

Отчёт по лабораторной работе №13

Фильтр пакетов

Агджабекова Эся Рустамовна

Содержание

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

Список иллюстраций

2.1	Определение зоны по умолчанию, доступных зон и сервисов . . .	6
2.2	Сравнение вывода list-all и list-all -zone	7
2.3	Добавление vnc-server и поведение после перезапуска	8
2.4	Добавление vnc-server в постоянную конфигурацию	9
2.5	Добавление порта 2022/tcp	9
2.6	Добавление сервисов в графическом интерфейсе	10
2.7	Добавление порта 2022/udp	11
2.8	Активированные службы после reload	12
2.9	Активированные службы: telnet, imap, pop3, smtp	13

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2 Выполнение работы

2.1 Управление брандмауэром с помощью firewall-cmd

1. Получены права администратора. Определена текущая зона по умолчанию, просмотрены доступные зоны и список поддерживаемых сервисов (см. рис. fig. 2.1).

```
eragdzhabekova@eragdzhabekova:~$ su
Password:
root@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --get-default-zone
public
root@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@eragdzhabekova:/home/eragdzhabekova# 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 auswebsapp2 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 ctddb 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-lid
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 lperf2 lperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerber
os kibana klogon 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 ndns memcache m
inecraft minidlna mndp mongod mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios
-ns netdata-dashboard nfs nfs3 nmap nmap-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex
pmcd pmpoxy pmwebapi pmwebapi3 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 vdsd vnc-server vrrp warpinator wben-http wben-https wiregua
rd ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wssd wssd-http wsmn 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@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@eragdzhabekova:/home/eragdzhabekova#
```

Рис. 2.1: Определение зоны по умолчанию, доступных зон и сервисов

2. Просмотрены активные сервисы в текущей зоне. Сравнён вывод информа-
ции при использовании `list-all` и `list-all --zone=public`
(см. рис. fig. 2.2).

```

root@eragdzhabekova:/home/eragdzhabekova# 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@eragdzhabekova:/home/eragdzhabekova# 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@eragdzhabekova:/home/eragdzhabekova# █

```

Рис. 2.2: Сравнение вывода list-all и list-all --zone

3. Временно добавлен сервис **vnc-server**. Выполнена проверка — сервис появился в конфигурации.
4. Выполнен перезапуск службы брандмауэра. Сервис **vnc-server** исчез из конфигурации, так как изменение было внесено только во время выполнения и не сохранилось в постоянной конфигурации (см. рис. fig. 2.3).

```

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

```

Рис. 2.3: Добавление vnc-server и поведение после перезапуска

- Сервис **vnc-server** добавлен повторно с сохранением в постоянной конфигурации. После перезагрузки конфигурации подтверждено его наличие (см. рис. fig. 2.4).

```

root@eragdzhabekova:/home/eragdzhabekova#
root@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --add-service=vnc-server --permanent
success
root@eragdzhabekova:/home/eragdzhabekova# 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@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --reload
success
root@eragdzhabekova:/home/eragdzhabekova# 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@eragdzhabekova:/home/eragdzhabekova# █

```

Рис. 2.4: Добавление vnc-server в постоянную конфигурацию

- В постоянную конфигурацию добавлен порт **2022/tcp**. После перезагрузки конфигурации подтверждено его появление (см. рис. fig. 2.5).

```

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

```

Рис. 2.5: Добавление порта 2022/tcp

2.2 Управление брандмауэром с помощью firewall-config

1. Запущен графический интерфейс firewall-config.
2. В параметре **Configuration** выбрано значение *Permanent*, чтобы все изменения становились постоянными.
3. Для зоны **public** включены службы **http**, **https** и **ftp** (см. рис. fig. 2.6).
4. На вкладке *Ports* добавлен порт **2022/udp** (см. рис. fig. 2.7).

