

Конфигурация Firewalld

1) Установка firewalld:

```
# apt install firewalld
```

2) Включение firewalld:

```
# systemctl start firewalld
```

```
# systemctl enable firewalld
```

3) Добавление портов и служб в firewalld:

```
# firewall-cmd --permanent --add-port=2223/tcp
```

```
# firewall-cmd --permanent --add-port=80/tcp
```

```
# firewall-cmd --permanent --add-port=443/tcp
```

```
# firewall-cmd --permanent --add-port=5432/tcp
```

```
# firewall-cmd --permanent --add-port=3306/tcp
```

```
# firewall-cmd --permanent --add-port=6379/tcp
```

```
# firewall-cmd --permanent --add-port=27017/tcp
```

```
# firewall-cmd --permanent --add-port=8000/tcp
```

```
# firewall-cmd --permanent --add-port=3000/tcp
```

```
# firewall-cmd --permanent --add-port=4200/tcp
```

```
# firewall-cmd --permanent --add-port=8080/tcp
```

```
# firewall-cmd --permanent --add-port=3310/tcp
```

```
# firewall-cmd --permanent --add-port=3311/tcp
```

```
# firewall-cmd --permanent --add-port=3311/udp
```

```
# firewall-cmd --permanent --add-service=ntp
```

```
# firewall-cmd --permanent --add-service=ftp
```

```
# firewall-cmd --permanent --add-service=imap
```

```
# firewall-cmd --permanent --add-service=smtp
```

```
# firewall-cmd --permanent --add-service=ipp
```

```
# firewall-cmd --permanent --add-service=openvpn
```

4) Добавление пользовательского сервиса (OSPF):

```
# firewall-cmd --permanent --new-service=ospf
```

```
# firewall-cmd --permanent --service=ospf --set-short="OSPF"
```

```
# firewall-cmd --permanent --service=ospf --set-description="Open Shortest Path First (OSPF)"
```

```
# firewall-cmd --permanent --service=ospf --add-port=179/tcp
```

```
# firewall-cmd --permanent --service=ospf --add-port=179/udp
```

5) Настройка правил маскарadingа для исходящего трафика:

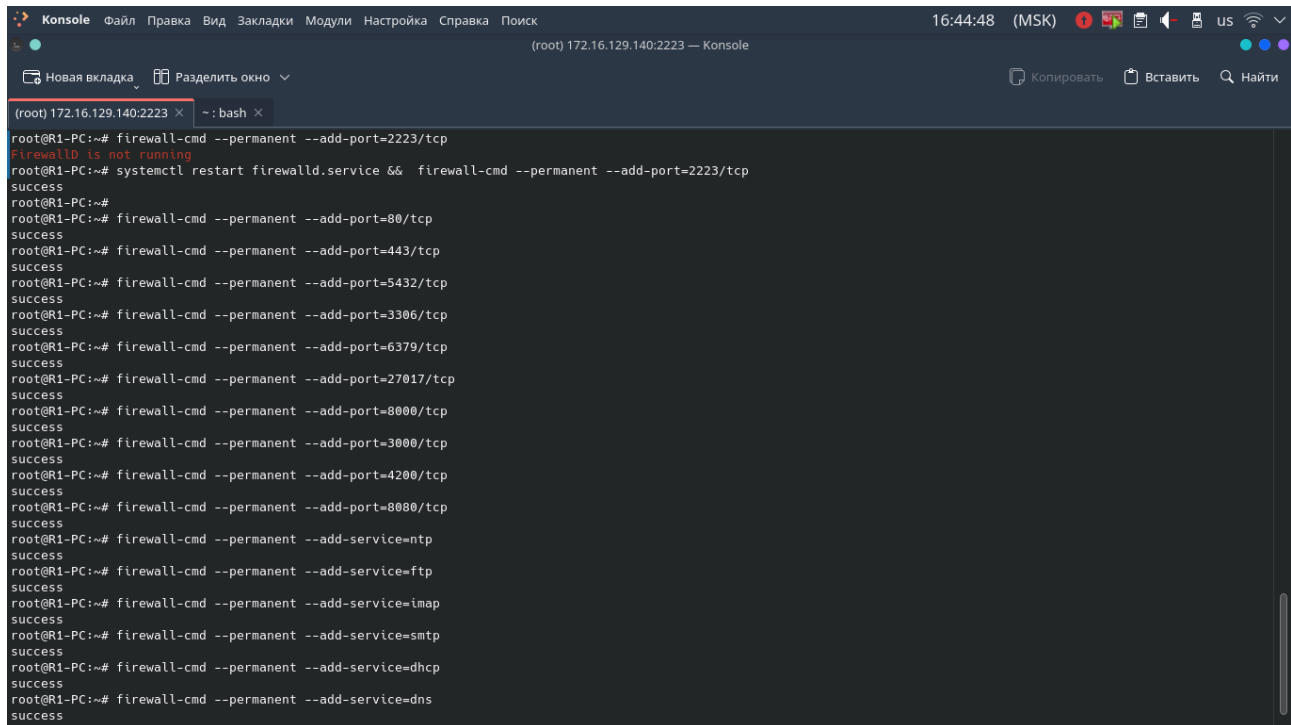
```
# firewall-cmd --permanent --add-masquerade
```

