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:

Группа:

МОСКВА

2024 г.

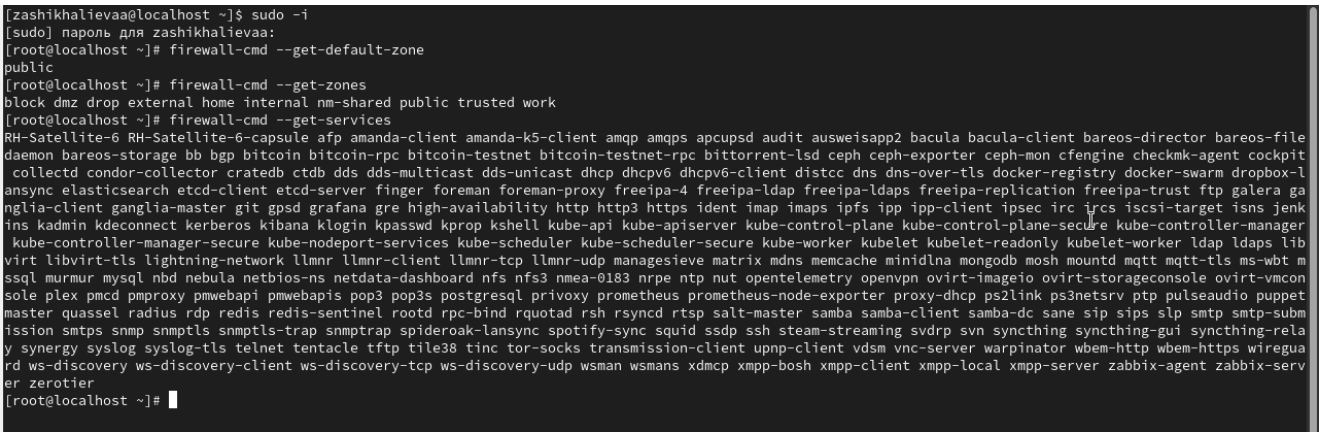
Постановка задачи

Получить навыки настройки пакетного фильтра в Linux.

Выполнение работы

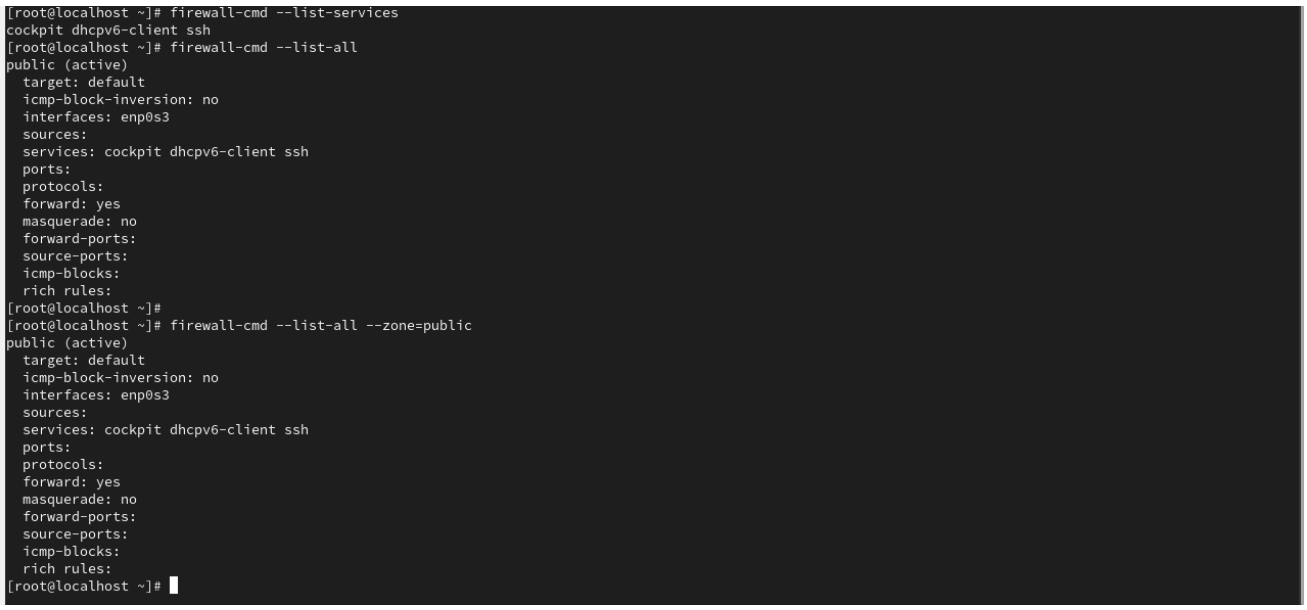
Управление брандмауэром с помощью firewall-cmd

