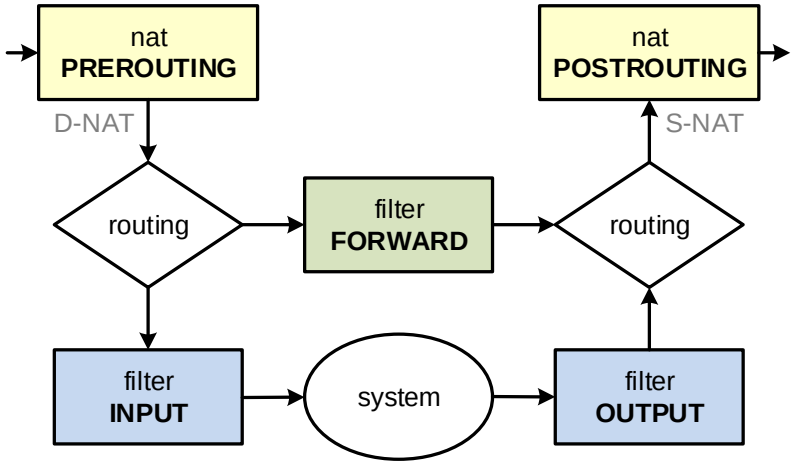
Filtracja datagramów

Celem ćwiczenia jest zdobycie umiejętności konfiguracji filtracji datagramów i budowy zapory sieciowej. Ćwiczenie będzie realizowane w SO Linux w wersji Live DVD - Knoppix.

Ćwiczenie należy wykonać w dwuosobowych grupach. Numerem grupy jest parzysty numer komputera podzielony przez dwa.

1. Trasy datagramów



2. Przykładowa zapora sieciowa dla stacji roboczej z SO Linux

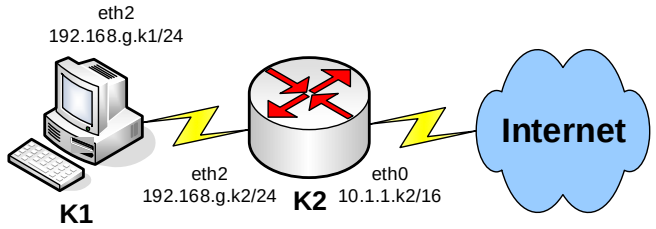
```
#wyczyszczenie wszystkich poprzednich reguł
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
#ustalenie domyślnych polityk
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
#zezwalamy na ruch lokalny loopback i odpowiedzi na wysłane żądania
iptables -A INPUT -j ACCEPT -i lo
iptables -A INPUT -j ACCEPT -m state --state ESTABLISHED,RELATED
#przykładowe wyjątki – zgoda na przychodzące żądanie echa (ping) i ssh
iptables -A INPUT -j ACCEPT -p icmp --icmp-type echo-request
iptables -A INPUT -j ACCEPT –p tcp --dport 22 -m state --state NEW
#przykładowe blokady – różnica w działaniu REJECT i DROP
iptables -A OUTPUT -j REJECT -d www.pg.edu.pl -p tcp --dport 80
iptables -A OUTPUT -j DROP -d student.eti.pg.gda.pl -p tcp --dport 80
```

3. Translacja adresów NAT i portów PAT

```
#SNAT – translacja adresów źródłowych – udostępnianie połączenia sieciowego
iptables –t nat –A POSTROUTING –s 192.168.12.0/24 –o eth0 –j MASQUERADE
#albo zamiast –j MASQUERADE można użyć -j SNAT --to-source 10.1.1.22
#DNAT – translacja adresów docelowych – przekierowanie portów – serwery wirtualne
iptables -t nat -A PREROUTING –i eth0 -p tcp --dport 8080 -j DNAT --to 192.168.12.13:80
```


POLITECHNIKA GDAŃSKA
Firewall - laboratorium

4. Zapora dla routera



Zadania dla stacji roboczej:

1. Wyłączyć interfejs eth0
2. Skonfigurować interfejs eth2 192.168.g.k1/24
3. Skonfigurować routing domyślny przez router 192.168.g.k2
4. Udostępnić dostęp zdalny przez ssh
5. Skontrolować dostęp do Internetu, routera, komputerów w sąsiednich grupach

Zadania dla routera:

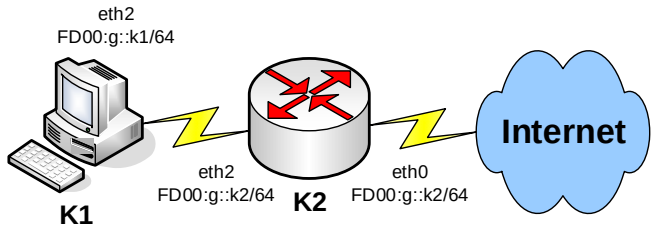
1. Skonfigurować interfejs eth2 192.168.g.k2/24
2. Udostępnić połączenie internetowe dla komputerów z sieci 192.168.g.0/24 (SNAT albo MASQUERADE)
3. Zapewnić dostęp do usługi ssh na komputerze 192.168.g.k1 (DNAT)
4. Zabronić komputerom z sieci 192.168.g.0/24 dostępu do wybranych serwisów internetowych
5. Udostępnić dostęp zdalny do routera przez ssh wyłącznie z sieci wewnętrznej 192.168.g.0/24

Uwaga! Nie wolno zmienić polityk firewalla ani na routerze, ani na stacji klienckiej!

Podpowiedź – uruchomienie przekazywania datagramów (routingu) IPv4:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
#albo sysctl –w net.ipv4.ip_forward=1
```

5. Zadania dodatkowe



Uzupełnić konfigurację o analogiczną do pkt. 2 i pkt. 4 filtrację datagramów IPv6.

```
ip6tables
```

Aby zapewnić poprawne działanie mechanizmu Neighbour Discovery dla IPv6 należy pamiętać o dodatkowych regułach dla ip6tables:

```
ip6tables -A INPUT -j ACCEPT -p icmpv6 --icmpv6-type neighbour-advertisement
ip6tables -A INPUT -j ACCEPT -p icmpv6 --icmpv6-type neighbour-solicitation
ip6tables -A INPUT -j ACCEPT -p icmpv6 --icmpv6-type router-advertisement
ip6tables -A INPUT -j ACCEPT -p icmpv6 --icmpv6-type router-solicitation
```

Podpowiedź – uruchomienie przekazywania datagramów (routingu) IPv6:

```
echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
#albo sysctl –w net.ipv6.conf.all.forwarding=1
```