Bezpieczeństwo w sieci. Ochrona sieciowa. Lab 04

Marcin Fabrykowski

1 czerwca 2012

Część I
Wstęp

1 Co to jest iptables?

Iptables jest programem pozwalającym na konfiguracje wbudowanego w jądro linuxa filtra pakietów. Iptables służy również do konfigurowania NAT-u.

1.1 Co to jest NAT?

Network Address Translation - system translacji adresów sieciowych. Wykorzystywany tam, gdzie nie każdy klient ma swój adres publiczny, a jedynie taki posiada. Pozwala on na komunikację komputerom za natem ze światem. Klienci za NATem posiadają swoje adresy prywatne, niewidoczne dla świata. NAT dzielimy na dwie grupy:

1. SNAT - Source NAT. Wykorzystywany, gdy chcemy żeby klient mógł połączyć się ze światem, a nie tylko z siecią lokalna. Jest to chyba najczęściej wykorzystywany NAT.
   Zasada działania: Kiedy klient próbuje wysłać pakiet w świat, wysyła on go z adresem docelowym "światowym" do routera. Tam zostaje zamieniony adres źródłowy z prywatnego klienta, na publiczny routera. Dzieje się tak dlatego, żeby host docelowy, chcąc odpowiedzieć, mógł skierować odpowiedź do routera który jest widoczny ze świata, a ten dopiero przekaże odpowiedź do klienta.

2. DNAT - Destination NAT. Rzadziej wykorzystywany. Realizuje on sytuację odwrotną. Gdy jakaś zewnętrzna stacją chce się podłączyć do komputera za NATem, nie ma takiej możliwości bez wykorzystania DNATu. Gdy przychodzi pakiet ze świata na router i zostanie on sklasyfikowany jako pakiet przeznaczony do wnętrza sieci, zostaje podmieniony adres docelowy (routera) na prywatny adres maszyny w sieci i pakiet jest wpuszczany.

2 Po co jest iptables?

Iptables pozwala na filtrowanie pakietów przychodzących, wychodzących i przechodzących przez filtrowaną maszynę. Pozwala także na modyfikowanie tych pakietów jak i ich logowanie.

3 Jak działa iptables?

Iptables analizuje każdy pakiet który przychodzi do niego. Przepuszczany jest on przez serię tablic. Schemat przejścia pakietu po tablicach, pokazuje rys. 1.

4 Dla kogo jest iptables?

1. Z poziomu zwykłego użytkownika, pozwala on zabezpieczyć nasz komputer przed niepożądanymi połączeniami przychodzącymi jak i wychodzącymi.

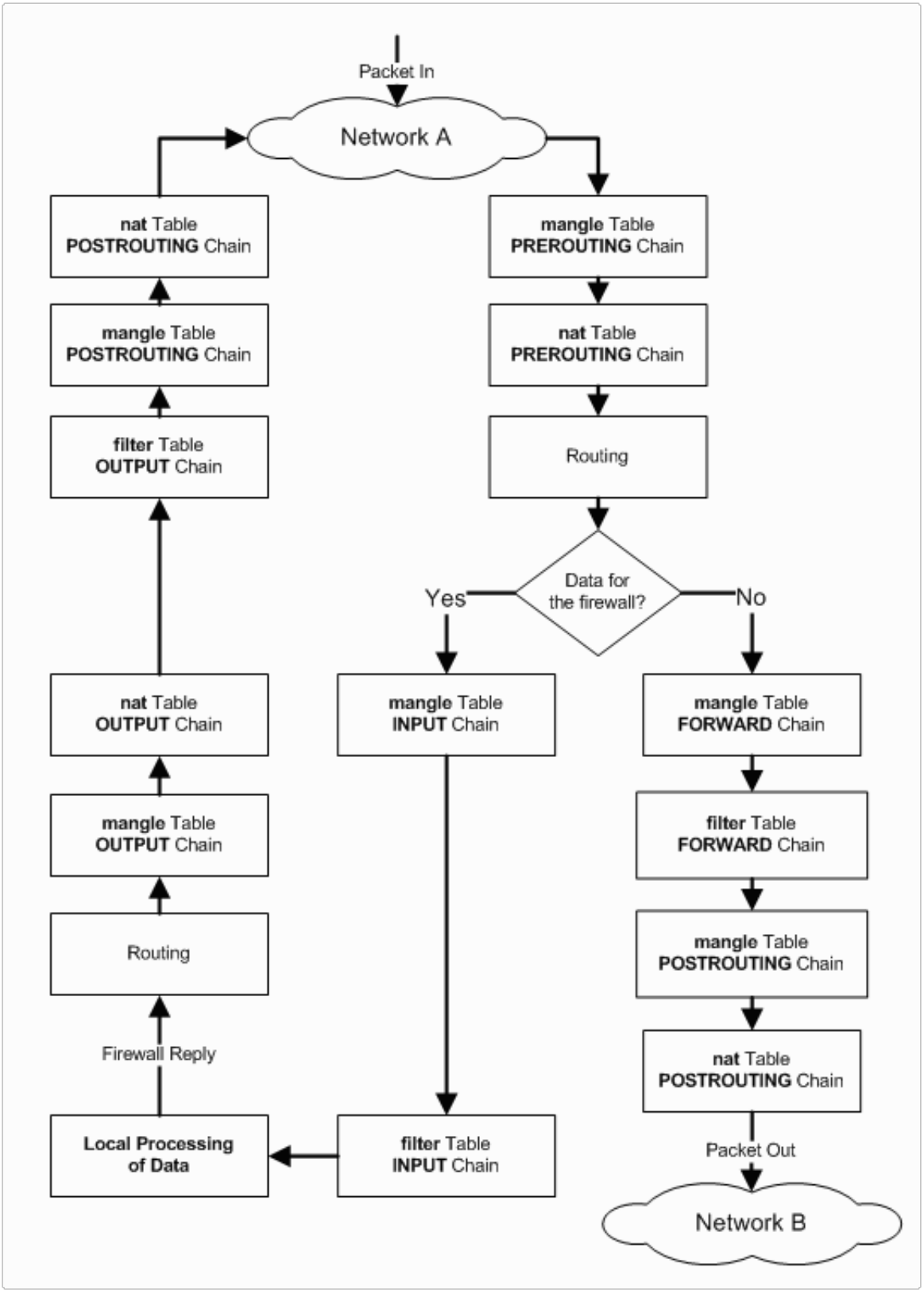
2. Z punktu widzenia administratora sieci, pozwala na ochronę serwera przed złym światem, jak również na logowanie i filtrowanie ruchu z i do sieci.

