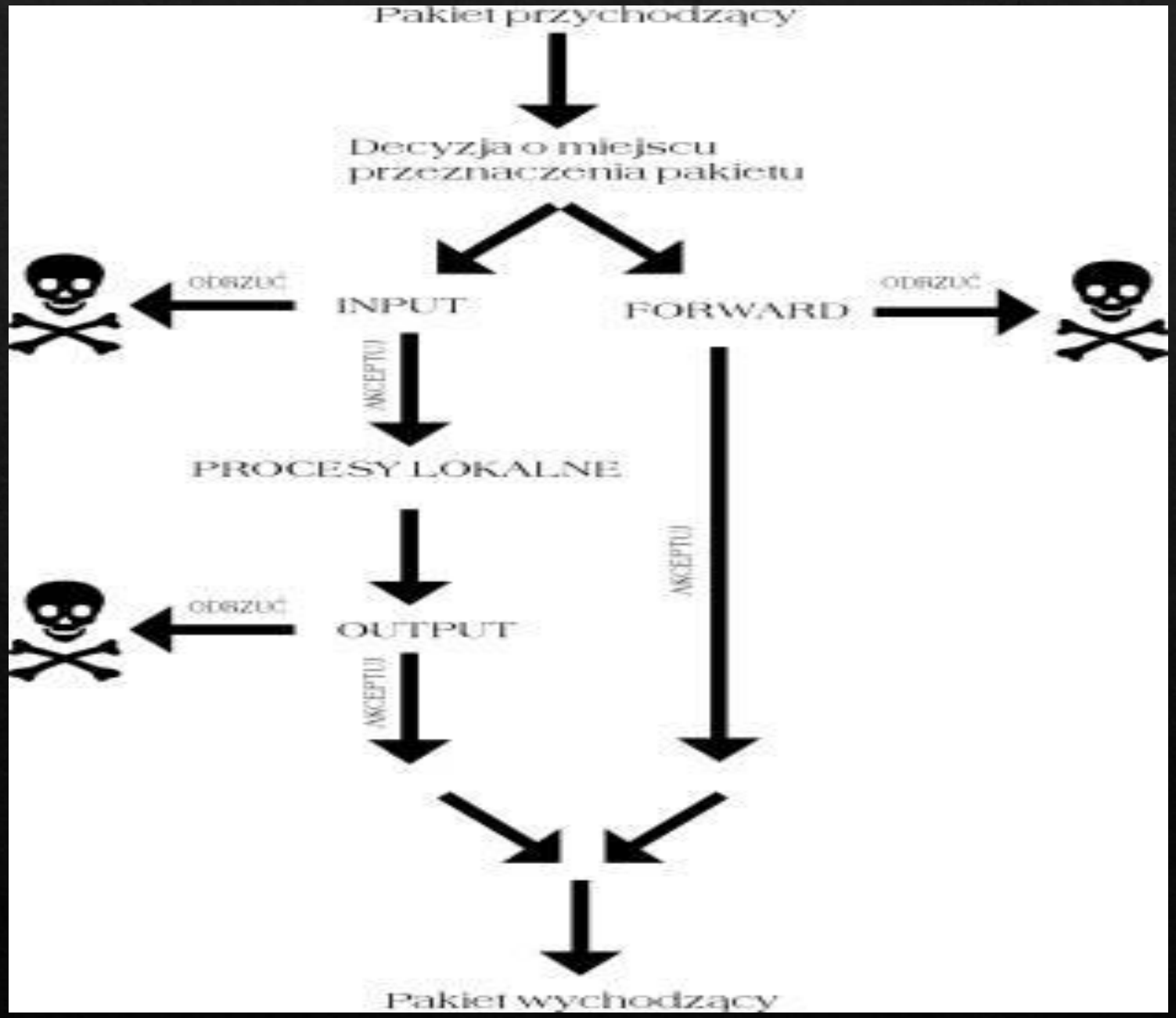
Firewall wprowadzenie

Źródła:
Wikipedia
http://www.physd.amu.edu.pl/~m_jurga/pld/firewall/
https://nsix.pl/kb/konfiguracja-iptables-na-debian/

