

Лабораторная работа №13

Отчет

Зубов Иван Александрович

Содержание

1 Цель работы	5
2 Задание	6
3 Выполнение лабораторной работы	7
3.1 Управление брандмауэром с помощью firewall-cmd	7
3.2 Управление брандмауэром с помощью firewall-config	9
3.3 Самостоятельная работа	11
4 Контрольные вопросы	13
5 Вывод	14

Список иллюстраций

3.1 Смотрим информацию	7
3.2 Сервер VNC	8
3.3 Постоянный сервер VNC	8
3.4 Конфигурацию межсетевого экрана	9
3.5 Интерфейс GUI firewall-config	9
3.6 Службы http, https и ftp	10
3.7 Порт 2022	10
3.8 Проверка изменений	11
3.9 Самостоятельная работа (Telnet)	11
3.10 Самостоятельная работа	12
3.11 Самостоятельная работа	12

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

3 Выполнение лабораторной работы

3.1 Управление брандмауэром с помощью firewall-cmd

Получаем полномочия администратора. Определяем текущую зону по умолчанию Определяем доступные зоны Посмотрим службы, доступные на нашем компьютере Определяем доступные службы в текущей зоне

```
[iazubov@iazubov ~]$ su -
Пароль:
[root@iazubov ~]# firewall-cmd --get-default-zone
public
[root@iazubov ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@iazubov ~]# 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-testnet bitcoin-test
tnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb
ctdb dds dds-multicast dds-unicast dhcp dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dro
pbox-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 gssd grafana greti high-availability htt
p http3 https ident imap imaps lpd ipp ipp-client ipsec irc ircs iscsi-target jenkins jenkins-kademot kerbero
s kibana klogin kpasswrd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-contr
oller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker k
ubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp
llmnr-udp managereside matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd n
ebula netbios-ns netdata-dashboard nfs nfss3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imagio ovirt-storagec
onsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 postgresql privoxy prometheus prometheus-node
-exporter proxy-dhcp ps2link ps3netsrv pptp puppetmaster quassel radius rdp redis redis-sentinel rootd rpc-b
ind rquotad rsh rsyncd rtspsalt-master samba samba-client samba-dc sane sip sipx sntp smtp smtp-submission smt
snp snmp snmptrap snmptrap_spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing sync
thing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client up
np-client vdsm vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp
ws-discovery-udp wsman wsman xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
[root@iazubov ~]# firewall-cmd --list-services
cockpit dhcpcv6-client ssh
[root@iazubov ~]# 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@iazubov ~]# firewall-cmd --list-all --zone=public
```

Рис. 3.1: Смотрим информацию

Добавим сервер VNC в конфигурацию брандмауэра командой `firewall-cmd –add-service=vnc-server` Проверим добавили или нет и перезапустим службу

```
[root@iazubov ~]# 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@iazubov ~]# systemctl restart firewalld
[root@iazubov ~]# 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:
```

Рис. 3.2: Сервер VNC

Добавим постоянную службу vnc-server Проверим наличие vnc-server в конфигурации Перезагрузим конфигурацию firewalld и просмотрим конфигурацию времени выполнения

