Лабораторная работа № 7. Расширенные настройки межсетевого экрана

7.1. Цель работы

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

7.2. Предварительные сведения

7.2.1. Динамическое управление межсетевым экраном FirewallD

В CentOS8 основным средством динамического управления межсетевым экраном является FirewallD — надстройка над встроенным в ядро операционной системы Linux межсетевым экраном Netfilter. Управление правилами FirewallD возможно через утилиту командной строки `firewall-cmd` или через графический интерфейс `firewall-config`.

В Firewalld введено понятие сетевой зоны, для которой применяются правила межсетевого экрана. По сетевой зоной в данном случае понимается сетевое соединение с определённым уровнем доверия. Предопределены следующие зоны:

- **block** — все входящие сетевые соединения отклоняются с сообщением «icmp-host-forbidden», при этом разрешены только сетевые подключения, которые были инициированы в этой системе;
- **dmz** — используется на компьютерах, находящихся в демилитаризованной зоне, при этом принимаются только выбранные входящие соединения, разрешён ограниченный доступ к внутренней сети;
- **drop** — все входящие пакеты отбрасываются, не информируя об этом источник, при этом разрешены исходящие соединения;
- **external** — используется во внешних сетях с включённым маскарадингом (Network Address Translation, NAT), например, на маршрутизаторах, при этом принимаются только выбранные входящие соединения;
- **home** — используется в домашних сетях, принимая во внимание, что большинство компьютеров в этой сети доверяют друг другу, при этом разрешено принимать только выбранные входящие соединения;
- **internal** — используется во внутренних сетях, в которых большинство компьютеров сети доверяют друг другу, при этом принимаются только выбранные входящие соединения;
- **public** — используется в общественных местах, принимая во внимание, что компьютеры в таких сетях не доверяют друг другу, при этом эта зона является зоной по умолчанию для всех вновь создаваемых сетевых интерфейсов;
- **trusted** — все сетевые подключения принимаются;
- **work** — используется во внутренних сетях организаций, где большинство компьютеров в сети доверяют друг другу, при этом принимаются только выбранные входящие соединения.

На серверах, имеющих только один сетевой интерфейс, вполне можно обойтись одной зоной, которая является зоной по умолчанию. Каждый пакет, который поступает в систему, анализируется для исходного адреса, и на основе этого исходного адреса анализируется `firewalld` на принадлежность к определённой зоне. Если какая-либо конкретная зона недоступна, пакет обрабатывается настройками в зоне по умолчанию.

FirewallD позволяет формировать правила доступа к службам операционной системы. Описание службы в FirewallD может быть представлено списком локальных портов,

а также перечнем вспомогательных модулей межсетевого экрана, загружаемых автоматически, если служба включена. Firewalld хранит все настройки, связанные со службами, в XML-файлах в каталоге `/usr/lib/firewalld/services`. Если требуется переопределить настройки имеющейся службы или подключить собственную службу, то необходимо файл с описанием службы разместить в каталоге `/etc/firewalld/services`. Опции конфигурации служб и общий информационный файл см. в `man firewalld.service`.

Общий синтаксис утилиты командной строки `firewall-cmd` для работы с правилами:

```
firewall-cmd [опции] [зона] <правило>
```

Здесь `<правило>` — правило межсетевого экрана; `[опции]` — дополнительные параметры создаваемого правила; `[зона]` — название зоны, для которой применяются правила (по умолчанию, правила создаются для зоны `public`).

