Отчёт по лабораторной работе №13

Фильтр пакетов

Сулейм Гамбердов

Содержание

Список иллюстраций

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 права через su -.
   Определена зона, используемая по умолчанию — активной зоной оказалась **public**.

```
root@sigamberdov:/home/sigamberdov# firewall-cmd --get-default-zone
public
root@sigamberdov:/home/sigamberdov# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@sigamberdov:/home/sigamberdov# 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 apcupsd aseqnet audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storag
e 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 docke
r-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-
4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git
gpsd grafana gre high-availability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec
 irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api k
ube-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 kubel
et-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesiev
e matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mys
ql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opente
lemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3
 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio pu
ppetmaster 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 smtp smtp-submission smtp
s snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfe
r 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-s
ocks transmission-client turn turns upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wiregua
rd ws-discovery ws-discovery-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 za
bbix-trapper zabbix-web-service zero-k zerotier
root@sigamberdov:/home/sigamberdov# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@sigamberdov:/home/sigamberdov#
```

Рис. 2.1: Определение зоны по умолчанию

2. Выполнен просмотр доступных зон брандмауэра. Система содержит несколько предопределённых зон, включая *public*, *home*, *work*, *internal* и другие.

3. Получен перечень всех предустановленных служб, поддерживаемых брандмауэром. На экране отображён длинный список сервисов.

4. Выполнен просмотр служб, разрешённых в текущей зоне.

5. Для сравнения выведены сведения о конфигурации активной зоны двумя способами: общий вывод и вывод с указанием зоны.
   Результаты совпали, так как активная зона — **public**.

```
root@sigamberdov:/home/sigamberdov# 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@sigamberdov:/home/sigamberdov# 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:
```

Рис. 2.2: Сравнение list-all и list-all –zone

6. Добавлена служба **vnc-server** в конфигурацию времени выполнения. Повторная проверка списка разрешённых служб показала, что она успешно появилась.

```
root@sigamberdov:/home/sigamberdov# firewall-cmd --add-service=vnc-server
success
root@sigamberdov:/home/sigamberdov# 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:
  source-ports:
  icmp-blocks:
  rich rules:
root@sigamberdov:/home/sigamberdov#
```

Рис. 2.3: Добавление vnc-server во временную конфигурацию

7. Выполнена перезагрузка службы брандмауэра. После перезапуска служба **vnc-server** исчезла из конфигурации.

```
root@sigamberdov:/home/sigamberdov# systemctl restart firewalld.service
root@sigamberdov:/home/sigamberdov# 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@sigamberdov:/home/sigamberdov#
```

Рис. 2.4: После перезапуска службы vnc-server исчезает

Причина: служба была добавлена только во временную конфигурацию (runtime), которая не сохраняется на диск.

8. Служба добавлена повторно, но уже в постоянную конфигурацию (на диск). После выполнения команда показывает, что сервис существует только в постоянной части и ещё не активирован.

```
root@sigamberdov:/home/sigamberdov#
root@sigamberdov:/home/sigamberdov# firewall-cmd --add-service=vnc-server --permanent
success
root@sigamberdov:/home/sigamberdov# 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@sigamberdov:/home/sigamberdov#
```

Рис. 2.5: Добавление службы в постоянную конфигурацию

9. Перезагружена конфигурация брандмауэра. Служба **vnc-server** отобразилась в активной конфигурации.