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

Рис. 3.3: Постоянный сервер VNC

Добавьте в конфигурацию межсетевого экрана порт 2022 протокола TCP Перезагрузим конфигурацию firewalld и сделаем проверку

```
[root@iazubov ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@iazubov ~]# firewall-cmd --reload
success
[root@iazubov ~]# 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. 3.4: Конфигурацию межсетевого экрана

3.2 Управление брандмауэром с помощью

firewall-config

Запустим интерфейс GUI firewall-config командой firewall-config

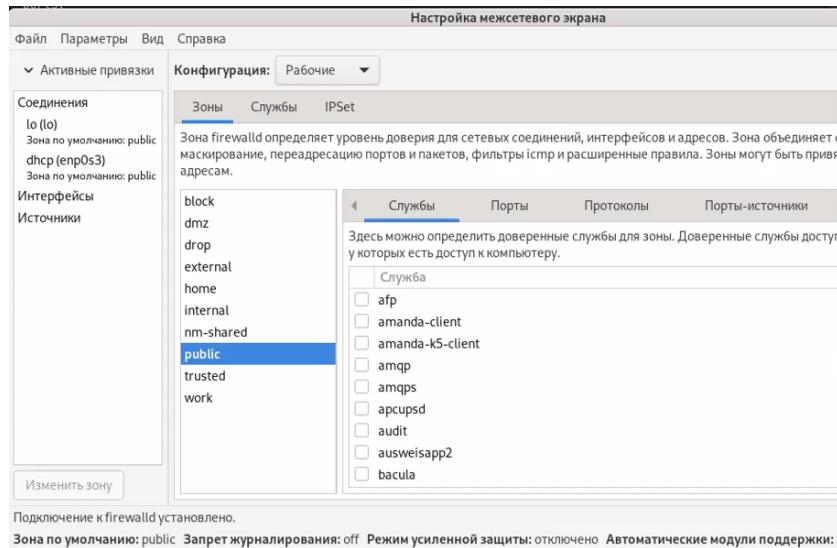


Рис. 3.5: Интерфейс GUI firewall-config

Выберем конфигурацию “Постоянная”. Затем выберем зону public и отметим службы http, https и ftp, чтобы включить их

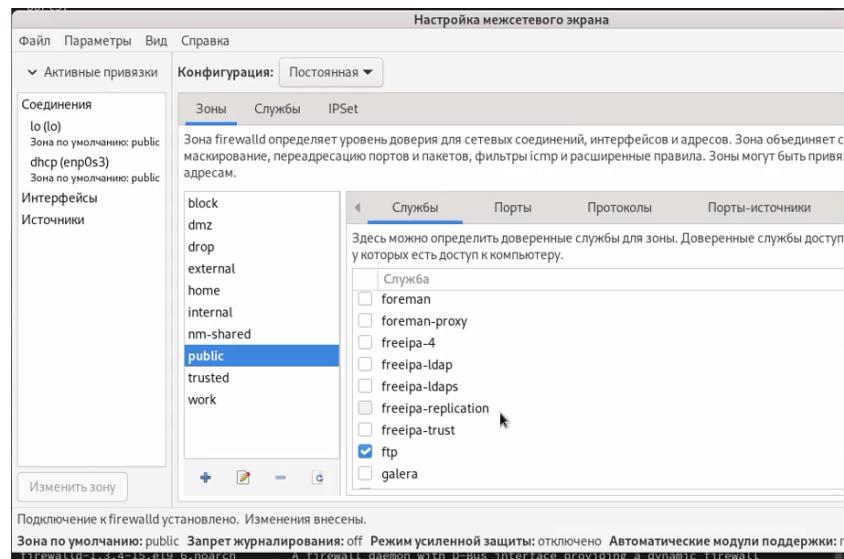


Рис. 3.6: Службы http, https и ftp

Выберем вкладку Ports и на этой вкладке нажмите Add . Вводим порт 2022 и протокол udp

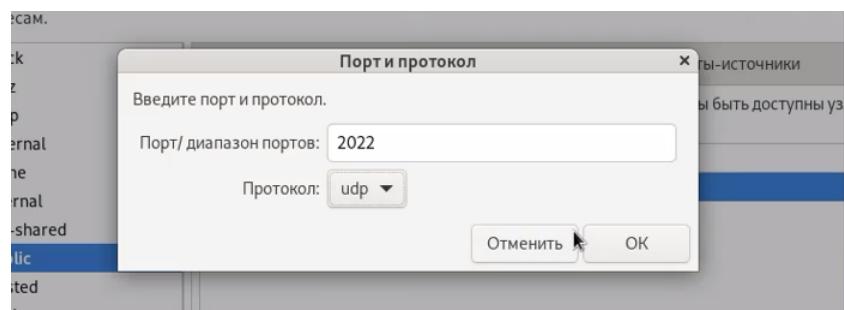


Рис. 3.7: Порт 2022

Вводя команду `firewall-cmd --list-all`, мы увидим что изменения, которые мы только что внесли, ещё не вступили в силу. Это связано с тем, что мы настроили их как постоянные изменения, а не как изменения времени выполнения. Поэтому дальше перезагружаем конфигурацию и проверяем, что изменения были применены

