Отчёт по лабораторной работе №13

Фильтр пакетов

Щемелев Илья Владимирович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2 Ход выполнения

2.1 Управление брандмауэром с помощью firewall-cmd

1. Для выполнения административных операций получены полномочия суперпользователя.
   В терминале выполнен вход в привилегированную оболочку командой su -, после чего дальнейшие действия выполнялись от имени root.

2. Определена зона брандмауэра, используемая по умолчанию.
   С помощью команды firewall-cmd –get-default-zone установлено, что зоной по умолчанию является public, что указывает на активную стандартную зону для сетевого интерфейса системы.

3. Получен список доступных зон firewalld.
   Командой firewall-cmd –get-zones выведен перечень зон, включая public, home, internal, trusted и другие, что подтверждает стандартную конфигурацию межсетевого экрана.

4. Просмотрены службы, доступные для использования в правилах брандмауэра.
   Командой firewall-cmd –get-services получен полный список предопределённых сервисов, таких как ssh, cockpit, vnc-server и другие, которые могут быть добавлены в зоны.

5. Определены службы, разрешённые в текущей зоне.

С помощью команды firewall-cmd –list-services установлено, что в зоне public разрешены службы cockpit, dhcpv6-client и ssh.

```
root@ivschemelev:~# firewall-cmd --get-default-zone
public
root@ivschemelev:~# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@ivschemelev:~# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcupsd ase
qnet audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitco
in-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization
-v cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over
-quic dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman
 foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-maste
r git gpsd grafana gre high-availability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs i
scsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-p
lane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler k
ube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llm
nr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqt
t-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe nt
p nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3
s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel rad
ius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane settl
ers-history-collection sip sips slimevr slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync s
potify-sync squid ssdp ssh statsrv steam-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission sup
ertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp
 tile38 tinc tor-socks transmission-client turn turns upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wiregu
ard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd wsdd-http wsman wsmans xdmcp xm
pp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-service z
ero-k zerotier
root@ivschemelev:~# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@ivschemelev:~#
```

Рис. 2.1: Службы текущей зоны

6. Выполнено сравнение вывода команд firewall-cmd –list-all и firewall-cmd –list-all –zone=public.

   В обоих случаях отображается идентичная информация, поскольку зона public является зоной по умолчанию и одновременно активной зоной системы.

```
root@ivschemelev:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@ivschemelev:~#
```

Рис. 2.2: Вывод firewall-cmd –list-all

```
root@ivschemelev:~# firewall-cmd --list-all --zone=public
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@ivschemelev:~#
```

Рис. 2.3: Вывод firewall-cmd –list-all –zone=public

7. В конфигурацию времени выполнения брандмауэра добавлен сервис VNC. Командой firewall-cmd –add-service=vnc-server сервис vnc-server был успешно добавлен в зону public.

8. Выполнена проверка добавленного сервиса.
   При выводе конфигурации с помощью firewall-cmd –list-all подтверждено

присутствие сервиса vnc-server в списке разрешённых сервисов зоны.

```
root@ivschemelev:~# firewall-cmd --add-service=vnc-server
success
root@ivschemelev:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@ivschemelev:~#
```

Рис. 2.4: Проверка добавленного сервиса

9. Выполнен перезапуск службы firewalld.

   Перезапуск выполнен с целью проверки сохранности ранее внесённых изменений.

10. После перезапуска службы firewalld выполнена повторная проверка конфигурации.

    Установлено, что сервис vnc-server отсутствует в списке разрешённых сервисов.

```
root@ivschemelev:~# systemctl restart firewalld.service
root@ivschemelev:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@ivschemelev:~#
```

Рис. 2.5: Сервис vnc-server отсутствует после перезапуска

Пояснение причины:

Сервис vnc-server был добавлен только в конфигурацию времени выполнения. При перезапуске службы firewalld runtime-конфигурация сбрасывается и загружается постоянная конфигурация, в которой данный сервис отсутствовал.

11. Сервис vnc-server добавлен в постоянную конфигурацию брандмауэра.
    Использование параметра –permanent обеспечивает сохранение правила на диске.