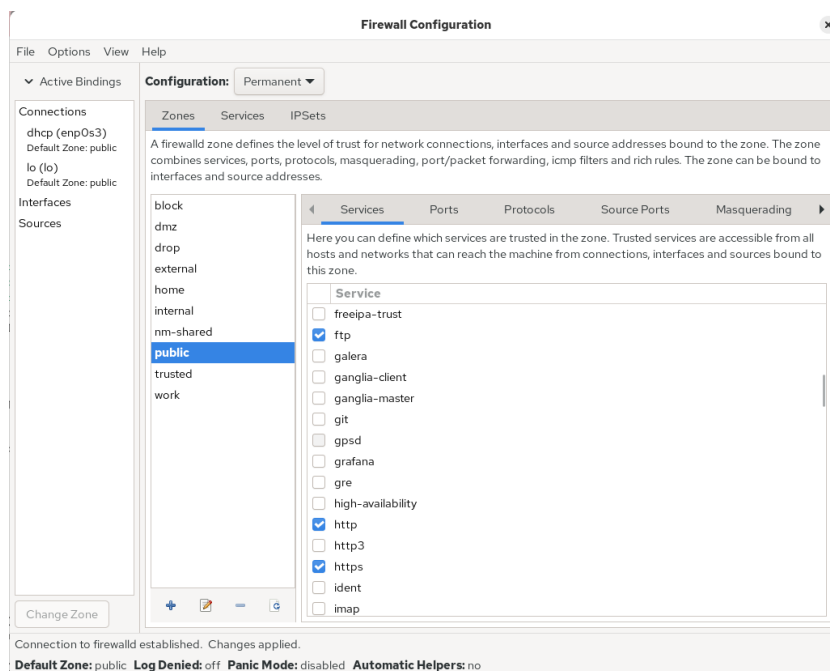


Рис. 2.6: Добавление сервисов в графическом интерфейсе

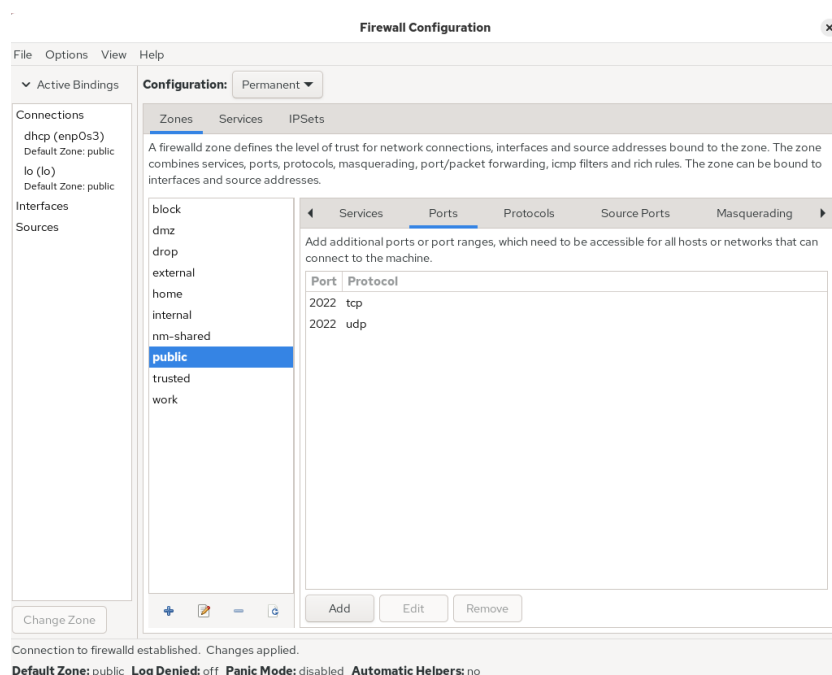


Рис. 2.7: Добавление порта 2022/udp

5. Проверка показала, что изменения ещё не применены, так как были внесены в постоянную конфигурацию.
6. После перезагрузки конфигурации все изменения вступили в силу (см. рис. fig. 2.8).

```

-----
root@eragdzhabekova:/home/eragdzhabekova# 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@eragdzhabekova:/home/eragdzhabekova# firewall-cmd --reload
success
root@eragdzhabekova:/home/eragdzhabekova# 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@eragdzhabekova:/home/eragdzhabekova# █

```

Рис. 2.8: Активированные службы после reload

2.3 Самостоятельная работа

1. Через командную строку добавлена служба **telnet**.
2. Через графический интерфейс включены службы **imap**, **pop3** и **smtp**.
3. Подтверждено, что все изменения сохранены и применены (см. рис. fig. 2.9).

```
root@eragdzhbekova:/home/eragdzhbekova# firewall-cmd --add-service=telnet
success
root@eragdzhbekova:/home/eragdzhbekova# firewall-cmd --reload
success
root@eragdzhbekova:/home/eragdzhbekova# 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 vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@eragdzhbekova:/home/eragdzhbekova# █
```

Рис. 2.9: Активированные службы: telnet, imap, pop3, smtp

3 Контрольные вопросы

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

Служба firewalld.

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

Используется параметр `--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?**

Используется параметр `--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?**

Используется параметр `--zone=public --add-interface=en01`.

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

В зону по умолчанию (*default zone*).

4 Заключение

В ходе выполнения лабораторной работы были изучены способы управления брандмауэром Linux с использованием инструментов `firewall-cmd` и графической утилиты `firewall-config`. Были получены навыки просмотра активных зон и служб, добавления сервисов и портов как во временную, так и в постоянную конфигурацию. На практике отработано различие между конфигурацией времени выполнения и постоянной конфигурацией, а также применение перезагрузки правил для их активации. В результате закрепились навыки администрирования сетевой безопасности и управления правилами доступа в системах на базе Linux.