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



5. Определите доступные службы в текущей зоне: firewall-cmd --list-services

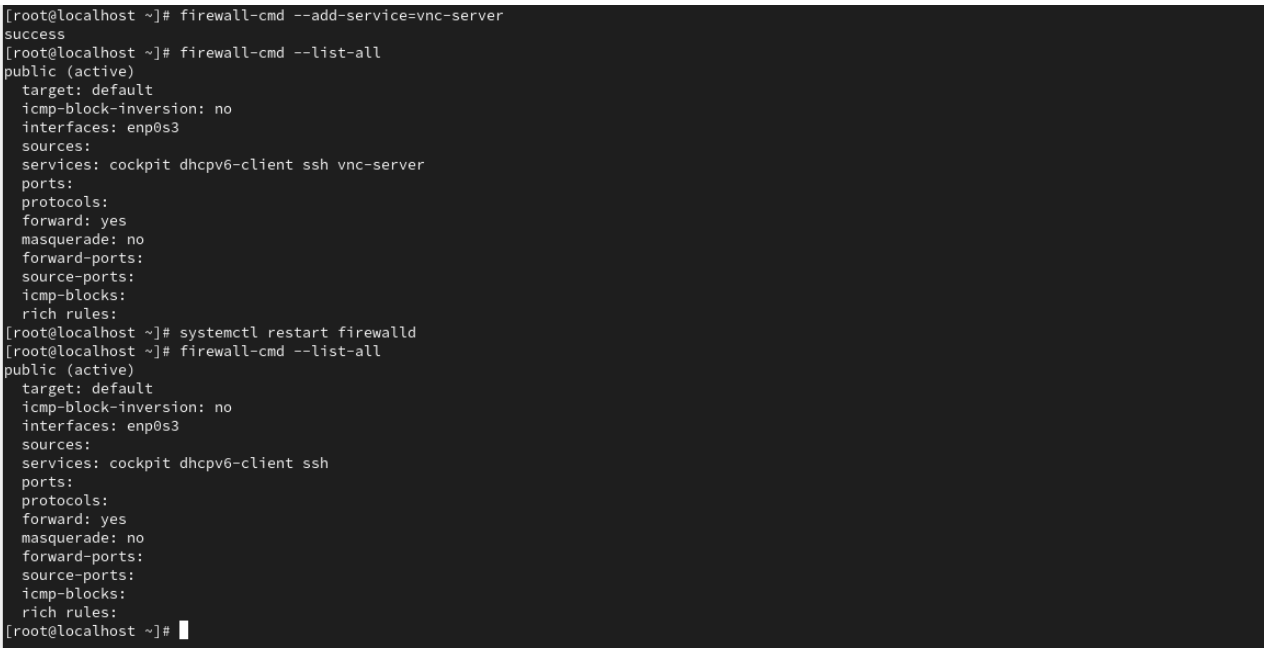
6. Сравните результаты вывода информации при использовании команды firewall-cmd --list-all и команды firewall-cmd --list-all --zone=public



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.

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

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

```
  rich rules:
[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 dhcpv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@localhost ~]#
```

