МИНИСТЕРСТВО ОБРАЗОВАНИЯ, КУЛЬТУРЫ И ИССЛЕДОВАНИЯ
РЕСПУБЛИКИ МОЛДОВА
БЕЛЬЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. «А. РУССО»
ФАКУЛЬТЕТ ТОЧНЫХ НАУК, ЭКОНОМИКИ И ОКРУЖАЮЩЕЙ СРЕДЫ
КАФЕДРЫ МАТЕМАТИКИ И ИНФОРМАТИКИ

ВИРТУАЛЬНЫЕ ПРИВАТНЫЕ СЕТИ. ПРИМЕНЕНИЕ VPN В CISCO PACKET TRACER.

РЕФЕРАТ

Автор:

Студент группы IS31Z

Валентин МИХАЙ

БЭЛЦЬ, 2020

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Темп развития информационных технологий растет с каждым днем. Одной из причин, которая обуславливает прогресс, является спрос потребителей.

Сегодня информация является важнейшим ресурсом во многих отраслях, который предполагает постоянный обмен между участниками сети одновременно с сохранением ее целостности и безопасности.

В роли сети передачи, как правило, выступают компьютерные сети. Спрос на такие сети значительно повлиял на их развитие и как следствие на ускорение передачи информации.

Одним из результатов прогресса компьютерных сетей стала VPN. Данная технология помогает решить проблему связи между сетями, которые физически находятся в разных местах, обеспечив достаточный уровень безопасности.

Таким образом дорогостоящие процедуры по объединению сетей по физическим каналам были оптимизированы.

1. ОСНОВНЫЕ ПРИНЦИПЫ РАБОТЫ VPN.

1.1. Основные понятия

Для того, чтобы разобраться в механизмах проектирования и применения VPN необходимо ввести ряд определений и понятий:

- *VPN*(Virtual Private Network) или “виртуальная частная сеть” - это логическая сеть, которая создана внутри другой, как правило общедоступной, сети, как правило, с применением средств шифрования информации[1].
- *Логическая сеть* - это сеть построенная независимо от физического расположения устройств и физической среды в общем - дополнительный уровень абстракции в сети.
- *Инкапсуляция протокола* - это процесс упаковки пакетов одного протокола в пакет другого протокола - расширение протокола, которое помогает реализовать новый уровень абстракции в сети(рис. №1).
- *Идентификация* - это процесс сравнения идентификатора сущности со списком существующих идентификаторов для определения ее наличия среди зарегистрированных объектов.
- *Аутентификация* - процесс проверки подлинности предоставленной информации (например: проверка соответствия пароля).

