

Лабораторная работа №13

Фильтр пакетов

Юсупова Ксения Равиловна

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выполнение самостоятельной работы	13
5	Ответы на контрольные вопросы	15
6	Выводы	17

Список иллюстраций

3.1	Выполнили пункты 1-4 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)	7
3.2	Выполнили пункты 5-6 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)	8
3.3	Выполнили пункты 7-10 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)	9
3.4	Выполнили пункты 11-13 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)	10
3.5	Выполнили пункты 14 и 15 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)	10
3.6	Выполнили пункт 1-3 из раздела 13.4.2. (Управление брандмауэром с помощью firewall-config)	11
3.7	Выполнили пункт 4 и 5 из раздела 13.4.2. (Управление брандмауэром с помощью firewall-config)	11
3.8	Выполнили пункты 6 и 7 из раздела 13.4.2. (Управление брандмауэром с помощью firewall-config)	12
4.1	Выполнили пункты 1 и 2 из раздела 13.5. (Самостоятельная работа)	13
4.2	Выполнили пункты 1 и 2 из раздела 13.5. (Самостоятельная работа)	13
4.3	Выполнили пункты 1 и 2 из раздела 13.5. (Самостоятельная работа)	14

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2 Задание

1. Используя `firewall-cmd`:

- определить текущую зону по умолчанию;
- определить доступные для настройки зоны;
- определить службы, включённые в текущую зону;
- добавить сервер VNC в конфигурацию брандмауэра.

2. Используя `firewall-config`:

- добавьте службы `http` и `ssh` в зону `public`;
- добавьте порт 2022 протокола UDP в зону `public`;
- добавьте службу `ftp`.

3. Выполните задание для самостоятельной работы (раздел 13.5).

3 Выполнение лабораторной работы

Получили полномочия администратора, определили текущую зону по умолчанию, доступные зоны и посмотрели службы, доступные на компьютере(рис. 3.1).

```
[ksyusha@yu ~]$ su -
Пароль:
[root@yu ~]# firewall-cmd --get-default-zone
public
[root@yu ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@yu ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp
amqps apcupsd audit ausweisapp2 bacula bacula-client bareos-director bareos-fi
ledaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-tes
tnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent coc
kpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp
dhcpcv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dro
pbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-prox
y freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp g
alera ganglia-client ganglia-master git gpsd grafana gre high-availability htt
p http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target
isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kpropp kshell ku
be-api kube-apiserver kube-control-plane kube-control-plane-secure kube-contro
ller-manager kube-controller-manager-secure kube-nodeport-services kube-schedu
ler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker
ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp
llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt m
qtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs
nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storagec
onsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgre
sql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv p
tp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rootd rpc-b
ind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip s
ips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroa
k-lansync spotify-sync squid sssd ssh steam-streaming svdrp svn syncthing sync
thing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftpd tile3
8 tinc tor-socks transmission-client upnp-client vdsu vnc-server warpinator wb
em-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp
ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-ser
ver zabbix-agent zabbix-server zerotier
```

Рис. 3.1: Выполнили пункты 1-4 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)

Определили доступные службы в текущей зоне и сравнили результаты вывода информации при использовании команды firewall-cmd --list-all и команды firewall-

cmd -list-all -zone=public (рис. 3.2).

```
[root@yu ~]# firewall-cmd --list-services
cockpit dhcpv6-client ssh
[root@yu ~]# firewall-cmd --list-all
public (active)
  target: default
  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@yu ~]# firewall-cmd --list-all --zone=public
public (active)
  target: default
  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:
```

Рис. 3.2: Выполнили пункты 5-6 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)

Добавили сервер VNC в конфигурацию брандмауэра, проверили, что добавился vnc-server в конфигурацию. Перезапустили службу firewalld и проверили, что vnc-server нет в конфигурации, так как при использовании команды firewall-cmd -add-service=vnc-server без параметра -permanent правило добавляется только в текущую (runtime) конфигурацию брандмауэра, но не сохраняется в постоянную конфигурацию.(рис. 3.3).


```

[root@yu ~]# firewall-cmd --add-service=vnc-server
success
[root@yu ~]# firewall-cmd --list-all
public (active)
  target: default
  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@yu ~]# systemctl restart firewalld
[root@yu ~]# firewall-cmd --list-all
public (active)
  target: default
  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:

```

Рис. 3.3: Выполнили пункты 7-10 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)

