

Лабораторная работа №13

Фильтр пакетов

Хохлачева Полина Дмитриевна

Российский университет дружбы народов, Москва, Россия

Информация

- Хохлачева Полина Дмитриевна
- Российский университет дружбы народов
- Номер студенческого билета- 1132242473
- [1132242473@pfur.ru]

Вводная часть

Получить навыки настройки пакетного фильтра в Linux

Получаем полномочия администратора, определяем текущую зону по умолчанию, определяем доступные зоны(рис. (fig:001?)).

```
[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
```

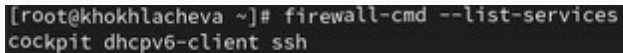
Рис. 1: Зоны

Выполнение лабораторной работы

Доступные службы на моём компьютере(рис. (fig:002?)).

```
[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-filer 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 dhcpv6-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 gpsd grafana gre high-availability http http3 https ident 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 memcached
memcached minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula
netbios-ns netdata-dashboard nfs nfs3 nmap nmap 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 ps3netserver ptp pulseaudio
puppetmaster quassel radius rdp redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master
samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmp-tls
snmp-tls-trap snmptrap spideroak-lansync spotify-sync squid sssd ssh steam-steamstreaming
svdrp svn syncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle
tftp tile38 tinc tor-socks transmission-client upnp-client vnc vnc-server warpinator
wbem-http wbem-https wireguard ws-discovery ws-discovery
```

Доступные службы в текущей зоне(рис. (fig:003?)).



```
[root@khokhlacheva ~]# firewall-cmd --list-services  
cockpit dhcpv6-client ssh
```

Рис. 3: Подключение

Выполнение лабораторной работы

Информация, выводимая обеими командами, абсолютно идентична - нет никаких различий в отображаемых настройках firewall(рис. (fig:004?)).

```
[root@khokhlacheva ~]# 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@khokhlacheva ~]# firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
```

Выполнение лабораторной работы

Добавляем сервер VNC в конфигурацию, проверяем добавился ли сервер в конфигурацию, перезапускаем службу(рис. (fig:005?)).

```
[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 dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@khokhlacheva ~]# systemctl restart firewalld
```

vnc-server больше не указан, потому что правило добавили без параметра `-permanent`(рис. (fig:006?)).

```
[root@khokhlacheva ~]# 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. 6: Параметр

Выполнение лабораторной работы

Добавляем службу ещё раз и делаем её постоянной, проверяем наличия vnc-server в конфигурации, перезагружаем конфигурацию и смотрим конфигурацию времени выполнения(рис. (fig:007?)).

```
[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 dhcpv6-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:
```

Выполнение лабораторной работы

Добавляем в конфигурацию порт 2022 протокола, перезагружаем конфигурацию, проверяем, что порт добавлен(рис. (fig:008?)).

```
[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 dhcpv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 8: Добавление

Открываем терминал под своей учётной записью(рис. (fig:009?)).



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

Рис. 9: Терминал

Выполнение лабораторной работы

В конфигурации выбираем “постоянная”, далее в public выбираем http, https и ftp(рис. (fig:009?)).

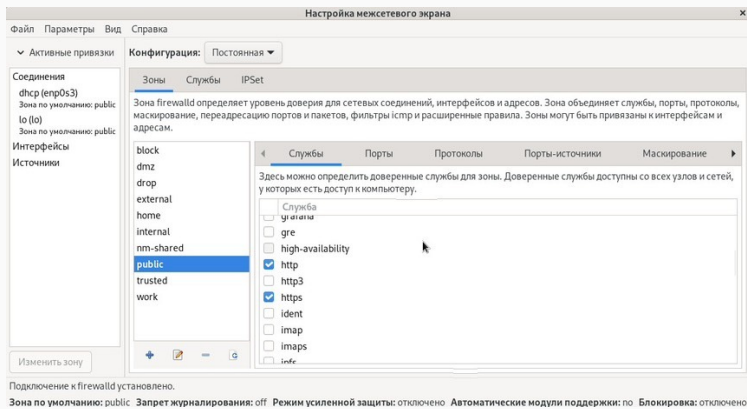


Рис. 10: Конфигурация

Добавляем порт 2022 и протокол, чтобы добавить их в список(рис. (fig:011?)).

