Настройка VPN по средствам IPsec протокола

**Цель работы:**

Целью работы является изучение технологии IPsec и практическая её реализация в организации VPN на имитации реальной сети.

**Краткие теоретические сведения:**

IPsec (IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. В основном, применяется для организации VPN-соединений. Состоит из двух фаз:

1-я фаза - ISAKMP (Internet Security Association and Key Management Protocol):

Сначала 2 конечных маршрутизатора аутентифицируют друг друга и договариваются какие алгоритмы шифрования будут использоваться для будущего IPSec туннеля, а также генерируют общий секретный ключ.

В 1-й фазе устройства должны договориться об использовании следующих параметров:

* Алгоритм шифрования.
* Метод аутентификации.
* Способ обмена секретными ключами.
* Срок жизни сессии (Security Association).

Набор данных параметров определяет политику ISAKMP. Каждая политика имеет свой приоритет. Когда устройства начинают договариваться друг с другом, то последовательно перебирают все установленные политики, начиная с высшего приоритета. Как только будет обнаружено, что устройства имеют одинаковые параметры в конкретной политике, то поиск прекращается.

2-я фаза - установление IPSec туннеля:

На данном этапе создается сам IPSec туннель для передачи пользовательских данных. Поэтому маршрутизаторы снова договариваются какие протоколы шифрования и хэширования будут использоваться между ними.

Он остается активным во время работы IPSec туннеля. У каждого туннеля есть свое время “жизни”. Поэтому, если необходимо продлить сеанс связи, то мини-туннель ISAKMP обновит таймер туннеля, а также секретные ключи безопасности. Теперь, когда с теорией немного разобрались, приступим к настройке необходимых параметров.

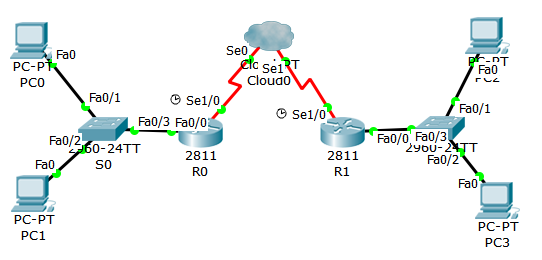
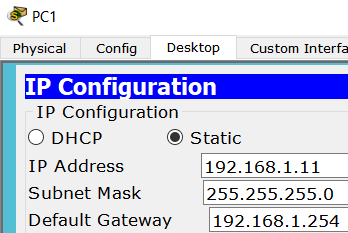
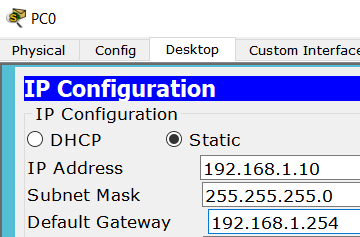


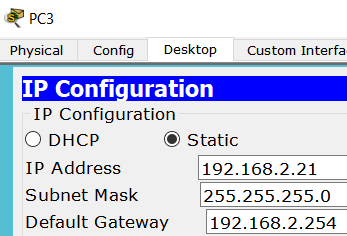
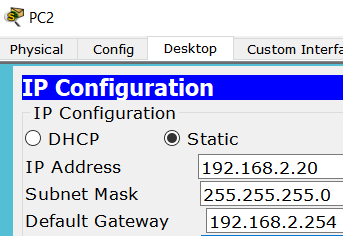
Рис. 1. Схема соединения сети

**Последовательность действий:**

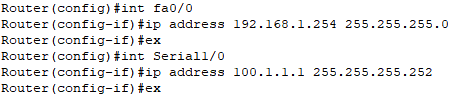
Шаг 1. Построить схему сети, как показано на рисунке 1. Предварительно в оба роутера необходимо добавить модуль NM-4A/S.

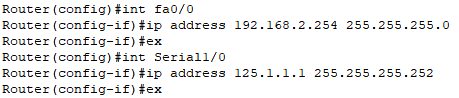
Шаг 2. Настроить IP адреса, маски и шлюз по умолчанию для конечных устройств (лкм по PC, вкладка Desktop -> IP Configuration):



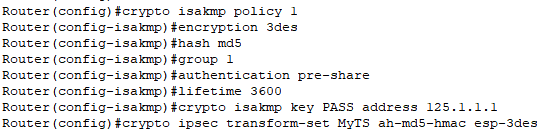


Шаг 3. Настроить интерфейсы маршрутизатора R0 и R1 соответственно:

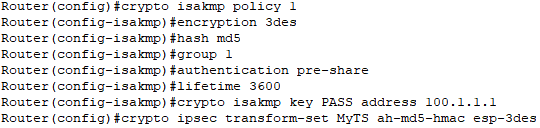




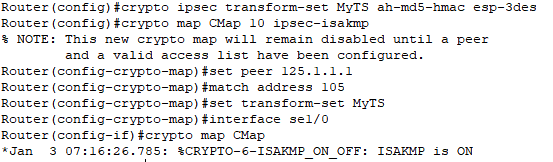
Шаг 5. Настроить политику ISAKMP на R0, последовательно указав метод шифрования, аутентификации и обмена секретными ключами, а также время жизни сессии. В конце указать IP адрес конечной точки туннеля, то есть маршрутизатора R1:



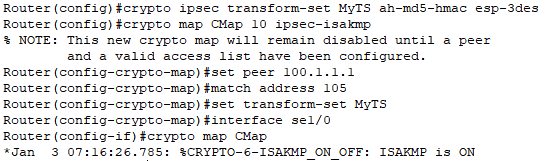
Шаг 6. Аналогично настроить политику ISAKMP на R1:



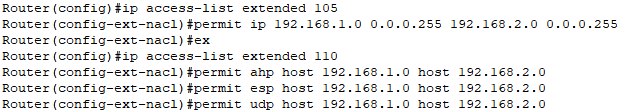
Шаг 7. Настроить параметры туннеля IPSec и создать карту шифрования для R0, привязав её к интерфейсу Serial1/0:



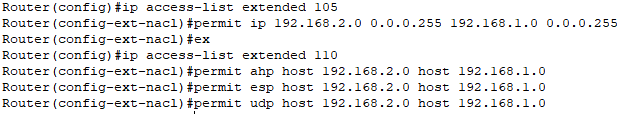
Шаг 8. Повторить предыдущий шаг для R1:



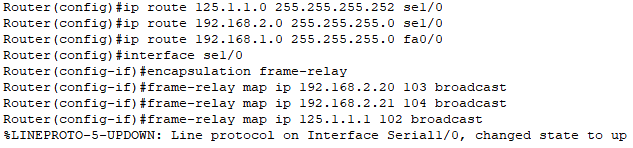
Шаг 9. Настроить ACL, где указывается шифруемый траффик, для R0, а также разрешаем протоколы:



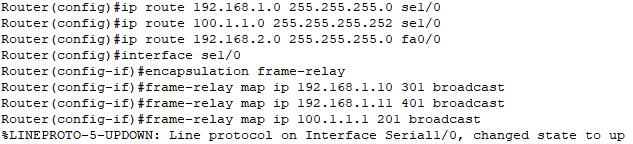
Шаг 10. Аналогично настроить ACL для R1:

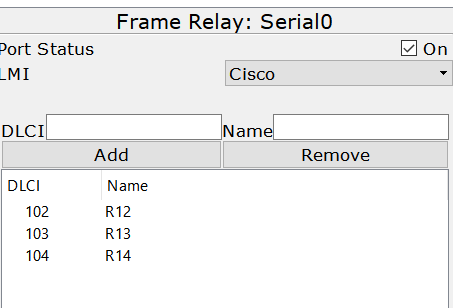


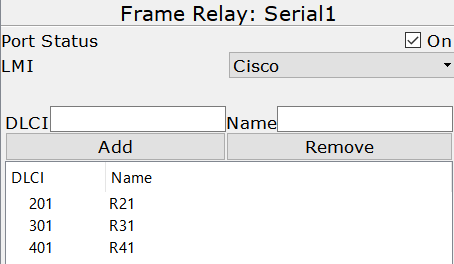
Шаг 11. Настроить маршрутизацию сети и frame-relay для R0:

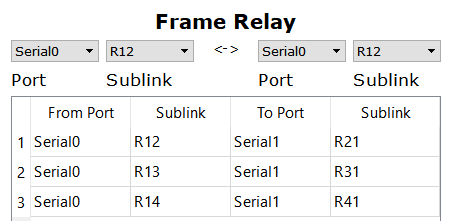


Шаг 12. Повторить предыдущий шаг для R1:

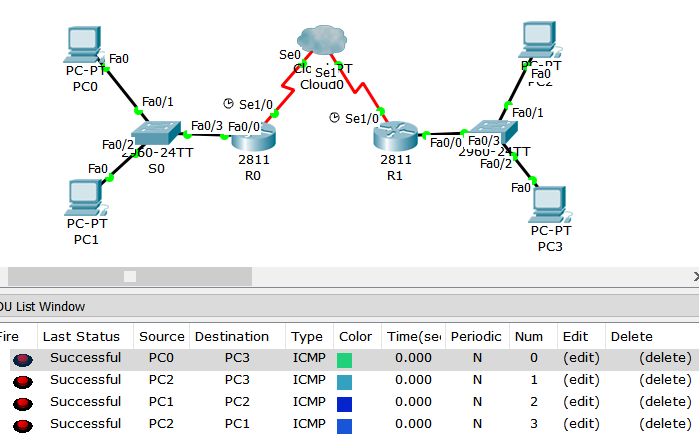


 Шаг 13. Для облака настроить интерфейсы Serial0 и Serial1, а также Frame Relay:





Шаг 14. Проверить конфигурацию системы путем отправки Simple PDU. При корректной настройке каждое конечное устройство должно быть доступно для любого другого (из-за особенностей Cisco PT при отправке первых двух PDU система производит настройку, в следствие чего может выдавать ошибку передачи):



**Вопросы и задания:**

1. Для чего применяется технология IPsec.
2. Из каких фаз состоит процесс настройки VPN на основе IPsec. Назовите их.
3. Набор каких параметров определяет политику ISAKMP.
4. Что происходит на второй фазе настройки VPN на основе IPsec.
5. Каким образом указывается системе на траффик, который необходимо шифровать.