Добавили службу vnc-server ещё раз, но на этот раз сделали её постоянной и проверили наличие vnc-server в конфигурации. Увидели, что VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения. Перезагрузилите конфигурацию firewalld и просмотрели конфигурацию времени выполнения(рис. 3.4).

```

[root@yu ~]# firewall-cmd --add-service=vnc-server --permanent
success
[root@yu ~]# firewall-cmd --list-all
public (active)
  target: default
  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@yu ~]# firewall-cmd --reload
success
[root@yu ~]# firewall-cmd --list-all
public (active)
  target: default
  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:

```

Рис. 3.4: Выполнили пункты 11-13 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)

Добавили в конфигурацию межсетевого экрана порт 2022 протокола TCP и перезагрузили конфигурацию firewalld. Проверили, что порт добавлен в конфигурацию(рис. 3.5).

```

[root@yu ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@yu ~]# firewall-cmd --reload
success
[root@yu ~]# firewall-cmd --list-all
public (active)
  target: default
  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:

```

Рис. 3.5: Выполнили пункты 14 и 15 из раздела 13.4.1. (Управление брандмауэром с помощью firewall-cmd)

Открыли терминал и под учётной записью своего пользователя запустили интерфейс GUI firewall-config. Нажали выпадающее меню рядом с параметром Configuration . Открыли раскрывающийся список и выбрали Permanent . Это позволило сделать постоянными все изменения, которые вносим при конфигурировании. Выбрали зону public и отметили службы http, https и ftp, чтобы включить их. (рис. 3.6).

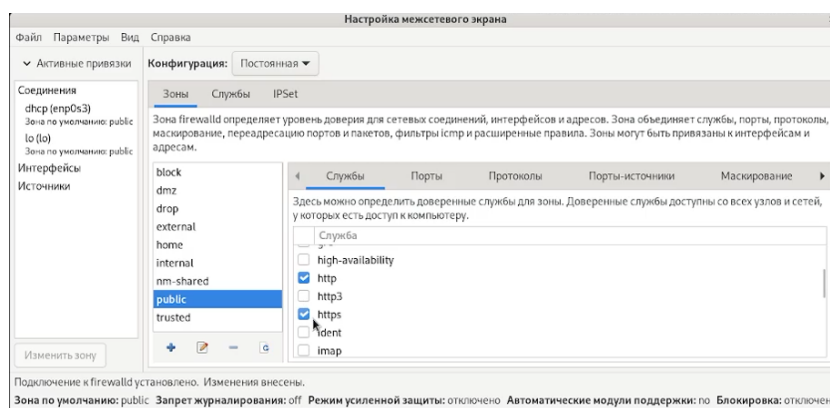


Рис. 3.6: Выполнили пункт 1-3 из раздела 13.4.2. (Управление брандмауэром с помощью firewall-config)

Выбрали вкладку Ports и на этой вкладке нажали Add . Ввели порт 2022 и протокол udp, закрыли утилиту firewall-config.(рис. 3.7).

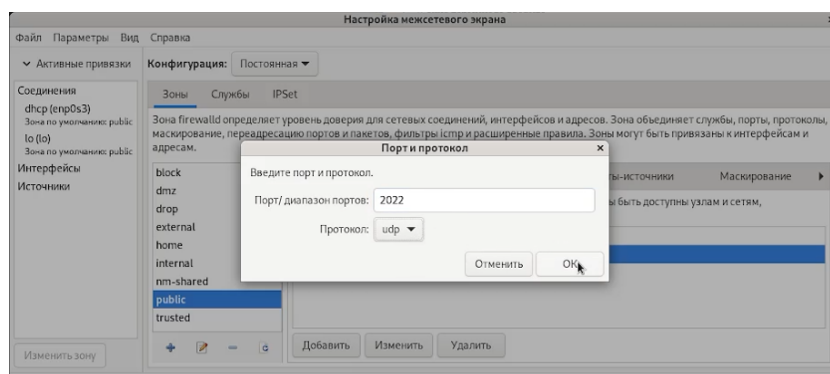


Рис. 3.7: Выполнили пункт 4 и 5 из раздела 13.4.2. (Управление брандмауэром с помощью firewall-config)

В окне терминала ввели `firewall-cmd –list-all`. Обратили внимание, что изменения, которые только что внесли, ещё не вступили в силу. Это связано с тем, что