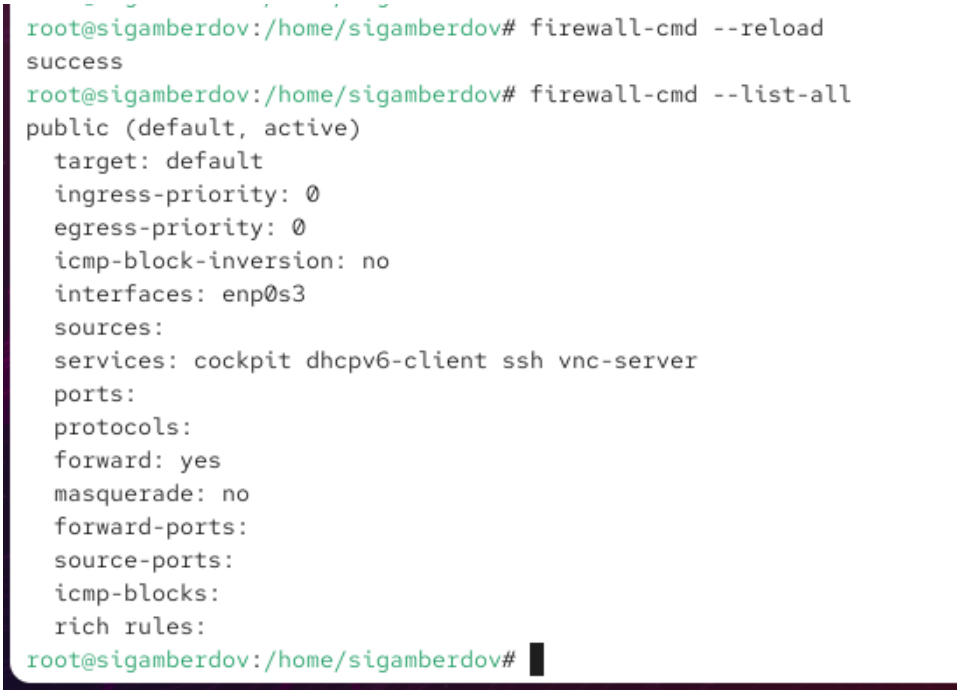

Рис. 2.6: Сервис vnc-server добавлен и активен

10. В конфигурацию добавлен порт **2022** по протоколу TCP, изменения сделаны постоянными.

    После перезагрузки конфигурации порт появился в текущей конфигурации брандмауэра.

```
root@sigamberdov:/home/sigamberdov# firewall-cmd --add-port=2022/tcp --permanent
success
root@sigamberdov:/home/sigamberdov# firewall-cmd --reload
success
root@sigamberdov:/home/sigamberdov# 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@sigamberdov:/home/sigamberdov#
```

Рис. 2.7: Добавление порта 2022/tcp

2.2 Управление брандмауэром с помощью *firewall-config*

1. Запущено приложение *firewall-config* из терминала. При запуске система запросила пароль пользователя с правами администратора.

2. В верхней части окна открыт список конфигураций, выбран режим **Permanent**. Это обеспечивает сохранение всех изменений как постоянных.

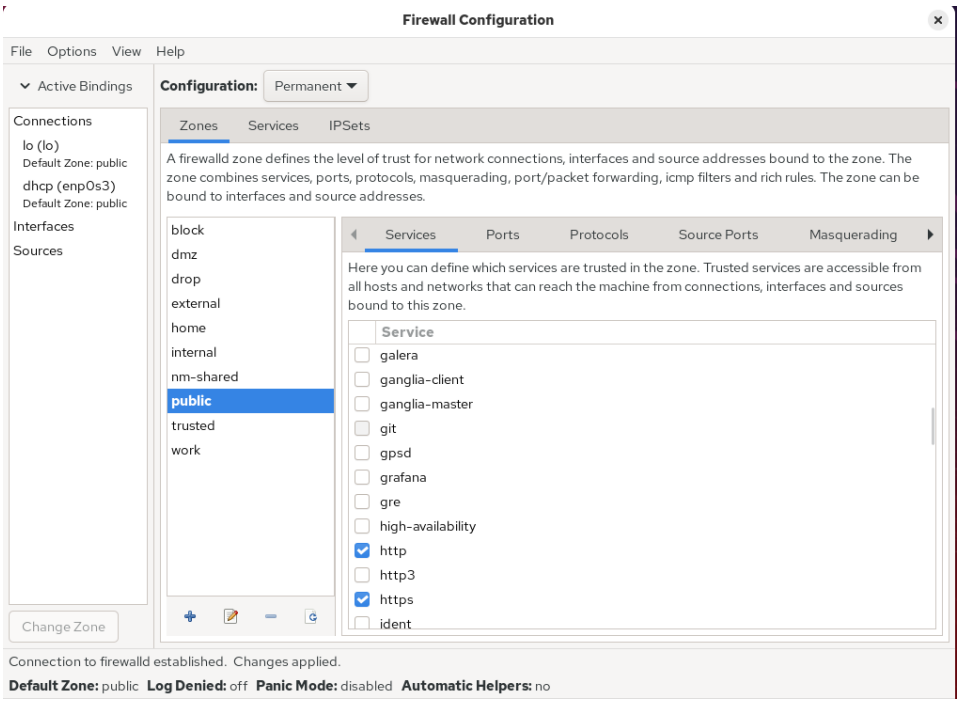

Рис. 2.8: Выбор режима Permanent

3. В левой панели выбрана зона **public**. На вкладке *Services* отмечены службы **http**, **https** и **ftp**, благодаря чему к ним разрешён доступ.

4. Перейдя на вкладку *Ports*, выполнено добавление порта. В появившемся окне введено:

   - Port: `2022`
   - Protocol: `udp`

   После нажатия OK порт был внесён в список.

