РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 13

Фильтр пакетов

Студент: Эйвази Мани

Группа: НПИбд-03-24

Студенческий билет №: 1032245107

Цель работы

Получить практические навыки настройки и управления динамическим межсетевым экраном (брандмауэром) в Linux с использованием firewalld. Освоить работу с зонами безопасности, добавлением служб и портов как через командную строку (firewall-cmd), так и через графический интерфейс (firewall-config).

Первый шаг: Получение базовой информации о настройках firewalld. Система использует зону public по умолчанию, в которой изначально

разрешены только критически важные службы (SSH для управления и DHCPv6-client).

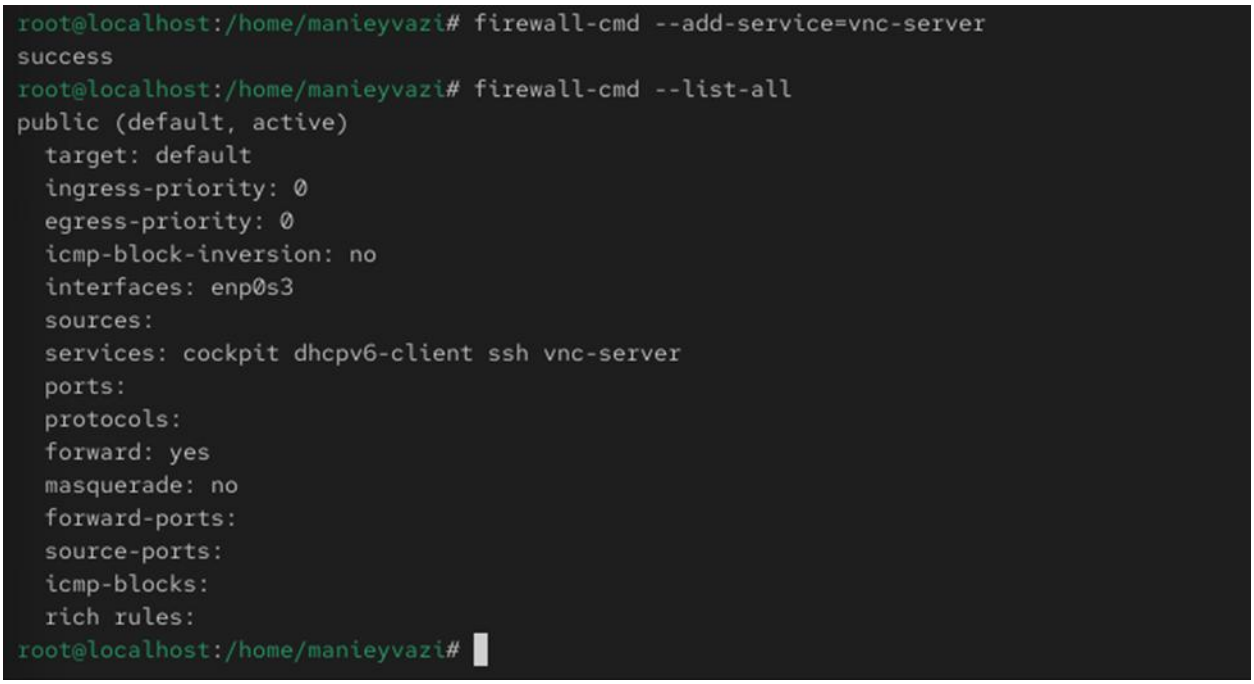
```
root@localhost:/home/manieyvazi# firewall-cmd --get-default-zone
public
root@localhost:/home/manieyvazi# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@localhost:/home/manieyvazi# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apc
upsd aseqnet audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin b
itcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civi
lization-iv civilization-v cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 d
hcpv6-client distcc dns dns-over-quic dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-cl
ient etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freei
pa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https ident imap
imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana kl
ogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manage
r kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kube
let-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp m
anagesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mys
ql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry o
penvpn 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 r
adsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane se
ttlers-history-collection sip sips slimevr slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroa
k-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfer steam-streaming stellaris stronghold-crusader stun s
tuns submission supertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls te
lnet tentacle terraria tftp tile38 tinc tor-socks transmission-client turn turns upnp-client vdsm vnc-server vrrp war
pinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discove
ry-udp wsdd wsdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gatewa
y zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
root@localhost:/home/manieyvazi# firewall-cmd --list-services
cockpit dhcpv6-client ssh
```

