



iptables

firewall w systemie Linux



Co to jest *iptables*?

- program obsługiwany z linii komend służący do konfiguracji jądra serii 2.4 oraz 2.6 pod kątem filtrowania pakietów
- przeznaczony do administratorów systemu
- ponieważ NAT (Network Address Translation) jest realizowany w oparciu o zasady filtrowania pakietów, *iptables* jest używany także do tego
- *iptables* zawiera również *ip6tables*, używany do filtrowania pakietów protokołu IP wersji 6



Historia *iptables*

- *iptables* został napisany w roku 1999 przez Rusty'ego Russela w języku C
- jest uważany za następcę *ipchains*
- współpraca Rusty'ego z Markiem Boucherem zaowocowała śmiercią projektu *ipnatctl* (oddzielnego narzędzia do konfiguracji NAT) oraz narodzinami bardziej uniwersalnego zestawu *iptables_{filter,nat,mangle}*
- przyłączenie się do projektu Jamesa Morrisa było przyczyną ukierunkowania wysiłków w celu uczynienia z *iptables* części jądra 2.4
- w kolejnych latach *core-team* powiększał się o kolejnych członków
- aktualni aktywni członkowie: Harald Welte (leader), Jozsef Kadlecsik, Martin Josefsson, Patrick McHardy, Yasuyuki Kozakai



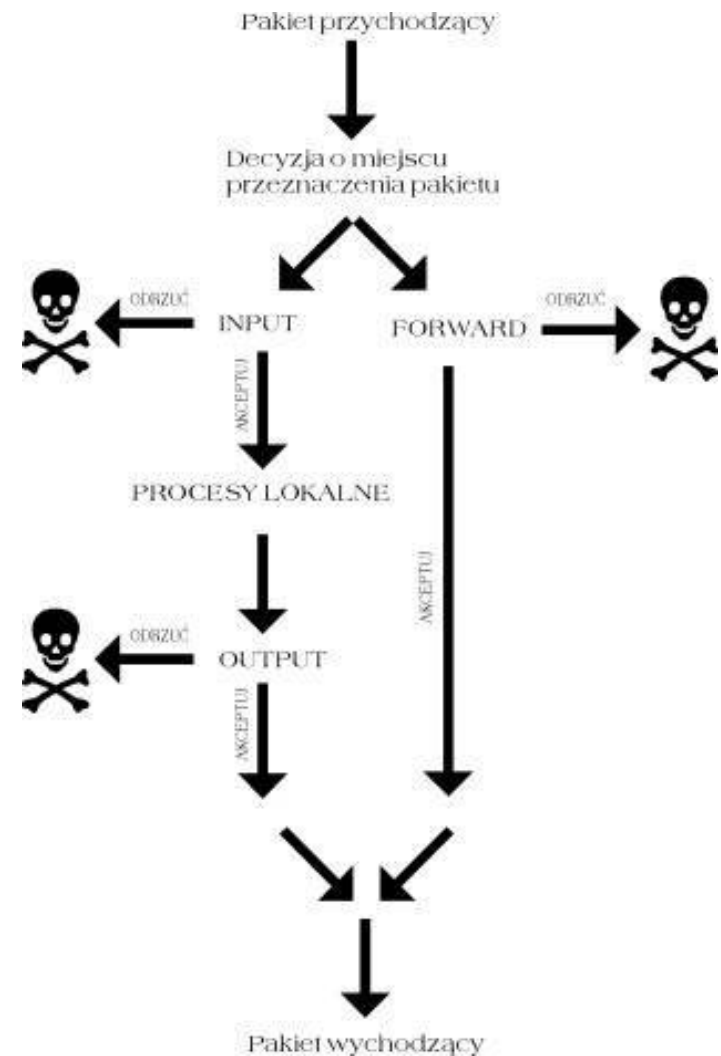
Główne „ficzery” *iptables* ;-)

- program działający w linii komend
- listowanie zawartości zbioru reguł filtrowania pakietów
- dodawanie, usuwanie, modyfikowanie reguł
- listowanie, zerowanie liczników poszczególnych reguł



Zasada działania:

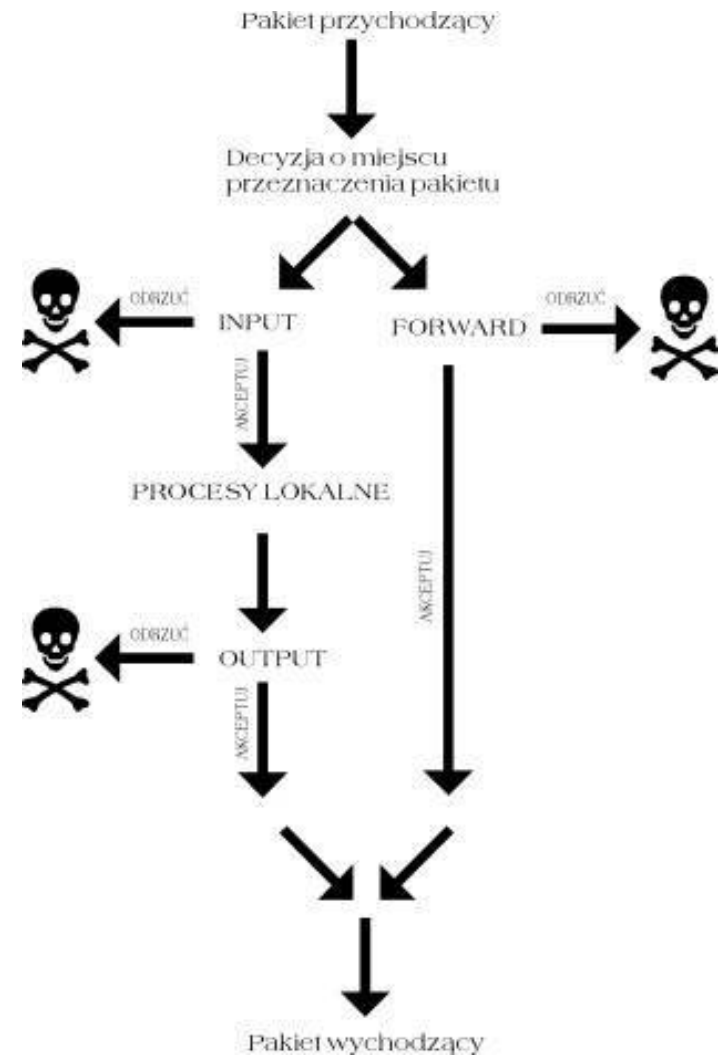
- jądro zaczyna pracę z trzema predefiniowanymi listami reguł:
 - INPUT
 - OUTPUT
 - FORWARD
- każdy pakiet docierający do hosta jest dopasowywany do dostępnych miejsc przeznaczenia
- UWAGA: do pakietu stosowana jest pierwsza reguła z listy (przykład)





Zasada działania - INPUT:

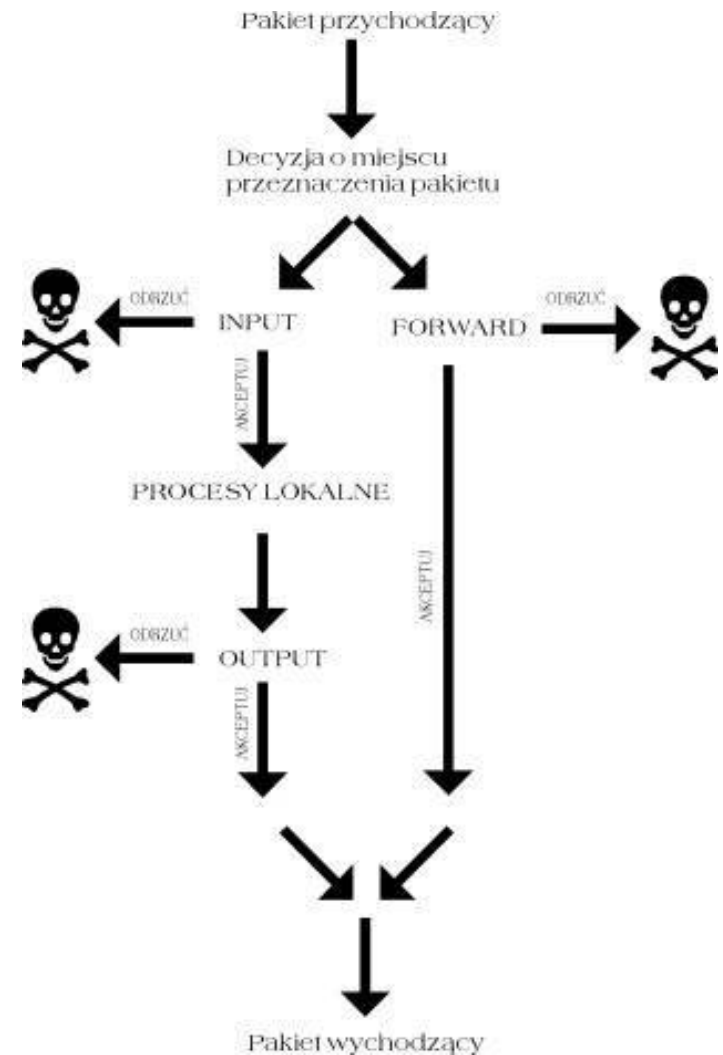
- jeśli pakiet został przystany z zewnątrz, a miejscem docelowym jest bieżący host, to zostaje przefiltrowany przez listę reguł INPUT
- jeśli pakiet pomyślnie przejdzie to filtrowanie zostanie dopuszczony do procesu, do którego jest kierowany
- w przeciwnym wypadku, zostanie odrzucony





