

Настройка NAT/PAT на пограничном Cisco ASA

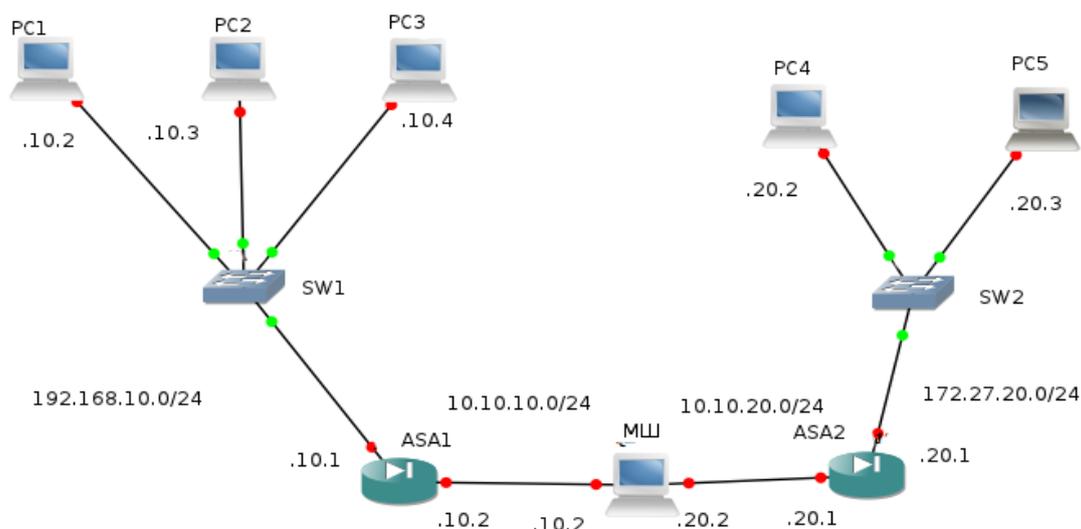
Практическая часть

Цель работы

Изучение технологии NAT/PAT инфраструктуры открытых ключей PKI и получение навыков настройки NAT/PAT на пограничных устройствах Cisco ASA, обеспечив доступ во внешнюю сеть к *http*-серверу.

Схема лабораторной работы

На рисунке показана схема, которую вы должны будете исследовать в процессе выполнения лабораторной работы.



Задание и порядок выполнения работы

Задание А Самостоятельная работа.

- 1) Соберите физическую схему сети, представленную на рисунке.
- 2) Выполните базовую настройку оборудования сети. Запустите *http* сервера на компьютерах для проверки соединений.
- 3) Настройте Dynamic PAT на ASA #2 и проверьте его работу.
- 4) Выполните проброс портов для одной из PC в сети за ASA #2.
- 5) Настройте NAT с пулом адресов на ASA #1 и проверьте его работу.
- 6) Настройте identity NAT на ASA #1 и проверьте его работу.
- 7) Настройте статическую маршрутизацию для одной из PC за ASA #1.
- 8) Сделайте выводы по исследованной вами работе.

Список используемых команд

Таблица 1 - Команды Arch Linux рабочих станций

Синтаксис	Описание
ifconfig <имя интерфейса> <ip адрес> netmask <маска сети> [up/down]	Без параметров команда показывает список работающих интерфейсов Служит для настройки параметров интерфейса
route add/del [-net -host] [default] target [gw]	Без параметров команда выводит таблицу

[netmask] [[dev] If]	маршрутизации Служит для настройки статической маршрутизации.
/etc/rc.d/<имя сервиса>	Служит для запуска программ-демонов в ОС linux
lynx <ip/имя>	Консольный браузер
tcpdump [-XX] [-i интерфейс]	Сниффер пакетов. Без параметров слушает все интерфейсы и показывает только заголовки пакетов

Таблица 2 - Команды Cisco ASA

Синтаксис	Описание
en	Вход в привилегированный режим
configure terminal	Вход в режим конфигурации
sh <сервис>	Просмотр настроек
dhcp address <пул адресов> <интерфейс>	Настройка dhcp сервера на интерфейсе
int <имя интерфейса>	Вход в режим конфигурации интерфейса
nameif <имя>	Настройка имени интерфейса
security-level <значение>	Настройка параметра защищенности сети
ip address <значение> <маска>	Настройка адреса интерфейса
switchport access <имя vlan>	Размещение интерфейса в указанной vlan
route <имя интерфейса> <сеть> <маска> <адрес шлюза>	Настройка статической маршрутизации
nat (<интерфейс>) <номер правила> <сеть> <маска>	Настройка NAT\PAT для замещения адреса из сети указанного интерфейса
access-list <имя\номер> [permit\deny] extended <тип трафика> <источник> <маска> <цель> <маска>	Создание списка доступа для выделения необходимого трафика.
static (inside,outside) <тип трафика> <внешний ip> <порт> <внутренний ip> <порт> netmask <маска>	Создание статического маршрута. Здесь (inside,outside) указывает направление трафика. Всегда проверяйте созданный статический маршрут после его описания.
access-group <имя ACL> <in/out> interface <имя>	Применение ACL на интерфейсе.
global (<имя>) <номер> <пул адресов>	Определяет пул внешних адресов на внешнем интерфейсе. Номер 0 для Identity NAT. Остальные – для обычного. Строка interface в поле пула адресов означает замену внутренних адресов на адрес внешнего интерфейса с применением PAT.
sh xlate detail	Просмотр соответствий адресов.

clear xlate	Очистка созданных соответствий
--------------------	--------------------------------

Задание В Самостоятельная работа с указаниями пошагового выполнения.

