Отчёт по лабораторной работе №13

Фильтр пакетов

Максат Хемраев

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2 Отчёт по выполнению работы

2.1 Управление брандмауэром с использованием `firewall-cmd`

1. Получил права суперпользователя и определил зону по умолчанию.
   Команда вывела значение **public**, что означает применение стандартных правил для входящих подключений.

2. Просмотрел доступные зоны и перечень служб, которые могут быть добавлены в правила брандмауэра.
   Вывод показал большое количество предустановленных сервисов.

```
mhemraev@mhemraev:~$ su
Password:
root@mhemraev:/home/mhemraev# firewall-cmd --get-default-zone
public
root@mhemraev:/home/mhemraev# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@mhemraev:/home/mhemraev# 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 au
dit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bit
coin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit collectd c
ondor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls docker-re
gistry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ld
ap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability h
ttp http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerber
os kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager k
ube-controller-manager-secure 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 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-wanted netbios
-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry 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 p
ulseaudio 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 smtp 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 s
ubmission supertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terrari
a tftp tile38 tinc tor-socks 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 zabbix-trapper zabbix-web-service zero-k zerotier
root@mhemraev:/home/mhemraev#
```

Рис. 2.1: Список зон и служб

3. Затем проверил, какие службы разрешены в текущей зоне.

   Команда `firewall-cmd --list-services` показала активные разрешённые сервисы — `cockpit`, `dhcpv6-client`, `ssh`.

```
root@mhemraev:/home/mhemraev# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@mhemraev:/home/mhemraev# 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@mhemraev:/home/mhemraev# 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@mhemraev:/home/mhemraev#
```

Рис. 2.2: Список разрешённых служб

4. Сравнил вывод команд `firewall-cmd --list-all` и `firewall-cmd --list-all --zone=public`.

   Результаты совпали, что подтверждает — активная зона действительно **public**.

5. Добавил службу **vnc-server** во временную конфигурацию (в runtime).

   Проверка показала, что служба появилась в списке разрешённых.

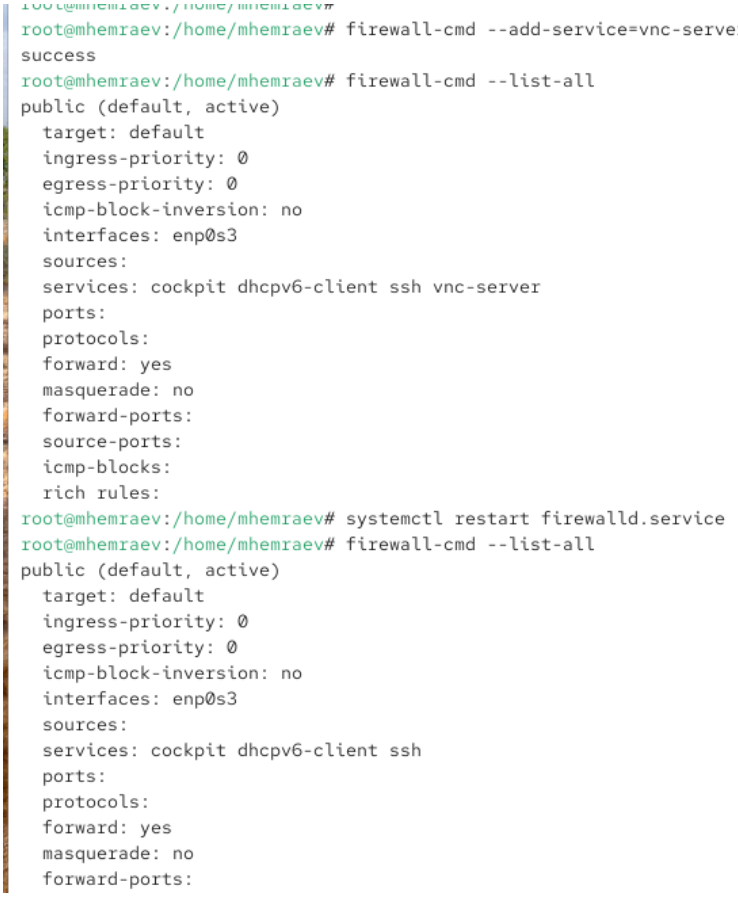

Рис. 2.3: Добавление vnc-server

6. Перезапустил службу `firewalld`.

   После перезапуска **vnc-server исчез из конфигурации**.

   Это происходит потому, что добавление было выполнено только во *временной (runtime)* конфигурации, а перезапуск сбросил её до значений *постоянной (permanent)*.

7. Повторно добавил службу **vnc-server**, но уже в постоянную конфигурацию:

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

После команды `firewall-cmd --reload` служба появилась и в runtime-конфигурации.

```
root@mhemraev:/home/mhemraev# firewall-cmd --add-service=vnc-server --permanent
success
root@mhemraev:/home/mhemraev# 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@mhemraev:/home/mhemraev# firewall-cmd --reload
success
root@mhemraev:/home/mhemraev# 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. 2.4: vnc-server добавлен permanent

8. Добавил порт **2022/tcp** в постоянную конфигурацию, затем перегрузил её. Проверка `firewall-cmd --list-all` показывает порт в списке разрешённых.

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

Рис. 2.5: Добавление порта 2022/tcp

2.2 Управление брандмауэром с использованием графического интерфейса `firewall-config`

1. Запустил утилиту `firewall-config`.

   Переключил параметр **Configuration → Permanent**, чтобы изменения сохранялись на диске.

2. В зоне **public** включил службы **http**, **https**, **ftp**.

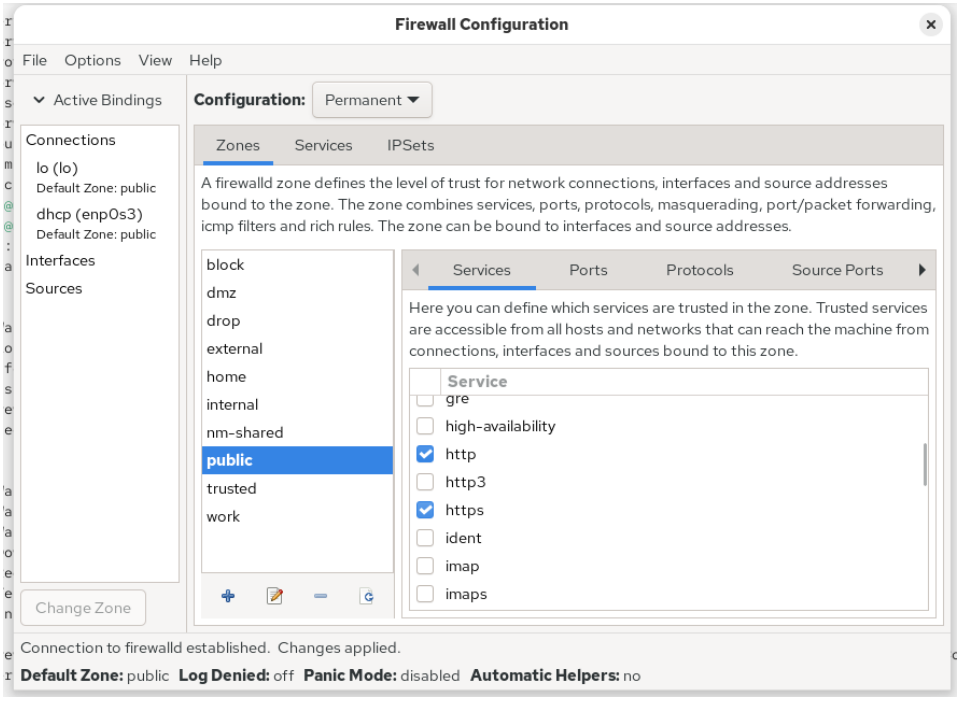

Рис. 2.6: Включение служб в GUI

3. На вкладке *Ports* добавил порт **2022/udp**.

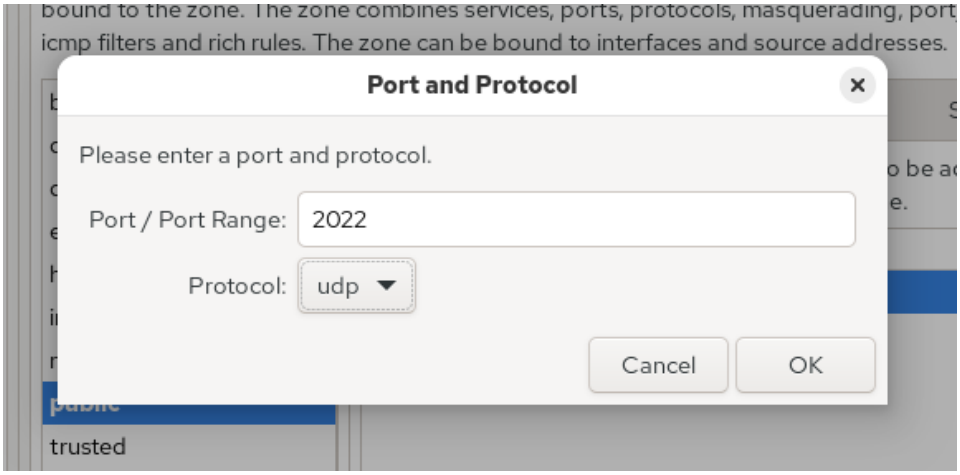

Рис. 2.7: Добавление порта 2022/udp

4. После внесения изменений выполнил: `firewall-cmd --reload`

Теперь в конфигурации времени выполнения отображаются как службы, так и новый порт.

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

Рис. 2.8: Синхронизация постоянной и runtime конфигурации

2.3 Самостоятельная работа

1. Конфигурация межсетевого экрана должна разрешать службы:

- **telnet** — добавлено через команду CLI:

```
firewall-cmd --add-service=telnet --permanent
firewall-cmd --reload
```

- **imap**, **pop3**, **smtp** — добавлены через GUI (`firewall-config`) во вкладке *Services* для зоны **public**.

2. Проверка конфигурации:

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

Рис. 2.9: Проверка конфигурации

3 Контрольные вопросы

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

Для работы утилиты **firewall-config** должна быть запущена служба `firewalld`.

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

Используется команда: `firewall-cmd --add-port=2355/udp --permanent`.

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

Команда: `firewall-cmd --list-all-zones`.

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

Удаление выполняется командой: `firewall-cmd --remove-service=vnc-server`.

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

Активация выполняется командой: `firewall-cmd --reload`.

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

Для просмотра используется команда: `firewall-cmd --list-all`.

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

Команда: `firewall-cmd --zone=public --change-interface=eno1 --permanent`.

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

Интерфейс будет добавлен в **зону по умолчанию**, чаще всего это `public`.

---

4 Заключение

В ходе работы были изучены команды и инструменты для управления брандмауэром firewalld, включая добавление служб и портов как во временную, так и в постоянную конфигурацию, а также применение изменений через firewall-config.