Отчет по лабораторной работе №12

Отчет о выполнении лабораторной работы по управлению брандмауэром с помощью firewall-cmd

Лупупа Чилеше

Цель работ

Получить навыки настройки пакетного фильтра в Linux.

Целью этой лабораторной работы было понять и попрактиковаться в управлении брандмауэром Linux с помощью утилиты firewall-cmd. Это включало проверку конфигураций, изменение правил и понимание различий между динамическими и постоянными конфигурациями.

Выполнение лабораторной работы

Управление брандмауэром с помощью firewall-cmd

Получение административных привилегий:

- Command: `su -`
- Успешно переключился на пользователя root. Этот шаг обеспечил нам наличие необходимых разрешений для управления брандмауэром.

Определение зоны по умолчанию:

- Команда: firewall-cmd --get-default-zone
- Вывод: была отображена зона по умолчанию (например, «публичная»).
- На этом этапе проверялась зона, которую система использует для неуправляемых подключений.

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

Список доступных зон:

- Команда: firewall-cmd --get-zones
- Вывод: был отображен список зон (например, «блокировать dmz, удалить внешний дом, внутреннюю общедоступную доверенную работу»)
- Подтверждены зоны, доступные для настройки сетевых интерфейсов.

```
[root@chileshelupupa ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@chileshelupupa ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd au
dit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp b
itcoin 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 dd
s-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropb
ox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeip
a-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-maste
r 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 kpr
op 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-s
ecure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls light
ning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna
mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dash
board nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconso
le plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-no
de-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis
redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane s
ip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync sp
otify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay sy
nergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-cl
ient vdsm vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-clien
t ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-s
erver zabbix-agent zabbix-server zerotier
```

Просмотр доступных услуг:

- Команда: firewall-cmd --get-services
- Вывод: отобразился список предопределенных служб, которыми можно управлять с помощью брандмауэра.
- Это было важно для понимания спектра сервисов, поддерживаемых firewalld.

Листинговые услуги в текущей зоне:

- Команда: firewall-cmd --list-services
- Вывод: список активных служб в текущей зоне по умолчанию.
- Проверено, какие службы уже разрешены через брандмауэр.

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

Сравнение результатов команд --list-all:

- Команды: firewall-cmd --list-all и firewall-cmd --list-all --zone=public

- Вывод: обе команды отображали аналогичную информацию, показывая активные службы, порты и интерфейсы для «общедоступной» зоны.
- Это продемонстрировало, как просмотреть подробные сведения о конфигурациях брандмауэра для конкретных зон.

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

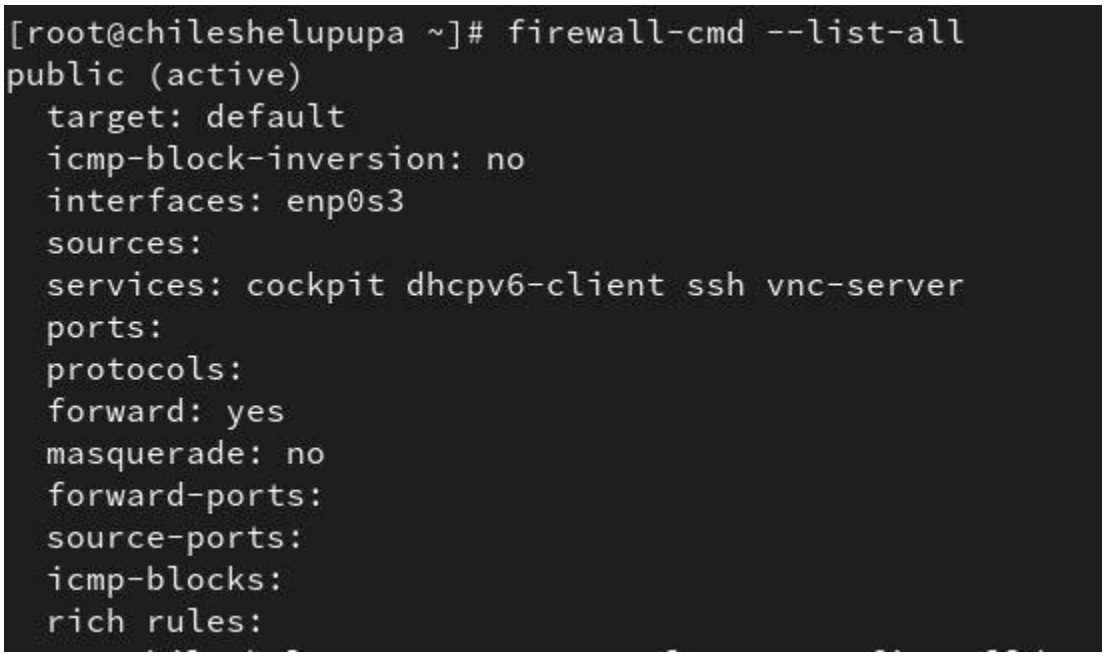
Добавление службы VNC-сервера:

