

Лабораторная работа № 13

Отчёт

Ермишина Мария Кирилловна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Контрольные вопросы	12
4	Выводы	13

Список иллюстраций

2.1	Добавление конфигураций	8
2.2	Настройки брандмауэра	9
2.3	Управление брандмауэром с помощью firewall-config	10
2.4	Самостоятельная работа	11

Список таблиц

1 Цель работы

Целью данной лабораторной работы является получение навыков настройки пакетного фильтра в Linux.

2 Выполнение лабораторной работы

1. Управление брандмауэром с помощью firewall-cmd Запустите терминал и получите полномочия администратора. Определите текущую зону по умолчанию, введя: (рис. ??)
 - firewall-cmd –get-default-zone Определите доступные зоны, введя: (рис. ??)
 - firewall-cmd –get-zones Посмотрите службы, доступные на вашем компьютере, используя (рис. ??)
 - firewall-cmd –get-services Определите доступные службы в текущей зоне: (рис. ??)
 - firewall-cmd –list-services Сравните результаты вывода информации при использовании команд: (рис. ??)
 - firewall-cmd –list-all
 - firewall-cmd –list-all –zone=public (рис. ??) Добавьте сервер VNC в конфигурацию брандмауэра: (рис. ??)
 - firewall-cmd –add-service=vnc-server Проверьте, добавился ли vnc-server в конфигурацию: (рис. ??)
 - firewall-cmd –list-all Перезапустите службу firewalld: (рис. ??)
 - systemctl restart firewalld Проверьте, есть ли vnc-server в конфигурации: (рис. ??)
 - firewall-cmd –list-all

```

termimash@termimash -j$ su -
Password:
[root@termimash ~]# firewall-cmd --get-default-zone
public
[root@termimash ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@termimash ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula
etcd-client bares-dstream bares-filedemon bares-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-test
et-rpc bittorrent-lsd ceph ceph-exporter ceph-mon ceph-ng cephfs checkm3-agent cockpit collectd condor-collector cratedb ct
b dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox
dynamips etcd-client etcd-server finger foreman foreman-proxy freepipa-1 freepipa-lamp freepipa-lamps fre
ip-replication freipa-trust ftp galera ganglia-client ganglia-master git gssd grafana gre high-availability http htt
3 https client imap imaps ipfs ipfs-ipp-client ipsec irc ircs ircs-target isns jenkins kadmin kdeconnect kerberos klibn
a klogix kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-man
ager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet k
ubelet-readyonly kubelet-worker-lamp ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp
managesieve matrix ndms memcache minidlna mongod mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netb
os-nfs netdata-dashboards nfs nf33 nmap-0183 nrpe ntp nut opentelemetry openvpn ovirt-imgaeo ovirt-storageconsole ovir
-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql proxysql prometheus prometheus-node-exporter pro
xy-dhcp ps2link ps3netvtr ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rood rpc-bind rquotad r
h rsyncd rtp salt-master samba samba-client samba-dc sane sip sipfs sip smtp smtp-submission smtps snmp snmp1s snmp2
s-trap snmptrap spidiroak-ldap sync spotify-sync sound sddp ssh stream-streaming svdrp svn syncthing syncthing-gui synt
hing-relay synergy syslog syslog-tls telnet telnetc telnetd tftp tile380 tinc tor-torcs transmission-client upnp-client vdsn v
server warpiator when-http when-https wireguard ws-discovery ws-discovery-client ws-discovery-client ws-discovery-vdm w
ssman wssans xdcmpp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier

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

[root@termimash ~]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp93
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:

[termimash@termimash ~]# systemctl restart firewallld
[termimash@termimash ~]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp93
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:

```

Добавьте службу vnc-server ещё раз, но на этот раз сделайте её постоянной, используя команду (рис. 2.1) - `firewall-cmd --add-service=vnc-server --permanent`. Проверьте наличие vnc-server в конфигурации: (рис. 2.1) - `firewall-cmd --list-all`. Перезагрузите конфигурацию firewalld и просмотрите конфигурацию времени выполнения: (рис. 2.1) - `firewall-cmd --reload` - `firewall-cmd --list-all`. Добавьте в конфигурацию межсетевого экрана порт 2022 протокола TCP: (рис. 2.1) - `firewall-cmd --add-port=2022/tcp --permanent`. Затем перезагрузите конфигурацию firewalld: (рис. 2.1) - `firewall-cmd --reload`. Проверьте, что порт добавлен в конфигурацию: (рис. 2.1) - `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@ermimash ~]# firewall-cmd --reload
success
[root@ermimash ~]# 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@ermimash ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@ermimash ~]# firewall-cmd --reload
success
[root@ermimash ~]# 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:

```

Рис. 2.1: Добавление конфигураций

2. Управление брандмауэром с помощью firewall-config Откройте терминал и под учётной записью своего пользователя запустите интерфейс GUI firewall-config: (рис. 2.3)

- firewall-config

Нажмите выпадающее меню рядом с параметром Configuration (рис. 2.2) Откройте раскрывающийся список и выберите Permanent. Это позволит сделать постоянными все изменения, которые вы вносите при конфигурировании Выберите зону public и отметьте службы http, https и ftp, чтобы включить их. Выберите вкладку Ports и на этой вкладке нажмите Add . Введите порт 2022 и протокол udp, нажмите ОК , чтобы добавить их в список. Закройте утилиту firewall-config

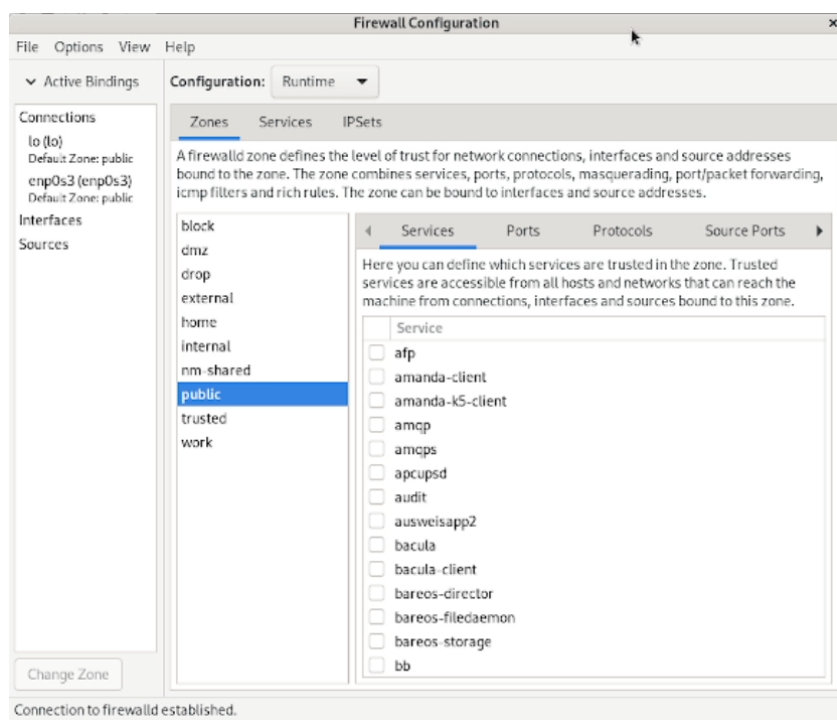


Рис. 2.2: Настройки брандмауэра

В окне терминала введите (рис. 2.3) - `firewall-cmd --list-all` Перегрузите конфигурацию `firewall-cmd`: (рис. 2.3) - `firewall-cmd --reload` и список доступных сервисов: - `firewall-cmd --list-all`

```
* Waiting in queue...
* Loading list of packages...
The following packages have to be installed:
dbus-x11:1:1.12.20-9.el9.x86_64      X11-requiring add-ons for D-BUS
firewall-config-1.3.4-15.el9_6.noarch Firewall configuration application
Proceed with changes? [N/y] y

* Waiting in queue...
* Waiting for authentication...

* Waiting in queue...
* Downloading packages...
* Requesting data...
* Testing changes...
* Installing packages...

[ermimash@ermimash ~]$
[ermimash@ermimash ~]$ 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:
[ermimash@ermimash ~]$ firewall-cmd --reload
success
[ermimash@ermimash ~]$ 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:
```

Рис. 2.3: Управление брандмауэром с помощью firewall-config

3. Самостоятельная работа (рис. 2.4) Создайте конфигурацию межсетевого экрана, которая позволяет получить доступ к следующим службам:

- telnet;
- imap;
- pop3;
- smtp. Сделайте это как в командной строке (для службы telnet), так и в графическом интерфейсе (для служб imap, pop3, smtp) Убедитесь, что конфигурация является постоянной и будет активирована после перезагрузки компьютера

```

[ermimash@ermimash ~]$ firewall-cmd --reload
success
[ermimash@ermimash ~]$ 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:
[ermimash@ermimash ~]$ su -
Password:
[root@ermimash ~]# firewall-cmd --add-service=telnet --permanent
success
[root@ermimash ~]# firewall-config
[root@ermimash ~]# firewall-cmd --reload
success
[root@ermimash ~]# 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:

```

Рис. 2.4: Самостоятельная работа

3 Контрольные вопросы

1. `sudo systemctl start firewalld`
2. `firewall-cmd -add-port/udp -permanent`
3. `firewall-cmd --list-all-zones`
4. `firewall-cmd --remove-service=vnc-server`
5. `firewall-cmd --reload`
6. `firewall-cmd --list-all --zone=`
7. `firewall-cmd --zone=public --change-interface=enol`
8. В зону по умолчанию (`firewall-cmd --get-default-zone`)

4 Выводы

Получены навыки настройки пакетного фильтра в Linux.