

Отчёт по лабораторной работе №13

Фильтр пакетов

Шаханеоядж Хаоладар

Содержание

1 Цель работы	5
2 Выполнение	6
2.1 Управление брандмауэром с помощью firewall-cmd	6
2.2 Управление с помощью графического интерфейса firewall-config .	10
2.3 Самостоятельная работа	12
3 Контрольные вопросы	14
4 Заключение	16

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2 Выполнение

2.1 Управление брандмауэром с помощью firewall-cmd

1. Получены привилегии администратора с помощью команды `su -`.
 2. Определена зона, активная по умолчанию. Вывод показал, что используется зона **public**.
 3. Просмотрены все зоны, доступные в `firewalld`.
 4. Отображён перечень доступных сервисов, поддерживаемых брандмауэром.

```
haoladar@haoladar:~$ su
Password:
root@haoladar:/home/haoladar# firewall-cmd --get-default-zone
public
root@haoladar:/home/haoladar# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@haoladar:/home/haoladar# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvra amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcupsd aseqnet
audit ausweispassp bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet
et bitcoin-testnet-rpc bittorent-lsd ceph ceph-exporter cepf-mon cfengine checkmk-agent civilization-iv civilization-v cockpit
collected condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpcv6 dhcpcv6-client distcc dns dns-over-quic dns-over-tls
docker-docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman proxy
frei0r-freeipa-freeipa-ldaps freeipa-implementation freeipa-trust ftp galera ganglia-client ganglia-master git gpgsql grafana gre
igh-availability httpd https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target ists jenkins kadem
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 libdnsp libvirt libvirt-tls lightning-network llmnz llmnz-client llmnz-tcp llmnz-uds manag
gesleve matrix mdns memcache minecraft mindnlp mndp mongdb mosh mountd mptt mqtt-tls ms-wbt mssql murmur myql nbd nebula n
eed-for-speed-most-wanted netbios-ns netdata-dashbaord nfs nfs3 nmea-0183 nrpe ntp npf opentelemetry openvpn ovirt-imageio ovirt-
storageconsole ovirt-vmconsole plex pmxmd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-expo
rter proxy-dhcp ps2link ps3netrv ptl pulsadev puppetmaster quassel radius radsec rdp redis reddit-sentinel rootd rpc-bind rquot
ad rsb rsysnd rtsp salt-master samba samba-client samba-dc same settlers-history-collection sip sipmlv slp smtp smtp-submission
smtps snmp snmpntls snmpntls-trap snmptrap spiderOak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfer steam-stre
aming stellaris stronghold-crusader stdu stuns submission supertuxkart svrdrp svr syncthing syncthing-gui syncthing-relay synergy
syscomlan syslog syslog-tls telnet tentacle terraria tftp title38 tinc tor-socks transmission-client turn turns upnp-client vdom v
nc-server vrpp warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-d
iscovery-udp wsdd wsdd-https wmsan wmsans xmcdp 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@haoladar:/home/haoladar# firewall-cmd -list-services
cockpit dhcpcv6-client ssh
root@haoladar:/home/haoladar#
```

5. Проверены службы, уже разрешённые в активной зоне.
 6. Выполнено сравнение вывода двух команд: `firewall-cmd --list-all` и `firewall-cmd --list-all --zone=public`.

Оба результата совпали, что подтверждает: активная зона — **public**.

```
root@haoladar:/home/haoladar#
root@haoladar:/home/haoladar# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@haoladar:/home/haoladar# 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 dhcpcv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@haoladar:/home/haoladar# █
```

7. Временное добавление сервиса `vnc-server` в конфигурацию брандмауэра.

```
root@haoladar:/home/haoladar# firewall-cmd --add-service=vnc-server
success
root@haoladar:/home/haoladar# firewall-cmd --list-all
\public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
    services: cockpit dhcpcv6-client ssh vnc-server
  ports:
  protocols:
    forward: yes
    masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@haoladar:/home/haoladar# systemctl restart firewalld.service
root@haoladar:/home/haoladar# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
    services: cockpit dhcpcv6-client ssh
  ports:
  protocols:
    forward: yes
    masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@haoladar:/home/haoladar#
```

8. Выполнена проверка — сервис появился в списке разрешённых.
9. Служба firewalld была перезапущена. После перезапуска сервис vnc-server исчез.
10. Причина: ранее сервис был добавлен только во время выполнения, а конфигурация не была сохранена как постоянная.
11. Повторное добавление vnc-server, теперь в постоянную конфигурацию.

