

Лабораторная работа №13

Фильтр пакетов

Комягин Андрей Николаевич

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Ответы на контрольные вопросы	15
4	Выводы	17

Список иллюстраций

2.1	Текущая и доступные зоны	6
2.2	Доступные службы	7
2.3	Доступные службы в текущей зоне	7
2.4	Сравнение двух выдач информации	8
2.5	Добавление сервера в конфигурацию	8
2.6	Перезапуск службы firewalld	9
2.7	Проверка наличия сервера в конфигурации	9
2.8	Добавление службы в конфигурацию на постоянной основе . . .	9
2.9	Перезагрузка firewalld и просмотр конфигурации времени выполнения	10
2.10	Добавление в конфигурацию порт	10
2.11	Открытый интерфейс GUI firewall-config	11
2.12	Параметр Configuration на Permanent	11
2.13	Включение служб http, https и ftp	12
2.14	Добавление порта	12
2.15	Вывод информации	13
2.16	Проверка применения изменений	13
2.17	Добавление telnet	14
2.18	Добавление почт	14

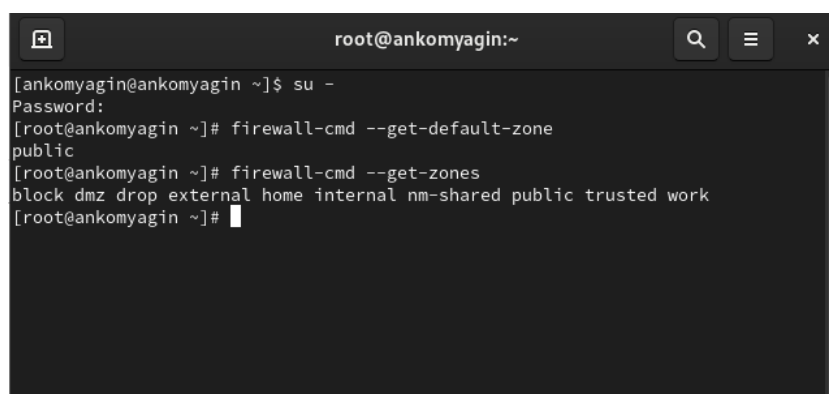
List of Tables

1 Цель работы

Получение навыков настройки пакетного фильтра в Linux.

2 Выполнение лабораторной работы

Получим полномочия администратора. Определим текущую зону по умолчанию. Определим доступные зоны. (рис. 2.1).



```
root@ankomyagin:~  
[ankomyagin@ankomyagin ~]$ su -  
Password:  
[root@ankomyagin ~]# firewall-cmd --get-default-zone  
public  
[root@ankomyagin ~]# firewall-cmd --get-zones  
block dmz drop external home internal nm-shared public trusted work  
[root@ankomyagin ~]#
```

Рис. 2.1: Текущая и доступные зоны

Посмотрим службы, доступные на компьютере. (рис. 2.2).

```
root@ankomyagin:~  
[ankomyagin@ankomyagin ~]$ su -  
Password:  
[root@ankomyagin ~]# firewall-cmd --get-default-zone  
public  
[root@ankomyagin ~]# firewall-cmd --get-zones  
block dmz drop external home internal nm-shared public trusted work  
[root@ankomyagin ~]# firewall-cmd --get-services  
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit au  
sweissapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitco  
in-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine check  
mk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dh  
cpv6-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-replica  
tion freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability h  
ttp http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin  
kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane k  
ube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-servic  
es kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap lda  
ps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix m  
dns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios  
-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovi  
rt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheu  
s-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis re  
dis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips  
slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squ  
id sssd ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy syslog syslog-  
tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsml vnc-server warpi  
nator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-  
udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerot  
ier  
[root@ankomyagin ~]#
```

Рис. 2.2: Доступные службы

Определим доступные службы в текущей зоне. (рис. 2.3).

```
root@ankomyagin:~  
[root@ankomyagin ~]# firewall-cmd --list-services  
cockpit dhcpv6-client ssh  
[root@ankomyagin ~]#
```

Рис. 2.3: Доступные службы в текущей зоне

Сравним результаты вывода информации при использовании команд. (рис. 2.4). Вывод одинаков

```
[root@ankomyagin ~]# 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@ankomyagin ~]# firewall-cmd --list-all --zone=public
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@ankomyagin ~]#
```

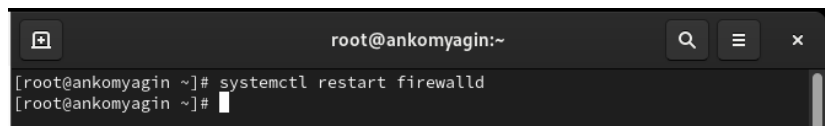
Рис. 2.4: Сравнение двух выдач информации

