Отчёт по лабораторной работе №13

Фильтр пакетов

Ришард Когенгар

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. Для выполнения операций управления межсетевым экраном были получены полномочия администратора.
   Вход в систему выполнен под пользователем **root**, что обеспечило доступ к системным настройкам и службам безопасности.

2. С помощью команды определения зоны по умолчанию установлено, что активной зоной firewalld является **public**.

3. Выполнен просмотр всех доступных зон межсетевого экрана.
   В результате получен список стандартных зон firewalld, включая block, dmz, drop, external, home, internal, nm-shared, public, trusted и work.

4. Получен список всех служб, поддерживаемых межсетевым экраном.
   В выводе представлены сетевые и серверные службы, доступные для использования в конфигурации firewalld.

```
root@rishardkogengar:/home/rishard# firewall-cmd --get-default-zone
public
root@rishardkogengar:/home/rishard# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@rishardkogengar:/home/rishard# 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 a
udit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet b
itcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit collect
d condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls docke
r-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4 freei
pa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availabi
lity 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 kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-m
anager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-reado
nly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns
memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wan
ted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmc
onsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps
3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-mast
er samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submission smtps snmp snmptls snmptl
s-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfer steam-streaming stellaris stronghold-crusa
der stun stuns submission supertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet
 tentacle terraria tftp tile38 tinc tor-socks transmission-client turn turns upnp-client vdsm vnc-server vrrp warpinator wbem-http
wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd wsdd-http wsman wsma
ns xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-serv
ice zero-k zerotier
root@rishardkogengar:/home/rishard# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@rishardkogengar:/home/rishard#
```

Рис. 2.1: Список доступных служб firewalld

5. Определены службы, разрешённые в текущей активной зоне.

   Установлено, что в зоне **public** разрешены службы **cockpit**, **dhcpv6-client** и **ssh**.

6. Выполнено сравнение конфигурации текущей зоны и явного указания зоны **public**.

   Результаты полностью совпали, что подтверждает использование зоны **public** в качестве зоны по умолчанию и её активное состояние.

```
root@rishardkogengar:/home/rishard# 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@rishardkogengar:/home/rishard#
```

Рис. 2.2: Просмотр конфигурации текущей зоны

```
root@rishardkogengar:/home/rishard# 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@rishardkogengar:/home/rishard#
```

Рис. 2.3: Просмотр конфигурации зоны public

7. В конфигурацию времени выполнения межсетевого экрана добавлена служ-

ба **vnc-server**.

Изменение применено успешно и вступило в силу немедленно.

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

Рис. 2.4: Добавление службы vnc-server

8. Проверка текущей конфигурации показала наличие службы **vnc-server** в списке разрешённых сервисов активной зоны.

9. Выполнен перезапуск службы firewalld для проверки сохранности временных изменений.

10. После перезапуска службы установлено, что **vnc-server** отсутствует в конфигурации.

    Это связано с тем, что служба была добавлена только в конфигурацию времени выполнения и не была сохранена на постоянной основе. При перезапуске firewalld временные правила были сброшены.

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

Рис. 2.5: Отсутствие vnc-server после перезапуска firewalld

11. Служба **vnc-server** добавлена в постоянную конфигурацию межсетевого экрана.

    Изменение сохранено в конфигурационных файлах firewalld.

12. При проверке конфигурации времени выполнения служба **vnc-server** не отображается.

    Это объясняется тем, что постоянная конфигурация автоматически не применяется без перезагрузки правил.

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

Рис. 2.6: Отсутствие vnc-server без перезагрузки конфигурации

13. Выполнена перезагрузка конфигурации firewalld.

    После применения постоянных правил служба **vnc-server** отобразилась в списке разрешённых сервисов активной зоны.

```
root@rishardkogengar:/home/rishard# firewall-cmd --reload
success
root@rishardkogengar:/home/rishard# 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@rishardkogengar:/home/rishard#
```

Рис. 2.7: Применение постоянной конфигурации firewalld

14. В постоянную конфигурацию межсетевого экрана добавлен TCP-порт **2022**. После этого выполнена перезагрузка конфигурации firewalld для применения изменений.

15. Проверка конфигурации подтвердила, что порт **2022/tcp** успешно добавлен и разрешён в активной зоне.

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

Рис. 2.8: Проверка добавленного порта 2022

2.2 Управление брандмауэром с помощью firewall-config

1. В графической среде операционной системы открыт терминал, после чего под учётной записью пользователя запущена утилита графического управления межсетевым экраном **firewall-config**.
   При запуске утилиты выполнена аутентификация пользователя с административными полномочиями, что позволило получить доступ к настройке службы firewalld.

