Отчёт по лабораторной работе 7

Расширенные настройки межсетевого экрана

Метвалли Ахмед Фарг Набеех

Содержание

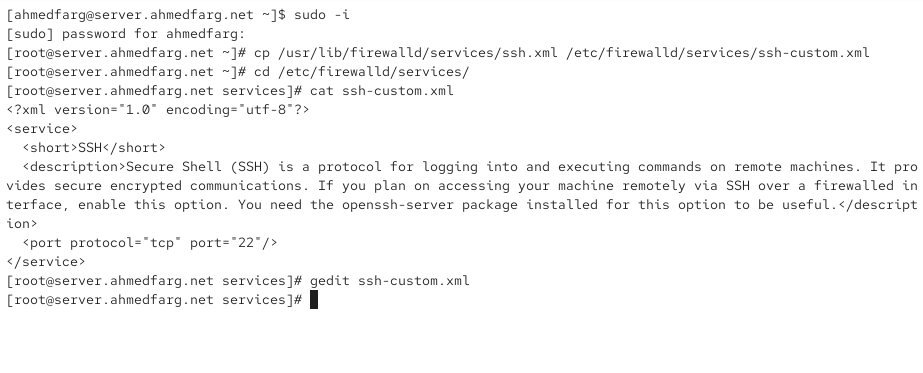
# 1 Цель работы

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

# 2 Выполнение

## 2.1 Создание пользовательской службы firewalld

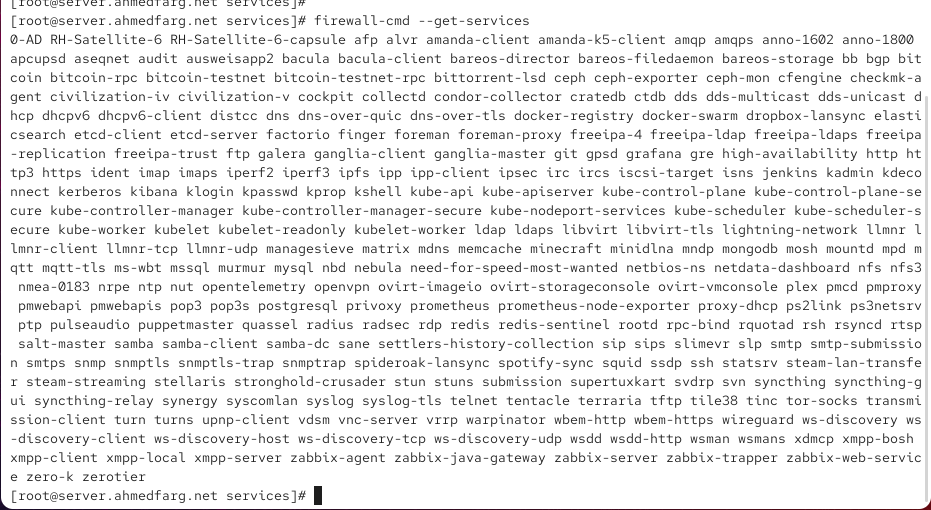
1. На виртуальной машине server создана пользовательская служба для **firewalld**, основанная на стандартной службе ssh.
2. На основе системного файла /usr/lib/firewalld/services/ssh.xml был создан новый файл **ssh-custom.xml** в каталоге /etc/firewalld/services/.

* 
* Рис. 1: Создание файла ssh-custom.xml и просмотр содержимого

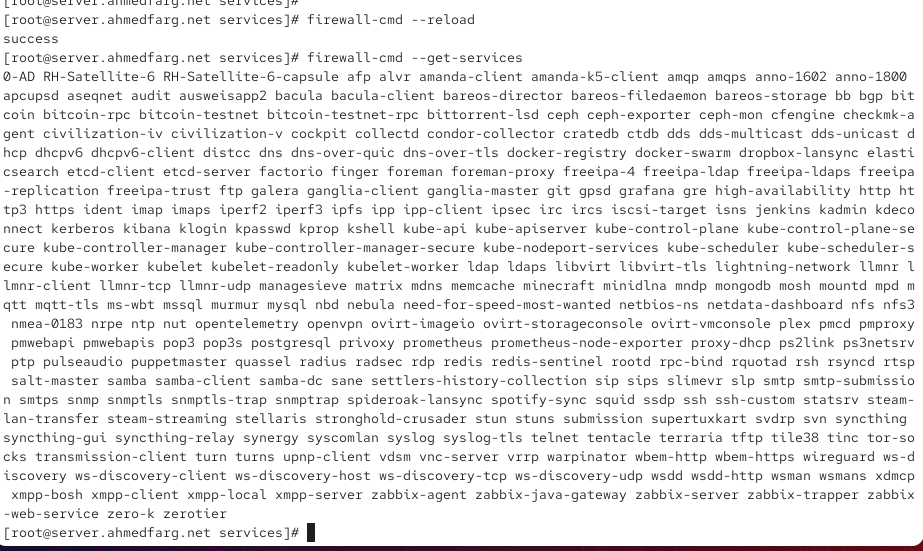
1. В исходном файле заданы основные элементы XML-описания службы:
   * <?xml version="1.0" encoding="utf-8"?> — объявление версии и кодировки XML;
   * <service> — корневой элемент, описывающий сетевую службу;
   * <short> — краткое имя службы, отображаемое в списках firewalld;
   * <description> — текстовое описание назначения службы и её особенностей;
   * <port protocol="tcp" port="22"/> — определение используемого сетевого порта и протокола.