Добавим сервер VNC в конфигурацию брандмауэра. Проверим, добавился ли vnc-server в конфигурацию. (добавился) (рис. 2.5).

```
root@ankomyagin:~
[root@ankomyagin ~]# firewall-cmd --add-service=vnc-server
success
[root@ankomyagin ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@ankomyagin ~]#
```

Рис. 2.5: Добавление сервера в конфигурацию

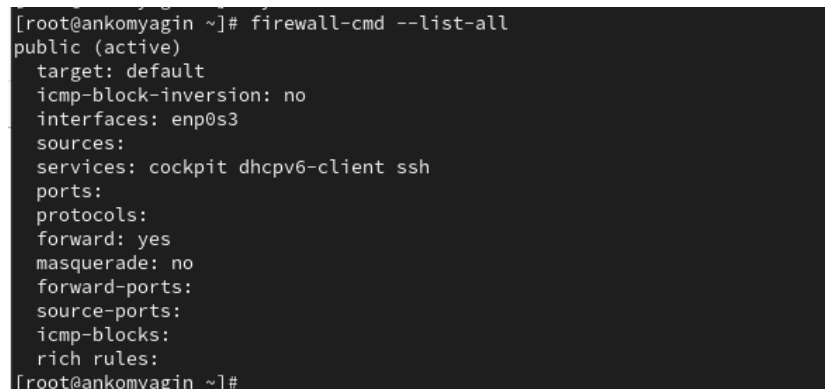
Перезапустим службу firewalld. (рис. 2.6).



```
root@ankomyagin:~  
[root@ankomyagin ~]# systemctl restart firewalld  
[root@ankomyagin ~]#
```

Рис. 2.6: Перезапуск службы firewalld

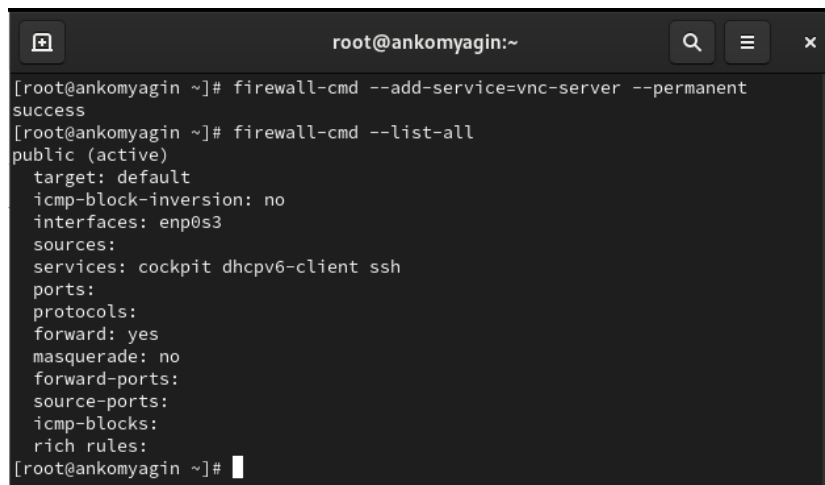
Проверим, есть ли vnc-server в конфигурации. (нет)(рис. 2.7).



```
[root@ankomyagin ~]# 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@ankomyagin ~]#
```

Рис. 2.7: Проверка наличия сервера в конфигурации

Добавим службу vnc-server ещё раз, но на этот раз сделайте её постоянной. Проверим наличие vnc-server в конфигурации. (рис. 2.8).

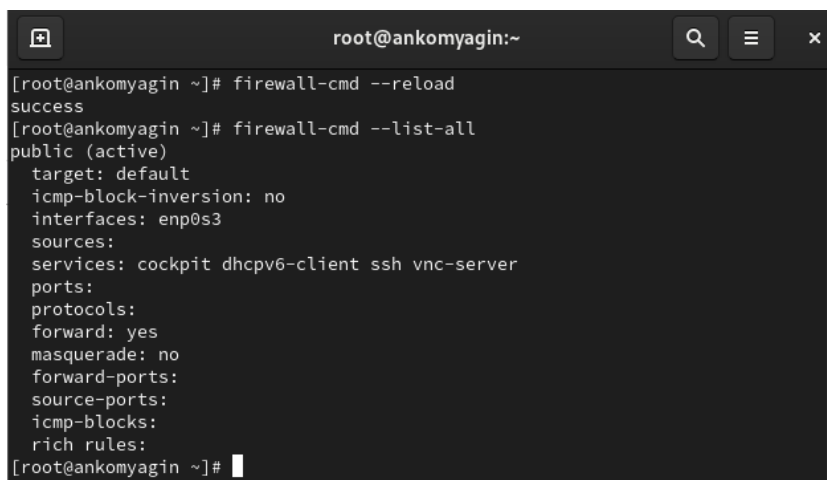


```
root@ankomyagin:~  
[root@ankomyagin ~]# firewall-cmd --add-service=vnc-server --permanent  
success  
[root@ankomyagin ~]# firewall-cmd --list-all  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services: cockpit dhcpv6-client ssh  
  ports:  
  protocols:  
  forward: yes  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
[root@ankomyagin ~]#
```

