

Лабораторная работа №13

Фильтр пакетов

Хохлачёва Полина Дмитриевна

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
3 Ответы на вопросы	13
4 Выводы	14

Список иллюстраций

2.1	Зоны	6
2.2	Службы	6
2.3	Службы	7
2.4	Информация	7
2.5	Добавление	8
2.6	Пармет	8
2.7	Добавление	9
2.8	Добавление	9
2.9	Терминал	10
2.10	Конфигурация	10
2.11	Добавление	10
2.12	Список	11
2.13	Создание	11
2.14	Выбор	12
2.15	Проверка	12

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux

2 Выполнение лабораторной работы

Получаем полномочия администратора, определяем текущую зону по умолчанию, определяем доступные зоны(рис. 2.1).

```
[khokhlacheva@khokhlacheva ~]$ su -
Пароль:
[root@khokhlacheva ~]# firewall-cmd --get-default-zone
public
[root@khokhlacheva ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
```

Рис. 2.1: Зоны

Доступные службы на моём компьютере(рис. 2.2).

```
[root@khokhlacheva ~]# 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-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpcv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server 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 iden t imap imaps 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 minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysq l nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmp proxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sipsl slp smtp smtp-submission smtps snmp snmp-tls snmptrap snmptrap_spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tor-socks transmission-client upnp-client vdsman vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman xmpp xdmcx xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
```

Рис. 2.2: Службы

Доступные службы в текущей зоне(рис. 2.3).

```
[root@khokhlacheva ~]# firewall-cmd --list-services  
cockpit dhcpcv6-client ssh
```

Рис. 2.3: Службы

Информация, выводимая обеими командами, абсолютно идентична - нет никаких различий в отображаемых настройках firewall.(рис. 2.4).

```
[root@khokhlacheva ~]# firewall-cmd --list-all  
public (active)  
  target: default  
  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@khokhlacheva ~]# firewall-cmd --list-all --zone=public  
public (active)  
  target: default  
  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:
```

Рис. 2.4: Информация

Добавляем сервер VNC в конфигурацию, проверяем добавился ли сервер в конфигурацию, перезапускаем службу(рис. 2.5).

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

Рис. 2.5: Добавление

vnc-server больше не указан, потому что правило добавили без параметра `-permanent`(рис. 2.6).

```
[root@khokhlacheva ~]# firewall-cmd --list-all  
public (active)  
    target: default  
    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:
```

Рис. 2.6: Пармет

Добавляем службу ещё раз и делаем её постоянной, проверяем наличия `vnc-server` в конфигурации, перезагружаем конфигурацию и смотрим конфигурацию времени выполнения(рис. 2.7).

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

Рис. 2.7: Добавление

Добавляем в конфигурацию порт 2022 протокола, перезагружаем конфигурацию, проверяем, что порт добавлен(рис. 2.8).

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

Рис. 2.8: Добавление

Открываем терминал под своей учётной записью(рис. 2.9).

```
[root@khokhlacheva ~]# firewall-config
```

Рис. 2.9: Терминал

В конфигурации выбираем “постоянная”, далее в public выбираем http, https и ftp(рис. ??).

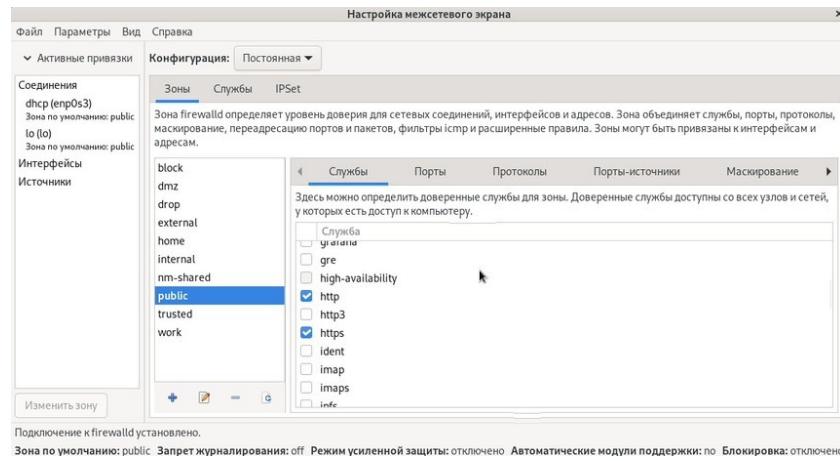


Рис. 2.10: Конфигурация

Добавляем порт 2022 и протокол, чтобы добавить их в список(рис. ??).