Zasada działania - FORWARD:

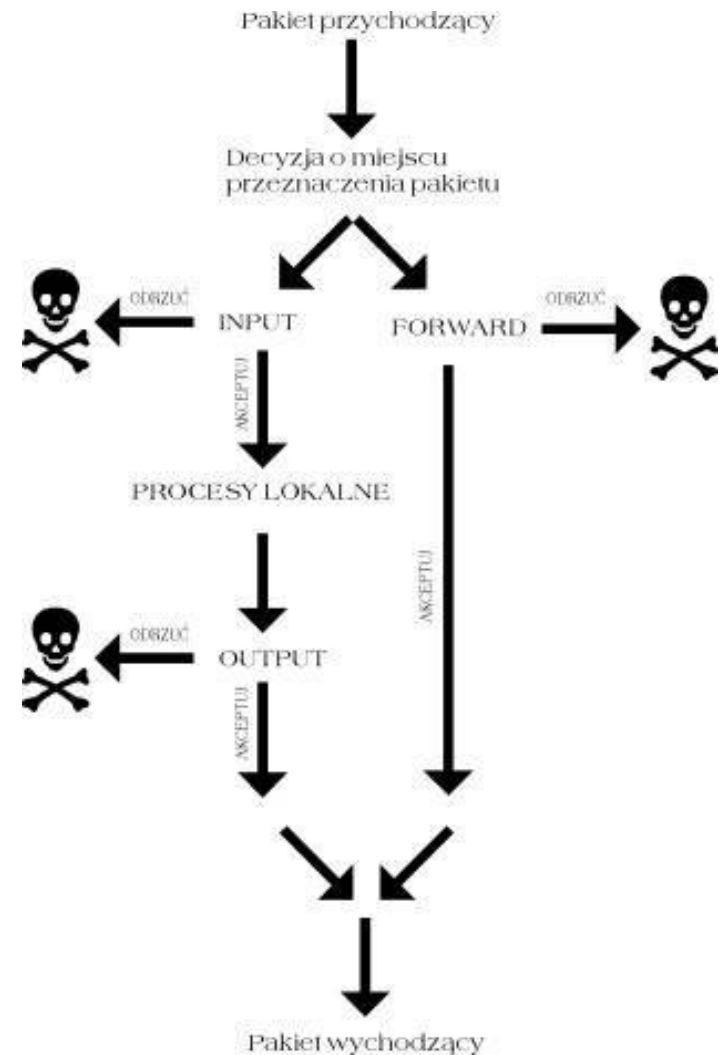
- jeśli w bieżącym systemie zostało włączone przekazywanie (*forward*) pakietów oraz pakiet jest przeznaczony dla innego interfejsu sieciowego, to zostaje poddany filtrowaniu na regułach określonych w łańcuchu FORWARD
- jeśli pakiet pomyślnie przejdzie to filtrowanie zostanie przekazany do docelowego interfejsu
- w przeciwnym wypadku, zostanie odrzucony





Zasada działania - OUTPUT:

- bieżący system może być również źródłem pakietów wychodzących - pakiety te przechodzą przez filtr OUTPUT
- jeśli pakiet pomyślnie przejdzie to filtrowanie zostanie 'wypuszczony' na świat
- w przeciwnym wypadku, zostanie odrzucony





Działania (cele) na pakietach:

- ACCEPT - akceptowanie pakietu
- DROP/DENY - odrzucenie pakietu
- REJECT - odrzucenie pakietu z powiadomieniem nadawcy
- LOG - zapisanie informacji o pakiecie w *messages*
- RETURN - powrót do łańcucha i dopasowywanie od następnej reguły
- MIRROR - wysłanie pakietu z powrotem do nadawcy
- SNAT - działanie to może być zdefiniowane tylko dla łańcucha POSTROUTING; powoduje, że zmieniany jest adres źródłowy (parametr: `--to-source`)
- MASQUERADE - podobnie jak wyżej; różnica polega na tym, że adres źródłowy jest zmieniany na adres interfejsu, do którego zostanie skierowany pakiet
- DNAT - zmiana adresu docelowego (parametr: `--to-destination`)



Backup konfiguracji *iptables*

Zrzucenie aktualnych reguł do pliku:

```
#iptables-save [-c] [-t tabela]
```

-c - zrzucenie także statystyk (liczników)

- output na stdout, przykład:

```
#iptables-save -c > /etc/backups/iptables-save
```