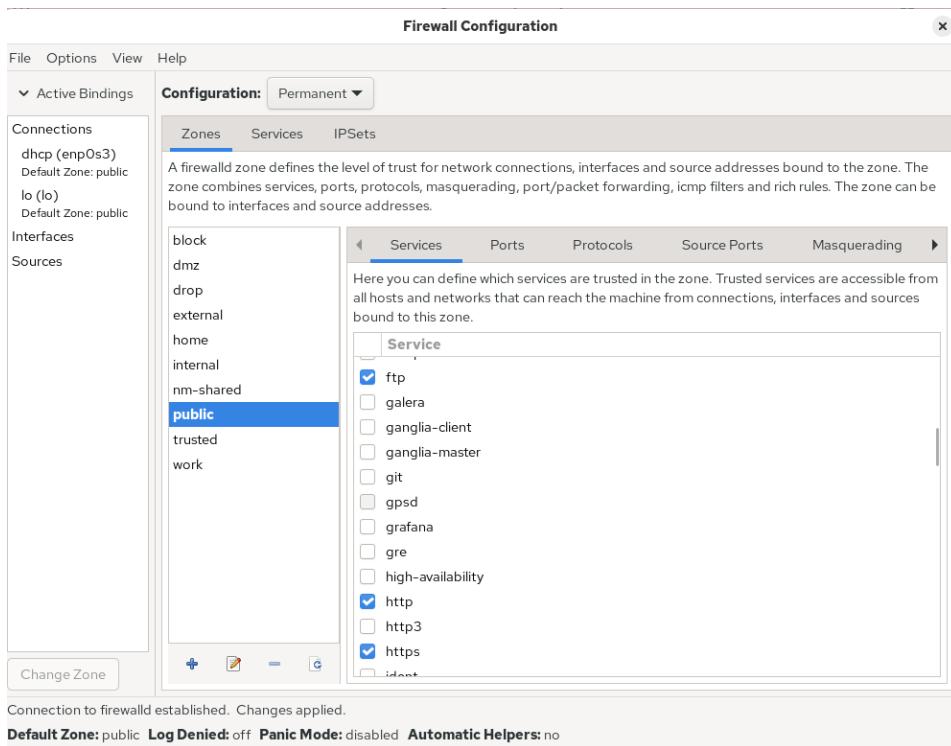
```
-----, -----  
root@haoladar:/home/haoladar# firewall-cmd --add-service=vnc-server --permanent  
success  
root@haoladar:/home/haoladar# firewall-cmd --list-all  
public (default, active)  
    target: default  
    ingress-priority: 0  
    egress-priority: 0  
    icmp-block-inversion: no  
    interfaces: enp0s3  
    sources:  
    services: cockpit dhcpcv6-client ssh  
    ports:  
    protocols:  
        forward: yes  
        masquerade: no  
        forward-ports:  
        source-ports:  
        icmp-blocks:  
        rich rules:  
root@haoladar:/home/haoladar# firewall-cmd --reload  
success  
root@haoladar:/home/haoladar# firewall-cmd --list-all  
public (default, active)  
    target: default  
    ingress-priority: 0  
    egress-priority: 0  
    icmp-block-inversion: no  
    interfaces: enp0s3  
    sources:  
    services: cockpit dhcpcv6-client ssh vnc-server  
    ports:  
    protocols:  
        forward: yes  
        masquerade: no  
        forward-ports:  
        source-ports:  
        icmp-blocks:  
        rich rules:  
root@haoladar:/home/haoladar#
```

12. Проверка конфигурации показывает, что сервис пока отсутствует — изменения сохранены на диск, но не активированы.
13. Выполнена перезагрузка конфигурации. После этого `vnc-server` стал активным.
14. В конфигурацию добавлен порт `2022/tcp` как постоянное правило. После перезагрузки конфигурации порт появился в списке.

