

Лабораторная работа № 13. Фильтр пакетов

Отчёт

Сергеев Даниил Олегович

Содержание

1	Цель работы	5
2	Задание	6
3	Ход выполнения лабораторной работы	7
3.1	Управление брандмауэром с помощью firewall-cmd	7
3.2	Управление брандмауэром с помощью firewall-config	13
4	Самостоятельная работа	17
5	Ответы на контрольные вопросы	20
6	Вывод	22
	Список литературы	23

Список иллюстраций

3.1	Название зоны по умолчанию	7
3.2	Доступные зоны firewalld	7
3.3	Список доступных служб	8
3.4	Службы для default зоны	8
3.5	Параметры текущей зоны и зоны public	9
3.6	Вывод параметров после изменений	10
3.7	Перезапуск firewalld.service	10
3.8	Параметры брандмауэра после перезапуска	11
3.9	Добавляем службу, но уже с параметром –permanent	11
3.10	Вывод после добавления постоянного изменения	12
3.11	Добавление порта в брандмауэр	12
3.12	Установка firewall-config	13
3.13	GUI службы firewall-config	14
3.14	Добавление порта в брандмауэр	15
3.15	Конфигурация после работы в графическом редакторе	16
3.16	Обновленная конфигурация	16
4.1	Обновленная конфигурация	17
4.2	GUI службы firewall-config	18
4.3	Смена зоны на интерфейсе	19
4.4	Конфигурация зоны test	19

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux. [1]

2 Задание

1. Используя `firewall-cmd`:

– определить текущую зону по умолчанию; – определить доступные для настройки зоны; – определить службы, включённые в текущую зону; – добавить сервер VNC в конфигурацию брандмауэра;

2. Используя `firewall-config`:

– добавьте службы `http` и `ssh` в зону `public`; – добавьте порт 2022 протокола UDP в зону `public`; – добавьте службу `ftp`;

3. Выполните задание для самостоятельной работы.

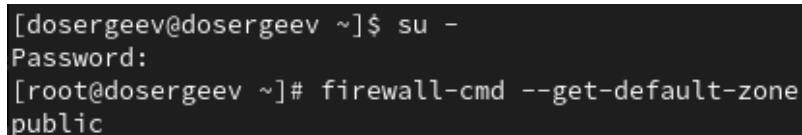
3 Ход выполнения лабораторной работы

3.1 Управление брандмауэром с помощью firewall-cmd

Запустим терминал и зайдем в учетную запись администратора (su -). Начнем с изучения текущей конфигурации брандмауэра.

Определим текущую зону по умолчанию:

```
firewall-cmd --get-default-zone
```



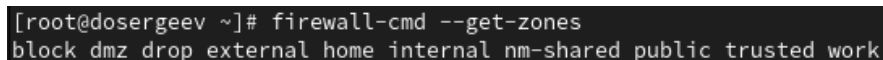
```
[dosergeev@dosergeev ~]$ su -  
Password:  
[root@dosergeev ~]# firewall-cmd --get-default-zone  
public
```

Рис. 3.1: Название зоны по умолчанию

Сейчас по умолчанию установлена зона public.

Определим доступные для настройки зоны:

```
firewall-cmd --get-zones
```



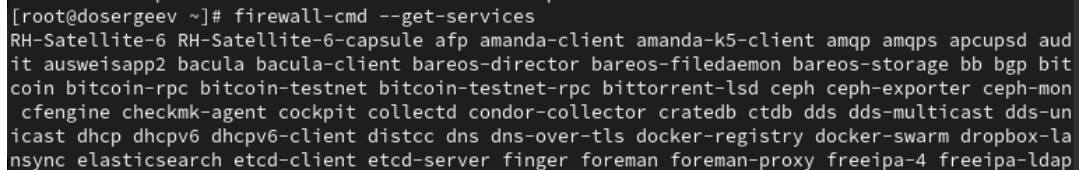
```
[root@dosergeev ~]# firewall-cmd --get-zones  
block dmz drop external home internal nm-shared public trusted work
```

Рис. 3.2: Доступные зоны firewalld

Доступны зоны: block, dmz, drop, external, home, internal, nm-shared, public, trusted, work.

