Практическая работа №7

Конфигурирование межсетевого экрана и NAT

Цель: Сформировать понимание принципов работы NAT и firewall, а так же начальные навыки в конфигурировании NAT и Firewall на платформе Windows (routing and remote access service) и Linux (iptables).

Необходимо:

1) Установленная на компьютере среда виртуализации ORACLE Virtual Box
2) Образы виртуальных жёстких дисков операционных систем Windows 2003 и Linux
3) Доступ к сети Интернет
4) Учетные записи пользователей с администраторскими правами

Краткие теоретические сведения:

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 полкучателю. 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 конфигурирования firewall в Linux необходимо сформировать набор правил iptables. В iptables реализовано несколько таблиц (filter, nat и т.д.). Каждая таблица содержит набор цепочек правил. Например цепочки INPUT для входящего трафика, OUTPUT для исходящего, FORWARD для пересылаемого, PREROUTING для обработки трафика перед пересылкой и т.д.. Набор цепочек для разных таблиц различен. Управление цепочками производится с помощью консольной команды iptables.

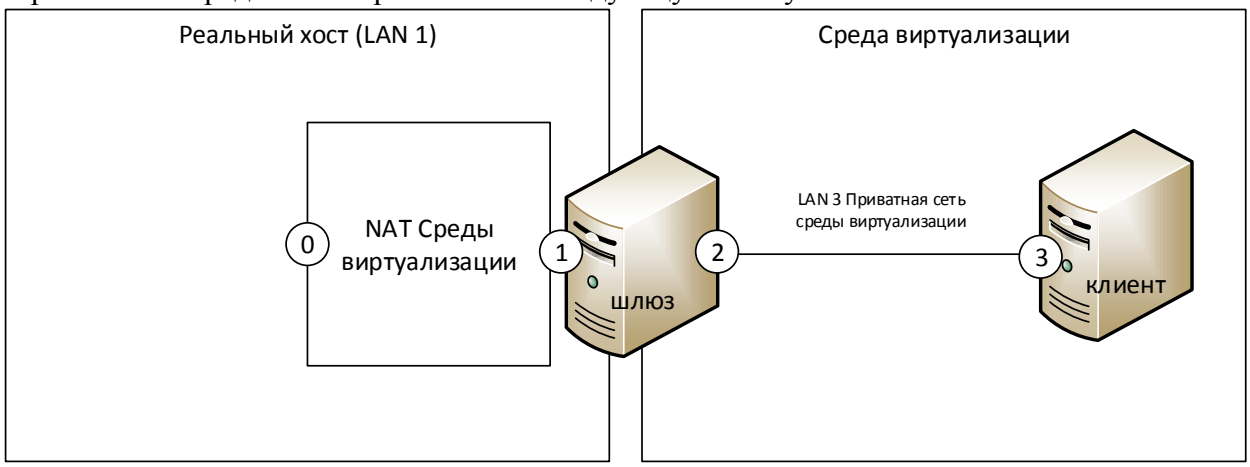
Примеры:

- iptables -t filter -A INPUT -s ws.mytrust.ru -j ACCEPT включает прием всех пакетов с хоста ws.mytrust.ru
- iptables -t filter -A OUTPUT -d mail.ifmo.ru --dport 25 -j DROP запрещает отправку всех пакетов на хост mail.ifmo.ru на порт 25
- iptables -t filter -A INPUT -j DROP запрещает прием всех сообщений

В протоколах TCP и UDP (семейства TCP/IP) порт — идентифицируемый номером системный ресурс, выделяемый приложению, выполняемому на некотором сетевом хосте, для связи с приложениями, выполняемыми на других сетевых хостах (в том числе с другими приложениями на этом же хосте).
На платформе Windows Server NAT настраивается с помощью службы Routing and Remote Access. В Windows 2003 в консоли этой службы можно настроить и правила фильтрации для передаваемого трафика. Для защиты конечных хостов в Windows служит отдельная служба windows firewall. Запуск этих служб на windows 2003 одновременно невозможен. В старших версиях Windows существует отдельный общий firewall – advfirewall, для всех случаев.
На платформе Linux и для настройки NAT и для фильтрации трафика используется iptables. Управление iptables осуществляется или из командной строки (см. выше) или через конфигурационный файл /etc/sysconfig/iptables (для CentOS и др. дистрибутивов семейства RedHat). 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.

