

Если вы видите что-то необычное, просто сообщите мне.

Пример настройки iptables

```
#!/iptables_rules.sh
#!/bin/bash

IPT="iptables"

## Внешний интерфейс
WAN=ens224
WAN_IP=ВАШ_внешний_IP
## Внутренний интерфейс
LAN1=ens192
LAN1_IP=ВАШ_внутренний_IP
LAN1_IP_RANGE=192.168.0.0/24
LAN2=IP_Jitsi

## Очищаем все цепочки перед применением новых правил
$IPT -F
$IPT -F -t nat
$IPT -F -t mangle
$IPT -X
$IPT -t nat -X
$IPT -t mangle -X

## Блокируем весь трафик, который не соответствует ни одному из правил
$IPT -P INPUT DROP
$IPT -P OUTPUT DROP
$IPT -P FORWARD DROP

## Разрешаем весь трафик в локалхост и локальной сети
$IPT -A INPUT -i lo -j ACCEPT
$IPT -A INPUT -i $LAN1 -j ACCEPT
$IPT -A OUTPUT -o lo -j ACCEPT
$IPT -A OUTPUT -o $LAN1 -j ACCEPT
```

Этот блок разрешает icmp-запросы (пинговать сервер) (опционально)

```
$IPT -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

```
$IPT -A INPUT -p icmp --icmp-type destination-unreachable -j ACCEPT
```

```
$IPT -A INPUT -p icmp --icmp-type time-exceeded -j ACCEPT
```

```
$IPT -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

Открываем доступ в интернет самому серверу

```
$IPT -A OUTPUT -o $WAN -j ACCEPT
```

```
#$IPT -A INPUT -i $WAN -j ACCEPT
```

Разрешаем все установленные соединения и дочерние от них

```
$IPT -A INPUT -p all -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
$IPT -A OUTPUT -p all -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
$IPT -A FORWARD -p all -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Защита от наиболее распространенных сетевых атак. (опционально)

Отбрасываем все пакеты без статуса (опционально)

```
$IPT -A INPUT -m state --state INVALID -j DROP
```

```
$IPT -A FORWARD -m state --state INVALID -j DROP
```

Блокируем нулевые пакеты (опционально)

```
$IPT -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
```

Закрываемся от syn-flood атак (опционально)

```
$IPT -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
```

```
$IPT -A OUTPUT -p tcp ! --syn -m state --state NEW -j DROP
```

Запрет доступа с определенных IP (опционально)

```
#$IPT -A INPUT -s ipaddress -j REJECT
```

Разрешаем доступ в интернет из локальной сети

```
$IPT -A FORWARD -i $LAN1 -o $WAN -j ACCEPT
```

Запрещаем доступ из интернета в локальную сеть (опционально)

```
#$IPT -A FORWARD -i $WAN -o $LAN1 -j REJECT
```

Чтобы в локальной сети был интернет включаем nat

```
$IPT -t nat -A POSTROUTING -o $WAN -s $LAN1_IP_RANGE -j MASQUERADE
```

Должен быть включен ip forwarding

Разрешаем ssh (порт 22 - это порт по умолчанию для ssh соединения, если вы его меняли, то обязательно значение 22 надо заменить своим, иначе будет потерян доступ к серверу)

```
$IPT -A INPUT -i $WAN -p tcp --dport 22 -j ACCEPT
```

Перенаправление трафика на сервер JITS

```
$IPT -A FORWARD -i $WAN -d $LAN2 -p tcp -m tcp --dport 80 -j ACCEPT
```

```
$IPT -A FORWARD -i $WAN -d $LAN2 -p tcp -m tcp --dport 443 -j ACCEPT
```

```
$IPT -A FORWARD -i $WAN -d $LAN2 -p udp -m udp --dport 10000 -j ACCEPT
```

```
$IPT -t nat -A PREROUTING -i $WAN -p tcp --dport 80 -j DNAT --to $LAN2
```

```
$IPT -t nat -A PREROUTING -i $WAN -p tcp --dport 443 -j DNAT --to $LAN2
```

```
$IPT -t nat -A PREROUTING -i $WAN -p udp --dport 10000 -j DNAT --to $LAN2
```

```
$IPT -t nat -A POSTROUTING -j MASQUERADE
```

Применить конфигу

```
chmod +x iptables_rules.sh
```

```
./iptables_rules.sh
```

```
iptables-save > /etc/iptables-conf/iptables_rules.ipv4
```

Revision #2

Created 11 June 2025 09:08:53 by gasick

Updated 11 June 2025 09:12:28 by gasick