Filtracja pakietów w systemie Linux

1 Wprowadzenie

Wymagania wstępne: wykonanie ćwiczenia „Statyczny wybór trasy w systemie Linux”.
Filtracja pakietów to działanie polegające na odrzucaniu jednych i akceptowaniu innych wiadomości. Odrzucane są te wiadomości, które z pewnych względów zostały uznane za niepożądane (np. generują niechciany ruch w sieci lub zagrażają bezpieczeństwu sieci). Filtracja może zatem podnosić wydajność i poziom bezpieczeństwa sieci.

System, w którym dokonuje się filtracji, nazywa się *zaporą sieciową* (ang. firewall). Może on zabezpieczać całą sieć (jest tak w przypadku zapory w ruterze, ang. firewall router) lub pojedynczy komputer (ang. personal firewall).

Niniejsze ćwiczenie polega na konfigurowaniu filtracji datagramów IP w systemie Linux z wykorzystaniem pakietu iptables. Dalsza część wstępu krótko omawia najważniejsze cechy pakietu.

1.1 Pakiet iptables – reguły, tablice i łańcuchy

Pakiet iptables jest następcą wcześniejszych, ipfwadm i ipchains. Pozwala filtrować wiadomości na podstawie dwóch źródeł informacji: informacji systemowych oraz informacji zawartych w samej wiadomości (z warstw łącza danych, sieciowej i transportowej). Konfigurowanie filtracji polega na definiowaniu tzw. *reguł* (ang. rule). Pojedyncza reguła składa się z *wzorca* i *akcji*. Gdy wiadomość poddawana jest analizie, najpierw dopasowywana jest do wzorca; jeśli do niego pasuje, o dalszym losie wiadomości decyduje akcja reguły. Jeśli zaś dane w wiadomości nie pasują do wzorca danej reguły, pod uwagę brana jest kolejna reguła. Reguły przeglądane są w takim porządku, w jakim zostały wprowadzone. Dla danej wiadomości przeszukiwanie reguł trwa do momentu pierwszego dopasowania do wzorca lub (w przypadku braku dopasowania) do wyczerpania reguł.

Akcja reguły zależy od jej typu. Wyróżnia się trzy typy reguł: reguły filtrujące, reguły translacji NAT oraz reguły do manipulacji zaawansowanymi opcjami protokołu IP. Dla przykładu, w regułach filtrujących, które są najważniejsze w tym ćwiczeniu, akcją jest najczęściej odrzucenie (DROP) lub akceptacja wiadomości (ACCEPT). Wszystkie reguły tego samego typu pamiętane są w strukturze zwanej *tablicą* (ang. table), od której pakiet bierze swą nazwę. Istnieją zatem trzy wbudowane tablice: filter (dla reguł filtrujących), nat (dla reguł translacji NAT) oraz mangle (dla reguł manipulujących opcjami IP).

Datagramy IP również dzielą się na kilka rodzajów. Rodzaj datagramu zależy od kombinacji adresów źródłowego i docelowego w nim zawartych. Wyróżnia się zatem 1) datagramy, dla których dana stacja jest celem, 2) datagramy, których dana stacja jest źródłem, 3) kombinację rodzajów 1 i 2 oraz 4) datagramy rutowane.

W zależności od rodzaju datagramu, jego przetwarzanie przebiega w kilku etapach. Na przykład dla datagramów rutowanych etapy te w uproszczeniu wyglądają następująco:

1 – pakiet dociera do interfejsu wejściowego,
2 – zostaje wybrany dla niego właściwy interfejs wyjściowy,
3 – pakiet opuszcza stację przez interfejs wyjściowy.

Na każdym etapie można stosować do datagramu różne typy reguł. Dlatego wewnątrz każdej tablicy reguły są dodatkowo grupowane ze względu na etap przetwarzania pakietu. Wobec tego różne tablice mogą zawierać grupy reguł związanych z tym samym etapem. Sekwencja reguł powstała przez połączenie tych grup nazywa się *łańcuchem* (ang. chain). Pakiet iptables zawiera pięć wbudowanych łańcuchów: INPUT (dla datagramów pierwszego rodzaju), OUTPUT (dla pakietów drugiego rodzaju), FORWARD (dla pakietów rutowanych) oraz

PREROUTING i POSTROUTING. Dwa ostatnie łańcuchy oraz tablica nat będą przedmiotem kolejnego ćwiczenia, dotyczącego translacji adresów sieciowych.

