Отчёт по лабораторной работе №13

Фильтр пакетов

Эзиз Хатамов

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 помощью firewall-cmd

1. Получены административные полномочия (`su -`).

2. Определена зона брандмауэра по умолчанию (`public`).

3. Выведен список доступных зон.

4. Просмотрены службы, поддерживаемые брандмауэром.

```
ehatamov@ehatamov:~$ sudo -i
[sudo] password for ehatamov:
root@ehatamov:~#
root@ehatamov:~# firewall-cmd --get-default-zone
public
root@ehatamov:~# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@ehatamov:~# 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-testnet
 bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit coll
ectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls d
ocker-registry docker-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-av
ailability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kde
connect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-cont
roller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kube
let-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve ma
trix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-spe
ed-most-wanted 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-exporter proxy-dh
cp 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 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 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 war
pinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd w
sdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-tra
pper zabbix-web-service zero-k zerotier
root@ehatamov:~#
```

Рис. 2.1: firewall zones and services

5. Получен перечень разрешённых сервисов в активной зоне.

6. Проанализирована полная конфигурация зоны по умолчанию и отдельный запрос конфигурации зоны `public`.

   Выводы совпали, так как зона `public` является используемой зоной по умолчанию.

```
root@ehatamov:~# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@ehatamov:~# 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@ehatamov:~# 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@ehatamov:~#
```

Рис. 2.2: firewall list-all output

2.1.1 Добавление сервиса VNC

7. Сервис `vnc-server` был добавлен в конфигурацию времени выполнения.

8. Проверено наличие сервиса — он присутствовал среди разрешённых.

```
root@ehatamov:~# firewall-cmd --add-service=vnc-server
success
root@ehatamov:~# 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@ehatamov:~# systemctl restart firewalld.service
root@ehatamov:~# 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@ehatamov:~#
```

Рис. 2.3: firewall add vnc

9. После перезапуска службы `firewalld` сервис исчез.

   Причина: изменение относилось только к runtime-конфигурации, которая

сбрасывается при перезапуске.

2.1.2 Добавление VNC-сервера как постоянной настройки

10. Сервис `vnc-server` был добавлен уже как постоянный.

11. После добавления он отсутствовал в выводе конфигурации — изменения были сохранены, но не применены.

12. После перезагрузки конфигурации `firewalld` сервис стал отображаться среди разрешённых.

```
root@ehatamov:~# firewall-cmd --add-service=vnc-server --permanent
success
root@ehatamov:~# 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@ehatamov:~# firewall-cmd --reload
success
root@ehatamov:~# 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@ehatamov:~#
```

Рис. 2.4: firewall add permanent + reload

2.1.3 Добавление порта 2022/TCP

13. В конфигурацию добавлен порт `2022/tcp` как постоянный.

14. После перезагрузки конфигурации порт появился в списке разрешённых.

2.2 Управление брандмауэром с помощью GUI firewall-config

1. Запущено приложение `firewall-config`.

2. Выбрано значение *Permanent* для сохранения всех вносимых изменений.

3. В зоне `public` включены службы `http`, `https` и `ftp`.

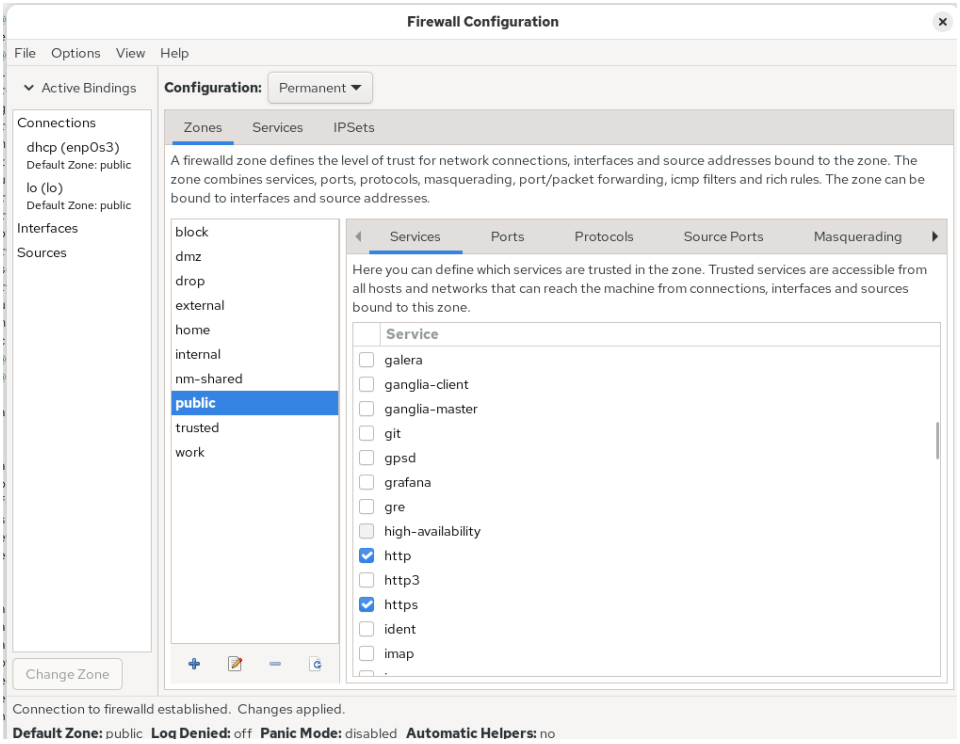

Рис. 2.5: GUI service enable

4. На вкладке **Ports** добавлен порт `2022/udp`.