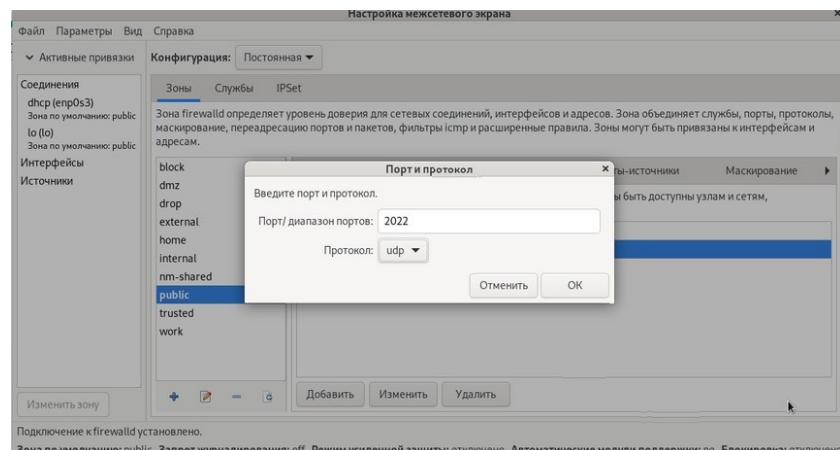


Рис. 2.11: Добавление

Перезагружаем конфигурацию и список доступных сервисов, чтобы увидеть изменения(рис. ??).

```
[root@khokhlacheva ~]# firewall-cmd --list-all
public (active)
  target: default
  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@khokhlacheva ~]# firewall-cmd --reload
success
[root@khokhlacheva ~]# firewall-cmd --list-all
public (active)
  target: default
  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:
```

Рис. 2.12: Список

#Выполнения самостоятельной работы

Создаём конфигурацию командной строкой(рис. ??).

```
[root@khokhlacheva ~]# firewall-cmd --add-service=telnet --permanent
success
```

Рис. 2.13: Создание

В графическом интерфейсе выбираем imap, pop3, smtp(рис. ??).

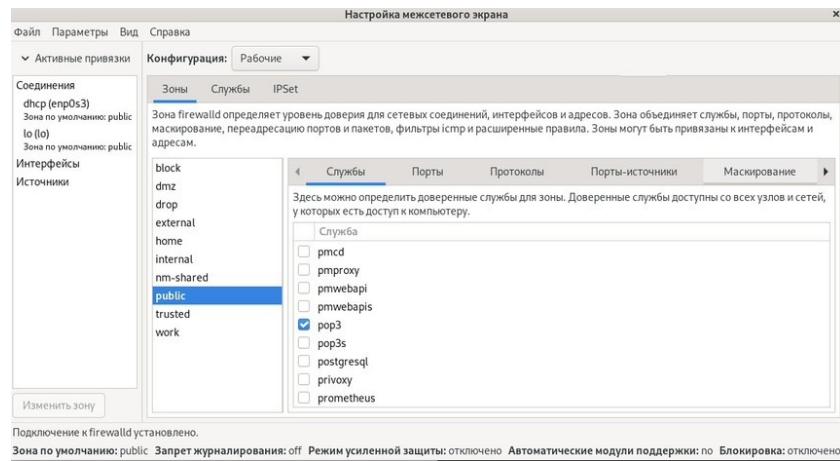


Рис. 2.14: Выбор

Убеждаемся, что конфигурация активна и постоянна после перезагрузки(рис. ??).

```
[root@khokhlacheva ~]# firewall-cmd --add-service=telnet --permanent
Warning: ALREADY_ENABLED: telnet
success
[root@khokhlacheva ~]# firewall-cmd --list-all
public (active)
  target: default
  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@khokhlacheva ~]# firewall-config
[root@khokhlacheva ~]#
```

Рис. 2.15: Проверка

3 Ответы на вопросы

1. firewalld
2. firewall-cmd –add-port=2355/udp
3. firewall-cmd –list-all-zones
4. firewall-cmd –remove-service=vnc-server
5. firewall-cmd –reload
6. –list-all
7. firewall-cmd –zone=public –add-interface=en01
8. В зону public (зона по умолчанию)

4 Выводы

Мы получили навыки настройки пакетного фильтра в Linux