Настройка Site-to-Site VPN IPSec с технологией NAT-T
Практическая часть

Цель работы

В данной лабораторной работе необходимо настроить Site-to-Site VPN IPSec между двумя Cisco ASA 5505, обеспечив при этом доступ во внешнюю сеть к http-серверу.

Схема лабораторной работы

На данном рисунке приведена схема, которую вы должны исследовать в процессе выполнения лабораторной работы.

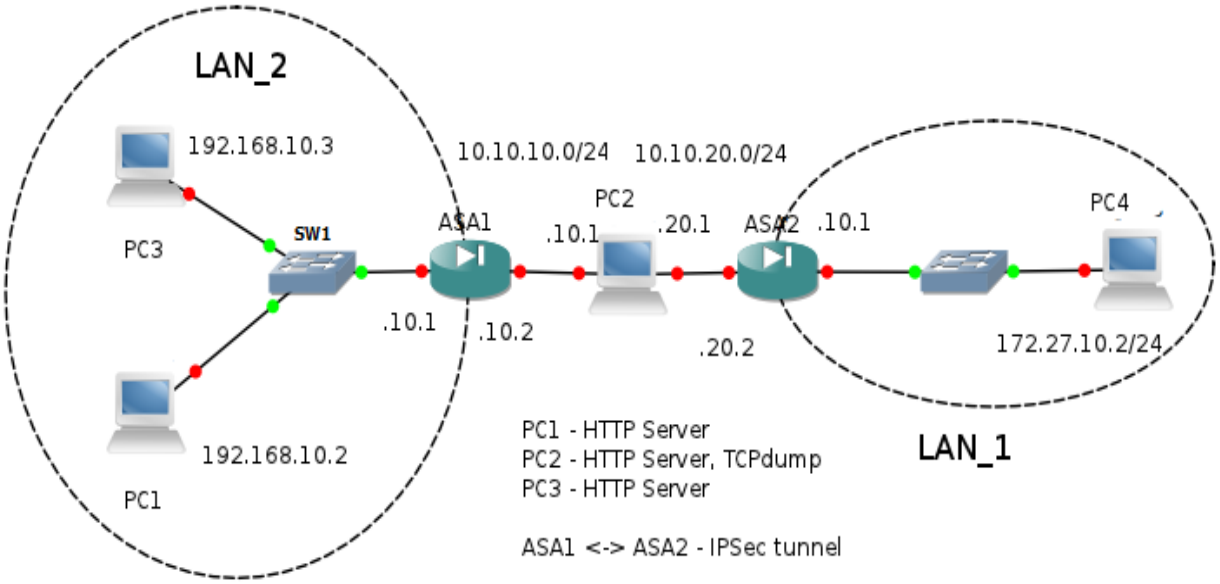

Рисунок 1 – Схема физической топологии сети

Задание и порядок выполнения работы

Задание А Самостоятельная работа.

1). Создайте IPSec туннель между двумя Cisco ASA.

2). Запустите сниффер на PC2 для изучения передаваемого траффика.

3). Запустите http сервер на PC1 для проверки IPSec соединения.

4). Настройте шифрование трафика от локальной сети LAN_1 к PC1, расположенной в локальной сети LAN 2.

5. Обеспечьте доступ всех PC к *http* серверу, расположенному на PC2.

6. Оформите отчет.

Список используемых команд

Таблица 1 - Команды 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] [netmask] [[dev] If]	Без параметров команда выводит таблицу 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
isakmp policy <номер> encryption <значение>	Выбор метода шифрования

isakmp policy <номер> hash <значение>	Выбор метода хеширования
isakmp policy <номер> authentication <значение>	Выбор метода аутентификации
isakmp policy <номер> group <значение>	Выбор группы Диффи-Хелмана
isakmp policy <номер> lifetime <значение>	Выбор lifetime соединения
isakmp enable <имя интерфейса>	Включение ISAKMP на интерфейсе
isakmp identity <значение>	Определение метода идентификации сторон
access-list <имя\номер> [permit\deny] extended <тип трафика> <источник> <маска> <цель> <маска>	Создание списка доступа для выделения необходимого трафика.
ipsec transform-set <имя> <значение>	Определение политики шифрования
map <имя> <номер> match address <список доступа>	Выделения трафика для шифрования
map <имя> <номер> set peer <ip>	Определение партнера
map <имя> <номер> set transform-set <имя>	Объединение настроек шифрования
map <имя> interface <имя>	Применение политики на интерфейсе
isakmp key <значение> address <ip>	Создание preshare ключа для партнера с заданным ip
static (inside,outside) <тип протокола> interface <внешний порт> <адрес назначения> <порт назначения> netmask 255.255.255.255	Проброс портов для доступа PC извне

Задание В Самостоятельная работа с указаниями пошагового выполнения.

1). Соберите физическую топологию сети, представленную на рисунке 1.

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 PC2.

2.4). Изучите передаваемый трафик, запустив на PC2 сниффер.

3). Выполните базовую настройку шифрования на ASA.

3.1). Настройте *isakmp*, указав методы шифрования, хеширования, аутентификации, группы Диффи-Хелмана, *lifetime* соединения и идентификации.

3.2). Включите функцию *isakmp* на внешнем интерфейсе.

3.3). Опишите список доступа, который будет выделять *http* трафик на PC4 для шифрования.

3.4). Настройте IPSec *transform-set.*

3.5). Объедините настройки шифрования IPSec и ACL в *policy map*, указав адрес соседней ASA.

3.6). Активируйте *policy map* на внешнем интерфейсе.

3.7). Задайте статичный *preshare*_ключ для соседней ASA.

3.8) Отключите NAT на интерфейсе по умолчанию.

3.9) Повторите настройку на соседней ASA.

4). Проверка соединения

4.1) Проверьте соединение PC4 с PC1 с помощью консольного браузера.

4.2) Изучите передаваемый трафик на рутере PC2.

4.3) Попробуйте соединиться с PC2.

5). Включение NAT\PAT.

5.1) Включите NAT на внутрених интерфейсах ASA

5.2) Пропишите статические маршруты (*port-mapping*) для доступа к PC, расположенным во внутренних сетях.

5.3) Добавьте внешние адреса ASA в ACL для шифрованного трафика.

5.4) Соединитесь с *http* сервером, расположенным на PC2.

5.5) Соединитесь с *http* сервером, расположенным за ASA.

6). Сбросьте конфигурацию.

Задание С Самостоятельная работа пошагового выполнения задания **В** ***с ключевыми указаниями преподавателя.***

Контрольные вопросы:

1. Что такое VPN?
2. Какие технологии создания VPN существуют?
3. Что такое IPSec?
4. В чем его преимущество перед другими протоколами?
5. Назовите основные режимы работы IPSec.
6. Почему IPSec в чистом виде не совместим с технологией NAT?
7. Опишите процедуру создания IPSec туннеля между двумя межсетевыми экранами.
8. Как возможно использовать IPSec вместе с NAT?
9. Что такое *lifetime* соединения IPSec?
10. Что такое ISAKMP?

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, топологию сети с обозначением всех сконфигурированных портов и интерфейсов,

3) последовательность пошагового выполнения всех действий в соответствии с заданием **В**, а именно:

- листинги команд с комментариями,
- скриншоты выполнения команд,

4) анализ и выводы по работе,

5) ответы на контрольные вопросы.

Литература, источники

1. James Boney, Cisco IOS in a Nutshell, O`Reilly, 2010
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2010

3. ru.wikipedia.org/wiki
4. www.archlinux.org/
5. www.linuxguide.it/command_line/linux_commands_ru.html