Рис. 2.8: Добавление службы в конфигурацию на постоянной основе

Служба не появилась сразу, при использовании опции --permanent нужно перезагрузить конфигурацию firewalld.

Перезагрузим конфигурацию firewalld и посмотрим конфигурацию времени выполнения (рис. 2.9).

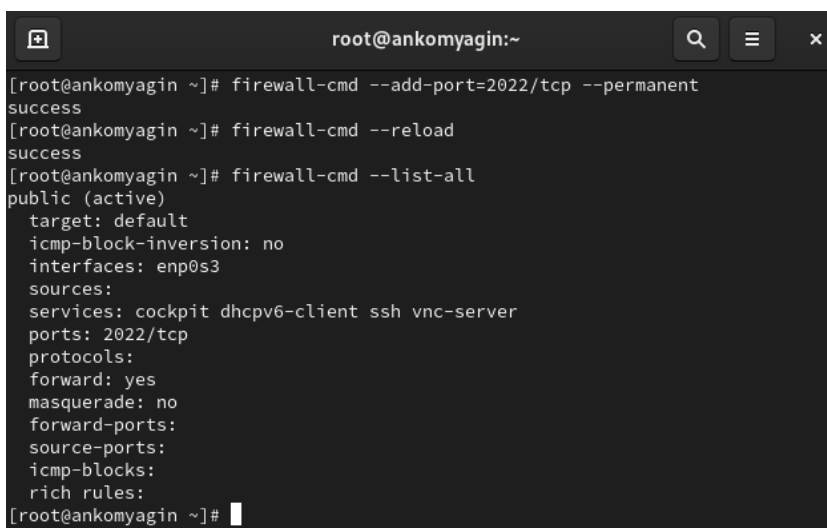


```
root@ankomyagin:~  
[root@ankomyagin ~]# firewall-cmd --reload  
success  
[root@ankomyagin ~]# firewall-cmd --list-all  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services: cockpit dhcpv6-client ssh vnc-server  
  ports:  
  protocols:  
  forward: yes  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
[root@ankomyagin ~]#
```

Рис. 2.9: Перезагрузка firewalld и просмотр конфигурации времени выполнения

Сервер vnc отображается в конфигурации.

Добавим в конфигурацию межсетевого экрана порт 2022 протокола TCP. Затем перезагрузим конфигурацию firewalld. Проверим, что порт добавлен в конфигурацию. (рис. 2.10).



```
root@ankomyagin:~  
[root@ankomyagin ~]# firewall-cmd --add-port=2022/tcp --permanent  
success  
[root@ankomyagin ~]# firewall-cmd --reload  
success  
[root@ankomyagin ~]# firewall-cmd --list-all  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services: cockpit dhcpv6-client ssh vnc-server  
  ports: 2022/tcp  
  protocols:  
  forward: yes  
  masquerade: no  
  forward-ports:  
  source-ports:  
  icmp-blocks:  
  rich rules:  
[root@ankomyagin ~]#
```

Рис. 2.10: Добавление в конфигурацию порт

Откроем терминал и под учётной записью пользователя запустим интерфейс

GUI firewall-config. (рис. 2.11).