Посмотрим службы, доступные на компьютере:

```
firewall-cmd --get-services
```

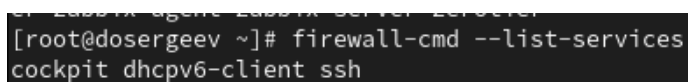


```
[root@dosergeev ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd aud
it ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bit
coin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon
cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-un
icast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-la
nsync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap
```

Рис. 3.3: Список доступных служб

Определим службы, доступные в текущей зоне:

```
firewall-cmd --list-services
```



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

Рис. 3.4: Службы для default зоны

Для зоны public доступны службы cockpit, dhcpv6-client, ssh.

Выведем список всех параметров без опции --zone и с ней.

```
firewall-cmd --list-all
```

```
firewall-cmd --list-all --zone=public
```



```

[root@dosergeev ~]# 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@dosergeev ~]# 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:

```

Рис. 3.5: Параметры текущей зоны и зоны public

Как мы видим, параметры одинаковые, так как public является зоной по умолчанию (ключ `--list-all` выводит параметры зоны по умолчанию или же default).

Добавим сервер VNC в конфигурацию брандмауэра и проверим, добавился ли он:

```

firewall-cmd --add-service=vnc-server
firewall-cmd --list-all

```

```
[root@dosergeev ~]# firewall-cmd --add-service=vnc-server
success
[root@dosergeev ~]# 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:
```

Рис. 3.6: Вывод параметров после изменений

Перезапустим службу firewalld и проверим, что она запущена:

```
systemctl restart firewalld
systemctl status firewalld
```

```
[root@dosergeev ~]# systemctl restart firewalld
[root@dosergeev ~]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
  Active: active (running) since Sat 2025-11-29 20:01:33 MSK; 7s ago
    Docs: man:firewalld(1)
  Process: 3624 ExecStartPost=/usr/bin/firewall-cmd --state (code=exited, status=0/SUCCESS)
 Main PID: 3621 (firewalld)
   Tasks: 2 (limit: 100279)
  Memory: 24.2M
    CPU: 916ms
  CGroup: /system.slice/firewalld.service
          └─3621 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

Nov 29 20:01:32 dosergeev.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon.
..
Nov 29 20:01:33 dosergeev.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
```

Рис. 3.7: Перезапуск firewalld.service

Проверим, есть ли vnc-server в конфигурации после перезапуска:

```
firewall-cmd --list-all
```

```

Nov 29 20:01:32 dosergeev.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon.
..
Nov 29 20:01:33 dosergeev.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
[root@dosergeev ~]# 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:

```

Рис. 3.8: Параметры брандмауэра после перезапуска

Служба `vnc-server` больше не указана. Это произошло потому, что изменения, внесенные без параметра `--permanent`, являются временными до перезагрузки службы и не добавляются в конфигурацию.

Добавим службу `vnc-server` еще раз, но на этот раз сделаем ее постоянной:

```

firewall-cmd --add-service=vnc-server --permanent
firewall-cmd --list-all

```

```

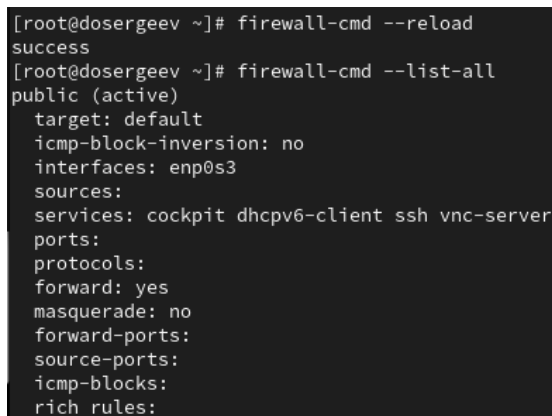
[root@dosergeev ~]# firewall-cmd --add-service=vnc-server --permanent
success
[root@dosergeev ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: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

