# Отчёт по лабораторной работе 7

**Расширенные настройки межсетевого экрана**

Элсаиед Адел

# Содержание

# Список иллюстраций

# Список таблиц

# 1 Цель работы

Получить навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

# 2 Выполнение

## 2.1 Создание пользовательской службы firewalld

1. В операционной системе Rocky Linux на виртуальной машине **server** выполнено создание пользовательского описания службы FirewallD на основе стандартной службы SSH. Для этого системный файл `/usr/lib/firewalld/services/ssh.xml` был скопирован в каталог пользовательских служб `/etc/firewalld/services/` под именем `ssh-custom.xml`. Данный подход позволяет изменять параметры службы без вмешательства в системные файлы, которые могут быть перезаписаны при обновлениях.

2. Выполнен просмотр содержимого файла `/etc/firewalld/services/ssh-custom.xml`. Файл представляет собой XML-описание службы, используемое FirewallD для определения правил доступа. Принцип синтаксиса файла:

    - строка `<?xml version="1.0" encoding="utf-8"?>` задаёт версию XML и используемую кодировку;
    - элемент `<service>` является корневым контейнером описания службы;
    - элемент `<short>` задаёт краткое имя службы (идентификатор/название, отображаемое в списках);
    - элемент `<description>` содержит развернутое текстовое описание назначения службы;
    - элемент `<port .../>` задаёт параметры сетевого доступа: протокол (`protocol="tcp"`) и номер порта (`port="22"` либо другой);

- закрывающий тег `</service>` завершает описание 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. 2.1: Просмотр содержимого ssh-custom.xml

3. Файл `ssh-custom.xml` был открыт на редактирование. В описании службы был изменён порт SSH со стандартного 22 на 2022, а также скорректировано описание службы для указания, что это модифицированная (пользовательская) версия службы SSH.


Рис. 2.2: Редактирование порта и описания службы

4. Выполнен вывод списка активных служб FirewallD. На этом этапе пользовательская служба ещё не отображалась в активном списке, так как она не была загружена/активирована правилами межсетевого экрана.

5. Служба `ssh-custom` была добавлена в FirewallD и активирована. После временного добавления выполнено сохранение правила на постоянной основе и перезагрузка конфигурации межсетевого экрана, что обеспечивает сохранение настройки после перезапуска системы.

```
[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. 2.3: Добавление ssh-custom и перезагрузка FirewallD

## 2.2 Перенаправление портов

1. На сервере настроено перенаправление входящих TCP-соединений с порта 2022 на стандартный SSH-порт 22. Такая схема позволяет принимать подключения на нестандартный порт при сохранении работы службы SSH на стандартном порту внутри системы.

```
[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. 2.4: Настройка port forward 2022 -> 22

2. На клиентской машине выполнена проверка подключения к серверу по SSH через порт 2022. Подключение установлено успешно, что подтверждает корректность настройки перенаправления портов и доступность службы.

```
[elsaiedadel@client.elsaiedadel.net ~]$
[elsaiedadel@client.elsaiedadel.net ~]$ ssh -p 2022 elsaiedadel@server.elsaiedadel.net
The authenticity of host '[server.elsaiedadel.net]:2022 ([192.168.1.1]:2022)' can't be established.
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[server.elsaiedadel.net]:2022' (ED25519) to the list of known hosts.
elsaiedadel@server.elsaiedadel.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Jan  3 08:19:09 2026
[elsaiedadel@server.elsaiedadel.net ~]$
logout
Connection to server.elsaiedadel.net closed.
[elsaiedadel@client.elsaiedadel.net ~]$
```

Рис. 2.5: Проверка SSH-подключения через порт 2022

## 2.3 Настройка Port Forwarding и Masquerading

1. На сервере выполнена проверка параметров ядра, связанных с пересылкой пакетов (forwarding). По результатам проверки было установлено, что пересылка IPv4-пакетов отключена (значение `net.ipv4.ip_forward = 0`).

2. Для включения пересылки IPv4-пакетов создан конфигурационный файл `/etc/sysctl.d/90-forward.conf` с параметром `net.ipv4.ip_forward = 1`. После применения настроек параметр стал активным, что обеспечивает возможность маршрутизации пакетов через сервер.

