Zapory sieciowe i techniki filtrowania danych

Robert Jaroszuk
<zim@iq.pl>

"Where you see a feature, I see a flaw..."

Zimowisko TLUG

Harcerski Ośrodek Morski w Pucku, styczeń 2008

- Wprowadzenie
- Kiedy i dlaczego stosujemy zapory sieciowe ?
- Mechanizmy działania zapór sieciowych
- Systemy pośredniczące (proxy)
- Kilka przykładów konfiguracji iptables

Zapora sieciowa (ang. firewall) – każdy program lub urządzenie, ograniczające korzystanie z sieci.

Termin pochodzi (m.in.) z budownictwa (USA) – zapora przeciwpożarowa

Zapory sieciowe stosujemy, gdy chcemy:

- zapewnić „bezpieczny” dostęp do sieci publicznej (np. Internet) użytkownikom sieci prywatnej
- zapewnić ochronę sieci prywatnej przed nieupoważnionym dostępem z sieci publicznej
- blokować całkowicie lub częściowo dostęp do określonych miejsc w sieci publicznej

Zapory sieciowe stosujemy, gdy chcemy:

- monitorować komunikację pomiędzy sieciami (np. między siecią prywatną a Internetem)
- rejestrować całość lub interesującą nas część ruchu pomiędzy sieciami
- uczynić zasoby sieci „niewidocznymi” z zewnątrz
- uczynić topologię sieci „niewidoczną” z zewnątrz

Strategie definiowania polityki zapory sieciowej

- domyślne blokowanie

```
-A FORWARD -s 192.168.0.0/24 -d 0/0 --dport 80 -j ACCEPT
-A FORWARD -s 192.168.0.0/24 -d 0/0 -j DROP
lub:
-P FORWARD DROP
```

- domyślne przepuszczanie

```
-P FORWARD ACCEPT (tak jest domyślnie)
-A FORWARD -s 192.168.0.0/24 -d 0/0 --dport 21 -j DROP
.
.
-A FORWARD -s 192.168.0.0/24 -d 0/0 --dport 995 -j DROP
```

Podstawowe mechanizmy działania zapór sieciowych

- filtrowanie pakietów
- translacja adresów IP (NAT)
- usługi proxy

Filtrowanie pakietów

Filtrowanie pakietów jest podstawową funkcją zapory sieciowej. Filtrowanie polega na analizie pakietów docierających do zapory i kontrolowaniu które pakiety mogą zostać przepuszczone a które mają zostać zatrzymane.

Filtrowanie pakietów

Może odbywać się na podstawie:

- analizy źródłowego i docelowego adresu
- analizie numerów portów
- analizie flag
- w rozszerzonych wersjach zapór może dochodzić:
  - analiza zawartości pakietu
  - reguły oparte o czas, quoty ruchu, analiza wartości TTL,
  - wiele innych

Filtrowanie pakietów (poziomy)

Wyróżnić można następujące poziomy filtrowania:

- warstwa sieci (adresacja MAC)
- warstwa IP
- warstwa transportowa (porty)
- warstwa aplikacji

Filtrowanie pakietów (sposoby)

- filtrowanie proste – analiza źródłowego i docelowego adresu IP oraz portu.
- filtrowanie zaawansowane – tzw. filtry dynamiczne – posiadają możliwość rozpoznawania przynależności pakietu do połączenia.

Filtrowanie pakietów (konfiguracja)

- przygotowanie polityki bezpieczeństwa – określenie co przepuszczamy a co blokujemy
- przepisanie polityki bezpieczeństwa na zestaw logicznych wyrażeń
- przepisanie logicznych wyrażeń na składnię danej zapory sieciowej

Filtrowanie pakietów (zalety)

- możliwość zabezpieczenia sieci prywatnej z jednego centralnego punktu
- możliwość wykrycia i odrzucenia nieporządanego ruchu
- możliwość wykrycia spoofingu z sieci lokalnej

