

Фильтр пакетов

Лабораторная работа №13

Казначеев С.И.

25 ноября 2025

Российский университет дружбы народов, Москва, Россия

Информация

::::::::::: {.columns align=center} :: {.column width="70%"}
:::

- Казначеев Сергей Ильич
- Студент
- Российский университет дружбы народов
- [1132240693@pfur.ru] :: {.column width="30%"}
::

Цель работы

Получить навыки настройки пакетного фильтра в Linux.

1. Используя `firewall-cmd`: – определить текущую зону по умолчанию; – определить доступные для настройки зоны; – определить службы, включённые в текущую зону; – добавить сервер VNC в конфигурацию брандмауэра.
2. Используя `firewall-config`: – добавьте службы `http` и `ssh` в зону `public`; – добавьте порт `2022` протокола `UDP` в зону `public`; – добавьте службу `ftp`.
3. Выполните задание для самостоятельной работы (раздел 13.5).

Выполнение лабораторной работы

Перейдем в супер пользователя

```
[sikaznacheev@localhost ~]$ su -  
Пароль:
```

Рис. 1: 1

Определение текищей зоны

После чего определим текущую зону

```
[root@localhost ~]# firewall-cmd --get-default-zone  
public
```

Рис. 2: 2

Определение доступной зоны

Определим доступные зоны

```
[root@localhost ~]# firewall-cmd --get-zones  
block dmz drop external home internal nm-shared public trusted work
```

Рис. 3: 3

Просмотр служб на нашем компьютере

Затем просмотрим службы доступные на нашем компьютере

```
[root@localhost ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacula-client
bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpgsql grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipp-sec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodbs mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmpd snmpd-trap snmptrap spiderOak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tiny tor-socks transmission transmission-client upnp-client vdsman vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsman-xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
```

Рис. 4: 4

Определяем доступные службы

Определим доступные службы в текущей зоне

```
[root@localhost ~]# firewall-cmd --list-services  
cockpit dhcpcv6-client ssh
```

Рис. 5: 5

Сравнение двух команд

После чего сравним вывод информации при использовании двух команд первая команда
firewall-cmd –list-all, вторая firewall-cmd –list-all –zone=public

```
[root@localhost ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@localhost ~]# i firewall-cmd --list-all --zone=public
bash: i firewall-cmd: команда не найдена...
[root@localhost ~]# firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
```

Добавление сервера VNC

Далее добавим сервер VNC в конфигурацию брандмауэра

```
[root@localhost ~]# firewall-cmd --add-service=vnc-server  
success
```

Рис. 7: 7

Проверка добавление сервера

И проверим добавился или нет

```
[root@localhost ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Запуск службы firewalld

После чего перезапустим службу firewalld

```
[root@localhost ~]# systemctl restart firewalld
```

Рис. 9: 9

Проверка vnc-server в конфигурации

Затем проверим есть ли vnc-server в конфигурации и мы обнаружим, что vnc-server больше не указан это из за того что не был постоянным

```
[root@localhost ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 10: 10

Добавление службы vnc-server только уже постоянной

Добавим службу vnc-server ещё раз, но на этот раз сделав её постоянной

```
[root@localhost ~]# firewall-cmd --add-service=vnc-server --permanent  
success
```

Рис. 11: 11

Проверка vnc-server в конфигурации

После чего проверим наличие vnc-server в конфигурации

```
[root@localhost ~]# firewall-cmd --list-all
public (active)
    target: default
    icmp-block-inversion: no
    interfaces: enp0s3
    sources:
    services: cockpit dhcpcv6-client ssh
    ports:
    protocols:
    forward: yes
    masquerade: no
    forward-ports:
    source-ports:
    icmp-blocks:
    rich rules:
```

Проверка vnc-server после перезагрузки firewalld

Теперь проверим перезагрузив конфигурацию firewalld

```
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# firewall-cmd --list-all
public (active)
    target: default
    icmp-block-inversion: no
    interfaces: enp0s3
    sources:
    services: cockpit dhcpcv6-client ssh vnc-server
    ports:
    protocols:
    forward: yes
    masquerade: no
    forward-ports:
    source-ports:
    icmp-blocks:
    rich rules:
```

Добавление конфигурации межсетевого экрана

Добавим в конфигурацию межсетевого экрана порт 2022 протокола TCP, после чего перезагрузим конфигурацию firewalld и проверим что порт добавился в конфигурацию

```
[root@localhost ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# firewall-cmd --list-all
public (active)
    target: default
    icmp-block-inversion: no
    interfaces: enp0s3
    sources:
    services: cockpit dhcpcv6-client ssh vnc-server
    ports: 2022/tcp
    protocols:
    forward: yes
    masquerade: no
    forward-ports:
    source-ports:
    icmp-blocks:
    rich rules:
```

Запускт интерфейса GUI firewall-config

После чего откроем терминал и под учетной записью пользователя запустим интерфейс GUI firewall-config

```
[sikaznacheev@localhost ~]$ firewall-config
```

Рис. 15: 15

Настройка интерфейса GUI firewall-config

Далее рядом с параметром Configuration откроем раскрывающийся список и выберем Permanent, после чего выберем зону public и отметим службы http, https и ftp

