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 CentOS 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. Для управления им служит утилита firewall-cmd.

Важно отметить, что для того чтобы Linux начал пересылать пакеты из интерфейса в интерфейс надо чтобы в параметре ядра net.ipv4.ip_forward = 1. Установить его можно с помощью утилиты sysctl, 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.

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

Инструментальные средства:

Утилиты:	sysctl firewall-cmd systemctl ip ping tcpdump useradd ss netstat lsof
Файлы:	/etc/ssh/sshd_config
Утилиты работы с текстом:	echo, grep, sed
Редакторы:	vi, nano

Порядок выполнения работы

Часть 1. Подготовка и проверка конфигурации.

В VirtualBox:

1. Сделайте связанный клон виртуальной машины. Одну машину назовите c7-1, другой c7-2
2. Для виртуальной машины c7-1 добавьте второй сетевой интерфейс.
3. Подключите сетевой интерфейс c7-2 и новый сетевой интерфейс c7-1 к внутренней сети intnet.
4. Подключите исходный сетевой интерфейс c7-1 к NAT.

В Linux :

5. 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.
6. Для исходного интерфейса c7-1 оставьте получение адреса автоматически от dhcp сервара VirtualBox
7. Для обоих хостов отключите использование ipv6.
8. Задайте имена хостов, советующие именам виртуальных машин.
9. Проверьте доступность хостов по внутренней сети и доступность внешней сети на хосте c7-1.
10. Убедитесь, что на c7-2 в качестве шлюза по умолчанию задан адрес c7-1.

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 перезапуска выведите на консоль состояние сервиса sshd и его журнал средствами system (утилита systemctl).
4. С машины c7-1 подключитесь к c7-2 по ssh, используя новую учетную запись.

Часть 3. Настройка шлюза

Цель этой части – настроить хост c7-1 как шлюз доступа к хосту c7-2, осуществляющий трансляцию адресов.

1. Включите на хосте c7-1 пересылку пакетов через ядро с помощью утилиты sysctl.
2. С помощью утилиты firewall-cmd настройте c7-1 так, чтобы:
    a. Запросы от c7-2 транслировались во внешнюю сеть
    b. На порту с номером 55022 внешнего сетевого интерфейса c7-1 был опубликован порт 22 на хосте c7-2.
3. Подключитесь к серверу c7-2 с вашей реальной операционной системы (используйте публикацию портов в NAT в VirtualBox или Сетевой Мост).
4. С помощью команды who выведите список пользователей на хосте c7-2.

Часть 4. Исследование соединений

1. На хосте c7-2 с помощью команд ss, netstat и lsof (с помощью каждой 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)