

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №13

дисциплина: Основы администрирования операционных систем

Студент: Хамди Мохаммад, 1032235868

МОСКВА

2024 г.

Постановка задачи

Получить навыки настройки пакетного фильтра в Linux.

Выполнение работы

Управление брандмауэром с помощью firewall-cmd

1. Получите полномочия администратора: su –
2. Определите текущую зону по умолчанию, введя: firewall-cmd --get-default-zone
3. Определите доступные зоны, введя: firewall-cmd --get-zones
4. Посмотрите службы, доступные на вашем компьютере, используя
firewall-cmd --get-services

```
[hmohammad@hamdimohammad ~]$ su
Password:
[root@hamdimohammad hmohammad]# firewall-cmd --get-default-zone
public
[root@hamdimohammad hmohammad]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@hamdimohammad hmohammad]# 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 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-registrator 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 gpsd grafana gre high-availability http 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 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 mongodb mongod mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-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 squid ssdp 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 vds vnc-server warpinator wbm-http wbm-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
[root@hamdimohammad hmohammad]#
[root@hamdimohammad hmohammad]#
```

5. Определите доступные службы в текущей зоне: `firewall-cmd --list-services`
6. Сравните результаты вывода информации при использовании команды `firewall-cmd --list-all` и команды `firewall-cmd --list-all --zone=public`

```
[root@hamdimohammad hmohammad]#  
[root@hamdimohammad hmohammad]# firewall-cmd --list-services  
cockpit dhcpv6-client ssh  
[root@hamdimohammad hmohammad]# 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@hamdimohammad hmohammad]# 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@hamdimohammad hmohammad]#
```

7. Добавьте сервер VNC в конфигурацию брандмауэра:

```
firewall-cmd --add-service=vnc-server
```

8. Проверьте, добавился ли vnc-server в конфигурацию: `firewall-cmd --list-all`

9. Перезапустите службу firewalld: `systemctl restart firewalld`

10. Проверьте, есть ли vnc-server в конфигурации: `firewall-cmd --list-all` Обратите внимание, что служба vnc-server больше не указана. Поясните, почему это произошло.

```
[root@hamdimohammad hmohammad]#  
[root@hamdimohammad hmohammad]# firewall-cmd --add-service=vnc-server  
success  
[root@hamdimohammad hmohammad]# 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@hamdimohammad hmohammad]# systemctl restart firewalld.service  
[root@hamdimohammad hmohammad]# 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@hamdimohammad hmohammad]#
```

11. Добавьте службу vnc-server ещё раз, но на этот раз сделайте её постоянной, используя команду `firewall-cmd --add-service=vnc-server --permanent`
12. Проверьте наличие vnc-server в конфигурации: `firewall-cmd --list-all` Вы увидите, что VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения.
13. Перезагрузите конфигурацию firewalld и просмотрите конфигурацию времени выполнения: `firewall-cmd --reload` `firewall-cmd --list-all`

```
[root@hamdimohammad hmohammad]#  
[root@hamdimohammad hmohammad]# firewall-cmd --add-service=vnc-server --permanent  
success  
[root@hamdimohammad hmohammad]# 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@hamdimohammad hmohammad]# firewall-cmd --reload  
success  
[root@hamdimohammad hmohammad]# 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@hamdimohammad hmohammad]#
```

14. Добавьте в конфигурацию межсетевого экрана порт 2022 протокола TCP:

```
firewall-cmd --add-port=2022/tcp --permanent
```

Затем перезагрузите конфигурацию firewalld: `firewall-cmd --reload`

15. Проверьте, что порт добавлен в конфигурацию: `firewall-cmd --list-all`

```
[root@hamdimohammad hmoammad]#  
[root@hamdimohammad hmoammad]#  
[root@hamdimohammad hmoammad]# firewall-cmd --add-port=2022/tcp  
success  
[root@hamdimohammad hmoammad]# firewall-cmd --add-port=2022/tcp --permanent  
success  
[root@hamdimohammad hmoammad]# firewall-cmd --reload  
success  
[root@hamdimohammad hmoammad]# 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@hamdimohammad hmoammad]#
```

