Отчёт по лабораторной работе 7

Расширенные настройки межсетевого экрана

Суннатилло Махмудов

Содержание

# 1 Цель работы

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

# 2 Теоретические сведения

Служба **firewalld** представляет собой динамически управляемый брандмауэр Linux, обеспечивающий гибкое управление сетевой безопасностью без необходимости перезапуска службы.  
Она использует концепцию **зон** и **служб**, позволяя применять различные правила фильтрации трафика в зависимости от уровня доверия к сетям.

Файлы описания служб имеют формат **XML** и содержатся в каталогах:  
– **/usr/lib/firewalld/services/** — системные шаблоны служб;  
– **/etc/firewalld/services/** — пользовательские службы и изменения.

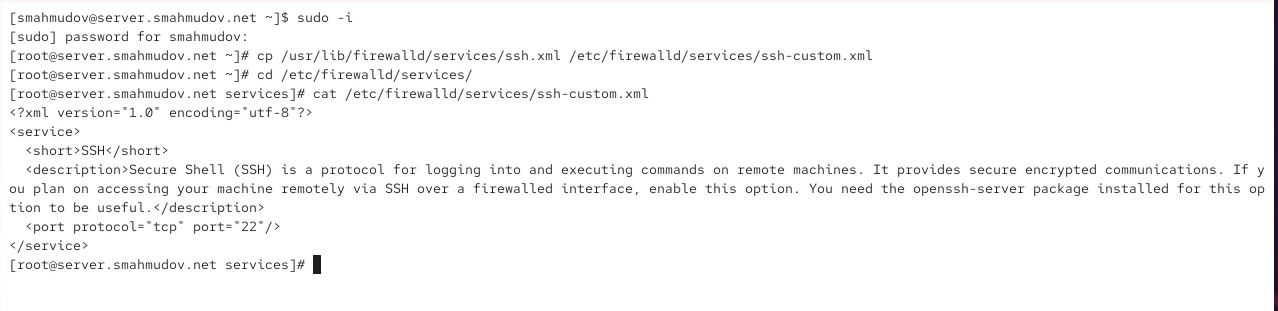
Создание пользовательской службы позволяет задать собственные порты и протоколы, отличные от стандартных, что используется, например, для переноса SSH на нестандартный порт (в работе — **2022**).

Механизм **Port Forwarding** обеспечивает перенаправление трафика с одного порта на другой, а **Masquerading** (маскарадинг) используется для подмены исходных IP-адресов пакетов, позволяя устройствам внутренней сети выходить в Интернет через общий внешний IP.

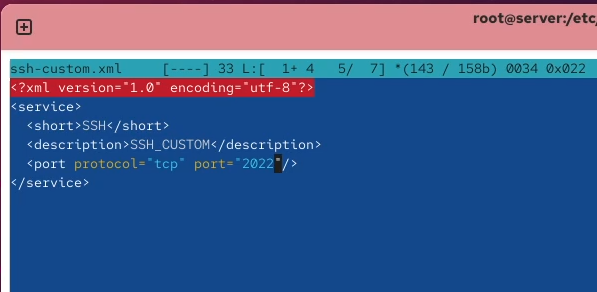
# 3 Выполнение лабораторной работы

## 3.1 Создание пользовательской службы firewalld

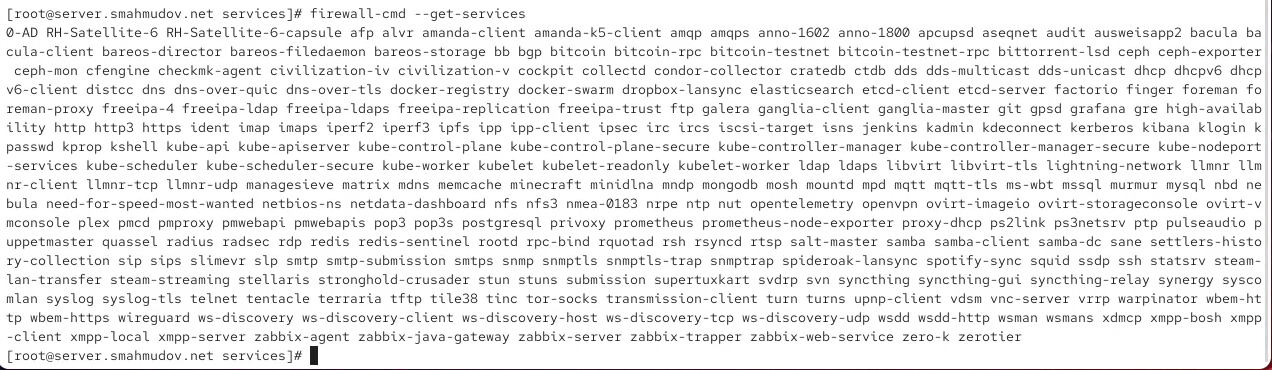
1. На виртуальной машине **server** был выполнен вход под пользователем *smahmudov* и произведён переход в режим суперпользователя.  
   После этого был создан собственный файл службы на основе системного описания **ssh.xml**:

* cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml  
  cd /etc/firewalld/services/
* 
* Рис. 1: Создание пользовательского файла службы

1. Было просмотрено содержимое нового файла **ssh-custom.xml**, чтобы проанализировать структуру описания службы.  
   Основные элементы XML:  
   – <service> — корневой элемент, в котором задаются параметры службы;  
   – <short> — краткое имя службы;  
   – <description> — описание назначения службы;  
   – <port protocol="tcp" port="22"/> — определяет используемый порт и протокол.