настроили их как постоянные изменения, а не как изменения времени выполнения. Перегрузили конфигурацию firewall-cmd и список доступных сервисов, увидели, что изменения были применены.(рис. 3.8).

```
[ksyusha@yu ~]$ firewall-config
[ksyusha@yu ~]$ firewall-cmd --list-all
public (active)
  target: default
  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:
[ksyusha@yu ~]$ firewall-cmd --reload
success
[ksyusha@yu ~]$ firewall-cmd --list-all
public (active)
  target: default
  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:
[ksyusha@yu ~]$
```

Рис. 3.8: Выполнили пункты 6 и 7 из раздела 13.4.2. (Управление брандмауэром с помощью firewall-config)

4 Выполнение самостоятельной работы

Создали в командной строке конфигурацию межсетевого экрана, которая позволяет получить доступ к службе telnet(рис. 4.1).

```
[ksyusha@yu ~]$ firewall-cmd --add-service=telnet --permanent  
success  
[ksyusha@yu ~]$
```

Рис. 4.1: Выполнили пункты 1 и 2 из раздела 13.5. (Самостоятельная работа)

Создали в графическом интерфейсе конфигурацию межсетевого экрана, которая позволяет получить доступ для служб imap, pop3, smtp (рис. 4.2).

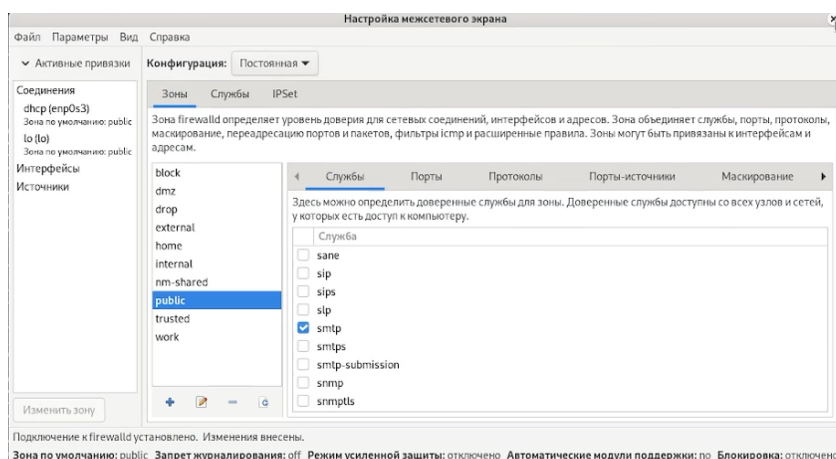


Рис. 4.2: Выполнили пункты 1 и 2 из раздела 13.5. (Самостоятельная работа)

Убедились, что конфигурация является постоянной и будет активирована после перезагрузки компьютера.(рис. 4.3).

```
[ksyusha@yu ~]$ firewall-cmd --reload
success
[ksyusha@yu ~]$ firewall-cmd --list-all
public (active)
  target: default
  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:
[ksyusha@yu ~]$
```

Рис. 4.3: Выполнили пункты 1 и 2 из раздела 13.5. (Самостоятельная работа)

5 Ответы на контрольные вопросы

1. Служба `firewalld.service` должна быть запущена перед работой с `firewall-config`, так как этот графический инструмент является фронтом для управления демоном `firewalld`.
2. Команда `firewall-cmd --add-port=2355/udp` добавляет UDP-порт 2355 в текущую зону. Без параметра `--permanent` изменение будет временным и сбросится после перезагрузки службы.
3. Команда `firewall-cmd --list-all-zones` показывает полную конфигурацию всех зон, включая службы, порты, протоколы и настройки каждой зоны.
4. Команда `firewall-cmd --remove-service=vnc-server` удаляет службу `vnc-server` из текущей конфигурации. Для постоянного удаления нужно добавить параметр `--permanent`.
5. Команда `firewall-cmd --reload` активирует постоянную конфигурацию, загружая правила, добавленные с параметром `--permanent`, без полной перезагрузки службы.
6. Параметр `--list-all` показывает текущую активную конфигурацию выбранной зоны, позволяя убедиться, что изменения применились и теперь активны.
7. Команда `firewall-cmd --zone=public --add-interface=en01` назначает интерфейс `en01` конкретной зоне `public`. Для постоянного назначения требуется параметр `--permanent`.

8. Новый интерфейс автоматически добавляется в зону по умолчанию (обычно public), если не указана конкретная зона. Зону по умолчанию можно проверить командой `firewall-cmd --get-default-zone`.

6 Выводы

В ходе лабораторной работы мы получили навыки настройки пакетного фильтра в Linux.