Отчёт по лабораторной работе №13

Фильтр пакетов

Руслан Алиев

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

1.1 Настройка брандмауэра с помощью firewall-cmd

1. Для начала выполнен переход в режим суперпользователя.
   Определена зона по умолчанию, которая оказалась `public`.

```
raliev@raliev:~$ su
Password:
root@raliev:/home/raliev# firewall-cmd --get-default-zone
public
root@raliev:/home/raliev# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@raliev:/home/raliev# 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-storage bb bgp bitcoin bitcoin-rpc bitcoin-testn
et bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit c
ollectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-t
ls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freei
pa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre h
igh-availability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kad
min kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure k
ube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kub
elet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp mana
gesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula n
eed-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-expo
rter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquot
ad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submis
sion smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfer steam-stre
aming stellaris stronghold-crusader 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 v
nc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-d
iscovery-udp wsdd wsdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabb
ix-server zabbix-trapper zabbix-web-service zero-k zerotier
root@raliev:/home/raliev# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@raliev:/home/raliev#
```

Рис. 1.1: Получение зоны по умолчанию

2. Команда получения доступных зон вывела перечень: `block`, `dmz`, `external`, `home`, `internal`, `nm-shared`, `public`, `trusted`, `work`.

3. Просмотр списка доступных служб показал большое количество доступных сервисов, включая `ssh`, `http`, `ftp`, `cockpit`, `vnc-server` и другие.

4. В текущей активной зоне отображены службы `cockpit`, `dhcpv6-client`, `ssh`.

5. При сравнении команд `--list-all` и `--list-all --zone=public` вывод оказался одинаковым, так как `public` — зона по умолчанию.

```
root@raliev:/home/raliev# 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@raliev:/home/raliev# 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@raliev:/home/raliev#
```

Рис. 1.2: Параметры зоны public

6. Временное добавление службы `vnc-server` позволило ей отобразиться в активной конфигурации зоны.

7. После перезапуска службы firewalld внесённые изменения исчезли. Это

произошло потому, что добавление было временным и не сохранялось в конфигурации.

```
root@raliev:/home/raliev#
root@raliev:/home/raliev# firewall-cmd --add-service=vnc-server
success
root@raliev:/home/raliev# 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@raliev:/home/raliev# systemctl restart firewalld.service
root@raliev:/home/raliev# 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:
```

Рис. 1.3: Добавление и исчезновение службы vnc-server

8. Повторное добавление `vnc-server` с ключом `--permanent` сохранило изменения в постоянной конфигурации. Однако, в конфигурации времени выполнения они пока не отразились.

9. После перезагрузки конфигурации командой `--reload` служба `vnc-server` появилась в активной конфигурации.

