

Лабораторная работа №13

Отчет

Устинова Виктория Вадимовна

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	13
4.1	Ответы на контрольные вопросы	13

Список иллюстраций

3.1	Текущая public, и смотрим остальные доступные	7
3.2	Вывод одинаковый так как public	7
3.3	Добавился в конфигурацию	8
3.4	VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения	8
3.5	после перезагрузки все есть	9
3.6	после перезагрузки все есть	9
3.7	Выполняем	10
3.8	Выполняем	10
3.9	теперь видны изменения все добавилось	11
3.10	Добавляем imap pop3 smtp через графический интерфейс	11
3.11	Добавляем telnet через командную строку	12
3.12	Мы проверили и у нас все добавилось!	12

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

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 (раздел 13.5).

Добавьте сервер VNC в конфигурацию брандмауэра, Проверьте, добавился ли vnc-server в конфигурацию, (рис. 3.3).

```
[root@vvustinova ~]# firewall-cmd --add-service=vnc-server
success
[root@vvustinova ~]# 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. 3.3: Добавился в конфигурацию

Перезапустите службу firewalld, проверьте, есть ли vnc-server в конфигурации, Добавьте службу vnc-server ещё раз, но на этот раз сделайте её постоянной, используя команду(рис. 3.4).

```
[root@vvustinova ~]# systemctl restart firewalld
[root@vvustinova ~]# 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@vvustinova ~]# firewall-cmd --add-service=vnc-server --permanent
success
```

Рис. 3.4: VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения

Проверьте наличие vnc-server в конфигурации, Перезагрузите конфигурацию firewalld и просмотрите конфигурацию времени выполнения(рис. 3.5).

```

success
[root@vvustinova ~]# 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@vvustinova ~]# firewall-cmd --reload
success
[root@vvustinova ~]# 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

```

Рис. 3.5: после перезагрузки все есть

Добавьте в конфигурацию межсетевого экрана порт 2022 протокола TCP, Затем перезагрузите конфигурацию firewalld, проверьте что добавлен(рис. 3.6).

