Konfigurace překladu adres (NAT) s pomocí Linux IPTables

Petr Grygárek, FEI, VŠB-TU Ostrava

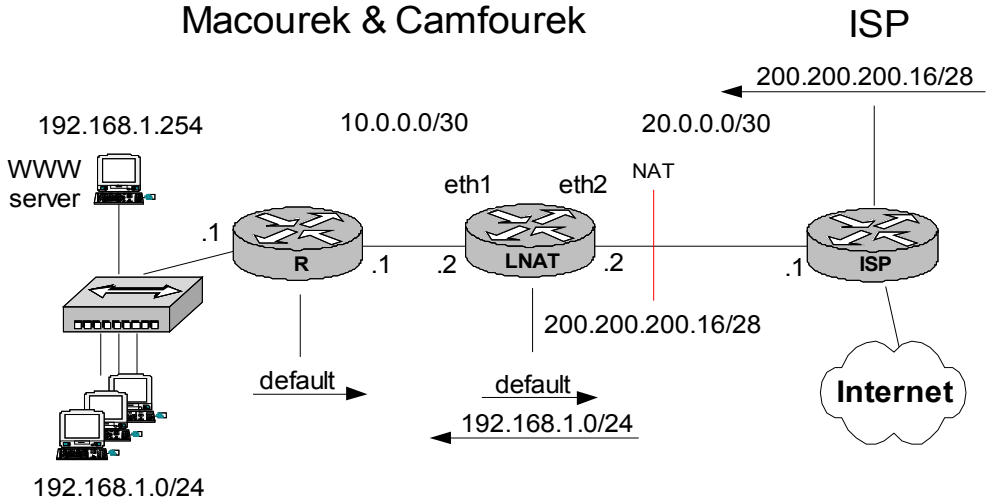
Rozšíření jádra Linuxu iptables umožňuje provádět manipulaci s procházejícími pakety, včetně filtrace a překladu adres. Celkový popis architektury iptables lze nalézt v příslušném HOWTO. V tomto textu si ukážeme příklad, jak pomocí iptables realizovat dynamický NAT a přesměrování provozu mířícího na určitý port linuxového směrovače na jinou IP adresu.

Situace

Firma Macourek & Camfourek, provozující směrovač R (viz obrázek), používala privátního rozsahu IP adres (192.168.1.0). Později se rozhodla připojit k Internetu prostřednictvím směrovače ISP. ISP firmě přidělil veřejný rozsah adres 200.200.200.16/28; linka mezi ISP a firmou dostala adresu sítě 20.0.0.0/30. Jelikož však firma provozuje větší množství stanic, než dovoluje přiřazený rozsah a také proto, aby nebylo třeba stanice firmy přeadresovat, bylo rozhodnuto o použití NAT.

Firma dále zamýšlí provozovat veřejně dostupný WWW server, který bude pod pevnou adresou 200.200.200.30 dostupný z Internetu. Hodlá jej však provozovat na vnitřní síti na stroji, jehož vnitřní adresa je 192.168.1.254.

Protože platforma směrovače R nepodporuje NAT a ani ISP není ochoten NAT provádět, rozhodl administrátor firmy Macourek & Camfourek mezi směrovače R a ISP vložit pomocný směrovač LNAT založený na Linuxu s použitím IPTables. Tím vznikla další síť (mezi směrovači R a LNAT), které se administrátor rozhodl přidělit privátní adresu 10.0.0.0/30. Adresy této sítě nejsou propagovány ani do Internetu, ani do vnitřní sítě firmy a nepodléhají ani překladu adres.



Konfigurace směrovače R

Na směrovači R je nakonfigurována pouze statická default cesta – veškeré pakety pro sítě přímo nepřipojené k R se posílají na přilehlé rozhraní směrovače LNAT.

