# Отчёт по лабораторной работе №13

**Фильтр пакетов**

Анна Саенко

# Содержание

# Список иллюстраций

# Список таблиц

# 1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

# 2 Ход выполнения работы

## 2.1 Управление брандмауэром с помощью firewall-cmd

Для начала работы я получила права суперпользователя и определила параметры текущей зоны.

Я узнала, какая зона используется по умолчанию, какие зоны доступны в системе, а также просмотрела список всех поддерживаемых сервисов.

На скриншоте видно вывод команд с информацией о зоне и доступных службах.

```
aasaenko@aasaenko:~$ su
Password:
root@aasaenko:/home/aasaenko# firewall-cmd --get-default-zone
public
root@aasaenko:/home/aasaenko# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@aasaenko:/home/aasaenko# 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 ausweis
app2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bitto
rrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit collectd condor-collector cratedb ctdb dds
dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls docker-registry docker-swarm dropbox-lansync elastics
earch 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 jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-pl
ane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secur
e kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp m
anagesieve matrix 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-storageconsole ovirt-vmco
nsole plex pmcd pmproxy pmwebapi pmwebapis 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 sam
ba-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spo
tify-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-cl
ient turn turns upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host w
s-discovery-tcp ws-discovery-udp wsdd wsdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gatewa
y zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
root@aasaenko:/home/aasaenko# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@aasaenko:/home/aasaenko#
```

Рис. 2.1: Получение информации о зонах и сервисах

### 2.1.1 Просмотр текущей конфигурации

Я проверила, какие службы разрешены в активной зоне.

Затем сравнила вывод конфигурации при просмотре стандартной зоны и при

указании зоны *public*.

Поскольку зона *public* является активной по умолчанию, результаты совпали.

```
root@aasaenko:/home/aasaenko# 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@aasaenko:/home/aasaenko# 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@aasaenko:/home/aasaenko#
```

Рис. 2.2: Просмотр активной зоны

### 2.1.2 Добавление сервиса VNC

Я добавила службу `vnc-server` в конфигурацию времени выполнения. Сервис появился в списке.

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

Рис. 2.3: Добавление службы vnc-server

После перезапуска службы firewalld изменения исчезли.
Это произошло потому, что служба была добавлена только во временную конфигурацию (runtime), которая теряется при перезагрузке службы.

### 2.1.3 Добавление сервиса VNC в постоянную конфигурацию

Я повторно добавила службу `vnc-server`, но на этот раз в постоянную конфигурацию.

Сервис не появился сразу в runtime, так как постоянные изменения не применяются автоматически.

После перезагрузки конфигурации изменения вступили в силу.

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

Рис. 2.4: Добавление в постоянную конфигурацию

### 2.1.4 Добавление порта 2022

Я добавила порт 2022/TCP в постоянную конфигурацию и перезагрузила настройки.

После обновления конфигурации порт появился в списке.

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

Рис. 2.5: Добавление порта 2022

## 2.2 Управление брандмауэром через firewall-config (GUI)

Я запустила графическую утилиту и переключила режим на *Permanent*.

В зоне *public* были включены службы ftp, http и https.

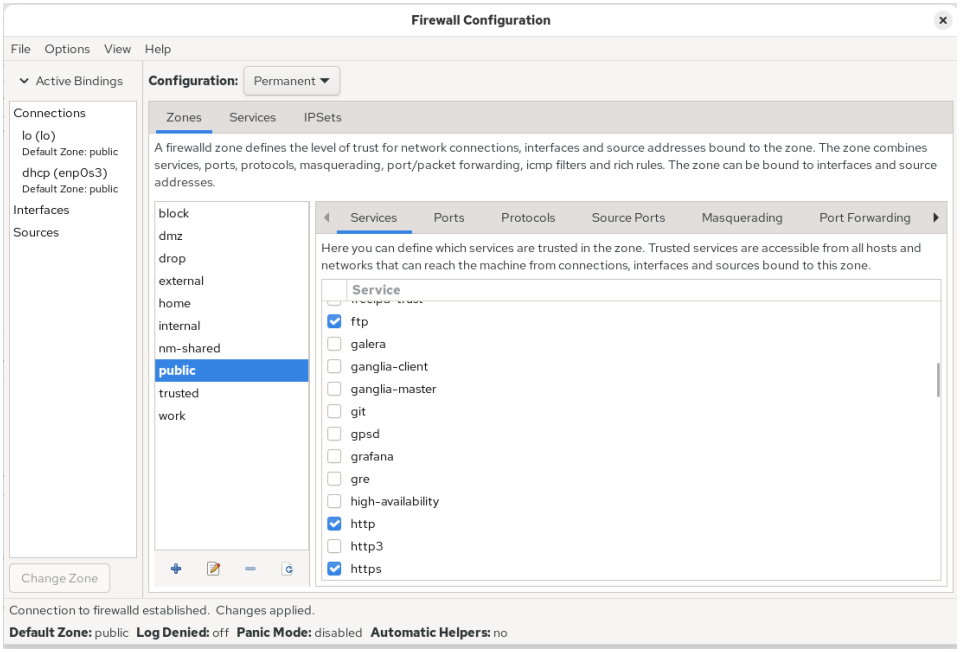


Рис. 2.6: Добавление служб через GUI

На вкладке *Ports* я добавила порт 2022/udp.

