Отчёт по лабораторной работе №13

Фильтр пакетов

Лабси Мохаммед

Содержание

1 Цель работы **5**

2 Ход выполнения **6**
2.1 Управление брандмауэром с помощью firewall-cmd 6
2.2 Управление брандмауэром через графический интерфейс firewall-config 12
2.3 Самостоятельная работа 15
2.4 Контрольные вопросы 15

3 Заключение **17**

Список иллюстраций

2.1 Просмотр зон 6
2.2 Просмотр конфигурации зоны public 8
2.3 Добавление VNC-сервера 9
2.4 VNC отсутствует после перезапуска 10
2.5 Добавление permanent 11
2.6 Добавление порта 2022 12
2.7 Включение служб в GUI 13
2.8 Добавление порта 2022/udp 13
2.9 Изменения применены 14

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2 Ход выполнения

2.1 Управление брандмауэром с помощью firewall-cmd

1. Получены административные полномочия через команду **su -**.

2. Определена зона, используемая по умолчанию — **public**.

3. Просмотрен список доступных зон. На экране отобразился перечень: *block, dmz, drop, external, home, internal, public, trusted, work и др.*

```
mlabsi@mlabsi:~$ su
Password:
root@mlabsi:/home/mlabsi# firewall-cmd --get-default-zone
public
root@mlabsi:/home/mlabsi# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@mlabsi:/home/mlabsi# firewall-cmd --get-services '
> ^C
root@mlabsi:/home/mlabsi# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcups
d aseqnet audit ausweisapp2 bacula 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 civilization-
iv civilization-v cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client
 distcc dns dns-over-quic dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-serve
r factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galer
a ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https ident imap imaps iperf2 iperf3 i
pfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshel
l kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-s
ecure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ld
ap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache m
inecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wa
nted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconso
le ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporte
r proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind
 rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp s
mtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam
-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing synct
hing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmi
ssion-client turn turns upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-disco
very-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd wsdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client
xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
root@mlabsi:/home/mlabsi#
```

Рис. 2.1: Просмотр зон

4. Запрошен список всех доступных сервисов на системе. Отобразился длинный перечень служб (ssh, http, https, vnc-server, ftp и др.).

5. Выполнен просмотр сервисов, разрешённых в текущей зоне. Активными были:

    - cockpit
    - dhcpv6-client
    - ssh

6. Сравнены результаты вывода:

    - информации о текущей зоне;
    - информации о зоне public.

    Вывод совпал, так как зона **public** является активной и используется по умолчанию.

```
root@mlabsi:/home/mlabsi# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@mlabsi:/home/mlabsi# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@mlabsi:/home/mlabsi# firewall-cmd --list-all --zone=public
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@mlabsi:/home/mlabsi#
```

Рис. 2.2: Просмотр конфигурации зоны public

7. Добавлена служба VNC-сервера в конфигурацию временного выполнения.

8. Проверено наличие сервиса vnc-server — он появился в списке активных служб.

