

Отчёт по лабораторной работе №13

Дисциплина: Основы администрирования операционных систем

Верниковская Екатерина Андреевна

Содержание

| | | |
|----------|---|-----------|
| 1 | Цель работы | 5 |
| 2 | Задание | 6 |
| 3 | Выполнение лабораторной работы | 7 |
| 3.1 | Управление брандмауэром с помощью firewall-cmd | 7 |
| 3.2 | Управление брандмауэром с помощью firewall-config | 12 |
| 3.3 | Самостоятельная работа | 17 |
| 4 | Контрольные вопросы + ответы | 20 |
| 5 | Выводы | 22 |
| 6 | Список литературы | 23 |

Список иллюстраций

| | | |
|------|---|----|
| 3.1 | Режим суперпользователя | 7 |
| 3.2 | Определение текущей зоны по умолчанию | 7 |
| 3.3 | Определение доступных зон | 7 |
| 3.4 | Службы доступные на нашем компьютере | 8 |
| 3.5 | Определение доступных служб в текущей зоне | 8 |
| 3.6 | Вывод команды <code>firewall-cmd --list-all</code> | 8 |
| 3.7 | Вывод команды <code>firewall-cmd --list-all --zone=public</code> | 9 |
| 3.8 | Добавление сервера VNC в конфигурацию брандмауэра | 9 |
| 3.9 | Проверка добавления сервера VNC в конфигурацию | 9 |
| 3.10 | Перезапуск службы <code>firewalld</code> | 10 |
| 3.11 | Проверка наличия сервера VNC в конфигурации после перезапуска | 10 |
| 3.12 | Добавление постоянного сервера VNC в конфигурацию брандмауэра | 10 |
| 3.13 | Проверка наличия постоянного сервера VNC в конфигурации | 11 |
| 3.14 | Перезагрузка конфигурации <code>firewalld</code> (1) | 11 |
| 3.15 | Просмотр конфигурации времени выполнения | 11 |
| 3.16 | Добавление порта в конфигурацию | 12 |
| 3.17 | Перезагрузка конфигурации <code>firewalld</code> (2) | 12 |
| 3.18 | Проверка добавления порта в конфигурацию | 12 |
| 3.19 | Установка <code>firewall-config</code> | 13 |
| 3.20 | Ввод пароля | 13 |
| 3.21 | Интерфейс GUI <code>firewall-config</code> | 14 |
| 3.22 | Выбор Permanent | 14 |
| 3.23 | Включение служб <code>http</code> , <code>https</code> и <code>ftp</code> | 15 |
| 3.24 | Добавление порта | 15 |
| 3.25 | Проверка внесённых изменений (1) | 16 |
| 3.26 | Перезагрузка конфигурации <code>firewall-cmd</code> (1) | 16 |
| 3.27 | Проверка внесённых изменений (2) | 16 |
| 3.28 | Добавление постоянного <code>telnet</code> | 17 |
| 3.29 | Открытие интерфейса GUI <code>firewall-config</code> | 17 |
| 3.30 | Включение служб <code>imap</code> , <code>pop3</code> и <code>smtp</code> | 18 |
| 3.31 | Перезагрузка конфигурации <code>firewall-cmd</code> (2) | 18 |
| 3.32 | Проверка внесённых изменений (3) | 19 |
| 3.33 | Перезагрузка ОС | 19 |
| 3.34 | Проверка внесённых изменений после перезагрузки ОС | 19 |

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`:

- добавить службы `http` и `ssh` в зону `public`
- добавить порт 2022 протокола UDP в зону `public`
- добавить службу `ftp`

3. Выполнить задание для самостоятельной работы

3 Выполнение лабораторной работы

3.1 Управление брандмауэром с помощью firewall-cmd

Запускаем терминала и получаем полномочия суперпользователя, используя *su* - (рис. 3.1)

```
[eavernikovskaya@eavernikovskaya ~]$ su -  
Password:  
[root@eavernikovskaya ~]#
```

