Отчёт по лабораторной работе №7

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

Содержание

# 1. Цель работы

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

# 2. Выполнение лабораторной работы

## 2.1 Создание пользовательской службы firewalld

В рабочем каталоге проекта выполнен переход в режим суперпользователя на виртуальной машине server, после чего на основе существующего файла описания службы ssh.xml создан пользовательский файл ssh-custom.xml в каталоге /etc/firewalld/services/ с помощью команды копирования. Далее осуществлён переход в соответствующий каталог для дальнейшей работы с файлом ([рис. 1](#fig-1)).

Содержимое файла /etc/firewalld/services/ssh-custom.xml выведено командой cat. Файл представляет собой XML-описание службы: корневой элемент <service>, краткое имя службы <short>, текстовое описание <description>, а также определение порта через элемент <port> с указанием протокола tcp и номера порта 22 ([рис. 1](#fig-1)).

|  |
| --- |
| Рисунок 1: Копирование файла службы ssh.xml в ssh-custom.xml |

Файл службы отредактирован: в элементе <port> изменён номер порта с 22 на 2022, а в элементе <description> указано, что используется модифицированная служба SSH для доступа через TCP-порт 2022. После редактирования содержимое файла повторно выведено на экран для проверки внесённых изменений ([рис. 3](#fig-3)).

|  |
| --- |
| Рисунок 2: Редактирование службы: изменение порта на 2022 и обновление описания |

С помощью команды firewall-cmd --get-services получен список доступных служб, затем выполнена перезагрузка правил межсетевого экрана командой firewall-cmd --reload ([рис. 4](#fig-4)) . После перезагрузки служба ssh-custom отображается в списке доступных служб, но отсутствует среди активных . Далее служба добавлена в активные с помощью firewall-cmd --add-service=ssh-custom, проверена командой firewall-cmd --list-services, затем добавлена на постоянной основе с ключом --permanent и выполнена повторная перезагрузка правил ([рис. 4](#fig-4)).

|  |
| --- |
| Рисунок 3: Добавление и активация пользовательской службы ssh-custom в firewalld |

|  |
| --- |
| Рисунок 4: Добавление и активация пользовательской службы ssh-custom в firewalld |

## 2.2 Перенаправление портов

На виртуальной машине server выполнена настройка перенаправления трафика с TCP-порта 2022 на стандартный порт SSH 22 с помощью команды firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22. Команда завершилась успешно, что подтверждает добавление правила переадресации в текущую конфигурацию firewalld ([рис. 5](#fig-5)).

|  |
| --- |
| Рисунок 5: Настройка перенаправления порта 2022 на 22 в firewalld |

На виртуальной машине client выполнена попытка подключения к серверу по SSH через порт 2022 командой ssh -p 2022 alkamal@server.alkamal.net. При первом подключении подтверждена подлинность хоста и его ключ добавлен в файл known\_hosts. После ввода пароля пользователя выполнен успешный вход в систему, что подтверждает корректную работу перенаправления с порта 2022 на порт 22 ([рис. 6](#fig-6)).

|  |
| --- |
| Рисунок 6: Подключение по SSH к серверу через порт 2022 с клиента |

На виртуальной машине server выполнена проверка состояния параметров пересылки пакетов в ядре с помощью команды sysctl -a | grep forward. В выводе параметр net.ipv4.ip\_forward имел значение 0, что означает отключённую маршрутизацию IPv4-пакетов ([рис. 7](#fig-7)).

Для включения пересылки IPv4-пакетов создан файл /etc/sysctl.d/90-forward.conf с параметром net.ipv4.ip\_forward = 1, после чего конфигурация применена командой sysctl -p /etc/sysctl.d/90-forward.conf, что подтвердило установку значения 1. Далее в зоне public активирован маскарадинг с помощью firewall-cmd --zone=public --add-masquerade --permanent и выполнена перезагрузка правил firewall-cmd --reload ([рис. 7](#fig-7)).

|  |
| --- |
| Рисунок 7: Проверка параметров пересылки IPv4 в ядре системы |

На виртуальной машине client проверена доступность сети Интернет командами ping 8.8.8.8 и ping google.com; получены ответы без потерь пакетов, что подтверждает корректную работу перенаправления и маскарадинга ([рис. 8](#fig-8)).

|  |
| --- |
| Рисунок 8: Проверка доступа в Интернет с клиента после включения IP-forward и masquerade |

## 2.3 Внесение изменений в настройки внутреннего

На виртуальной машине server выполнен переход в каталог /vagrant/provision/server, после чего создана структура каталогов firewall/etc/firewalld/services и firewall/etc/sysctl.d. В данные каталоги скопированы файл пользовательской службы ssh-custom.xml и файл конфигурации 90-forward.conf, что обеспечивает сохранение настроек firewalld и параметра ip\_forward во внутреннем окружении виртуальной машины ([рис. 9](#fig-9)).

|  |
| --- |
| Рисунок 9: Создание структуры каталогов и копирование конфигурационных файлов FirewallD |

В каталоге /vagrant/provision/server создан исполняемый файл firewall.sh, которому назначены права на выполнение. В скрипте реализовано копирование подготовленных конфигурационных файлов в каталог /etc, добавление службы ssh-custom, настройка перенаправления порта 2022 на 22, включение маскарадинга в зоне public, перезагрузка правил firewalld и восстановление контекстов SELinux командой restorecon -vR /etc ([рис. 10](#fig-10)).

|  |
| --- |
| Рисунок 10: Содержимое provisioning-скрипта firewall.sh |

В конфигурационный файл Vagrantfile в разделе настройки виртуальной машины server добавлен блок provision с типом shell, параметром preserve\_order: true и указанием пути provision/server/firewall.sh. Это обеспечивает автоматическое выполнение созданного скрипта при запуске или пересоздании виртуальной машины ([рис. 11](#fig-11)).

|  |
| --- |
| Рисунок 11: Добавление provisioning-скрипта firewall.sh в Vagrantfile |

# 3. Выводы

В ходе работы была создана пользовательская служба ssh-custom в системе firewalld с изменённым портом TCP 2022, что позволило организовать доступ к SSH через нестандартный порт. Реализовано перенаправление трафика с порта 2022 на порт 22, подтверждённое успешным подключением по SSH.

В ядре системы включена пересылка IPv4-пакетов (net.ipv4.ip\_forward = 1), а также настроен маскарадинг в зоне public, что обеспечило корректную маршрутизацию и выход клиента в Интернет через сервер.

Конфигурационные файлы и параметры были вынесены во внутреннее окружение виртуальной машины и автоматизированы с помощью provisioning-скрипта firewall.sh, подключённого в Vagrantfile. Это обеспечивает воспроизводимость настроек при повторном развёртывании виртуальной машины.

# 4. Ответы на контрольные вопросы

1. Где хранятся пользовательские файлы firewalld?

* В firewalld пользовательские файлы хранятся в директории /etc/firewalld/.

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

* Для указания порта TCP 2022 в пользовательском файле службы, вы можете добавить строку в секцию port следующим образом:

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

* firewall-cmd –get-services

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

* Разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading) заключается в том, что в случае NAT исходный IP-адрес пакета заменяется на IP-адрес маршрутизатора, а в случае маскарадинга используется маршрутизатора.

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

firewall-cmd --zone=public --add-port=4404/tcp --permanent  
firewall-cmd --zone=public --add-forward-port=port=4404  
 :proto=tcp:toport=22:toaddr=10.0.0.10 --permanent  
firewall-cmd --reload

1. Какая команда используется для включения маcкарадинга IP- пакетов для всех пакетов, выходящих в зону public?

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