

Translacja adresów sieciowych w systemie Linux

1 Wprowadzenie

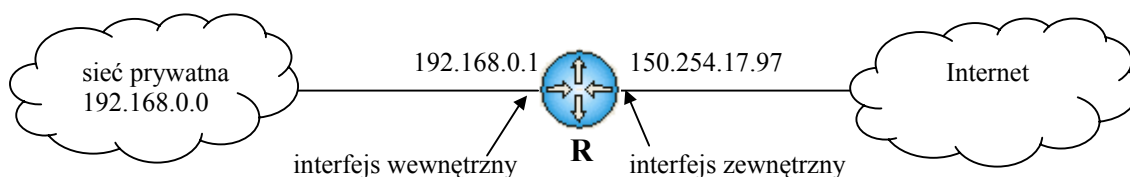
Wymagania wstępne: wykonanie ćwiczenia „Filtracja pakietów w systemie Linux”.

Technologia translacji adresów sieciowych (ang. Network Address Translation, w skrócie NAT) została po raz pierwszy zaproponowana przez firmę Cisco i w roku 1993 opisana w dokumencie RFC1631. Od końca lat 80-tych liczba komputerów dołączanych do sieci Internet wzrasta wykładniczo. To spowodowało, że przestrzeń adresów IP już w latach 90-tych się wyczerpywała. Zaobserwowano wówczas, że jeśli tempo zużycia przestrzeni IP się utrzyma, to w niedalekiej przyszłości (przewidywanej na lata 1994-95) zupełnie zabraknie publicznych adresów IP dla nowobudowanych sieci. Technologia NAT i leżące u jej podstaw nowe podejście do projektowania sieci IP, pozwoliły przedłużyć tę „niedaleką przyszłość” co najmniej do dziś. Poniżej opisana została idea technologii NAT.

Wiele dzisiejszych sieci IP nie opiera się już na *publicznych* adresach sieci, bo takich już brakuje. Zamiast tego stosowane są dla tych sieci adresy *prywatne*. Należą do nich:

- dla klasy A – adresy z zakresu 10.0.0.0 - 10.255.255.255
- dla klasy B – adresy z zakresu 172.16.0.0 - 172.31.255.255
- dla klasy C – adresy z zakresu 192.168.0.0 - 192.168.255.255

Ponieważ powyższe adresy nie są rejestrowane, może istnieć wiele sieci wykorzystujących tę samą pulę adresów prywatnych, a to czyni sieć Internet skalowalną. Ale z drugiej strony fakt, że adresy prywatne nie są unikalne, stwarza pewne ograniczenie. Otóż pakiety z takimi adresami nie mogą być przesyłane w Internecie, gdyż nie można określić dla nich trasy. I właśnie ten problem rozwiązuje technologia NAT. Dzięki niej do uzyskania łączności sieci prywatnej z Internetem wystarcza jeden adres publiczny IP – adres zewnętrznego interfejsu rutera. Od strony Internetu cała sieć prywatna widziana jest pod tym jednym adresem. Dalej opisano dwie główne odmiany NAT: translację adresów źródłowych SNAT (ang. Source NAT) i adresów docelowych DNAT (ang. Destination NAT). Aby opis był bardziej zrozumiały, został wsparty poniższym przykładem. Zilustrowano w nim dwie sieci, między którymi znajduje się ruter pełniący dodatkowo funkcję NAT.



1.1 SNAT

Translacja SNAT umożliwia komputerom w sieci prywatnej dostęp do Internetu, a dokładniej – do usług oferowanych przez różne serwery. Oznacza to, że pakiety, których źródłem są komputery sieci prywatnej, powinny docierać do tych serwerów, a odpowiedzi – wracać z powrotem. Proces translacji SNAT przebiega w dwóch krokach:

1. Gdy pakiet opuszcza sieć źródłową, ruter zamienia prywatny adres IP źródła na adres swojego publicznego interfejsu oraz numer portu źródłowego na inny, nie zajęty numer portu. Zapamiętuje tę zmianę w *tablicy translacji* w postaci odwzorowania `oryginalny_adres_IP:oryginalny_port→nowy_adres_IP:nowy_port`.

Dzięki zamianie adresu źródłowego na publiczny można dla pakietu z odpowiedzią

jednoznacznie określić trasę. Nowy numer portu zaś pozwala dodatkowo rozróżniać poszczególne adresy prywatne, dzięki czemu z usług Internetu może jednocześnie korzystać wiele komputerów sieci prywatnej.

2. Gdy ruter otrzymuje pakiet-odpowiedź, publiczny adres docelowy (będący adresem źródłowym w poprzednim pakiecie) wraz z numerem portu docelowego są zamieniane z powrotem na oryginalne wartości zgodnie z zapamiętanym wcześniej odwzorowaniem. Dzięki temu odpowiedź dociera do właściwego procesu na właściwym komputerze.

Przykład:

Uwaga – skróty SA, DA, SP i DP oznaczają kolejno: adres IP źródłowy, adres IP docelowy, numer portu źródłowego i numer portu docelowego.

