Linux 2.4 NAT HOWTO

Rusty Russell, mailing list `netfilter@lists.samba.org` $Revision: 487 $ $Date: 2002-01-14 10:35:13 +0100 (Mon, 14 Jan 2002) $

Do èeźtiny pøelo¿il Ivo Raisr (iq_soft@home.zcu.cz)

Contents

1 Úvod

Vítej, vá¿ený ètenáøi.

Chystáź se ponoøit do fascinujícího (a nìkdy straźlivého) svìta NAT: Network Address Translation a tento HOWTO je nìco jako tvùj návod k jádru Linuxu 2.4 a mo¿ná i dále.

V Linuxu 2.4 byla pøedstavena nová infrastruktura pro øízení paketù, nazývaná 'netfilter'. NAT zprostøedkovává vrstvu nad touto infrastrukturou, kompletnì pøepracovanou od minulých verzí jádra.

2 Kde mù¿eź najít oficiální WWW stránky a konferenci?

Existují tøi oficiální místa:

- Díky *Filewatcher* `http://netfilter.filewatcher.org/` .
- Díky *The Samba Team and SGI* `http://netfilter.samba.org/` .
- Díky *Harald Welte* `http://netfilter.gnumonks.org/` .

Oficiální poźtovní konference:

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

2.1 Co to je Network Address Translation?

Normálnì putují pakety sítí ze zdroje (napøíklad z tvého poèítaèe) ke svému cíli (napøíklad www.gnumonks.org) mnoha rùznými uzly: pøibli¿nì devatenácti z mého místa v Austrálii. őádný z tìchto mezilehlých uzlù nic nemìní, jen pakety posílá dále.

Jestli¿e jeden z tìchto uzlù provádí NAT (pøeklad sí¿ových adres), pak mù¿e být zmìnìn zdroj nebo cíl paketu, který tímto uzlem prochází. Urèitì si domyslí¹, ¿e toto není zpùsob, jakým by mìl systém pracovat; NAT je tudí¾ nìco mezi. Obvykle si uzel provádìjící NAT pamatuje, jakým zpùsobem zmìnil paket, a zpìtnì modifikuje ty pakety, které prochází nazpátek, tak¿e v¹e funguje tak, jak má.

2.2 Proè mám chtít NAT?

V dokonalém svìtì nemusí¹. V mezidobí jsou hlavními dùvody:

Modemová pøipojení k Internetu

Vìt¹ina Internetových poskytovatelù ti poskytne pro pøipojení jednu IP adresu. Mù¿e¹ odesílat pakety s libovolnou zdrojovou adresou, ale budou se ti vracet jen odpovìdi na pakety s touto pøidìlenou IP adresou. Jestli¿e chce¹ pøipojit více rùzných poèítaèù (domácí sí») k Internetu pomocí tohoto jednoho uzlu, potøebuje¹ NAT.

Toto je dnes nejbì¿nìj¹í pou¿ití NAT, v Linuxovém svìtì bì¿nì nazývané 'masquerading'. Nazývám jej SNAT, proto¿e mìní¹ **zdrojovou** ('source') adresu prvního paketu.

Více serverù

Nìkdy chce¹ zmìnit, kam budou smìøovat pakety pøicházející do tvé sítì. Èasto je to proto¿e (viz vý¹e) má¹ jedinou IP adresu, ale chce¹, aby se lidi zvenèí dostali k tvým poèítaèùm schovaným za tím jediným se 'skuteènou' IP adresou. To lze provést, pokud bude¹ pøepisovat cíl pøíchozích paketù. Tento druh NAT byl nazýván port-forwarding v pøedchozích verzích Linuxu.

Bì¿nou variantou je rozlo¿ení zatí¿ení (load-sharing), pøi kterém je mapování rozlo¿eno na mno¿inu poèítaèù. Mo¿ná pro tebe bude stát za to se podívat na

Linux Virtual Server http://linuxvirtualserver.org/ , pokud zamý¹lí¹ provádìt load-sharing ve vìt¹ím mìøítku.