Рис. 3.1: Режим суперпользователя

Определим текущую зону по умолчанию, введя: *firewall-cmd --get-default-zone* (рис. 3.2)

```
[root@eavernikovskaya ~]# firewall-cmd --get-default-zone  
public  
[root@eavernikovskaya ~]#
```

Рис. 3.2: Определение текущей зоны по умолчанию

Определим доступные зоны, введя: *firewall-cmd --get-zones* (рис. 3.3)

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

Рис. 3.3: Определение доступных зон

Посмотрим службы, доступные на нашем компьютере, используя *firewall-cmd --get-services* (рис. 3.4)

```
[root@eavernikovskaya ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacul
a bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin
-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cr
atedb etdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-s
warm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap free
ipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gnsd grafana gre high-avail
lability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdec
onnect kerberos kibana klogind kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-se
cure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-se
cure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llm
nr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountrd mqtt mqtt-tls ms-wbt ms
sql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovir
t-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prom
etheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentin
el rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submission
smtps snmp snmp-tls snmp-tls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn sy
ncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmi
sion-client upnp-client vdsms vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client
ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbbx-agent zabb
ix-server zerotier
[root@eavernikovskaya ~]#
```

Рис. 3.4: Службы доступные на нашем компьютере

Определим доступные службы в текущей зоне: *firewall-cmd --list-services* (рис. 3.5)

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

Рис. 3.5: Определение доступных служб в текущей зоне

Сравним результаты вывода информации при использовании команд *firewall-cmd --list-all* и *firewall-cmd --list-all --zone=public*. Результат одинаковый, так как в настоящее время зона *public* является активной зоной по умолчанию (рис. 3.6), (рис. 3.7)

```
[root@eavernikovskaya ~]# 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@eavernikovskaya ~]#
```

Рис. 3.6: Вывод команды *firewall-cmd --list-all*


```
[root@eavernikovskaya ~]# 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@eavernikovskaya ~]#
```

Рис. 3.7: Вывод команды `firewall-cmd --list-all --zone=public`

Добавим сервер VNC в конфигурацию брандмауэра: `firewall-cmd --add-service=vnc-server` (рис. 3.8)

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

Рис. 3.8: Добавление сервера VNC в конфигурацию брандмауэра

Проверим, добавился ли `vnc-server` в конфигурацию: `firewall-cmd --list-all` (рис. 3.9)

```
[root@eavernikovskaya ~]# 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@eavernikovskaya ~]#
```

Рис. 3.9: Проверка добавления сервера VNC в конфигурацию

Перезапустим службу `firewalld`: `systemctl restart firewalld` (рис. 3.10)

```
[root@eavernikovskaya ~]# systemctl restart firewalld
[root@eavernikovskaya ~]#
```

Рис. 3.10: Перезапуск службы `firewalld`

Проверим, есть ли `vnc-server` в конфигурации: `firewall-cmd --list-all`. Его нет, так как служба `vnc-server` не постоянная (рис. 3.11)

```
[root@eavernikovskaya ~]# 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@eavernikovskaya ~]#
```

Рис. 3.11: Проверка наличия сервера VNC в конфигурации после перезапуска

Добавим службу `vnc-server` ещё раз, но на этот раз сделаем её постоянной, используя команду `firewall-cmd --add-service=vnc-server --permanent` (рис. 3.12)

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

Рис. 3.12: Добавление постоянного сервера VNC в конфигурацию брандмауэра

Проверим наличие `vnc-server` в конфигурации: `firewall-cmd --list-all`. Мы увидим, что VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения (рис. 3.13)

```
[root@eavernikovskaya ~]# 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@eavernikovskaya ~]#
```

Рис. 3.13: Проверка наличия постоянного сервера VNC в конфигурации

Перезагрузим конфигурацию firewalld и посмотрим конфигурацию времени выполнения: *firewall-cmd --reload* и *firewall-cmd --list-all* (рис. 3.14), (рис. 3.15)

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

Рис. 3.14: Перезагрузка конфигурации firewalld (1)

```
[root@eavernikovskaya ~]# 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@eavernikovskaya ~]#
```

