Установим Firevalld

Машина RTR-L

Установка

```
root@debian:~# apt update
```

```
root@debian:~# apt install firewalld
```

Проверим работает ли он

```
root@debian:~# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2022-10-30 12:44:23 MSK; 26min ago
       Docs: man:firewalld(1)
   Main PID: 1229 (firewalld)
      Tasks: 2 (limit: 2296)
     Memory: 28.4M
        CPU: 366ms
     CGroup: /system.slice/firewalld.service
             └─1229 /usr/bin/python3 /usr/sbin/firewalld --nofork --nopid

окт 30 12:44:23 debian systemd[1]: Starting firewalld - dynamic firewall daemon...
окт 30 12:44:23 debian systemd[1]: Started firewalld - dynamic firewall daemon.
```

Проверим активные зоны. (если они есть то удаляем их)

```
root@debian:~# firewall-cmd --get-active-zones _
```

Покажет все зоны которые есть и можно настроить.

```
root@debian:~# firewall-cmd --list-all-zones_
```

Теперь создадим свои зоны внутреннюю(trusted) и внешнюю(external)

```
root@debian:~# firewall-cmd --zone=trusted --add-interface=ens33
```

```
root@debian:~# firewall-cmd --zone=external --add-interface=ens37
```

Проверим всё ли создалось.

```
root@debian:~# firewall-cmd --get-active-zones
external
  interfaces: ens37
trusted
  interfaces: ens33
```

Теперь настроим внешнюю зону.

Разрешим доступ к сервисам “http”, “https” и “DNS”.

```
root@debian:~# firewall-cmd --zone=external --add-service=http_
```

```
root@debian:~# firewall-cmd --zone=external --add-service=https
```

```
root@debian:~# firewall-cmd --zone=external --add-service=dns
```

Теперь необходимо выполнить проброс портов.

Пробросим порт SSH(порты 2222,22,80)(протокол tcp)

192.168.103.100 это адрес WEB-L

```
root@debian:~# firewall-cmd --zone=external --add-forward-port=port=2222:proto=tcp:toport=22:toaddr=
192.168.103.100
-------
root@debian:~# firewall-cmd --zone=external --add-forward-port=port=80:proto=tcp:toport=80:toaddr=19
2.168.103.100
```

Далее пробросим порт DNS (53 порт)(протокол udp)

192.168.103.200 это адрес SRV

```
root@debian:~# firewall-cmd --zone=external --add-forward-port=port=53:proto=udp:toport=53:toaddr=19
2.168.103.200
```

Также добавим на будуще порт VPN.(т.к. VPN работает на произвольном порту, то можно указать произвольный порт в данном случае 12345)

```
root@debian:~# firewall-cmd --zone=external --add-port=12345/udp
```

Проверим наши настройки.

```
root@debian:~# firewall-cmd --zone=external --list-all
```

Должно выглядеть примерно так.

```
external (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens37
  sources:
  services: dns http https ssh
  ports: 12345/udp
  protocols:
  forward: no
  masquerade: yes
  forward-ports:
        port=2222:proto=tcp:toport=22:toaddr=192.168.103.100
        port=80:proto=tcp:toport=80:toaddr=192.168.103.100
        port=53:proto=udp:toport=53:toaddr=192.168.103.200
  source-ports:
  icmp-blocks:
  rich rules:
root@debian:~#
```

Сохраним настройки.

```
root@debian:~# firewall-cmd --runtime-to-permanent_
```

И перезагружаем Firewall.

```
root@debian:~# firewall-cmd --reload
```

Машина RTR-R

Установка

```
root@debian:~# apt update
```

```
root@debian:~# apt install firewalld
```

Проверим работает ли он

```
root@debian:~# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2022-10-30 12:44:23 MSK; 26min ago
       Docs: man:firewalld(1)
   Main PID: 1229 (firewalld)
      Tasks: 2 (limit: 2296)
     Memory: 28.4M
        CPU: 366ms
     CGroup: /system.slice/firewalld.service
             └─1229 /usr/bin/python3 /usr/sbin/firewalld --nofork --nopid

окт 30 12:44:23 debian systemd[1]: Starting firewalld - dynamic firewall daemon...
окт 30 12:44:23 debian systemd[1]: Started firewalld - dynamic firewall daemon.
```

Проверим активные зоны. (если они есть то удаляем их)

```
root@debian:~# firewall-cmd --get-active-zones _
```

Покажет все зоны которые есть и можно настроить.

```
root@debian:~# firewall-cmd --list-all-zones_
```

Теперь создадим свои зоны внутреннюю(trusted) и внешнюю(external)

```
root@debian:~# firewall-cmd --zone=trusted --add-interface=ens33
```

```
root@debian:~# firewall-cmd --zone=external --add-interface=ens37
```

Проверим всё ли создалось.

```
root@debian:~# firewall-cmd --get-active-zones
external
  interfaces: ens37
trusted
  interfaces: ens33
```

Теперь настроим внешнюю зону.

Разрешим доступ к сервисам “http”, “https” и “DNS”.

```
root@debian:~# firewall-cmd --zone=external --add-service=http_
```

```
root@debian:~# firewall-cmd --zone=external --add-service=https
```

```
root@debian:~# firewall-cmd --zone=external --add-service=dns
```

Теперь необходимо выполнить проброс портов.

Пробросим порт SSH(порты 2244,22,80)(протокол tcp)

172.16.103.100 это адрес WEB-R

```
root@debian:~# firewall-cmd --zone=external --add-forward-port=port=2244:proto=tcp:toport=22:toaddr=
172.16.103.100
```

```
root@debian:~# firewall-cmd --zone=external --add-forward-port=port=80:proto=tcp:toport=80:toaddr=17
2.16.103.100
```

На этой машине не нужно пробрасывать порт DNS.

Также добавим на будущие порт VPN.(т.к. VPN работает на произвольном порту, то можно указать произвольный порт в данном случае 12345)

```
root@debian:~# firewall-cmd --zone=external --add-port=12345/udp
```

Проверим наши настройки.

```
root@debian:~# firewall-cmd --zone=external --list-all
```

Должно выглядеть примерно так.

```
external (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens37
  sources:
  services: dns http https ssh
  ports: 12345/udp
  protocols:
  forward: no
  masquerade: yes
  forward-ports:
        port=2244:proto=tcp:toport=22:toaddr=172.16.103.100
        port=80:proto=tcp:toport=80:toaddr=172.16.103.100
  source-ports:
  icmp-blocks:
  rich rules:
```

Сохраним настройки.

```
root@debian:~# firewall-cmd --runtime-to-permanent_
```

И перезагружаем Firewall.

```
root@debian:~# firewall-cmd --reload
```