Управление брандмауэром с помощью firewall-config

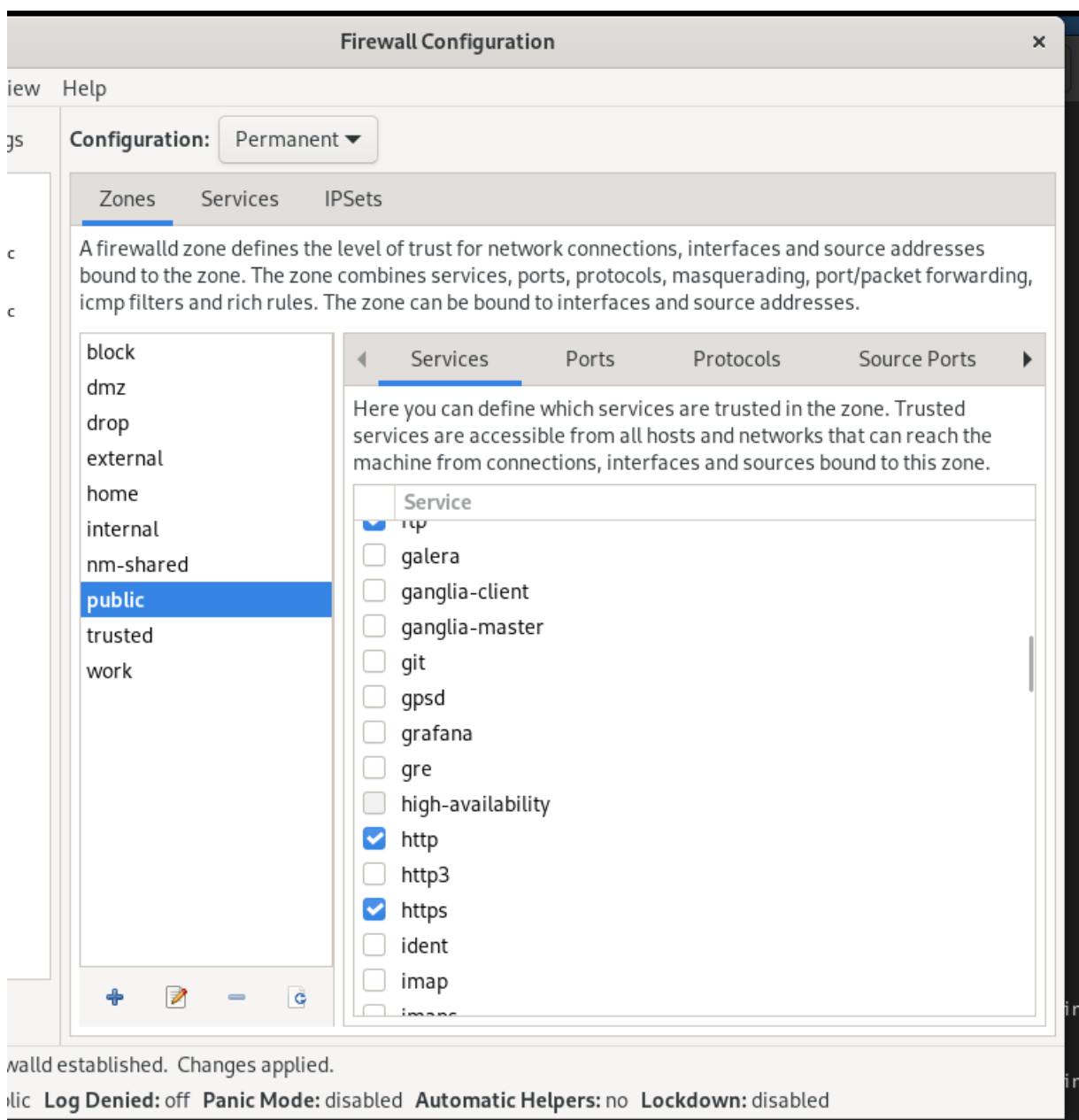
1. Откройте терминал и под учётной записью своего пользователя запустите интерфейс GUI firewall-config: firewall-config