6) Применение изменений конфигурации firewalld:

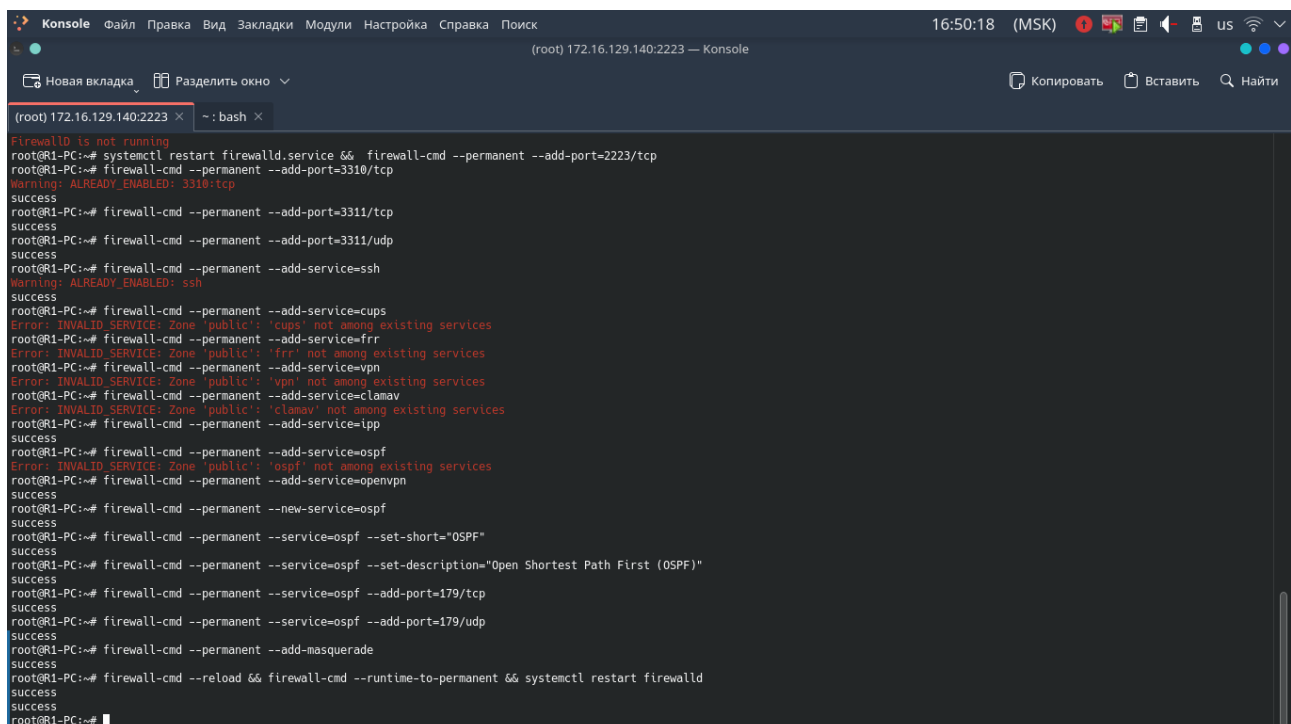
```
# firewall-cmd --reload
```

7) Сохранение временной конфигурации firewalld в постоянную и *перезагрузка firewalld*:

```
# firewall-cmd --runtime-to-permanent && systemctl restart firewalld
```



```
Konsole 16:44:48 (MSK) (root) 172.16.129.140:2223 — Konsole
( root) 172.16.129.140:2223 x ~: bash x
root@R1-PC:~# firewall-cmd --permanent --add-port=2223/tcp
Firewalld is not running
root@R1-PC:~# systemctl restart firewalld.service && firewall-cmd --permanent --add-port=2223/tcp
success
root@R1-PC:~#
root@R1-PC:~# firewall-cmd --permanent --add-port=80/tcp
success
root@R1-PC:~# firewall-cmd --permanent --add-port=443/tcp
success
root@R1-PC:~# firewall-cmd --permanent --add-port=5432/tcp
success
root@R1-PC:~# firewall-cmd --permanent --add-port=3306/tcp
success
root@R1-PC:~# firewall-cmd --permanent --add-port=6379/tcp
success
root@R1-PC:~# firewall-cmd --permanent --add-port=27017/tcp
success
root@R1-PC:~# firewall-cmd --permanent --add-port=8080/tcp
success
root@R1-PC:~# firewall-cmd --permanent --add-port=3000/tcp
success
root@R1-PC:~# firewall-cmd --permanent --add-port=4200/tcp
success
root@R1-PC:~# firewall-cmd --permanent --add-port=8080/tcp
success
root@R1-PC:~# firewall-cmd --permanent --add-service=ntp
success
root@R1-PC:~# firewall-cmd --permanent --add-service=ftp
success
root@R1-PC:~# firewall-cmd --permanent --add-service=imap
success
root@R1-PC:~# firewall-cmd --permanent --add-service=smtp
success
root@R1-PC:~# firewall-cmd --permanent --add-service=dhcp
success
root@R1-PC:~# firewall-cmd --permanent --add-service=dns
success
```



```
Konsole 16:50:18 (MSK) (root) 172.16.129.140:2223 — Konsole
( root) 172.16.129.140:2223 x ~: bash x
Firewalld is not running
root@R1-PC:~# systemctl restart firewalld.service && firewall-cmd --permanent --add-port=2223/tcp
root@R1-PC:~# firewall-cmd --permanent --add-port=3310/tcp
Warning: ALREADY_ENABLED: 3310/tcp