Второй шаг: Получение полной информации о настройках активной и конкретной зоны. Команда --list-all предоставляет исчерпывающий обзор всех правил в зоне.

```
root@localhost:/home/manieyvazi# 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:
```

```
root@localhost:/home/manieyvazi# firewall-cmd --list-all --zone-public
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man page
firewall-cmd: error: unrecognized arguments: --zone-public
```

Третий шаг: Временное открытие доступа к серверу VNC. Служба vnc-server добавлена в runtime-конфигурацию. Изменение действует немедленно, но не сохраняется после перезагрузки службы или системы.



Четвертый шаг: Проверка сохранности временных изменений. Служба vnc-server исчезла из конфигурации. Это произошло потому, что команда --add-service без флага --permanent вносит изменение только в runtime-конфигурацию, которая хранится в оперативной памяти. Перезапуск службы сбрасывает runtime-конфигурацию до состояния, описанного в permanent-конфигурации (хранится на диске). На диске правило для VNC сохранено не было.

systemctl restart firewalld

firewall-cmd--list-all *(vnc-server исчез из списка!)*

Пятый шаг: Внесение постоянного изменения и его активация. Ключевой вывод — постоянные изменения (--permanent) требуют

применения командой --reload (или перезапуска службы), чтобы вступить в силу в runtime.