- 1) Соберите физическую схему сети, изображенную на рисунке.
- 2) Выполните базовую настройку оборудования:
 - 2.1) Пропишите ip-адреса на всех PC и сетевых устройствах, включив их в указанные *vlan* и прописав статическую маршрутизацию.
 - 2.2) Запустите на PC, с которыми будет проводиться проверка соединения, *http*-сервера.
 - 2.3) Проверьте соединение всех рабочих станций с сервером, расположенным на роутере.
 - 2.4) Изучите передаваемый трафик, запустив сниффер на роутере.
- 3) Настройте Динамиче PAT на ASA #2 и проверьте его работу.
 - 3.1) Отключите стандартную трансляцию адресов *nat*
 - 3.2) Укажите внутреннюю сеть 172.27.20.0/24 в качестве внутренней для трансляции адресов *nat*
 - 3.3) Соединитесь с роутером с рабочих станций, расположенных внутри сети.
 - 3.4) Изучите передаваемые заголовки при помощи сниффера.
- 4) Выполните проброс портов для одной из PC в сети за ASA #2
 - 4.1) Настройте проброс портов для одной из PC внутри сети для *http* трафика.
 - 4.2) Соединитесь с этой PC с маршрутизатора.
- 5) Настройте NAT с пулом адресов на ASA #1 и проверьте его работу.
 - 5.1) Отключите PAT на внешнем интерфейсе (трансляцию внутренних адресов в один глобальный адрес).
 - 5.2) Опишите пул из двух адресов на внешнем интерфейсе.
 - 5.3) Настройте список доступа, разрешающий ICMP трафик во внутреннюю сеть извне и примените его на внешнем интерфейсе.
 - 5.4) Пропингуйте роутер с трёх PC. Проанализируйте результаты.
 - 5.5) Пропингуйте одну из внутренних PC с роутера, используя IP, который обнаружен с помощью *tcpdump*.
 - 5.6) Отключите стандартное определение NAT за внешним интерфейсом.
- 6) Настройте identity NAT на ASA #1 и проверьте его работу.
 - 6.1) Настройте Identity NAT для внутренней сети (это *nat*, у которого номер правила - 0).
 - 6.2) Попробуйте снова пропинговать сначала роутер, а затем внутреннюю PC по обратному адресу. Сделайте выводы.
 - 6.3) Снова верните прежние настройки NAT.
- 7) Настройте статическую маршрутизацию для одной из PC за ASA #1.
 - 7.1) Очистите таблицу соответствия адресов.
 - 7.2) Настройте статический маршрут на одну из внутренних PC.
 - 7.3) Пропингуйте PC с роутера.
 - 7.4) Сбросьте настройки ASA Cisco.
- 8) Сделайте выводы по исследованной вами работе.

Задание С Самостоятельная работа пошагового выполнения задания В с ключевыми указаниями преподавателя.**Требования к оформлению лабораторной работы**

Отчет студента по проделанной работе оформляется в электронном и печатном виде и должен содержать:

- 1) титульный лист по принятой форме с название работы, ФИО студента,
- 2) цель работы, схему сети с обозначением всех сконфигурированных портов и интерфейсов,
- 3) последовательность выполнения всех действий, а именно:
 - введенные команды,
 - листинги команд с соответствующими комментариями,
 - скриншоты по каждому действию,
- 4) анализ и выводы по работе,
- 5) ответы на контрольные вопросы.

Контрольные вопросы

1. Опишите принцип работы NAT.
2. Опишите принцип работы PAT.
3. В каких случаях используется технология трансляции адресов?
4. Почему в пункте 5.8 не удалось пропинговать PC по обратному адресу?
5. Что такое технология Identity NAT?
6. В каких случаях используется статическая трансляция адресов?
7. Как технология PAT использует несколько внешних адресов?
8. Почему для возможности передачи ICMP трафика понадобился список доступа?
9. В каких случаях используется проброс портов (port-mapping)?
10. Какая трансляция адресов была задана в Cisco ASA по умолчанию?

Литература, источники

1. James Boney, Cisco IOS in a Nutshell, O`Reilly, 2010
2. David Hucaby, Cisco ASA, PIX, and FWSM firewall handbook, Cisco Press, 2008
3. <http://www.cisco.com/go/asa>
4. ru.wikipedia.org/wiki
5. www.archlinux.org/
6. www.linuxguide.it/command_line/linux_commands_ru.html