Отчёт по лабораторной работе 7

Расширенные настройки межсетевого экрана

Заур Мустафаев

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Выполнение работы

2.1 Создание пользовательской службы firewalld

1. Выполнен вход в рабочий каталог проекта и запущена виртуальная машина **server**. После загрузки системы выполнен переход в режим суперпользователя для выполнения административных операций.

2. На основе стандартного файла описания службы **ssh** создан пользовательский файл службы **ssh-custom.xml**. Файл был скопирован из системного каталога `/usr/lib/firewalld/services/` в каталог пользовательских служб `/etc/firewalld/services/`.

3. Просмотрено содержимое файла `ssh-custom.xml`. Файл представляет собой XML-описание службы firewalld и включает:

    - декларацию версии XML;
    - корневой элемент `<service>`;
    - элемент `<short>`, содержащий краткое имя службы;
    - элемент `<description>`, описывающий назначение службы;
    - элемент `<port>`, задающий протокол и номер порта, разрешённого для данной службы.

```
[root@server.zmustafaev.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.zmustafaev.net ~]# cd /etc/firewalld/services/
[root@server.zmustafaev.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 encrypte
d communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You need the
openssh-server package installed for this option to be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server.zmustafaev.net services]#
```

Рис. 2.1: Просмотр содержимого ssh-custom.xml

4. Файл службы был открыт для редактирования. В нём изменён номер порта с **22** на **2022**, а описание службы скорректировано для указания, что используется модифицированная версия службы SSH.

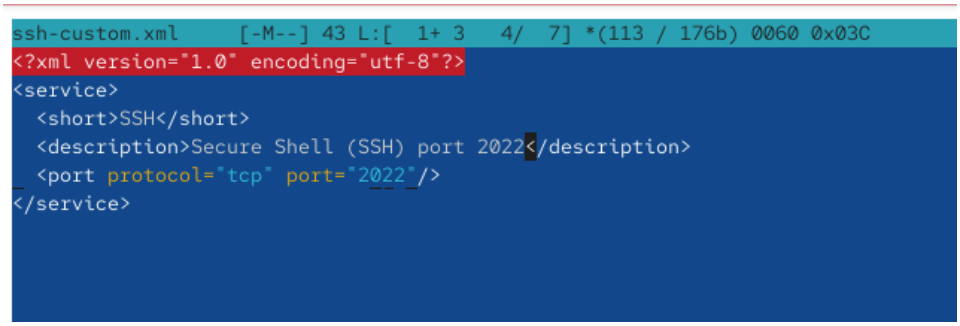

Рис. 2.2: Редактирование файла ssh-custom.xml

5. Получен список доступных служб firewalld. Установлено, что созданная пользовательская служба на данном этапе ещё не активна.

Рис. 2.3: Список доступных служб firewalld

6. Выполнена перезагрузка правил межсетевого экрана с сохранением текущего состояния. После перезагрузки повторно выведен список служб, в котором появилась служба **ssh-custom**, однако она не была активирована.

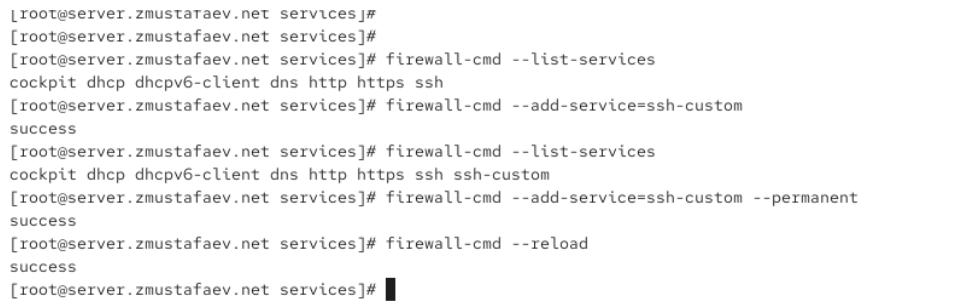

Рис. 2.4: Перезагрузка firewalld и проверка служб

7. Пользовательская служба **ssh-custom** добавлена в активные службы текущей зоны. После этого выполнено постоянное добавление службы с сохранением конфигурации и повторная перезагрузка firewalld.

2.2 Перенаправление портов

1. На сервере настроено перенаправление входящих TCP-соединений с порта **2022** на стандартный порт службы SSH **22**.

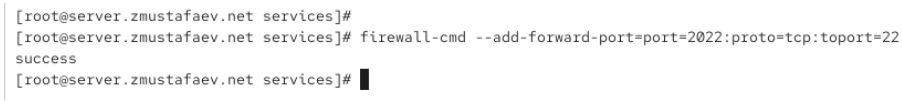

Рис. 2.5: Настройка перенаправления портов

2. На клиентской виртуальной машине выполнена попытка подключения к серверу по SSH через порт **2022**. Подключение прошло успешно, что подтверждает корректность настройки перенаправления портов.

Рис. 2.6: Подключение к серверу по SSH через порт 2022

2.3 Настройка Port Forwarding и Masquerading

1. Проверено состояние параметров ядра, отвечающих за пересылку IPv4-пакетов. Установлено, что перенаправление пакетов по умолчанию отключено.

2. Включена поддержка перенаправления IPv4-пакетов путём добавления соответствующей настройки в файл `/etc/sysctl.d/90-forward.conf` и применения параметров ядра.

