## IPTABLES – konfiguracja routingu i zapory

**T: Instalacja i konfigurowanie firewalla (iptables).**

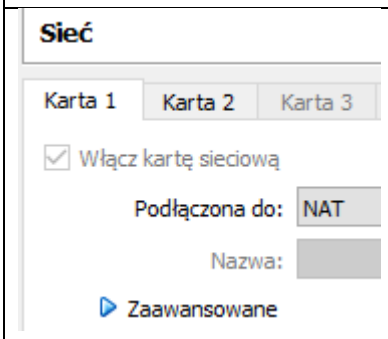
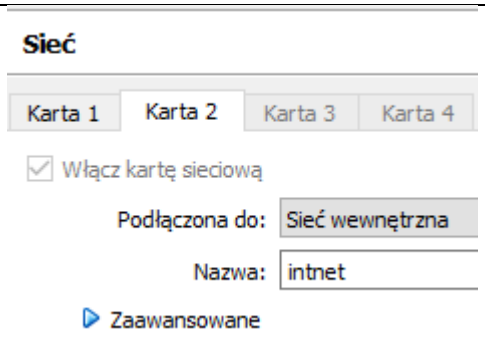
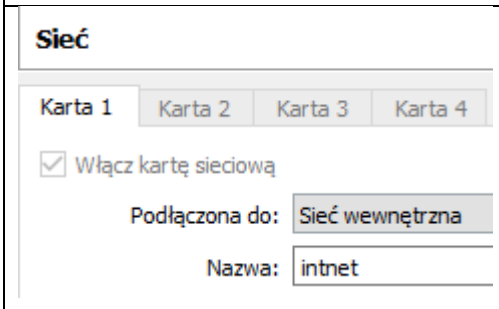
Podczas wykonywania poniższych zadań w zeszycie w sprawozdaniu

1. podaj i wyjaśnij polecenia które użyjesz aby:
   - wyjaśnić pojęcia związane z iptables,
   - zainstalować iptables,
   - uruchomić lub zatrzymać iptables,
   - konfigurować iptables,
   - korzystać z iptables.
2. podaj odpowiedzi na pytania zadane w treści zadań.

Do ćwiczenia potrzebna jest nowa (czysta) instalacja Ubuntu serwer i klient. Przygotuj Ubuntu.

Do ćwiczenia potrzebna jest nowa (czysta) instalacja Windows. Przygotuj Windows.

Przed przystąpieniem do ćwiczenia sprawdź czy ustawienie maszyny wirtualnej pozwala na dostęp do Internetu, jeżeli ustawienia są niezgodne wykonaj konfigurację pierwszej i drugiej karty sieciowej według instrukcji, a następnie uruchom Ubuntu.

| Ubuntu serwer Adapter 1 | Ubuntu serwer Adapter 2 |
|---|---|
|  |  |
| **Windows Adapter 1** | |
|  | |

Po uruchomieniu Ubuntu podaj **login**: ubuntu **Password**: 1234

Wisz sudo -s **Password**: 1234

```
ubuntu@dlp:~$ sudo -s
[sudo] password for ubuntu:
```

**Przygotowanie do ćwiczenia**. Przywróć migawkę z ustawieniami sieci jak poniżej lub wykonaj poniższe ustawienie adresu dynamicznego przydzielanego z NAT i statycznego adresu IP.

1. Za pomocą polecenia ifconfig -a ustal dostępne interfejsy sieciowe.

```
root@dlp:~# ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe68:a08  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:68:0a:08  txqueuelen 1000  (Ethernet)
        RX packets 2712  bytes 2450820 (2.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1142  bytes 77401 (77.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

Plik /etc/netplan/01-netcfg.yaml - opisuje interfejsy sieciowe dostępne w systemie i jak je aktywować.

2. Zmień adres IP dla Ubuntu na enp0s8 (Adapter 2) na statyczny.

Otwórz plik, który opisuje interfejsy sieciowe nano /etc/netplan/01-netcfg.yaml

Pozostaw zalecane wpisy w tym pliku