Некоторые часто используемые команды `firewall-cmd`:

- вывод на экран описания опций `firewall-cmd`:
  ```
  firewall-cmd --help
  ```
- проверка активности `firewalld`:
  ```
  firewall-cmd --state
  ```
- перезагрузка правил межсетевого экрана с сохранением информации о состоянии:
  ```
  firewall-cmd --reload
  ```
- вывод на экран списка поддерживаемых зон /служб:
  ```
  firewall-cmd --get-zones
  firewall-cmd --get-services
  ```
- вывод на экран включённых в зоне служб:
  ```
  firewall-cmd [ --zone=<zone> ] --list-services
  ```
- включение службы в пределах зоны:
  ```
  firewall-cmd [--zone=<zone>] --add-service=<service>
  ```
- включение маскарадинга в пределах зоны:
  ```
  firewall-cmd [--zone=<zone>] --add-masquerad
  ```
- включение переадресации или переназначения портов в пределах зоны:
  ```
  firewall-cmd [--zone=<zone>]
   ↪  --add-forward-port=port=<port>[-<port>]:proto=<protocol> {
   ↪  :toport=<port>[-<port>] | :toaddr=<address> |
   ↪  :toport=<port>[-<port>]:toaddr=<address> }
  ```
- обработка зон с постоянными параметрами (опция `--permanent` должна быть первой для всех постоянных вызовов):
  ```
  firewall-cmd --permanent <опция>
  ```

  Более подробное описание см., например, в [2].

7.2.2. NAT, Masquerading, Port Forwarding

Network Address Translation (NAT) — механизм преобразования IP-адресов транзитных пакетов.

В частности, механизм NAT используется для обеспечения доступа устройств локальных сетей с внутренними IP-адресами к сети Интернет.

Типы NAT:

- *статический NAT (Static NAT, SNAT)* — осуществляет преобразование адресов по принципу 1:1 (в частности, один локальный IP-адрес преобразуется во внешний адрес, выделенный, например, провайдером);
- *динамический NAT (Dynamic NAT, DNAT)* — осуществляет преобразование адресов по принципу 1:N (например, один адрес устройства локальной сети преобразуется в один из адресов диапазона внешних адресов);

– *NAT Overload (или NAT Masquerading, или Port Address Translation, PAT)* — осуществляет преобразование адресов по принципу N:1 (например, адреса группы устройств локальной подсети преобразуются в один внешний адрес, при этом дополнительно используется механизм адресации через номера портов).

Маскарадинг (Masquerading) — тип трансляции сетевого адреса, при которой вместо адреса отправителя динамически подставляется адрес назначенного интерфейса (сетевой адрес + порт).

Принцип функционирования Маскарадинга:

– пакеты (запросы) для внешней сети от узлов локальной сети, имеющих внутренние IP-адреса, направляются на узел-шлюз с выделенным внешним IP-адресом, который заменяет обратные сетевые адреса на свой сетевой адрес (по сути NAT);
– ответ из внешней сети приходит на узел-шлюз;
– для перенаправления узлу локальной сети ответного пакета из внешней сети узел-шлюз обратно заменяет не только сетевой адрес, но и указывает порт отправителя.

Port Forwarding — технология, позволяющая обращаться из внешней сети (Интернет) к узлам, расположенным во внутренней сети за маршрутизатором, использующим NAT (NAPT). Трафик из внешней сети перенаправляется через интерфейс маршрутизатора с внешним адресом и определённый порт на этом интерфейсе на адрес выбранного компьютера в локальной сети.

7.3. Задание

1. Настройте межсетевой экран виртуальной машины `server` для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022 (см. разделы 7.4.1 и 7.4.2).
2. Настройте Port Forwarding на виртуальной машине `server` (см. разделы 7.4.3).
3. Настройте маскарадинг на виртуальной машине `server` для организации доступа клиента к сети Интернет (см. раздел 7.4.3).
4. Напишите скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана. Соответствующим образом внести изменения в `Vagrantfile` (см. раздел 7.4.4).