12. Выполнена проверка конфигурации сразу после добавления сервиса в permanent.
    Сервис vnc-server по-прежнему не отображается в выводе, так как изменения в постоянной конфигурации не применяются автоматически к конфигурации времени выполнения.

```
root@ivschemelev:~# firewall-cmd --add-service=vnc-server --permanent
success
root@ivschemelev:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@ivschemelev:~#
```

Рис. 2.6: Runtime-конфигурация без изменений

13. Выполнена перезагрузка конфигурации firewalld.

    После выполнения reload постоянная конфигурация была применена к текущей, и сервис vnc-server появился в списке разрешённых.

```
root@ivschemelev:~# firewall-cmd --reload
success
root@ivschemelev:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@ivschemelev:~#
```

Рис. 2.7: Применение permanent-конфигурации

14. В постоянную конфигурацию межсетевого экрана добавлен порт 2022 протокола TCP.
    После добавления порта выполнена перезагрузка конфигурации firewalld для применения изменений.

15. Выполнена итоговая проверка конфигурации брандмауэра.
    Установлено, что порт 2022/tcp присутствует в списке открытых портов, а сервис vnc-server корректно добавлен в конфигурацию зоны public.

```
root@ivschemelev:~# firewall-cmd --add-port=2022/tcp --permanent
success
root@ivschemelev:~# firewall-cmd --reload
success
root@ivschemelev:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@ivschemelev:~#
```

Рис. 2.8: Итоговая конфигурация firewalld

2.2 Управление брандмауэром с помощью firewall-config

1. Осуществлён запуск графического интерфейса управления брандмауэром.
   В терминале под учётной записью пользователя выполнен запуск утилиты **firewall-config**.

При запуске был запрошен пароль пользователя с административными полномочиями для управления службой firewalld. После аутентификации интерфейс был успешно открыт.

2. Выполнен переход к постоянной конфигурации брандмауэра.
   В верхней части окна в параметре **Configuration** из выпадающего списка выбрано значение **Permanent**, что обеспечивает сохранение всех вносимых изменений в постоянной конфигурации и их автоматическую загрузку после перезагрузки системы.

3. В зоне **public** включены службы **http**, **https** и **ftp**.
   В списке зон выбрана зона **public**, после чего на вкладке **Services** отмечены соответствующие службы. Данные действия разрешают доступ к веб-сервисам и FTP-серверу через межсетевой экран.