* После редактирования порт был изменён с **22** на **2022**, а в описании указано, что это модифицированная служба.
* 
* Рис. 2: Редактирование файла ssh-custom.xml

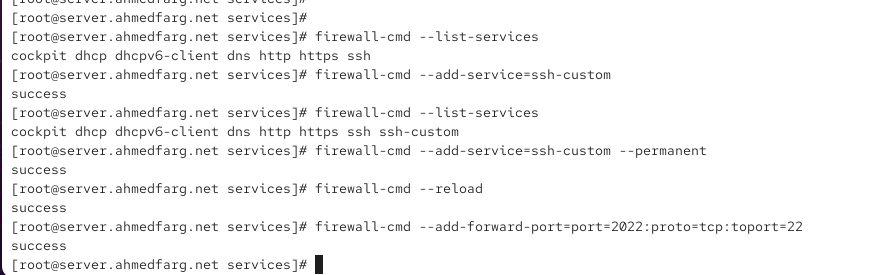
1. Для проверки доступных служб firewalld выполнена команда:

* firewall-cmd --get-services
* В списке отображаются все предустановленные службы, однако созданная служба ssh-custom на этом этапе ещё отсутствует.
* 
* Рис. 3: Список служб firewalld до перезагрузки

1. После перезагрузки конфигурации firewalld командами:

* firewall-cmd --reload  
  firewall-cmd --get-services
* служба ssh-custom появилась в списке доступных.
* 
* Рис. 4: Служба ssh-custom после перезагрузки firewalld

1. Далее выполнено добавление пользовательской службы в список активных:

* firewall-cmd --add-service=ssh-custom  
  firewall-cmd --add-service=ssh-custom --permanent  
  firewall-cmd --reload
* После этого служба **ssh-custom** успешно активирована и отображается в списке активных служб.
* 
* Рис. 5: Добавление и активация пользовательской службы

# 3 Выполнение

## 3.1 Перенаправление портов

1. На сервере выполнена настройка переадресации входящих подключений с порта **2022** на порт **22** с помощью команды:

* firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22

1. На клиентской машине выполнено подключение к серверу по SSH через порт **2022**.  
   Подключение прошло успешно, что подтверждает корректную работу правила переадресации.

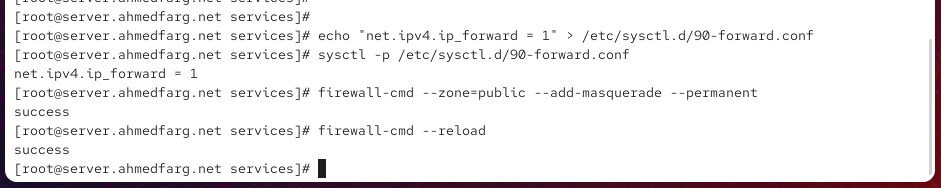
* 
* Рис. 6: Подключение к серверу по порту 2022

