

Konfiguracja firewall'a

1. Firewall

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

2. Podstawowa konfiguracja

Najpopularniejszym filtrem sieciowym dla systemu Linux jest iptables. W dalszej części pokażemy podstawową konfigurację dla systemu operacyjnego Linux z zainstalowanym 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
```

Przeanalizujemy 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 odrzucić. 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 jednego hosta.