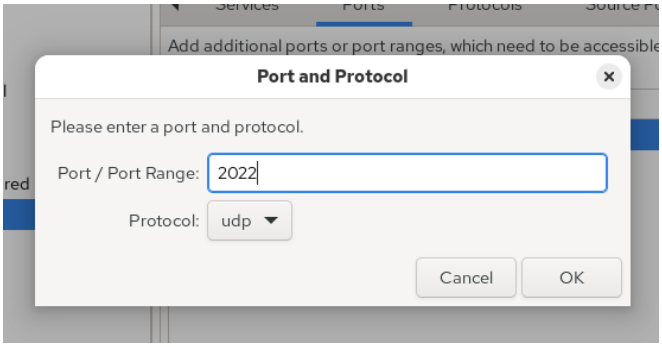

Рис. 2.6: GUI add port

5. В конфигурации времени выполнения изменения отсутствовали — они были внесены только в постоянную конфигурацию.

6. После перезагрузки конфигурации настройки вступили в силу.

```
root@ehatamov:~# 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@ehatamov:~# firewall-cmd --reload
success
root@ehatamov:~# 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@ehatamov:~#
```

Рис. 2.7: GUI reload results

2.3 Самостоятельная работа

1. В конфигурацию брандмауэра добавлены службы:

    - telnet (через командную строку)
    - imap
    - pop3
    - smtp

(три последних — через `firewall-config` на вкладке **Services**)

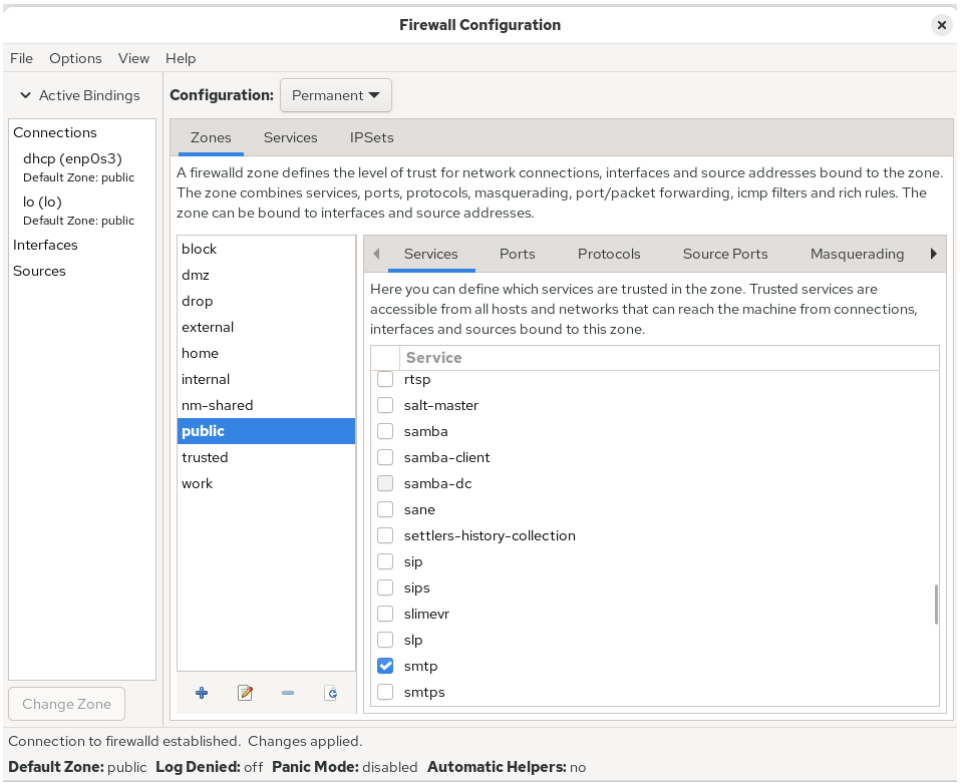

Рис. 2.8: GUI enable imap pop3 smtp

2. После перезагрузки конфигурации все службы отображаются как разрешённые и являются постоянными.

```
root@ehatamov:~# firewall-config
root@ehatamov:~#
root@ehatamov:~# firewall-cmd --add-service=telnet
success
root@ehatamov:~# firewall-cmd --add-service=telnet --permanent
success
root@ehatamov:~# firewall-cmd --reload
success
root@ehatamov:~# 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@ehatamov:~#
```

Рис. 2.9: final config

3 Контрольные вопросы

1. **Какая служба должна быть запущена перед началом работы с менеджером конфигурации брандмауэра firewall-config?**
    - Должна быть запущена служба `firewalld`.
2. **Какая команда позволяет добавить UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию?**
    - `firewall-cmd --add-port=2355/udp`
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 --add-interface=eno1`

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

    - Он будет добавлен в зону по умолчанию (обычно `public`).

4 Заключение

В ходе работы были освоены команды и инструменты для управления конфигурацией брандмауэра в Linux с помощью `firewall-cmd` и `firewall-config`, включая добавление сервисов, портов и изменение настроек зон.