3. Для обеспечения корректного выхода клиентов в сеть через сервер включён режим маскарадинга (NAT) для зоны `public`. После внесения изменений конфигурация FirewallD была перезагружена, что применило настройку на практике.

```
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]#
```

Рис. 2.6: Включение ip_forward и masquerading

4. На клиентской машине выполнена проверка выхода в Интернет, что подтверждает корректную настройку пересылки IPv4-пакетов и маскарадинга.

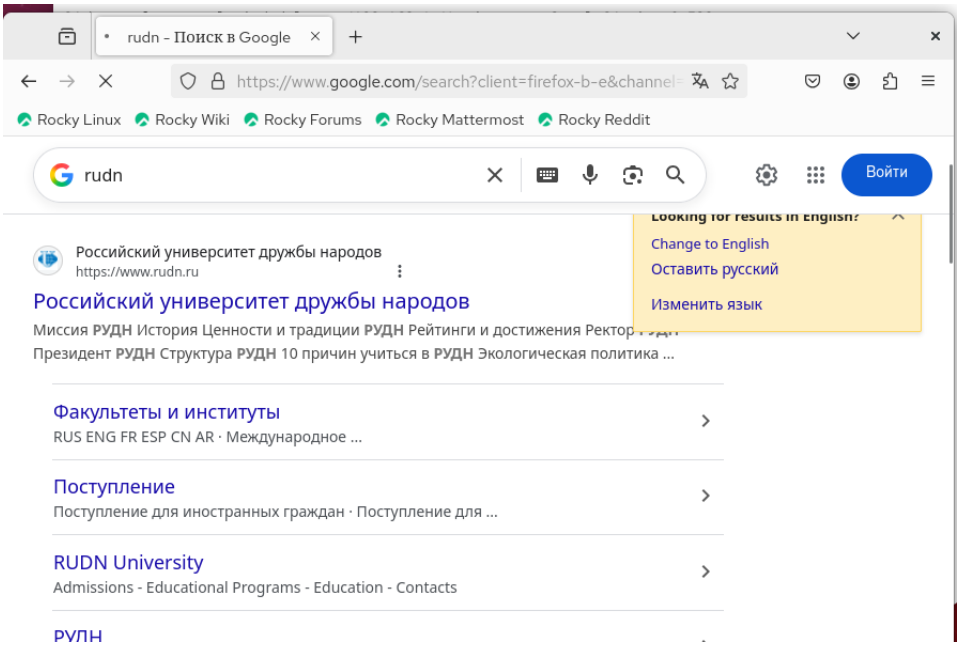


Рис. 2.7: Проверка выхода в Интернет на клиенте

## 2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. В каталоге `/vagrant/provision/server/` подготовлена структура каталогов для хранения конфигурационных файлов FirewallD и sysctl, после чего в соответствующие подкаталоги были скопированы:

   - файл пользовательской службы FirewallD `ssh-custom.xml`;
   - файл настройки пересылки пакетов `/etc/sysctl.d/90-forward.conf`. Это обеспечивает переносимость конфигурации и возможность автоматического применения при развёртывании виртуальной машины.

```
[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. 2.8: Подготовка каталогов и копирование конфигураций в provision

2. В каталоге `/vagrant/provision/server/` создан скрипт `firewall.sh` и назначены права на выполнение. Скрипт предназначен для автоматизации настройки: копирует конфигурационные файлы в систему, активирует службу `ssh-custom`, настраивает перенаправление порта 2022 на 22, включает маскарадинг, перезагружает FirewallD и восстанавливает контексты SELinux для каталога `/etc`.

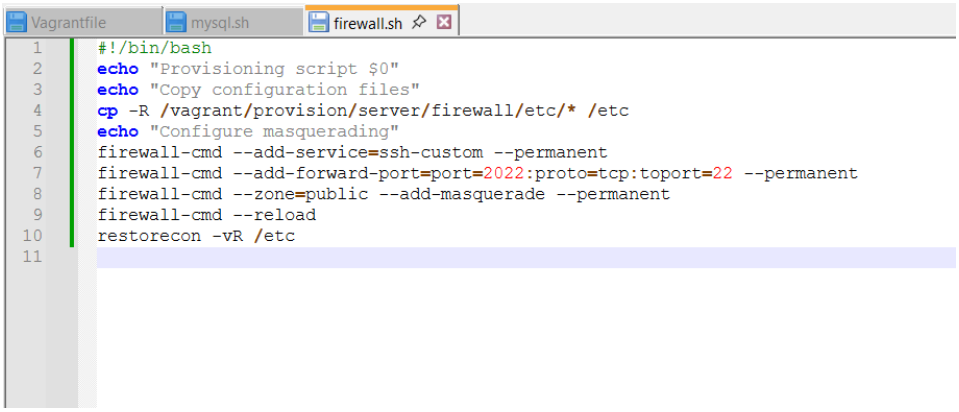


Рис. 2.9: Содержимое скрипта firewall.sh

3. Для выполнения сценария при старте виртуальной машины в файле `Vagrantfile` должен быть добавлен provisioning-блок, указывающий на запуск `provision/server/firewall.sh`. Это обеспечивает автоматическое применение сетевых настроек при каждом развёртывании окружения.

# 3 Вывод

В ходе выполнения лабораторной работы была выполнена настройка пользовательских правил межсетевого экрана FirewallD на виртуальной машине server. Создано пользовательское описание службы SSH с изменённым номером порта, произведена активация службы и её интеграция в конфигурацию FirewallD. Реализовано перенаправление портов для доступа к службе SSH через нестандартный порт, а также выполнена настройка пересылки IPv4-пакетов и маскарадинга для обеспечения корректной маршрутизации сетевого трафика. Дополнительно была подготовлена автоматизация сетевых настроек с использованием provisioning-скрипта Vagrant, что обеспечивает воспроизводимость конфигурации при повторном развёртывании виртуальной машины. Проверка показала корректную работу настроенных сервисов, успешное подключение по SSH и доступ клиента к внешним сетевым ресурсам.

# 4 Контрольные вопросы

**1. Где хранятся пользовательские файлы firewalld?**

Пользовательские файлы конфигурации FirewallD, включая описания служб, хранятся в каталоге `/etc/firewalld/`. В частности, пользовательские файлы служб располагаются в подкаталоге `/etc/firewalld/services/`. В отличие от системных файлов, размещённых в `/usr/lib/firewalld/`, пользовательские файлы не перезаписываются при обновлении системы.

**2. Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022?**

Для указания TCP-порта 2022 в пользовательском файле службы необходимо добавить или изменить строку с описанием порта следующим образом:

```
<port protocol="tcp" port="2022"/>
```

**3. Какая команда позволяет вам перечислить все службы, доступные в настоящее время на вашем сервере?**

Для вывода списка всех служб, доступных в настоящий момент в FirewallD, используется команда:

```
firewall-cmd --get-services
```

**4. В чем разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading)?**

NAT (Network Address Translation) — это общий механизм трансляции сетевых адресов, при котором один IP-адрес или диапазон адресов преобразуется в другой в соответствии с заданными правилами.

Маскарадинг (masquerading) является частным случаем NAT и используется, как

правило, при динамическом внешнем IP-адресе. При маскарадинге исходящий трафик автоматически подменяет исходный IP-адрес на адрес внешнего интерфейса сервера, что удобно для организации доступа клиентов в сеть Интернет без явного указания внешнего IP.

**5. Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10?**

Для разрешения входящего TCP-трафика на порт 4404 и его перенаправления на SSH-службу (порт 22) узла с IP-адресом 10.0.0.10 используется команда:

```
firewall-cmd --add-forward-port=port=4404:proto=tcp:toport=22:toaddr=10.0.0.10
```

**6. Какая команда используется для включения маскарадинга IP-пакетов для всех пакетов, выходящих в зону public?**

Для включения маскарадинга IP-пакетов в зоне `public` применяется команда:

```
firewall-cmd --zone=public --add-masquerade --permanent
```