

Отчет по лабораторной работе 13

Генералов Даниил, НПИбд-01-21, 1032202280

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	13
5	Контрольные вопросы	14

Список иллюстраций

3.1	firewall-cmd	7
3.2	firewall-cmd	8
3.3	firewall-cmd	9
3.4	yum	10
3.5	firewall-cmd	11
3.6	firewall-cmd	11
3.7	firewall-cmd	12
5.1	systemctl	14
5.2	firewall-cmd	15

Список таблиц

1 Цель работы

В рамках этой лабораторной работы требуется выполнить операции по настройке фильтра пакетов в Linux.

2 Задание

1. Используя `firewall-cmd`: – определить текущую зону по умолчанию; – определить доступные для настройки зоны; – определить службы, включённые в текущую зону; – добавить сервер VNC в конфигурацию брандмауэра.
2. Используя `firewall-config`: – добавьте службы `http` и `ssh` в зону `public`; – добавьте порт 2022 протокола UDP в зону `public`; – добавьте службу `ftp`.
3. Выполните задание для самостоятельной работы (раздел 13.5).

3 Выполнение лабораторной работы

Сначала я использовал `firewall-cmd`, чтобы определить текущую зону, доступные для настройки зоны и службы, включённые в текущую зону.

```
Rocky Linux 9.1 (Blue Onyx)
Kernel 5.14.0-162.6.1.el9_1.0.1.x86_64 on an x86_64

dmgeneralov login: [ 39.150045] systemd-journal(653): File /var/log/journal/cdffcd2cb9b4b04b7fec2821691b511/user-1001.journal corrupted or uncleanly shut down, renaming and replacing.
root
Password:
Last login: Sat Dec 17 14:52:25 on tty1
[root@dmgeneralov ~]# firewall-cmd --get-default-zone
public
[root@dmgeneralov ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@dmgeneralov ~]# firewall-cmd --get-services
DH-Satellite-6 DH-Satellite-6-capsule atp amanda-client amanda-k5-client amqp amqps apcupsd audit bacula bacula-client bb bpp bitcoin bitcoin-rpc bitcoin-testnet
stry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ltd freeipa-replication fr
eeipa-trust ftp galera ganglia-client ganglia-master git grafana gre high-availability http http3 https imap imaps ipp ipp-client ipsec irc ircs iscsi-target is
ns jellyfin jenkins kadmin kdeconnect kerberos kibana klogon kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-controller-manager kube-schedu
ler kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmr llmr-tcp llmr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt
mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pncd pmproxy
pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh
rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroak-lansync spotify-sync squid ssdp ssh ste
am-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upmp-client vdsd vnc-ser
ver wbem-http wbm-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsman5 xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-s
erver zabbix-agent zabbix-server zerotier
[root@dmgeneralov ~]# firewall-cmd --list-services
cockpit dhcpv6-client ssh
[root@dmgeneralov ~]#
```

Рис. 3.1: firewall-cmd

Поскольку активна зона `public`, то вывод команды `firewall-cmd --list-all` не меняется от добавления ключа `--zone=public`.

```

[root@dmgeneralov ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp1s0
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@dmgeneralov ~]# firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp1s0
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@dmgeneralov ~]#

```

Рис. 3.2: firewall-cmd

Можно добавить сервер VNC в конфигурацию брандмауэра, используя команду `firewall-cmd --add-service=vnc-server` – флаг `--permanent` сделает, чтобы это изменение было применено в файлы конфигурации. После этого нужно перезагрузить файлы конфигурации брандмауэра командой `firewall-cmd --reload`. Помимо служб, можно добавлять порты, например `--add-port=2022/tcp`.


```

target: default
icmp-block-inversion: no
interfaces: enp1s0
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
[root@dmgeneralov ~]# firewall-cmd --reload
success
[root@dmgeneralov ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp1s0
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@dmgeneralov ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@dmgeneralov ~]# firewall-cmd --reload
success
[root@dmgeneralov ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp1s0
  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@dmgeneralov ~]# _

```

Рис. 3.3: firewall-cmd

Следующую часть работы предлагается сделать с помощью `firewall-config`, графической утилиты для настройки брандмауэра. У меня на виртуальной ма-

шине не установлен графический интерфейс, и все зависимости для него не установлены.