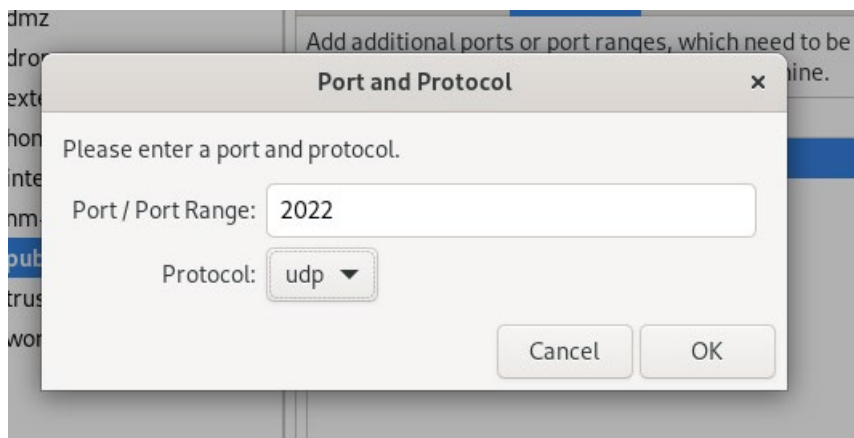
Если служба отсутствует, то система предложит вам её установить. Также при запуске потребуется ввести пароль пользователя с полномочиями управления этой службой.

2. Нажмите выпадающее меню рядом с параметром Configuration . Откройте раскрывающийся список и выберите Permanent . Это позволит сделать постоянными все изменения, которые вы вносите при конфигурировании.

3. Выберите зону public и отметьте службы http, https и ftp, чтобы включить их.

4. Выберите вкладку Ports и на этой вкладке нажмите Add . Введите порт 2022 и протокол udp, нажмите ОК , чтобы добавить их в список.





5. Закройте утилиту firewall-config.

6. В окне терминала введите `firewall-cmd --list-all`

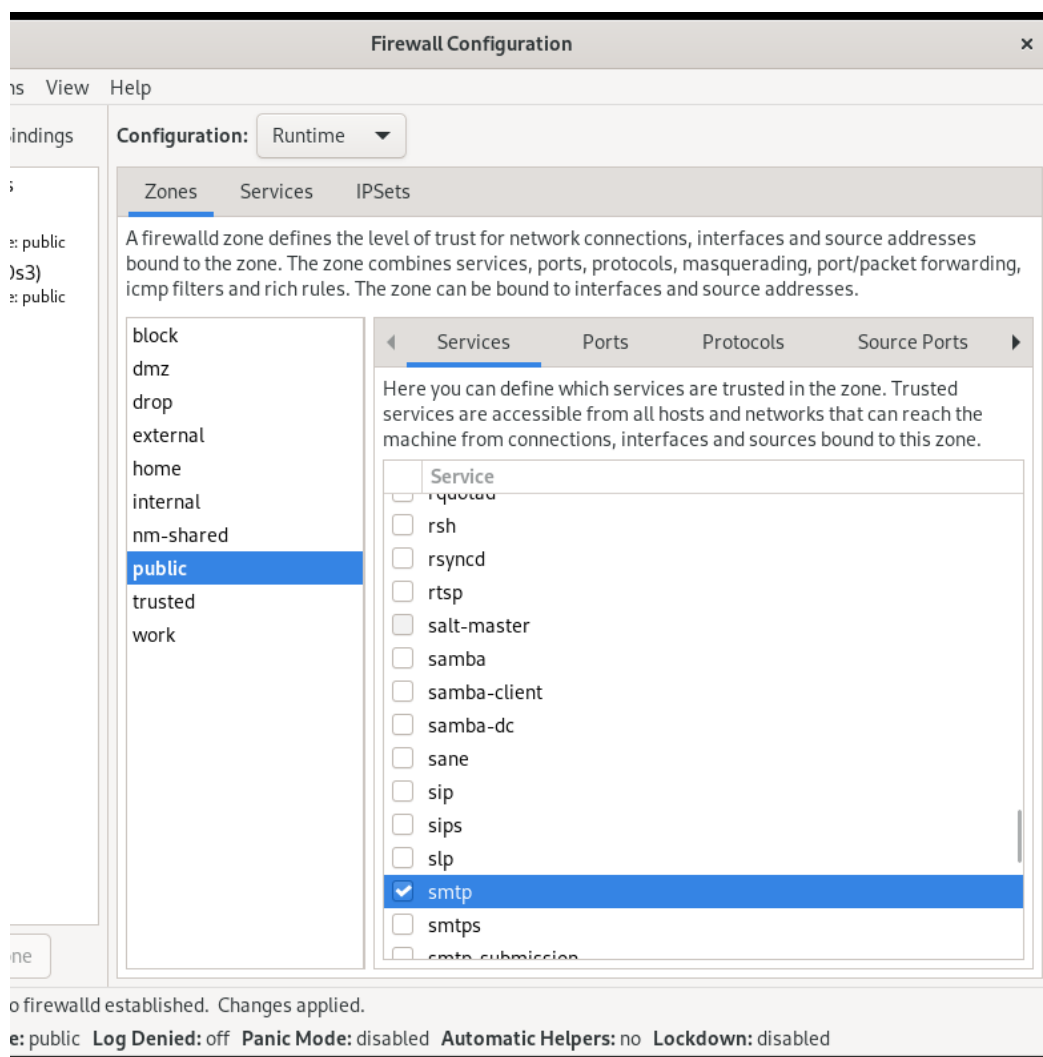
Обратите внимание, что изменения, которые вы только что внесли, ещё не вступили в силу. Это связано с тем, что вы настроили их как постоянные изменения, а не как изменения времени выполнения.

