T: Firewall – zapora sieciowa.

Zadania oprogramowania firewall:
- filtrowanie i analiza pakietów – jeśli otrzymam taki pakiet, to…,
- blokowanie protokołów lub zawartości,
- autoryzacja użytkowników i szyfrowanie połączeń oraz sesji.

Zadanie1:

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

Zadanie2:

Zapoznaj się z zawartością następujących witryn sieciowych:
http://iptables.ovh.org/
http://wasil.org/iptables-i-blokowanie-stron-www

Zadanie3:

Odszukaj informacje na temat narzędzi TCP Wrappers. Zapoznaj się ze strukturą i zawartością plików:
`/etc/hosts.allow`
`/etc/hosts.deny`

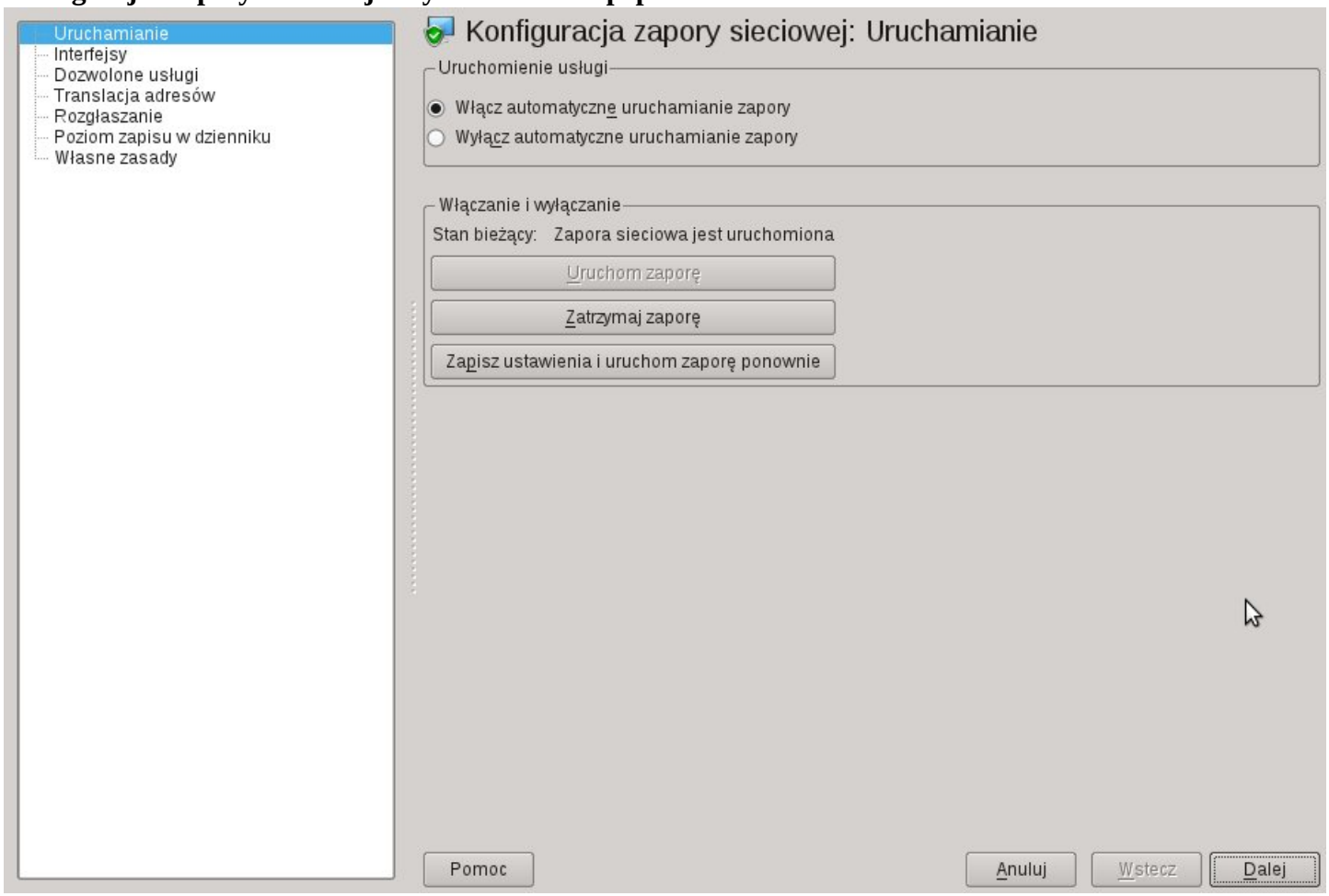
```
sshd : 192.168.10.21
ALL : ALL
ALL : ALL EXCEPT localhost
ALL : .elektronik.pl EXCEPT s27st02.elektronik.pl
in.telnetd : .elektronik.pl EXCEPT s27st02.elektronik.pl
```