## 3.2 Настройка Port Forwarding и Masquerading

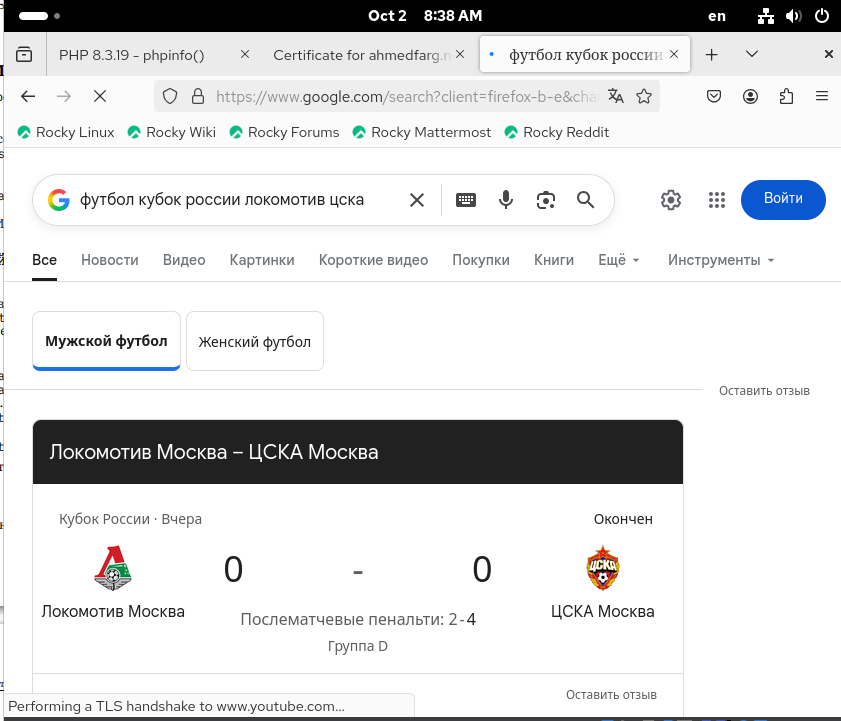
1. На сервере проверено текущее состояние параметра перенаправления IPv4-пакетов.  
   По выводу команды видно, что параметр net.ipv4.ip\_forward установлен в значение **0**, то есть переадресация отключена.

* 
* Рис. 7: Проверка параметра ip\_forward

1. Для включения пересылки IPv4-пакетов создан файл /etc/sysctl.d/90-forward.conf с содержимым net.ipv4.ip\_forward = 1.  
   После применения параметров командой sysctl -p /etc/sysctl.d/90-forward.conf пересылка пакетов успешно активировалась.

* 
* Рис. 8: Включение пересылки IPv4-пакетов

1. Включён маскарадинг в зоне **public** для обеспечения NAT и маршрутизации.  
   После перезагрузки конфигурации (firewall-cmd --reload) система подтвердила успешное применение настроек.
2. С клиентской машины выполнена проверка выхода в Интернет — соединение установлено успешно, что подтверждает корректность настроек перенаправления и маскарадинга.

* 
* Рис. 9: Проверка доступа в Интернет с клиента

## 3.3 Внесение изменений во внутренние настройки виртуальной машины

1. На сервере создана структура каталогов для хранения конфигурационных файлов **FirewallD** и системных параметров:
   * /vagrant/provision/server/firewall/etc/firewalld/services
   * /vagrant/provision/server/firewall/etc/sysctl.d

* В соответствующие каталоги скопированы файлы ssh-custom.xml и 90-forward.conf.

1. Затем в каталоге /vagrant/provision/server/ создан исполняемый файл **firewall.sh**, предназначенный для автоматического применения конфигурации при развертывании виртуальной машины.

* 
* Рис. 10: Создание структуры каталогов и скрипта firewall.sh

# 4 Заключение

Была выполнена настройка пользовательской службы **firewalld** с переназначением порта SSH на 2022.  
Проверена возможность подключения по новому порту, реализовано перенаправление и включён маскарадинг.  
Создана структура каталогов и подготовлены конфигурационные файлы для автоматического применения параметров при развёртывании виртуальной машины.

# 5 Контрольные вопросы

1. **Где хранятся пользовательские файлы firewalld?**  
   В каталоге /etc/firewalld/services/, где можно размещать собственные XML-файлы описания служб.
2. **Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022?**  
   <port protocol="tcp" port="2022"/>
3. **Какая команда позволяет вам перечислить все службы, доступные в настоящее время на вашем сервере?**  
   firewall-cmd --get-services
4. **В чем разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading)?**  
   NAT — общий механизм подмены адресов при прохождении пакетов через маршрутизатор.  
   Маскарадинг — частный случай NAT, при котором исходящий трафик получает динамический внешний IP-адрес интерфейса, через который осуществляется доступ в сеть.
5. **Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10?**  
   firewall-cmd --add-forward-port=port=4404:proto=tcp:toaddr=10.0.0.10:toport=22
6. **Какая команда используется для включения маскарадинга IP-пакетов для всех пакетов, выходящих в зону public?**  
   firewall-cmd --zone=public --add-masquerade --permanent