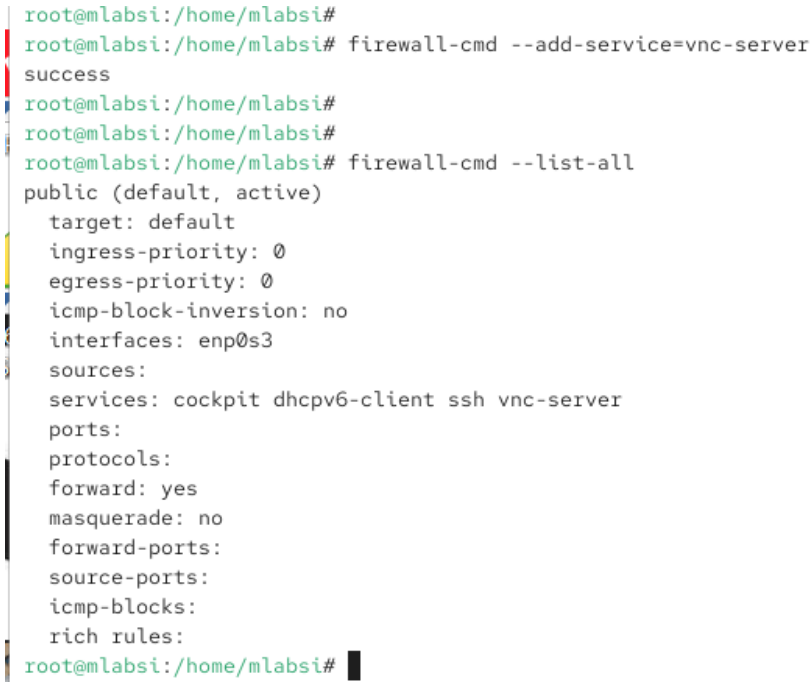


Рис. 2.3: Добавление VNC-сервера

9. Выполнен перезапуск службы **firewalld**.

10. После перезапуска службы vnc-server исчез.

    Причина: добавление производилось только во временную конфигурацию, не было сохранено на диск.

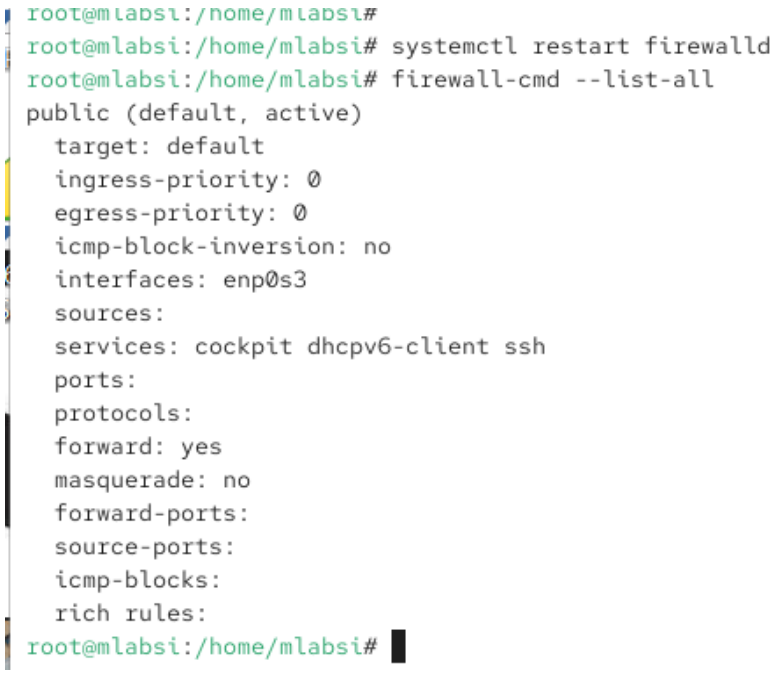


Рис. 2.4: VNC отсутствует после перезапуска

11. Повторно добавлена служба vnc-server, но уже как постоянная (записанная на диск).

12. После проверки службы vnc-server не было видно, так как постоянная конфигурация ещё не была применена.

```
root@mlabsi:/home/mlabsi#
root@mlabsi:/home/mlabsi# firewall-cmd --add-service=vnc-server --permanent
success
root@mlabsi:/home/mlabsi# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@mlabsi:/home/mlabsi# firewall-cmd --reload
success
root@mlabsi:/home/mlabsi# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
```

Рис. 2.5: Добавление permanent

13. Выполнена перезагрузка конфигурации брандмауэра. После этого служба появилась в активной конфигурации.

14. В конфигурацию добавлен порт **2022/tcp** как постоянный. Далее выполнена перезагрузка конфигурации брандмауэра.

15. Проверено, что порт добавлен — он появился в разделе *ports*.