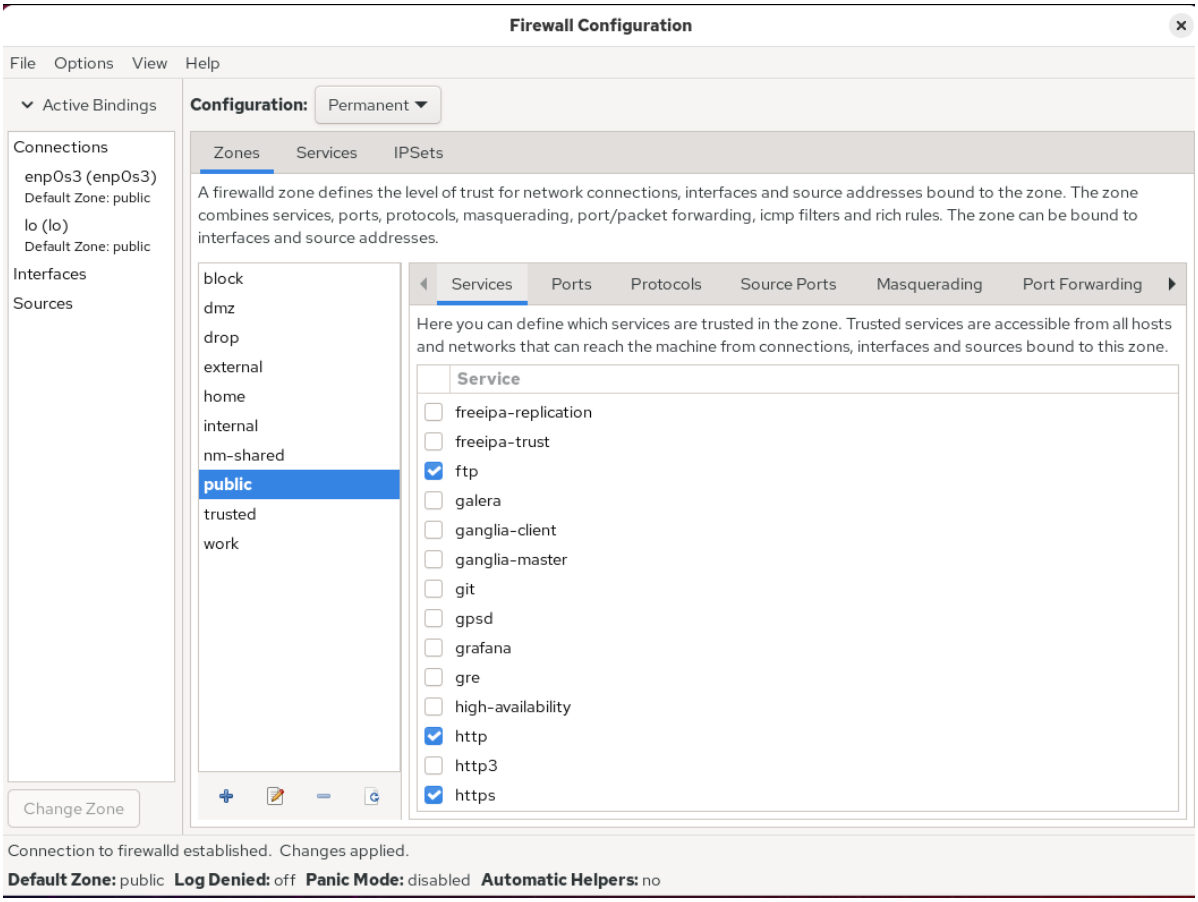

Рис. 2.9: Включение служб http, https и ftp

4. В зону **public** добавлен порт **2022** с протоколом **UDP**.

   На вкладке **Ports** нажата кнопка **Add**, в открывшемся диалоговом окне указан порт **2022** и выбран протокол **udp**, после чего изменения подтверждены нажатием кнопки **OK**.

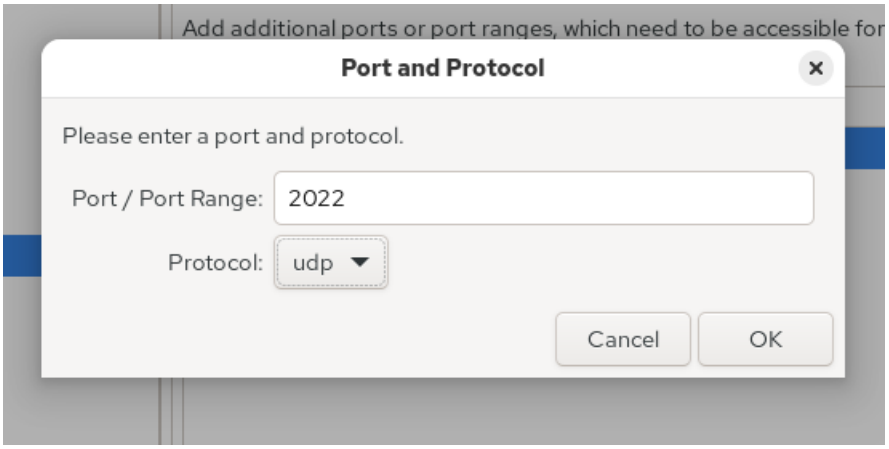

Рис. 2.10: Добавление порта 2022/udp

5. Утилита **firewall-config** закрыта после завершения конфигурирования.
   Все изменения были сохранены в постоянной конфигурации брандмауэра, но ещё не применены к конфигурации времени выполнения.