success
root@R1-PC:~# firewall-cmd --permanent --add-port=3311/tcp
success
root@R1-PC:~# firewall-cmd --permanent --add-port=3311/udp
success
root@R1-PC:~# firewall-cmd --permanent --add-service=ssh
Warning: ALREADY_ENABLED: ssh
success
root@R1-PC:~# firewall-cmd --permanent --add-service=cups
Error: INVALID_SERVICE: Zone 'public': 'cups' not among existing services
root@R1-PC:~# firewall-cmd --permanent --add-service=frr
Error: INVALID_SERVICE: Zone 'public': 'frr' not among existing services
root@R1-PC:~# firewall-cmd --permanent --add-service=vpn
Error: INVALID_SERVICE: Zone 'public': 'vpn' not among existing services
root@R1-PC:~# firewall-cmd --permanent --add-service=clamav
Error: INVALID_SERVICE: Zone 'public': 'clamav' not among existing services
root@R1-PC:~# firewall-cmd --permanent --add-service=ipsec
success
root@R1-PC:~# firewall-cmd --permanent --add-service=ospf
Error: INVALID_SERVICE: Zone 'public': 'ospf' not among existing services
root@R1-PC:~# firewall-cmd --permanent --add-service=openvpn
success
root@R1-PC:~# firewall-cmd --permanent --new-service=ospf
success
root@R1-PC:~# firewall-cmd --permanent --service=ospf --set-short="OSPF"
success
root@R1-PC:~# firewall-cmd --permanent --service=ospf --set-description="Open Shortest Path First (OSPF)"
success
root@R1-PC:~# firewall-cmd --permanent --service=ospf --add-port=179/tcp
success
root@R1-PC:~# firewall-cmd --permanent --service=ospf --add-port=179/udp
success
root@R1-PC:~# firewall-cmd --permanent --add-masquerade
success
root@R1-PC:~# firewall-cmd --reload && firewall-cmd --runtime-to-permanent && systemctl restart firewalld
success
root@R1-PC:~#
```

Настройка правил брандмауэра

1) Установка пакета iptables-persistent:

```
# apt install iptables-persistent
```

2) Блокировка порта 23 TCP с помощью iptables:

```
# iptables -A INPUT -p tcp --dport 23 -j DROP
```

3) Разрешение входящих пакетов по SSH:

```
# iptables -A INPUT -p tcp --dport 2223 -j ACCEPT
```