```

Рис. 3.9: Добавляем службу, но уже с параметром `--permanent`

VNC-сервер все ещё не указан. Перезагрузим конфигурацию `firewalld` и посмотрим конфигурацию времени выполнения:

```
firewall-cmd --reload  
firewall-cmd --list-all
```



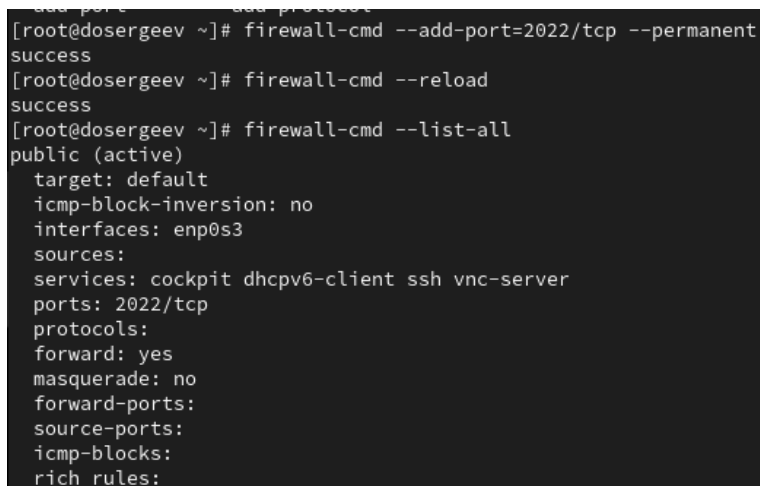
```
[root@dosergeev ~]# firewall-cmd --reload  
success  
[root@dosergeev ~]# firewall-cmd --list-all  
public (active)  
  target: default  
  icmp-block-inversion: no  
  interfaces: enp0s3  
  sources:  
  services: cockpit dhcpv6-client ssh vnc-server  
  ports:  
  protocols:  
  forward: yes  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

Рис. 3.10: Вывод после добавления постоянного изменения

Теперь сервер запущен.

Добавим в конфигурацию порт 2022 протокола TCP, затем перезагрузим брандмауэр:

```
firewall-cmd --add-port=2022/tcp --permanent  
firewall-cmd --reload  
firewall-cmd --list-all
```



```
add port      add protocol  
[root@dosergeev ~]# firewall-cmd --add-port=2022/tcp --permanent  
success  
[root@dosergeev ~]# firewall-cmd --reload  
success  
[root@dosergeev ~]# 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:
```

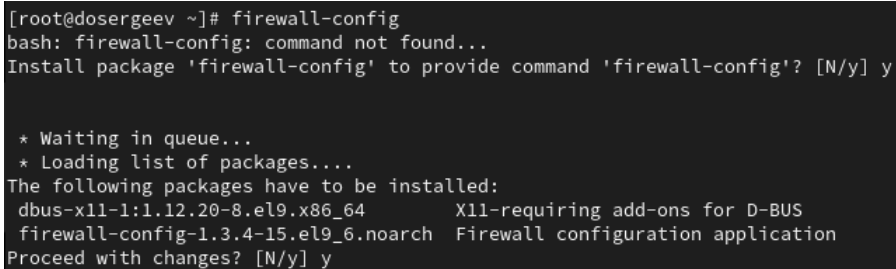
Рис. 3.11: Добавление порта в брандмауэр

3.2 Управление брандмауэром с помощью firewall-config

Под той же учетной записью (root) установим firewall-config и запустим его.