1. Komputer o adresie 192.168.0.2 wysyła pakiet do Internetu na adres 130.130.1.1.
W pakiecie SA=192.168.0.2, DA=130.130.1.1, SP=3345, DP=80.
2. Pakiet dociera do rutera R, będącego bramą dla komputerów sieci prywatnej.
3. Ruter zamienia SA na adres 150.254.17.97, a SP na inny numer nie zajętego portu, np. SP=5523. Ruter zapamiętuje odwzorowanie 192.168.0.2:3345→150.254.17.97:5523 i wysyła pakiet do Internetu. Prawa część odwzorowania służy jako indeks przy przeszukiwaniu tablicy.
4. Ruter otrzymuje pakiet-odpowiedź, w którym SA=130.130.1.1, DA=150.254.17.97, SP=80, DP=5523 i na podstawie zapamiętanego odwzorowania ustawia w pakiecie DA=192.168.0.2 oraz DP=3345.

1.1 DNAT

Translacja DNAT umożliwia komputerom z sieci publicznej (tu - Internet) dostęp do usług oferowanych przez serwery znajdujące się w sieci prywatnej. Oznacza to, że pakiety, których źródłem są komputery sieci publicznej, powinny docierać do tych serwerów, a odpowiedzi – wracać z powrotem. Usługi sieci prywatnej dostępne są dla sieci zewnętrznej pod publicznym adresem interfejsu rutera. Translacja DNAT przebiega w dwóch krokach:

1. Gdy pakiet dociera do sieci prywatnej, jego adres IP docelowy jest ustawiony na publiczny adres zewnętrznego interfejsu rutera; pod tym adresem bowiem usługa jest dostępna. Ruter zamienia ten adres na właściwy adres serwera; w najprostszym przypadku numer portu docelowego nie ulega zmianie.
2. Gdy ruter otrzymuje pakiet-odpowiedź, z powrotem zamienia prywatny adres źródłowy na adres publiczny swojego zewnętrznego interfejsu.

1.2 Szablon reguły

Dla translacji SNAT:

```
iptables -t nat -A POSTROUTING <wzorzec> -j SNAT --to-source <adres_publiczny>
```

Dla translacji DNAT:

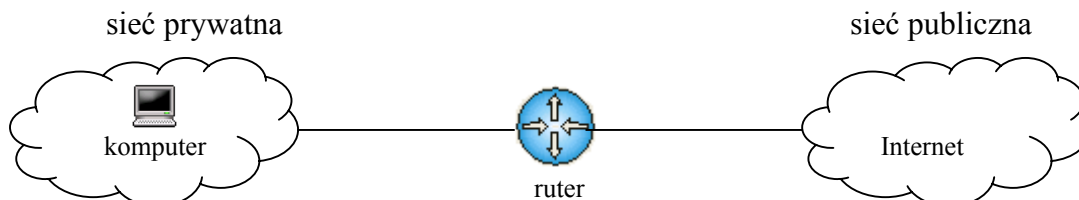
```
iptables -t nat -A PREROUTING <wzorzec> -j DNAT --to-destination <adres_prywatny>
```

2. Organizacja, wymagany sprzęt i oprogramowanie

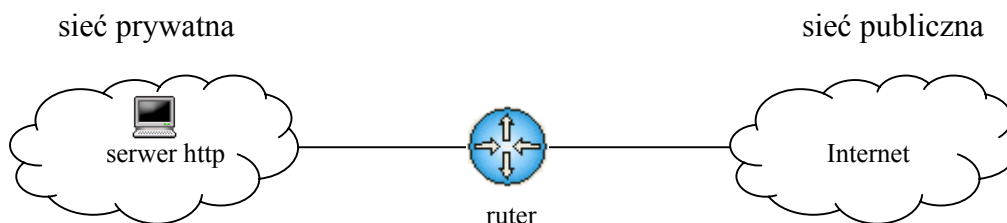
- zadania wykonywane są w grupach 2-osobowych;
- sprzęt: 2 komputery PC – jeden pracuje jako ruter, a drugi - jako komputer (zad. 3.1) lub serwer (zad. 3.2);
- oprogramowanie: system Linux z modułem iptables.

3. Zadania

1. Zgodnie z podanym niżej rysunkiem należy skonfigurować w systemie Linux komputer i ruter do pracy w sieci. Następnie, używając programu iptables, należy w routerze włączyć funkcję SNAT, tak by komputer z sieci prywatnej miał dostęp do usług Internetu.



2. Zgodnie z podanym niżej rysunkiem należy skonfigurować w systemie Linux komputer i ruter do pracy w sieci. Komputer ma ponadto pełnić rolę serwera http. Następnie, używając programu iptables, należy w routerze włączyć funkcję DNAT, tak by komputery z sieci publicznej miały dostęp do usług tego serwera.



4. Pytania sprawdzające

1. Należy samodzielnie opracować przykład ilustrujący działanie translacji DNAT.
2. Czy NAT jest protokołem sieciowym?
3. Ile (teoretycznie) komputerów sieci prywatnej może jednocześnie korzystać z usług sieci Internet, gdy zastosowano SNAT?
4. Dlaczego przy translacji SNAT wykorzystany jest łańcuch POSTROUTING, a przy DNAT – łańcuch PREROUTING?
5. Technologia NAT ma zarówno swoich zwolenników, jak i przeciwników. Dlaczego?

5. Literatura

1. Wprowadzenie do technologii NAT: książki A. S. Tanenbaum „Computer Networks” oraz J. Kurose i K. Ross „Computer Networking – A Top-Down Approach Featuring the Internet”; dokumenty RFC1631, RFC2663, RFC3022 (www.ietf.org/rfc) oraz serwis internetowy www.cisco.com.
2. Podręcznik internetowy o iptables: <http://iptables-tutorial.frozentux.net/>