```
 GNU nano 2.9.3                        /etc/netplan/01-netcfg.yaml

# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: yes
    enp0s8:
      dhcp4: no
      addresses: [10.0.0.30/24]
```

3. Zastosuj ustawienia

root@dlp:~# netplan apply

```
root@dlp:/# netplan apply
```

4. Wyświetl domyślną bramę (adres rutera) dla interfejsów sieciowych serwera

```
root@dlp:~# ip route show default
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
```

Jeżeli jeszcze nie masz wykonaj migawkę z skonfigurowanymi interfejsami sieciowymi a będzie łatwiej kolejnym razem.

Opisz w zeszycie:

- procedurę instalacji i konfiguracji oraz uruchomienia iptables,
- testowania uruchomionego iptables,

Zakładam, że interfejsy sieciowe są skonfigurowane jak w poprzednich ćwiczeniach (eth0 - net eth1 - lan).

Zapisz w zeszycie co się stało po wykonaniu poleceń. Wpisz kolejno polecenia. Wydaj polecenie:

**iptables -L**

dowiedziesz się, jakie reguły zostały wprowadzone do systemu.

Na zrzucie poniżej przedstawiłem oczekiwany wynik działania polecenia.

```
root@dlp:~# iptables -L
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
```

Jak widać żadnych reguł jeszcze nie wprowadzono. Wykonaj prostą konfigurację, dzięki której możliwy będzie routing na konfigurowanym serwerze. Dodatkowo dodaj przekierowania dla konkretnych adresów IP i domen oraz zezwól/zabroń dostępu do konkretnych usług zainstalowanych na serwerze.

W celu prostej konfiguracji i rozbudowy skryptów utwórz plik:

**/etc/router**

w którym wpisz kolejne reguły dla poszczególnych usług. Wpisane reguły obowiązują tak długo, jak długo uruchomiony jest serwer lub do czasu ich wyczyszczenia z tablicy.
Z tego powodu pierwszą regułą w pliku /etc/router powinno być wyczyszczenie wszystkich reguł.
Wyczyszczenie reguł następuje poprzez podanie parametru -F.

**iptables -F**

**iptables -t nat -F**

powyższe instrukcje wyczyszczą reguły z tabel filter (tabela domyślna) oraz nat.
Umieszczenie powyższych poleceń na początku pliku /etc/router da pewność, że tablica zostaną wyczyszczone przed dodaniem nowych wpisów. Dobrym zwyczajem jest dodanie na początku również wpisów blokujących całkowicie ruch wchodzący, wychodzący oraz routing.
Dzięki takiemu rozwiązaniu będziesz mógł udostępnić wyłącznie te usługi, które chcemy – reszta zostanie zablokowana. Zablokowanie dostępu dla wszystkich pakietów uzyskamy wpisując:

**iptables -P INPUT DROP**

**iptables -P OUTPUT DROP**

**iptables -P FORWARD DROP**

Wykonaj

```
root@dlp:~# chmod +x /etc/router
root@dlp:~# ls -la /etc/router
-rwxr-xr-x 1 root root 104 Mar 30 15:43 /etc/router
```

Wykonaj `root@dlp:/etc# ./router`

W tym momencie wszystkie pakiety przychodzące na serwer zostaną odrzucone (łańcuch INPUT), wszystkie pakiety wychodzące z serwera (łańcuch OUTPUT) zostaną odrzucone oraz wszystkie pakiety, które powinny być routowane zostaną odrzucone (łańcuch FORWARD).
W tym momencie masz przygotowany grunt do utworzenia niezbędnych regułek.
Sprawdź, czy rzeczywiście ograniczyłeś dostęp do serwera. Z pozycji Windows 10 parametry interfejsu sieciowego w Windows

| | |
|---|---|
| DHCP włączone | Nie |
| Adres IPv4 | 10.0.0.31 |
| Maska podsieci IPv4 | 255.255.255.0 |

wykonaj „pingowanie”.

**ping 10.0.0.30**

W efekcie otrzymasz komunikat, że upłynął limit czasu żądania. Na poniższym zrzucie pokazano efekt działania polecenia ping z systemu Windows 10.