1.2 Moduł Connection Tracking

Pakiet iptables zawiera również moduł śledzenia stanu interakcji sieciowych, zwanych też połączeniami. Ponieważ jednak termin „połączenie" najczęściej kojarzony jest z połączeniem TCP, dalej używane będzie ogólniejsze określenie „interakcja".

Moduł Connection Tracking (w skrócie conntrack) wyróżnia cztery stany interakcji:

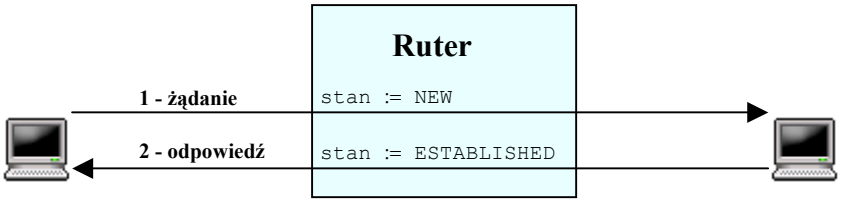
NEW – interakcja otrzymuje stan NEW, gdy do rutera dotrze pierwszy pakiet z nią związany (np. jeden komputer wysyła do innego pakiet ICMP Echo request);

ESTABLISHED – interakcja przechodzi ze stanu NEW do tego stanu, gdy do rutera dotrze pakiet będący odpowiedzią na pierwszy pakiet (np. wysłanie pakietu ICMP Echo reply w odpowiedzi na wcześniejszy Echo request, patrz poniższy rysunek);

RELATED - ten stan otrzyma interakcja, która jest związana z inną, będącą w stanie ESTABLISHED. O istnieniu związku między interakcjami decyduje specyfika protokołu. Na przykład kanał kontrolny protokołu FTP jest związany z kanałem danych;

INVALID – interakcji, która nie znalazła się w żadnym z powyższych trzech stanów, przypisywany jest stan INVALID.

Jądro systemu Linux zapamiętuje bieżące interakcje wraz z ich stanami w pliku **`/proc/net/ip_conntrack`**.



1.3 Budowa reguły

Ogólna składnia reguły jest następująca:

iptables [-t tablica] komenda [wzorzec] [akcja]

Komendy:

-P ustawienie domyślnej akcji dla łańcucha. Domyślna akcja jest stosowana dopiero wówczas, gdy pakiet nie pasuje do wzorca żadnej reguły łańcucha
-A dodanie reguły do określonego łańcucha
-L -n wyświetlenie wszystkich reguł łańcucha
-F usunięcie wszystkich reguł łańcucha

Opcje wzorca:

-p wybór protokołu: tcp, udp icmp lub all (wszystkie protokoły stosu TCP/IP)
-s adres IP źródłowy (może być uogólniony do adresu sieci)
-d adres IP docelowy (może być uogólniony do adresu sieci)
-i interfejs wejściowy
-o interfejs wyjściowy
--sport port źródłowy
--dport port docelowy
-m dopasowanie jawne – ogólniejsza postać dopasowania, pozwalająca odwoływać się do atrybutów, które (w odróżnieniu od powyższych) nie posiadają predefiniowanych opcji. Zaliczamy do nich na przykład stany interakcji modułu conntrack.

Do najważniejszych akcji należą: ACCEPT, DROP, REJECT, LOG, SNAT lub DNAT. Akcję poprzedza przełącznik –j.