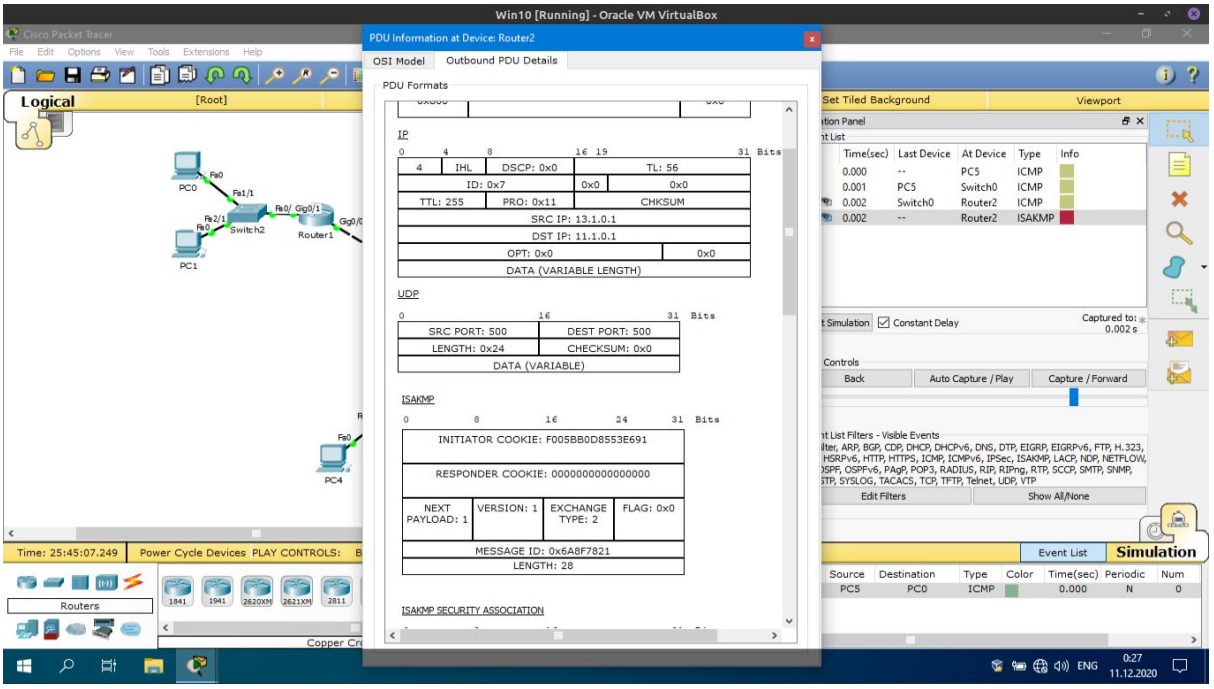

Рис. №1. Пример инкапсуляции протокола ISAKMP в протокол IP

VPN представляет собой соединение в логической сети, пакеты передающиеся по которой инкапсулируются в пакеты из общедоступного трафика.

Другими словами - VPN соединение выстраивает логический туннель между участниками, в котором происходит передача информации. Безопасность передачи

обеспечивается шифрованием данных, а доступ к туннелю получают только идентифицированные и авторизованные клиенты.

Для внешней среды передача данных оказывается скрытой за счет инкапсуляции протоколов, которые использует VPN. Таким образом, две не связанные сети, которые могут быть расположены физически в разных местах, объединяются в одну логическую[2].

1.2. Классификация VPN

Для реализации VPN существует несколько решений, которые можно классифицировать по нескольким признакам:

- Тип среды
    - Защищенные - в таких VPN для передачи используется незащищенная сеть, а защита информации обеспечивается на уровне VPN.
    - Доверительные - для передачи используется сеть, которая считается безопасной. Следственно обеспечение безопасности переходит в обязанности внешней сети.
- Тип реализации
    - Программно-аппаратная реализация - функциональность VPN обеспечивается комплексом специальных устройств и программного обеспечения(рис. №2).
    - Программная реализация - функциональность VPN обеспечивается машиной, где установлено специальное программное обеспечение.
- Назначение
    - Intranet VPN - представляет собой объединение нескольких филиальных сетей в одну корпоративную.
    - Remote Access VPN - реализует удаленный доступ хоста к приватной сети.
    - Extranet VPN - часть приватной сети доступная из общественной сети.

Рис. №2. Программно-аппаратная реализация VPN

1.3. Сферы применение VPN

Множество способов реализации обуславливает наличие множество способов применения VPN на практике.

С помощью VPN можно создать несколько логических сетей в одной физической среде для разделения трафика. Это может быть полезным в ситуациях, когда необходимо ограничить канал передачи для группы клиентов, например разделение сетей между департаментами предприятия.

Другим применением может стать предоставление доступа для сторонних клиентов к части ресурсов и блокировки доступа к остальным без физического изменения сети.

Также возможно настроить доступ удаленным клиентам в небезопасной сети к необходимым ресурсам в сети предприятия. Для этого, на машине клиента должен быть установлен клиент VPN[2].

2. ПРОЕКТИРОВАНИЕ VPN В CISCO PACKET TRACER

Для настройки VPN в Cisco Packet Tracer необходимо выполнить несколько подготовительных шагов:

1. Выбрать подходящие оборудование
2. Спроектировать макет сети
3. Подписать лицензионное соглашение для оборудования
4. Настроить туннель передачи и авторизацию клиентов в нем
5. Применить настройки VPN на оборудование

Для начала необходимо выбрать оборудование, которое поддерживает используемые технологии и для которого доступен необходимый пакет лицензий.

В рамках данной демонстрации будет использоваться набор протоколов IPSec (IP Security), который направлен на обеспечение безопасности передачи данных по протоколу IP[3]. Для использования данной технологии с оборудованием Cisco необходимо активировать лицензию security9k (набор лицензий связанных с обеспечением безопасности)[4].