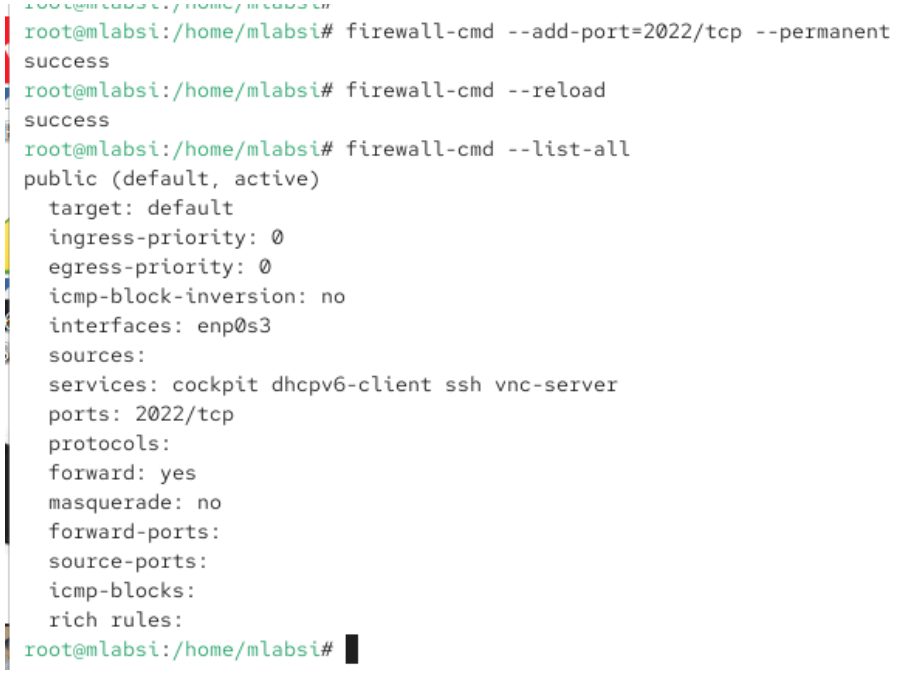


Рис. 2.6: Добавление порта 2022

2.2 Управление брандмауэром через графический интерфейс firewall-config

1. Запущено приложение **firewall-config**.
2. В меню **Configuration** выбрано состояние **Permanent**, чтобы изменения сохранялись.
3. Для зоны **public** активированы службы:
   - http
   - https
   - ftp