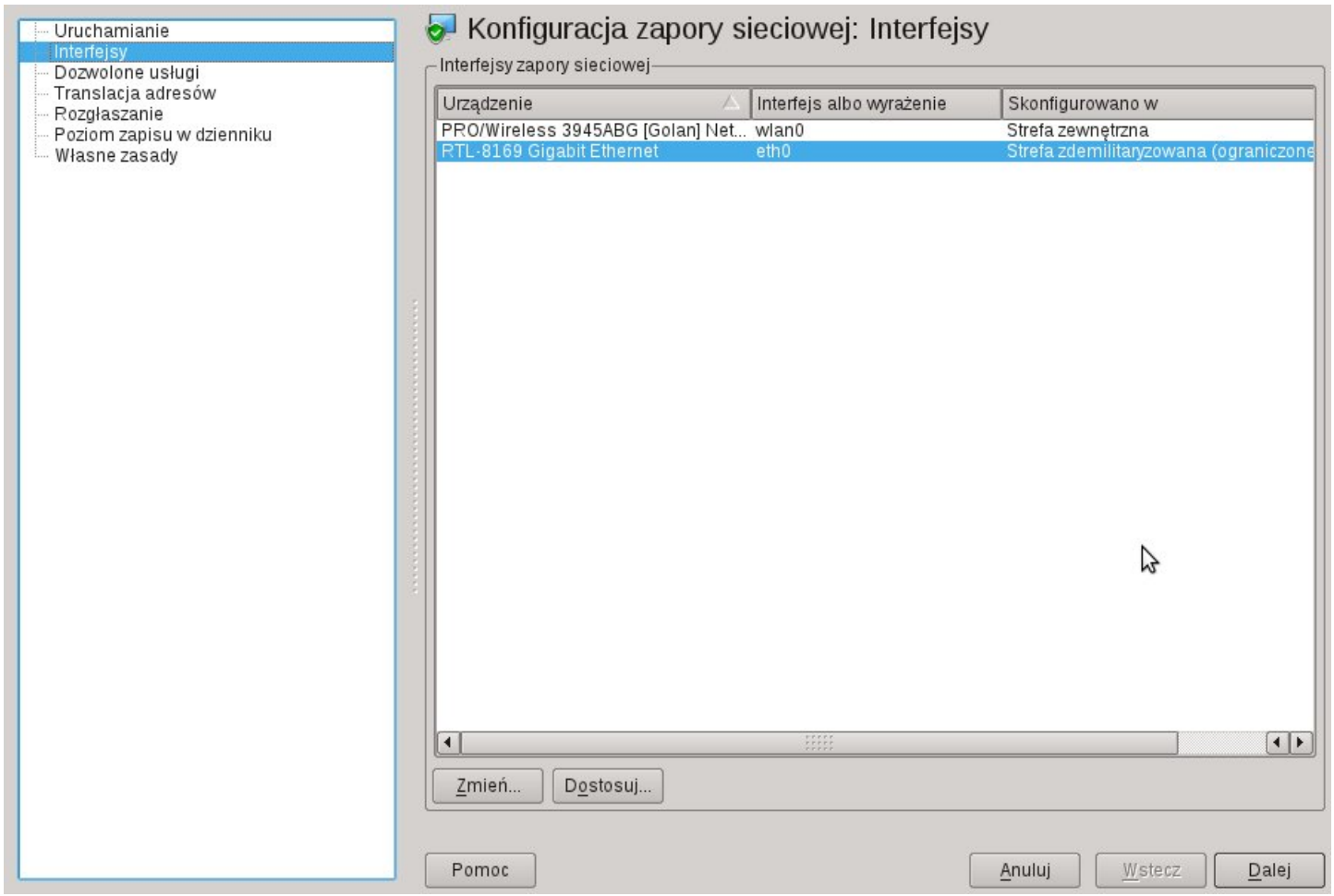
Zadanie4:

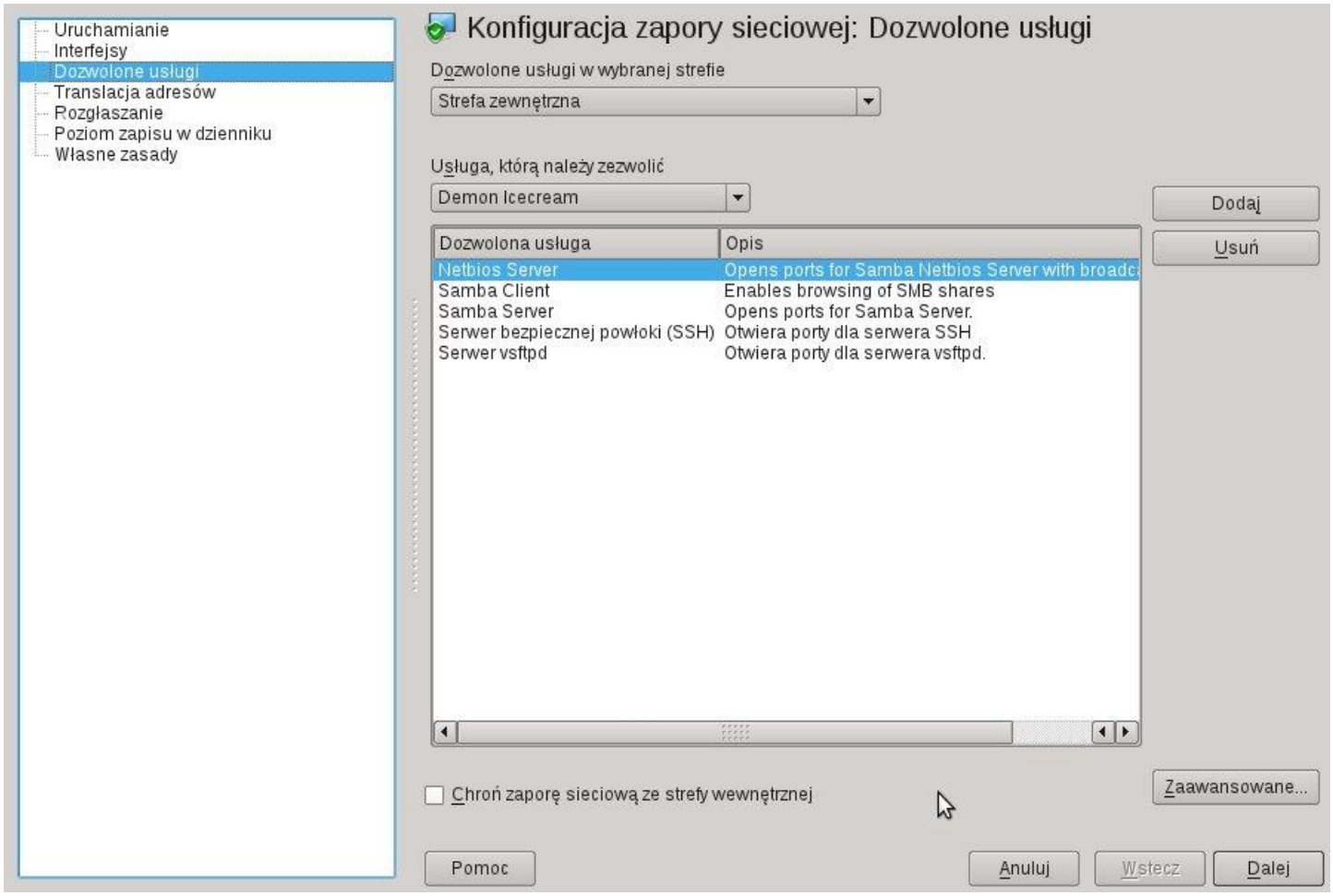
Utwórz prezentację w programie LibreOffice Impress na konfiguracji zapory sieciowej w systemie Linux OpenSUSE. W prezentacji zastosuj jednolite przejście slajdów bez dodatkowych efektów. Pracę zachowaj pod nazwą **$nazwisko_firewall.odp** na dysku h: w katalogu asso lub prześlij pocztą elektroniczną do nauczyciela na adres greszata@zs9elektronik.pl.

