Отчёт по лабораторной работе №13

Фильтр пакетов

Анастасия Мазуркевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2 Ход выполнения

2.1 Управление брандмауэром с помощью firewalld

После получения прав администратора через `su -` выполнена настройка межсетевого экрана.

2.1.1 Просмотр активной конфигурации

Определена зона, используемая по умолчанию. Система возвращает `public`. Затем просмотрены доступные зоны и список всех поддерживаемых сервисов.

```
admazurkevich@admazurkevich:~$ su
Password:
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# firewall-cmd --get-default-zone
public
root@admazurkevich:/home/admazurkevich# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@admazurkevich:/home/admazurkevich# 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 aseqne
t audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-tes
tnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpi
t collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-ov
er-tls docker-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-availability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenk
ins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-
secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-w
orker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmn
r-udp managesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql n
bd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-im
ageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometh
eus-node-exporter proxy-dhcp 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 s
mtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-tra
nsfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing syncthing-gui syncthi
ng-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 wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabb
ix-java-gateway zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
root@admazurkevich:/home/admazurkevich#
```

Рис. 2.1: Информация о зоне и доступных службах

Для сравнения получены сведения о текущей конфигурации зоны: как общим запросом (`firewall-cmd --list-all`), так и с указанием зоны

(`firewall-cmd --list-all --zone=public`).

Оба результата совпали, что подтверждает использование зоны `public`.

Рис. 2.2: Просмотр конфигурации зоны

2.1.2 Добавление службы VNC

В конфигурацию времени исполнения добавлен сервис `vnc-server`. После выполнения он появился в списке разрешённых.

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

Рис. 2.3: Добавление VNC на время выполнения

После перезапуска службы `firewalld` запись пропала.
Причина: добавление без параметра `--permanent` изменяет только конфигурацию *runtime*, которая очищается при перезапуске.

2.1.3 Добавление VNC на постоянной основе

Сервис повторно добавлен, но уже с сохранением в конфигурационные файлы. После внесения изменений был выполнен `reload`, что применило настройки на активную конфигурацию.
Теперь `vnc-server` присутствует постоянно.

```
root@admazurkevich:/home/admazurkevich#
root@admazurkevich:/home/admazurkevich# firewall-cmd --add-service=vnc-server --permanent
success
root@admazurkevich:/home/admazurkevich# 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@admazurkevich:/home/admazurkevich# firewall-cmd --reload
success
root@admazurkevich:/home/admazurkevich# 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: Добавление VNC permanent + reload

2.1.4 Добавление TCP-порта 2022

В конфигурацию записан порт `2022/tcp` с последующим `reload`. В результате в параметре *ports* появилась строка `2022/tcp`.

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

{

#fig:009 005=70% }

2.2 Управление через графический интерфейс firewall-config

Инструмент GUI запущен командой `firewall-config`.

В раскрывающемся меню выбрано значение *Permanent*, чтобы все изменения сохранялись.

Для зоны `public` включены сервисы `http`, `https`, `ftp`.

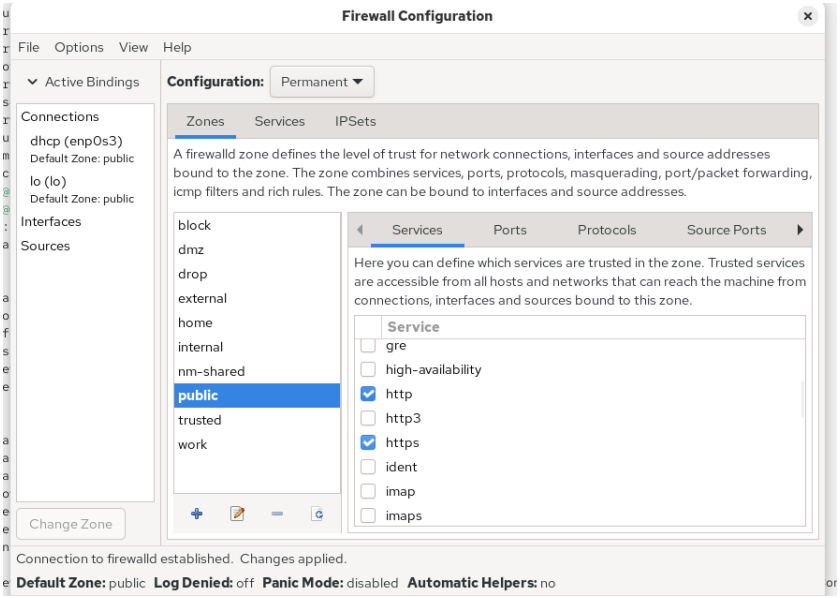

Рис. 2.5: GUI — включение служб

На вкладке *Ports* добавлен порт 2022 с протоколом udp.

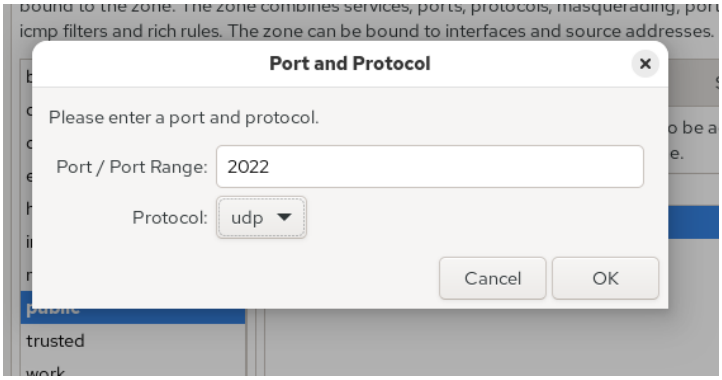

Рис. 2.6: GUI — добавление порта udp 2022

После закрытия GUI изменения ещё не применены в runtime. Перезагрузка конфигурации активирует новые правила, и теперь они отображаются в списке.

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

Рис. 2.7: Изменения вступили в силу после reload

2.3 Самостоятельная часть

В конфигурацию межсетевого экрана добавлены службы `telnet`, `imap`, `pop3`, `smtp`.

- `telnet` был добавлен через командную строку с сохранением.
- `imap`, `pop3`, `smtp` добавлены через GUI.

После `reload` все службы отображаются в активной конфигурации зоны `public`.

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

Рис. 2.8: Добавленные службы telnet, imap, pop3, smtp

3 Контрольные вопросы

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

Перед использованием firewall-config должна быть запущена служба firewalld.

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

Добавление выполняется командой firewall-cmd с параметром добавления порта и протокола UDP в постоянную конфигурацию.

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

Для отображения полной конфигурации используется вывод всех зон.

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

Удаление выполняется командой firewall-cmd с параметром удаления сервиса vnc-server.

5. Какая команда позволяет активировать новую конфигурацию, добавленную опцией `--permanent`?

Для применения постоянных изменений используется перезагрузка конфигурации.

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

Проверка выполняется через вывод текущей конфигурации зоны.

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

Интерфейс добавляется в зону public с помощью параметра добавления интерфейса.

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

Интерфейс будет помещён в зону по умолчанию, которой является public.

4 Заключение

В ходе работы была изучена конфигурация межсетевого экрана на основе firewalld. Выполнены операции с временными и постоянными правилами, добавлены службы и порты, а также использованы оба способа управления — через терминал и графическую утилиту firewall-config. Полученные навыки позволяют уверенно настраивать сетевую безопасность в Linux, контролировать доступ к сервисам и адаптировать конфигурацию в соответствии с требованиями системы.