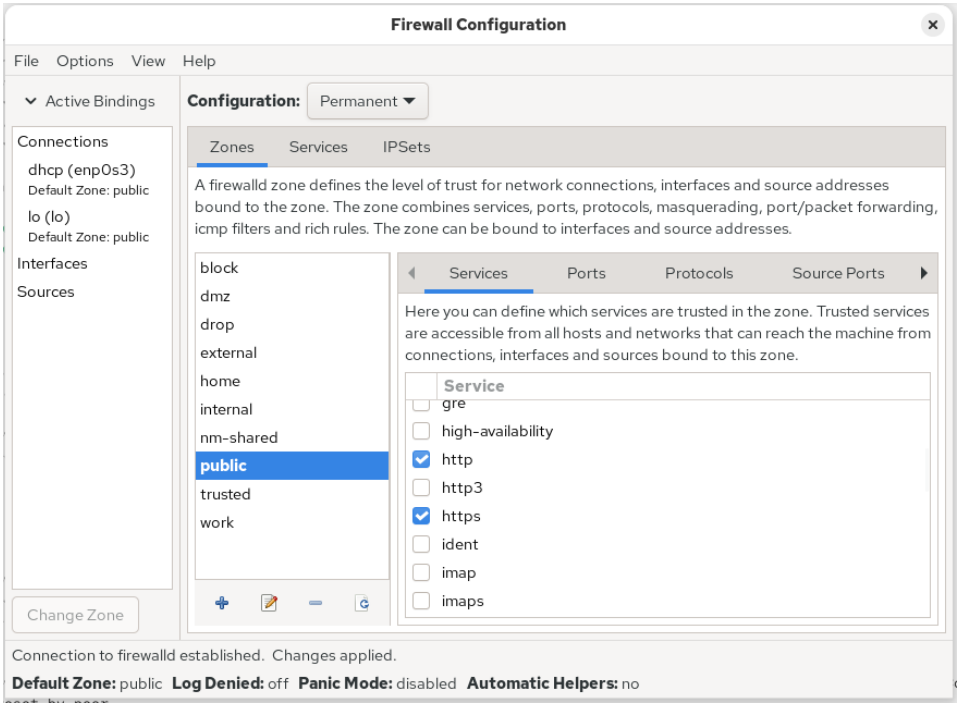


Рис. 2.7: Включение служб в GUI

4. На вкладке **Ports** добавлен порт 2022 протокола UDP.

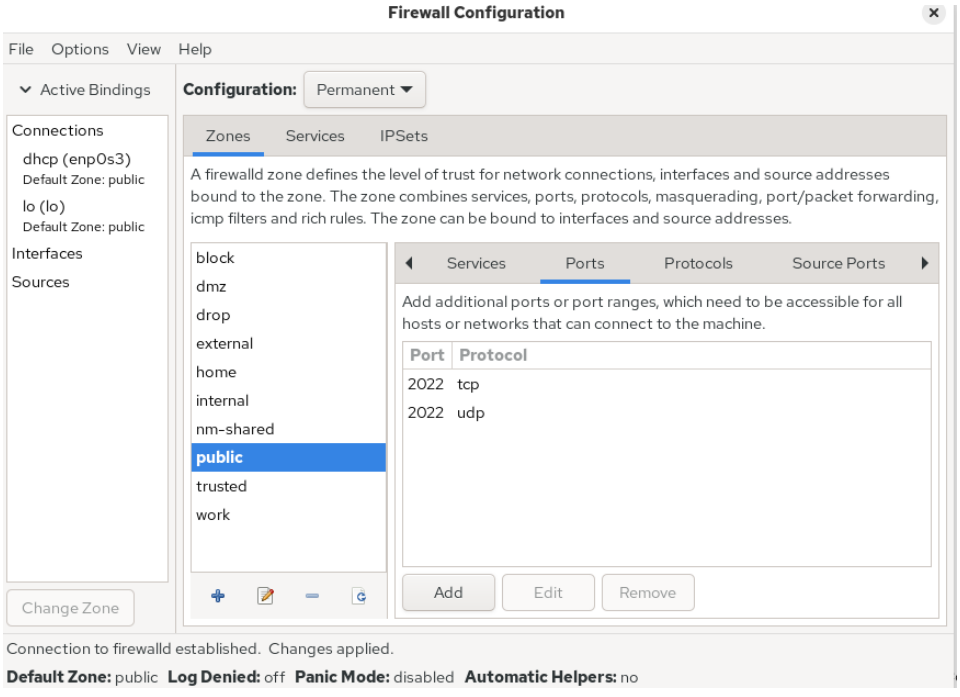


Рис. 2.8: Добавление порта 2022/udp

5. Приложение закрыто.

6. Проверка через firewall-cmd показала, что изменения ещё не применены (так как это постоянные настройки).