Порядок выполнения работы:

В работе вам предлагается реализовать следующую схему:



1) В среде виртуализации будет запущен клиент (Windows 2003) и шлюз (Windows 2003 или Linux Centos).
2) Между Клиентом и шлюзом следует организовать приватную сеть с адресом 10.0.0.0 и маской 255.0.0.0. Из этой сети назначаются адреса для интерфейсов 2 и 3.
3) Адрес на интерфейсе 1 назначается автоматически средой виртуализации.
4) Интерфейс 0 - адрес хоста виртуализации (реального компьютера).

Часть 1: Платформа Windows.

1) Настройте средствами среды виртуализации приватную сеть между хостами. На клиенте укажите шлюз равный адресу шлюза (интерфейс 2) и DNS = адресу DNS на реальном хосте.
2) Настройте автоматическое получение ip-адресов на интерфейсе 1.
3) Настройте на шлюзе клиентский NAT с помощью мастера службы Routing and Remote Access.
4) Убедитесь в доступности внешней сети с клиента (в случае необходимости использования proxy не забудьте указать его в параметрах браузера).
5) С помощью firewall консоли Routing and Remote Access запретите передачу данных между приватной сетью и хостом de.ifmo.ru (учтите, что при проверке через

браузер вы можете работать с proxy сервером, а не напрямую с de.ifmo.ru. Работа же по протоколу ICMP идет напрямую).

6) На клиенте ознакомитесь с назначением параметрами утилит netstat, sc и netsh с дерективами firewall и diag.
7) Создать на клиенте скрипт, который:
    - включает автоматическую загрузка Брандмауэра Windows
    - запускает брандмауэр
    - включает протоколирование входящих соединений
    - настраивает службу Telnet на ручной запуск
    - добавляет правило, разрешающее доступ с IP адресов сети компьютерного класса к службе Telnet
    - разрешает системе отвечать на запросы echo-request ICMP
    - запускает службу Telnet
8) На шлюзе опубликуйте порт службы Telnet на клиенте.
9) Запустить сеанс Telnet из реального компьютера в гостевую ОС. Войдите в систему. (Предварительно следует настроить публикацию соответствующего порта через NAT в свойствах системы виртуализации).
10) На клиенте вывести на экран данные только об установленных соединениях со службой Telnet, с указанием IP адресов и портов в численной форме.

Часть 2: Платформа Linux

1) Используя в качестве платформы шлюза Linux CentOS, настройте средствами среды виртуализации приватную сеть между хостами. На клиенте укажите шлюз равный адресу шлюза (интерфейс 2) и DNS = адресу DNS на реальном хосте.
2) Настройте автоматическое получение ip-адресов на интерфейсе 1. (Используйте для конфигурации интерфейсов скрипты /etc/sysconfig/network-scripts/ifcfg-ethX где X номер интерфейса). Для получения информации об интерфейсах используйте ifconfig.
3) Включите пересылку пакетов IP v 4 в ядре.
4) Ознакомитесь с таблицами nat и filter системы iptables и цепочками этих таблиц. Уясните порядок обработки пакетов по цепочкам.
5) С помощью скрипта /etc/sysconfig/iptables настройте клиентский NAT и публикацию порта telnet клиента на порту № 2222.
6) Запретите передачу данных между приватной сетью и хостом de.ifmo.ru
7) На клиенте убедитесь в доступности внешних ресурсов и недоступности хоста de.ifmo.ru
8) Запустить сеанс Telnet из реального компьютера в гостевую ОС. Войдите в систему. (Предварительно следует настроить публикацию соответствующего порта через NAT в свойствах системы виртуализации).
9) На шлюзе реализуйте следующую политику доступа:

- Должен быть доступен DNS сервер с адресом, равным DNS на реальном компьютере (определить и установить вручную).
- Должны быть не доступны все наружные Web сервера
- Должен быть доступен и HTTP прокси с адресом proxy.ifmo.ru
- Должен быть доступен FTP сервер ftp.ifmo.ru,
- Должны быть доступны все наружные POP3 сервера
- Должен быть доступен SMTP сервер mail.ifmo.ru,
- Со всех узлов подсети 83.0.0.0/16 должен быть доступен SSH сервер на компьютере – шлюзе.
- Отдельно должен быть заблокирован доступ к шлюзу и к внутренней сети с хоста 10.10.11.173
- Шлюз не должен отвечать на запросы команды PING с внутренней сети.

- Работа с остальными сервисами должна быть блокирована

В отчет:

В отчет представить

1) Вывод конфигурации Routing And Remote Access средствами команды netsh,
2) Скрипт из п.7 части 1.
3) Консольный вывод п.10 части 1
4) Файл /etc/sysconfig/iptables или результат выполнения команды Iptables-save