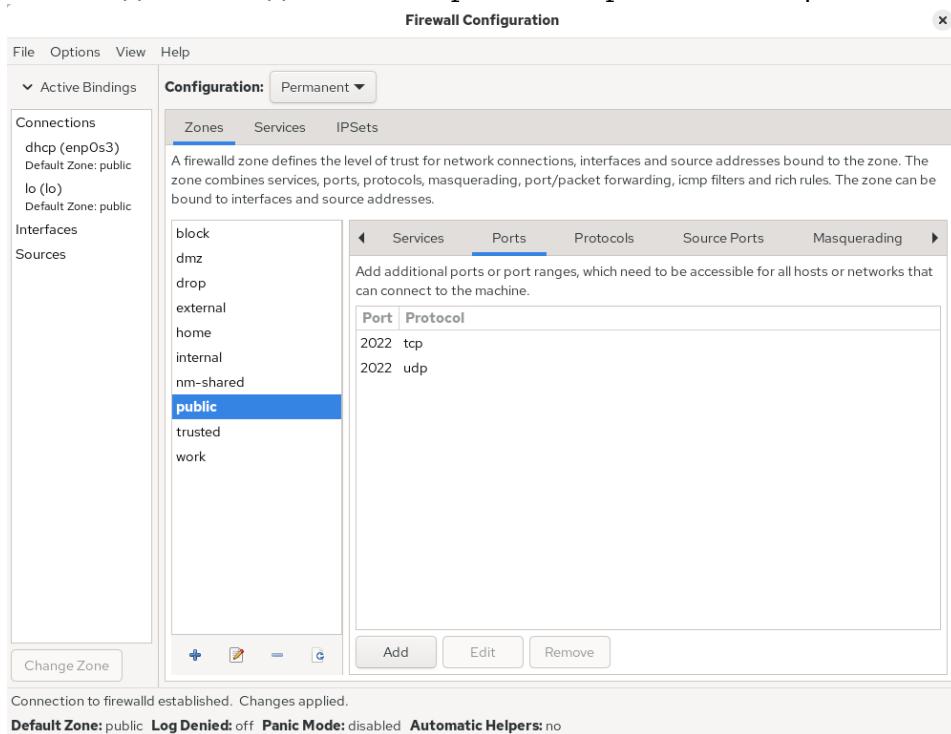
```
root@haoladar:/home/haoladar# firewall-cmd --add-port=2022/tcp --per
success
root@haoladar:/home/haoladar# firewall-cmd --add-port=2022/tcp --permanent
Warning: ALREADY_ENABLED: 2022:tcp
success
root@haoladar:/home/haoladar# firewall-cmd --reload
success
root@haoladar:/home/haoladar# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@haoladar:/home/haoladar# █
```

2.2 Управление с помощью графического интерфейса **firewall-config**

1. Запущено приложение **firewall-config**.
2. В параметре *Configuration* выбрано значение **Permanent**, чтобы сохранить изменения на постоянной основе.
3. В зоне **public** включены службы **http, https, ftp**.



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



5. После закрытия утилиты изменения были сохранены, но не применены к

текущему состоянию.

6. Для применения изменений выполнена перезагрузка конфигурации. После этого они стали активны.

```
root@haoladar:/home/haoladar# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@haoladar:/home/haoladar# firewall-cmd --reload
success
root@haoladar:/home/haoladar# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpcv6-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@haoladar:/home/haoladar#
```

2.3 Самостоятельная работа

1. Настроена конфигурация межсетевого экрана, разрешающая доступ к службам:
 - telnet

- imap
 - pop3
 - smtp
2. Служба `telnet` добавлена через командную строку. Сервисы `imap`, `pop3`, `smtp` включены через `firewall-config`.
3. После выполнения `firewall-cmd --reload` конфигурация стала активной.

В списке сервисов появились требуемые службы.

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

(firewall-config:5755): dconf-WARNING **: 10:15:58.347: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe

(firewall-config:5755): dconf-WARNING **: 10:15:58.347: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
root@haoladar:/home/haoladar# firewall-cmd --reload
success
root@haoladar:/home/haoladar# firewall-cmd --list-all
public (default, active)
    target: default
    ingress-priority: 0
    egress-priority: 0
    icmp-block-inversion: no
    interfaces: enp0s3
    sources:
    services: cockpit dhcpcv6-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@haoladar:/home/haoladar#
```

3 Контрольные вопросы

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

firewalld.service – именно эта служба должна быть активна для работы `firewall-config`.

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

firewall-cmd –add-port=2355/udp – временно (runtime)

firewall-cmd –add-port=2355/udp –permanent – в постоянную конфигурацию

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?

В зону по умолчанию

4 Заключение

В ходе работы освоено управление брандмауэром с использованием **firewall-cmd** и **firewall-config**. На практике выполнено добавление сервисов и портов, применение временных и постоянных правил, а также управление зонами и интерфейсами. Получены навыки работы как с командной строкой, так и с графическим интерфейсом настройки межсетевого экрана.