Рис. 3.15: Просмотр конфигурации времени выполнения

Добавим в конфигурацию межсетевого экрана порт 2022 протокола TCP: *firewall-cmd --add-port=2022/tcp --permanent* (рис. 3.16)

```
[root@eavernikovskaya ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@eavernikovskaya ~]#
```

Рис. 3.16: Добавление порта в конфигурацию

Затем снова перезагрузим конфигурацию firewalld: *firewall-cmd --reload* (рис. 3.17)

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

Рис. 3.17: Перезагрузка конфигурации firewalld (2)

И проверим, что порт добавлен в конфигурацию: *firewall-cmd --list-all* (рис. 3.18)

```
[root@eavernikovskaya ~]# 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@eavernikovskaya ~]#
```

Рис. 3.18: Проверка добавления порта в конфигурацию

3.2 Управление брандмауэром с помощью *firewall-config*

Открываем терминал и под учётной записью нашего пользователя запускаем интерфейс GUI *firewall-config*: *firewall-config*. Служба отсутствует, и система

предлагает нам её установить. Также при запуске вводим пароль пользователя с полномочиями управления этой службой (рис. 3.19), (рис. 3.20), (рис. 3.21)

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

Рис. 3.19: Установка firewall-config

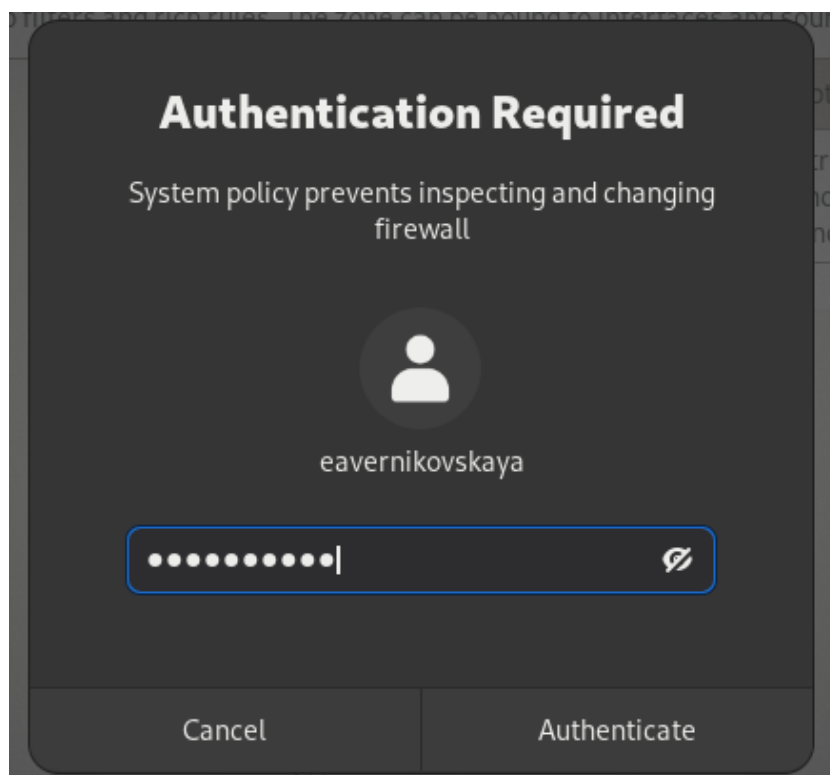


Рис. 3.20: Ввод пароля

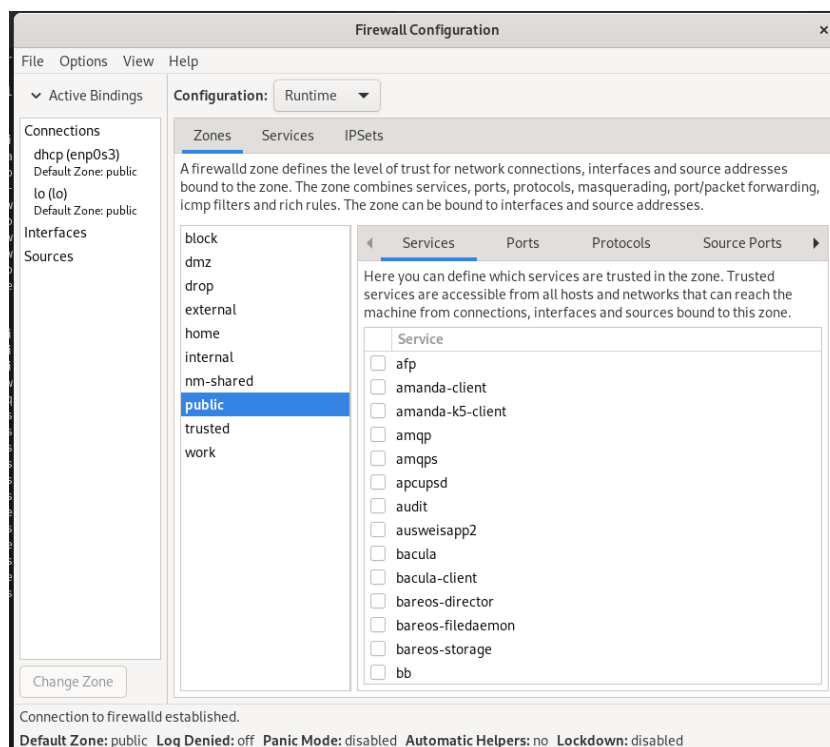


Рис. 3.21: Интерфейс GUI firewall-config

Нажимаем выпадающее меню рядом с параметром Configuration. Открываем раскрывающийся список и выбираем Permanent. Это позволит сделать постоянными все изменения, которые мы вносим при конфигурировании (рис. 3.22)

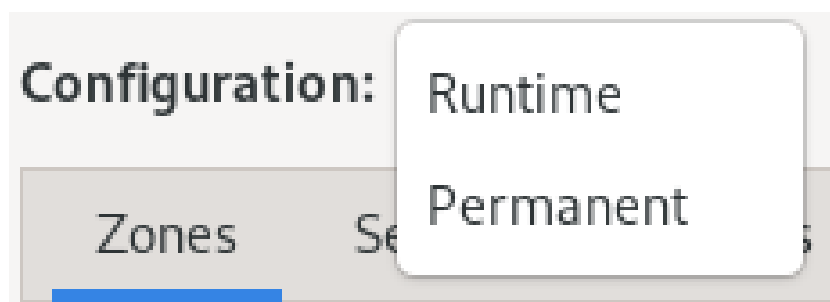


Рис. 3.22: Выбор Permanent

Выбираем зону public и отмечаем службы http, https и ftp, чтобы включить их (рис. 3.23)