```
[root@iazubov ~]# 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@iazubov ~]# firewall-cmd --reload
success
[root@iazubov ~]# 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. 3.8: Проверка изменений

3.3 Самостоятельная работа

Через командную строку создаем конфигурацию межсетевого экрана, которая позволяет получить доступ к службе telnet

```
rich rules:
[root@iazubov ~]# firewall-cmd --add-service=telnet --permanent
success
```

Рис. 3.9: Самостоятельная работа (Telnet)

Выберем конфигурацию “Постоянная”. Затем выберем зону public и отметку службы imap, pop3 и smtp, чтобы включить их

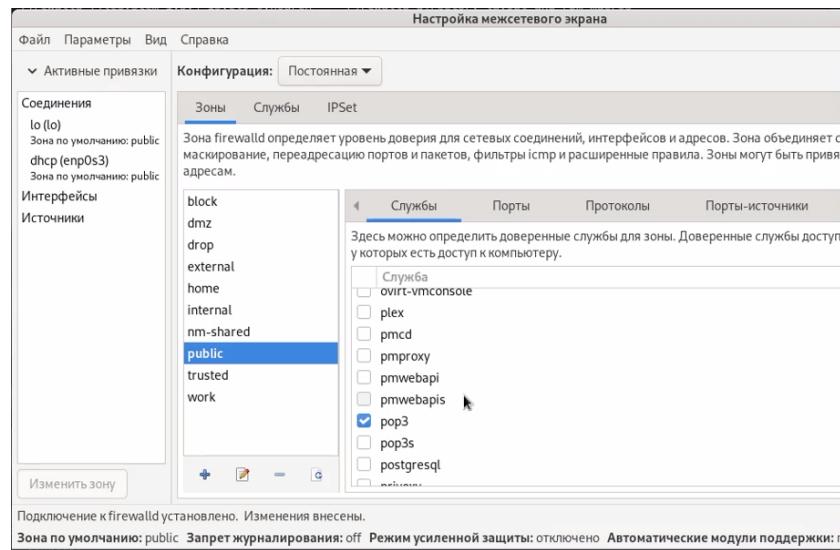


Рис. 3.10: Самостоятельная работа

Перезагружаем службу и смотрим как мы их добавили

```
[root@iazubov ~]# firewall-cmd --reload
success
[root@iazubov ~]# 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: 2222/tcp 2222/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Рис. 3.11: Самостоятельная работа

4 Контрольные вопросы

1. Какая служба должна быть запущена перед началом работы с менеджером конфигурации брандмауэра firewall-config? firewalld
2. Какая команда позволяет добавить UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию? firewall-cmd –add-port=2355/udp
3. Какая команда позволяет показать всю конфигурацию брандмауэра во всех зонах? firewall-cmd –list-all-zones
4. Какая команда позволяет удалить службу vnc-server из текущей конфигурации брандмауэра? firewall-cmd –remove-service=vnc-server
5. Какая команда firewall-cmd позволяет активировать новую конфигурацию, добавленную опцией –permanent? firewall-cmd –reload
6. Какой параметр firewall-cmd позволяет проверить, что новая конфигурация была добавлена в текущую зону и теперь активна? –list-all
7. Какая команда позволяет добавить интерфейс eno1 в зону public? 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? В зону public

5 Вывод

Я получил навыки настройки пакетного фильтра в Linux.