Konfiguracja firewall'a

1. Firewall

Firewall - (z ang. ściana ogniowa) - rodzaj oprogramowania lub dedykowany sprzęt do zabezpieczenia komputer/sieci przed niepowołanym dostępem

2. Podstawowa konfiguracja

Najpopularniejszym filtrem sieciowym dla systmu Linux jest iptables. W dalszej części pokażemy podstawową konfigurację dla systemu operacyjnego Linux z zainstalownym systemem eDokumenty:

```
iptables -F INPUT
iptables -F FORWARD
iptables -P INPUT DROP
iptables -P FORWARD DROP

iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT
for PORT in 22 25 80 443 6000
do
   iptables -A INPUT -p tcp -m state --state NEW --dport $PORT -j ACCEPT
done
```

Przeanalizujmy wpisy.

Pierwsze dwie wpisy czyszczą łańcuchy z reguł. Łańcuch INPUT filtruje ruch kierowany do tego komputera. Domyślnie mamy jeszcze wbudowane 2 łańcuchy OUTPUT - ruch wychodzący, FORWARD - ruch przekazywany.

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
```

Powyższe wpisy ustawiają domyślną politykę dla łańcuchów INPUT i FORWARD na DROP czyli odrzuć. Domyślna polityka to zachowanie firewalla dla przypadku, w którym pakiet nie został zakwalifikowany do żadnej reguły danego łańcucha.

```
iptables -A INPUT -i lo -j ACCEPT
```

Reguła zezwalająca na ruch w obrębie interfejsu loopback. Loopback to adres komputera lokalnego, interfejs z adresem 127.0.0.1 nie zbędny do komunikacji wewnątrz jedengo hosta.

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Reguła przedstawiona powyżej wykorzystuje rozszerzenie *state* do filtrowania ruch przychodzącego na podstawie stanu połączenia. Zgodnie z tą regułą akceptowane będą tylko pakiety z nawiązanym juz połączeniem (ESTABLISHED) i należace do danego połączenia oraz pakiety z nawiąznym juz połączeniem ale nie wiążące się już z istniejącym połączeniem (RELATED).

```
iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT
```

Powyższa reguła akceptuje pakiety icmp (popularny ping wysyła właśnie tego typu pakiety). Akceptowane są tylko pakiety icmp typu czyli Echo Request (żądanie echa). Jest to prośba o odpowiedź czy host jest w sieci. W odpoiedzi komputer wysyła icmp typu 0 czyli Echo Reply (zwrot echa). Brak odpowiedzi nie oznacza że hosta nie ma w sieci. Popularny komercyjny system ooperacyjny domyślnie blokuje żądanie echa.

```
for PORT in 22 25 80 443 6000
do
   iptables -A INPUT -p tcp -m state --state NEW --dport $PORT -j ACCEPT
done
```

Powyższy kawałek kody to pętla wpisująca do firewall'a kolejno dla poszczególnych usług reguły zezawalającę na dostęp do nich. Te usługi to:

port 22 - SSH (ang. secure shell) - zdalny dostęp do systemu w trybie tekstowym

port 25 - smtp (ang. Simple Mail Transfer Protocol) - protokół wykorzystywany do wysyłania poczty

port 80 - http (ang. Hypertext Transfer Protocol) - popularne www, strony internetowe

port 443 - https (ang. HyperText Transfer Protocol Secure) - szyfrowane www, wykorzystywane m.in. przy połączeniach z bankami

port 6000 - X Window System - zdalny dostęp do systemu w trybie graficznym.