Definicja

- Zapora sieciowa (ang. firewall – ściana ogniowa) – jeden ze sposobów zabezpieczania sieci i systemów przed intruzami.
- Termin ten może odnosić się zarówno do sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do komputera, na którego straży stoi. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz, tzn. sieci publicznych, Internetu, chroni też przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz. Często jest to komputer wyposażony w system operacyjny (np. Linux, BSD) z odpowiednim oprogramowaniem. Do jego podstawowych zadań należy filtrowanie połączeń wchodzących i wychodzących oraz tym samym odmawianie żądań dostępu uznanych za niebezpieczne.
- Najczęściej używanymi technikami obrony są:
  - filtrowanie pakietów, czyli sprawdzanie pochodzenia pakietów i akceptowanie pożądanych (np. SPI),
  - stosowanie algorytmów identyfikacji użytkownika (hasła, cyfrowe certyfikaty),
  - zabezpieczanie programów obsługujących niektóre protokoły (np. FTP, TELNET).

Model działania Firewalla



Model działania Firewalla

Jądro rozpoczyna pracę z trzema predefiniowanymi listami reguł w tabeli filtrującej.
Są to łańcuchy:
- INPUT (wejściowy),
- OUTPUT (wyjściowy)
- FORWARD (przekazujący).
Każdy pakiet docierający do hosta jest sprawdzany pod kątem miejsca przeznaczenia.
Na tej podstawie kernel decyduje, czy ma zostać przekazany do sieci położonej gdzieś dalej czy skierowany do niego samego.
Pakiet skierowany do tego komputera pozostaje "przetrawiony" przez reguły łańcucha INPUT.
Jeżeli jego obecność zostanie tu zaakceptowana, pakiet będzie dopuszczony do procesu, do którego został skierowany.
W przeciwnym wypadku zostanie odrzucony.
Jeżeli posiadasz włączone przekazywanie pakietów i pakiet jest przeznaczony dla innego interfejsu sieciowego,
pakiet przechodzi przez zestaw reguł łańcucha FORWARD. Reguły łańcucha zadecydują, czy może zostać przesłany dalej czy zostać odrzucony.
Procesu uruchamiane na naszym hoście także mogą być źródłem pakietów wydostających się do Internetu.
Takie pakiety przechodzą przez łańcuch OUTPUT. Po akceptacji docierają do interfejsu sieciowego.

Pusta tabela nie będzie zawierała żadnych reguł, ale jak można zauważyć znajdują się w niej trzy łańcuchy (INPUT, OUTPUT oraz FORWARD):

```
Chain INPUT (policy ACCEPT)
 target     prot opt source               destination
 Chain FORWARD (policy ACCEPT)
 target     prot opt source               destination
 Chain OUTPUT (policy ACCEPT)
 target     prot opt source               destination
```

Nazwy łańcuchów wskazują, do którego ruchu zostaną zastosowane reguły na każdej liście. INPUT dotyczy wszystkich połączeń przychodzących na maszynę wirtualną, OUTPUT dotyczy wszystkich połączeń wychodzących z maszyny wirtualnej, FORWARD dotyczy połączeń, które zostaną przekazane dalej. Każdy łańcuch ma również swoje ustawienie zasad (policy), które określają sposób obsługi ruchu. Jeżeli nie pasuje do żadnych określonych reguł, domyślnie jest ustawiony na akceptację (ACCEPT).

Podstawowe operacje na łańcuchach.

-P - zmiana zasady dla wbudowanego łańcucha
-L - listowanie reguł w łańcuchu
-F - wyczyszczenie reguł z łańcucha
-A - dodanie nowej reguły do łańcucha
-I - wstawienie reguły do łańcucha na określoną pozycję
-R - wymiana reguły na określonej pozycji
-D - skasowanie reguły
-X - skasowanie pustego łańcucha
-Z - zerowanie liczników w łańcuchu

Opcje filtrowania.