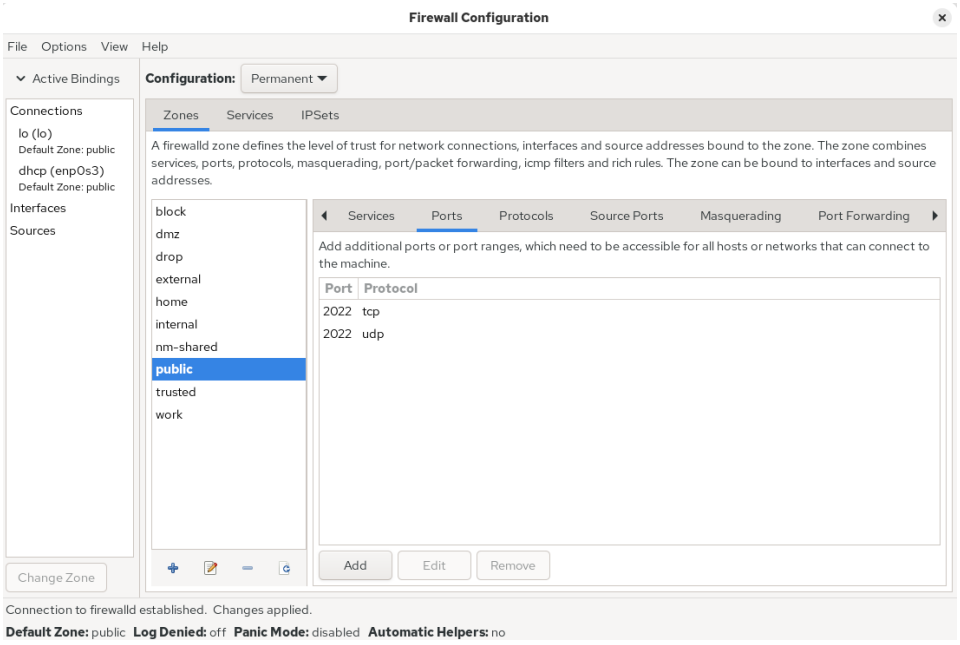


Рис. 2.7: Добавление порта через GUI

После выхода из утилиты изменения ещё не были активны.

Загрузка конфигурации применила их к runtime, и новые параметры стали вид-

ны.

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

Рис. 2.8: Финальная конфигурация

## 2.3 Самостоятельная работа

Я настроила доступ к службам telnet, imap, pop3 и smtp:

– telnet добавлен через командную строку;

– imap, pop3 и smtp включены через графический интерфейс `firewall-config`.

Изменения сохранены как постоянные, и будут активны после перезагрузки системы.

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

Рис. 2.9: Финальная конфигурация

# 3 Контрольные вопросы

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

2. **Какая команда позволяет добавить UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию?**
   Для добавления порта используется команда:
   `firewall-cmd --add-port=2355/udp --permanent`

3. **Какая команда позволяет показать всю конфигурацию брандмауэра во всех зонах?**
   Для отображения полной конфигурации используется команда:
   `firewall-cmd --list-all-zones`

4. **Какая команда позволяет удалить службу vnc-server из текущей конфигурации брандмауэра?**
   Удаление службы выполняется командой:
   `firewall-cmd --remove-service=vnc-server`

5. **Какая команда firewall-cmd позволяет активировать новую конфигурацию, добавленную опцией –permanent?**
   Чтобы применить постоянные изменения, используется команда:
   `firewall-cmd --reload`

6. **Какой параметр firewall-cmd позволяет проверить, что новая конфигу-**

**рация была добавлена в текущую зону и теперь активна?**

Проверка активной конфигурации выполняется командой:

`firewall-cmd --list-all`

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

   Добавление интерфейса в зону выполняется командой:

   `firewall-cmd --zone=public --add-interface=eno1 --permanent`

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

   Если зона не указана, интерфейс будет добавлен в **зону по умолчанию** (default zone), обычно это `public`.

# 4 Заключение

В результате выполнения лабораторной работы я получила практические навыки управления брандмауэром Linux с помощью утилит `firewall-cmd` и `firewall-config`.
Были выполнены следующие действия:

- определение активной зоны и просмотр доступных зон и служб;
- сравнение конфигурации зоны по умолчанию с явным указанием зоны;
- добавление сервиса в конфигурацию времени выполнения и в постоянную конфигурацию;
- объяснение различий между runtime- и permanent-настройками;
- добавление сетевых портов в брандмауэр;
- применение изменений и проверка итоговой конфигурации;
- использование графического интерфейса `firewall-config` для управления службами и портами.