```
C:\Users\admin>ping 10.0.0.30

Badanie 10.0.0.30 z 32 bajtami danych:
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.

Statystyka badania ping dla 10.0.0.30:
    Pakiety: Wysłane = 4, Odebrane = 0, Utracone = 4
             (100% straty),
```

Wykonaj z serwera **ping 10.0.0.301**

```
root@dlp:/etc# ping 10.0.0.31
PING 10.0.0.31 (10.0.0.31) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 10.0.0.31 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2063ms
```

Jak widać serwer nie odpowiada na komunikaty echa (ICMP), ponieważ w regułach wpisałeś, że wszystkie pakiety ma odrzucać. Dodaj wpisy reguł, które umożliwią odpowiadanie na pingi.

**iptables -A INPUT -p ICMP -j ACCEPT**

**iptables -A OUTPUT -p ICMP -j ACCEPT**

Komunikaty echa, to pakiety, które trzeba odebrać i odesłać, dlatego należy dodać wpis zarówno do łańcucha wejściowego jak również do łańcucha wyjściowego. Poszczególne fragmenty wpisów oznaczają:

-A INPUT – dodanie wpisu do łańcucha wejściowego (może być OUTPUT, FORWARD),

-p ICMP – protokół, którego dotyczy wpis (może być TCP, UDP),

-j ACCEPT – co zrobić z pakietem (zaakceptować, DROP odrzucić, REJECT odrzucić z powiadomieniem nadawcy).

Wykonaj

```
root@dlp:/etc# ./router
```

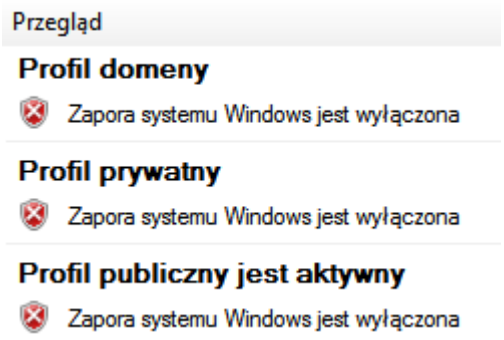
Poniżej potwierdzenie prawidłowego działania reguł ICMP:

```
C:\Users\admin>ping 10.0.0.30

Badanie 10.0.0.30 z 32 bajtami danych:
Odpowiedź z 10.0.0.30: bajtów=32 czas<1 ms TTL=64
Odpowiedź z 10.0.0.30: bajtów=32 czas<1 ms TTL=64
Odpowiedź z 10.0.0.30: bajtów=32 czas=1ms TTL=64
Odpowiedź z 10.0.0.30: bajtów=32 czas<1 ms TTL=64

Statystyki badania ping dla 10.0.0.30:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
             (0% straty),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 0 ms, Maksimum = 1 ms, Czas średni = 0 ms
```

Wyłącz zapory




Wykonaj test z serwera

```
root@dlp:/etc# ping 10.0.0.31 -c4
PING 10.0.0.31 (10.0.0.31) 56(84) bytes of data.
64 bytes from 10.0.0.31: icmp_seq=1 ttl=128 time=0.286 ms
64 bytes from 10.0.0.31: icmp_seq=2 ttl=128 time=0.534 ms
64 bytes from 10.0.0.31: icmp_seq=3 ttl=128 time=0.710 ms
64 bytes from 10.0.0.31: icmp_seq=4 ttl=128 time=0.803 ms