2. В верхней части окна утилиты в параметре **Configuration** из выпадающего списка выбрано значение **Permanent**.
   Это обеспечило сохранение всех вносимых изменений в постоянной кон-

фигурации межсетевого экрана, которая применяется после перезагрузки службы или системы.

3. В списке зон выбрана зона **public**, используемая в системе по умолчанию. На вкладке **Services** отмечены службы **http**, **https** и **ftp**, что разрешило входящие соединения для соответствующих сетевых сервисов в данной зоне.

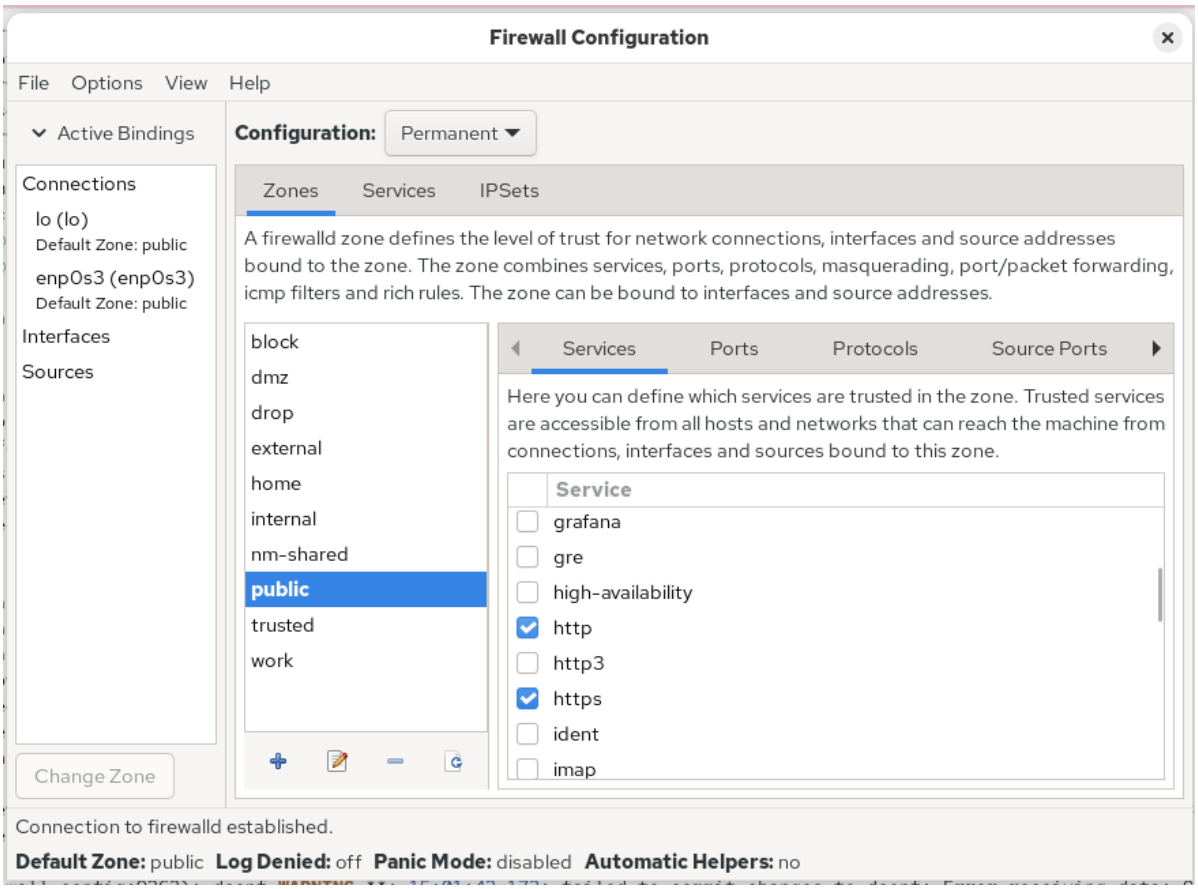

Рис. 2.9: Включение служб http, https и ftp

4. На вкладке **Ports** нажата кнопка **Add**, после чего в открывшемся диалоговом окне указан порт **2022** и выбран протокол **udp**.
   После подтверждения порт был добавлен в список разрешённых портов зоны **public**.