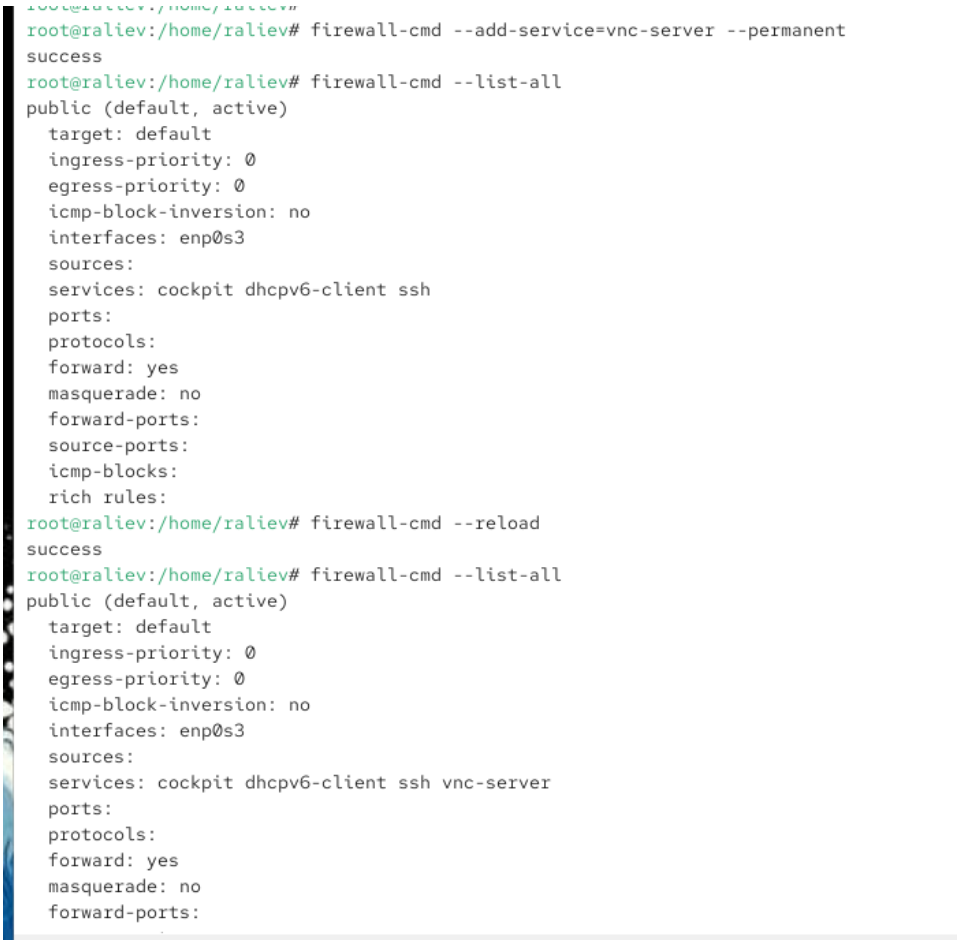

Рис. 1.4: Добавление vnc-server на постоянной основе

10. В конфигурацию добавлен порт `2022/tcp` с постоянной фиксацией изменений и последующей перезагрузкой.

    Порт отобразился в списке как `2022/tcp`.

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

Рис. 1.5: Добавление порта 2022/tcp

1.2 Использование графического интерфейса firewall-config

1. В GUI-интерфейсе firewall-config была выбрана конфигурация Permanent. В зоне `public` активированы службы `ftp`, `http`, `https`.

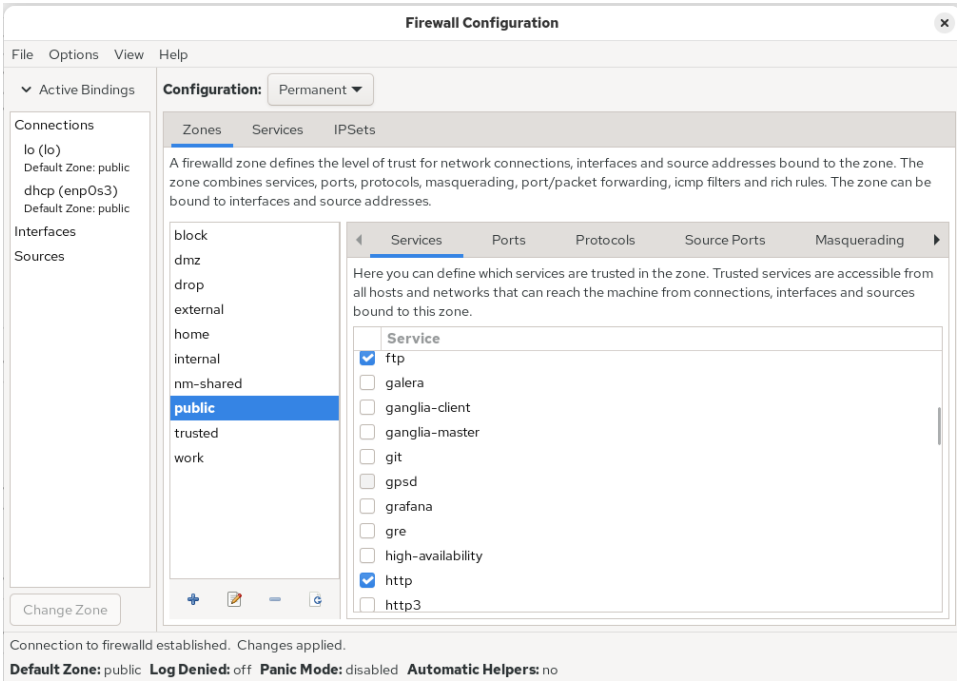

Рис. 1.6: Включение служб в графическом интерфейсе

2. На вкладке **Ports** добавлены порты `2022/tcp` и `2022/udp`.