--- 10.0.0.31 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.286/0.583/0.803/0.197 ms
```

W analogiczny sposób skonfiguruj dostęp do serwera HTTP zainstalowanego na serwerze.

**iptables -A INPUT -p TCP --dport http -j ACCEPT**

W tym momencie pojawia się problem... Dodanie analogicznego wpisu dla strumienia wyjściowego nie spowoduje prawidłowego funkcjonowania usługi. Związane jest to z faktem, że serwer nasłuchuje na porcie 80, ale transmisja odbywa się z wykorzystaniem innego uzgodnionego portu. Ta sama sytuacja dotyczy innych usług. Najprostszym rozwiązaniem jest umożliwienie ruchu wyjściowego dla wszystkich portów i zablokowanie tylko wybranych.
Należy zmienić wpis:

**iptables -P OUTPUT DROP**

na

**iptables -P OUTPUT ACCEPT**

Po tej modyfikacji serwer będzie odpowiadał na zapytania HTTP.
Dodamy jeszcze jeden analogiczny wpis dla protokołu SSH:

**iptables -A INPUT -p TCP --dport ssh -j ACCEPT**

Cały gotowy skrypt będzie wyglądał w sposób następujący:

**iptables -F**

**iptables -t nat -F**

**iptables -P INPUT DROP**

**iptables -P OUTPUT ACCEPT**

**iptables -P FORWARD DROP**

**iptables -A INPUT -p ICMP -j ACCEPT**

**iptables -A OUTPUT -p ICMP -j ACCEPT //w zasadzie nie potrzebne**

**iptables -A INPUT -p TCP --dport http -j ACCEPT**

**iptables -A INPUT -p TCP --dport ssh -j ACCEPT**

Następnym krokiem w konfiguracji serwera będzie dodanie reguł dla ruchu przechodzącego (FORWARD). Umożliwi to dostęp maszynom klienckim do sieci Internet.
Najprostszym sposobem na konfigurację dostępu do sieci jest dokonanie dwóch wpisów w łańcuchu FORWARD:

**iptables -A FORWARD -s 192.167.0.0/24 -j ACCEPT**

**iptables -A FORWARD -d 192.167.0.0/24 -j ACCEPT**

Aby reguły łańcucha FORWARD zadziałały należy włączyć w jądrze moduł odpowiedzialny za przekazywanie pakietów:

**echo 1 > /proc/sys/net/ipv4/ip_forward**

oraz

**iptables -t nat -A POSTROUTING -j MASQUERADE**

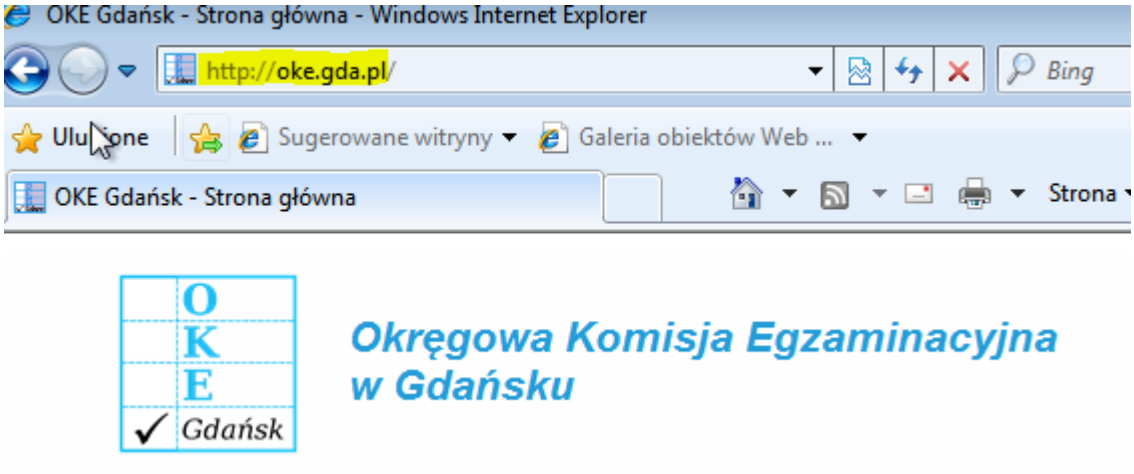
Na komputerze klienckim >

| | |
|---|---|
| DHCP włączone | Nie |
| Adres IPv4 | 10.0.0.31 |
| Maska podsieci IPv4 | 255.255.255.0 |
| Brama domyślna IPv4 | 10.0.0.30 |