Одним из аппаратов, который поддерживает IPSec и security9k является маршрутизатор 1941 из группы c1900. Данное оборудование будет использоваться при проектировании схемы далее. Для того чтобы проверить список поддерживаемых лицензий для конкретного маршрутизатора необходимо выполнить команду:

show license all;

Следующим шагом необходимо собрать начальный макет сети(рис. №3). Для примера будут использоваться:

- Три маршрутизатора 1941 и один маршрутизатор 2811
- Три коммутатора
- Шесть персональных компьютеров

Каждая пара персональных компьютеров подключается к общему коммутатору. Каждый коммутатор, в свою очередь, подключается к маршрутизатору. Три маршрутизатора подключаются к четвертому - центральному маршрутизатору, который имитирует внешнюю сеть, а три получившиеся группы представляют собой сети в корпоративных зданиях.

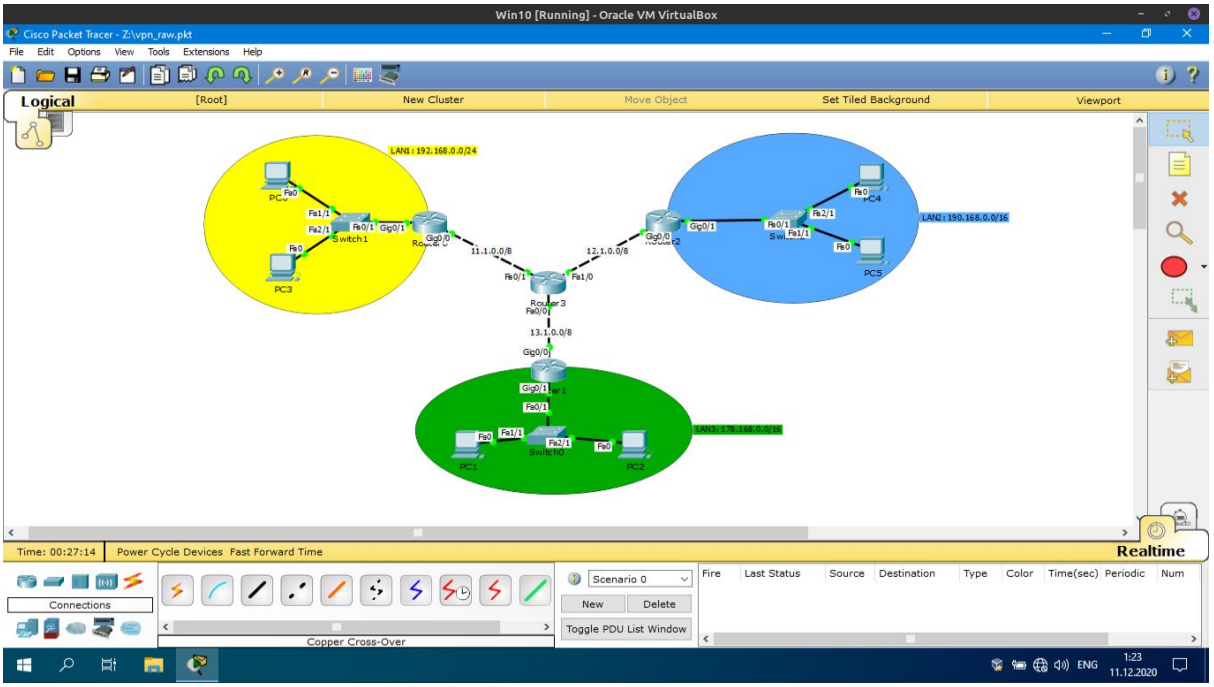

Рис. №3. Макет сети

После подготовки макета следует первичная настройка сетей и подготовка оборудования для применения VPN.

В каждой из частей корпоративной сети необходимо настроить исходные параметры:

- Распределение IP адресов для терминальных хостов
- Добавить для каждого маршрутизатора абстрактный статический маршрут для сети *0.0.0.0* с маской *0.0.0.0* следующий шаг для которого представляет центральный маршрутизатор.

Для первого сегмента сети будет использоваться сеть LAN1 с адресом *192.168.0.0/24*, для второго - LAN2 - *190.168.0.0/16* и для третьего - LAN3 - *178.168.0.0/16*. Настройка IP адреса для интерфейса осуществляется командой:

ip address <IP>

Внешние интерфейсы маршрутизаторов получат адреса согласно правилу: *1n.1.0.1/8*, где n - номер сегмента. В свою очередь ближайший к сегменту внешний интерфейс центрального маршрутизатора будет настроен по правилу: *1n.1.0.2/8*, где n - номер сегмента.