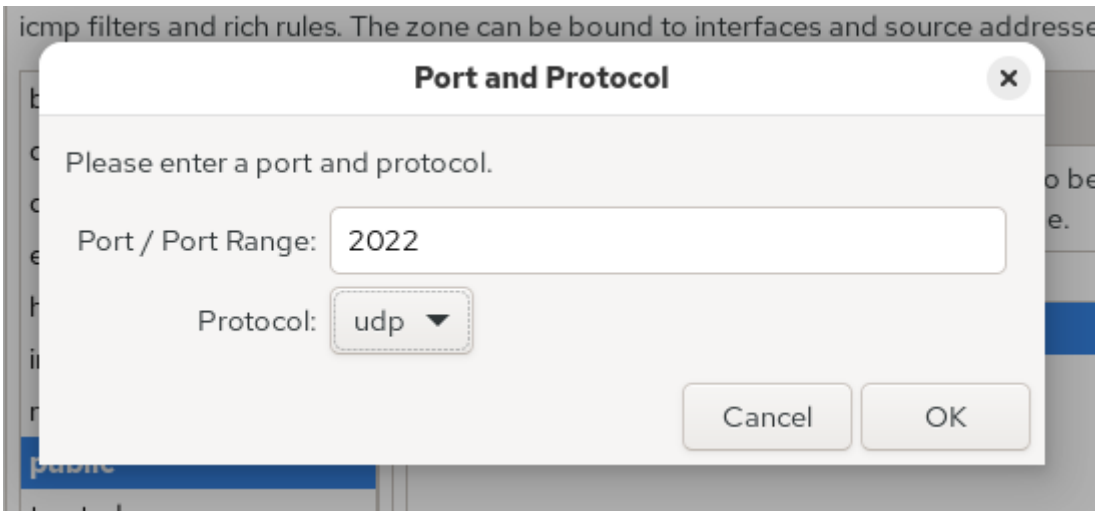

Рис. 2.10: Добавление UDP-порта 2022

5. После завершения настройки графическая утилита **firewall-config** была закрыта. Все изменения были сохранены в постоянной конфигурации межсетевого экрана.

6. В терминале выполнен просмотр текущей конфигурации зоны с помощью команды просмотра параметров firewalld.
   В выводе установлено, что изменения, выполненные через графический интерфейс, ещё не применены к конфигурации времени выполнения, так как они были сохранены только в постоянной конфигурации.

```
root@rishardkogengar:/home/rishard# 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@rishardkogengar:/home/rishard#
```

Рис. 2.11: Просмотр конфигурации до перезагрузки

7. Для применения постоянной конфигурации выполнена перезагрузка правил межсетевого экрана.

   После этого повторный просмотр конфигурации показал, что службы **http**, **https**, **ftp**, а также порт **2022/udp** успешно применены и активны.

```
root@rishardkogengar:/home/rishard# firewall-cmd --reload
success
root@rishardkogengar:/home/rishard# 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@rishardkogengar:/home/rishard#
```

Рис. 2.12: Применение изменений после reload

2.3 Самостоятельная работа

1. Создана конфигурация межсетевого экрана, разрешающая доступ к службам **telnet**, **imap**, **pop3** и **smtp**.

2. Служба **telnet** была добавлена в постоянную конфигурацию с использованием интерфейса командной строки.
   После перезагрузки конфигурации firewalld служба стала доступна в активной зоне.

3. Службы **imap**, **pop3** и **smtp** были добавлены через графический интерфейс **firewall-config** в зоне **public**.
   Все изменения выполнены в режиме **Permanent**, что гарантирует их сохранение после перезагрузки системы.