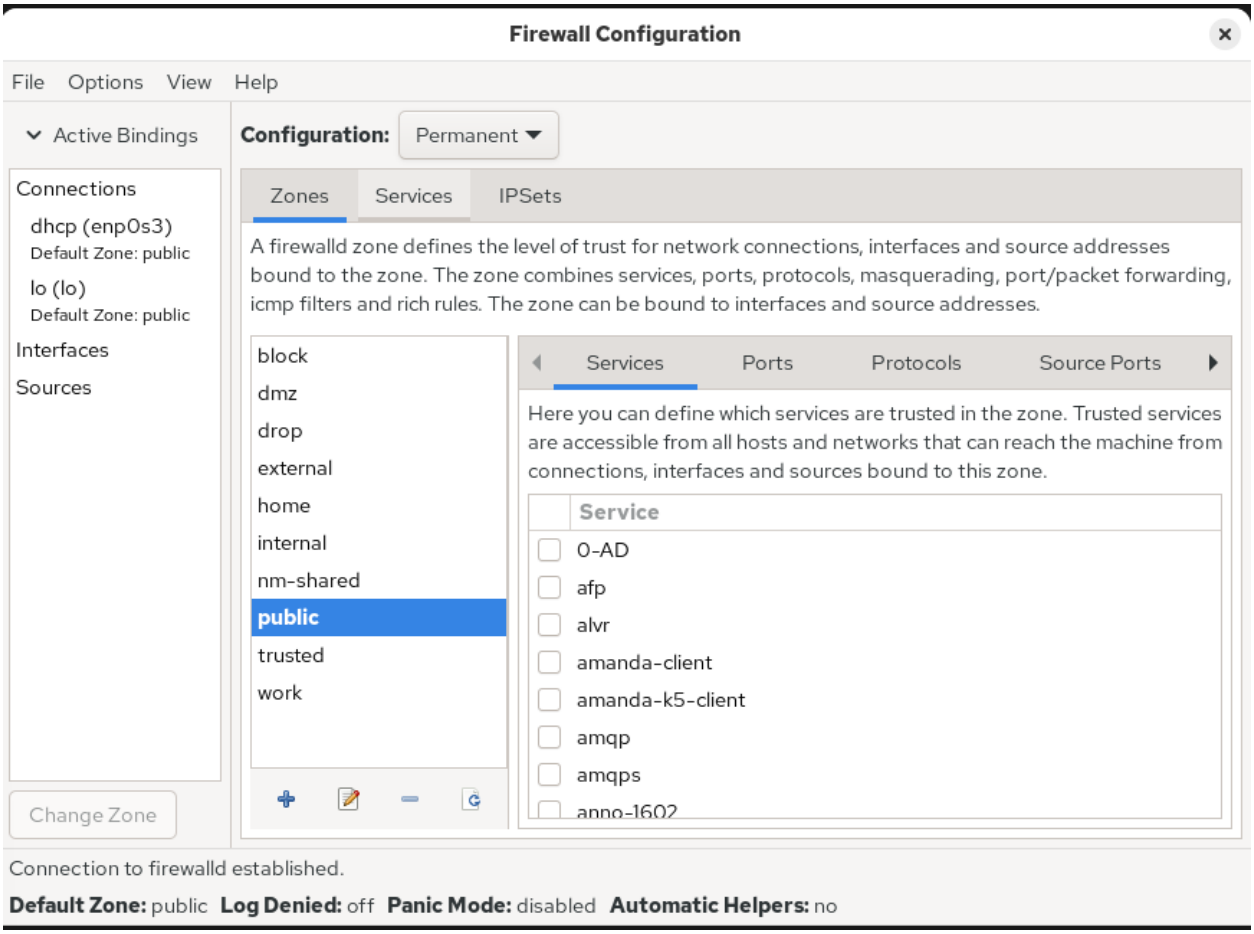
```
root@localhost:/home/manieyvazi# firewall-cmd --add-service=vnc-server
success
root@localhost:/home/manieyvazi# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@localhost:/home/manieyvazi#
```

```
root@localhost:/home/manieyvazi# firewall-cmd --reload
success
root@localhost:/home/manieyvazi# 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:
```