Odzyskanie reguł z pliku:

```
#iptables-restore [-c] [-n]
```

-n - nienadpisywanie obowiązujących reguł

- input ze stdin, przykład:

```
#cat /etc/backups/iptables-save | iptables-restore -c
```



Krótkie omówienie opcji *iptables* - operacje na łańcuchach:

- Zmiana zasady dla wbudowanego łańcucha (-P)
- Listowanie reguł w łańcuchu (-L)
- Utworzenie nowego łańcucha (-F)
- Wyczyszczenie reguł z łańcucha (-F)
- Dodanie nowej reguły do łańcucha (-A)
- Wstawienie reguły do łańcucha na określoną pozycję (-I)
- Wymiana reguły na określonej pozycji (-R)
- Skasowanie reguły (-D)
- Skasowanie pustego łańcucha (-X)
- Zerowanie liczników w łańcuchu (-Z)



Krótkie omówienie opcji *iptables* - filtrowanie:

- Użycie reguły dla konkretnego protokołu (-p)
- Określenie adresu źródłowego pakietu (-s)
- Określenie adresu docelowego pakietu (-d)
- Określenie interfejsu sieciowego (-i)
- Określenie portu źródłowego i docelowego odpowiednio (--sport i --dport)



Zaczynamy pracę!

- *netfilter* może być wkompilowany w jądro albo skompilowany w postaci modułów
- jeśli nie jest częścią jądra, należy załadować odpowiednie moduły:
 - *ip_tables*
 - *ip_conntrack*
 - *ip_table_filter*
 - *ip_table_nat* (w przypadku korzystania z NAT)



Przykłady - 1:

- zablokowanie całego ruchu wychodzącego:

```
#iptables -A INPUT -j DROP
```

```
#iptables -A FORWARD -j DROP
```

```
#iptables -A FORWARD -j ACCEPT
```

- włączamy dostęp przez SSH tylko z juliusza:

```
#iptables -A INPUT -s 158.75.2.230 -p tcp --dport 22 -j  
ACCEPT
```

- włączamy dostęp do naszego WWW dla wszystkich:

```
#iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

- wylistowanie tabeli INPUT:

```
#iptables -L INPUT
```



Przykłady - 2:

- umożliwienie pingowania naszej maszyny:

```
#iptables -A INPUT -p icmp -j ACCEPT
```

- sprawdzamy, czy ktoś nie korzysta z eDonkeya:

```
#iptables -A INPUT -p tcp --dport 4662 -j LOG
```

```
#iptables -A INPUT -p udp --dport 4662 -j LOG
```

- i uniemożliwiamy „dzielenie się” zasobami

```
#iptables -A OUTPUT -p tcp --sport 4662 -j DROP
```

```
#iptables -A OUTPUT -p udp --sport 4662 -j DROP
```

- po namyśle uznajemy, że będziemy mniej restrykcyjni, usuwamy regułę:

```
#iptables -D OUTPUT -p tcp --sport 4662 -j DROP
```

```
#iptables -D OUTPUT -p tcp --sport 4662 -j DROP
```



Przykłady - 3:

- umożliwienie logowania się przez SSH z konkretnego komputera

```
#iptables -A INPUT -s 350.450.660.808 -m mac --mac-source  
00:11:22:33:44:55 -p tcp --dport 22 -j ACCEPT
```

- zmieniamy ip w powyższej regule:

```
#iptables -R INPUT -s 850.150.660.808 -m mac --mac-source  
00:11:22:33:44:55 -p tcp --dport 22 -j ACCEPT -s  
350.450.660.808 -m mac --mac-source 00:11:22:33:44:55 --dport  
22 -j ACCEPT
```

- odrzucenie pakietów inicjujących połączenie (ustawiony bit *SYN*) z *wszystkich komputerów za wyjątkiem naszego*:

```
#iptables -A INPUT -p tcp -s !350.450.660.808 --syn -j DROP
```

- wstawiamy regułę przed powyższą:

```
#iptables -I INPUT 1 -p tcp -s 850.150.660.808 --syn -j  
ACCEPT
```



Przykłady - 4:

- tworzenie własnego łańcucha

```
#iptables -N myinput
```

- dodawanie reguł do własnego łańcucha

```
#iptables -A myinput -p tcp -s !350.450.660.808 --syn -j DROP
```

- podpięcie naszego łańcucha do łańcucha INPUT

```
#iptables -A INPUT -j myinput
```



Resources:

- Wikipedia
- <http://zlobek.tcz.wroclaw.pl/dzial.php3?dzial=28>
- <http://www.netfilter.org/>
- manpages do iptables
- <http://www.jazwiniak.com/download/firewall.pdf>