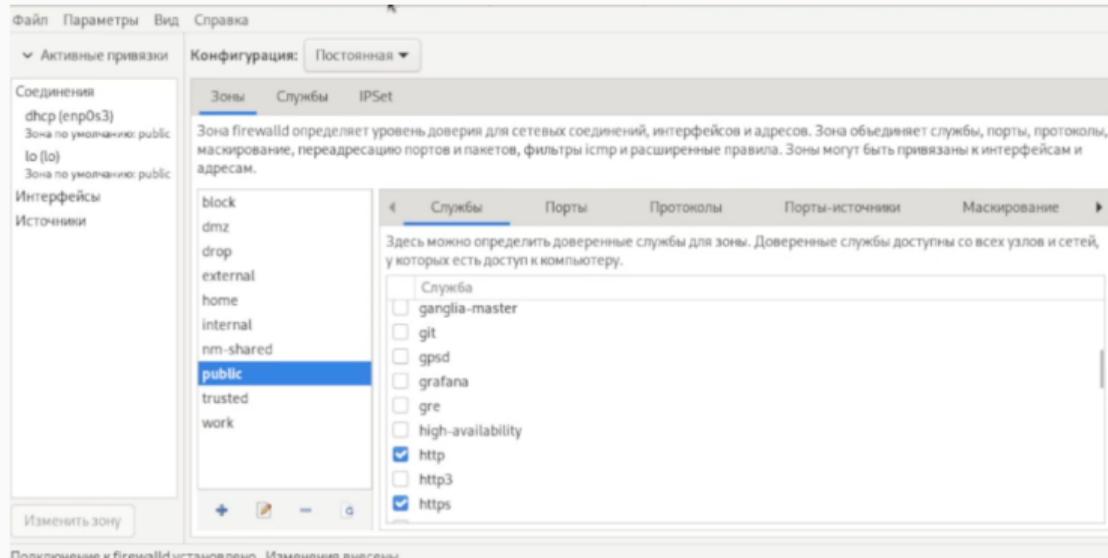


Рис. 16: 16

Скрин



Рис. 17: 17

Добавление порта через GUI firewall-config

Полче чего выберем вкладку Ports и добавим порт 2022 udp

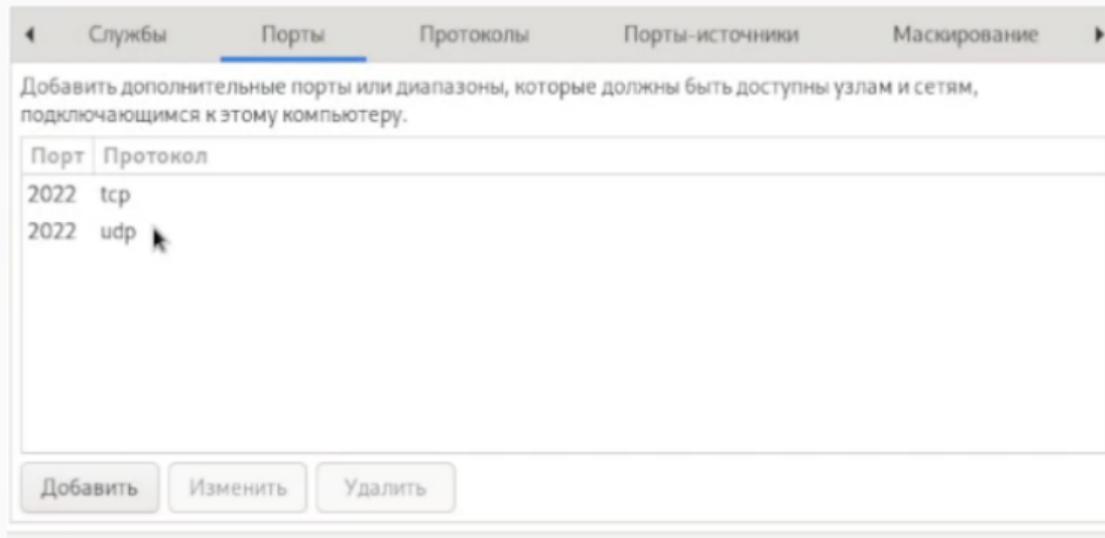


Рис. 18: 18

Проверка всех изменений

И проверим все изменения которые мы только что внесли

```
[sikaznacheev@localhost ~]$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 19: 19

Перезапуск конфигурации firewall-cmd

Перезапустим конфигурацию firewall-cmd для того, чтобы изменения вступили в силу и проверим это

```
[sikaznacheev@localhost ~]$ firewall-cmd --reload
success
[sikaznacheev@localhost ~]$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ftp http https ssh vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Создадим конфигурацию межсетевого экрана которая позволяет получить доступ к следующим службам telnet,imap, pop3, smtp

```
[sikaznacheev@localhost ~]$ firewall-cmd --add-service=telnet --permanent  
success
```