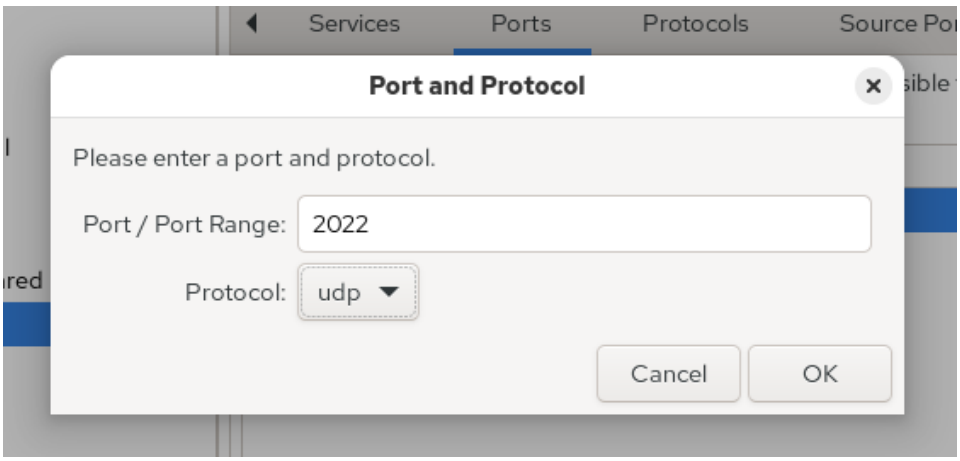

Рис. 2.9: Добавление порта 2022/udp

5. Приложение *firewall-config* закрыто.

6. В терминале выведена текущая конфигурация брандмауэра. Порт и службы ещё не активны, так как изменения внесены только в постоянную конфигурацию.

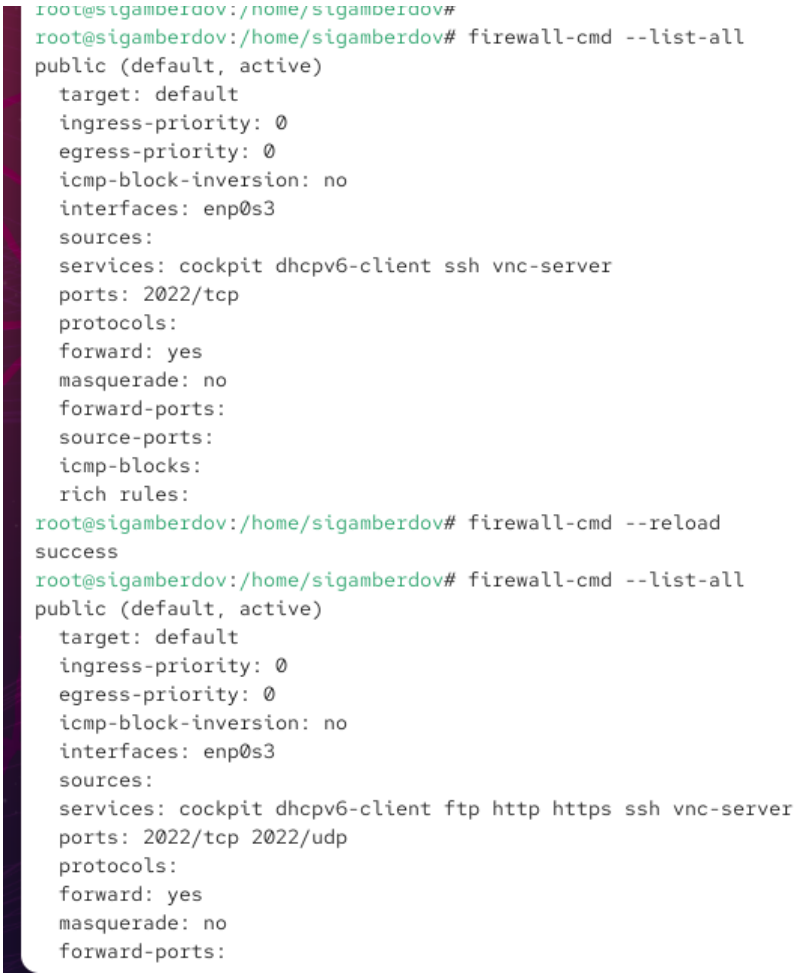

Рис. 2.10: Проверка конфигурации перед reload

7. Выполнена перезагрузка конфигурации с помощью `firewall-cmd --reload`, после чего повторный вывод параметров подтвердил применение изменений: службы и порт отобразились в списке активных.

