

T: Konfiguracja zapory sieciowej w systemie Linux.**Zadanie1:**

Odszukaj informacje na temat narzędzi TCP Wrappers. Zapoznaj się ze strukturą i zawartością plików:

```
/etc/hosts.allow
/etc/hosts.deny
    sshd : 192.168.10.21
    ALL : ALL
    ALL : ALL EXCEPT localhost
    ALL : .elektronik.pl EXCEPT s27st02.elektronik.pl
    in.telnetd : .elektronik.pl EXCEPT s27st02.elektronik.pl
```

Zadanie2:

Odszukaj w pomocy systemowej informacje na temat programu **iptables**.

```
rpm -qa | grep iptables
chkconfig SuSEfirewall2_setup
chkconfig SuSEfirewall2_setup on
chkconfig SuSEfirewall2_setup off
/etc/init.d/SuSEfirewall2_setup status
/etc/init.d/SuSEfirewall2_setup stop
/etc/init.d/SuSEfirewall2_setup start
SuSEfirewall2 stop
SuSEfirewall2 start
netstat -ant
iptables -L
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -I INPUT -p icmp -j ACCEPT
iptables -I OUTPUT -p icmp -j ACCEPT
iptables -D OUTPUT -p udp -s 0/0 --sport 67 -d 0/0 --dport 68 -j REJECT
```

Zadanie3:

Zapoznaj się z zawartością następujących witryn sieciowych:

<http://iptables.ovh.org/>
<http://wasil.org/iptables-i-blokowanie-stron-www>
<http://plociennik.info/index.php/iptables>

Zadanie4:

Skonfiguruj zaporę sieciową do akceptowania połączeń poprzez usługę ssh dla jednego komputera w sieci lokalnej (przykład dla komputera 192.168.19.22):

```
/usr/sbin/iptables -F
/usr/sbin/iptables -X
/usr/sbin/iptables -A INPUT -s localhost -j ACCEPT
/usr/sbin/iptables -A INPUT -p tcp -s 192.168.19.21 --dport 22 -j ACCEPT
/usr/sbin/iptables -A INPUT -p tcp -s 192.168.19.23 --sport 22 -j ACCEPT
```

Zadanie5:

Skonfiguruj zaporę sieciową do akceptowania połączeń z usługą www (przykład dla komputera 192.168.19.21).

Przykładowe rozwiązanie:

```
/usr/sbin/iptables -F
/usr/sbin/iptables -X
/usr/sbin/iptables -P INPUT ACCEPT
/usr/sbin/iptables -P OUTPUT DROP
```

```
/usr/sbin/iptables -A OUTPUT -s localhost -j ACCEPT
/usr/sbin/iptables -A OUTPUT -p tcp -s 192.168.19.21 --dport 80 -j ACCEPT
/usr/sbin/iptables -A OUTPUT -p tcp -s 192.168.19.21 --dport 443 -j ACCEPT
/usr/sbin/iptables -A OUTPUT -p tcp -s 192.168.19.21 --dport 8080 -j ACCEPT
/usr/sbin/iptables -A OUTPUT -p tcp -s 192.168.19.21 --dport 53 -j ACCEPT
```

Zadanie6:

Utwórz prezentację w programie LibreOffice Impress na temat konfiguracji zapory sieciowej w systemie Linux OpenSUSE. W prezentacji zastosuj jednolite przejście slajdów bez dodatkowych efektów. Pracę zachowaj w pliku pod nazwą **\$nazwisko_\$klasa_\$gr_iptables.odp** i prześlij pocztą elektroniczną do nauczyciela na adres greszata@zs9elektronik.pl.