7. Перегрузите конфигурацию firewall-cmd: `firewall-cmd --reload` и список доступных сервисов: `firewall-cmd --list-all` Вы увидите, что изменения были применены.

```
[root@hamdimohammad hmohammad]#  
[root@hamdimohammad hmohammad]# 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@hamdimohammad hmohammad]# firewall-cmd --reload  
success  
[root@hamdimohammad hmohammad]# 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:  
[root@hamdimohammad hmohammad]#
```


Самостоятельная работа

1. Создайте конфигурацию межсетевого экрана, которая позволяет получить доступ к следующим службам:
 - telnet;
 - imap;
 - pop3;
 - smtp.
2. Сделайте это как в командной строке (для службы telnet), так и в графическом интерфейсе (для служб imap, pop3, smtp).
3. Убедитесь, что конфигурация является постоянной и будет активирована после перезагрузки компьютера.



w Help

Configuration: Permanent ▼

Zones Services IPSets

A firewalld zone defines the level of trust for network connections, interfaces and source addresses bound to the zone. The zone combines services, ports, protocols, masquerading, port/packet forwarding, icmp filters and rich rules. The zone can be bound to interfaces and source addresses.

block
dmz
drop
external
home
internal
nm-shared
public
trusted
work

Services Ports Protocols Source Ports

Here you can define which services are trusted in the zone. Trusted services are accessible from all hosts and networks that can reach the machine from connections, interfaces and sources bound to this zone.

Service
<input type="checkbox"/> rquota
<input type="checkbox"/> rsh
<input type="checkbox"/> rsyncd
<input type="checkbox"/> rtsp
<input type="checkbox"/> salt-master
<input type="checkbox"/> samba
<input type="checkbox"/> samba-client
<input type="checkbox"/> samba-dc
<input type="checkbox"/> sane
<input type="checkbox"/> sip
<input type="checkbox"/> sips
<input type="checkbox"/> slp
<input checked="" type="checkbox"/> smtp
<input type="checkbox"/> smtps
<input type="checkbox"/> smtp-submission

all established. Changes applied.

Log Denied: off Panic Mode: disabled Automatic Helpers: no Lockdown: disabled

```

tials: Error sending message: Broken pipe
[root@hamdimohammad hmohammad]#
[root@hamdimohammad hmohammad]# firewall-cmd --reload
success
[root@hamdimohammad hmohammad]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp0s3
sources:
services: cockpit dhcpv6-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:
[root@hamdimohammad hmohammad]#

```

Контрольные вопросы

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

Перед работой с `firewall-config` должна быть запущена служба `firewalld`. Команда для её запуска: `sudo systemctl start firewalld`

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

Для добавления UDP-порта 2355 в текущую зону (по умолчанию обычно это зона `public`): `sudo firewall-cmd --add-port=2355/udp`

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

Чтобы увидеть всю конфигурацию брандмауэра в разных зонах:

`sudo firewall-cmd --list-all-zones`

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

Чтобы удалить службу `vnc-server` из текущей зоны:

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

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

Чтобы применить изменения, добавленные с параметром `--permanent` (для их постоянного сохранения): `sudo firewall-cmd --reload`

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

Для проверки активных изменений в текущей зоне можно использовать:

`sudo firewall-cmd --list-all`

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

Чтобы добавить интерфейс `eno1` в зону `public`:

`sudo firewall-cmd --zone=public --add-interface=eno1`

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

Если не указана зона, новый интерфейс по умолчанию будет добавлен в зону default.

Это зона, которая используется, если не указано иное.

Заключение

Получены навыки настройки сетевого пакетного фильтра.