```
dnf install firewall-config
```

или (как в моем случае) из подсказки после ввода `firewall-config`



```
[root@dosergeev ~]# firewall-config
bash: firewall-config: command not found...
Install package 'firewall-config' to provide command 'firewall-config'? [N/y] y

* Waiting in queue...
* Loading list of packages....
The following packages have to be installed:
dbus-x11-1:1.12.20-8.el9.x86_64      X11-requiring add-ons for D-BUS
firewall-config-1.3.4-15.el9_6.noarch Firewall configuration application
Proceed with changes? [N/y] y
```

Рис. 3.12: Установка firewall-config

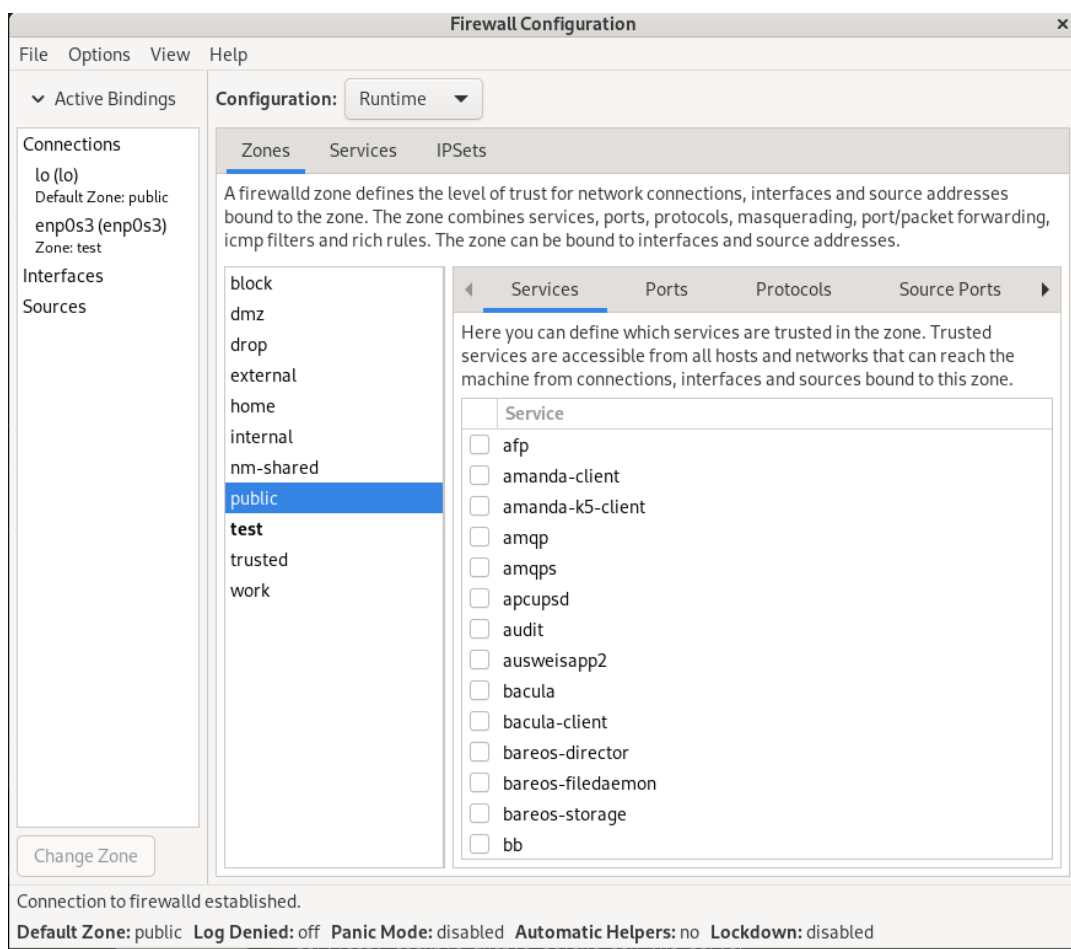


Рис. 3.13: GUI службы firewall-config

Нажмем выпадающее меню рядом с параметром Configuration. Откроем раскрывающийся список и выберем Permanent. Это позволит сделать все изменения постоянными. Выберем зону public и отметим службы http, https и ftp (в поле Services), чтобы включить их.

Теперь выберем вкладку Ports и на этой вкладке нажмем Add. Введем порт 2022 и укажем протокол udp.

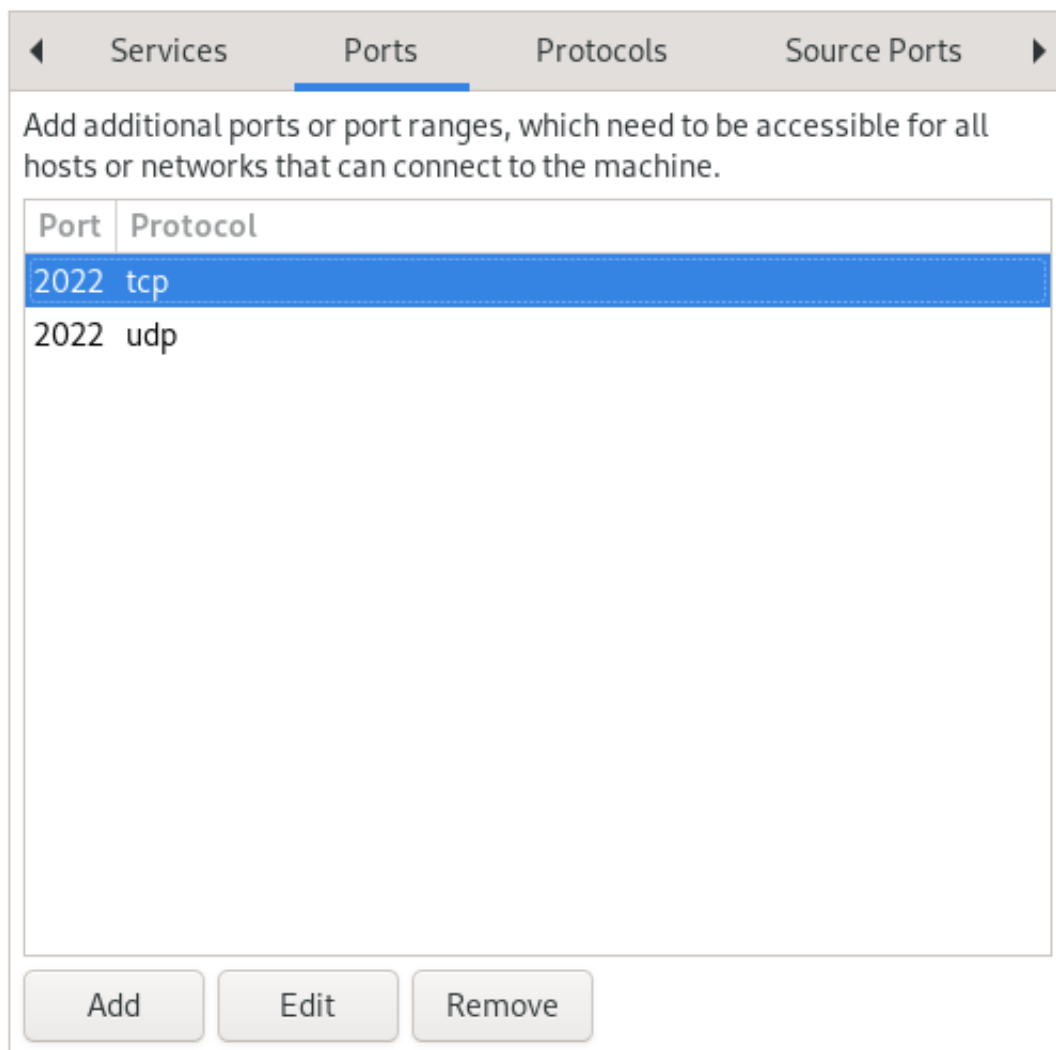


Рис. 3.14: Добавление порта в брандмауэр

Закроем утилиту `firewall-config` и проверим изменения.

