

Фильтр пакетов

Отчет

Казначеев Сергей Ильич

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Самостоятельная работа	14
5	Контрольные вопросы	16
6	Выводы	18

Список иллюстраций

3.1	1	7
3.2	2	7
3.3	3	7
3.4	4	7
3.5	5	8
3.6	6	8
3.7	7	8
3.8	8	9
3.9	9	9
3.10	10	9
3.11	11	10
3.12	12	10
3.13	13	10
3.14	14	11
3.15	15	11
3.16	16	12
3.17	17	12
3.18	18	12
3.19	19	13
3.20	20	13
4.1	21	14
4.2	22	14
4.3	23	14
4.4	24	14
4.5	25	15

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра 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

Перейдем в супер пользователя

```
[sikaznacheev@localhost ~]$ su -  
Пароль:
```

Рис. 3.1: 1

После чего определим текущую зону

```
[root@localhost ~]# firewall-cmd --get-default-zone  
public
```

Рис. 3.2: 2

Определим доступные зоны

```
[root@localhost ~]# firewall-cmd --get-zones  
block dmz drop external home internal nm-shared public trusted work
```

Рис. 3.3: 3

Затем посмотрим службы доступные на нашем компьютере

```
[root@localhost ~]# firewall-cmd --get-services  
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacula-cl  
ient bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorren  
t-bsd 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-clie  
nt etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera  
ganglia-client ganglia-master git ppsd grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ips  
irc ircs iscsi-target isns jenkins kadm5 kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver ku  
be-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-n  
etwork llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidna mongodb mosh mountr mqtqt mqtqt-tls ms-w  
at mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmap-0183 nrpe ntp nut opentelemetry openvpn ovirt-inag  
eo ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometh  
eus-node-exporter proxy-dhcp ps2link ps3netrvr ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rootd rpc-b  
ind quoted rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmpdis  
smptls-trap snmptrap spideroak-lansync spotify-sync squid ssh steam-streaming svdrp svn syncthing syncthing-gui syncthin  
g-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsim vnc-server w  
arpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp  
xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
```

Рис. 3.4: 4

Определим доступные службы в текущей зоне

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

Рис. 3.5: 5

После чего сравним вывод информации при использовании двух команд первая команда `firewall-cmd --list-all`, вторая `firewall-cmd --list-all --zone=public`

```
[root@localhost ~]# 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@localhost ~]# firewall-cmd --list-all --zone=public
bash: firewall-cmd: команда не найдена...
[root@localhost ~]# firewall-cmd --list-all --zone=public
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. 3.6: 6

Далее добавим сервер VNC в конфигурацию брандмауэра

```
[root@localhost ~]# firewall-cmd --add-service=vnc-server
success
```

Рис. 3.7: 7

И проверим добавился или нет

```
[root@localhost ~]# 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:
```

Рис. 3.8: 8

После чего перезапустим службу firewalld

```
[root@localhost ~]# systemctl restart firewalld
```

Рис. 3.9: 9

Затем проверим есть ли vnc-server в конфигурации и мы обнаружим, что vnc-server больше не указан это из-за того что не был постоянным

```
[root@localhost ~]# 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. 3.10: 10

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

```
[root@localhost ~]# firewall-cmd --add-service=vnc-server --permanent  
success
```

Рис. 3.11: 11

После чего проверим наличие vnc-server в конфигурации

```
[root@localhost ~]# 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. 3.12: 12

Теперь проверим перезагрузив конфигурацию firewalld

```
[root@localhost ~]# firewall-cmd --reload  
success  
[root@localhost ~]# 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:
```

Рис. 3.13: 13

Добавим в конфигурацию межсетевого экрана порт 2022 протокола TCP, после чего перезагрузим конфигурацию firewalld и проверим что порт добавился в конфигурацию

```
[root@localhost ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# 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. 3.14: 14

После чего откроем терминал и под учетной записью пользователя запустим интерфейс GUI firewall-config:

```
[sikaznacheev@localhost ~]$ firewall-config
```

Рис. 3.15: 15

Далее рядом с параметром Configuration откроем раскрывающийся список и выберем Permanent, после чего выберем зону public и отметим службы http, https и ftp

