Практическая работа к занятию №6

# Трансляция адресов в ОС Linux

**Цель работы:** закрепить понимание принципов работы NAT и firewall, а также сформировать начальные навыки в конфигурировании NAT и Firewall на платформе и Linux;

**Требования:** установленная на компьютере среда виртуализации ORACLE Virtual Box с виртуальной машиной Linux Cent OS 7 (выполнять работу можно в любой ОС Linux, но все описания будут даваться для CentOS 7).

**Краткие теоретические сведения**

Linux сейчас является основной операционной системой для развертывания сервисов обработки данных. ОС Linux содержит необходимые средства для организации защищенного удаленного доступа и организации Интернет-шлюза.

NAT (Network Address Translation) – технология стека TCP\IP. Она позволяет модифицировать заголовки пересылаемых через NAT IP-пакетов и TCP\UDP сообщений.

NAT в общем случае представляет собой компьютер или аппаратный маршрутизатор, подключенный одним интерфейсом к внешней сети, а другими к внутренней. Оба интерфейса имеют IP адреса в каждой из сетей. Типичным применением NAT является обеспечение доступа из локальной сети с приватными IP-адресами к ресурсам внешней сети с IP-адресами интернет. При передаче запроса от локального клиента к внешнему ресурсу подменяется сокет отправителя: IP адрес меняется на внешний IP адрес NAT, а порт на свободный порт на внешнем интерфейсе NAT. Когда приходит ответ от внешнего ресурса, происходит обратная замена сокета и пакет передается в локальную сеть получателю. Так же с помощью NAT можно публиковать локальные сокеты на реальном IP адресе и реальном порту. Например, для обеспечения доступа извне к Web серверу, расположенному в локальной сети. В этом случае на NAT делается статическое отображение внешнего сокета на внутренний.

Под межсетевым экраном или брандмауэром понимают фильтр IP пакетов предназначенный для формального ограничения соединений клиентов и серверов работающих «поверх» стека TCP\IP.

В основу работы классического firewall положен контроль формальных признаков. В общем случае фильтрация осуществляется по:

- IP адресам отправителя и получателя в заголовке IP пакета
- номерам портов приложения-получателя и приложения-отправителя
- инкапсулированным в IP протоколам транспортного (TCP, UDP) и сетевого уровней (ICMP).

Правила фильтрации формируются в виде списка. Все проходящие пакеты проверяются по списку последовательно, до первого срабатывания. Последующие правила к пакету не применяются.

Для управления шлюзом используются различные инструменты управления брандмауэром Linux, такие как iptables, nftables и firewalld.

В CentOS 7 используется firewalld. Однако, все еще самым распространенным является iptables.

Важно отметить, что для того, чтобы Linux начал пересылать пакеты из интерфейса в интерфейс надо чтобы в параметре ядра net.ipv4.conf.all.forwarding = 1. Установить его можно с помощью утилиты sysctl (файл /etc/sysctl.conf), или записью в конфигурационный файл в каталоге /proc.

В Linux для удаленного доступа к серверам используется протокол SSH (secure shell). Он создает шифрованное соединение между клиентом и сервером. Благодаря этой технологии может осуществляться удаленное управление компьютером.

Сервер ssh (openssh-server) устанавливается по умолчанию и выполняется службой sshd. Конфигурация сервера осуществляется в конфигурационном файле /etc/ssh/sshd_config.

С помощью ssh можно не только подключаться к удаленным хостам, но и получать доступ к другим сервисам и сетям через эти хосты. Например, можно опубликовать на локальном сокете любой удаленный сокет, доступный с ssh хоста, к которому осуществляется подключение.

ssh -L [LOCAL_IP:]LOCAL_PORT:DESTINATION:DESTINATION_PORT [USER@]SSH_SERVER

где:

- [LOCAL_IP:]LOCAL_PORT — IP-адрес и номер порта локального компьютера,
- DESTINATION:DESTINATION_PORT — IP или имя хоста и порт конечного компьютера,
- [USER@]SERVER_IP — удаленный пользователь SSH и IP-адрес сервера.

Для управления запуском и просмотра состояния сервиса используется системная утилита systemctl.

### Инструментальные средства:

| | |
|---|---|
| Утилиты: | sysctl systemctl ip ping tcpdump useradd ss netstat iptables iptables-save iptables-restore |
| Файлы: | /etc/ssh/sshd_config |
| Утилиты работы с текстом: | echo, grep, sed |
| Редакторы: | vi, nano |

### Порядок выполнения работы

Далее описан порядок выполнения работы. Пункты работы, результаты которых прямо или косвенно используются в отчете, помечены знаком **(!)**.