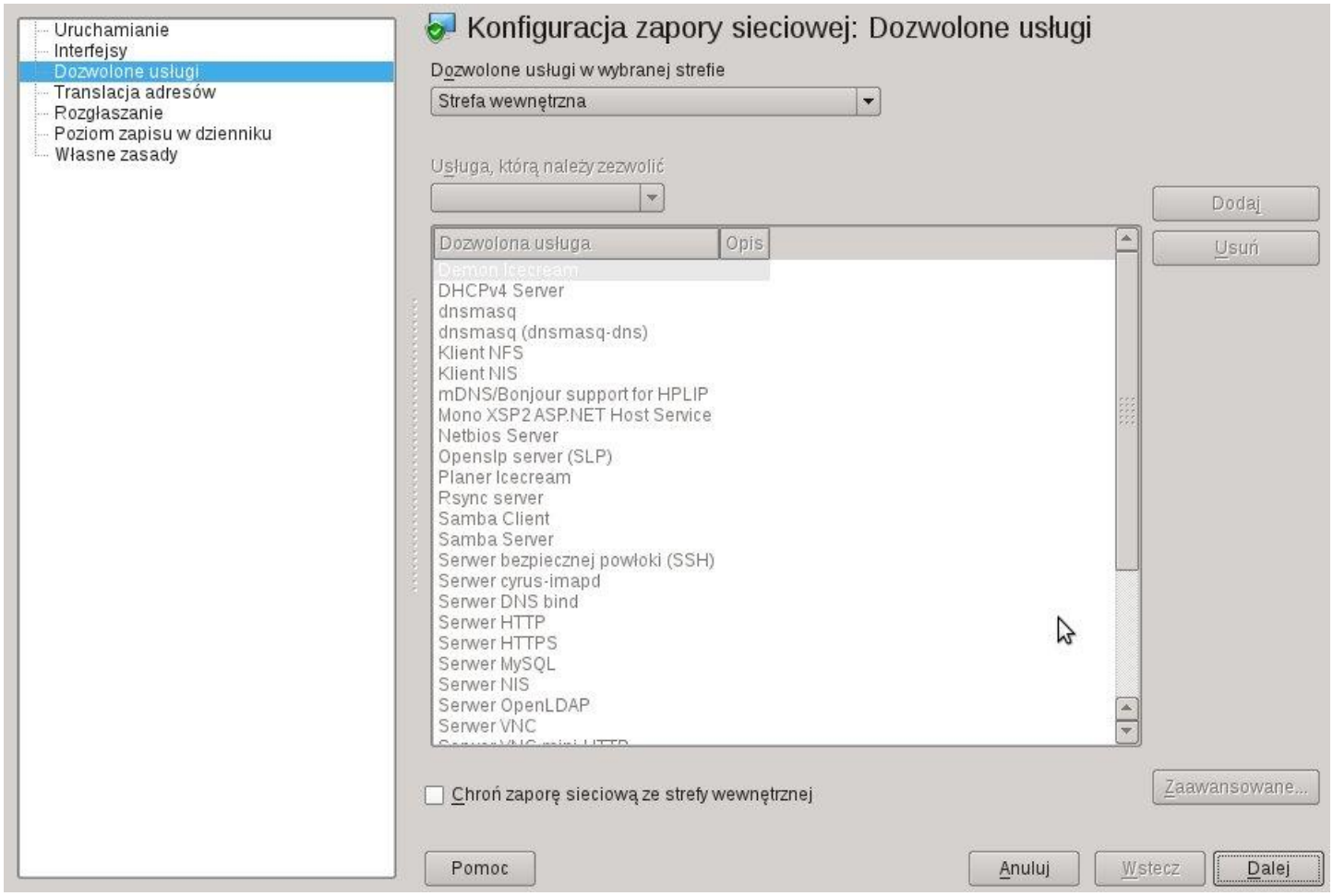
W prezentacji należy zamieścić następujące elementy:
- slajd tytułowy,
- wyjaśnienie zagadnienia zapory sieciowej firewall i oprogramowania iptables,
- konfigurację zapory sieciowej poprzez narzędzie dostępne w YaST,
- metodę włączania i wyłączania zapory w konsoli tekstowej,
- ustawienie automatycznego 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,
- slajd zakończeniowy.

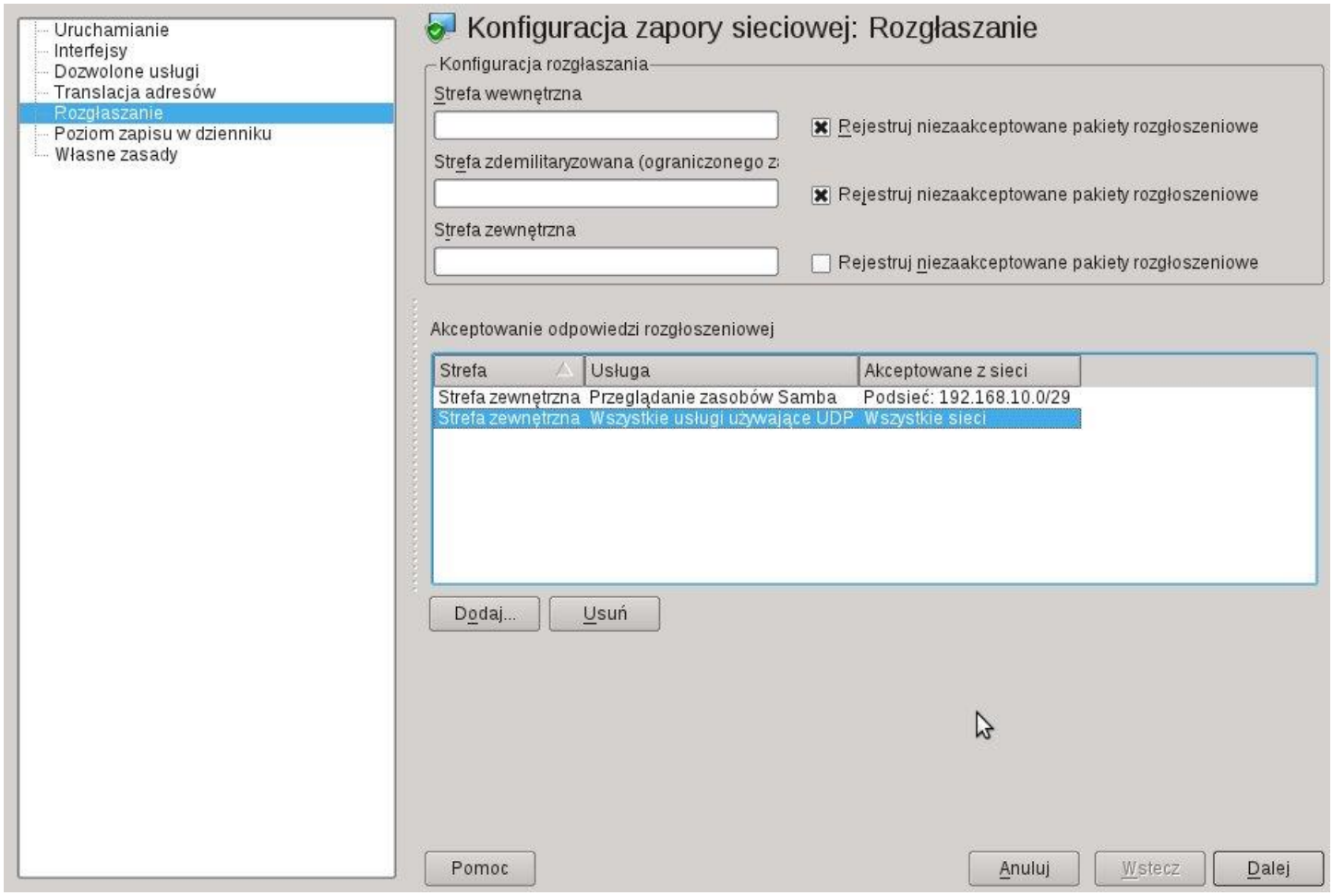
Konfiguraja zapory sieciowej w systemie Linux poprzez Centrum sterowania YAST