Управление брандмауэром с помощью firewall-config

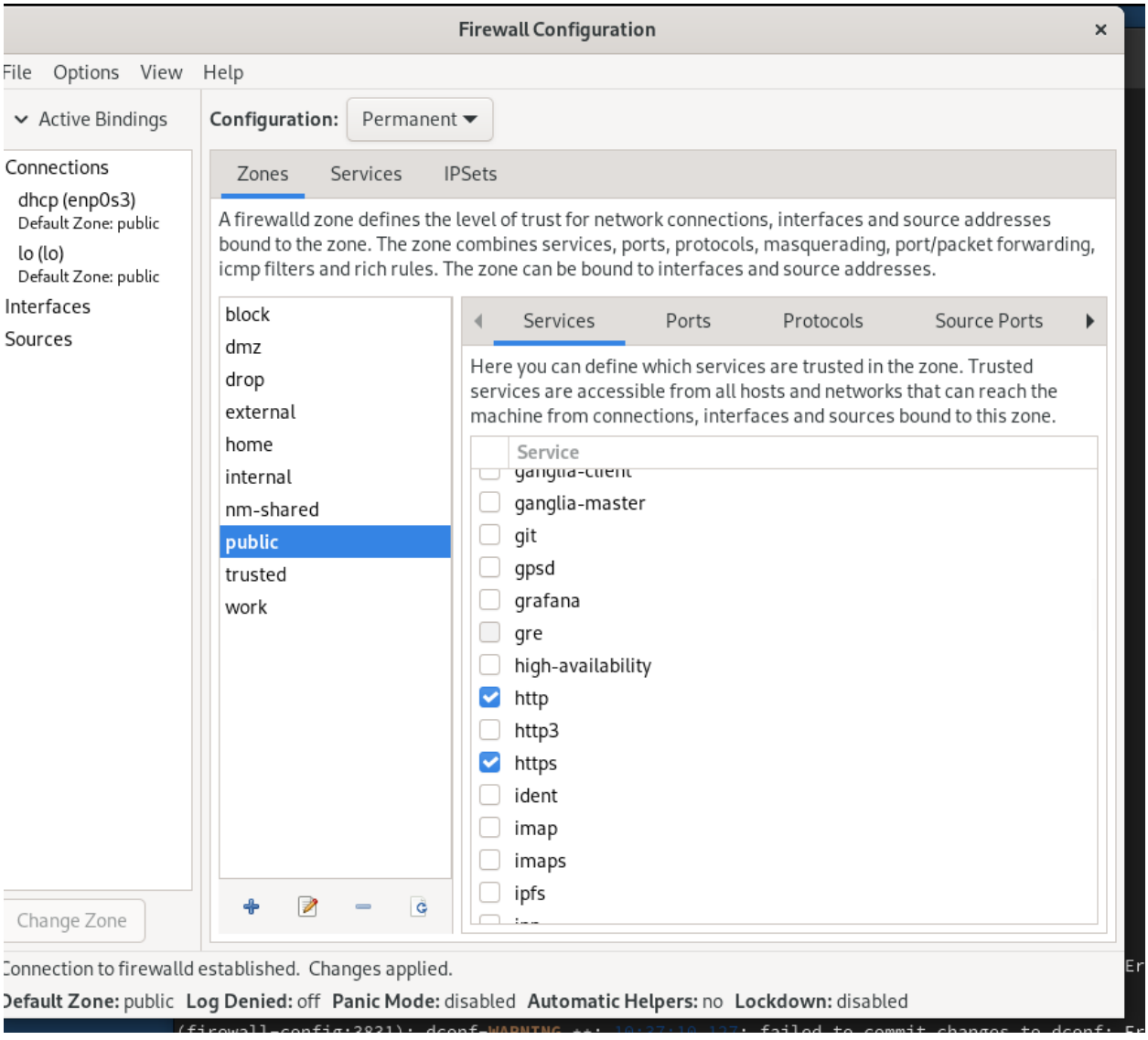
1. Откройте терминал и под учётной записью своего пользователя запустите интерфейс GUI firewall-config: firewall-config