**Примечание:** вместо iptables можно выполнить работу на nftables.

### Часть 1. Подготовка и проверка конфигурации.

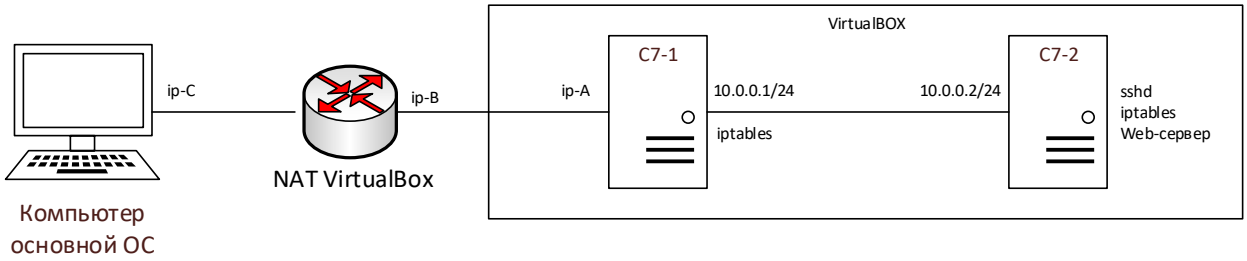
В VirtualBox:

1. Запустите виртуальную машину Linux. Удалите на хосте сервис firewalld.

   *Примечание: можно использовать утилиту systemctl. Для остановки сервиса используйте команду systemctl stop, для запуска systemctl start, для запрета автозапуска systemctl disable, для включения автозагрузки сервиса systemctl enable.*
2. Установите iptables (пакет называется iptables-services), настройте автозапуск iptables.
3. Сделайте связанный клон виртуальной машины. Одну машину назовите c7-1, другой c7-2
4. Для виртуальной машины c7-1 добавьте второй сетевой интерфейс.

5. Подключите сетевой интерфейс c7-2 и новый сетевой интерфейс c7-1 к внутренней сети intnet.
6. Подключите исходный сетевой интерфейс c7-1 к NAT.
7. Для внутренней сети задайте для машин c7-1 и c7-2 адреса 10.0.0.1 и 10.0.0.2 с маской 255.255.255.0.
8. Для исходного интерфейса c7-1 оставьте получение адреса автоматически от dhcp сервара VirtualBox
9. Для обоих хостов отключите использование ipv6.
10. Задайте имена хостов, советующие именам виртуальных машин. Изменить имя хоста можно изменить с помощью утилиты hostnamectl
11. Проверьте доступность хостов по внутренней сети и доступность внешней сети на хосте c7-1.
12. Убедитесь, что на c7-2 в качестве шлюза по умолчанию задан адрес c7-1.
13. В качестве адреса DNS сервера на c7-2 указать адрес 8.8.8.8 и 77.88.8.1
14. Убедитесь, что на машине c7-1 параметры ядра позволяют передавать сетевые пакеты между сетевыми интерфейсами.

Должна получиться следующая схема:




## Часть 2. Создание пользователей и настройка OpenSSH Server (sshd).

1. На хосте c7-2 создайте пользователя с именем FIOuser, где FIO – ваши инициалы.
2. Редактируя файл /etc/ssh/sshd_config, настройте ssh сервер так, чтобы **(!)**:
    a. Пользователю root нельзя было бы входить по ssh
    b. Количество попыток ввода неверного пароля = 2
    c. Время ожидания авторизации = 30 секундам.
    d. Отключить определение имен хостов по DNS
3. После изменения конфигурации перезапустите сервис sshd.
4. С машины c7-1 подключитесь к c7-2 по ssh, используя новую учетную запись.

## Часть 3. Настройка NAT на шлюзе

1. На хосте c7-1 разрешите передачу IP пакетов между интерфейсами.
2. Настройте на хосте клиентский NAT (действие SNAT или MASQUERADE), так чтобы внешняя сеть стала доступна из внутренней сети.
3. Настройте публикацию порта tcp\22 на хосте c7-2 на порту tcp\55022 на внешнем сетевом интерфейсе c7-1.
4. Используя утилиту iptables-save выведите автоматически созданные правила в текстовый файл

/etc/sysconfig/iptables . Определите назначение каждой строки.

5. Подключитесь к ssh серверу на c7-2 с вашей реальной операционной системы (предварительно настройте публикацию портов в NAT в VirtualBox).
6. Проверьте командой ping с хоста c7-2 доступность любого работающего сервиса в Интернет (например адреса 8.8.8.8 или 77.88.8.1). Если хост недоступен, а подключение в п.5 удалось установить, то отредактируйте файл /etc/sysconfig/iptables, изменив правила так, чтобы запросы утилиты ping проходили. Для применения правил можно просто перезапустить сервис (systemctl reload или restart). Корректнее использовать iptables-restore (текущие соединения не сбрасываются).

### Часть 4. Установка дополнительного ПО

1. На хосте c7-1 установите консольный броузер (lynx или links) и утилиту nmap.
2. На хосте c7-2 установите Web-сервер lighttpd, запустите его и разрешите автоматический запуск. Определите на каком сокете запускается сервер. Если по умолчанию он стартует на сокете ipv6, то измените конфигурационный файл Web-сервера, так, чтобы сервер запускался на ipv4.
3. С хоста c7-1 с помощью утилиты nmap проверьте какие порты открыты на хосте c7-2 **(!)**.
4. На хосте c7-1 с помощью консольного броузера попробуйте открыть сайт на 10.0.0.2. Если сайт не отрывается, отредактируйте правила iptables, так, чтобы доступ к web-серверу был разрешен. Проверьте, что доступ появился.