Transparentní proxy

Nìkdy mù¿e¹ chtít, aby ka¿dý paket, který prochází tvým Linuxovým poèítaèem, byl urèen pro nìjaký program na tomto poèítaèi. Takto se dìlá transparentní proxy: proxy je program uprostøed, který zprostøedkovává komunikaci mezi tvou sítí a okolním svìtem. Transparentní proto, ¿e tvá sí» vùbec neví, ¿e komunikuje s proxy (ov¹em za pøedpokladu, ¿e proxy funguje).

Squid mù¿e být takto nakonfigurován, v pøedchozích verzích Linuxu to bylo nazýváno pøesmìrování (redirection) nebo transparentní proxy.

3 Dva druhy NAT

Rozdìluji NAT na dva rùzné druhy: **Zdrojová NAT** (SNAT) a **Cílová NAT** (DNAT).

Kdy¾ modifikuje¹ zdrojovou adresu prvního paketu, pak je to Zdrojová NAT - napøíklad mìní¹ zdroj vysílání. Zdrojová NAT je v¾dy provádìna a¾ po dokonèení smìrování, tìsnì pøedtím ne¾ je paket vyslán po drátech. Masquerading je speciální forma SNAT.

Kdy¾ modifikuje¹ cílovou adresu prvního paketu, pak je to Cílová NAT - napøíklad mìní¹ cíl. Cílová NAT je v¾dy provádìna pøed zapoèetím smìrování, tìsnì po pøijetí paketu z drátù. Port-forwarding, load-sharing a transparentní proxy jsou speciální formou DNAT.

4 Rychlý pøestup z 2.0 a 2.2 jádra

Sorry vźem, kteøí jsou stále jeźtì źokováni pøechodem z 2.0 (ipfwadm) na 2.2 (ipchains). Jsou zde dobré a źpatné zprávy.

Za prvé, mù¿eź pou¿ívat ipchains a ipfwadm stejnì jako pøedtím. Abys je mohl pou¿ívat, musíź nejprve zavést moduly jádra 'ipchains.o' nebo 'ipfwadm.o', které najdeź v poslední distribuci netfilter. Tyto moduly se vzájemnì vyluèují (byl jsi varován) a nemìly by být kombinovány s ¿ádnými jinými moduly netfilteru.

Jakmile je jeden z tìchto modulù zaveden, mù¿eź pou¿ívat ipchains a ipfwadm zcela bì¿ným zpùsobem, pouze s tìmito odliźnostmi:

- Nastavení masquerading timeoutù pomocí ipchains -M -S nebo ipfwadm -M -s nic nedìlá. Nevadí to, jeliko¿ timeouty pro novou NAT infrastrukturu jsou delźí.
- Polo¿ky init_seq, delta a previous_delta v ukecaném masquerading výpisu jsou v¿dy nulové.
- Nulování a výpis èítaèù najednou pomocí '-Z -L' u¿ dále nefunguje: èítaèe nebudou vynulovány.
- Zpìtnì kompatibilní vrstva není dobøe źkálovatelná pro velký poèet spojení - nepou¿ívej ji na exponovaném místì!

Pro hackery:

- Mù¿eź se nyní navázat na porty 61000-65095 i kdy¿ provádíź masquerading. Kód pro masquerading byl zvyklý pova¿ovat vźechny porty v tomto rozmezí za volné, tak¿e je programy nemohly pou¿ívat.
- Ji¿ nefunguje (nedokumentovaný) 'getsockname' hack, pomocí kterého programy pou¿ívající transparentní proxy mohly zjistit skuteèný cíl spojení.
- Také (nedokumentovaný) hack 'bind-to-foreign-address' ji¿ není implementován. Ten byl pou¿íván k dovrźení iluze transparentní proxy.