pipewire-libs	x86_64	0.3.47-2.e19	appstream	1.5 M
pixman	x86_64	0.40.0-5.e19	appstream	269 k
polkit-libs	x86_64	0.117-10.e19_0	baseos	8.2 M
polkit-pkla-compat	x86_64	0.1-21.e19	baseos	44 k
poppler	x86_64	21.01.0-13.e19	appstream	1.1 M
poppler-data	noarch	0.4.9-9.e19	appstream	1.8 M
poppler-glib	x86_64	21.01.0-13.e19	appstream	153 k
pulseaudio-libs	x86_64	15.0-2.e19	appstream	666 k
pulseaudio-utils	x86_64	15.0-2.e19	appstream	72 k
python3-cairo	x86_64	1.20.1-1.e19	appstream	91 k
python3-gobject	x86_64	3.40.1-6.e19	appstream	16 k
rtkit	x86_64	0.11-28.e19	appstream	55 k
shared-mime-info	x86_64	2.1-4.e19	baseos	373 k
sound-theme-freedesktop	noarch	0.8-17.e19	appstream	377 k
totem-pl-parser	x86_64	3.26.6-2.e19	appstream	138 k
tracker	x86_64	3.1.2-2.e19	appstream	539 k
upower	x86_64	0.99.13-2.e19	appstream	165 k
vulkan-loader	x86_64	1.3.224.0-2.e19	appstream	139 k
webkit2gtk3-jsc	x86_64	2.36.7-1.e19	appstream	6.3 M
webkit-audio-processing	x86_64	0.3.1-8.e19	appstream	304 k
wireplumber	x86_64	0.4.0-1.e19	appstream	73 k
wireplumber-libs	x86_64	0.4.0-1.e19	appstream	316 k
xdg-dbus-proxy	x86_64	0.1.3-1.e19	appstream	41 k
xdg-desktop-portal	x86_64	1.12.4-1.e19	appstream	366 k
xkeyboard-config	noarch	2.33-2.e19	appstream	779 k
xsl-common	noarch	0.6.3-58.e19	appstream	31 k
Installing weak dependencies:				
abattis-cantarell-fonts	noarch	0.301-4.e19	appstream	364 k
adobe-source-code-pro-fonts	noarch	2.030.1.050-12.e19.1	appstream	831 k
dconf	x86_64	0.40.0-6.e19	appstream	187 k
exiv2	x86_64	0.27.5-2.e19	appstream	975 k
flatpak	x86_64	1.12.7-2.e19	appstream	1.7 M
libcanberra-gtk3	x86_64	0.30-26.e19	appstream	31 k
libproxy-webkitgtk4	x86_64	0.4.15-35.e19	appstream	21 k
p11-kit-server	x86_64	0.24.1-2.e19	appstream	194 k
pipewire	x86_64	0.3.47-2.e19	appstream	35 k
pipewire-alsa	x86_64	0.3.47-2.e19	appstream	58 k
pipewire-jack-audio-connection-kit	x86_64	0.3.47-2.e19	appstream	138 k
pipewire-pulseaudio	x86_64	0.3.47-2.e19	appstream	23 k
polkit	x86_64	0.117-10.e19_0	baseos	146 k
tracker-miners	x86_64	3.1.2-1.e19	appstream	880 k
xdg-desktop-portal-gtk	x86_64	1.12.0-3.e19	appstream	138 k
Transaction Summary				
=====				
Install 170 Packages				
Total download size: 188 M				
Installed size: 359 M				
Is this ok [y/N]:				

Рис. 3.4: yum

К счастью, аналогичные действия можно выполнить с помощью `firewall-cmd`: чтобы добавить службы `http`, `ssh` и `ftp` в зону `public`, нужно выполнить команду `firewall-cmd --add-service=http --add-service=ssh --add-service=ftp --zone=public --permanent`, и чтобы добавить порт 2022 протокола UDP в зону `public`, нужно выполнить команду `firewall-cmd --add-port=2022/udp --zone=public --permanent`.

```

[root@dmgeneralov ~]# firewall-cmd --add-service=http --add-service=ssh --add-service=ftp --zone=public --permanent
Warning: ALREADY_ENABLED: ssh
success
[root@dmgeneralov ~]# firewall-cmd --add-port=2022/udp --zone=public --permanent
success
[root@dmgeneralov ~]# firewall-cmd --reload
success
[root@dmgeneralov ~]# firewall-cmd --show-all
usage: see firewall-cmd man page
firewall-cmd: error: unrecognized arguments: --show-all
[root@dmgeneralov ~]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp1s0
sources:
services: cockpit dhcpv6-client ftp http ssh vnc-server
ports: 2022/tcp 2022/udp
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
[root@dmgeneralov ~]# _