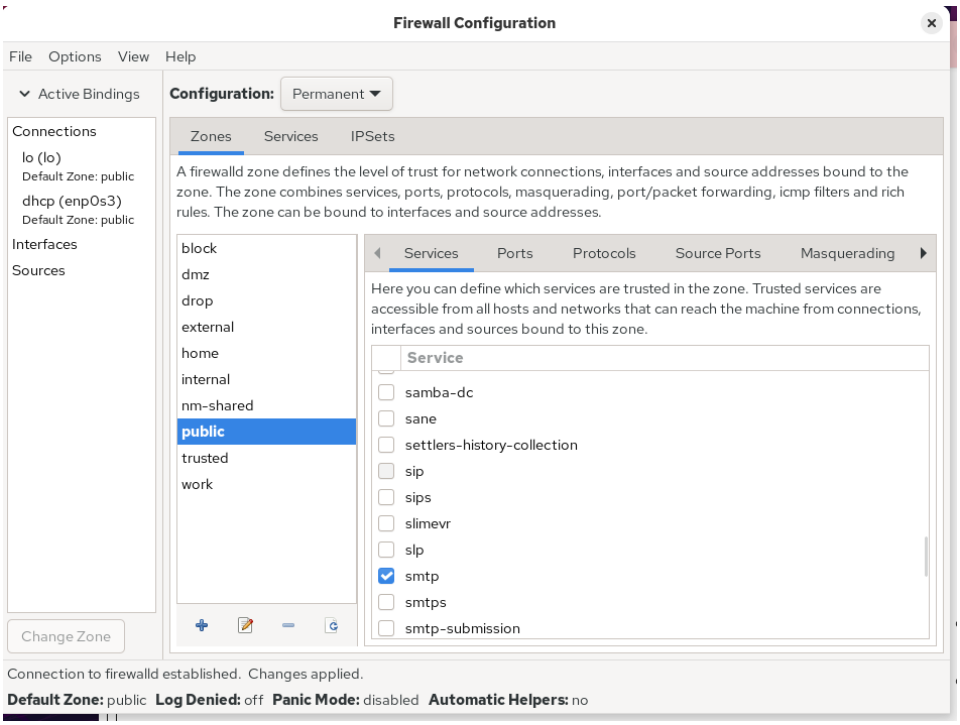

Рис. 2.11: Настройки вступили в силу после reload

2.3 Самостоятельная работа

1. Настроена конфигурация, разрешающая доступ к службам:

   - **telnet**
   - **imap**
   - **pop3**
   - **smtp**

2. Добавление услуги **telnet** выполнено в командной строке. Затем команда выполнена повторно с флагом `--permanent`, чтобы изменить конфигурацию на постоянную.

3. Через графический интерфейс *firewall-config* добавлены службы **imap**, **pop3**, **smtp**. Службы выбраны в списке на вкладке *Services* для зоны *public*.

4. Выполнена перезагрузка конфигурации `firewall-cmd --reload`. Проверка

списка активных параметров показала, что все службы и порт находятся в постоянной конфигурации и активированы.

```
root@sigamberdov:/home/sigamberdov# firewall-cmd --add-service=telnet
success
root@sigamberdov:/home/sigamberdov# firewall-cmd --add-service=telnet --permanent
success
root@sigamberdov:/home/sigamberdov# firewall-cmd --reload
success
root@sigamberdov:/home/sigamberdov# 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 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:
root@sigamberdov:/home/sigamberdov#
```

Рис. 2.12: Итоговая конфигурация с telnet, imap, pop3, smtp

3 Контрольные вопросы

1. Перед началом работы с менеджером конфигурации брандмауэра **firewall-config** должна быть запущена служба **firewalld**.

2. Добавление UDP-порта **2355** в зону по умолчанию выполняется командой: `firewall-cmd --add-port=2355/udp`

3. Для отображения полной конфигурации брандмауэра во всех зонах используется команда: `firewall-cmd --list-all-zones`

4. Удаление службы **vnc-server** из текущей конфигурации выполняется командой: `firewall-cmd --remove-service=vnc-server`

5. Применение конфигурации, добавленной с параметром `--permanent`, выполняется командой: `firewall-cmd --reload`

6. Проверка активной конфигурации и подтверждение внесённых изменений выполняется командой: `firewall-cmd --list-all`

7. Добавление интерфейса **eno1** в зону *public* выполняется с помощью: `firewall-cmd --zone=public --add-interface=eno1`

8. Если интерфейс добавляется без указания зоны, он будет помещён в **зону по умолчанию**. Узнать её можно командой: `firewall-cmd --get-default-zone`

4 Заключение

В ходе работы были изучены основные приёмы управления брандмауэром в Linux с использованием инструментов **firewall-cmd** и **firewall-config**. На практике были выполнены задачи по добавлению и удалению служб, открытию TCP/UDP-портов, а также различению временной и постоянной конфигураций. Через GUI и командную строку были настроены службы telnet, imap, pop3 и smtp, что позволило закрепить навыки администрирования.