-p -użycie reguły dla konkretnego protokołu
-s -określenie adresu źródłowego pakietu
-d -określenie adresu docelowego pakietu
-i -określenie interfejsu sieciowego
--sport -określenie portu źródłowego
--dport -określenie portu docelowego
-j - określa co należy wykonać z pakietem pasującym do reguły

Możliwe stany dla –j to:

DENY
ACCEPT
DROP
RETURN

[Uwaga: Wielkość liter ma znaczenie!!!]

dodawanie reguł iptables:

Zapory można zazwyczaj konfigurować na jeden z dwóch sposobów: albo ustawić domyślną regułę na akceptowanie, a następnie blokować niepożądany ruch za pomocą określonych reguł, albo za pomocą reguł definiować dozwolony ruch i blokować wszystko inne. Ta ostatnia jest często zalecana, ponieważ pozwala na prewencyjne blokowanie ruchu, zamiast konieczności reaktywnego odrzucania połączeń, które nie powinny próbować uzyskać dostępu do maszyny wirtualnej.

Aby rozpocząć korzystanie z iptables, należy najpierw dodać reguły dla dozwolonego ruchu przychodzącego dla potrzebnych usług. Iptables może śledzić stan połączenia. Aby dodać regułę dla połączeń nawiązanych, należy użyć poniższego polecenia:

```
# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

Można teraz sprawdzić, czy reguła została dodana w tabeli przy użyciu polecenia jak poprzednio:

```
# iptables -L
```

Aby to wyjaśnić posłużymy się konkretnym przykładem. Chcemy, aby nasz firewall udostępniał innym serwer ftp.
Najprościej zrobić to tak:
#iptables –A INPUT –p tcp --dport 20:21 –j ACCEPT
Na przykład usługa SSH działa na porcie 5244/tcp. Należy więc dodać regułę z tym numerem portu poleceniem:
iptables -A INPUT -p tcp --dport 5244 -j ACCEPT
Jeżeli na maszynie wirtualnej działają popularne usługi takie jak http, https również należy dodać regułę pozwalająca na ruch przychodzący dla tych usług:
otworzenie http na porcie 80:
iptables -I INPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
otworzenie https na porcie 443:
iptables -I INPUT -p tcp --dport 443 -m state --state NEW -j ACCEPT
Blokowanie strony:
iptables -A FORWARD -p tcp --destination www.sejm.gov.pl -j DROP
Jeśli chcesz blokować połączenia wyjściowe z komputera, który nie jest ruterem, to zamiast FORWARD daj OUTPUT
Ten przykład pokazuje, jak blokować połączenia SSH od 10.10.10.10.
iptables -A INPUT -p tcp --dport ssh -s 10.10.10.10 -j DROP
Możesz zastąpić "ssh" dowolnym protokołem lub numerem portu. The -p tcp część kodu informuje iptables, jakiego rodzaju połączenia używa protokół. Jeśli blokowałeś protokół używający UDP zamiast TCP, to -p udp byłoby konieczne zamiast tego.
Ten przykład pokazuje, jak blokować połączenia SSH z dowolnego adresu IP.
iptables -A INPUT -p tcp --dport ssh -j DROP

Aby zezwolić na ruch sieciowy HTTP, wprowadź następujące polecenie:
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
Aby zezwolić tylko na ruch przychodzący przez SSH (Secure Shell), wprowadź:
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
Aby zezwolić na ruch internetowy HTTPS, wprowadź następujące polecenie:
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

kontrola ruchu na adres IP

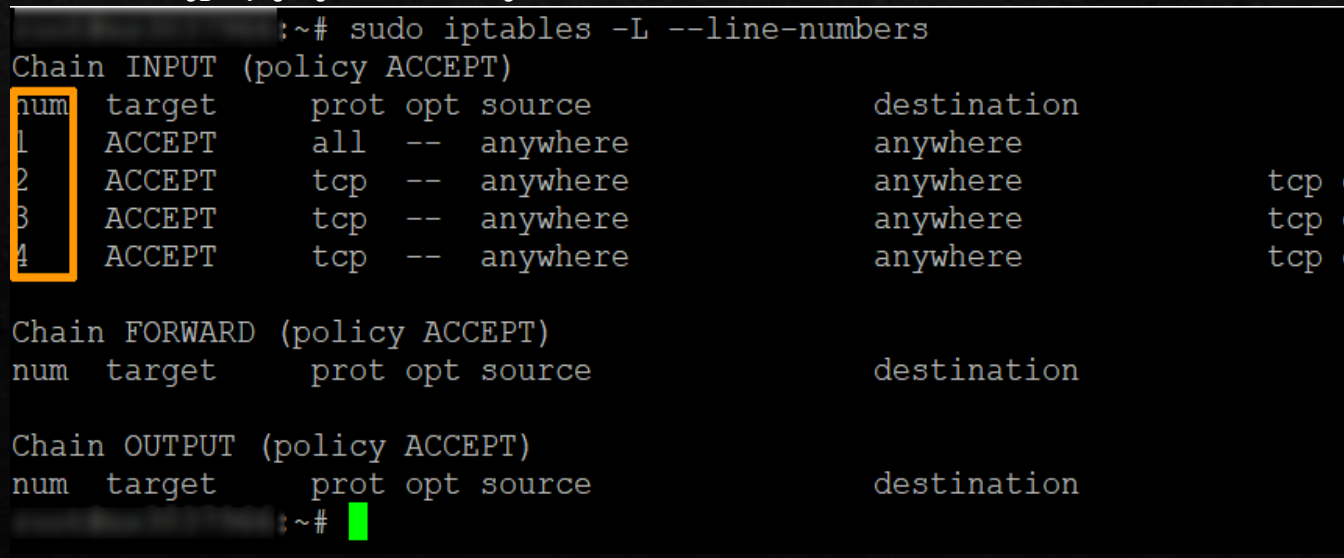
Aby zaakceptować ruch z określonego adresu IP, użyj następującego polecenia.
sudo iptables -A INPUT -s adres_IP_do_autoryzacji -j ACCEPT
Zastąp adres IP w zamówieniu adresem IP, który chcesz autoryzować.
Możesz również zablokować ruch z adresu IP
sudo iptables -A INPUT -s adres_IP_do_blokowania -j DROP
Zastąp adres IP w zamówieniu adresem IP, który chcesz zablokować.
Możesz odrzucić ruch z zakresu adresów IP, używając następującego polecenia:
sudo iptables -A INPUT -m iprange --src-range adres_IP_początku_adresu_IP_fin -j REJECT
Opcje iptables, których używaliśmy w przykładach działają następująco:
-m : Odpowiada określonej opcji.
-iprange: Wskazuje, że system będzie czekać na określony zakres adresów IP zamiast na jeden.
—src-range: Określa zakres adresów IP.

usuń niepożądany ruch

Jeśli określisz reguły firewalla iptables, musisz zapobiec nieautoryzowanemu dostępowi poprzez usunięcie wszelkiego ruchu z innych portów:
sudo iptables -A INPUT -j DROP
Opcja -A dodaje nową regułę do łańcucha. Jeśli połączenie przechodzi przez porty inne niż te, które zdefiniowałeś, zostanie ono przerwane.

usuń regułę

Bardziej precyzyjna metoda polega na usunięciu numeru linii z reguły.
sudo iptables -P INPUT DROP
Po pierwsze, wprowadź wszystkie reguły:
sudo iptables -L --line-numbers
Wyszukaj wiersz reguły firewalla, którą chcesz usunąć i wprowadź następującą komendę:
sudo iptables -D INPUT <Number>
Zastąp Number numerem linii reguły, którą chcesz usunąć.



zapisz zmiany

Podczas restartu systemu, iptables nie zachowuje reguł, które utworzyłeś. Za każdym razem, gdy skonfigurujesz iptables w Linuxie, wszystkie wprowadzone przez Ciebie zmiany dotyczą tylko do kolejnego restartu.

Aby zarejestrować reguły w systemach opartych na Ubuntu, wprowadź:

sudo -s iptables-save -c

Zadanie do wykonania na lekcji:
Zablokuj możliwość pingowania(zablokuj port)
Zablokuj wejścia na stronę www.dacia.pl
Zablokuj adres ip 212.77.98.9 ->wp.pl