5 Co potrafi iptables?

5.1 Rozpoznawanie pakietów

Iptables potrafi dopasować pakiety wedle wielu różnych kryteriów, m.in.:

- protoków
- adres źródłowy
- adres docelowy
- interfejs wejściowy
- interfejs wyjściowy
- port źródłowy
- port docelowy
- flagi TCP
- typ ICMP
- mark
- liczbie pakietów na jednostkę czasu



Rysunek 1: Schemat przejścia pakietu po tablicach w iptables

- MAC adres
- TTL
- dzień,godzina

i wiele innych kryteriów pozwalających dokładnie określić, który pakiet należy zaakceptować a który odrzucić

5.2 Decydowanie o pakiecie

Po dopasowaniu pakietu, należy zdecydować, co z takim pakietem zrobić. Najpopularniejszymi akcjami jakie można zrobić z pakietami są:

- zaakceptować
- odrzucić
- sklasyfikować
- DNAT
- SNAT
- zalogować
- zmienić ttl

oraz wiele innych

5.3 Sekwencje wykonywania

Iptables pozwala na bardziej przejrzyste budowanie firewalla poprzez tworzenie łańcuchów z własnymi sekwencjami akcji.

5.4 Portknocking

Jest to sztuczka, polegająca na odrzucaniu pakietów przychodzących na dany port, z możliwością przepuszczania pakietu, jeżeli wcześniej została wysłana specjalna sekwencja pakietów na inne porty, tzw. *pukanie*.

5.5 Load Balancing

Inna ciekawą możliwością jest load balancing. Wykonuje się to za pomocą dopasowania *state* oraz wykorzystaniem licznika. Każde nowe połączenie jest kierowane do innego serwera z puli. W efekcie otrzymuje się zrównoważenie obciążenia redundantnych serwerów w sieci.

5.6 IPset

Zdarza się, że nasze reguły obejmują sprawdzanie czy np: ip wychodzącego pakietu należy do zarejestrowanego użytkownika czy też do nowo podpiętego. Znając listę adresów ip naszych klientów, moglibyśmy napisać po jednej regule na każdy komputer z odpowiednimi opcjami –src. Jednak takie wyjście jest czasochłonne, zaciemnia firewalla dużą liczba reguł, a dodanie bądź usunięcie klienta, wiąże się z ingerencją w reguły co bywa czasem niebezpieczne. Z pomocą przychodzą ipsety. Pozwalają stworzyć, np: bazę adresów ip naszych klientów, a w firewallu jedynie odwołać się, czy adres źródłowy pakietu znajduje się w danych ipsecie.
W takiej sytuacji dodanie bądź usunięcie klienta odbywa się tylko w ipsecie bez zmiany reguł w iptables. Dodatkowo przeszukiwanie ipseta jest wydajniejsze niż sprawdzanie wszystkich reguł w iptables.

Część II
Wykonanie ćwiczenia