Лабораторная работа №7

Расширенные настройки межсетевого экрана (FirewallD)

Элсаиед Адел

3 января 2026

Цели и ожидаемый результат

Цель работы

Получить навыки настройки межсетевого экрана в Linux: - переадресация (port forwarding); - маскарадинг (masquerading / NAT).

Выполнение работы

Создание пользовательской службы FirewallD (ssh-custom)

- скопирован файл `/usr/lib/firewalld/services/ssh.xml`;
- создан пользовательский файл `/etc/firewalld/services/ssh-custom.xml`;
- изучена структура XML-описания службы.

```
[root@server.elsaiedadel.net server]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.elsaiedadel.net server]# cd /etc/firewalld/services/
[root@server.elsaiedadel.net services]# cat ssh-custom.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines. It provides secure encry
pted communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You nee
d the openssh-server package installed for this option to be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server.elsaiedadel.net services]#
```

Рис. 1: Просмотр содержимого ssh-custom.xml

Редактирование ssh-custom: порт и описание

Изменения в `/etc/firewalld/services/ssh-custom.xml`: - порт SSH изменён со стандартного 22 на 2022; - описание уточнено как пользовательская модификация.

Рис. 2: Редактирование порта и описания службы

Активация службы ssh-custom

Служба добавлена в правила FirewallD:

```
[root@server.elsaiedadel.net services]#
[root@server.elsaiedadel.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.elsaiedadel.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.elsaiedadel.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.elsaiedadel.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server.elsaiedadel.net services]# firewall-cmd --reload
success
[root@server.elsaiedadel.net services]#
```

Рис. 3: Добавление ssh-custom и перезагрузка FirewallD

Перенаправление портов 2022 → 22 на сервере

Настройка позволяет: - принимать подключения на внешнем порту `2022`, - при этом обслуживать их локальной SSH-службой на `22`.

```
[root@server.elsaiedadel.net services]#
[root@server.elsaiedadel.net services]#
[root@server.elsaiedadel.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
[root@server.elsaiedadel.net services]#
```

Рис. 4: Настройка port forward 2022 -> 22

Проверка SSH-подключения с клиента

На `client` выполнено подключение по SSH к `server` через порт `2022`.

Рис. 5: Проверка SSH-подключения через порт 2022

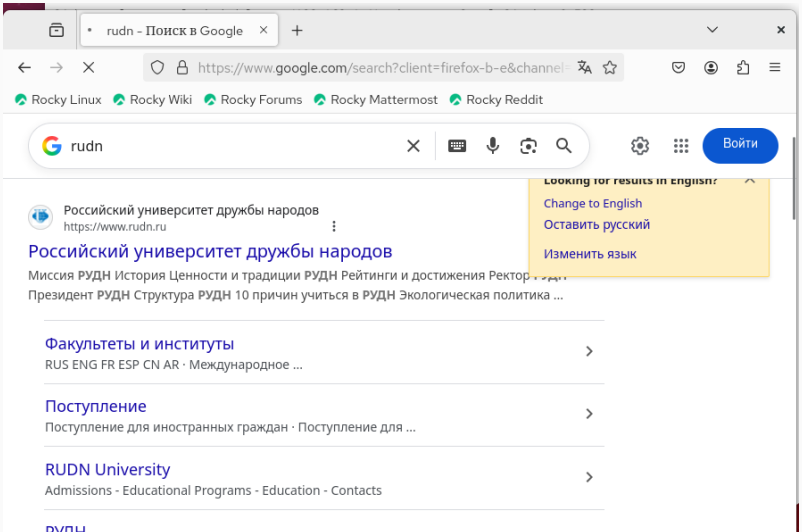
Включение IPv4 forwarding + masquerading (NAT)

- создан `/etc/sysctl.d/90-forward.conf` с `net.ipv4.ip_forward = 1`;
- применены sysctl-настройки;
- включён masquerading (NAT) для зоны `public`;
- перезагружен FirewallD для применения конфигурации.

```
net.ipv4.conf.lo.bc_forwarding = 0
net.ipv4.conf.lo.forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.ip_forward = 0
net.ipv4.ip_forward_update_priority = 1
net.ipv4.ip_forward_use_pmtu = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.all.mc_forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.default.mc_forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth0.mc_forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth1.mc_forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv6.conf.lo.mc_forwarding = 0
[root@server.elsaiedadel.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.elsaiedadel.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.elsaiedadel.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.elsaiedadel.net services]# firewall-cmd --reload
success
[root@server.elsaiedadel.net services]#
```

Проверка выхода клиента в Интернет

На `client` проверен доступ во внешнюю сеть.



Подготовка файлов в provision-структуре

Для воспроизводимости окружения подготовлены файлы в `/vagrant/provision/server/`: - `ssh-custom.xml` (служба FirewallD); - `90-forward.conf` (sysctl-настройка forwarding).

```
[root@server.elsaiedadel.net services]#
[root@server.elsaiedadel.net services]# cd /vagrant/provision/server/
[root@server.elsaiedadel.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server.elsaiedadel.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.elsaiedadel.net server]# cp -R /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc/firewalld/
services/
[root@server.elsaiedadel.net server]#
[root@server.elsaiedadel.net server]# cp -R /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d/
[root@server.elsaiedadel.net server]# touch firewall.sh
[root@server.elsaiedadel.net server]# chmod +x firewall
[root@server.elsaiedadel.net server]#
```

Рис. 8: Подготовка каталогов и копирование конфигураций

Скрипт firewall.sh для автоматической настройки

Vagrantfile | mysql.sh | firewall.sh

```
1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Copy configuration files"
4  cp -R /vagrant/provision/server/firewall/etc/* /etc
5  echo "Configure masquerading"
6  firewall-cmd --add-service=ssh-custom --permanent
7  firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22 --permanent
8  firewall-cmd --zone=public --add-masquerade --permanent
9  firewall-cmd --reload
10 restorecon -vR /etc
11
```

Рис. 9: Содержимое скрипта firewall.sh

Итоги

Выводы по работе

В ходе лабораторной работы: - создана пользовательская служба FirewallD для SSH с портом `2022`; - настроено перенаправление `2022 → 22` и подтверждено успешным SSH-подключением; - включены IPv4 forwarding и masquerading для маршрутизации трафика клиента; - подготовлена автоматизация через provisioning для повторяемого развёртывания.