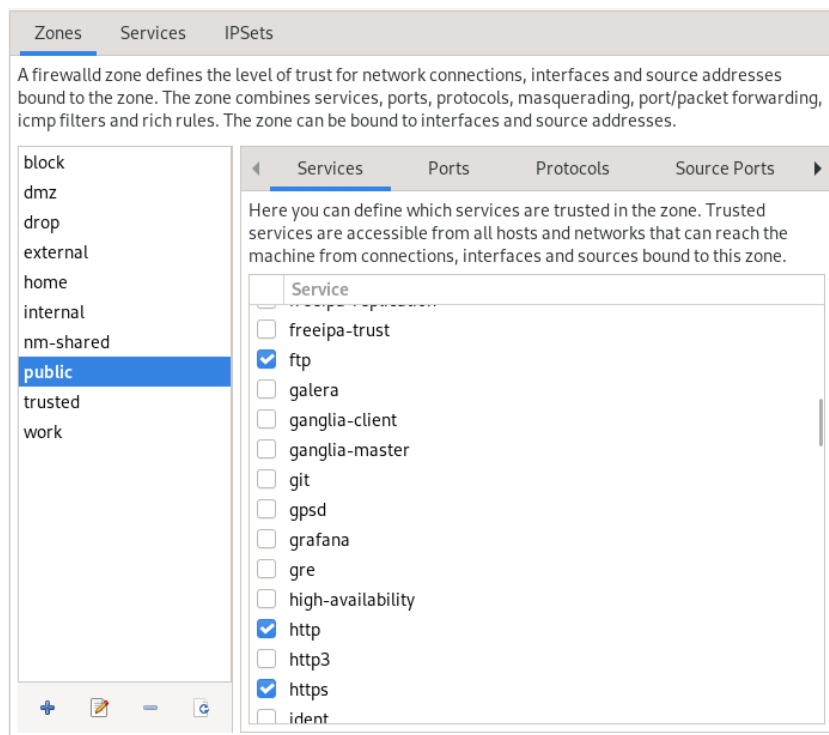


Рис. 3.23: Включение служб http, https и ftp

Выбираем вкладку Ports и на этой вкладке нажимаем Add. Вводим порт 2022 и протокол udp, нажимаем ОК, чтобы добавить их в список (рис. 3.24)

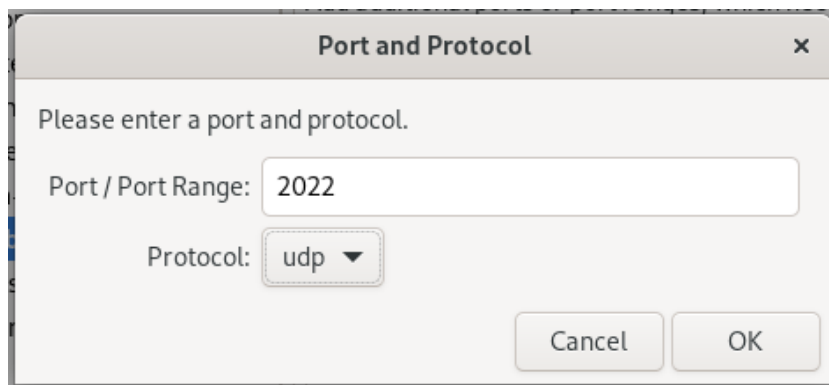


Рис. 3.24: Добавление порта

Закрываем утилиту firewall-config. В окне терминала вводим *firewall-cmd --list-all*. Изменения, которые мы только что внесли, ещё не вступили в силу. Это связано с тем, что мы настроили их как постоянные изменения, а не как изменения времени выполнения (рис. 3.25)

```
[eavernikovskaya@eavernikovskaya ~]$ 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:
[eavernikovskaya@eavernikovskaya ~]$
```

Рис. 3.25: Проверка внесённых изменений (1)

Перезагрузим конфигурацию firewall-cmd: *firewall-cmd --reload* (рис. 3.26)

```
[eavernikovskaya@eavernikovskaya ~]$ firewall-cmd --reload
success
[eavernikovskaya@eavernikovskaya ~]$
```

Рис. 3.26: Перезагрузка конфигурации firewall-cmd (1)

Снова проверяем список доступных сервисов. Мы видим, что изменения вступили в силу (рис. 3.27)

```
[eavernikovskaya@eavernikovskaya ~]$ 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:
[eavernikovskaya@eavernikovskaya ~]$
```

Рис. 3.27: Проверка внесённых изменений (2)

3.3 Самостоятельная работа

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

Сделаем службу telnet постоянной в командной строке: *firewall-cmd --add-service=telnet --permanent* (рис. 3.28)

```
[root@eavernikovskaya ~]# firewall-cmd --add-service=telnet --permanent
success
[root@eavernikovskaya ~]#
```

Рис. 3.28: Добавление постоянного telnet

Открываем интерфейс GUI firewall-config: *firewall-config* (рис. 3.29)

```
[eavernikovskaya@eavernikovskaya ~]$ firewall-config
```