* Пример содержимого:
* SSH Secure Shell (SSH) is a protocol…
* 
* Рис. 2: Просмотр исходного содержимого файла службы

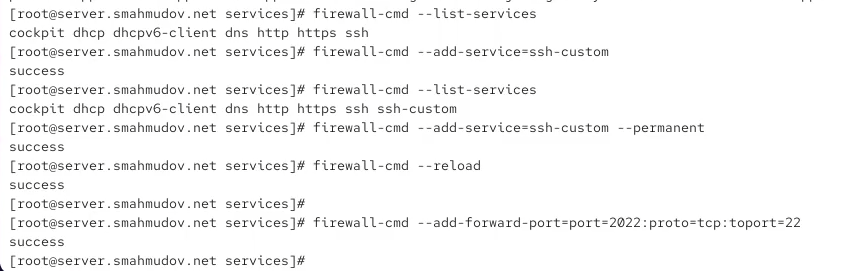
1. Файл **ssh-custom.xml** был отредактирован: описание изменено для указания, что это модифицированная служба, а номер порта заменён с **22** на **2022**.

* SSH SSH\_CUSTOM
* 
* Рис. 3: Редактирование параметров пользовательской службы

1. Для проверки наличия новой службы был выполнен просмотр списка всех доступных служб FirewallD:

* firewall-cmd –get-services
* На данном этапе служба **ssh-custom** ещё не отображалась в списке.
* 
* Рис. 4: Просмотр доступных служб до перезагрузки

1. Для обновления конфигурации FirewallD была выполнена команда:

* firewall-cmd –reload
* После этого новая служба появилась в общем списке доступных, что подтверждает успешное считывание изменённого XML-файла.
* firewall-cmd –get-services
* 
* Рис. 5: Появление службы ssh-custom после перезагрузки правил

1. Затем пользовательская служба **ssh-custom** была добавлена в активные:

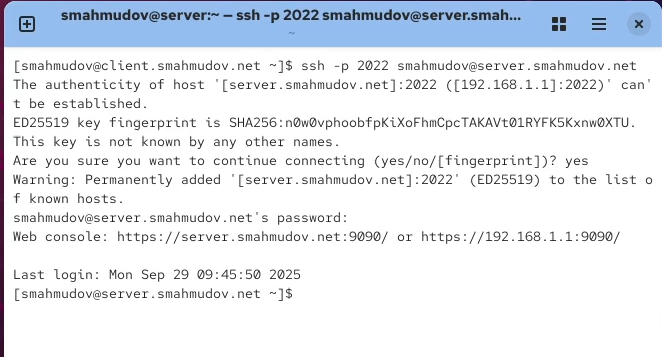
* firewall-cmd –add-service=ssh-custom  
  firewall-cmd –list-services
* После успешного добавления конфигурация была сохранена навсегда:
* firewall-cmd –add-service=ssh-custom –permanent  
  firewall-cmd –reload

## 3.2 Перенаправление портов

1. На сервере была организована переадресация с порта **2022** на порт **22**, что позволяет подключаться к SSH через пользовательский порт:

* firewall-cmd –add-forward-port=port=2022:proto=tcp:toport=22
* После выполнения команды система сообщила об успешном применении перенаправления.

1. На клиентской машине было выполнено подключение по SSH через порт **2022**, что подтвердило корректность настроек:

* ssh -p 2022 smahmudov@server.smahmudov.net
* После ввода пароля подключение было установлено, а система вывела приветственное сообщение с адресом веб-консоли сервера.
* 
* Рис. 6: Подключение по SSH через перенаправленный порт

## 3.3 Настройка Port Forwarding и Masquerading

1. На сервере была проверена текущая конфигурация перенаправления IPv4-пакетов:

* sysctl -a | grep forward
* Большинство параметров имели значение **0**, что означало, что пересылка пакетов была отключена.