| Serwer DNS IPv4 | 8.8.4.4 |

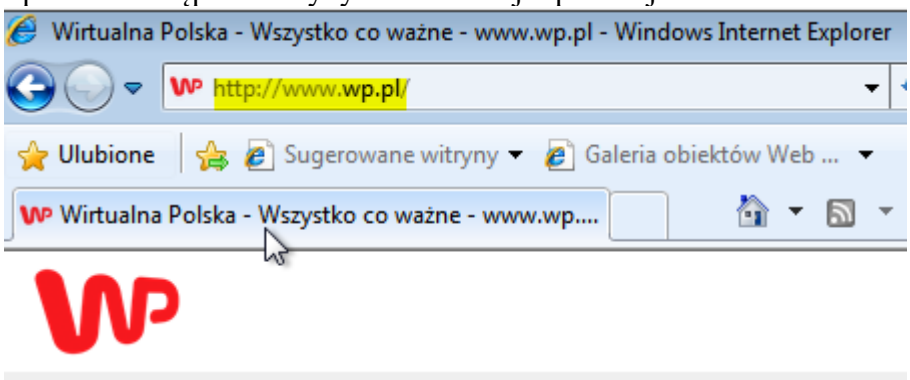
Po wykonaniu powyższych czynności komputer kliencki będzie miał dostęp do sieci Internet (pod warunkiem, że serwer ma dostęp do Internetu).

cmd > tracert oke.gda.pl

Powyżej pokaże się trasa pakietu z komputera klienckiego do serwera oke.gda.pl.




Sprawdź dostęp do witryny internetowej o podanej nazwie.




W następnym kroku zablokuj dostęp do witryny internetowej o podanej nazwie.
Zablokowanie całego ruchu do domeny uzyskamy wpisując:

**iptables -I FORWARD -d wp.pl -j DROP**

lub

**iptables -A OUTPUT -p tcp --destination www.wp.pl -j ACCEPT**

**iptables -A OUTPUT -p tpc --dport 80 -j DROP**

lub

**iptables -A INPUT -p tcp -m tcp -d www.wp.pl -j DROP**

lub

**iptables -N STREAM**

**iptables -I OUTPUT -m string --string "www.wp.pl" --algo bm --from 1 --to 600 -j STREAM**

**iptables -I OUTPUT -m string --string "wp.pl" --algo bm --from 1 --to 600 -j STREAM**

**iptables -I FORWARD -m string --string "www.wp.pl" --algo bm --from 1 --to 600 -j STREAM**

**iptables -I FORWARD -m string --string "wp.pl" --algo bm --from 1 --to 600 -j STREAM iptables -A STREAM -j REJECT**

Podaj prawidłową/łe regułę/ły blokującą/e.

Czy dobrym pomysłem jest blokowanie po adresie.

Wykonaj przekierowanie całego ruchu na serwer wewnętrzny. Składnia polecenia iptables została podana poniżej:

**iptables -A PREROUTING -t nat -s 10.0.0.0/24 -p tcp - -dport 1:65535 -j DNAT - -to- 10.0.0.30:8001**

Powyższe polecenie przekierowuje cały ruch TCP na serwer lokalny na port 8001.
W podobny sposób można przekierować ruch z konkretnego hosta lub na konkretny port.

Dopisz ruter aby routing uruchamiał się zawsze podczas startu interfejsu sieciowego.

pre-up iptables-restore < /etc/router

Pakiet iptables ma bardzo duże możliwości konfiguracyjne.
Przykładowe wpisy IPTABLES znajdują się na stronie iptables.pl

Wyjaśnij w zeszycie powyższy przykładowy plik.

*Plik można wygenerować za pomocą iptables generator.*

*Wygeneruj plik za pomocą generatora i zastosuj dla zapory korzystając np z http://iptables.rzeźniczak.pl.*