4) Разрешение входящих пакетов только с определенного IP-адреса:

```
# iptables -A INPUT -s 1.1.1.1 -j ACCEPT
```

```
# iptables -A INPUT -s 2.2.2.1 -j ACCEPT
```

```
# iptables -A INPUT -s 2.2.2.100 -j ACCEPT
```

```
# iptables -A INPUT -s 172.28.14.252 -j ACCEPT
```

```
# iptables -A INPUT -s 172.16.0.33 -j ACCEPT
```

```
# iptables -A INPUT -s 172.16.0.42 -j ACCEPT
```

```
# iptables -A INPUT -s 192.168.0.60 -j ACCEPT
```

5) Заблокировать все остальные входящие пакеты:

```
# iptables -A INPUT -j DROP
```

6) Разрешить доступ к VPN-серверу только с определенных IP-адресов:

```
# iptables -A INPUT -p gre -s 172.16.0.42 -j ACCEPT
```

```
# iptables -A INPUT -p gre -s 192.168.0.60 -j ACCEPT
```

```
# iptables -A INPUT -p gre -s 10.0.0.1 -j ACCEPT
```

7) Заблокировать доступ к VPN-серверу с остальных IP-адресов:

```
# iptables -A INPUT -p gre -j DROP
```

8) Разрешить перенаправление пакетов между интерфейсами:

```
# iptables -A FORWARD -j ACCEPT
```

9) Ограничить количество соединений от одного IP-адреса:

```
# iptables -A INPUT -p tcp --syn -m connlimit --connlimit-above 5 -j REJECT
```

10) Установка ограничения на скорость соединений:

```
# iptables -A INPUT -p tcp --match limit --limit 1/second -j ACCEPT
```

11) Отбросить все остальные пакеты с флагом SYN:

```
# iptables -A INPUT -p tcp --tcp-flags SYN SYN -j DROP
```

12) Сохранение правил iptables в файл:

```
# iptables-save > /etc/iptables/rules.v4
```

Настройка сетевых правил

1) Настройка правила логирования TCP трафика с помощью firewalld:

```
# firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" protocol value="tcp" log prefix="TCP_IN: " level="info"' --permanent
```

2) Создание зоны для внутренних сетей:

```
# firewall-cmd --permanent --new-zone=internal_zone
```

3) Назначение интерфейса для зоны внутренних сетей:

```
# firewall-cmd --permanent --zone=internal_zone --add-interface=ens33
```

4) Добавление правил для доступа по SSH через интерфейс ens33 в зону internal_zone:

```
# firewall-cmd --permanent --zone=internal_zone --add-port=2223/tcp
```

5) Включение NAT для зоны внутренних сетей:

```
# firewall-cmd --permanent --zone=internal_zone --add-masquerade
```

6) Применение изменений конфигурации firewalld:

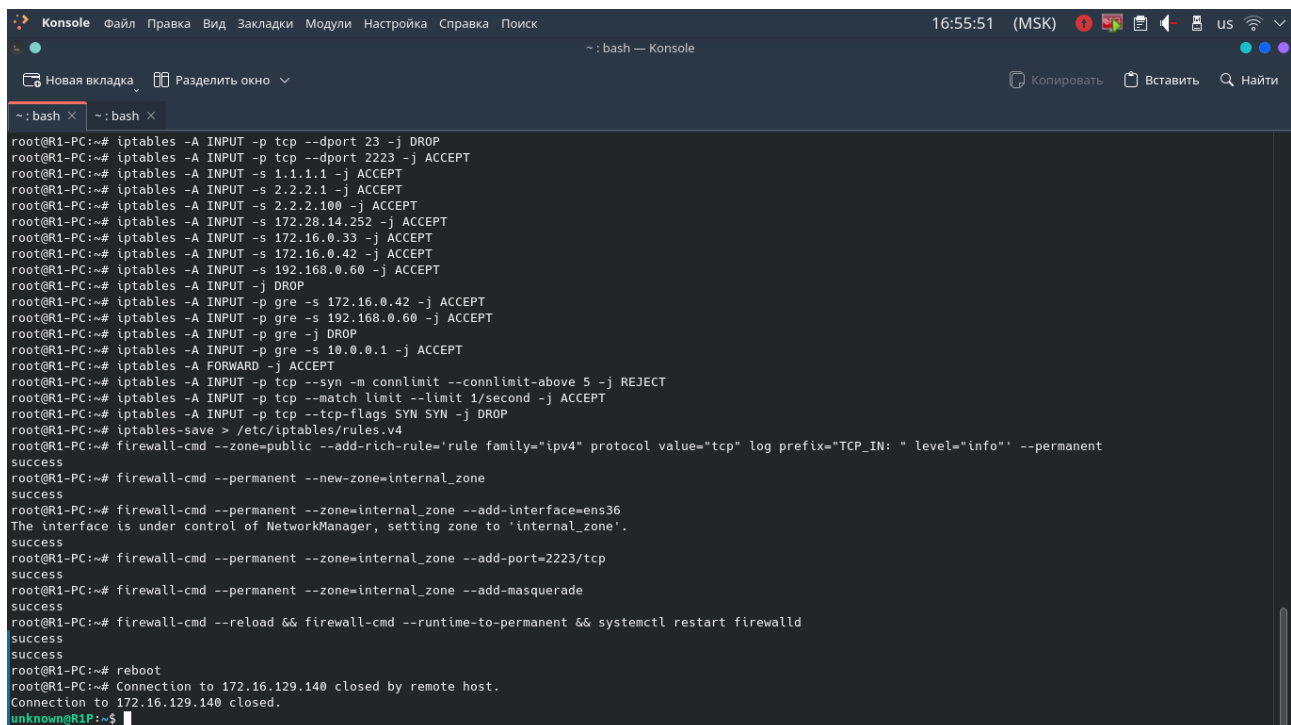
```
# firewall-cmd --reload
```

7) Сохранение временной конфигурации firewalld в постоянную:

```
# firewall-cmd --runtime-to-permanent
```

8) Перезагрузка firewalld:

```
# systemctl restart firewalld
```



```
root@R1-PC:~# iptables -A INPUT -p tcp --dport 23 -j DROP
root@R1-PC:~# iptables -A INPUT -p tcp --dport 2223 -j ACCEPT
root@R1-PC:~# iptables -A INPUT -s 1.1.1.1 -j ACCEPT
root@R1-PC:~# iptables -A INPUT -s 2.2.2.1 -j ACCEPT
root@R1-PC:~# iptables -A INPUT -s 2.2.2.100 -j ACCEPT
root@R1-PC:~# iptables -A INPUT -s 172.28.14.252 -j ACCEPT
root@R1-PC:~# iptables -A INPUT -s 172.16.0.33 -j ACCEPT
root@R1-PC:~# iptables -A INPUT -s 172.16.0.42 -j ACCEPT
root@R1-PC:~# iptables -A INPUT -s 192.168.0.60 -j ACCEPT
root@R1-PC:~# iptables -A INPUT -j DROP
root@R1-PC:~# iptables -A INPUT -p gre -s 172.16.0.42 -j ACCEPT
root@R1-PC:~# iptables -A INPUT -p gre -s 192.168.0.60 -j ACCEPT
root@R1-PC:~# iptables -A INPUT -p gre -j DROP
root@R1-PC:~# iptables -A INPUT -p gre -s 10.0.0.1 -j ACCEPT
root@R1-PC:~# iptables -A FORWARD -j ACCEPT
root@R1-PC:~# iptables -A INPUT -p tcp --syn -m connlimit --connlimit-above 5 -j REJECT
root@R1-PC:~# iptables -A INPUT -p tcp --match limit --limit 1/second -j ACCEPT
root@R1-PC:~# iptables -A INPUT -p tcp --tcp-flags SYN SYN -j DROP
root@R1-PC:~# iptables-save > /etc/iptables/rules.v4
root@R1-PC:~# firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" protocol value="tcp" log prefix="TCP_IN: " level="info"' --permanent
success
root@R1-PC:~# firewall-cmd --permanent --new-zone=internal_zone
success
root@R1-PC:~# firewall-cmd --permanent --zone=internal_zone --add-interface=ens36
The interface is under control of NetworkManager, setting zone to 'internal_zone'.
success
root@R1-PC:~# firewall-cmd --permanent --zone=internal_zone --add-port=2223/tcp
success
root@R1-PC:~# firewall-cmd --permanent --zone=internal_zone --add-masquerade
success
root@R1-PC:~# firewall-cmd --reload && firewall-cmd --runtime-to-permanent && systemctl restart firewalld
success
success
root@R1-PC:~# reboot
root@R1-PC:~# Connection to 172.16.129.140 closed by remote host.
Connection to 172.16.129.140 closed.
unknown@R1P:~$
```

Примечание:

Дабы минимизировать количество работы было решено настроить firewalld и iptables одинаково на всех серверах, даже если на некоторых серверах это не требуется.