Лабораторная работа: ACLs, NAT, PAT

Цели

Получение практического навыка по построению защищенной сети, изучение принципов работы стека TCP/IP, развитие практических навыков работы с командами сетевого администрирования ОС Microsoft Windows.

Задачи

- Создать начальную конфигурацию маршрутизатора, необходимую для удаленного администрирования (с помощью протокола telnet или ssh).
- Создавать стандартный и расширенный списки доступа.
- Создать статический NAT, создать PAT.

Оборудование

Router 1605, Switch Catalyst 2960 (для выполнения достаточно одного маршрутизатора и двух портов коммутатора). Допускается также использование эмулятора GNS3.

Предварительная настройка

- Маршрутизатор должен иметь нулевую конфигурацию.
- Коммутатор должен быть настроен для удаленного доступа к нему из локальной сети класса.
- Один компьютер класса (например, компьютер преподавателя, этот компьютер мы будем называть "выделенным") должен быть подключен к порту коммутатора. Этот порт должен находиться в другом VLAN, не в том в котором находится порт, подключенный к локальной сети.

Время выполнения

1 пара

Параметры выставления оценок

Пункты задания, выделенные зеленым цветом, предполагают или некоторое исследование со стороны студента или проверяют то, насколько хорошо студент осознал проделанное. Например, некоторые пункты невозможно выполнить без настройки таблиц маршрутизации на компьютерах, о чем в самом задании ничего не говорится. Студент должен найти проблему и решить ее самостоятельно. Так же студент при демонстрации правильности работы NAT/PAT должен продемонстрировать навыки работы с Ethereal. Потому работа должна оцениваться по нижеприведённым позициям.

- Общее ориентирование в круге вопросов. Стек TCP/IP (IP адреса, порты TCP), технология NAT/PAT, маршрутизация.
- Навыки работы с административными командами и Ethereal.
- Способность быстро ориентироваться и находить решения.
- Дополнительные вопросы и беседа.

Ход работы

1. С помощью консольного порта настройте маршрутизатор так, чтобы на него можно было зайти удаленно по протоколу telnet.

На маршрутизатор можно попасть через консольный интерфейс по протоколу RS-232. Для этого можно использовать программу PuTTy или HyperTerminal (Programs|Accessories|Communications|). Настройки RS-232 протокола: bits per second 9600, data bits 8, parity none, stop bits 1. Для того чтобы можно было зайти на маршрутизатор cisco по протоколу telnet, необходимо выполнить нижеприведённые пункты.

a) Настроить IP-адрес на интерфейсе Ethernet 0 (в режиме конфигурации интерфейса).

ip address *ip_address mask*

b) Включить интерфейс (в режиме конфигурации интерфейса).

no shu
exit

c) Настроить пароль для входа через telnet (в режиме конфигурации).

line vty 0 4
pass *password*
exit

d) Настроить пароль для входа в привилегированный режим (в режиме конфигурации).

enable secret *password*

2. Установите telnet сессию.

После установления telnet сессии, если были правильно выполнены предыдущие настройки, маршуртизатор потребует введение пароля. Надо ввести пароль, который был сконфигурирован на line vty.

a) Далее для входа в привилегированный режим введите команду.

enable

b) Введите пароль, который был сконфигурирован ранее.

3. Настройте логический интерфейс с произвольным ip адресом и "хостовой" маской (в подсети может быть только один IP-адрес).

Для этого в режиме конфигурации выполняются следующие команды.

interface loopback 0
ip address *ip_address mask*
exit

4. Выйдите из telnet сессии – последовательно команды.

exit
exit

5. Попытайтесь "попасть телнетом" на логический интерфейс маршрутизатора.

Почему получили такой результат? Сделайте так, чтобы команда выполнялась успешно.

6. Создайте список доступа, пропускающий только пакеты с source ip адрес вашего компьютера.

Для этого можно использовать так называемый "стандартный" список доступа. Для создания такого списка в режиме конфигурации выполняются следующие команды.

access-list *number* permit | deny {any} | {host ip_adrress_host } | {ip_address_host} | { ip_address_network invert_mask }

number – номер списка доступа (1-99).
permit – разрешение
deny – запрещение
ip_adrress_host – IP адрес хоста
ip_address_network – идентификатор сети.
invert_mask – инвертированная маска
| - или
{} – группирует команды

Эти команды вводятся последовательно, и обрабатываются процессором последовательно сверху вниз. Если в конце нет явного permit any, то все пакеты, для которых не нашлось соответствия в списке, уничтожаются.

Пример (разрешает пакеты с хостов **1.1.1.1**, **2.2.2.2**, запрещает из сетки **3.0.0.0 255.0.0.0**, разрешает все остальные, **log** – включение "журналирования" для данной строчки).

access-list 1 permit 1.1.1.1
access-list 1 permit host 2.2.2.2
access-list 1 deny 3.0.0.0 0.0.0.255
accee-list 1 permit any log

7. Поставить список доступа на интерфейс.