```
firewall-cmd --list-all
```

```
[root@dosergeev ~]# 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:
```

Рис. 3.15: Конфигурация после работы в графическом редакторе

Чтобы изменения вступили в силу, перезагрузим конфигурацию firewalld.

```
firewall-cmd --reload
```

```
firewall-cmd --list-all
```

```
[root@dosergeev ~]# firewall-cmd --reload
success
[root@dosergeev ~]# 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@dosergeev ~]#
```

Рис. 3.16: Обновленная конфигурация

4 Самостоятельная работа

Создадим новую зону для работы. Назовем её test:

обязательно укажем параметр --permanent, иначе зона не создастся

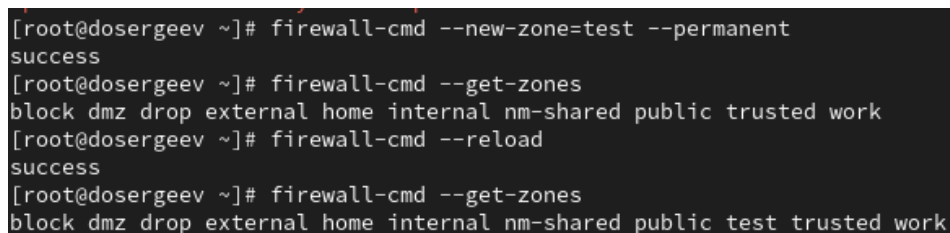
```
firewall-cmd --new-zone=test --permanent
```

проверим, добавилась ли зона

```
firewall-cmd --get-zones
```

```
firewall-cmd --reload
```

```
firewall-cmd --get-zones
```

A screenshot of a terminal window showing the execution of firewall commands. The commands and their outputs are: 1. 'firewall-cmd --new-zone=test --permanent' returns 'success'. 2. 'firewall-cmd --get-zones' returns 'block dmz drop external home internal nm-shared public trusted work'. 3. 'firewall-cmd --reload' returns 'success'. 4. 'firewall-cmd --get-zones' returns 'block dmz drop external home internal nm-shared public test trusted work'. The 'test' zone has been successfully added to the list of zones.

```
[root@dosergeev ~]# firewall-cmd --new-zone=test --permanent
success
[root@dosergeev ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@dosergeev ~]# firewall-cmd --reload
success
[root@dosergeev ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public test trusted work
```

Рис. 4.1: Обновленная конфигурация

Добавим службу telnet в командной строке:

```
firewall-cmd --add-service=telnet --zone=test --permanent
```

Теперь откроем графический интерфейс и в нем добавим службы imap, pop3 и smtp.

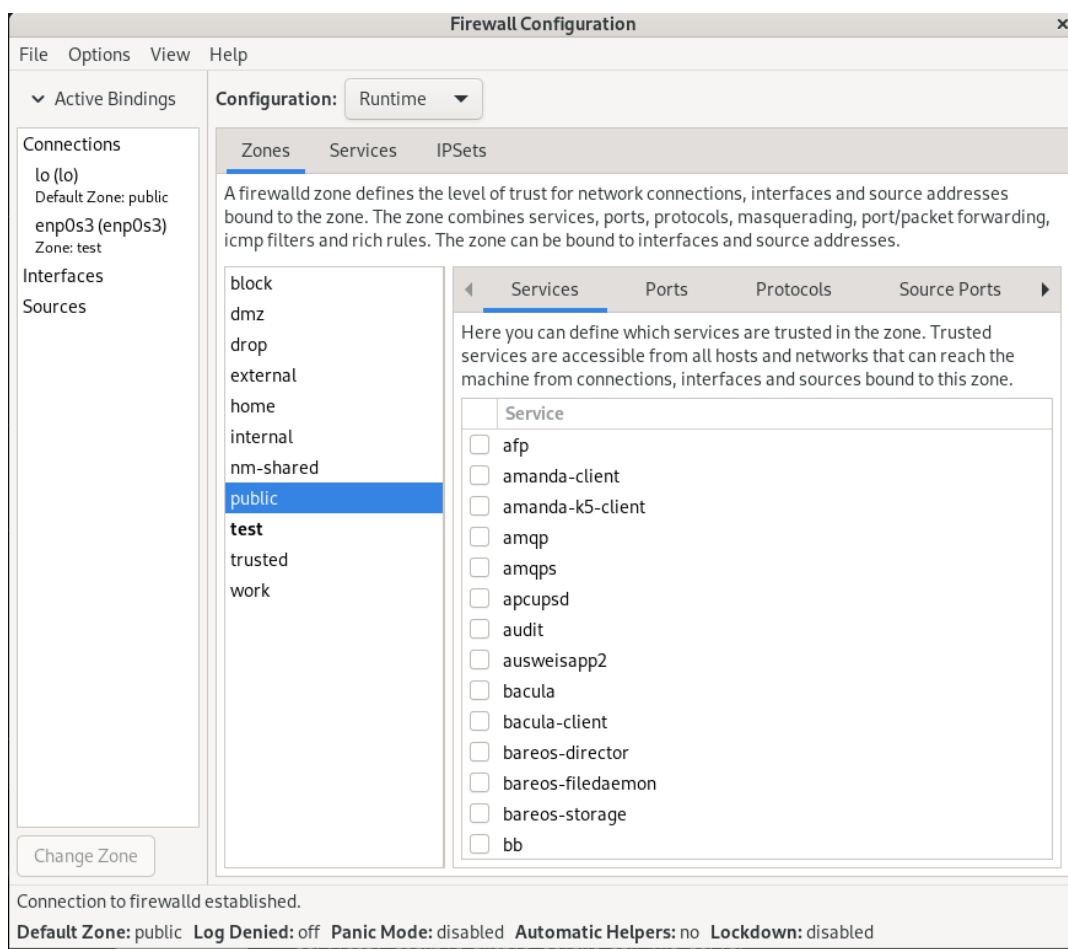


Рис. 4.2: GUI службы firewall-config

Сменим активную зону интерфейса enp0s3 с public на test