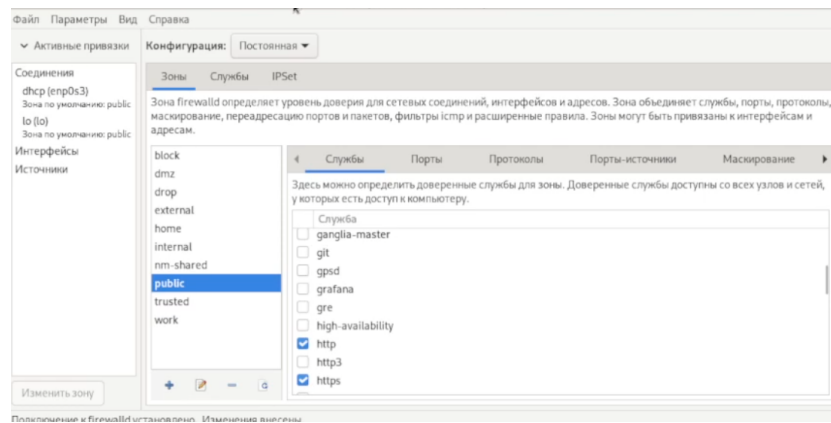


Рис. 3.16: 16



Рис. 3.17: 17

Полче чего выберем вкладку Ports и добавим порт 2022 udp

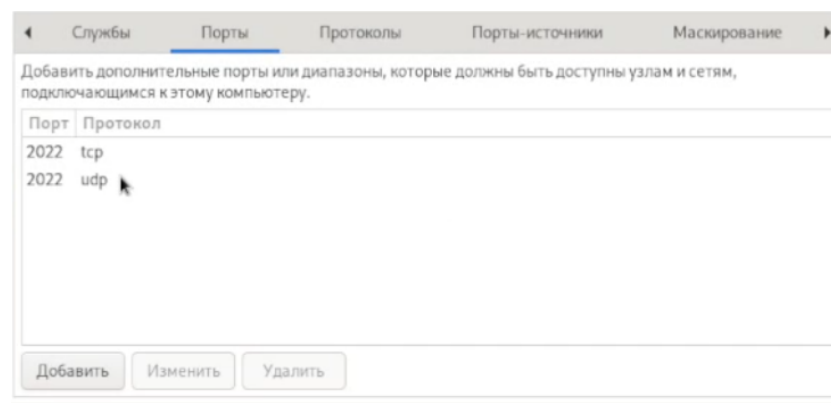


Рис. 3.18: 18

И проверим все изменения которые мы только что внесли

```
[sikaznacheev@localhost ~]$ 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. 3.19: 19

Перезапустим конфигурацию firewall-cmd для того, чтобы изменения вступили в силу и проверим это

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

Рис. 3.20: 20

4 Самостоятельная работа

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

```
[sikaznacheev@localhost ~]$ firewall-cmd --add-service=telnet --permanent  
success
```

Рис. 4.1: 21

Добавляем imap, pop3, smtp

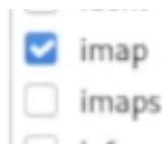


Рис. 4.2: 22

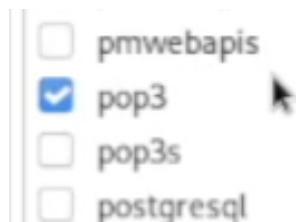


Рис. 4.3: 23



Рис. 4.4: 24

И проверяем, что конфигурация является постоянной и будет активирована после перезагрузки компьютера

```
isikaznacheev@localhost ~]$ 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:
```

Рис. 4.5: 25

5 Контрольные вопросы

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

Ответ - `firewall` должна быть запущена

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

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

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

Ответ - `firewall-cmd --list-all-zones`

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

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

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

Ответ - `firewall-cmd --reload`

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

Ответ - firewall-cmd --list-all

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

Ответ - firewall-cmd --zone=public --add-interface=eno1

8. Если добавить новый интерфейс в конфигурацию брандмауэра, пока не указана зона, в какую зону он будет добавлен?

Ответ - интерфейс попадет в зону по умолчанию (public)

6 Выводы

В ходе выполнения лабораторной работы я получил навыки настройки пакетного фильтра в Linux.