Список доступа может быть поставлен на **in** или на **out**. Для маршрутизатора **in** – это то, что входит в маршрутизатор, **out** – то, что выходит из него.

Команда в режиме конфигурирования интерфейса:

ip access-group number in | out

number – номер списка доступа.

Если все сделано правильно – сессия telnet не должна прерваться. Если прервалась – студент должен использовать консоль, чтобы найти ошибку и поправить. Для этого используются, например, следующие диагностические команды в привилегированном режиме.

sh run
sh access-list number
sh inter e 0
sh ip inter e 0
term mon
term nomon
deb ip packet
no deb all

Если не получилось понять, в чем ошибка или непонятна диагностика – обратитесь к преподавателю. После выполнения – покажите преподавателю.

8. Студент создает список доступа позволяющий делать только telnet, только на interface loopback 0 (сконфигурированный ранее) и только с его компьютера. При этом предполагается, что telnet сессия установлена на интерфейс loopback 0.

Для этого используется список доступа, называемый “расширенным”. Такой список доступа позволяет при фильтрации использовать не только IP-адрес источника, но так же и IP-адрес получателя и информацию четвёртого уровня – номера TCP/UDP портов, флаги протокола TCP. Для расширенного списка доступа используются номера от 100 до 199 или можно создавать именованные списки доступа. Пример (в режиме конфигурации) представлен ниже.

```
ip access-list extend 100
permit ip 1.1.1.1 0.0.0.0 192.168.5.0 0.0.0.255
permit tcp host 2.2.2.2 host 192.168.5.1 0.0.0.0 eq 80
deny ip any host 192.168.5.1 eq 139
deny udp any any eq rip
permit ip any any log
```

При написании команды пользуйтесь командой “?”.

9. Поставьте этот список доступа на interface e 0 на in. Если все сделано правильно, telnet сессия не должна быть прервана. Если прервалась – пользуйтесь консолью для выявления и исправление ошибки.

a) Проверьте, что с другим ip адресом telnet “не проходит”.
b) Проверьте, что ping “не проходит”.
c) Проверьте, что telnet на Ethernet 0 не проходит.
d) Покажите преподавателю.

10. Все списки доступа удаляются.

Все сконфигурированные строчки удаляются введением той же самой команды с префиксом “no ”.

11. Студент узнает у преподавателя адрес коммутатора и пароли. Заходит на него с помощью telnet.

Входит в привилегированный режим (пароль – у преподавателя).

12. Настройте другой Ethernet порт (Ethernet1) маршрутизатора.

Он должен быть в той же сети, что и выделенный (см. “предварительные настройки”) компьютер (узнайте у преподавателя).

13. Подключите этот порт маршрутизатора к коммутатору. Добейтесь того, чтобы команда ping с маршрутизатора на IP-адрес выделенного компьютера выполнилась успешно.

a) На коммутаторе нужно правильно настроить порт.
b) Предложите алгоритм действий. Если алгоритм правильный, преподаватель подскажет команды, которые необходимо ввести.
c) После выполнения этого пункта мы должны получить следующую топологию сети. Два интерфейса маршрутизатора смотрят в разные локальные сегменты. В одном сегменте находится компьютер студента (и вся локальная сеть), в другом - компьютер преподавателя.

14. Настройте статический NAT таким образом, чтобы вы могли выполнить telnet соединение с открытым TCP-портом на “выделенном” компьютере (компьютере преподавателя), таким образом, чтобы на “выделенный” компьютер приходили пакеты с IP-адресом источника – IP-адресом логического интерфейса маршрутизатора.

a) Для этого надо определить, какой локальный сегмент считать внутренним, какой внешним. На том интерфейсе, который “смотрит” во внутренний сегмент надо прописать команду.
```
ip nat inside
```
b) На том интерфейсе, который “смотрит” во внешний сегмент надо прописать команду.
```
ip nat outside
```
c) Для настройки статического NAT надо выполнить команду.
```
ip nat inside source static inside_local_address inside_global_address
```

Пользуйтесь командой “?”.

15. Добейтесь результата. На компьютере преподавателя продемонстрируйте, что пакеты действительно приходят с IP-адреса loopback.

При выполнении этого пункта вам, возможно, придется менять некоторые настройки и на компьютере преподавателя.

16. Настройте PAT таким образом, чтобы вся локальная сеть класса имела доступ по telnet к открытому TCP-порту “выделенного” компьютера.

a) Сначала удалите команду статического NAT.
b) Создайте список доступа, в котором укажите какие IP-адреса разрешено “патить”.
c) В режиме конфигурации введите нижеприведённую команду.
```
ip nat inside source list number interface loopback 0 overload
```

17. Продемонстрируйте преподавателю, что все работает правильно.