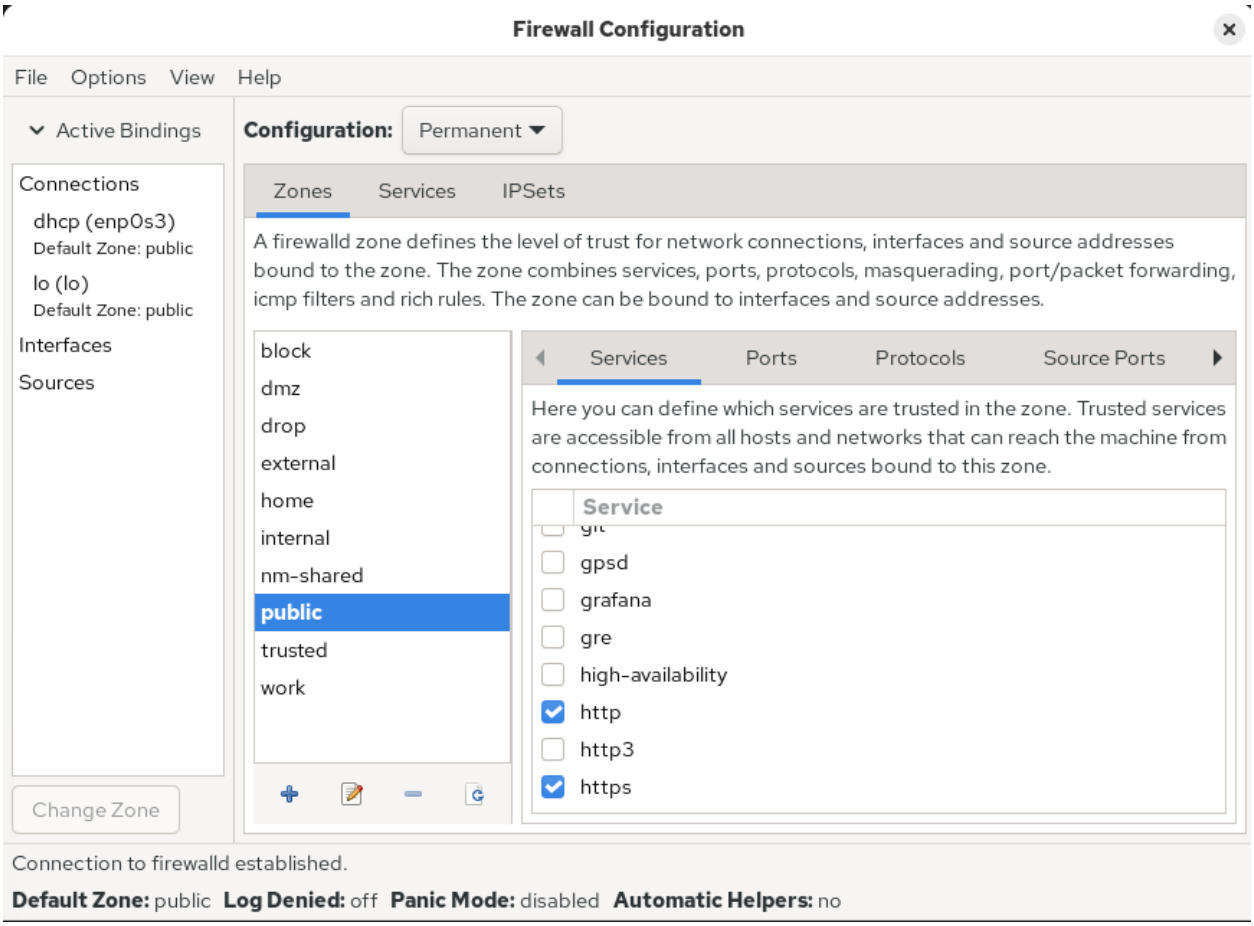
Шестой шаг: Открытие произвольного TCP-порта (например, для нестандартной службы). Успешно добавлено правило, разрешающее входящие подключения по протоколу TCP на порт 2022 в зоне public.

```
root@localhost:/home/manieyvazi# firewall-cmd --add-port=2022/top --permanent
Error: INVALID_PROTOCOL: 'top' not in {'tcp'|'udp'|'sctp'|'dccp'}
root@localhost:/home/manieyvazi# firewall-cmd --add-port=2022/tcp --permanent
success
root@localhost:/home/manieyvazi# firewall-cmd --reload
success
```