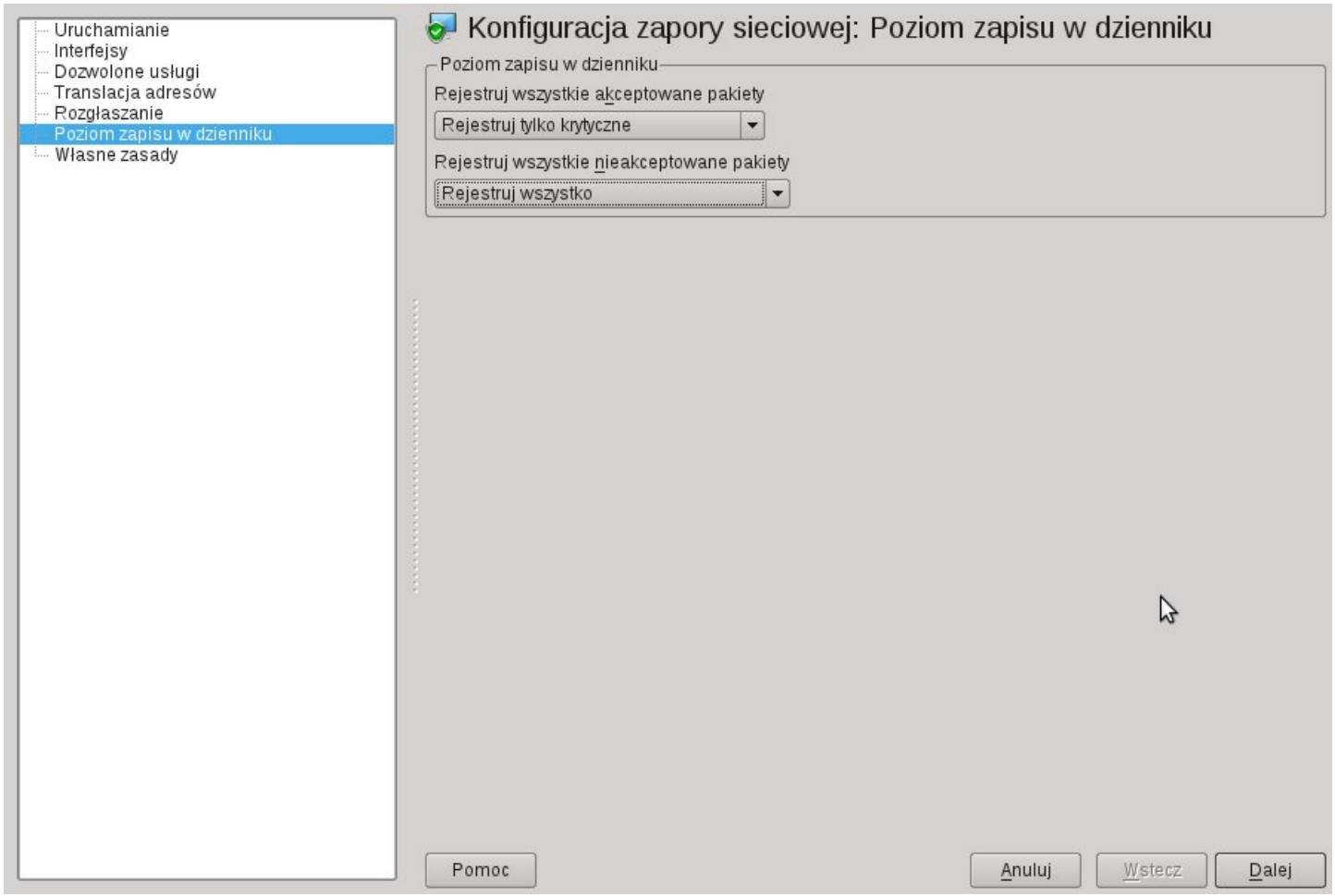


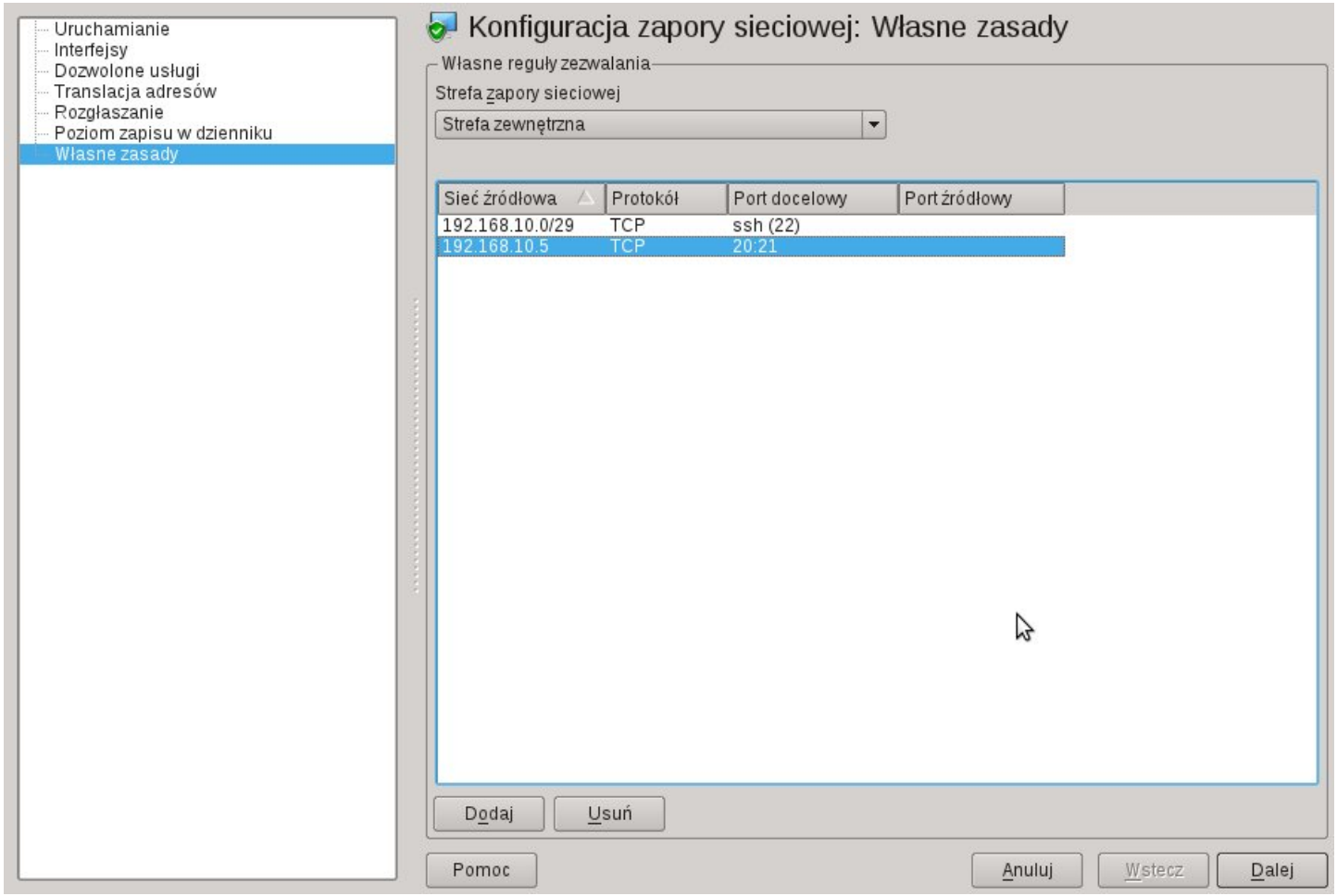



Uruchamianie
Interfejsy
Dozwolone usługi
Translacja adresów
Rozgłaszanie
Poziom zapisu w dzienniku
Własne zasady
Konfiguracja zapory sieciowej: Dozwolone usługi
Dozwolone usługi w wybranej strefie
Strefa zewnętrzna
Usługa, którą należy zezwolić
Demon Icecream
Dodaj
Usuń
Dozwolona usługa
Opis
Netbios Server
Opens ports for Samba Netbios Server with broadc
Samba Client
Enables browsing of SMB shares
Samba Server
Opens ports for Samba Server.
Serwer bezpiecznej powłoki (SSH)
Otwiera porty dla serwera SSH
Serwer vsftpd
Otwiera porty dla serwera vsftpd.
Chroń zaporę sieciową ze strefy wewnętrznej
Zaawansowane...
Pomoc
Anuluj
Wstecz
Dalej