7. После перезагрузки конфигурации изменения вступили в силу:

   - службы http, https, ftp активированы;
   - порты `2022/tcp` и `2022/udp` присутствуют.

```
root@mlabsi:/home/mlabsi#
root@mlabsi:/home/mlabsi# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@mlabsi:/home/mlabsi# firewall-cmd --reload
success
root@mlabsi:/home/mlabsi# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  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@mlabsi:/home/mlabsi#
```

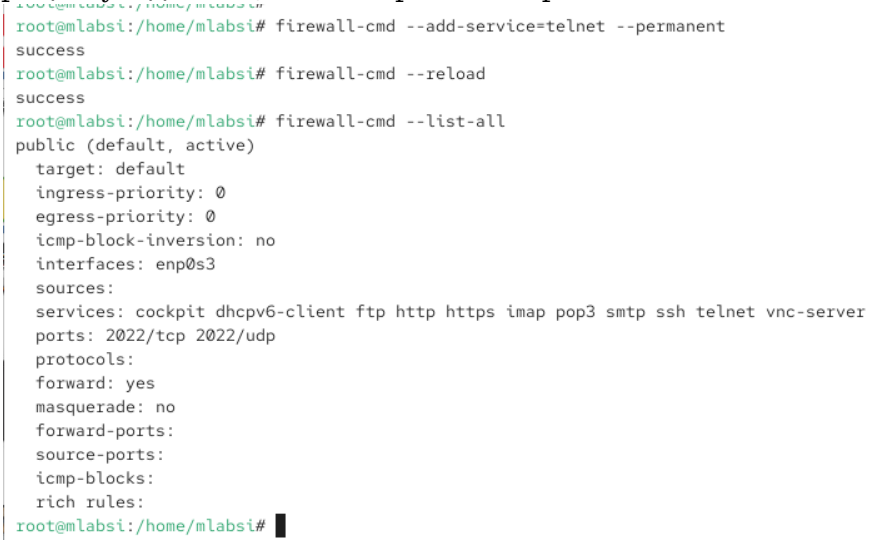
Рис. 2.9: Изменения применены

2.3 Самостоятельная работа

1. В конфигурацию добавлена служба **telnet** (через командную строку) как постоянная.

2. Через интерфейс **firewall-config** добавлены службы **imap**, **pop3**, **smtp**.

3. После перезагрузки конфигурации убедились, что настройки сохранены и загружаются автоматически.



2.4 Контрольные вопросы

1. **Какая служба должна быть запущена перед началом работы с менеджером конфигурации брандмауэра firewall-config?**
   Перед запуском графического менеджера **firewall-config** должна быть активна служба **firewalld**.

2. **Какая команда позволяет добавить UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию?**
   UDP-порт 2355 можно добавить с помощью команды:
   firewall-cmd –add-port=2355/udp –permanent

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

Для просмотра настроек во всех зонах используется команда:
firewall-cmd –list-all-zones

4. **Какая команда позволяет удалить службу vnc-server из текущей конфигурации брандмауэра?**
   Удаление выполняется командой:
   firewall-cmd –remove-service=vnc-server

5. **Какая команда firewall-cmd позволяет активировать новую конфигурацию, добавленную опцией –permanent?**
   Чтобы изменения вступили в силу, выполняется команда:
   firewall-cmd –reload

6. **Какой параметр firewall-cmd позволяет проверить, что новая конфигурация была добавлена в текущую зону и теперь активна?**
   Проверка выполняется командой:
   firewall-cmd –list-all

7. **Какая команда позволяет добавить интерфейс eno1 в зону public?**
   Чтобы добавить интерфейс, используется команда:
   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 зона не указана, интерфейс автоматически будет добавлен в **зону по умолчанию**, указанную в системе (как правило, это *public*).

3 Заключение

В ходе выполнения работы были изучены возможности управления межсетевым экраном в Linux с использованием утилиты **firewall-cmd** и графического интерфейса **firewall-config**. Были получены навыки просмотра активных зон и сервисов, добавления и удаления служб и портов, работы с временной и постоянной конфигурациями, а также применения изменений путём перезагрузки конфигурации. Кроме того, была создана пользовательская конфигурация брандмауэра, позволяющая доступ к определённым службам, как через командную строку, так и через графический интерфейс. Это позволило закрепить практические навыки администрирования сетевой безопасности в операционных системах семейства Linux.