```

Рис. 3.5: firewall-cmd

Наконец, нужно сделать то же самое, чтобы включить службы telnet, imap, pop3 и smtp в зону public. Как раньше, те шаги, которые требуют графического интерфейса, я пропускаю.

```

[root@dmgeneralov ~]# firewall-cmd --add-service=telnet --add-service=imap --add-service=pop3 --add-service=smtp --zone=public --permanent
success
[root@dmgeneralov ~]# firewall-cmd --reload
success
[root@dmgeneralov ~]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp1s0
sources:
services: cockpit dhcpv6-client ftp http 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@dmgeneralov ~]#

```

Рис. 3.6: firewall-cmd

Перезагрузив систему, можно увидеть, что все эти изменения применены.

```
Rocky Linux 9.1 (Blue Onyx)
Kernel 5.14.0-162.6.1.el9_1.0.1.x86_64 on an x86_64

dmgeneralov login: root
Password:
Last login: Sat Dec 24 12:48:26 on tty1
[root@dmgeneralov ~]# uptime
13:06:48 up 0 min, 1 user, load average: 0.20, 0.05, 0.02
[root@dmgeneralov ~]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp1s0
sources:
services: cockpit dhcpv6-client ftp http 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@dmgeneralov ~]#
```

Рис. 3.7: firewall-cmd

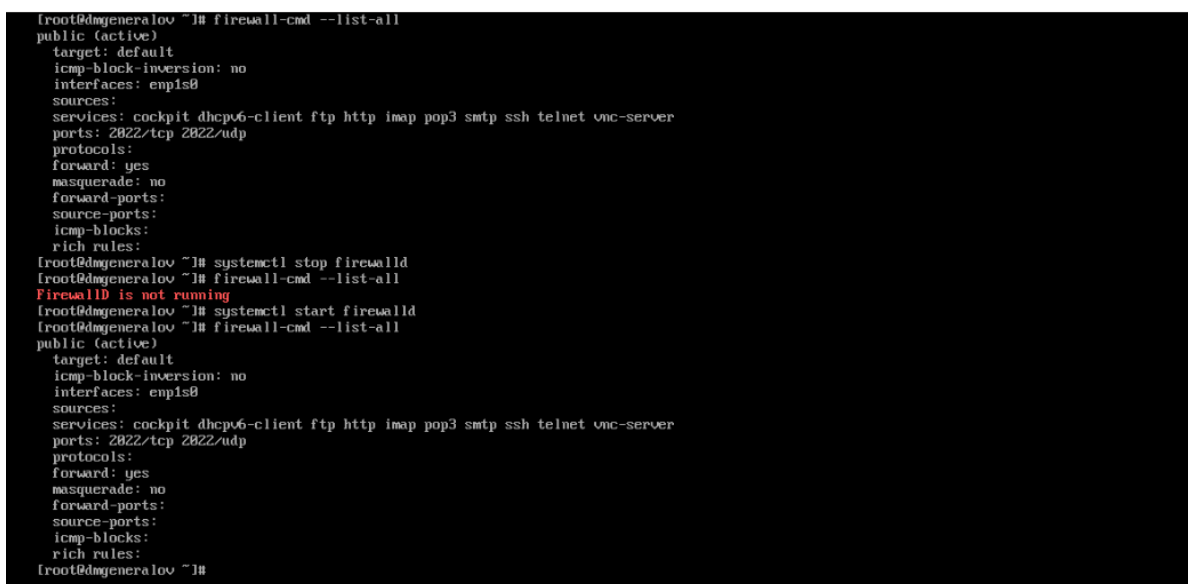
4 Выводы

Я получил опыт работы с фильтром пакетов в Linux.