W prezentacji należy zamieścić następujące elementy:

- slajd tytułowy,
- wyjaśnienie zagadnienia zapory sieciowej firewall i oprogramowania iptables,
- konfigurację zapory sieciowej poprzez narzędzie dostępne w YaST,
- metodę włączania i wyłączania zapory w konsoli tekstowej,
- ustawienie automatycznego włączania zapory podczas uruchamiania systemu w konsoli tekstowej,
- wyświetlania skonfigurowanych reguł zapory w konsoli tekstowej,
- metodę wyzerowania reguł zapory w konsoli tekstowej,
- metodę ustawienia domyślnej polityki zapory w konsoli tekstowej,
- podsumowanie, wnioski, wskazania,
- slajd zakończeniowy.

Konfiguracja firewall'a w systemie Linux z konsoli tekstowej (iptables)

Sprawdzenie bieżącej konfiguracji firewalla

```
iptables -L
```

Firewall wyzerujemy poleceniami

```
iptables -F
```

```
iptables -X
```

a potem sprawdzamy jego stan po odblokowaniu poleceniem

```
iptables -L -n -v
```

Jeżeli wszystko ACCEPT to serwer jest odblokowany.

Jeżeli wszystko DROP to serwer jest zablokowany.

Zasady bezpieczeństwa konfigurowane są dla:

```
input -> wejścia
```

```
output -> wyjścia
```

```
forward -> przekazywania (gdy więcej urządzeń sieciowych)
```

Domyślne zasady blokowania pakietów ustawiamy poleceniami z opcją P:

```
iptables -P FORWARD DROP
```

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT DROP
```

Sprawdzamy uzyskaną konfigurację:

```
iptables -L
```

Domyślne zasady odblokowania pakietów ustawiamy poleceniami:

```
iptables -P FORWARD ACCEPT
```

```
iptables -P INPUT ACCEPT
```

```
iptables -P OUTPUT ACCEPT
```

Sprawdzamy uzyskaną konfigurację:

```
iptables -L
```

```
netstat -antp
```

Zablokowanie portu telnet na komputerze serwer wyglądałoby następująco:

```
iptables -A INPUT -p tcp -s 0.0.0.0/0 -d 192.168.10.1/24 --dport 23 -j DROP
```

Usunięcie poprzedniego ustawienia uzyskujemy poleceniem:

```
iptables -D INPUT -p tcp -s 0.0.0.0/0 -d 192.168.10.1/24 --dport 23 -j DROP
```

Przykładowe reguły:

```
iptables -A INPUT -p tcp -s 192.168.10.0/24 --sport 20:23 -d 192.168.10.1/24
-i eth0 -j ACCEPT
```

```
iptables -A FORWARD -s 192.168.10.5 -d 0.0.0.0/0 -i eth0 -j MASQUERADE
```

gdzie:

```
-A -> dodawanie reguły
-D -> usuwanie reguły
-s -> źródło sygnału
-d -> cel sygnału
-p -> protokół sieciowy (tcp/udp/icmp)
-i -> interfejs sieciowy
-j -> zasada reakcji
--sport -> port źródłowy
--dport -> port docelowy
/24 -> maska 255.255.255.0
20:23 -> dla portów usług sieciowych od 21 do 23
0.0.0.0/0 -> dla dowolnych adresów sieciowych
```

```
iptables -A INPUT -p tcp ! -s 192.168.19.35 -d 0.0.0.0 --dport 22 -j DROP
```

Odblokowanie ruchu dla pętli zwrotnej LOOPBACK

```
/usr/sbin/iptables -A INPUT -i lo -j ACCEPT
```

Jeżeli nasz komputer ma udostępniać Internet w sieci wewnętrznej to dodajemy regułę maskowania pakietów pochodzących z wewnętrznej sieci. Przykłady ustawień maskowania adresów:

```
#dynamicznie przydzielany adres IP
/usr/sbin/iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
/usr/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
/usr/sbin/iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -d 0/0 -j MASQUERADE
/usr/sbin/iptables -t nat -A POSTROUTING -s 192.168.10.201 -d 0/0 -j MASQUERADE
#statycznie przydzielany adres IP
/usr/sbin/iptables -t nat -A POSTROUTING -j SNAT --to-source 192.168.11.2
/usr/sbin/iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth0 -j SNAT --to
192.168.11.2
/usr/sbin/iptables -t nat -A POSTROUTING -s 192.168.10.201 -o eth0 -j SNAT --to
192.168.11.2
/usr/sbin/iptables -t nat -A POSTROUTING -j SNAT --to-source 192.168.11.2-
192.168.11.16
```

Ustawienie gdy posiadamy zewnętrzny adres IP przypisywany dynamicznie:

```
/usr/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Ustawienie, gdy adres jest stały:

```
/usr/sbin/iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 12.12.12.12
```

Powrotne pakiety (z Internetu):

```
/usr/sbin/iptables -t nat -A PREROUTING -p tcp -d 15.15.15.15 --dport 80 -j DNAT --
to-destination 10.0.0.25
/usr/sbin/iptables -t nat -A PREROUTING -p tcp -d 192.168.11.1/32 --dport 3389 -j
DNAT --to-destination 192.168.10.4:3389
```

Ograniczenie ilości połączeń - 15 na sekundę:

```
/usr/sbin/iptables -A INPUT -p tcp --syn --dport 80 -m limit --limit 15/second --
limit-burst 35 -j ACCEPT
```

Przykładowy skrypt konfigurujący maskaradę adresów sieciowych:

```
#!/bin/sh
#wlaczanie przekazywania pakietow
echo "1" > /proc/sys/net/ipv4/ip_forward
#echo "1" > /proc/sys/kernel/panic
#nieodpowiadanie na zapytania ping
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all
#czyszczenie ustawien firewalla
/sbin/iptables -F
/sbin/iptables -F -t nat
/sbin/iptables -X -t nat
/sbin/iptables -F -t filter
/sbin/iptables -X -t filter
#negatywna domyslna polityka przekazywania pakietow (odrzucaenie pakietow)
/sbin/iptables -t filter -P FORWARD DROP
#przekazywanie pakietow dostepne dla sieci 192.168.0.0/16
```

```
/sbin/iptables -t filter -A FORWARD -s 192.168.0.0/255.255.0.0 -d 0/0 -j ACCEPT
/sbin/iptables -t filter -A FORWARD -s 0/0 -d 192.168.0.0/255.255.0.0 -j ACCEPT
#włączenie translacji adresów źródłowych (SNAT)
/sbin/iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth0 -j SNAT --to 192.168.11.2
```

#blokowanie reklam gadu-gadu

```
iptables -t nat -A PREROUTING -s adserver.gadu-gadu.pl -p tcp --dport 80 -j DROP
iptables -t nat -A POSTROUTING -d adserver.gadu-gadu.pl -p tcp --dport 80 -j DROP
```

