

Лабораторная работа №13

Фильтр пакетов

Перфилов Александр Константинович | группа НПИбд 03-24

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
3 Ответы на контрольные вопросы	14
4 Выводы	16

Список иллюстраций

2.1	Текущая и доступные зоны	6
2.2	Доступные службы	7
2.3	Доступные службы в текущей зоне	7
2.4	Сравнение двух выдач информации	8
2.5	Добавление сервера в конфигурацию	8
2.6	Перезапуск службы firewalld	8
2.7	Проверка наличия сервера в конфигурации	9
2.8	Добавление службы в конфигурацию на постоянной основе	9
2.9	Перезагрузка firewalld и просмотр конфигурации времени выполнения	10
2.10	Добавление в конфигурацию порт	10
2.11	Открытый интерфейс GUI firewall-config	11
2.12	Параметр Configuration на Permanent	11
2.13	Включение служб http, https и ftp	11
2.14	Добавление порта	12
2.15	Вывод информации	12
2.16	Проверка применения изменений	13
2.17	Добавление telnet	13
2.18	Проверка применения изменений	13

Список таблиц

1 Цель работы

Получение навыков настройки пакетного фильтра в Linux.

2 Выполнение лабораторной работы

Получим полномочия администратора. Определим текущую зону по умолчанию. Определим доступные зоны.

```
akpperfilov@akpperfilov:~$ su -  
Пароль:  
Последний вход в систему: Сб ноя 22 16:28:03 MSK 2025 на pts/0  
root@akpperfilov:~# firewall-cmd --get-default-zone  
public  
root@akpperfilov:~# firewall-cmd --get-zones  
block dmz drop external home internal nm-shared public trusted work  
root@akpperfilov:~#
```

Рисунок 2.1: Текущая и доступные зоны

Посмотрим службы, доступные на компьютере.

```
root@akpperfilov:~# 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 ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin-bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-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 dhcpcv6 dhcpcv6-client distcc dns dns-over-quic dns-over-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 gpgsql 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-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler 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 minecraft minidlna mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-nost-manted netbios-ns netdata -dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapis pop3 pop3s postgresql privoxy prometheus-prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd salt-master samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp smtp sntp-submission smtsp snmp snmpTLS snmpTLS-trap snmptrap spideroak-lansync spotify-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-client turn turns upnp-client vdsm vnc-server vrpp 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 xmpp-bosh xmpp-client xmpp-local xmpp-serve zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-service zero-k zero-tier
```

Рисунок 2.2: Доступные службы

Определим доступные службы в текущей зоне.

```
root@akpperfilov:~# firewall-cmd --list-services
cockpit dhcpcv6-client ssh
```

Рисунок 2.3: Доступные службы в текущей зоне

Сравним результаты вывода информации при использовании команд.

Вывод одинаков

```
root@akpperfilov:~# 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:
```

Рисунок 2.4: Сравнение двух выдач информации

Добавим сервер VNC в конфигурацию брандмауэра. Проверим, добавился ли vnc-server в конфигурацию.

```
root@akpperfilov:~# firewall-cmd --add-service=vnc-server
success
root@akpperfilov:~# 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:
```

Рисунок 2.5: Добавление сервера в конфигурацию

Перезапустим службу firewalld.

```
root@akpperfilov:~# systemctl restart firewalld
```

Рисунок 2.6: Перезапуск службы firewalld

Проверим, есть ли vnc-server в конфигурации. (нет)

```
root@akpperfilov:~# 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:
```

Рисунок 2.7: Проверка наличия сервера в конфигурации

Добавим службу vnc-server ещё раз, но на этот раз сделайте её постоянной.

Проверим наличие vnc-server в конфигурации.

```
root@akpperfilov:~# firewall-cmd --add-service=vnc-server --permanent
success
root@akpperfilov:~# 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:
```

Рисунок 2.8: Добавление службы в конфигурацию на постоянной основе

Служба не появилась сразу, при использовании опции –permanent нужно перезагрузить конфигурацию firewalld.