- Команда: firewall-cmd --add-service=vnc-server
- Команда выполнена успешно. Служба vnc-сервера была добавлена в конфигурацию среды выполнения.

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

Проверка добавления VNC-сервера:

- Команда: firewall-cmd --list-all
- Вывод: подтверждено, что служба vnc-сервера указана в списке активных служб.



Перезапускаем firewalld:

- Команда: systemctl перезапустить firewalld
- Служба firewalld успешно перезапущена.
- Команда: firewall-cmd --list-all
- Вывод: служба vnc-сервера больше не отображается.

- Объяснение: Это произошло потому, что в конфигурацию среды выполнения было внесено предыдущее дополнение, которое сбрасывается при перезапуске службы.

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

Добавление VNC-сервера на постоянной основе:

- Команда: firewall-cmd --add-service=vnc-server --permanent
- Команда выполнена успешно, гарантируя сохранение службы vnc-сервера в постоянной конфигурации.

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

Проверка постоянного добавления:

- Команда: firewall-cmd --list-all
- Вывод: служба vnc-сервера не была сразу видна в конфигурации среды выполнения.

- Объяснение: Постоянные конфигурации не применяются автоматически к среде выполнения.

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

Перезагрузка конфигурации firewalld:

- Команды: firewall-cmd --reload и firewall-cmd --list-all
- Вывод: После перезагрузки в рантайм-конфигурации появился сервис vnc-сервера.
- Этот шаг подчеркнул необходимость перезагрузки firewalld, чтобы постоянные изменения вступили в силу.

Добавление TCP-порта 2022 в постоянную конфигурацию:

- Команда: firewall-cmd --add-port=2022/tcp --permanent
- Порт успешно добавлен в постоянную конфигурацию.