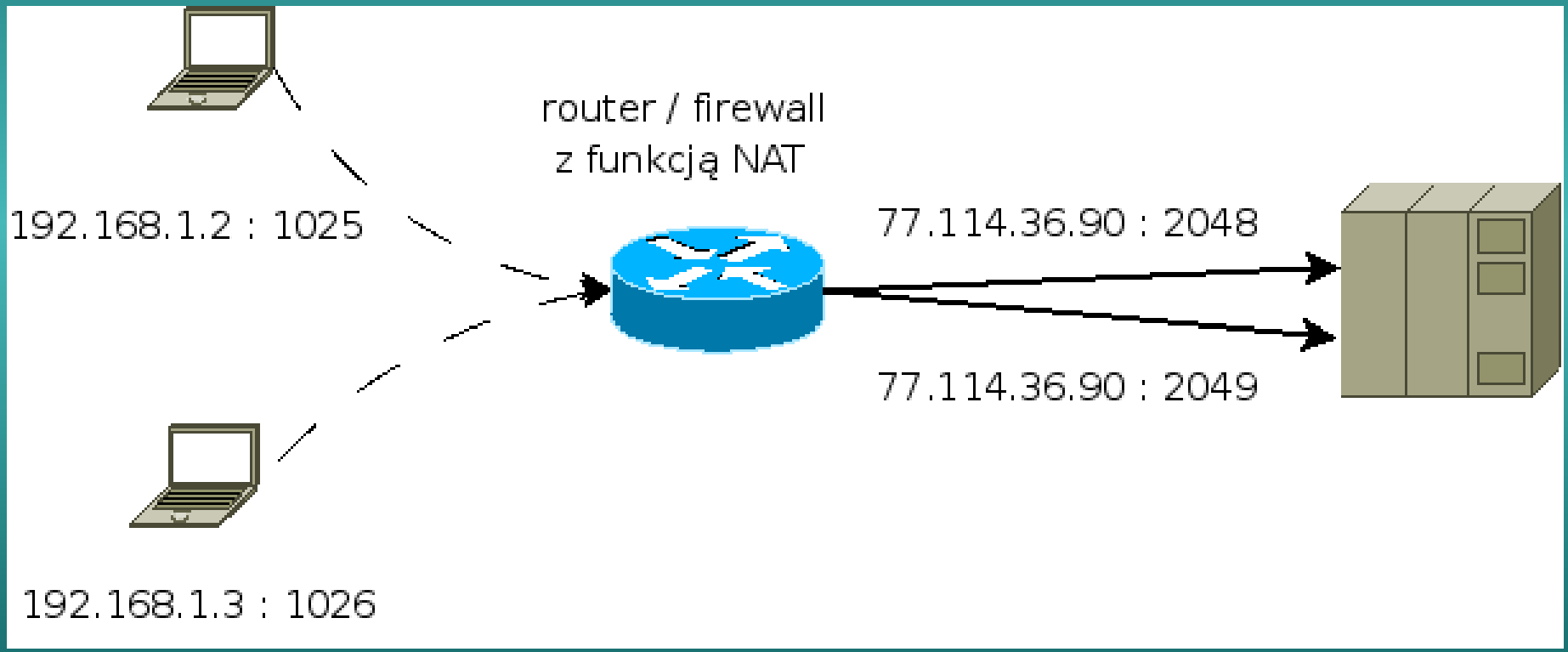
Filtrowanie pakietów (wady)

- przygotowanie bardziej rozbudowanej polityki bezpieczeństwa dla zapory nie jest łatwym zadaniem
- dodatkowe zadanie dla routera (przy kilkudziesięciu Mbps ruchu obciążenie jest już zauważalne)
- W przypadku popełnienia błędu w konfiguracji może być trudno go znaleźć

Translacja adresów

Translacja adresów – NAT (ang. Network Address Translation) pozwala na używanie innych adresów IP w sieci prywatnej, a innych w publicznej. Podstawową zaletą jest możliwość zbudowania rozległej sieci prywatnej za jednym routerem, posiadającym np. jeden publiczny adres IP.

Translacja adresów



Translacja adresów (metody)

Wyróżniamy dwie metody działania NAT:

- statyczna – dla każdego adresu sieci prywatnej przydzielony jest konkretny adres sieci publicznej
- dynamiczna – dla grupy adresów, lub dla całej sieci prywatnej przydzielony jest jeden lub więcej adres publiczny.