Upozornění:

Protože adresy spojovací linky mezi R a LNAT nepodléhají překladu adres, není možné ověřovat konektivitu na ISP ze směrovače R pomocí zpráv echo request (ping) se zdrojovou adresou rozhraní připojeného k LNAT (10.0.0.1). Adresy z rozsahu 10.0.0.0/30 jsou totiž známy pouze směrovačům R a LNAT, takže ISP neví, kam směrovat odpověď (echo reply). Ping lze pro testování použít jen

tehdy, je-li příslušnou volbou příkazu ping zajištěno nastavení adresy rozhraní k segmentu 192.168.1.0 jako zdrojové adresy vysílané žádosti o odezvu (echo request).

Konfigurace směrovače ISP

Na směrovači ISP je nakonfigurována statická cesta, která adresy veřejného rozsahu 200.200.200.16/28 přiděleného firmě Macourek & Camfourek směruje na přilehlé rozhraní směrovače LNAT.

Konfigurace směrovače LNAT

Na směrovači LNAT musíme povolit směrování, naplnit směrovací tabulku a aplikovat NAT.

Povolení směrování paketů

Nejprve musíme povolit směrování paketů jádrem. U jádra verze 2.4 se to provede zapsáním jedničky (znaku „1“) do souboru /proc/net/ipv4/ip_forward.

Jednou z možností jak toto realizovat, je příkaz

```
echo 1 >  /proc/sys/net/ipv4/ip_forward
```

Definice směrovací tabulky

Směrovač LNAT musí být schopen nejen překládat adresy, ale také směrovat. Pakety na adresy vnitřní sítě (přišlé od ISP s cílovými adresami rozsahu 200.200.200.16/28 a přeloženými NATem) musí být zasílány na přilehlé rozhraní směrovače R. To se zajistí definicí přislušné statické cesty. Naopak pakety s adresami z Internetu budou díky nakonfigurování statické default cesty zasílány na směrovač ISP.

Aplikace NAT

Aplikace NAT na směrovači LNAT podle požadavků zadání bude sestávat ze dvou kroků:

1. Překlad adres rozsahu 192.168.1.0/24 na dynamicky volené adresy rozsahu 200.200.200.17-200.200.200.29.

2. Přesměrování veškerého provozu přicházejícího od ISP na adresu 200.200.200.30 a port 80 (služba WWW) a odpovídajícího opačného směru provozu na vnitřní adresu 192.168.1.254.

Krok 1

Do tabulky NAT udržované iptables musíme přidat pravidlo do řetězu POSTROUTING, které říká, že u všech paketů odcházejících rozhraním eth2 se zdrojovou adresou z rozsahu 192.168.1.0/24 má být zdrojová adresa překládána na dynamicky volenou adresu z rozsahu 200.200.200.17-200.200.200.29. K tomu bude využito tzv. Source NAT (SNAT).

Pravidlo je přidáno do řetězu POSTROUTING, protože přepis zdrojové adresy se děje až poté, co směrování rozhodne o rozhraní, kterým má být paket odeslán. :

```
iptables -t nat -s 192.168.1.0/24 -o eth2 -A POSTROUTING -j SNAT \
  --to 200.200.200.17-200.200.200.29
```

Krok 2

K přesměrování portu 80/TCP z navenek prezentované adresy 200.200.200.30 na vnitřní adresu 192.168.1.254 použijeme přepis cílové adresy, tzv. Destination NAT (DNAT). Příslušné pravidlo

přidáme do řetězu PREROUTING tabulky NAT, protože překlad cílové adresy musí být uskutečněn ihned po příchodu paketu zvnějšku, ještě před rozhodnutím, na které rozhraní má být směrován.

iptables -t nat -d 200.200.200.30 -p tcp --dport 80 -A PREROUTING -j DNAT --to 192.168.1.254

Pro ověření lze seznam pravidel, které iptables uchovávají v tabulce NAT, vypsat příkazem

iptables -t nat -n - - list

Přepínačem -n říkáme, že preferujeme výpis IP adres v numerickém formátu. Systém se tak nebude pokoušet kontaktovat DNS server a překládat adresy na doménová jména.

Chybně zapsané pravidlo můžeme odstranit příkazem
iptables -t nat -D {POSTROUTING|PREROUTING} <c_pravidla>