7.4. Последовательность выполнения работы

7.4.1. Создание пользовательской службы firewalld

1. На основе существующего файла описания службы `ssh` создайте файл с собственным описанием:
```
cp /usr/lib/firewalld/services/ssh.xml
 ↪  /etc/firewalld/services/ssh-custom.xml
cd /etc/firewalld/services/
```
2. Посмотрите содержимое файла службы:
```
cat /etc/firewalld/services/ssh-custom.xml
```
В отчёте построчно прокомментируйте принцип синтаксиса файла описания службы.
3. Откройте файл описания службы на редактирование и замените порт 22 на новый порт (2022):
```
<port protocol="tcp" port="2022"/>
```
В этом же файле скорректируйте описание службы для демонстрации, что это модифицированный файл службы.
4. Просмотрите список доступных FirewallD служб:
```
firewall-cmd --get-services
```
Обратите внимание, что новая служба ещё не отображается в списке.

5. Перегрузите правила межсетевого экрана с сохранением информации о состоянии и вновь выведите на экран список служб, а также список активных служб:
```
firewall-cmd --reload
firewall-cmd --get-services
firewall-cmd --list-services
```
Убедитесь, что созданная вами служба отображается в списке доступных для FirewallD служб, но не активирована.
6. Добавьте новую службу в FirewallD и выведите на экран список активных служб:
```
firewall-cmd --add-service=ssh-custom
firewall-cmd --list-services
```

7.4.2. Перенаправление портов

1. Организуйте на сервере переадресацию с порта 2022 на порт 22:
```
firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
```
2. На клиенте попробуйте получить доступ по SSH к серверу через порт 2022:
```
ssh -p 2022 user@server.user.net
```
(вместо `user` укажите свой логин).

7.4.3. Настройка Port Forwarding и Masquerading

1. На сервере посмотрите, активирована ли в ядре системы возможность перенаправления IPv4-пакетов пакетов:
```
sysctl -a | grep forward
```
2. Включите перенаправление IPv4-пакетов на сервере:
```
echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
sysctl -p /etc/sysctl.d/90-forward.conf
```
3. Включите маскарадинг на сервере:
```
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload
```
4. На клиенте проверьте доступность выхода в Интернет.

7.4.4. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине `server` перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создайте в нём каталог `firewall`, в который поместите в соответствующие подкаталоги конфигурационные файлы FirewallD:
```
cd /vagrant/provision/server
mkdir -p
 ↪  /vagrant/provision/server/firewall/etc/firewalld/services
mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
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/
```
2. В каталоге `/vagrant/provision/server` создайте файл `firewall.sh`:
```
cd /vagrant/provision/server
touch firewall.sh
chmod +x firewall.sh
```
Открыв его на редактирование, пропишите в нём следующий скрипт:

```
#!/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
```

3. Для отработки созданного скрипта во время загрузки виртуальной машины `server` в конфигурационном файле `Vagrantfile` необходимо добавить в разделе конфигурации для сервера:

```
server.vm.provision "server firewall",
   type: "shell",
   preserve_order: true,
   path: "provision/server/firewall.sh"
```

7.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
   - скриншоты (снимки экрана), фиксирующие выполнение работы;
   - подробное описание настроек служб в соответствии с заданием;
   - полные тексты конфигурационных файлов настраиваемых в работе служб;
   - результаты проверки корректности настроек служб в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

7.6. Контрольные вопросы

1. Где хранятся пользовательские файлы `firewalld`?
2. Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022?
3. Какая команда позволяет вам перечислить все службы, доступные в настоящее время на вашем сервере?
4. В чем разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading)?
5. Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу `ssh` по IP-адресу 10.0.0.10?
6. Какая команда используется для включения маскарадинга IP-пакетов для всех пакетов, выходящих в зону `public`?

При ответах на вопросы рекомендуется ознакомиться с информацией из источников [1—4].

Список литературы

1. NAT: вопросы и ответы. — URL: https://www.cisco.com/cisco/web/support/RU/9/92/92029_nat-faq.html.
2. Динамический брандмауэр с использованием FirewallD. — URL: https://fedoraproject.org/wiki/FirewallD/ru.
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). — ISBN 978-5-8459-1906-9.
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.