Przykłady:

```
iptables -P INPUT DROP
```

ustawienie domyślnej akcji dla łańcucha INPUT na DROP

```
iptables -A INPUT -s 150.254.17.100 -j DROP
```

odrzucenie pakietów kierowanych do tej stacji spod adresu 150.254.17.100

```
iptables -A OUTPUT -p tcp --dport 22 -j ACCEPT
```

akceptacja pakietów protokołu ssh wysyłanych z tej stacji (pakiety są wypuszczane)

```
iptables -A INPUT -p udp -s 150.254.17.100 --sport 52 --dport 53 -j ACCEPT
```

akceptacja zapytań klienta DNS wysyłanych z adresu 150.254.17.100

```
iptables -A FORWARD -s 150.254.17.96/27 -m state --state NEW -j ACCEPT
```

akceptacja pakietów inicjalizujących sesje, wysyłanych z sieci 150.254.17.96

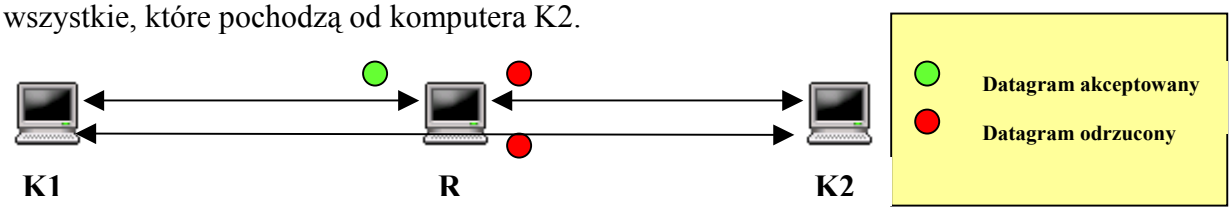
2. Organizacja, wymagany sprzęt i oprogramowanie

- zadania wykonywane są w grupach 2 lub 3-osobowych;
- sprzęt: 3 komputery PC;
- oprogramowanie: system Linux z zainstalowanym pakietem iptables.

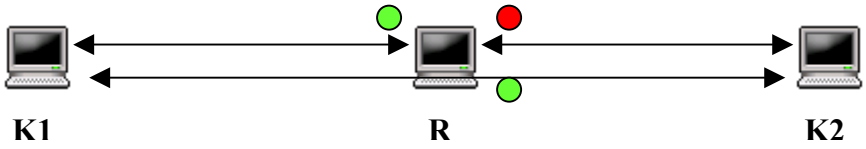
3. Zadania

Należy skonfigurować filtrację dla trzech poniższych sytuacji:

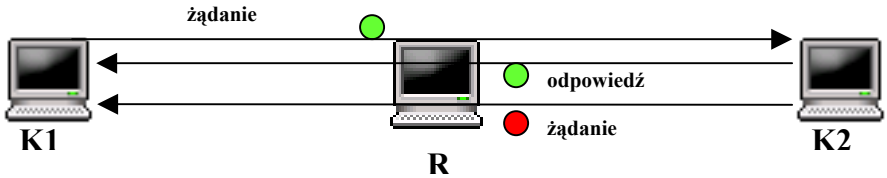
1. Ruter R akceptuje wszystkie datagramy przysyłane od komputera K1, a blokuje wszystkie, które pochodzą od komputera K2.



2. Ruter R akceptuje wszystkie datagramy przysyłane od K1, blokuje wszystkie, które pochodzą od K2 i są adresowane do R, ale jednocześnie akceptuje wszystkie datagramy z K2 adresowane do K1; wszystkie pozostałe datagramy są blokowane.



3. (Uwaga – należy wykorzystać moduł Connection Tracking)
Ruter R akceptuje wszystkie datagramy przesyłane (w dowolnym kierunku) w ramach interakcji inicjowanych przez komputer K1, a blokuje wszystkie, których inicjatorem jest komputer K2 (przykładowe zachowanie: ping K1→K2 się powiedzie, a ping K2→K1 nie). Taki rodzaj ochrony, nazywany filtracją stanową, jest często stosowany w sieciach, które nie udostępniają żadnych usług w sieci Internet.



4. Pytania sprawdzające

1. Opisz architekturę pakietu iptables.
2. Jakie zastosowanie mają łańcuchy PREROUTING i POSTROUTING?
3. Jaki jest związek między „szczelnością” a elastycznością reguł filtracji?

5. Literatura

1. Składnia reguł iptables: podręcznik man systemu Linux.
2. Strona domowa projektu iptables: www.netfilter.org.
3. Internetowy podręcznik o iptables: http://iptables-tutorial.frozentux.net/
4. Bezpieczeństwo w sieci komputerowej: książki A. S. Tanenbaum „Computer Networks” oraz J. Kurose i K. Ross „Computer Networking – A Top-Down Approach Featuring the Internet”.