cyprzyk*^{3}*admaskarady, ktryjestdosypowszechny* :

1. **Nawi**±*zywanejestpo*^{3}±*czenieprzezmaszyn*192.1.1.1*zportu*1024*domaszynywww.netscape.comnaport*80.*Po*^{3}± *czeniejestmaskaradowaneprzezmaszynprowadz* ± *c* ± *NATiuywajejadresuIP*(1.2.3.4).

2. **Maszyna ta stara siê wykonaæ po**^{3}±*czeniedowww.netscape.comnaport*80*z*1.2.3.4(*swojegoadresuzewntrznego*)*zportu*10 *czeniana*1025*takbytedwaportyniekolidowa*^{3}*yzesob* ± .

   Kiedy odbywa siê takie mapowanie, porty dzielone s±*natrzyklasy* :

   - **porty poni¿ej 512**
   - **porty pomiêdzy 512 a 1023**
   - **porty 1024 i wy¿sze**

   Port nie zostanie nigdy zmapowany w tym przypadku do innej klasy.

6.3.5 Co dzieje siê gdy NAT zawiedzie

Je¶li nie istnieje sposób by unikalnie zmapowaæ po^3 ± *czeniena* ± *danieuytkownika, zostanieonoodrzucone.Dotyczytorwniepakietwniesklasyfikowanychjakocz¶istniej* ± *cegopo*^{3} ± *czenia, poniewas* ± *zniekszta*^{3}*cone, maszynawyczerpa*^{3}*apamiitd.*

6.3.6 Wiele mapowañ, nak^3*adaniesiikonflikty*

Mo¿esz stworzyæ regu^3*yNATktremapuj* ± *pakietydotegosamegozakresu*; *kodNATjestnatylem* ± *drybyunikn*±*konfliktw.Oznaczatoedwieregu*^{3}*ymapuj*±*ceadresy*$\frac{1}{4}$*rd*^{3}*owe*192.168.1.1*i*192.168.1.2*na*1.2.3.4*bdz*± *dzia*^{3}*apoprawnie.*

Co wiêcej, mo¿esz mapowaæ nawet na realne, u¿ywane adresy IP dopóki przechodz±*oneprzezmaszynmapuj* ± *c* ± *.Je¶limaszzatemprzydzielon* ± *sie*(1.2.3.0/24), *alemaszjedn* ± *siewewntrzn* ± *uywaj* ± *c* ± *tychadreswijedn* ± *uywaj* ± *c* ± *zakresuadreswprywatnych*192.168.1.0/24, *moeszpoprostuwykonaNATnaadresy*$\frac{1}{4}$*rd*^{3}*owe*192.168.1.0/24*dosieci*1.2.3.0, *bezst*

```
# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth1 \
        -j SNAT --to 1.2.3.0/24
```

Ta sama logika dotyczy adresów u¿ywanych przez sam±*maszynprowadz* ± *c* ± *NAT* : *takw*^{3}*a¶niedzia*^{3}*amaskarada*(*wsp*^{3}*dziel*±*cadresinterfejsupomidzypakietymaskaradowanea*′*prawdziwe*′*pakietywychodz*± *ceztejmaszyny*).

Co wiêcej, mo¿esz mapowaæ te same pakiety na wiele maszyn docelowych, i bêd±*onewsp*^{3}*dzielone.Naprzyk*^{3}*ad*, *je¶liniechceszmapowaniczegona*1.2.3.5*moesznapisa* :

```
# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth1 \
        -j SNAT --to 1.2.3.0-1.2.3.4 --to 1.2.3.6-1.2.3.254
```

6.3.7 Zmiana adresu docelowego dla lokalnie generowanych po^3 ± *cze*

Kod wykonuj±*cyNATpozwalanawstawianieregu*^{3}*wykorzystuj*±*cychcelDNATdo*^{3}*acuchaOUTPUT*, *aleniejesttowpe*^{3}*nic cych*, *testowaniaitrochkodududopiania*, *wicje¶likto¶niezlecitegoRusty*′*emuniespodziewa*^{3}*bymsitegoszybko*).

Aktualne ograniczenie polega na tym, ¿e mo¿esz zmieniaæ tylko adres docelowy na maszynê lokaln±(*tzn.*′ − *jDNAT* − −*to*127.0.0.1′), *anienadoweln* ± *inn*±, *poniewaodpowiedziniebd* ± *prawid*^{3}*owot*^{3}*umaczone.*

7 Protoko^3*yspecjalne*

Niektóre protoko^3*ynielubi* ± *bypoddawaneNAT.Dlakadegoztychprotoko*^{3}*wmusz* ± *zostanapisanedwarozszerzenia* : *jednodla¶ledzeniapo*^{3}±*czesamegoprotoko*^{3}*u*, *drugiedlawykonanianaimNAT.*

W dystrybucji netfilter znajduj±*siaktualniemodu*^{3}*ydlaftp* : *ip_conntrack_ftp.oiip_nat_ftp.o.Moeszuyinsmodbydo*^{3}± *czyjedokernela*(*lubskompilowanasta*^{3}*e*)*iodtegomomentupo*^{3}±*czeniaftpprzezNATpowinnydzia*^{3}*apoprawnie.Je¶litegoniez wyst* ± *piproblemyje¶liwykonujeszco¶wicejnitylkoprosySNAT.*