```
firewall-cmd --change-interface=enp0s3 --zone=test --permanent
firewall-cmd --reload
firewall-cmd --list-all
```

```

[root@dosergeev ~]# firewall-cmd --change-interface=enp0s3 --zone=test --permanent
The interface is under control of NetworkManager, setting zone to 'test'.
success
[root@dosergeev ~]# firewall-cmd --reload
success
[root@dosergeev ~]# firewall-cmd --list-all
You're performing an operation over default zone ('public'),
but your connections/interfaces are in zone 'test' (see --get-active-zones)
You most likely need to use --zone=test option.

public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: cockpit dhcpv6-client ftp http https ssh telnet vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

```

Рис. 4.3: Смена зоны на интерфейсе

Так как по умолчанию стоит зона public, выводим параметры с указанием конкретной зоны:

```
firewall-cmd --list-all --zone=test
```

```

[root@dosergeev ~]# firewall-cmd --list-all --zone=test
test (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: imap pop3 smtp telnet
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

```

Рис. 4.4: Конфигурация зоны test

5 Ответы на контрольные вопросы

1. Какая служба должна быть запущена перед началом работы с менеджером конфигурации брандмауэра `firewall-config`?
 - `firewalld.service`
2. Какая команда позволяет добавить UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию?
 - `firewall-cmd --add-port=2355/udp --permanent`
3. Какая команда позволяет показать всю конфигурацию брандмауэра во всех зонах?
 - `firewall-cmd --list-all-zones`
4. Какая команда позволяет удалить службу `vnc-server` из текущей конфигурации брандмауэра?
 - `firewall-cmd --remove-service=vnc-server --permanent`
5. Какая команда `firewall-cmd` позволяет активировать новую конфигурацию, добавленную опцией `--permanent`?
 - `firewall-cmd --reload`
6. Какой параметр `firewall-cmd` позволяет проверить, что новая конфигурация была добавлена в текущую зону и теперь активна?

- `firewall-cmd --list-all`

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

- `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?

- В зону по умолчанию. Её можно узнать, используя команду `firewall-cmd --get-default-zone`

6 Вывод

В результате выполнения лабораторной работы я получил навыки работы с брандмауэром службы `firewalld`, узнал как настраивать и применять конфигурацию для текущей зоны и как упростить конфигурацию с помощью утилиты `firewall-config`

Список литературы

1. Kulyabov, Korolykova. Лабораторная работа № 13. Фильтр пакетов. https://esystem.rudn.ru/pluginfile.php/2843521/mod_resource/content/4/014-firewall.pdf; RUDN.