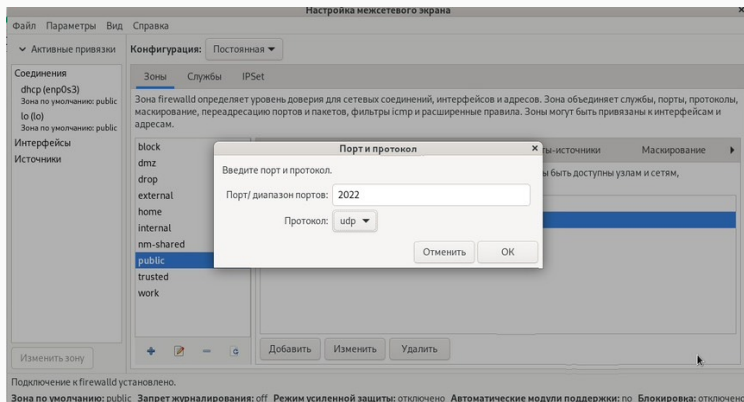


Рис. 11: Добавление

Выполнение лабораторной работы

Перезагружаем конфигурацию и список доступных сервисов, чтобы увидеть изменения((рис. (fig:012?)).

```
[root@khokhlacheva ~]# 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:

[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 dhcpv6-client ftp http https ssh vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
```

Выполнение самостоятельной работы

Создаём конфигурацию командной строкой(рис. (fig:013?)).



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

Рис. 13: Добавление

Выполнение самостоятельной работы

В графическом интерфейсе выбираем `imap`, `pop3`, `smtp`(рис. (fig:014?)).

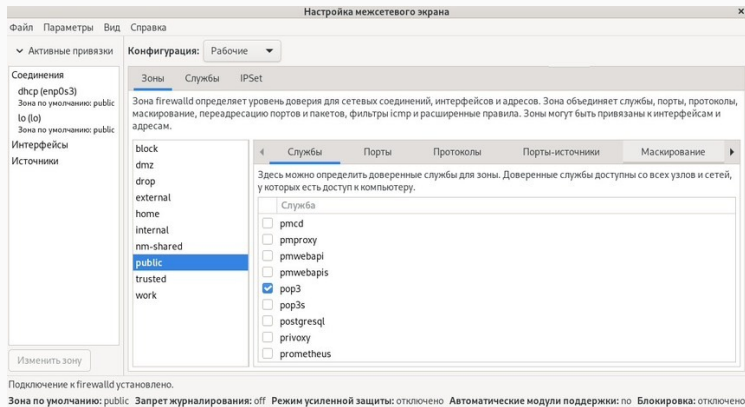
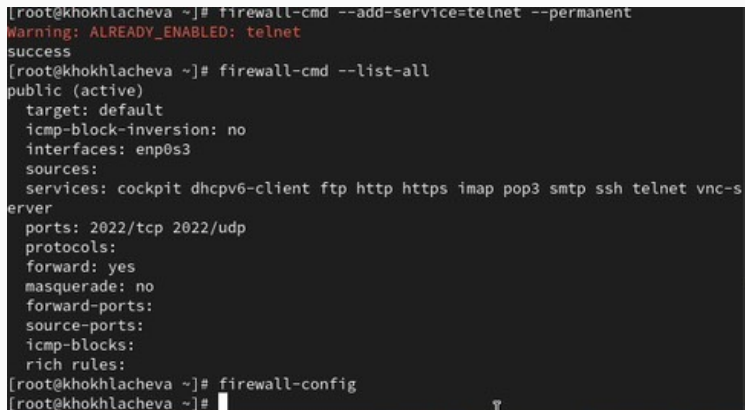


Рис. 14: Выбор

Убеждаемся, что конфигурация активна и постоянна после перезагрузки(рис. (fig:015?)).

A terminal window with a dark background and light-colored text. The user is at a root prompt on a machine named khokhlacheva. They run 'firewall-cmd --add-service=telnet --permanent', which returns a warning that telnet is already enabled and then 'success'. Next, they run 'firewall-cmd --list-all', which displays the current firewall configuration for the 'public' zone, showing it is active with various settings like target, interfaces, services, ports, and protocols. Finally, they run 'firewall-config', which returns to the root prompt.

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

Рис. 15: Выбор

Выводы

Мы получили навыки настройки сетевых параметров системы.