Uruchamianie
Interfejsy
Dozwolone usługi
Translacja adresów
Rozgłaszanie
Poziom zapisu w dzienniku
Własne zasady
Konfiguracja zapory sieciowej: Dozwolone usługi
Dozwolone usługi w wybranej strefie
Strefa wewnętrzna
Usługa, którą należy zezwolić
Dodaj
Usuń
Dozwolona usługa
Opis
Demon Icecream
DHCPv4 Server
dnsmasq
dnsmasq (dnsmasq-dns)
Klient NFS
Klient NIS
mDNS/Bonjour support for HPLIP
Mono XSP2 ASP.NET Host Service
Netbios Server
Openslp server (SLP)
Planer Icecream
Psync server
Samba Client
Samba Server
Serwer bezpiecznej powłoki (SSH)
Serwer cyrus-imapd
Serwer DNS bind
Serwer HTTP
Serwer HTTPS
Serwer MySQL
Serwer NIS
Serwer OpenLDAP
Serwer VNC
Chroń zaporę sieciową ze strefy wewnętrznej
Zaawansowane...
Pomoc
Anuluj
Wstecz
Dalej


Uruchamianie
Interfejsy
Dozwolone usługi
Translacja adresów
Rozgłaszanie
Poziom zapisu w dzienniku
Własne zasady
Konfiguracja zapory sieciowej: Rozgłaszanie
Konfiguracja rozgłaszania
Strefa wewnętrzna
Rejestruj niezaakceptowane pakiety rozgłoszeniowe
Strefa zdemilitaryzowana (ograniczonego z
Rejestruj niezaakceptowane pakiety rozgłoszeniowe
Strefa zewnętrzna
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...
Usuń
Pomoc
Anuluj
Wstecz
Dalej


Uruchamianie
Interfejsy
Dozwolone usługi
Translacja adresów
Rozgłaszanie
Poziom zapisu w dzienniku
Własne zasady
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



Konfiguraja 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 opcja 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 uzyskana konfiguracje:

```
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 regułkę 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
#wlaczenie 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 (odrzucanie 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
#wlaczenie translacji adresow zrodlowych (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
```

Przykładowy skrypt konfiguracji zapory sieciowej systemu Linux do zadania projektowego:

```
#!/bin/sh

echo wlaczenie przekazywania pakietow i nie odpowiadanie na pingi
echo 1 > /proc/sys/net/ipv4/ip_forward
sysctl net.ipv4.ip_forward=1
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all

echo czyszczenie poprzednich wpisow zapory
/usr/sbin/iptables -F
/usr/sbin/iptables -X

echo ustawienie domyslnej polityki bezpieczenstwa
/usr/sbin/iptables -P INPUT DROP
/usr/sbin/iptables -P FORWARD DROP
/usr/sbin/iptables -P OUTPUT ACCEPT

echo udostepnianie polaczenia z karty eth0 - zewnetrzna, dynamiczny IP
/usr/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# udostepnianie polaczenia z karty eth0 (zewnetrzna, statyczny IP)
#/usr/sbin/iptables -t nat -A POSTROUTING -j SNAT --to-source 192.168.19.35
# lub
#/usr/sbin/iptables -t nat -A POSTROUTING -s 192.168.35.0/24 -o eth0 -j SNAT --to 192.168.19.35

echo konfiguracja aliasu dla karty sieciowej
/sbin/ifconfig eth0:1 192.168.35.1 netmask 255.255.255.0

echo odblokowanie ruchu dla petli zwrotnej LOOPBACK
/usr/sbin/iptables -A INPUT -i lo -j ACCEPT
#/usr/sbin/iptables -A OUTPUT -o lo -j ACCEPT

echo odblokowujemy uslugi dla polaczen przychodzacych z zewnatrz
/usr/sbin/iptables -A INPUT -p tcp -s 0/0 --dport 20:21 -j ACCEPT
/usr/sbin/iptables -A INPUT -p tcp -s 0/0 --dport 80 -j ACCEPT
/usr/sbin/iptables -A INPUT -p udp -s 0/0 --dport 20:21 -j ACCEPT
/usr/sbin/iptables -A INPUT -p tcp -s 0/0 --dport 8074 -j ACCEPT
/usr/sbin/iptables -A INPUT -p tcp -s 0/0 --dport 443 -j ACCEPT
```

```
/usr/sbin/iptables -A INPUT -p tcp -s 192.168.19.35 --dport 22 -j ACCEPT
/usr/sbin/iptables -A INPUT -p tcp -s 0/0 --dport 113 -j ACCEPT
/usr/sbin/iptables -A INPUT -p udp -s 0/0 --dport 1025:1100 -j ACCEPT
/usr/sbin/iptables -A INPUT -p tcp -s 0/0 --sport 53 -j ACCEPT
/usr/sbin/iptables -A INPUT -p udp -s 0/0 --sport 53 -j ACCEPT
/usr/sbin/iptables -A INPUT -p tcp -s 0/0 --sport 67 --dport 68 -j ACCEPT
/usr/sbin/iptables -A INPUT -p udp -s 0/0 --sport 67 --dport 68 -j ACCEPT

echo odblokowanie przegladania www z serwera
/usr/sbin/iptables -A INPUT -p tcp -s 0/0 --sport 80 -j ACCEPT
```