Терминальные хосты будут получать конфигурацию IP от DHCP настроенного на маршрутизаторах. Конфигурация DHCP средствами роутера осуществляется командами:

1. *ip dhcp pool <название>* - для создания набора адресов
2. *network <network address> <netmask>* - для задания сети, которая используется в наборе
3. *default-router <IP>* - для указания стандартного шлюза в сети

Заключительным этапом первичной настройки является добавление абстрактных статических маршрутов к центральному маршрутизатору. Данная настройка выполняется командой: *ip route <network address> <netmask> <next hop>*.

В итоге, каждый из сегментов настроен для работы с локальной сетью и реализации VPN.

После завершения макета сети и его первоначальной настройки необходимо активировать лицензионные соглашения для маршрутизаторов командой:

license boot module c1900 technology-package security9k

Затем необходимо принять соглашение, сохранить настройки и перезагрузить маршрутизатор(команды: *copy run start*; *reload*).

Результатом данных действий является оборудование готовое к работе с набором протоколов IPSec и настройке VPN.

Настройка VPN начинается с создания списков ACL между участниками туннеля:

access-list <номер> permit ip <адрес сети источника> <wildcard> <адрес сети получателя> <wildcard>

Следующим шагом необходимо настроить среду обмена создания и обмена ключами для дальнейшей идентификации и авторизации в тоннеле VPN. Для этого будет использоваться протокол *ISAKMP*, который был разработан специально для подобных целей. Для создания ключей будет использоваться протокол Диффи — Хеллмана и его группа номер пять[5]. Для шифрования будет использоваться алгоритм AES 256. Такая конфигурация реализуется следующими командами:

1. *crypto isakmp policy <номер>*
2. *encryption aes 256*
3. *group 5*
4. *authentication pre-share*

После подготовки среды для работы с ключами следует настроить сами ключи: *crypto isakmp key <пароль> address <peer>*, где peer - адрес внешнего интерфейса получателя.

На данном этапе виртуальная приватная сеть готова к авторизации. Теперь необходимо настроить алгоритм шифрования(трансформации) информации внутри защищенного туннеля. Для хеширования будет использоваться алгоритм *sha-hmac:*

crypto ipsec transform-set <название> esp-aes 256 esp-sha-hmac

Заключительным этапом конфигурации является применение предыдущих конфигураций на определенном интерфейса маршрутизатора. Данная операция состоит из двух частей[6][7]:

1. Компоновка настроек в карту шифрования:
    a. *crypto map <название> <номер> ipsec-isakmp*
    b. *set peer <peer>*
    c. *set security-association lifetime seconds <время в секундах>*
    d. *set pfs group5*
    e. *set transform-set <название>*
    f. *match address <ACL>*
2. Назначение полученный карты на интерфейс: *crypto map <название>*

Таким образом все участники получили настройки для предоставления доступа, среды создания и обмена ключами, среды шифрования и передачи информации, - или VPN.

ЗАКЛЮЧЕНИЕ

Технология VPN является мощным инструментом, который позволяет:

- Расширять физические сети используя логический уровень, посредством создания виртуальных сетей
- Осуществлять контроль доступа к сетям с помощью настройки идентификации и авторизации клиентов
- Обеспечивать безопасность передачи информации за счет ее трансформации в виртуальном тоннеле(шифрование).

Cisco Packet Tracer предоставляет исчерпывающий набор функций для моделирования и изучения компьютерных сетей, в частности проектирования VPN используя устройства Cisco.

БИБЛИОГРАФИЯ

1. Толковый словарь - доступен: https://official.academic.ru/22895/%D0%A1%D0%B5%D1%82%D1%8C
2. Справочник IBM - доступен: https://www.ibm.com/support/knowledgecenter/ru/ssw_ibm_i_71/rzaja/rzajagetstart.htm
3. Cisco инструкция по IPSec - доступна: https://www.cisco.com/c/ru_ru/support/docs/routers/3600-series-multiservice-platforms/91193-rtr-ipsec-internet-connect.pdf
4. Работа с лицензиями в Cisco Packet Tracer - доступна: https://resources.intenseschool.com/cisco-ios-licensing/
5. Владимиров С., «Криптосистемы-протоколы»: Диффи—Хеллмана, Эль-Гамаля, MTI/A(0), STS - доступна: https://habr.com/ru/post/476106/
6. Справочник по Cisco Packet Tracer - доступен: https://www.packettracernetwork.com/tutorials/ipsec-vpn.html
7. Cisco VPN справочник - доступен: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14132-ios-D.html