Рис. 3.29: Открытие интерфейса GUI firewall-config

Далее нажимаем выпадающее меню рядом с параметром Configuration. Открываем раскрывающийся список и выбираем Permanent. Выбираем зону public и отмечаем службы imap, pop3 и smtp, чтобы включить их (рис. 3.30)

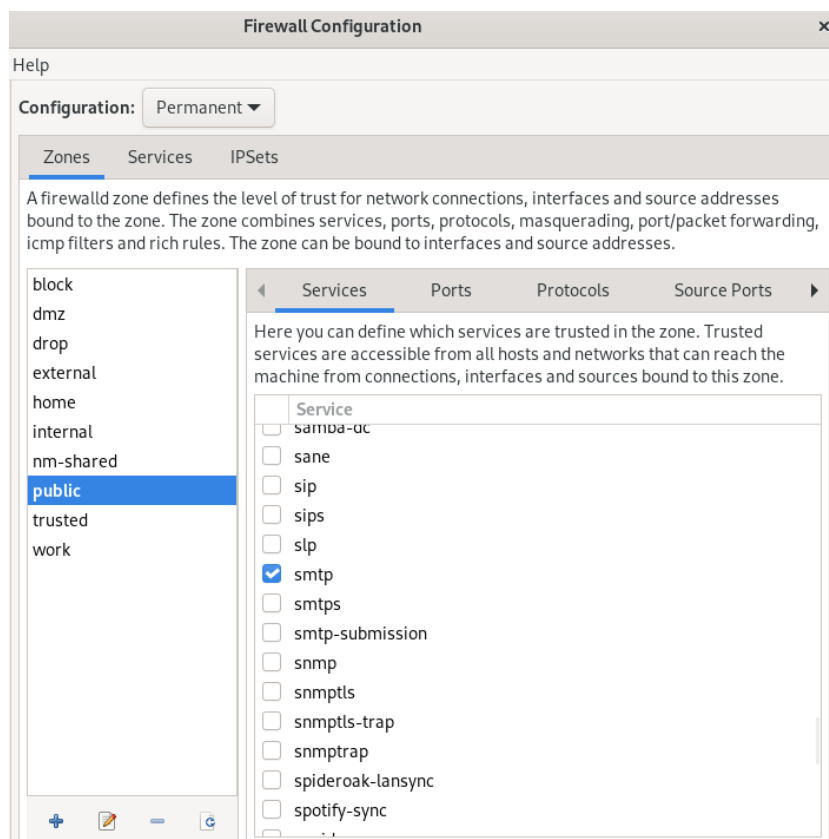


Рис. 3.30: Включение служб imap, pop3 и smtp

Перезагружаем конфигурацию firewall-cmd и проверяем, что изменения были применены (рис. 3.31), (рис. 3.32)

```
[eavernikovskaya@eavernikovskaya ~]$ firewall-cmd --reload
success
[eavernikovskaya@eavernikovskaya ~]$
```

Рис. 3.31: Перезагрузка конфигурации firewall-cmd (2)

```
[eavernikovskaya@eavernikovskaya ~]$ 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:
```

Рис. 3.32: Проверка внесённых изменений (3)

Далее убедимся, что конфигурация является постоянной и будет активирована после перезагрузки компьютера (рис. 3.33), (рис. 3.34)

```
[eavernikovskaya@eavernikovskaya ~]$ reboot
```

Рис. 3.33: Перезагрузка ОС

```
[eavernikovskaya@eavernikovskaya ~]$ 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:
```

Рис. 3.34: Проверка внесённых изменений после перезагрузки ОС

4 Контрольные вопросы + ответы

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

`sudo systemctl start firewalld`

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`

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 --zone="zone-name"`

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

`firewall-cmd --zone=public --change-interface=eno1`

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

В зону по умолчанию (`firewall-cmd --get-default-zone`)

5 Выводы

В ходе выполнения лабораторной работы мы получили навыки настройки пакетного фильтра в Linux

6 Список литературы

1. Лабораторная работа №13 [Электронный ресурс] URL: https://esystem.rudn.ru/pluginfile.php/13111/mod_resource/content/1/firewall.pdf