3. Для внешнего сетевого интерфейса включён режим маскарадинга, обеспечивающий трансляцию сетевых адресов. После внесения изменений выполнена перезагрузка правил межсетевого экрана.

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

Рис. 2.7: Включение IP forwarding и masquerading

4. На клиентской виртуальной машине проверена доступность выхода в сеть Интернет. Доступ подтверждён, что свидетельствует о корректной работе настроек Port Forwarding и Masquerading.

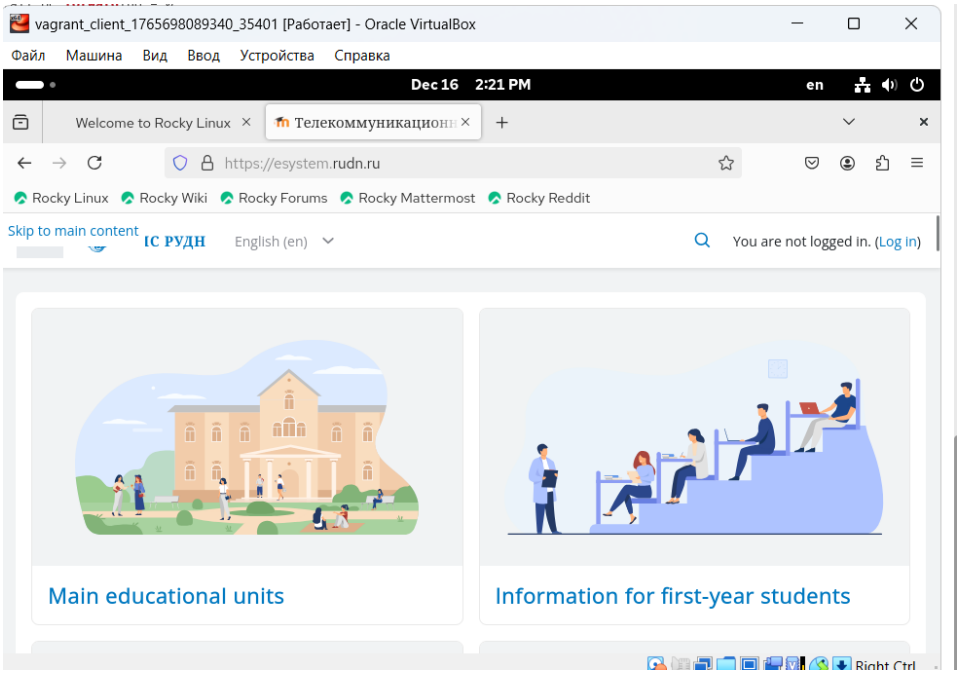

Рис. 2.8: Выход в сеть Интернет

2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. В каталоге `/vagrant/provision/server` создана структура каталогов для хранения конфигурационных файлов FirewallD и параметров ядра.

2. В соответствующие подкаталоги помещены конфигурационные файлы пользовательской службы `ssh-custom.xml` и файл настроек ядра `90-forward.conf`.

3. В каталоге `/vagrant/provision/server` создан исполняемый файл `firewall.sh`, предназначенный для автоматизации настройки межсетевого экрана, применения перенаправления портов и маскарадинга при развёртывании виртуальной машины.

Vagrantfile | mysql.sh | firewall.sh

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

Рис. 2.9: firewall.sh

3 Вывод

В ходе работы была создана и настроена пользовательская служба **firewalld** на основе стандартной службы SSH. Выполнена модификация конфигурации с изменением порта, произведена активация службы и проверка её работы. Реализовано перенаправление портов, включены механизмы **Port Forwarding** и **Masquerading**, что обеспечило корректную маршрутизацию и доступ клиентов к внешней сети. Дополнительно подготовлены файлы и скрипт автоматизации для применения настроек в среде Vagrant.

4 Контрольные вопросы

1. **Где хранятся пользовательские файлы firewalld?**
   Пользовательские файлы firewalld хранятся в каталоге `/etc/firewalld/`, в частности описания служб размещаются в `/etc/firewalld/services/`.

2. **Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022?**
   Для указания порта необходимо добавить строку `<port protocol="tcp" port="2022"/>`.

3. **Какая команда позволяет перечислить все службы, доступные в настоящее время на вашем сервере?**
   Для вывода списка всех доступных служб используется команда `firewall-cmd --get-services`.

4. **В чем разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading)?**
   NAT предполагает статическое сопоставление внутренних и внешних IP-адресов, тогда как маскарадинг является динамической формой NAT и автоматически подставляет внешний IP-адрес интерфейса, что удобно при использовании изменяемых адресов.

5. **Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10?**
   Для этого используется команда перенаправления портов с указанием целевого адреса и порта службы SSH.

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

   Маскарадинг для зоны public включается с помощью команды `firewall-cmd --zone=public --add-masquerade --permanent`.

5 Список литературы

1. NAT: вопросы и ответы. — URL: https://www.cisco.com/cisco/web/support/RU/9/92/92029_nat-faq.html (дата обр. 13.09.2021).
2. Динамический брандмауэр с использованием FirewallD. — URL: https://fedoraproject.org/wik (дата обр. 13.09.2021).
3. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М.: Вильямс, 2017. — 912 с. — (Cisco Press Core Series).
4. Часто задаваемые вопросы по технологии NAT / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/c/ru_ru/support/docs/ip/network address-translation-nat/26704-nat-faq-00.html (дата обр. 13.09.2021).