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

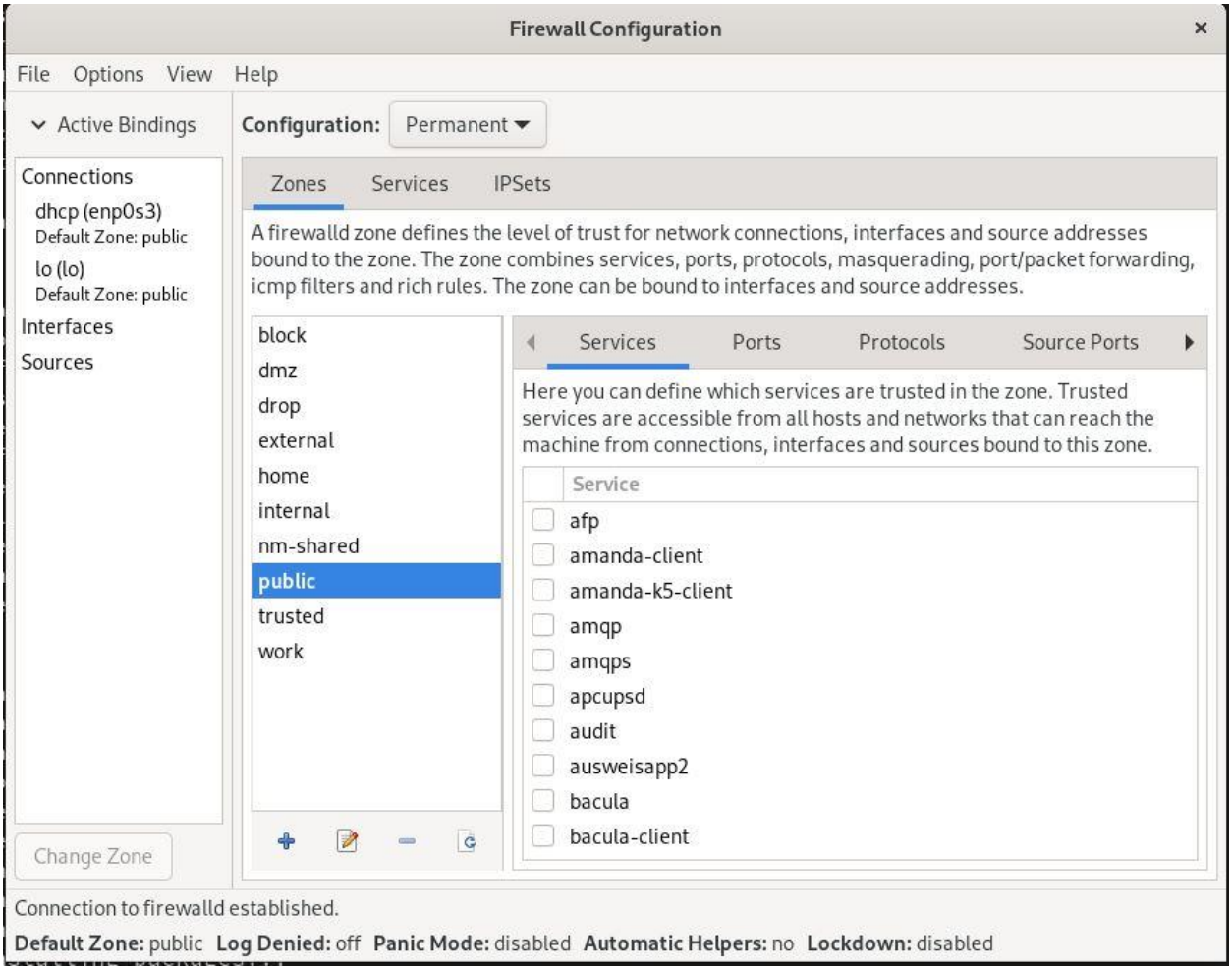
- Это подтвердило, что порт был правильно добавлен и активен как во время выполнения, так и в постоянной конфигурации.

Управление брандмауэром с помощью firewall-config

Запускаем конфигурацию брандмауэра

Команда: firewall-config

Объяснение: Команда firewall-config запускает графический интерфейс пользователя (GUI) для управления брандмауэром. Этот интерфейс упрощает процесс настройки. Если инструмент firewall-config не установлен, система предложит пользователю установить его. Для управления брандмауэром необходимы права администратора, поэтому пользователь должен указать пароль root.