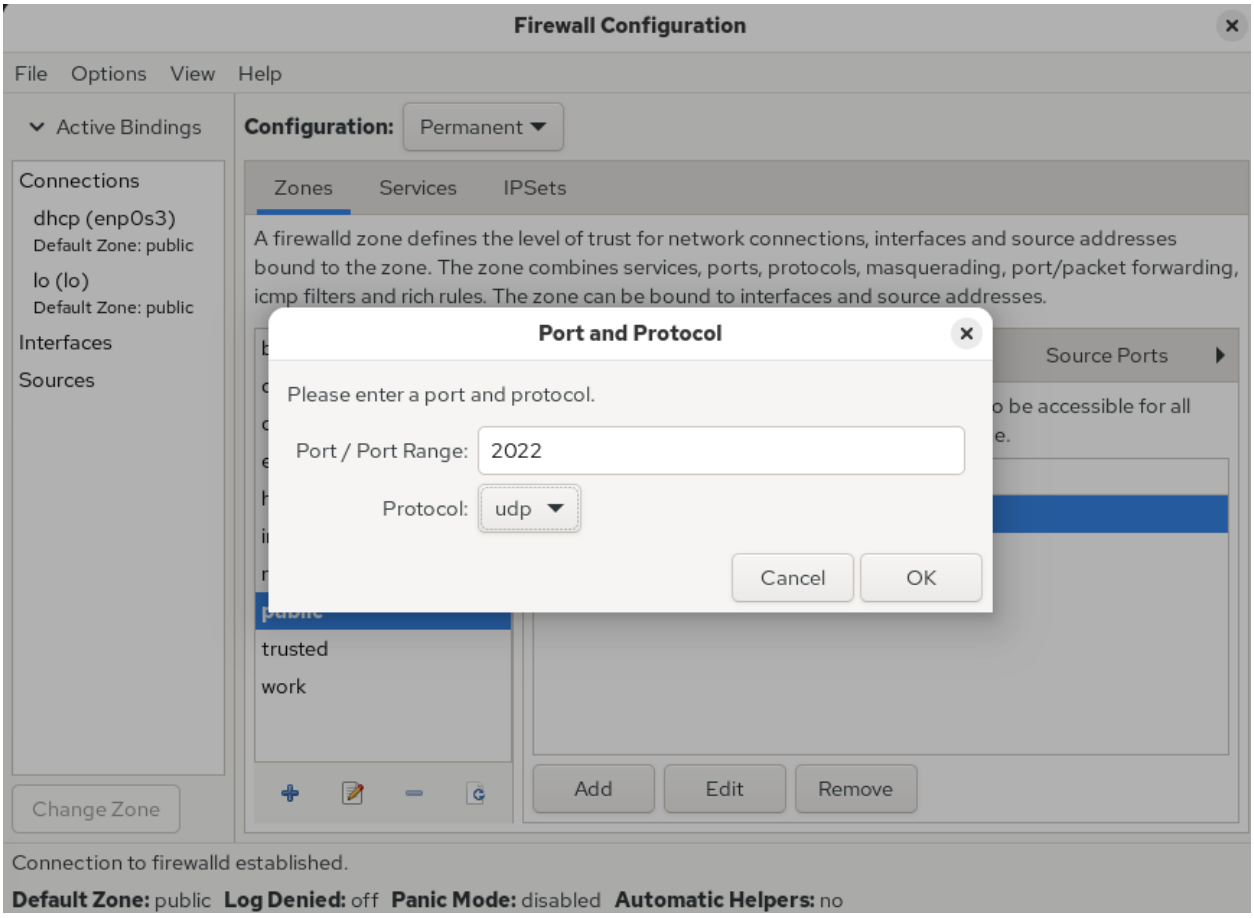
Седьмой шаг: Открытие утилиты firewall-config (требует прав root, запрашивает пароль). Запущен графический интерфейс для настройки firewalld. В верхнем выпадающем списке Configuration выбирается режим Permanent. Это гарантирует, что все изменения будут сохранены на диске. Интерфейс переключен в режим редактирования постоянной конфигурации.



Восьмой шаг: В левой панели выбирается зона public. На вкладке Services отмечаются флажки для служб http, https, ftp. Службы добавлены в постоянную конфигурацию зоны public.



девяти шаг: Переход на вкладку Ports, нажатие кнопки Add. В диалоговом окне вводится порт 2022 и выбирается протокол udp.файл /etc/resolv.conf автоматически обновится, содержая оба DNS-сервера. Порт 2022/udp добавлен в постоянную конфигурацию зоны public



Десятый шаг: После закрытия firewall-config изменения, внесенные в режиме Permanent, требуют перезагрузки конфигурации, чтобы вступить в силу.Все изменения, сделанные в графическом интерфейсе (службы и порт), успешно применены и активны.

```
root@localhost:/home/manieyvazi# 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@localhost:/home/manieyvazi# firewall-cmd --reload
success
root@localhost:/home/manieyvazi# 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@localhost:/home/manieyvazi#
```

Работа с NetworkManager через текстовый пользовательский интерфейс.

