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.

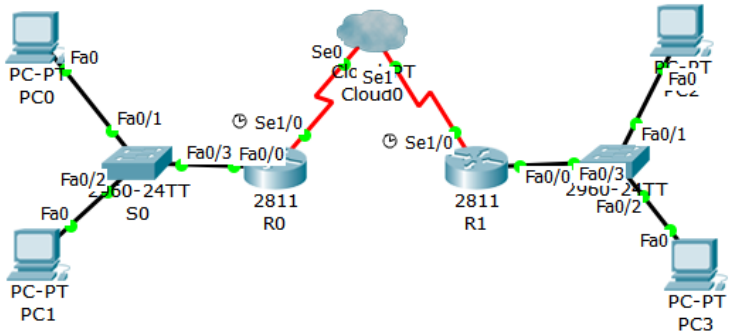
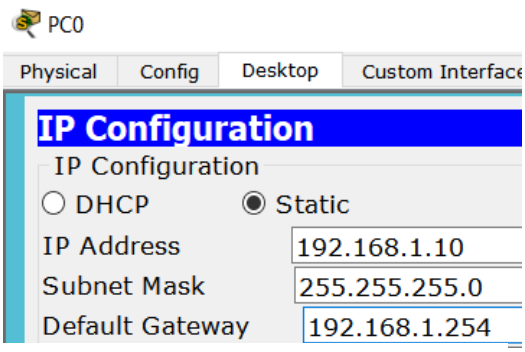


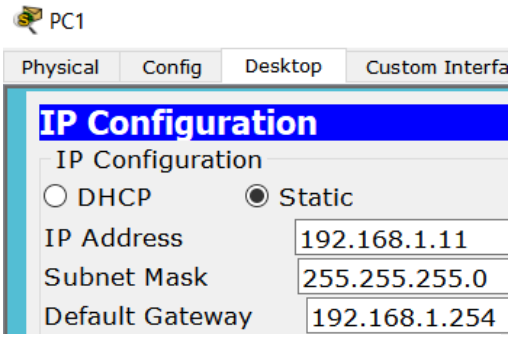
Рис. 1. Схема соединения сети

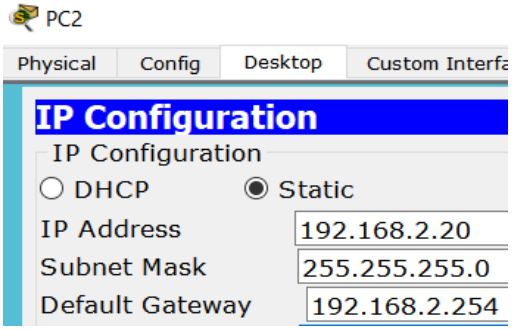
Последовательность действий:

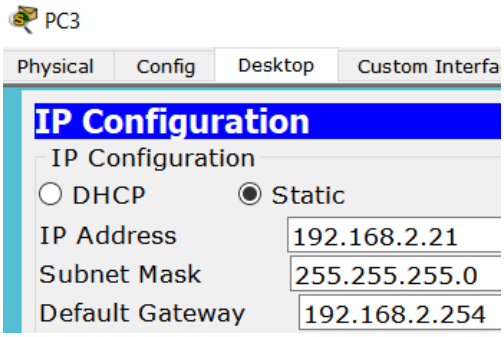
Шаг 1. Построить схему сети, как показано на рисунке 1. Предварительно в оба роутера необходимо добавить модуль NM-4A/S.

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:

```
Router(config)#int fa0/0
Router(config-if)#ip address 192.168.1.254 255.255.255.0
Router(config-if)#ex
Router(config)#int Serial1/0
Router(config-if)#ip address 100.1.1.1 255.255.255.252
Router(config-if)#ex
Router(config)#int fa0/0
Router(config-if)#ip address 192.168.2.254 255.255.255.0
Router(config-if)#ex
Router(config)#int Serial1/0
Router(config-if)#ip address 125.1.1.1 255.255.255.252
Router(config-if)#ex
```

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:

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#group 1
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#lifetime 3600
Router(config-isakmp)#crypto isakmp key PASS address 125.1.1.1
```

Шаг 6. Аналогично настроить политику ISAKMP на R1:

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#group 1
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#lifetime 3600
Router(config-isakmp)#crypto isakmp key PASS address 100.1.1.1
```