#przekierowanie reklam gadu-gadu na lokalny serwer

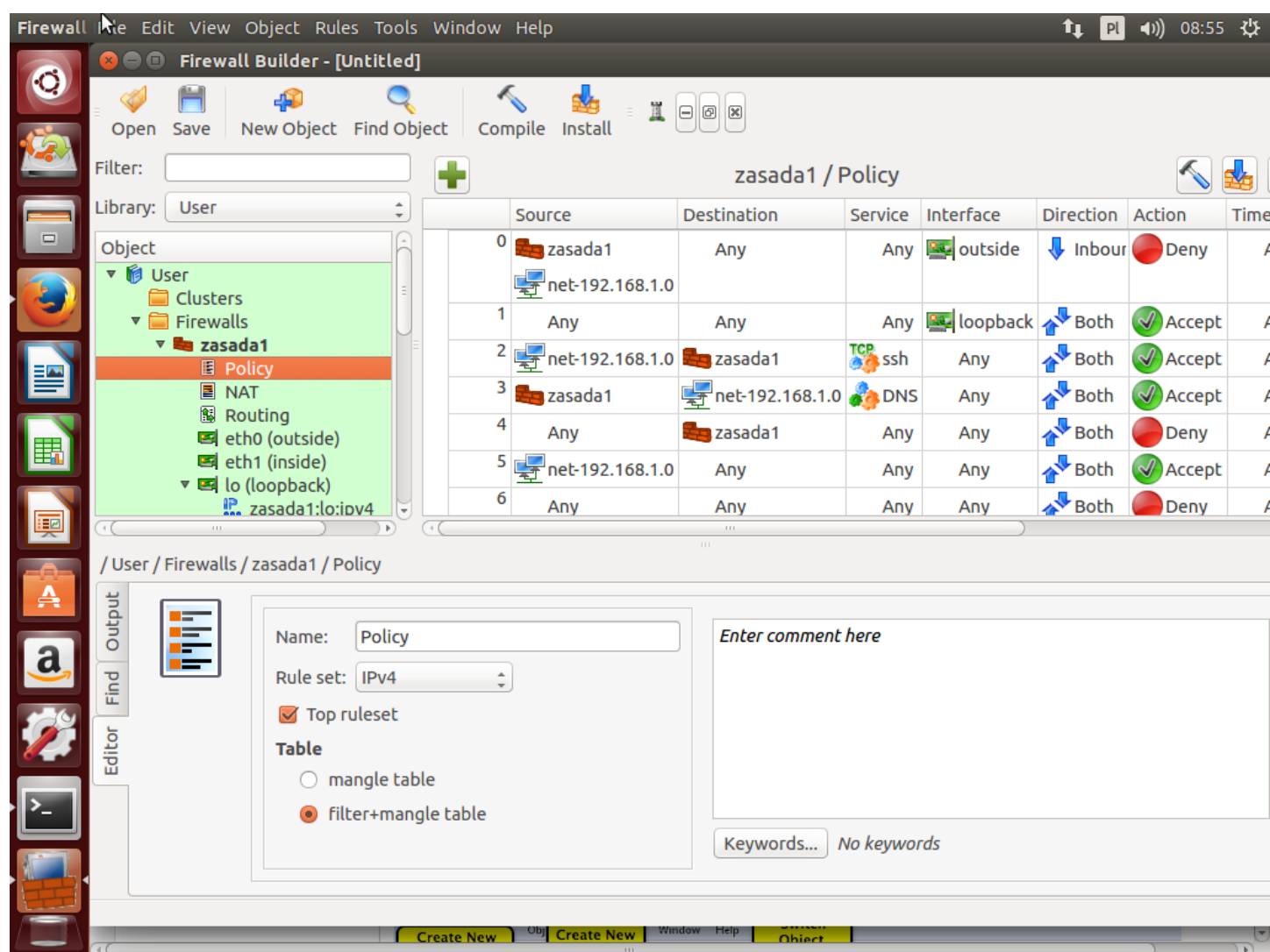
```
iptables -t nat -A PREROUTING -d adserver.gadu-gadu.pl -p tcp --dport 80 -j DNAT --to
192.168.0.1:88
```

Zadanie7:

Utwórz prezentację na temat instalacji i konfiguracji nakładki graficznej na zapórę sieciową w systemie Linux Ubuntu Live. Pracę zachowaj pod nazwą **\$nazwisko_firewall_ubuntu**.

```
dpkg -l | grep gufw
```

```
apt-get install fwbuilder #wymaga źródeł pakietów universe
```



Konfiguracja zapory sieciowej w systemie Linux SUSE poprzez Centrum sterowania YAST:

Konfiguracja zapory sieciowej: Uruchamianie

Uruchomienie usługi:

- ☒ Włącz automatyczne uruchamianie zapory
- ☐ Wyłącz automatyczne uruchamianie zapory

Włączanie i wyłączanie

Stan bieżący: Zapora sieciowa jest uruchomiona

Uruchom zaporę

Zatrzymaj zaporę

Zapisz ustawienia i uruchom zaporę ponownie

Pomoc Anuluj Wstecz Dalej

Konfiguracja zapory sieciowej: Interfejsy

Interfejsy zapory sieciowej:

Urządzenie	Interfejs albo wyrażenie	Konfigurowano w
PRO/Wireless 3945ABG (Golan) Net...	wlan0	Strefa zewnętrzna
RTL 8169 Gigabit Ethernet	eth0	Strefa zdemilitaryzowana (ograniczona)

Zmień... Dostosuj...