Translacja adresów (zalety)

- możliwość zbudowania rozległej sieci, posiadając ograniczoną ilość publicznych adresów IP.
- oszczędność publicznych klas adresowych (RIPE bardzo niechętnie rozdaje adresy IP, providerzy podobnie).

Translacja adresów (wady i problemy)

- NAT może być problemem jeśli chcemy korzystać z IPsec, ponieważ nagłówek może być szyfrowany, i/lub sprawdzana jest jego suma kontrolna.
- W przypadku bardziej skomplikowanych protokołów (np. FTP) NAT musi go rozumieć, aby prawidłowo tłumaczyć ukryte w nich adresy IP.

Systemy pośredniczące

Systemy pośredniczące są to systemy, które mają dostęp zarówno do sieci prywatnej jak i publicznej. Realizują funkcję pośredniczącą pomiędzy obiema sieciami. Nazywane są także serwerami proxy. Nie należy mylić ich z routerami.

Systemy pośredniczące

- mają bezpośredni dostęp do sieci zewnętrznej – izolują tym samym sieć prywatną
- są narażone na bezpośredni atak z zewnątrz, dlatego muszą być dobrze zabezpieczone
- umożliwiają uwierzytelnianie na poziomie użytkownika
- nie są routerami ani firewallami

Systemy pośredniczące

- działają w warstwie aplikacji
- mogą być uniwersalne (obwodowe) albo przeznaczone dla konkretnego rodzaju ruchu
- mogą buforować dane (cache serwery)
- mogą posiadać funkcję rejestracji zdarzeń, kontroli dostępu oraz wiele innych.

moduł *multiport*

Otwieramy dla świata kilka usług:

```
-A INPUT -i eth0 -p tcp -m state --state NEW --dport 22  -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW --dport 25  -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW --dport 80  -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW --dport 443 -j ACCEPT
```

Zamiast pisać 4 regułki, możemy użyć modułu *multiport* i napisać jedną:

```
-A INPUT -i eth0 -p tcp -m state --state NEW -m multiport --dports
22,25,80,443 -j ACCEPT
```

Load Balancing #1 – moduł *nth*

```
-A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m nth --
counter 0 --every 3 --packet 0 -j DNAT --to-destination 192.168.1.2:80
-A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m nth --
counter 0 --every 3 --packet 1 -j DNAT --to-destination 192.168.1.3:80
-A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m nth --
counter 0 --every 3 --packet 2 -j DNAT --to-destination 192.168.1.4:80
```

Load Balancing #2 - moduł *random*

```
-A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m random
--average 33 -j DNAT --to-destination 192.168.1.2:80
-A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m random
--average 50 -j DNAT --to-destination 192.168.1.3:80
-A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -j DNAT
--to-destination 192.168.1.4:80
```

Limitowanie ilości połączeń – moduły *connlimit, limit*

Limitowanie ilości jednoczesnych połączeń do wybranego hosta:

```
-A FORWARD -p tcp -s 0/0 --dport 80 -d 192.168.1.2 -m connlimit --
connlimit-above 600 -j REJECT
```

Limitowanie ilości połączeń do hosta w danej jednostce czasu:

```
-A FORWARD -p tcp -i eth1 -o eth0 -m multiport --dports 80,443 -m
state --state NEW -m limit --limit 60/hour --limit-burst 5 -j ACCEPT
```

Blokowanie pakietów zawierających określony ciąg znaków – moduł *string*

```
-A FORWARD -i eth0 -p tcp -m string --string 'Lepper' -j DROP
```

Blokowanie w oparciu o czas – moduł *time*

```
-A FORWARD -i eth1 -o eth0 -p tcp --dport 873 -m time --timestart
02:00 --timestop 04:00 -j ACCEPT
```

Blokowanie w oparciu o ilość przesłanych danych – moduł *quota*

```
-A FORWARD -i eth0 -o eth1 -d 192.168.1.2 -m quota --quota 2147483648
-j ACCEPT
-A FORWARD -i eth0 -o eth1 -d 192.168.1.2 -j REJECT

Monitorowanie:
iptables -v -L
```

Dziękuję za uwagę.

Pytania ?