#skrypt konfiguracji firewalla ze strony www

```
#!/bin/sh
################################################################################
#KONFIGURACJA SKRYPTU
IPTABLES=/sbin/iptables       #scieka do iptables
STRONY=/root/webaccept        #sciezka do pliku z odblokowanymi stronami
CONF_ROUTING=1                #wlaczamy routing
CONF_PROXY=1                  #transparetne proxy na porcie 81 serwera
CONF_BLOKADA_PORTY=1          #blokada wszystkich portow
CONF_BLOKADA_OTWARTE=1        #otwarcie wybranych portow
#21   FTP         443  HTTPS            25   SMTP       444  SharePoint
#53   DNS         500  VPN IPSEC        80   HTTP       1701 VPN L2TP
#81   PROXY       1723 VPN PPTP        110  POP3       3389 MSTSC
#123  NTP         4125 OWA            143  IMAP       4500 VPN IPSEC
#220  IMAP3       22   SSH
#TCP
PORTYODBT="21 25 110 143 220"
#UDP
PORTYODBU=""
CONF_BLOKADA_BANKI=1    #otwieramy port tcp 443 tylko dla wybranych stron
CONF_BLOKADA_GG=1        #blokowanie kontaktu z serwerami Gadu Gadu
################################################################################
#czycimy tablicz poprzednich regu
echo Czyscimy reguly firewall-a
$IPTABLES -F
$IPTABLES -X
$IPTABLES -t nat -X
$IPTABLES -t nat -F
$IPTABLES -t mangle -X
$IPTABLES -t mangle -F
################################################################################
#ustawiamy domyln polityke
echo Domyslna polityka
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -P FORWARD ACCEPT
################################################################################
if [ "$CONF_ROUTING" = "1" ]; then
echo Wlaczamy routing i udostepnianie internetu
echo 1 > /proc/sys/net/ipv4/ip_forward
$IPTABLES -t nat -A POSTROUTING -o eth0 -s 192.168.0.0/24 -j MASQUERADE
fi
################################################################################
if [ "$CONF_PROXY" = "1" ]; then
echo Transparetne PROXY
$IPTABLES -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 81
fi
################################################################################
if [ "$CONF_BLOKADA_PORTY" = "1" ]; then
echo Ubijanie UDP i TCP
$IPTABLES -I FORWARD -s 192.168.0.0/24 -p udp --dport 1:65534 -j DROP
$IPTABLES -I FORWARD -s 192.168.0.0/24 -p tcp --dport 1:65534 -j DROP
fi
################################################################################
```

```
if [ "$CONF_BLOKADA_OTWARTE" = "1" ]; then
echo Otwieramy porty:
echo TCP:
for adres in $PORTYODBT
do
    echo $adres
    $IPTABLES -I FORWARD -s 192.168.0.0/24 -p tcp --dport $adres -j ACCEPT
done
echo UDP:
for adres in $PORTYODBU
do
    echo $adres
    $IPTABLES -I FORWARD -s 192.168.0.0/24 -p udp --dport $adres -j ACCEPT
done
fi
################################################################################
if [ "$CONF_BLOKADA_BANKI" = "1" ]; then
echo Otwieramy dostep do stron
cat $STRONY | while read domena; do
echo -n $domena,
$IPTABLES -I FORWARD 1 -d 192.168.0.0/24 -s $domena -p tcp --dport 443 -j ACCEPT >
/dev/null 2> /dev/null
$IPTABLES -I FORWARD 1 -s 192.168.0.0/24 -d $domena -p tcp --dport 443 -j ACCEPT >
/dev/null 2> /dev/null
done
echo #
fi
################################################################################
if [ "$CONF_BLOKADA_GG" = "1" ]; then
echo Blokujemy adresy GaduGadu
$IPTABLES -I FORWARD -i eth1 -s 192.168.0.0/24 -p tcp -d 91.197.13.0/24 -j DROP
$IPTABLES -I FORWARD -i eth1 -s 192.168.0.0/24 -p tcp -d 217.17.41.82/28 -j DROP
$IPTABLES -I FORWARD -i eth1 -s 192.168.0.0/24 -p tcp -d 217.17.45.133/27 -j DROP
$IPTABLES -I FORWARD -i eth1 -s 192.168.0.0/24 -p tcp -d 217.17.46.250/24 -j DROP
fi
################################################################################
```