6. Выполнена проверка текущей конфигурации брандмауэра через терминал.
   При просмотре конфигурации с помощью команды firewall-cmd –list-all установлено, что добавленные службы и порт отсутствуют в выводе, так как изменения были выполнены в режиме **Permanent** и ещё не применены к runtime-конфигурации.

7. Выполнена перезагрузка конфигурации firewalld.
   После выполнения reload постоянная конфигурация была применена к конфигурации времени выполнения. Повторный просмотр настроек подтвердил наличие добавленных служб и порта.

```
root@ivschemelev:~#
root@ivschemelev:~# firewall-cmd --reload
success
root@ivschemelev:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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:
root@ivschemelev:~#
```

Рис. 2.11: Применение permanent-конфигурации

2.3 Самостоятельная работа

8. В постоянную конфигурацию брандмауэра добавлена служба **telnet** с использованием командной строки.
   Служба telnet добавлена в зону public как постоянная, после чего конфигурация была перезагружена для применения изменений.

9. С помощью графического интерфейса firewall-config в зону **public** добавлены службы **imap**, **pop3** и **smtp**.
   Для каждой службы была установлена отметка на вкладке **Services** при активном режиме **Permanent**, что обеспечило сохранение конфигурации на диске.

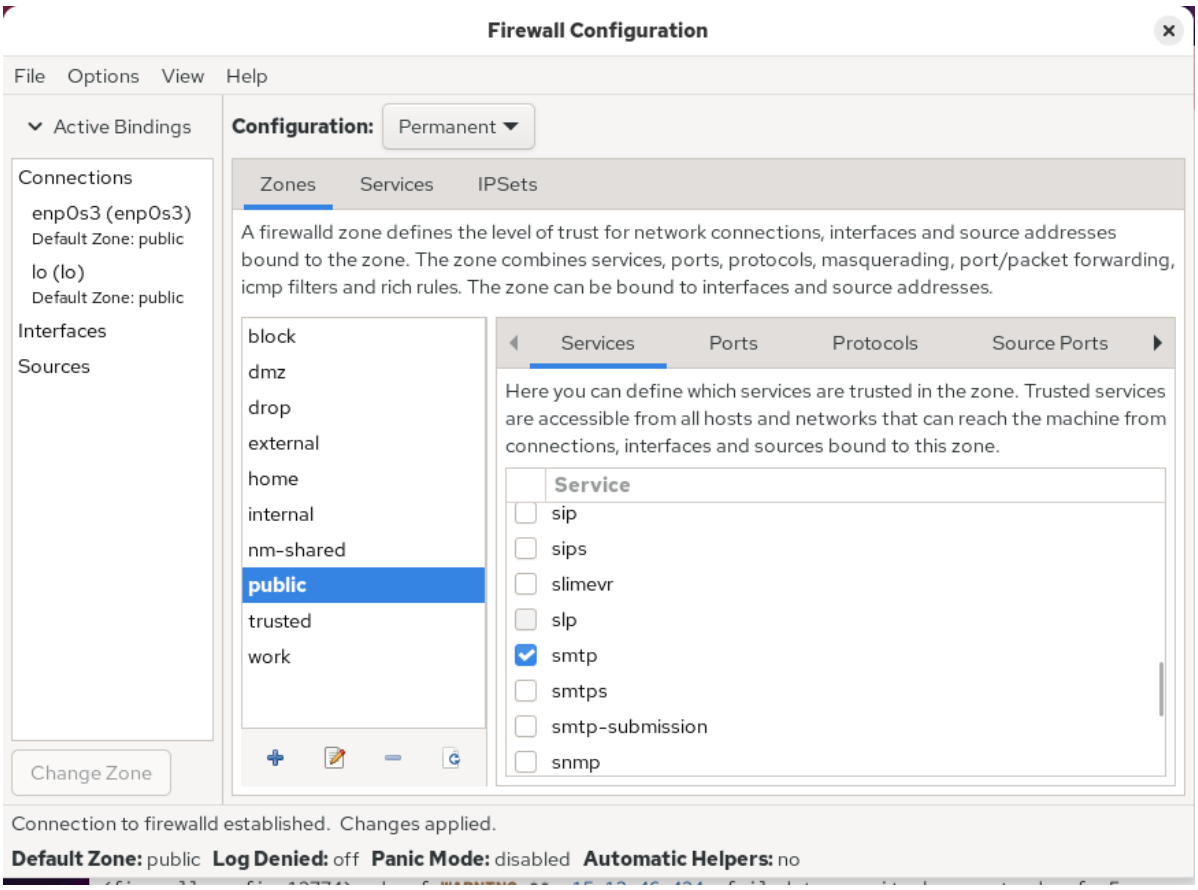

Рис. 2.12: Добавление служб imap, pop3 и smtp через GUI

10. Выполнена итоговая проверка конфигурации межсетевого экрана.

    Просмотр конфигурации подтвердил, что службы **telnet**, **imap**, **pop3**, **smtp**, а также ранее добавленные **http**, **https**, **ftp**, **vnc-server** и порт **2022/tcp, 2022/udp** присутствуют в зоне **public**.

    Таким образом, конфигурация является постоянной и будет автоматически активирована после перезагрузки системы.

```
root@ivschemelev:~#
root@ivschemelev:~# firewall-cmd --add-service=telnet --permanent
success
root@ivschemelev:~# firewall-cmd --reload
success
root@ivschemelev:~# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ftp http https ident pop3 smtp ssh telnet vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@ivschemelev:~#
```

Рис. 2.13: Итоговая конфигурация firewalld

3 Контрольные вопросы

1. Перед началом работы с менеджером конфигурации брандмауэра **firewall-config** должна быть запущена служба **firewalld**.