```

rich rules:
[root@vvustinova ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@vvustinova ~]# firewall-cmd --reload
success
[root@vvustinova ~]# 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@vvustinova ~]#

```

Рис. 3.6: после перезагрузки все есть

Нажмите выпадающее меню рядом с параметром Configuration . Откройте раскрывающийся список и выберите Permanent Выберите зону public и отметьте службы http, https и ftp, чтобы включить их.(рис. 3.7).

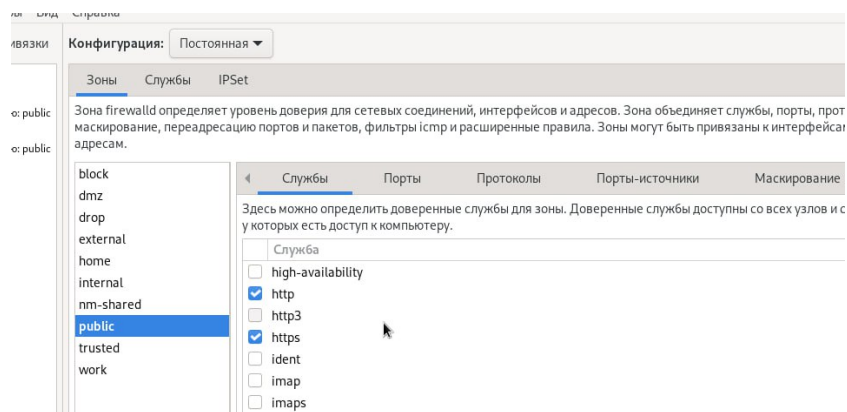


Рис. 3.7: Выполняем

Выберите вкладку Ports и на этой вкладке нажмите Add . Введите порт 2022 и протокол udp, нажмите ОК(рис. 3.8).

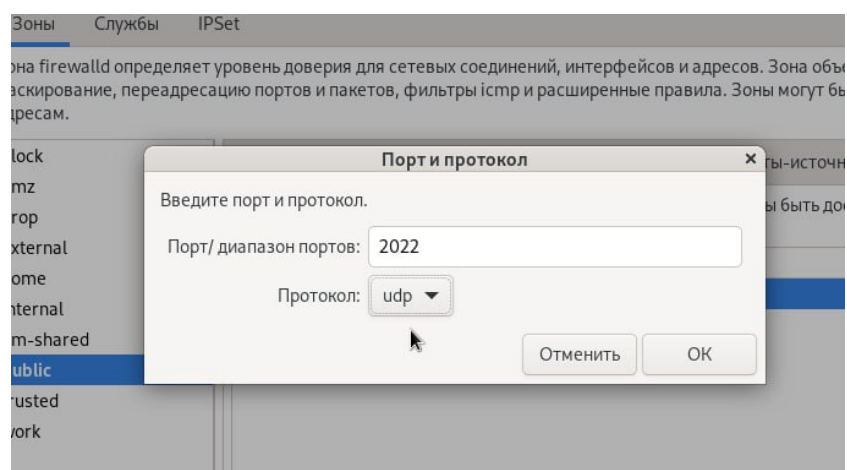


Рис. 3.8: Выполняем

Перегрузите конфигурацию firewall-cmd, и список доступных сервисов(рис. 3.9).

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

Рис. 3.9: теперь видны изменения все добавилось

Создайте конфигурацию межсетевого экрана, которая позволяет получить доступ к следующим службам:– telnet;– imap;– pop3;– smtp.(рис. 3.10).

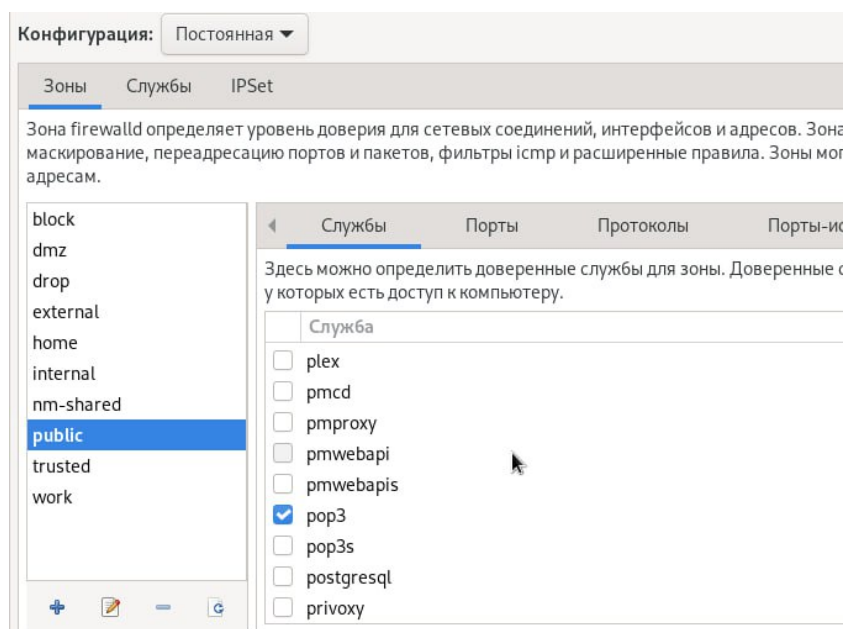
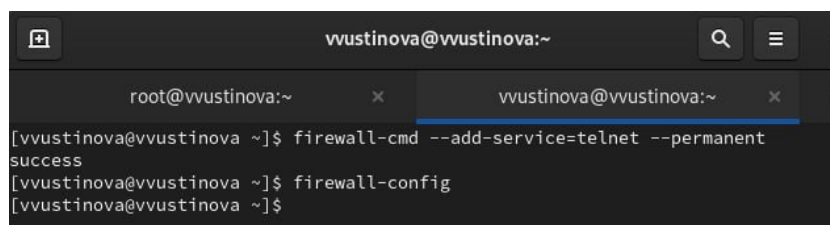


Рис. 3.10: Добавляем imap pop3 smtp через графический интерфейс

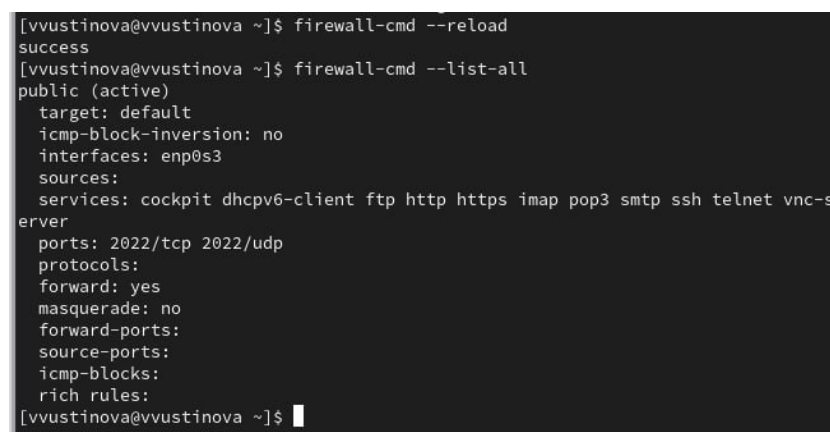
Создайте конфигурацию межсетевого экрана, которая позволяет получить доступ к следующим службам:– telnet;– imap;– pop3;– smtp.(рис. 3.11).



```
vvustinova@vvustinova:~  
root@vvustinova:~  
vvustinova@vvustinova:~  
[vvustinova@vvustinova ~]$ firewall-cmd --add-service=telnet --permanent  
success  
[vvustinova@vvustinova ~]$ firewall-config  
[vvustinova@vvustinova ~]$
```

Рис. 3.11: Добавляем telnet через командную строку

Убедитесь, что конфигурация является постоянной и будет активирована после перезагрузки компьютера(рис. 3.12).



```
[vvustinova@vvustinova ~]$ firewall-cmd --reload  
success  
[vvustinova@vvustinova ~]$ 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:  
[vvustinova@vvustinova ~]$
```

Рис. 3.12: Мы проверили и у нас все добавилось!

4 Выводы

Мы успешно получили навыки настройки пакетного фильтра в Linux.

4.1 Ответы на контрольные вопросы

Вот ответы на ваши вопросы по firewalld:

1. Какая служба должна быть запущена перед началом работы с менеджером конфигурации брандмауэра firewall-config? Служба firewalld (или firewalld.service).
2. Какая команда позволяет добавить UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию? firewall-cmd --add-port=2355/udp (Если зона по умолчанию не public, можно явно указать --zone=public, например: firewall-cmd --zone=public --add-port=2355/udp)
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
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` (показывает всю активную конфигурацию для текущей/дефолтной зоны). Или, если вы добавляли что-то конкретное (например, сервис или порт): `firewall-cmd --query-service=http` (проверить сервис) `firewall-cmd --query-port=80/tcp` (проверить порт)
7. Какая команда позволяет добавить интерфейс `eno1` в зону `public`? `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? Он будет добавлен в зону по умолчанию (`default zone`), которая установлена для вашей системы `firewalld`. Эту зону можно узнать командой `firewall-cmd --get-default-zone`.