4.1 Chci jen masquerading! Pomoc!

To chce vìtźina. Jestli¿e máź dynamicky pøidìlenou IP adresu PPP pøipojení (pokud nevíź, tak jsi to ty), chceź prostì sdìlit svému poèítaèi, ¿e vźechny pakety pocházející z tvé vnitøní sítì mají vypadat jako by pocházely z poèítaèe s PPP pøipojením.

```
# Zavést NAT modul (to zavede vźechny ostatní).
modprobe iptable_nat

# V tabulce NAT (-t nat) pøipoj pravidlo (-A), ¿e po dokonèení smìrování
# (POSTROUTING) má být u vźech paketù odcházející z ppp0 (-o ppp0) provádìno
# MASQUERADE spojení (-j MASQUERADE).
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE

# Zapnutí IP forwardování
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Povźimni si, ¿e neprovádíź ¿ádné filtrování paketù: k tomu si pøeèti Packet Filtering HOWTO: 'Mixing NAT and Packet Filtering'.

4.2 A co ipmasqadm?

Neobtì¿oval jsem se tolik se zachováním zpìtné kompatibility, proto¿e je to velmi choulostivá vìc. Pro port forwarding mù¿eź jednoduźe pou¿ít 'iptables -t nat'. Tedy napøíklad v Linuxu 2.2 mù¿eź mít:

```
# Linux 2.2
# Smìruj TCP pakety z 1.2.3.4, port 8080 na 192.168.1.1, port 80
ipmasqadm portfw -a -P tcp -L 1.2.3.4 8080 -R 192.168.1.1 80
```

Nyní bys mìl mít:

```
# Linux 2.4
# Pøipoj pravidlo pøed smìrováním (-A PREROUTING) do NAT tabulky (-t nat), ¿e
# TCP pakety (-p tcp) z 1.2.3.4 (-d 1.2.3.4) port 8080 (--dport 8080)
# mají cíl mapován (-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 Øízení provádìní NAT

Potøebujeź vytvoøit pravidla pro NAT, která øeknou jádru, jaká spojení a jakým zpùsobem se mají zmìnit. K tomu se pou¿ívá velmi vźestranný nástroj `iptables` s pøepínaèem '-t nat' pro modifikaci NAT tabulky.

Tabulka pravidel NAT obsahuje tøi seznamy nazývané 'øetìzy' ('chains'); pravidla jsou postupnì zkoumána, dokud se nenalezne nìjaké vyhovujcící. Dva øetìzy jsou nazývané PREROUTING (pøed smìrováním, pro Cílovou NAT) a POSTROUTING (po smìrování, pro Zdrojovou NAT).

Následující obrázek by to mìl celkem dobøe osvìtlit, kdybych mìl nìjaké umìlecké nadání:

```
      -----                                   -----
     /     \                                 /     \
   PREROUTING -->[Smìrování ]----------------->POSTROUTING----->
     \D-NAT/          |                      \S-NAT/
                      |                         ^
                      |                         |
                      |                         |
                      |                         |
                      |                         |
                      |                         |
                      |                         |
                      --------> lokální proces -----
```

Jak paket prochází, u ka¿dého bodu (viz výźe) se nejdøíve najde, s kterým spojením je asociován. Jestli¿e jde o nové spojení, nalezne se odpovídající øetìz v NAT tabulce a zkoumá se, co se dále provede. Pokud se bude nìco provádìt, bude to ovlivòovat vźechny následující pakety.

5.1 Jednoduchý výbìr s pou¿itím iptables

`iptables` má velké mno¿ství pøepínaèù, které jsou uvedeny dále. Vźechny pøepínaèe s dvojitou pomlèkou mohou být zkráceny pokud je zachována jednoznaènost. Pokud je podpora iptables zabudována v jádøe jako modul, musí se tento modul nejdøíve zavést: 'insmod ip_tables'.