Перезагрузим конфигурацию firewalld и просмотрим конфигурацию времени выполнения .

```
root@akpperfilov:~# firewall-cmd --reload
success
root@akpperfilov:~# 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: 22/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рисунок 2.9: Перезагрузка firewalld и просмотр конфигурации времени выполнения

Сервер vnc отображается в конфигурации.

Добавим в конфигурацию межсетевого экрана порт 2022 протокола TCP. Затем перезагрузим конфигурацию firewalld. Проверим, что порт добавлен в конфигурацию.

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

Рисунок 2.10: Добавление в конфигурацию порт

Откроем терминал и под учётной записью пользователя запустим интерфейс **GUI firewall-config**.

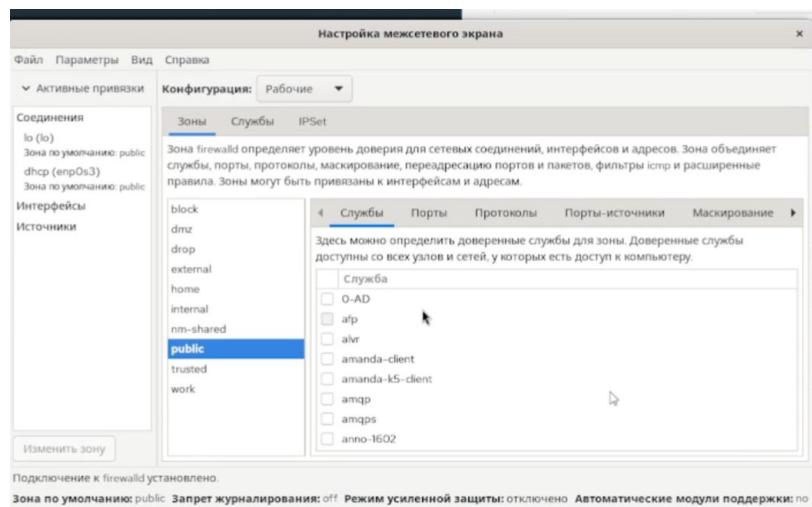


Рисунок 2.11: Открытый интерфейс GUI firewall-config

Нажмём выпадающее меню рядом с параметром **Configuration**. Откроем раскрывающийся список и выберем **Permanent**. Это позволит сделать постоянными все изменения .

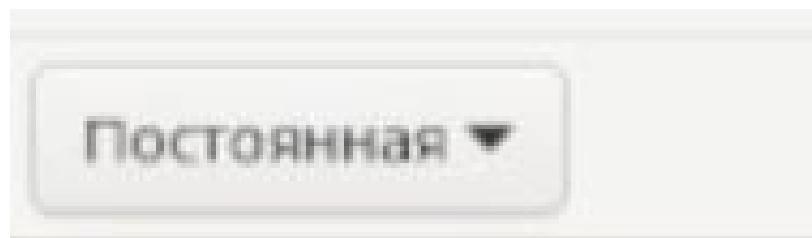


Рисунок 2.12: Параметр Configuration на Permanent

Выберем зону **public** и отметим службы **http**, **https** и **ftp**, чтобы включить их.

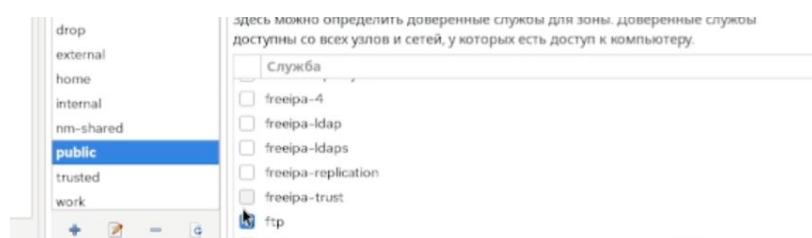


Рисунок 2.13: Включение служб http, https и ftp

Выберем вкладку **Ports** и на этой вкладке нажмём **Add**. Введём порт 2022 и

протокол **udp**, нажмём OK , чтобы добавить их в список.

internal		2022 tcp
nm-shared		80 tcp
public		2022 udp

Рисунок 2.14: Добавление порта

Закроем утилиту **firewall-config**. В окне терминала введём **firewall-cmd –list-all**.

```
root@akppel:~# 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:
```

Рисунок 2.15: Вывод информации

Изменения ещё не вступили в силу, так как конфигурация выбрана постоянная.

Перегрузим конфигурацию **firewall-cmd**. Вызовем список доступных сервисов.

```
root@akpperflov:~# 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 80/tcp 2022/udp
    protocols:
      forward: yes
      masquerade: no
      forward-ports:
      source-ports:
    icmp-blocks:
    rich rules:
```

Рисунок 2.16: Проверка применения изменений

Создадим конфигурацию межсетевого экрана, которая позволяет получить доступ к следующим службам: - telnet; - imap; - pop3; - smtp.

Сделаем это как в командной строке (для службы telnet), так и в графическом интерфейсе (для служб imap, pop3, smtp). .



Рисунок 2.17: Добавление telnet

Затем добавим оставшиеся службы через графический интерфейс по аналогии.

Перезагрузим конфигурации, чтобы убедиться, что конфигурация является постоянной

```
root@akpperflov:~# 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 80/tcp 2022/udp
    protocols:
      forward: yes
      masquerade: no
      forward-ports:
      source-ports:
    icmp-blocks:
    rich rules:
```

Рисунок 2.18: Проверка применения изменений

3 Ответы на контрольные вопросы

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

Нужно запустить службу firewalld, это можно сделать командой systemctl start firewalld.

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

Команда firewall-cmd –add-port=2355/udp –permanent.

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

Команда firewall-cmd –list-all-zones.

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

Команда firewall-cmd –remove-service=vnc-server –permanent.

5. Какая команда firewall-cmd позволяет активировать новую конфигурацию, добавленную опцией –permanent?

Команда firewall-cmd –reload.

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

Команда `firewall-cmd --list-all`.

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

Команда `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?

Он будет добавлен в зону по умолчанию.

4 Выводы

В ходе выполнения лабораторной работы я получил навыки работы с фильтрами пакетов.