   Данная служба является фоновым демоном, который управляет правилами межсетевого экрана. Без её запуска графический интерфейс firewall-config не сможет подключиться к системе управления брандмауэром и применить настройки.

2. Для добавления UDP-порта **2355** в конфигурацию брандмауэра в зоне по умолчанию используется команда:
   firewall-cmd –add-port=2355/udp.
   Эта команда добавляет указанный порт в конфигурацию времени выполнения активной зоны.

3. Для отображения полной конфигурации брандмауэра для всех зон применяется команда:
   firewall-cmd –list-all-zones.
   Она выводит параметры всех зон, включая разрешённые службы, открытые порты, интерфейсы и дополнительные правила.

4. Для удаления службы **vnc-server** из текущей (runtime) конфигурации брандмауэра используется команда:
   firewall-cmd –remove-service=vnc-server.
   Удаление производится только из конфигурации времени выполнения и не затрагивает постоянную конфигурацию, если не указан параметр

permanent.

5. Для активации новой конфигурации, добавленной с использованием параметра **–permanent**, применяется команда:
   firewall-cmd –reload.
   Эта команда перечитывает постоянную конфигурацию и применяет её к текущей рабочей конфигурации брандмауэра.

6. Для проверки того, что новая конфигурация была добавлена в текущую зону и является активной, используется команда:
   firewall-cmd –list-all.
   Она отображает параметры активной зоны, включая разрешённые службы и открытые порты.

7. Для добавления сетевого интерфейса **eno1** в зону **public** используется команда:
   firewall-cmd –zone=public –add-interface=eno1.
   После выполнения команды указанный интерфейс будет привязан к выбранной зоне.

8. Если при добавлении нового интерфейса в конфигурацию брандмауэра зона не указана явно, интерфейс будет добавлен в **зону по умолчанию**.
   Зона по умолчанию определяется настройками firewalld и может быть просмотрена с помощью команды **firewall-cmd –get-default-zone**.

4 Заключение

В ходе выполнения работы были изучены и отработаны основные способы управления межсетевым экраном firewalld с использованием как командной строки, так и графического интерфейса firewall-config. Были рассмотрены различия между конфигурацией времени выполнения и постоянной конфигурацией, а также порядок применения изменений. Полученные навыки позволяют настраивать доступ к сетевым службам и портам, обеспечивая корректную и устойчивую работу системы после перезагрузки.