Nejdùle¿itìjźím pøepínaèem je výbìr tabulky, '-t'. Pro vźechny operace s NAT tabulkou tedy pou¿ívej '-t nat'. Druhým nejdùle¿itìjźím pøepínaèem je pou¿ití '-A' k pøipojení pravidla na konec øetìzu (napø. '-A POSTROUTING') nebo vlo¿ení pravidla na zaèátek (napø. '-I PREROUTING').

Mù¿eź zadat zdroj ('-s' nebo '–source') a cíl ('-d' nebo '–destination') paketù, na které chceź aplikovat NAT. Za tìmito volbami mù¿e být jediná IP adresa (napø. 192.168.1.1), jméno (napø. www.gnumonks.org) nebo adresa sítì (napø. 192.168.1.0/24 nebo 192.168.1.0/255.255.255.0).

Mù¿eź zadat vstupní ('-i' nebo '–in-interface') nebo výstupní ('-o' nebo '–out-interface') rozhraní, které má odpovídat. Zále¿í ale na øetìzu, do kterého dáváź pravidlo: u PREROUTING øetìzu mù¿eź zadat pouze vstupní rozhraní, u POSTROUTING øetìzu pak výstupní rozhraní. Jestli¿e zadáź źpatné rozhraní, `iptables` zahlásí chybu.

5.2 Jemnìjźí èlenìní paketù pro modifikaci

Jak jsem ji¿ øekl, mù¿eź zadat zdrojovou a cílovou adresu. Jestli¿e vynecháź pøepínaè se zdrojovou adresou, pak budou odpovídat vźechny zdrojové adresy. To samé platí i pro cílovou adresu.

Mù¿eź také oznaèit specifický protokol ('-p' nebo '–protocol') jako TCP èi UDP; jen pakety tohoto protokolu budou odpovídat pravidlu. Mo¿nost zadání dalźích speciálních pøepínaèù je hlavním dùvodem, proè zadat protokol: speciálnì mù¿eź zadat zdrojový port ('–source-port' nebo '–sport') a cílový port ('–destination-port' nebo '–dport').

Tyto pøepínaèe ti umo¿ní zadat pravidlo, kterému budou odpovídat jen pakety s urèitými zdrojovými a cílovými porty. To je u¿iteèné pro pøesmìrovávání WWW po¿adavkù (TCP port 80 nebo 8080), zatímco s ostatními pakety se nic nedìje.

Tyto pøepínaèe musí následovat pøepínaè '-p' (co¿ má vedlejźí efekt zavedení sdílené rozźiøující knihovny pro tento protokol). Mù¿eź u¿ít èísla portù nebo jméno portu ze souboru /etc/services.

Vźechny rozlièné cesty, kterými mù¿eź vybrat paket, jsou velmi detailnì popsány v manuálových stránkách (`man iptables`).

6 Jak modifikovat pakety

Teï u¿ tedy víme, jak vybrat pakety, které se budou modifikovat. K dokonèení naźeho pravidla zbývá øíci jádru co pøesnì chceme s tìmito pakety provádìt.

6.1 Zdrojová NAT

Chceź provádìt SNAT, tzn. mìnit zdrojovou adresu spojení na nìjakou jinou. To se dìlá v POSTROUTING øetìzu, tìsnì pøedtím ne¿ je paket koneènì vyslán. To je velice dùle¿itý detail; znamená to, ¿e cokoliv dalźího (smìrování, filtrování paketù) na samotném Linuxovém poèítaèi bude pracovat s nezmìnìným paketem. Znamená to také, ¿e mù¿e být pou¿it pøepínaè '-o' (výstupní rozhraní).

Zdrojová NAT je zadána pou¿itím '-j SNAT' a pøepínaè '–to-source' urèuje IP adresu, rozsah IP adres a pøípadnì port nebo rozsah portù (jen pro protokoly TCP a UDP).

```
## Zmìò zdrojové adresy na 1.2.3.4
# iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4

## Zmìò zdrojové adresy na 1.2.3.4, 1.2.3.5 nebo 1.2.3.6
# iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4-1.2.3.6

## Zmìò zdrojové adresy na 1.2.3.4, porty 1-1023
# iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT --to 1.2.3.4:1-1023
```

6.1.1 Masquerading

Masquerading je speciální pøípad SNAT a mìlo by být pou¿ito jen pro dynamicky pøidìlované IP adresy, jako napøíklad standardní telefonní vytáèení (pro statické IP adresy pou¿ij SNAT viz výźe).