### Часть 5. Исследование соединений

1. На хосте c7-2 с помощью команд ss, netstat и lsof (любой из команд) выведите на консоль информацию о **(!)**:
    a. Открытых соединениях.
    b. Открытых сетевых сокетах, ждущих подключение.
2. На машине c7-1 с помощью утилиты tcpdump выведите на разных консолях трафик с внутреннего и внешнего интерфейса, так чтобы отображались адреса отправителя и получателя, номера портов отправителя и получателя,
3. Запустите с хоста c7-2 передачу 5 TCP сегментов до хоста ya.ru с помощью утилиты mtr.
4. Наблюдая за консольными выводами tcpdump определите, как были изменены исходящие сообщения при трансляции адресов **(!)**.
5. Закройте все ssh сессии с машиной c7-2
6. На машине c7-2 запустите с помощью утилиты tcpdump выведите консоль трафик, так чтобы отображались адреса отправителя и получателя, номера портов отправителя и получателя и флаги tcp **(!)**.
7. Подключитесь с основной операционной системы к хосту c7-2 по ssh.
8. Определите какие флаги использовались при установлении соединения, как менялось значение полей ack и syn после начала передачи данных **(!)**.

**Примечание:** значения флагов в выводе tcpdump следующие [.] - ACK (Acknowledgment), [S] - SYN (Start Connection); [P] - PSH (Push Data); [F] - FIN (Finish Connection); [R] - RST (Reset Connection); [S.] - SYN-ACK (SynAcK Packet)

### Часть 6. Настройка шлюза

1. Задайте политики по умолчанию для цепочек INPUT и FORWARD – запрет передачи.
2. Добавьте правила, которые бы
    a. Разрешали подключение к опубликованному порту ssh сервера c7-2 из IP сети реального хоста
    b. Разрешили подключение из внутренней сети к DNS только на 8.8.8.8 и 77.88.8.1
    c. Разрешали доступ из внутренней сети к протоколам POP3 (tcp 110), Web (tcp 80, 443, 8080), ssh (tcp 22).
    d. Разрешили доступ к сервисам SMTP (tcp 25) на любом хосте сети вашего основного компьютера.
    e. Запрещают любой трафик с хостов 192.56.0.11 и с подсети 14.12.44.0/18 как непосредственно на машину c7-1, так и во внутреннюю сеть.
    f. Запрещают доступ к ssh серверу на c7-1 из внешней сети.
    g. Разрешает доступ к ssh серверу на c7-1 из внутренней сети.
    h. Разрешает icmp эхо запросы из внутренней сети наружу только на хост 8.8.8.8
    i. Запрещает хосту c7-1 давать icmp эхо ответы, но при этом сохраняет возможность с самого хоста c7-1 делать icmp это запросы и получать на них ответы.

### Часть 7. Доступ через ssh к защищенным сервисам

1. Используя возможности протокола ssh сделайте так, чтобы на основном компьютере Web-сервер с хоста c7-2 был доступен по адресу 127.0.0.80:8888.

### Содержание отчета

Требуется подготовить отчеты в формате DOC\DOCX или PDF. Отчет содержит титульный лист, артефакты выполнения и ответы на вопросы и задания.

Артефакты:

1. Измененные параметры sshd из Части 2.
2. Итоговые файлы /etc/sysconfig/iptables с хостов c7-1 и c7-2
3. Команду и консольный вывод из Части 4 п.3

4. Команды и существенные части консольного вывода Части 5, п. 1,4,6,8
5. Текст итоговых правил iptables с с7-1.
6. Команду подключения из Части 7, п.1.

Вопросы и задания:

1. В чем разница между действиями SNAT или MASQUERADE? Когда уместно использовать одно, а когда другое?
1. Какие цепочки и какие таблицы существуют в iptables по умолчанию?
2. Как добавить новую цепочку? Как перенаправить в нее трафик?
3. Имеет ли смысл порядок правил?
4. Как с помощью iptables можно реализовать настройки, при которых брандмауэр пропускает пакеты тех соединений, которые были инициированы изнутри. Учтите, что правило позволяло установить соединение, т.е. передать пакеты наружу, так и получать ответы, то есть принять ответные пакеты.

Отчет выслать в течение 4-х недель на адрес edu-net@yandex.ru.

В теме письма: №группы ФИО (латинскими буквами) №работы (например: 5555 Fedor Sumkin 6)

**Поддержка работы**

Дополнительные материалы по теме курса публикуются на Telegram-канале ITSMDao (t.me/itsmdao). Обсуждать работу и задавать вопросы можно в чате ITSMDaoChat (t.me/itsmdaochat).