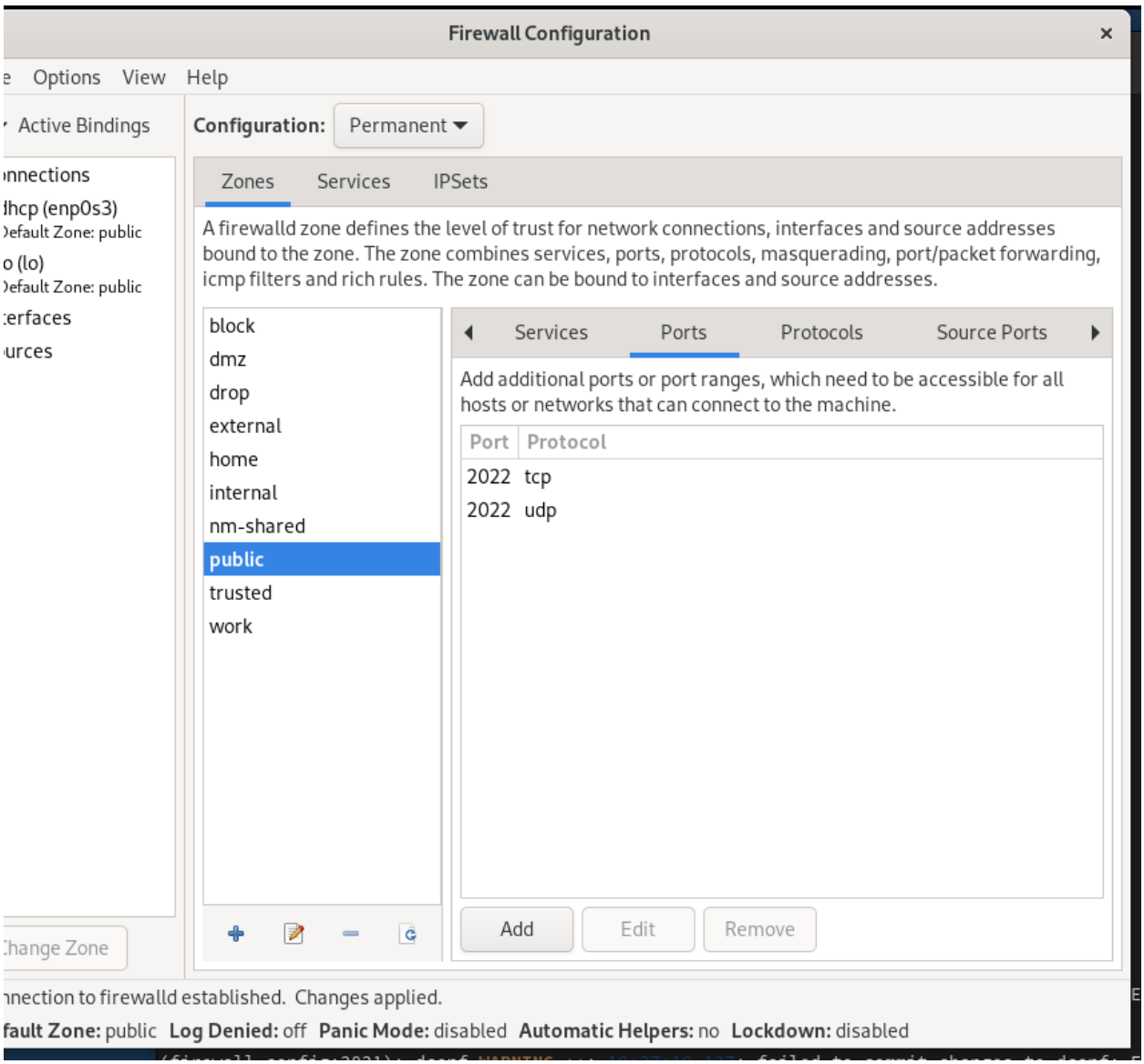
Если служба отсутствует, то система предложит вам её установить. Также при запуске потребуется ввести пароль пользователя с полномочиями управления этой службой.

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 OK , чтобы добавить их в список.