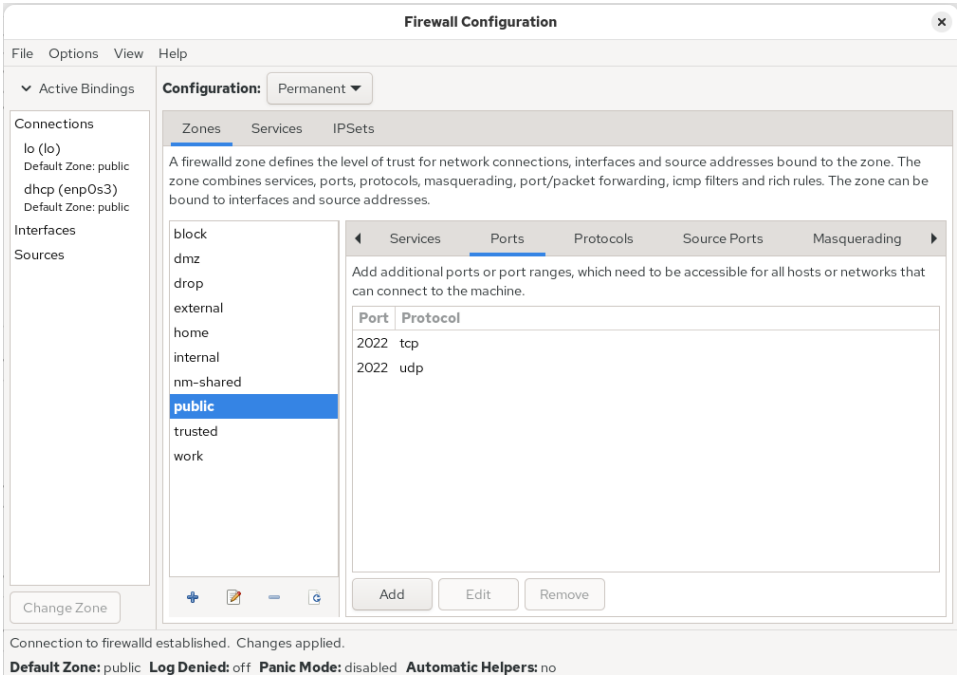

Рис. 1.7: Добавление портов 2022/tcp и 2022/udp

3. После перезагрузки конфигурации все внесённые изменения вступили в силу и отобразились в списке:
   службы — `ftp`, `http`, `https`, порты — `2022/tcp`, `2022/udp`.

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

Рис. 1.8: Применение всех изменений

1.3 Добавление служб в рамках самостоятельной работы

1. Служба `telnet` была добавлена через CLI на постоянной основе.

   После перезагрузки firewalld она появилась в конфигурации.

2. Через графический интерфейс были включены службы `imap`, `pop3`, `smtp`.

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

Рис. 1.9: Итоговая конфигурация зоны public

2 Контрольные вопросы

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

7. **Какая команда позволяет добавить интерфейс eno1 в зону public?**
   firewall-cmd –zone=public –change-interface=eno1 –permanent

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

   В зону по умолчанию (default zone), чаще всего — public

3 Заключение

В рамках выполненной работы была изучена система управления сетевыми подключениями с использованием службы **firewalld** и утилиты **firewall-cmd**. Рассматривались текущие параметры зон, активные службы и способы изменения конфигурации брандмауэра как временно, так и на постоянной основе. Были отработаны команды добавления и удаления служб и портов, перезагрузка конфигурации и работа с интерфейсами.