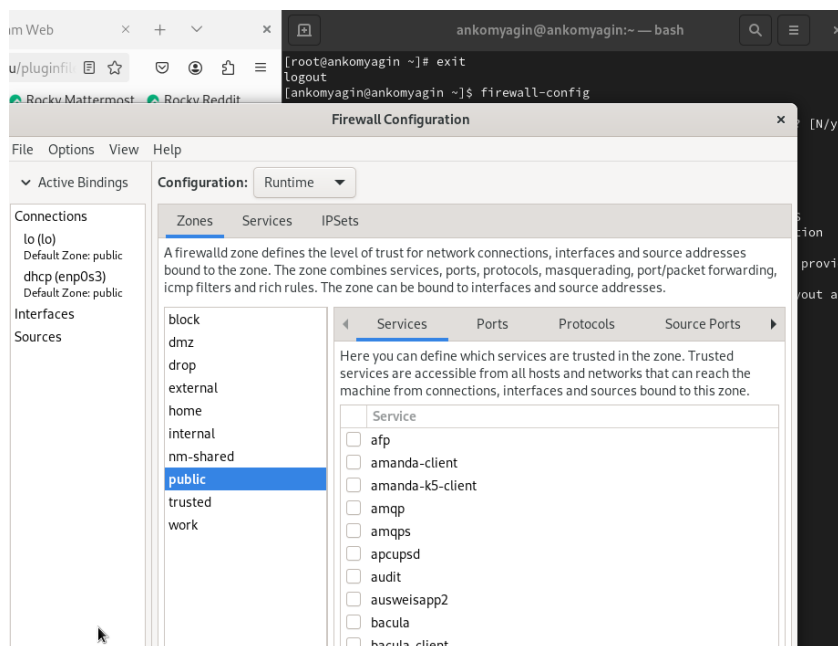


Рис. 2.11: Открытый интерфейс GUI firewall-config

Нажмём выпадающее меню рядом с параметром **Configuration**. Откроем раскрывающийся список и выберем **Permanent** Это позволит сделать постоянными все изменения (рис. 2.12).

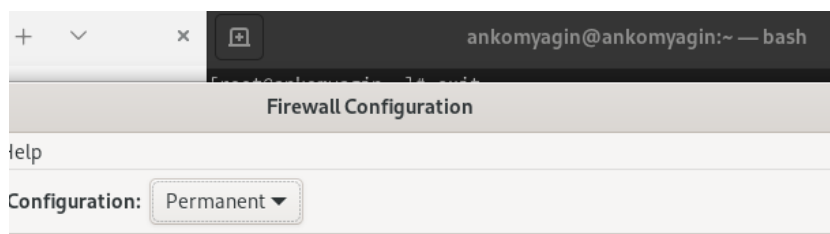


Рис. 2.12: Параметр Configuration на Permanent

Выберем зону public и отметим службы **http**, **https** и **ftp**, чтобы включить их. (рис. 2.13).

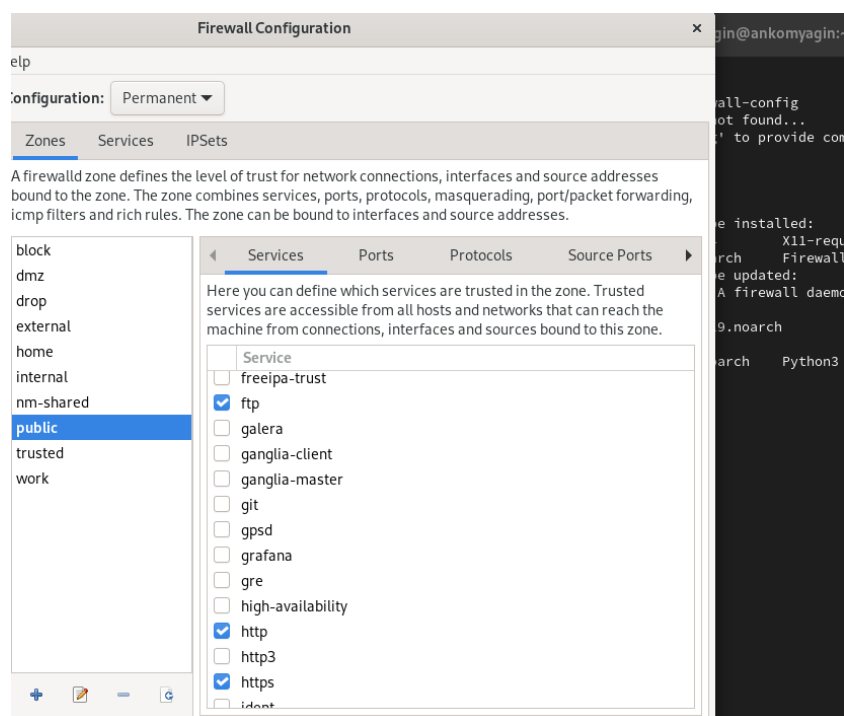


Рис. 2.13: Включение служб http, https и ftp

Выберем вкладку **Ports** и на этой вкладке нажмём **Add**. Введём порт 2022 и протокол **udp**, нажмём **OK**, чтобы добавить их в список.(рис. 2.14).