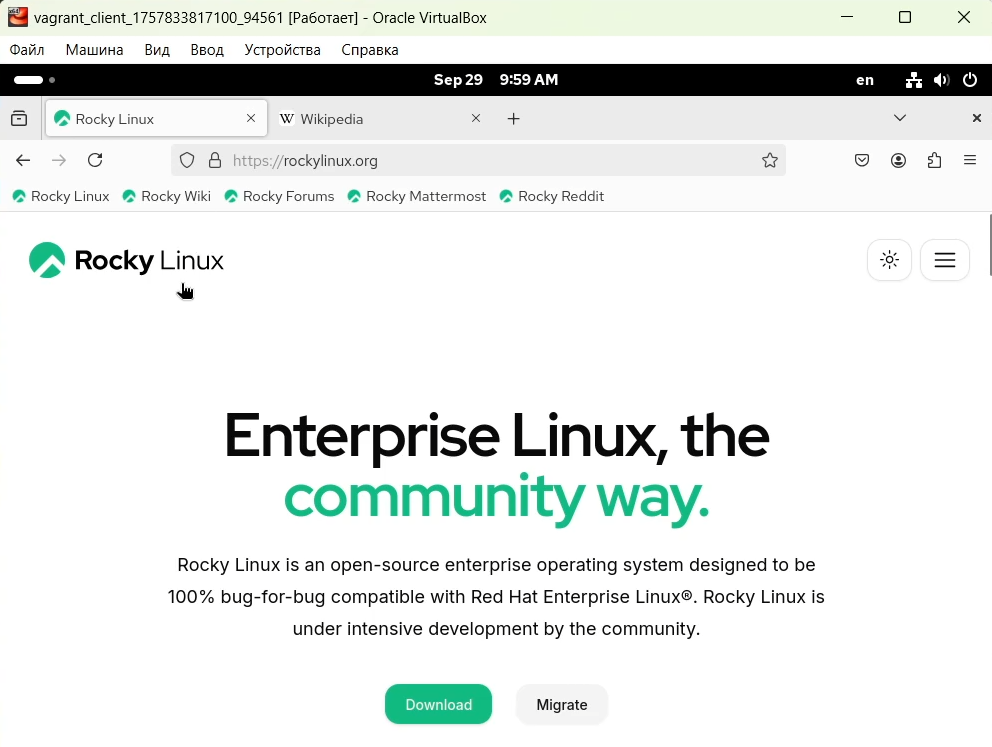
1. Для включения пересылки IPv4-пакетов был создан конфигурационный файл:

* echo “net.ipv4.ip\_forward = 1” > /etc/sysctl.d/90-forward.conf  
  sysctl -p /etc/sysctl.d/90-forward.conf
* В результате параметр **net.ipv4.ip\_forward** был установлен в значение **1**, что активировало возможность маршрутизации пакетов.

1. Далее был включён маскарадинг в публичной зоне FirewallD:

* firewall-cmd –zone=public –add-masquerade –permanent  
  firewall-cmd –reload
* После применения настроек система выдала сообщение **success**, подтверждающее корректное выполнение команд.
* 
* Рис. 7: Включение пересылки пакетов и маскарадинга

1. После активации маскарадинга клиентская машина получила доступ в Интернет, что было проверено открытием сайта **rockylinux.org** в браузере.

* 
* Рис. 8: Проверка доступа в Интернет после настройки маскарадинга

## 3.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине **server** был выполнен переход в каталог внутреннего окружения:

* cd /vagrant/provision/server/
* В нём был создан каталог **firewall** с подкаталогами для хранения конфигурационных файлов:
* mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services  
  mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
* Затем в созданные директории были скопированы соответствующие конфигурационные файлы:
* cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc/firewalld/services/  
  cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d/

1. В каталоге **/vagrant/provision/server** был создан скрипт **firewall.sh**, предназначенный для автоматического применения настроек:

* touch firewall.sh  
  chmod +x firewall.sh
* 
* Рис. 9: Создание каталогов и скрипта firewall.sh для сохранения конфигурации

# 4 Вывод

В ходе лабораторной работы была выполнена настройка системы управления сетевой безопасностью **firewalld**, включая создание пользовательской службы **ssh-custom**, перенаправление портов и активацию механизма маскарадинга.  
Реализовано подключение по SSH через нестандартный порт **2022** с автоматическим перенаправлением на порт **22**, а также включена маршрутизация и маскарадинг IPv4-пакетов.

# 5 Контрольные вопросы

1. **Где хранятся пользовательские файлы firewalld?**  
   Пользовательские файлы служб **firewalld** хранятся в каталоге **/etc/firewalld/services/**.  
   Этот каталог используется для размещения изменённых или собственных XML-файлов описания служб, в отличие от системных шаблонов, находящихся в **/usr/lib/firewalld/services/**.
2. **Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022?**  
   Для указания порта **2022** в пользовательском файле службы необходимо добавить следующую строку в блок <service>:
3. **Какая команда позволяет вам перечислить все службы, доступные в настоящее время на вашем сервере?**  
   Для вывода списка всех доступных служб используется команда:

* firewall-cmd –get-services

1. **В чем разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading)?**  
   **NAT (Network Address Translation)** — общий механизм преобразования IP-адресов, позволяющий устройствам внутренней сети обращаться к внешней, заменяя их внутренние адреса на публичные.  
   **Маскарадинг (Masquerading)** — частный случай NAT, при котором используется один общий внешний IP-адрес для всех исходящих соединений, причём адрес подставляется динамически (обычно при подключении к интернету через роутер).
2. **Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10?**  
   Для разрешения входящих соединений и перенаправления их на указанный адрес используется команда:

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

1. **Какая команда используется для включения маскарадинга IP-пакетов для всех пакетов, выходящих в зону public?**  
   Для включения маскарадинга в публичной зоне применяется следующая команда:

* firewall-cmd –zone=public –add-masquerade –permanent

# 6 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/wiki/FirewallD/ru (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 PressCore 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).