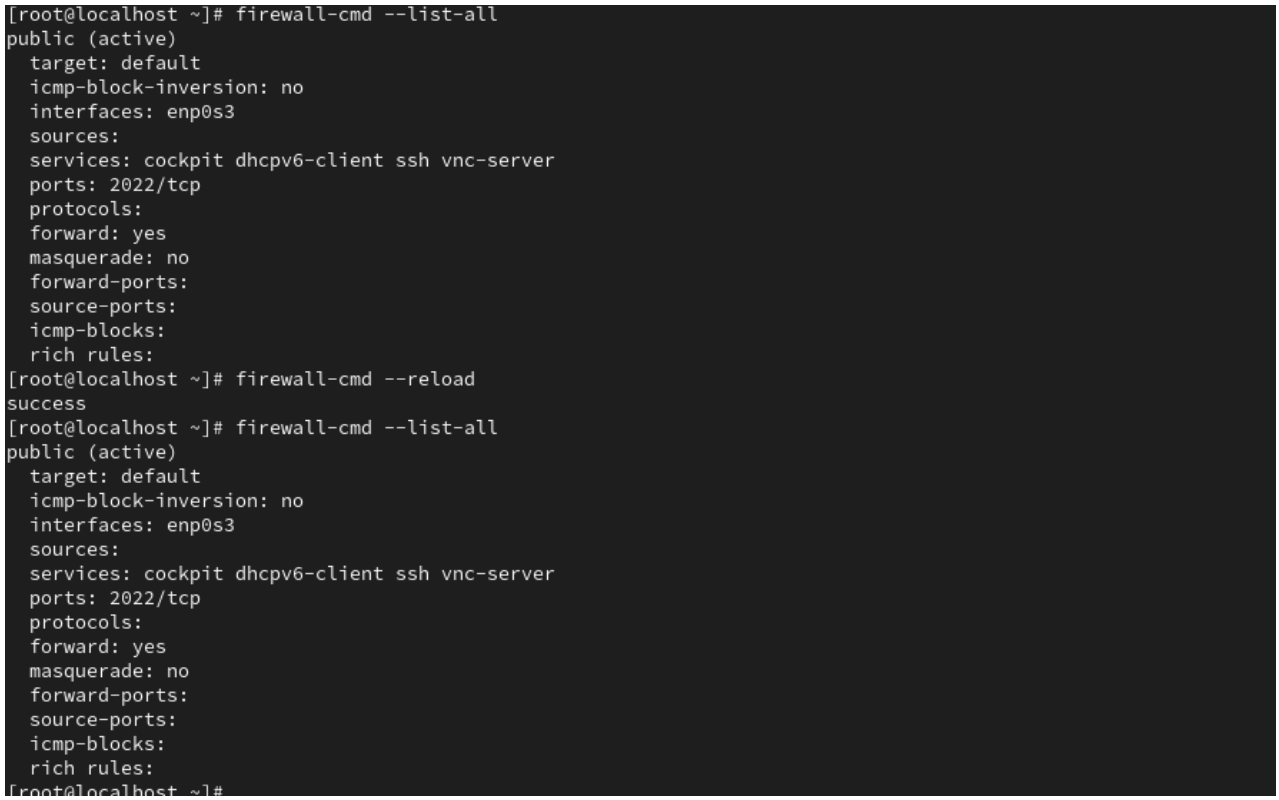

Firewall Configuration
Options
View
Help
Active Bindings
Configuration:
Permanent
Zones
Services
IPSets
A firewalld zone defines the level of trust for network connections, interfaces and source addresses bound to the zone. The zone combines services, ports, protocols, masquerading, port/packet forwarding, 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
Add additional ports or port ranges, which need to be accessible for all hosts or networks that can connect to the machine.
Port
Protocol
2022 tcp
2022 udp
Add
Edit
Remove
Change Zone
nnection to firewalld established. Changes applied.
fault Zone: public Log Denied: off Panic Mode: disabled Automatic Helpers: no Lockdown: disabled

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 вступилив 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.



Самостоятельная работа

1. Создайте конфигурацию межсетевого экрана, которая позволяет получить доступ к следующим службам:

– telnet;

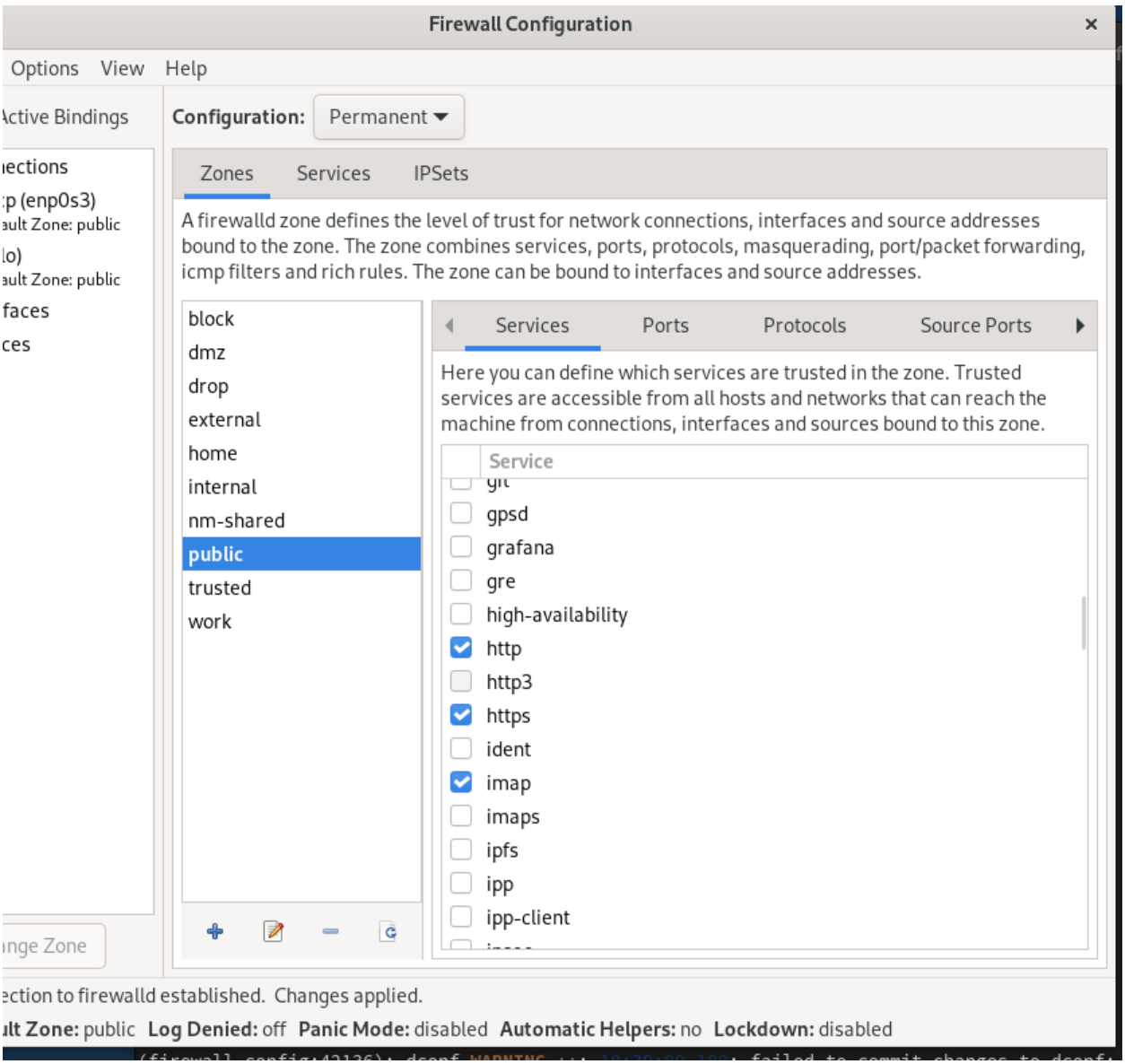
– imap;