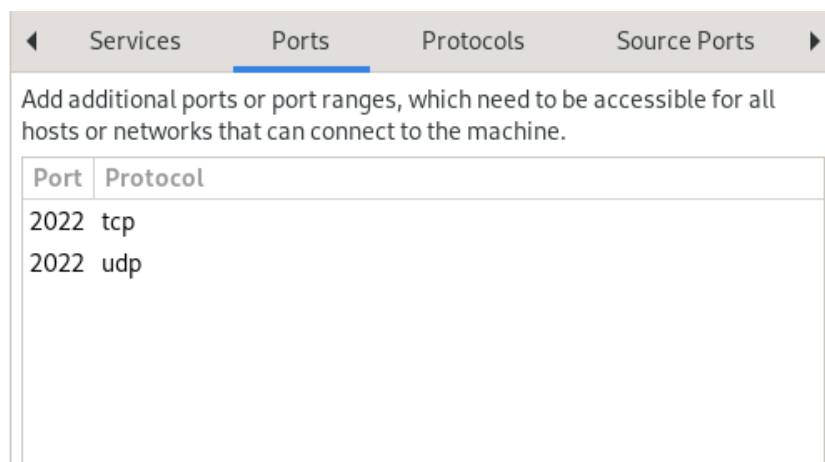


Рис. 2.14: Добавление порта

Закроем утилиту **firewall-config**. В окне терминала введём **firewall-cmd --list-all** (рис. 2.15).

```
[ankomyagin@ankomyagin ~]$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[ankomyagin@ankomyagin ~]$
```

Рис. 2.15: Вывод информации

Изменения ещё не вступили в силу, так как конфигурация выбрана постоянная.

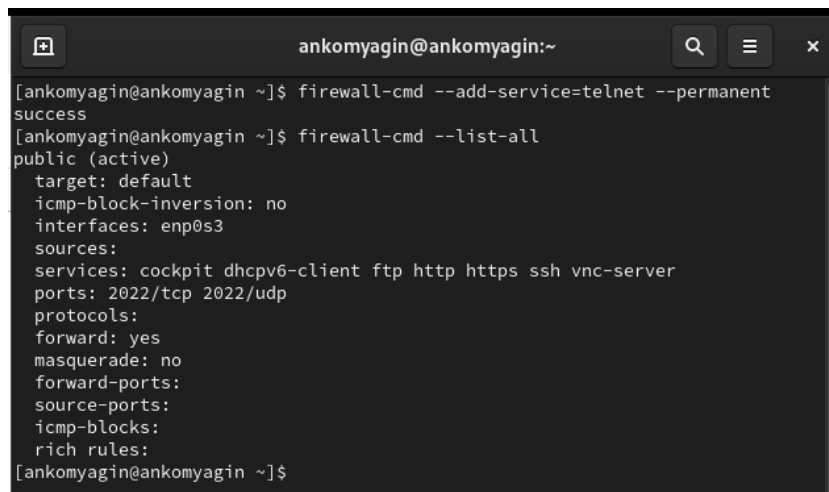
Перегрузим конфигурацию **firewall-cmd**. Вызовем список доступных сервисов.(рис. 2.16).

```
ankomyagin@ankomyagin:~
[ankomyagin@ankomyagin ~]$ firewall-cmd --reload
success
[ankomyagin@ankomyagin ~]$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-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:
[ankomyagin@ankomyagin ~]$
```

Рис. 2.16: Проверка применения изменений

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

Сделаем это как в командной строке (для службы telnet), так и в графическом интерфейсе (для служб imap, pop3, smtp). (рис. 2.17).



```
ankomyagin@ankomyagin:~  
[ankomyagin@ankomyagin ~]$ firewall-cmd --add-service=telnet --permanent  
success  
[ankomyagin@ankomyagin ~]$ firewall-cmd --list-all  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services: cockpit dhcpv6-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:  
[ankomyagin@ankomyagin ~]$
```

Рис. 2.17: Добавление telnet

Затем добавим оставшиеся службы через графический интерфейс (рис. 2.18).

- ☐ ident
- ☒ imap
- ☐ imaps
- ☐ ipfs
- ☐ ipp
- ☐ ipp-client

Рис. 2.18: Добавление почт

3 Ответы на контрольные вопросы

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

Нужно запустить службу `firewalld`, это можно сделать командой `systemctl start firewalld`.

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

Команда `firewall-cmd --add-port=2355/udp --permanent`.

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

Команда `firewall-cmd --list-all-zones`.

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

Команда `firewall-cmd --remove-service=vnc-server --permanent`.

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

Команда `firewall-cmd --reload`.

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

Команда `firewall-cmd --list-all`.

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

Команда `firewall-cmd --zone=public --add-interface=eno1 --permanent`.

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

Он будет добавлен в зону по умолчанию.

4 Выводы

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