Рис. 21: 21

Добавляем imap, pop3, smtp

Добавляем imap, pop3, smtp

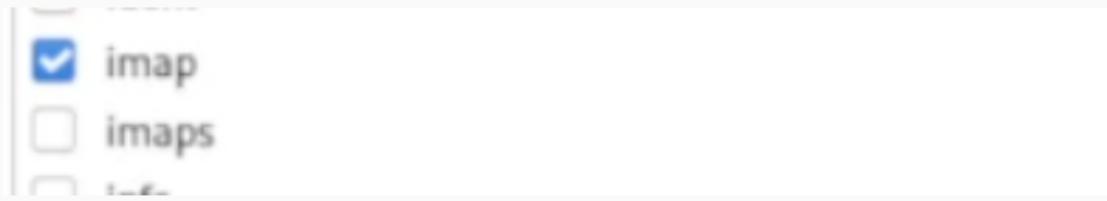


Рис. 22: 22

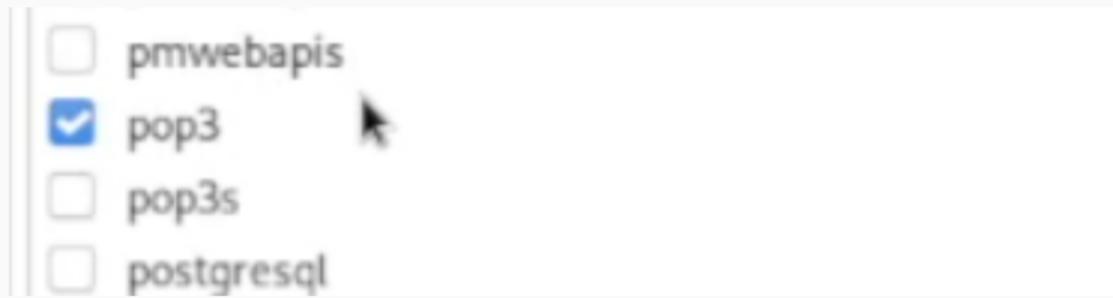


Рис. 23: 23

Скрин 3

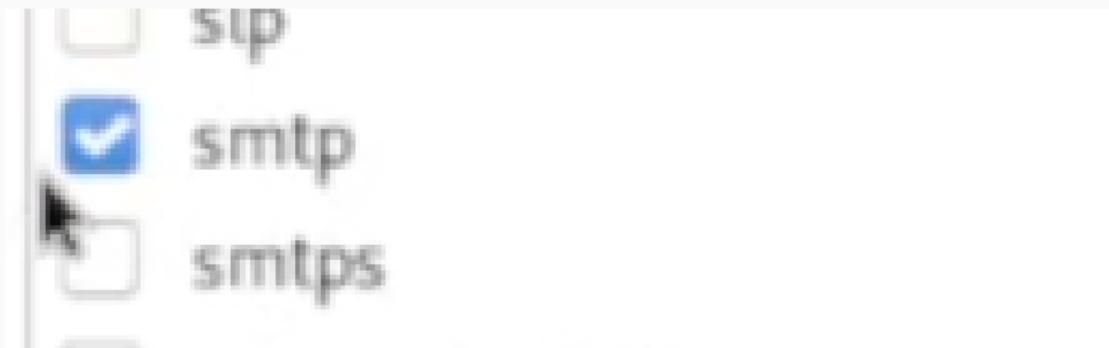


Рис. 24: 24

Проверка что конфигурация является постоянной

И проверяем, что конфигурация является постоянной и будет активирована после перезагрузки компьютера

```
[sikaznacheev@localhost ~]$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ftp http https imap pop3 smtp ssh telnet vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 25: 25

Контрольные вопросы 1

1. Какая служба должна быть запущена перед началом работы с менеджером конфигурации брандмауэра firewall-config?

Ответ - firewall должна быть запущена

Контрольные вопросы 2

2. Какая команда позволяет добавить UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию?

Ответ - `firewall-cmd --add-port=2355/udp`

Контрольные вопросы 3

3. Какая команда позволяет показать всю конфигурацию брандмауэра во всех зонах?

Ответ - `firewall-cmd --list-all-zones`

Контрольные вопросы 4

4. Какая команда позволяет удалить службу vnc-server из текущей конфигурации брандмауэра?

Ответ - `firewall-cmd --remove-service=vnc-server`

Контрольные вопросы 5

5. Какая команда firewall-cmd позволяет активировать новую конфигурацию, добавленную опцией –permanent?

Ответ - `firewall-cmd --reload`

Контрольные вопросы 6

6. Какой параметр firewall-cmd позволяет проверить, что новая конфигурация была добавлена в текущую зону и теперь активна?

Ответ - `firewall-cmd --list-all`

Контрольные вопросы 7

7. Какая команда позволяет добавить интерфейс eno1 в зону public?

Ответ - firewall-cmd –zone=public –add-interface=eno1

Контрольные вопросы 8

8. Если добавить новый интерфейс в конфигурацию брандмауэра, пока не указана зона, в какую зону он будет добавлен?

Ответ - интерфейс попадет в зону по умолчанию (public)

Выводы

В ходе выполнения лабораторной работы я получил навыки настройки пакетного фильтра в Linux.