8 Problemy z NAT

Je¶li wykonujesz NAT na konkretnym po^3 ± *czeniu*, *wszystkiepakietypodruj* ± *cewobukierunkach*(*doizsieci*)*musz* ± *przechodziprzezmaszynwykonuj* ± *c* ± *NAT*, *winnymprzypadkuniebdzietodzia*^{3}*a*^{3}*odobrze.Wszczeglno¶ci*, *kod¶ledzeniapo*^{3} ±

$czesk^3adajafragmenty, cooznaczaenietylkoniebdzieondzia^3a^3poprawnie, alerwnieito, etwojepakietymog\pm$
$woglenigdzieniedotrze, poniewajakofragmentyzostan \pm zatrzymane.$

9 $\neg rd^3 owyNAT(SNAT)irouting$

Je¶li wykonujesz SNAT, musisz upewniæ siê ¿e ka¿da maszyna do której docieraj$\pm pakietypoddane\neg rd^3 owemuNATodpowienaniekieruj \pm$
$cpakietyw^3a¶niedomaszynywykonuj \pm cejSNAT.Naprzyk^3ad, je¶limapujeszpakietywychodz \pm$
$cenaadres\frac{1}{4}rd^3ow$1.2.3.4, $zewntrznyroutermusiwiedzieepakietyzodpowiedziami(ktreprzeznaczones \pm$
dla1.2.3.4)$musz\pm trafizpowrotemdotegokomputeranaktrymodbywasimapowanie.Monatowykonananastpuj\pm$
$cesposoby$:

1. **Je¶li robisz SNAT na adres w**$^3asnymaszynyktragowykonuje(aroutingdlaniejjudzia^3a), niemusiszrobinic.Je¶lir$
   $cyNATbdziemusia^3odpowiadanazapytaniaARPdotegoadresu, oprczzapytadojegow^3asnegoadresu$:
   $najprostszymsposobembytoosi \pm gn \pm jeststworzenieliasuIP,$ np. :
2. **3.** `# ip address add 1.2.3.99 dev eth0`

Je¶li robisz SNAT na kompletnie inny adres, bêdziesz siê musia$^3upewniemaszynydoktrychbd \pm$
$dociera^3ypakietySNATbd \pm routowaodpowiedzizpowrotemdomaszynywykonuj \pm$
$cejNAT.Taksidziejeje¶likomputerwykonuj \pm cyNATjestdomy¶ln \pm bramk \pm$
$(gateway), winnymprzypadkubdzietrzebarozg^3ositak\pm tras(je¶liwykorzystujeszjaki¶protok^3routowania)lubrczniedodatr$

10 Docelowy NAT (DNAT) do tej samej sieci

Je¶li wykonujesz przekazywanie portów (ang. *portforwarding*) do tej samej sieci, musisz upewniæ siê ¿e zarówno przysz$^3epakietyjakiodpowiedzinanieprzejd \pm przezmaszynprowadz \pm$
$c \pm NAT(bymog^3ybyzmodyfikowane).Kododpowiedzialnyza NATblokujeobecnie(od$2.4.0 $-$
$test$6)$wychodz \pm cepakietyprzekierowuj \pm ceICMP(ang.ICMPredirect), ktreprodukowanes \pm$
$wmomenciegdypakietypoprzej¶ciuprzezNATwychodz\pm tymsamyminterfejsemdoktregodotar^3y, alemaszynadoktrejs\pm$
$skierowanenadalstarasiodpowiedziebezpo¶redniodoklienta(ktrynierozpoznaodpowiedzi).$

Klasycznym przyk$^3ademjestprbadostpuprzezpersonelwewntrznydo'publicznego'serweraWWW, ktrytaknaprawdprzes^3oni$

```
# iptables -t nat -A PREROUTING -d 1.2.3.4 \
        -p tcp --dport 80 -j DNAT --to 192.168.1.1
```

Jednym ze sposobów jest utrzymywanie wewnêtrznego serwera DNS który zna prawdziwe (wewnêtrzne) adresy IP publicznego serwera WWW i przekazuje wszystkie inne wywo$^3aniadozewntrznegoserweraDNS.Oznaczatoelogowaniedostpunatwoimserwerze WWW wskaeadresyIPzsieciwewnt$

Innym sposobem jest zapewnienie, by maszyna prowadz$\pm caNATmapowa^3arwnie\frac{1}{4}rd^3owyadresIPnajejw^3asny, dlapo^3\pm$
$czetegotypu, og^3upiaj\pm cserwerisprawiaj\pm cbyodpowiada^3przezni\pm.Wtymprzyk^3adzie, wykonujemyconastpuje(zak^3adaj\pm$
$cewewntrznyadresIPkomputeraprowadz \pm cegoNATto$192.168.1.250) :

```
# iptables -t nat -A POSTROUTING -d 192.168.1.1 -s 192.168.1.0/24 \
        -p tcp --dport 80 -j SNAT --to 192.168.1.250
```

Poniewa¿ regu^3$aPREROUTINGjestsprawdzanapierwsza, pakietybd\pm odrazuskierowanedowewntrznegoserweraWWW$: $moemystwierdziktrewywo^3aniapochodz \pm zsieciwewntrznejsprawdzaj \pm c\frac{1}{4}rd^3oweadresyIP.$

11 Podziêkowania

Dziêkuje przede wszystkim WatchGuard, oraz Davidowi Bonn, który wierzy^3$natylewidenetfilterbywsieramniekiedynadni \pm pracowa^3em.$

Oraz dla wszystkich, którzy podnie¶li moje zorientowanie w temacie, gdy uczy^3$emsiobrzydliwychstronNAT, szczeglniedlatychktrzyczytalimjdziennik.$

Rusty.