Pro masquerading nemusíź explicitnì urèovat zdrojovou adresu: pou¿ije se zdrojová adresa rozhraní, ze kterého odchází paket. Dùle¿itìjźí je ovźem fakt, ¿e kdy¿ spadne linka, tak jsou spojení (která jsou tak jako tak stejnì ztracena) zapomenuta, co¿ znamená ménì ruźivých zmìn jakmile je spojení opìt nahozeno s novou IP adresou.

```
## Provádìj masquerading na vźem, co odchází z ppp0
# iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

6.2 Cílová NAT

Provádí se v PREROUTING øetìzu, ihned jakmile je paket pøijat. Znamená to, ¿e cokoliv dalźího (smìrování, filtrování paketù) na samotném Linuxovém poèítaèi bude pracovat se 'skuteèným' cílem. Znamená to také, ¿e mù¿e být pou¿it pøepínaè '-i' (vstupní rozhraní).

Cílová NAT je zadána pou¿itím '-j DNAT' a pøepínaè '–to-destination' urèuje IP adresu, rozsah IP adres a pøípadnì port nebo rozsah portù (jen pro protokoly TCP a UDP).

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

## Zmìò cílové adresy na 5.6.7.8, 5.6.7.9 nebo 5.6.7.10.
# iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 5.6.7.8-5.6.7.10

## Zmìò cílové adresy 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 Pøesmìrovávání

Pøesmìrovávání je speciálním pøípadem DNAT a je to èistì jen konvence, proto¿e je navlas stejné s provádìním DNAT na adresu vstupního rozhraní.