5 Контрольные вопросы

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

`firewall-config` и `firewall-cmd` — это два разных инструмента для настройки службы `firewalld`.



```
[root@dmgeneralov ~]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp1s8
sources:
services: cockpit dhcpv6-client ftp http imap pop3 smtp ssh telnet vnc-server
ports: 2822/tcp 2822/udp
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
[root@dmgeneralov ~]# systemctl stop firewalld
[root@dmgeneralov ~]# firewall-cmd --list-all
Firewalld is not running
[root@dmgeneralov ~]# systemctl start firewalld
[root@dmgeneralov ~]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp1s8
sources:
services: cockpit dhcpv6-client ftp http imap pop3 smtp ssh telnet vnc-server
ports: 2822/tcp 2822/udp
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
[root@dmgeneralov ~]#
```

Рис. 5.1: `systemctl`

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

```
firewall-cmd --add-port=2355/udp --permanent
```

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

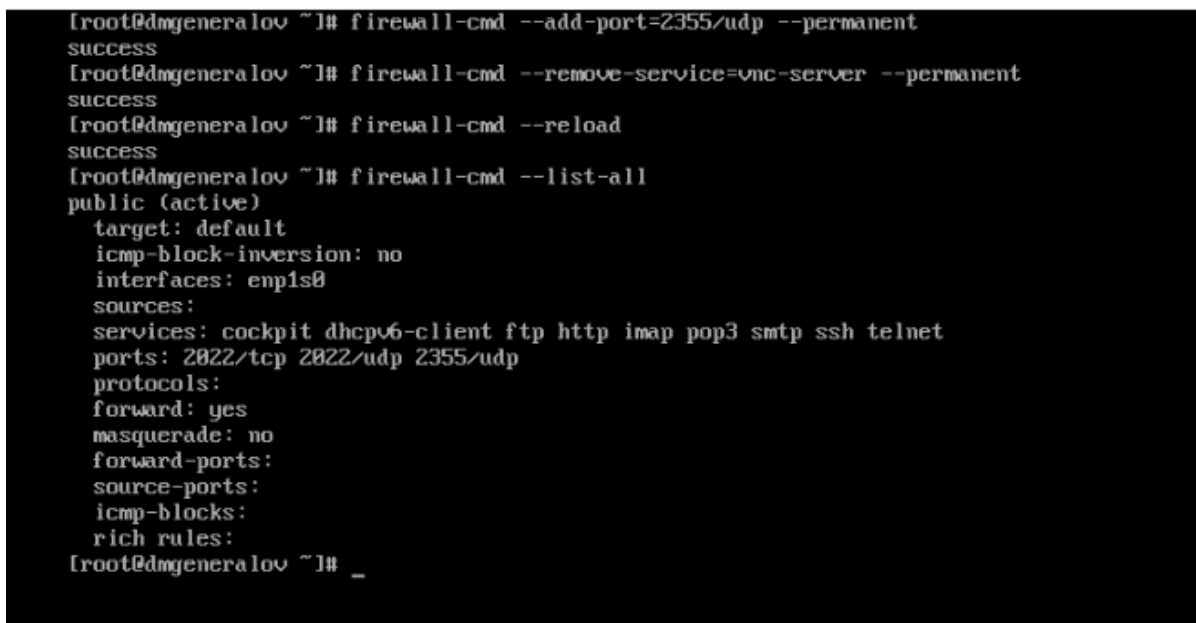
```
firewall-cmd --list-all
```

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

```
firewall-cmd --remove-service=vnc-server --permanent
```

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

```
firewall-cmd --reload
```



```
[root@dmgeneralov ~]# firewall-cmd --add-port=2355/udp --permanent
success
[root@dmgeneralov ~]# firewall-cmd --remove-service=vnc-server --permanent
success
[root@dmgeneralov ~]# firewall-cmd --reload
success
[root@dmgeneralov ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp1s8
  sources:
  services: cockpit dhcpv6-client ftp http imap pop3 smtp ssh telnet
  ports: 2022/tcp 2022/udp 2355/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@dmgeneralov ~]# _
```

Рис. 5.2: firewall-cmd

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

Опция --runtime-to-permanent позволяет записать текущую активную конфигурацию в файлы. Обычно настраивают firewalld так: сначала добавляют правила без опции --permanent, проверяют, что они работают, а затем добавляют опцию --runtime-to-permanent.

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

```
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?

В текущую зону по умолчанию.