- Команда: nmtui
- Результат: Открывается меню, позволяющее в удобной форме просматривать, редактировать, активировать и удалять подключения, а также изменять параметры

системы (Edit a connection, Activate a connection и т.д.). Все изменения, внесенные через nmtui, соответствуют командам nmcli.

заключение

В ходе лабораторной работы были успешно освоены принципы и инструменты работы с динамическим межсетевым экраном firewalld в Linux:

1. **Концепция зон:** Понята и применена ключевая абстракция firewalld — **зоны безопасности** (public, home, internal и др.). Зоны позволяют гибко назначать разные наборы правил для разных сетевых интерфейсов или источников трафика, что критически важно для серверов с несколькими сетевыми картами.
2. **Двойная конфигурация:** Освоена фундаментальная архитектура firewalld, разделяющая конфигурацию на:
    - **Runtime (время выполнения):** Активные правила в памяти. Изменяются командами без флага --permanent. Сбрасываются при перезагрузке службы.
    - **Permanent (постоянная):** Правила, хранящиеся на диске (в файлах /etc/firewalld/). Изменяются с флагом --permanent. Для применения требуют выполнения firewall-cmd--reload.
3. **Управление через CLI (**firewall-cmd**):** Получены навыки использования основного командного инструмента для всех операций: просмотр состояния, добавление/удаление предопределенных служб (--add-service) и пользовательских портов (--add-port), управление зонами, перезагрузка конфигурации.
4. **Управление через GUI (**firewall-config**):** Освоена работа с графической утилитой, которая предоставляет удобный визуальный интерфейс для тех же операций. Особое внимание уделено переключению между режимами Runtime и Permanent в интерфейсе.
5. **Практическое применение:** Создана комплексная конфигурация брандмауэра, разрешающая доступ к стандартным веб- и почтовым службам, а также к пользовательским портам, что моделирует типичную задачу системного администратора.

Работа показала, что firewalld предоставляет мощный, гибкий и относительно простой в использовании инструмент для управления сетевой безопасностью, заменяя собой более сложные и низкоуровневые механизмы вроде прямого управления iptables.

1. Какая служба должна быть запущена перед началом работы с мен еджером конфигурации брандмауэра firewall-config?
   Служба firewalld. Проверить: systemctl status firewalld. Она должна быть в состоянии active (running).

2. Какая команда позволяет добавить UDP-порт 2355 в конфигураци ю брандмауэра в зоне по умолчанию?
   firewall-cmd--add-port=2355/udp (временное) или firewall-cmd--ad d-port=2355/udp--permanent (постоянное, с последующим --reload).

3. Какая команда позволяет показать всю конфигурацию брандмауэр а во всех зонах?
   firewall-cmd--list-all-zones.

4. Какая команда позволяет удалить службу vnc-server из текущей ко нфигурации брандмауэра?
   firewall-cmd--remove-service=vnc-server (из runtime) или firewall-cm d--remove-service=vnc-server--permanent (из permanent-конфигура ции).

5. Какая команда firewall-cmd позволяет активировать новую конфиг урацию, добавленную опцией --permanent?
   firewall-cmd--reload.

6. Какой параметр firewall-cmd позволяет проверить, что новая конф игурация была добавлена в текущую зону и теперь активна?
   firewall-cmd--list-all (показывает активную runtime-конфигурацию д ля текущей/указанной зоны).

7. Какая команда позволяет добавить интерфейс eno1 в зону public?
   firewall-cmd--zone=public--add-interface=eno1--permanent (и зате м --reload).

8. Если добавить новый интерфейс в конфигурацию брандмауэра, по ка не указана зона, в какую зону он будет добавлен?
   В зону по умолчанию (default zone). Узнать её можно командой fire wall-cmd--get-default-zone (обычно public).