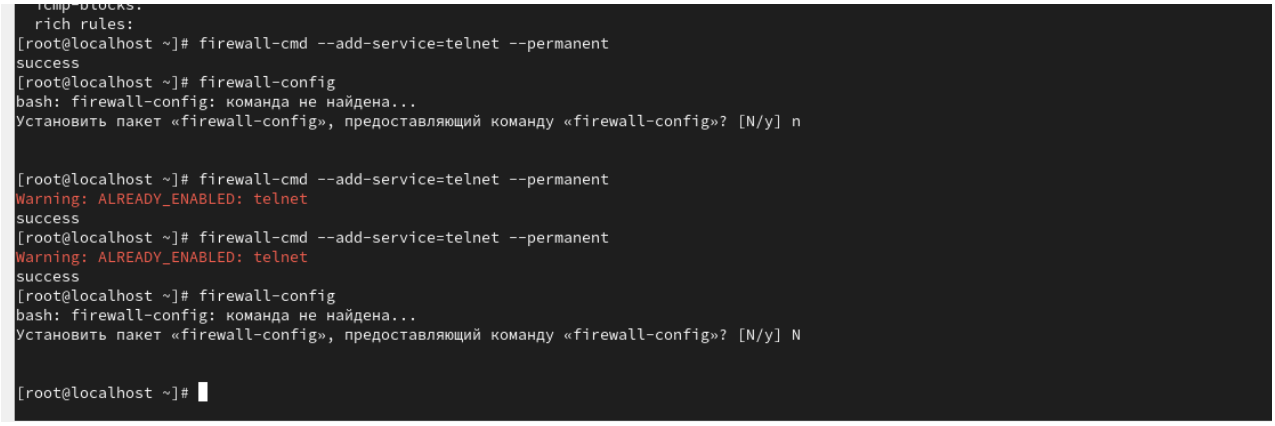
– pop3;

– 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.





Контрольные вопросы

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

Служба, которая должна быть запущена — это 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 порта в зону по умолчанию можно использовать следующую команду:
sudo firewall-cmd --add-port=2355/udp –permanent
Опция --permanent сохраняет изменения после перезагрузки.

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

Для вывода всей конфигурации брандмауэра в всех зонах используйте команду:

sudo firewall-cmd --list-all-zones

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

Для удаления службы из текущей конфигурации используйте команду:

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

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

Для активации конфигурации после применения опции --permanent, используйте команду:

sudo firewall-cmd –reload

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

Чтобы проверить, что конфигурация активна в текущей зоне, используйте команду:

sudo firewall-cmd --list-all

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

Для добавления интерфейса в зону используйте команду:

sudo 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?

Если не указана зона, новый интерфейс будет добавлен в зону по умолчанию, которая, как правило, является зоной public.

Заключение

Получены навыки настройки сетевого пакетного фильтра.