```
## Posílej pøíchozí pakety s portem 80 (WWW) na naźi transparentní proxy
## (squid)
# iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 \
        -j REDIRECT --to-port 3128
```

Nezapomeò, ¿e squid musí být nakonfigurován jako transparentní proxy!

6.3

6.4 Mapování detailnì

S nìkteré jemnùstkami NAT vìtźina lidí vùbec nepøijde do styku. Jsou zde zdokumentovány pro zvídavé.

6.4.1 Výbìr rozsahu adres

Jestli¿e je zadán rozsah IP adres, pak IP adresa, která se pou¿ije, je vybrána na základì nejménì pou¿ívané IP adresy pro poèítaèi známá spojení. Dosahuje se tím primitivního rozlo¿ení zatí¿ení.

6.4.2 Vytváøení prázdných NAT mapování

Mù¿eź pou¿ít '-j ACCEPT', co¿ propustí spojení bez dalźího provádìní NAT.

6.4.3 Normální chování NAT

Pøedem nastavené chování je mìnit spojení co mo¿ná nejménì, s dodr¿ováním omezení, které pravidly zadal u¿ivatel. To znamená, ¿e se nepøemapovávají porty (dokud se nemusí).

6.4.4 Implicitní mapování zdrojových portù

I kdy¿ pro spojení není po¿adováno provádìní NAT, mù¿e nastat pøeklad zdrojových portù, jestli¿e jiné spojení bylo mapováno pøes nové. Uva¿ pøípad s masquerading, který je celkem bì¿ný:

1. WWW spojení je navázáno z nìjakého poèítaèe 192.1.1.1, port 1024 na www.netscape.com, port 80.
2. Na toto spojení je aplikováno masquerading pomocí Linuxového poèítaèe tak, aby pou¿ívalo jeho zdrojovou IP adresu (1.2.3.4).
3. Linuxový poèítaè navá¿e spojení s www.netscape.com, port 80 z 1.2.3.4 (adresa výstupního rozhraní), port 1024.
4. NAT zmìní zdrojový port druhého spojení na 1025, aby spolu nekolidovala.

Pokud nastane implicitní mapování zdrojových portù, tak jsou porty rozdìleny do tøí tøíd:

- Porty pod 512,
- porty mezi 512 a 1023
- porty nad 1024 vèetnì.

Port nebude nikdy implicitnì mapován do jiné tøídy.

6.4.5 Co se stane kdy¿ NAT sel¿e

Jestli¿e není ¿ádná mo¿nost, jak jednoznaènì namapovat spojení na u¿ivatelovu ¿ádost, je spojení zahozeno. To také platí pro pakety, které nemohou být pøiøazeny k ¿ádnému spojení, až u¿ kvùli jejich poźkození nebo pro nedostatek pamìti poèítaèe apod.

6.4.6 Vícenásobné mapování, pøekrývání a kolize

Mohou existovat pravidla NAT, která mapují pakety do toho samého rozsahu; kód NAT je natolik chytrý, aby zabránil kolizím. Tudí¿ dvì pravidla, která mapují zdrojovou adresu 192.168.1.1 a 192.168.1.2 na 1.2.3.4 jsou v poøádku.

Co více, mù¿eź mapovat pøes opravdové, pou¿ívané IP adresy tak dlouho, dokud tyto adresy projdou pøes mapovací poèítaè. Tedy, pokud máź pøiøazenou síż (1.2.3.0/24), ale jedna vnitøní síż pou¿ívá tyto adresy a druhá privátní Internetové adresy 192.168.1.0/24, mù¿eź aplikovat NAT ze zdrojových adres 192.168.1.0/24 na síż 1.2.3.0 bez obav z kolizí:

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

Podobný postup platí i pro adresy pou¿íváné samotným NAT poèítaèem: to je zpùsob, jakým pracuje masquerading (sdílením adresy rozhraní mezi ‘opravdovými ’pakety z NAT poèítaèe a pakety, na které bylo provedeno masquerading).

Dále mù¿eź mapovat ty samé pakety na mnoho rùzných cílù s tím, ¿e budou sdílené. Pokud nechceź napøíklad mapovat nic na 1.2.3.5, mù¿eź zadat:

```
# 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
```

6.4.7 Mìnìní cílù lokálnì vytváøených spojení

NAT ti dovoluje vlo¿it pravidla DNAT do výstupního øetìzu, co¿ ale není plnì podporováno v 2.4 (mù¿e být, vy¿aduje to ale nové pøepínaèe, trochu testování a trochu vìtźí kus programování, tak¿e dokud se nìkdo nedohodne s Rustym, neoèekával bych to brzy).

Souèasným omezením je nemo¿nost zmìnit cíl na jiné poèítaèe ne¿ localhost (tedy ‘-j DNAT –to 127.0.0.1’), proto¿e jinak jsou odpovìdi źpatnì pøekládány.

7 Speciální protokoly

Nìkteré protokoly nemají rády, pokud se na nì aplikuje NAT. Pro ka¿dý z tìchto protokolù musí být napsána dvì rozšíøení: jedno pro sledování spojení protokolu a druhé pro samotné NAT.

V distribuci netfilteru jsou zatím moduly pro ftp: ip_conntrack_ftp.o a ip_nat_ftp.o. Pokud tyto moduly zavedeš do jádra (nebo je do jádra zakompiluješ), pak by mìlo pracovat jakékoli NAT na ftp spojení. Pokud tyto moduly nepou¿iješ, mù¿eš pou¿ít pouze pasivní ftp a i to nemusí fungovat spolehlivì jestli¿e provádíš slo¿itìjší SNAT.

8 Upozornìní k NAT

Pokud aplikuješ na spojení NAT, všechny pakety, které procházejí **obìma** smìry (do a ze sítì), musí procházet NAT poèítaèem, jinak to nebude spolehlivì fungovat. Pøedevším, kód pro sledování spojení sestavuje fragmenty paketù, co¿ znamená, ¿e nejen sledování spojení nebude spolehlivé, ale i ¿e pakety samotné nemusejí vùbec projít kvùli odmítnutým fragmentùm.

9 SNAT a smìrování

U SNAT musíš dodr¿et to, ¿e ka¿dý poèítaè musí na SNAT pakety odpovídat zpìt poèítaèi, který tyto pakety vyslal. Napøíklad mapuješ nìjaké odchozí pakety na zdrojovou adresu 1.2.3.4. Pak venkovní smìrovaè musí vìdìt, ¿e odpovìdi (které mají **cíl** 1.2.3.4) musí posílat zpìt tomuto poèítaèi. Toto se dá provést následujícími zpùsoby:

1. Pokud provádíš SNAT na vlastní adresu poèítaèe (pro kterého smìrování a všechno ostatní u¿ pracuje), nemusíš dìlat nic.
2. Pokud provádíš SNAT na nepou¿ívanou adresu na lokální síti (napøíklad mapuješ na 1.2.3.99, volnou adresu na síti 1.2.3.0/24), musí tvùj NAT poèítaè odpovídat na ARP ¿ádosti pro tyto adresy stejnì tak jako pro svojí. Nejjednodušší je vytvoøit IP alias, napø.:

   ```
   # ip address add 1.2.3.99 dev eth0
   ```

3. Pokud provádíš SNAT na úplnì odlišnou adresu, musíš zajistit, aby poèítaèe, které obdr¿í SNAT paket, smìrovaly tuto adresu zpìt k NAT poèítaèi. To je splnìno, pokud je NAT poèítaè pøednastavená brána (gateway). Jinak musíš propagovat cestu (pokud pou¿íváš smìrovací protokol) nebo ruènì pøidat cesty na ka¿dý takto 'posti¿ený' poèítaè.

10 DNAT na tu samou sí»

Pokud provádíš portforwarding zpìt na tu samou sí», musíš zajistit, aby všechny následující pakety i odpovìdi na nì procházely NAT poèítaèem (aby mohly být zmìnìny). Kód NAT nyní (od verze 2.4.0-test6) dovoluje blokovat odchozí ICMP pøesmìrování, které je vysíláno pokud NAT paket odchází tím samým rozhraním, kterým pøišel, a server stále zkouší odpovídat pøímo klientovi (který nerozpozná odpovìï).

Klasickým pøípadem je kdy¿ vnitøní poèítaèe zkouší pøistoupit k 'veøejnému' WWW serveru, na kterém je ale provádìno DNAT z veøejné adresy (1.2.3.4) na vnitøní poèítaè (192.168.1.1):

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

Jeden zpùsob je rozbìhnout DNS server, který zná opravdovou (vnitøní) IP adresu veøejného WWW serveru a smìrovat vźechny ostatní ¿ádosti na vnìjźí DNS server. To znamená, ¿e na WWW serveru se budou vnitøní IP adresy zobrazovat správnì.

Pøi druhém zpùsobu NAT poèítaè mapuje také zdrojovou IP adresu na svoji vlastní pro tato WWW spojení a klame tak server tím, ¿e skrz nìj odpovídá. V tomto pøíkladì pøedpokládáme, ¿e IP adresa NAT poèítaèe je 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
```

Proto¿e **PREROUTING** pravidlo se zkoumá jako první, pakety budou ji¿ urèeny pro vnitøní WWW server a mù¿eme tak urèit, které z nich mají vnitøní zdrojovu adresu.

11 Podìkování

Rád bych podìkoval pøedevźím firmì WatchGuard a Davidu Bonnovi, který vìøil v ideu netfilteru natolik, ¿e mì podporoval v mé práci.

Také vźem ostatním, kteøí klidnì snáźeli moje nadávky, kdy¿ jsem objevoval źkaredosti NAT, a obzvláźtì tìm, kteøí pøeèetli mùj deník.

Rusty.