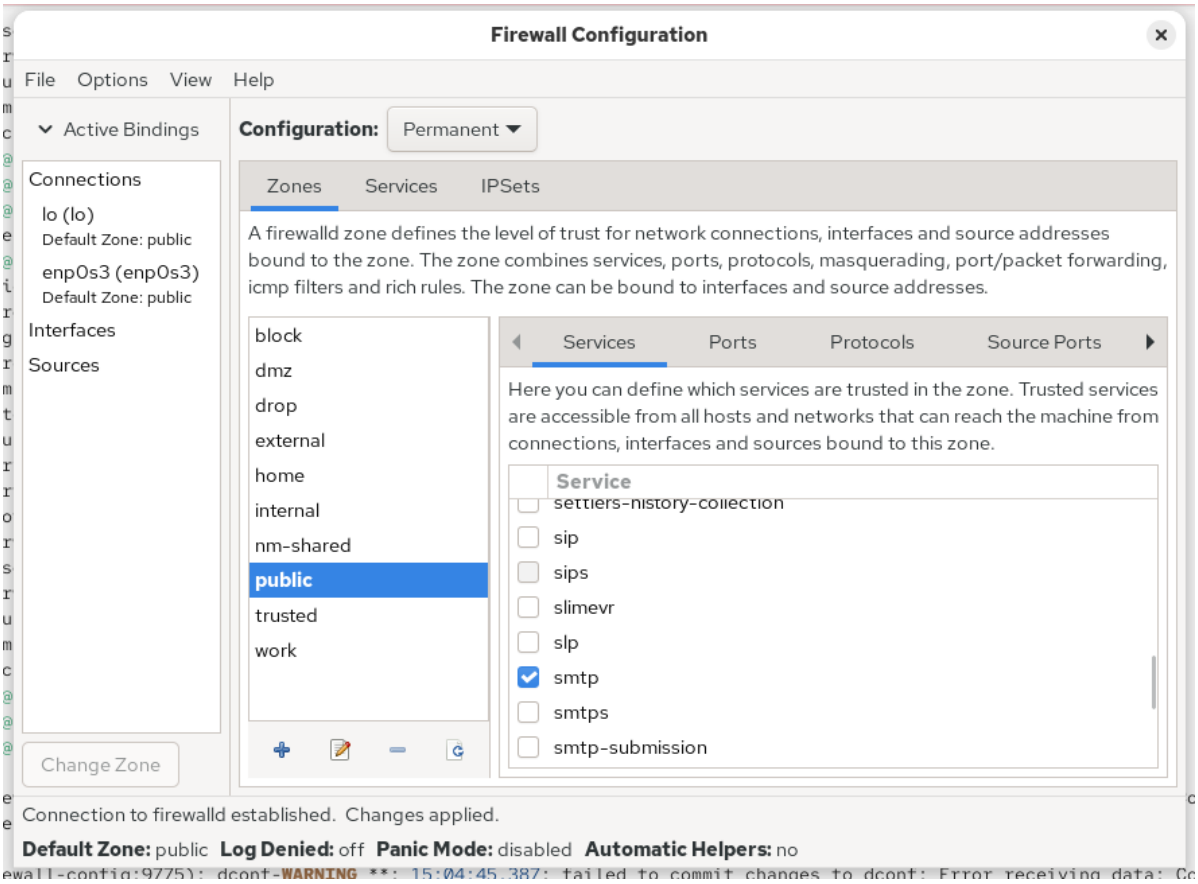

Рис. 2.13: Добавление служб imap, pop3 и smtp через GUI

4. После перезагрузки конфигурации межсетевого экрана выполнена проверка параметров.

   Установлено, что все добавленные службы и порты присутствуют в конфигурации и будут автоматически активированы после перезагрузки компьютера.

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

Рис. 2.14: Итоговая конфигурация firewalld

2.4 Вывод

В ходе работы были изучены и практически применены способы управления межсетевым экраном firewalld с использованием как командной строки (`firewall-cmd`), так и графического интерфейса (`firewall-config`). Были освоены принципы работы конфигураций времени выполнения и постоянных конфигураций, а также порядок их применения. В результате настроена постоянная конфигурация брандмауэра, обеспечивающая доступ к необходимым сетевым службам и портам и сохраняющаяся после перезагрузки системы.

3 Контрольные вопросы

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

Перед началом работы с утилитой **firewall-config** должна быть запущена служба **firewalld**, так как именно она отвечает за управление межсетевым экраном и хранение его конфигурации.

2. Какая команда позволяет добавить UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию?

Для добавления UDP-порта 2355 в зону по умолчанию используется команда:

```
firewall-cmd --add-port=2355/udp
```

Для добавления порта на постоянной основе:

```
firewall-cmd --add-port=2355/udp --permanent
```

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

Для отображения полной конфигурации межсетевого экрана по всем зонам используется команда:

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

4. Какая команда позволяет удалить службу vnc-server из текущей конфигурации брандмауэра?

Для удаления службы **vnc-server** из конфигурации времени выполнения применяется команда:

```
firewall-cmd --remove-service=vnc-server
```

Для удаления службы из постоянной конфигурации:

```
firewall-cmd --remove-service=vnc-server --permanent
```

5. Какая команда firewall-cmd позволяет активировать новую конфигурацию, добавленную опцией –permanent?

Для применения постоянной конфигурации к текущему состоянию используется команда:

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

6. Какой параметр firewall-cmd позволяет проверить, что новая конфигурация была добавлена в текущую зону и теперь активна?

Для проверки активной конфигурации текущей зоны применяется команда:

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

Она отображает список разрешённых служб, портов и других параметров активной зоны.

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

Для привязки сетевого интерфейса **eno1** к зоне **public** используется команда:

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

Для сохранения изменения на постоянной основе:

```
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 при добавлении сетевого интерфейса зона не указана явно, интерфейс будет автоматически добавлен в **зону по умолчанию**, которая определяется параметром default zone (в большинстве систем — зона **public**).