Pomoc Anuluj Wstecz Dalej

Konfiguracja zapory sieciowej: Dozwolone usługi

Dozwolone usługi w wybranej strefie

Strefa zewnętrzna

Usługa, którą należy zezwolić:

Demon Iccream

Dozwolona usługa Opis

Samba Client	Enables browsing for Samba's Netbios Server with broadc...
Samba Server	Opens ports for Samba Server.
Server bezpiecznej powłoki (SSH)	Otwiera porty dla serwera SSH.
Server vsftpd	Otwiera porty dla serwera vsftpd.

Dodaj Usun

☐ Chron zaporę sieciową ze strefy wewnętrznej

Zaawansowane...

Pomoc Anuluj Wstecz Dalej

Konfiguracja zapory sieciowej: Dozwolone usługi

Dozwolone usługi w wybranej strefie

Strefa wewnętrzna

Usługa, którą należy zezwolić:

Dozwolona usługa Opis

DHCPv4 Server	dnsmasq
dnsmasq	dnsmasq (dnsmasq-dns)
Klient NFS	Client NFS
Klient NIS	mDNS/Bonjour support for HPLIP
Mono XSP2 ASP.NET Host Service	Netbios Server
OpenSLP server (SLP)	Planer Iccream
Rsync server	Samba Client
Samba Client	Samba Server
Server bezpiecznej powłoki (SSH)	Server cyrus-imapd
Server DNS bind	Server HTTP
Server HTTP	Server MySQL
Server MySQL	Server NIS
Server NIS	Server OpenLDAP
Server VNC	Server VNC

Dodaj Usun

☐ Chron zaporę sieciową ze strefy wewnętrznej

Zaawansowane...

Pomoc Anuluj Wstecz Dalej

Konfiguracja zapory sieciowej: Rozgłaszanie

Konfiguracja rozgłaszania

Strefa wewnętrzna

Strefa zdemilitaryzowana (ograniczona) z:

Strefa zewnętrzna

☒ Rejestruj niezaakceptowane pakiety rozgłoszeniowe

☒ Rejestruj niezaakceptowane pakiety rozgłoszeniowe

☐ Rejestruj niezaakceptowane pakiety rozgłoszeniowe

Akceptowanie odpowiedzi rozgłoszeniowej

Strefa	Usługa	Akceptowane z sieci
Strefa zewnętrzna	Przeglądanie zasobów Samba	Podsieć: 192.168.10.0/29
Strefa zewnętrzna	Wszystkie usługi używające UDP	Wszystkie sieci

Dodaj Usun

Pomoc Anuluj Wstecz Dalej

Konfiguracja zapory sieciowej: Poziom zapisu w dzienniku

Poziom zapisu w dzienniku

Rejestruj wszystkie akceptowane pakiety

Rejestruj tylko krytyczne

Rejestruj wszystkie nieakceptowane pakiety

Rejestruj wszystko

Pomoc Anuluj Wstecz Dalej

Konfiguracja zapory sieciowej: Własne zasady

Własne reguły zezwalania

Strefa zapory sieciowej

Strefa zewnętrzna

Sieć źródłowa	Protokół	Port docelowy	Port źródłowy
192.168.10.0/29	TCP	ssh (22)	
192.168.10.5	TCP	20,21	

Dodaj Usun

Pomoc Anuluj Wstecz Dalej