Переключиться на постоянную конфигурацию

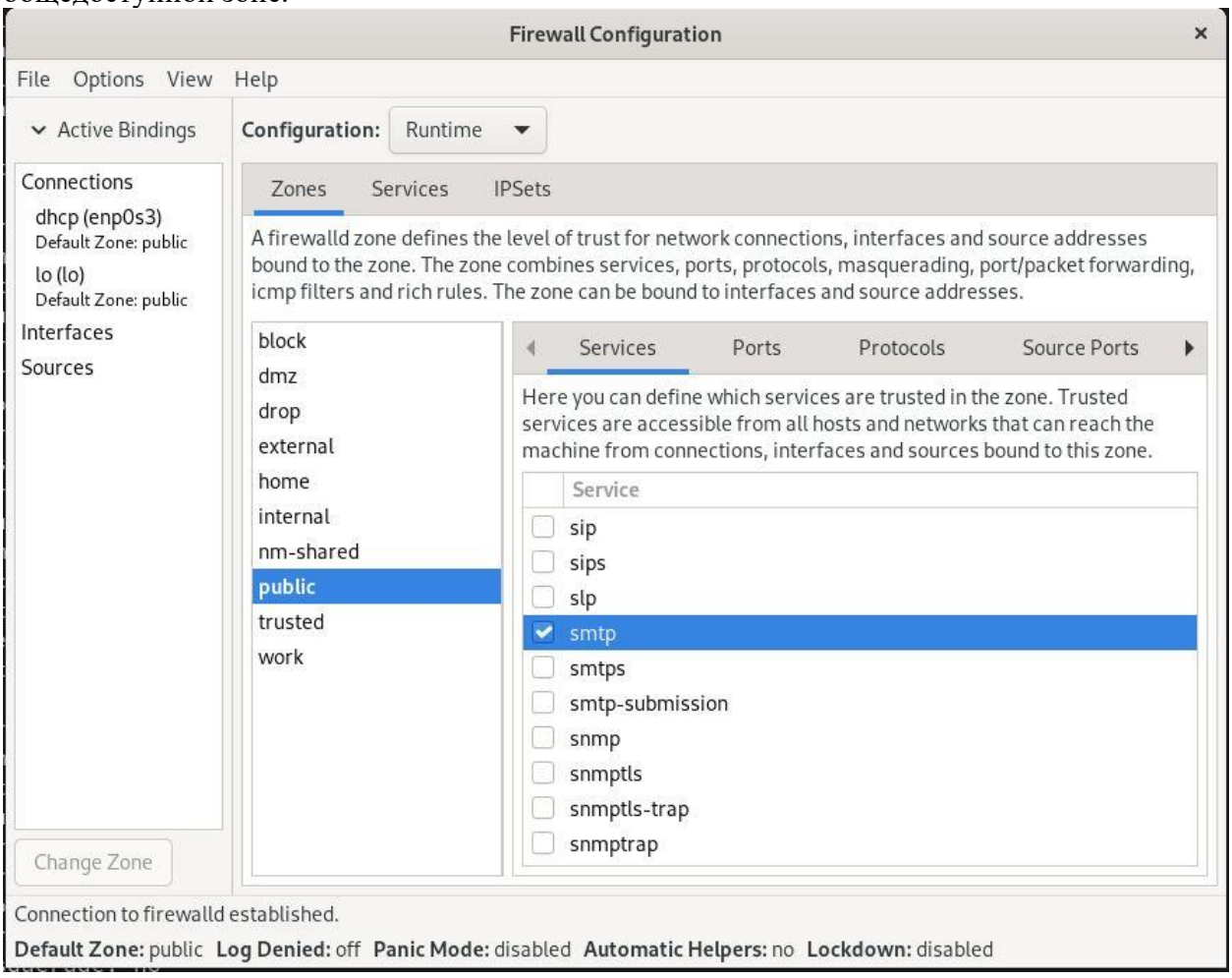
Действие: выберите «Постоянно» в раскрывающемся меню «Конфигурация».

Объяснение: Параметр конфигурации определяет, будут ли изменения применяться временно (во время выполнения) или постоянно. Если выбрать «Постоянно», любые внесенные изменения сохранятся даже после перезагрузки системы. Это гарантирует, что правила брандмауэра остаются согласованными и их не нужно повторно применять вручную.

Включите службы HTTP, HTTPS и FTP

Действие: В "общедоступной" зоне включите службы http, https и ftp.

Пояснение: Зоны в брандмауэре определяют уровень доверия для сетевых подключений. "Общедоступная" зона обычно используется для ненадежных сетей, таких как Интернет. Включив эти службы, брандмауэр разрешает входящие подключения для веб-трафика (HTTP/HTTPS) и передачи файлов (FTP) в общедоступной зоне.



Проверьте текущую конфигурацию брандмауэра

Команда: firewall-cmd --list-all

Пояснение: Эта команда отображает текущую конфигурацию брандмауэра, включая активные зоны, разрешенные службы, порты и протоколы. Поскольку изменения были внесены в постоянную конфигурацию, они еще не отражены в конфигурации среды выполнения.

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

Вывод

Заключение Лабораторная работа позволила получить практический опыт работы с firewall-cmd и лучше понять правила управления брандмауэром в системе Linux. Различие между конфигурациями во время выполнения и постоянными конфигурациями и их соответствующими вариантами использования является фундаментальной концепцией, обеспечивающей эффективное управление брандмауэром.

В этой лабораторной работе было продемонстрировано, как настроить брандмауэр с помощью графического интерфейса firewall-config. Благодаря включению определенных служб, добавлению портов и внесению изменений сетевая безопасность системы была адаптирована к конкретным требованиям. Различие между конфигурациями во время выполнения и постоянными конфигурациями обеспечивает гибкость и контроль над настройками брандмауэра.