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

```
Router(config)#crypto ipsec transform-set MyTS ah-md5-hmac esp-3des
Router(config)#crypto map CMap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#set peer 125.1.1.1
Router(config-crypto-map)#match address 105
Router(config-crypto-map)#set transform-set MyTS
Router(config-crypto-map)#interface se1/0
Router(config-if)#crypto map CMap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Шаг 8. Повторить предыдущий шаг для R1:

```
Router(config)#crypto ipsec transform-set MyTS ah-md5-hmac esp-3des
Router(config)#crypto map CMap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#set peer 100.1.1.1
Router(config-crypto-map)#match address 105
Router(config-crypto-map)#set transform-set MyTS
Router(config-crypto-map)#interface se1/0
Router(config-if)#crypto map CMap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

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

```
Router(config)#ip access-list extended 105
Router(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config-ext-nacl)#ex
Router(config)#ip access-list extended 110
Router(config-ext-nacl)#permit ahp host 192.168.1.0 host 192.168.2.0
Router(config-ext-nacl)#permit esp host 192.168.1.0 host 192.168.2.0
Router(config-ext-nacl)#permit udp host 192.168.1.0 host 192.168.2.0
```

Шаг 10. Аналогично настроить ACL для R1:

```
Router(config)#ip access-list extended 105
Router(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#ex
Router(config)#ip access-list extended 110
Router(config-ext-nacl)#permit ahp host 192.168.2.0 host 192.168.1.0
Router(config-ext-nacl)#permit esp host 192.168.2.0 host 192.168.1.0
Router(config-ext-nacl)#permit udp host 192.168.2.0 host 192.168.1.0
```

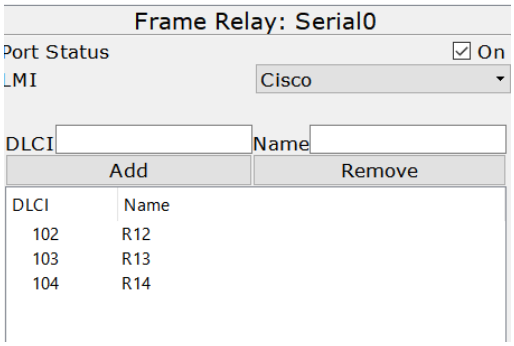
Шаг 11. Настроить маршрутизацию сети и frame-relay для R0:

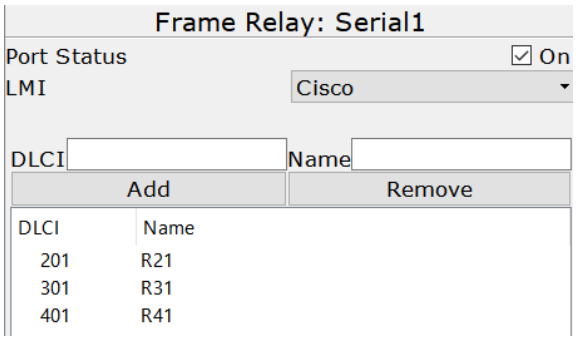
```
Router(config)#ip route 125.1.1.0 255.255.255.252 se1/0
Router(config)#ip route 192.168.2.0 255.255.255.0 se1/0
Router(config)#ip route 192.168.1.0 255.255.255.0 fa0/0
Router(config)#interface se1/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#frame-relay map ip 192.168.2.20 103 broadcast
Router(config-if)#frame-relay map ip 192.168.2.21 104 broadcast
Router(config-if)#frame-relay map ip 125.1.1.1 102 broadcast
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
```

Шаг 12. Повторить предыдущий шаг для R1:

```
Router(config)#ip route 192.168.1.0 255.255.255.0 se1/0
Router(config)#ip route 100.1.1.0 255.255.255.252 se1/0
Router(config)#ip route 192.168.2.0 255.255.255.0 fa0/0
Router(config)#interface se1/0
Router(config-if)#encapsulation frame-relay
Router(config-if)#frame-relay map ip 192.168.1.10 301 broadcast
Router(config-if)#frame-relay map ip 192.168.1.11 401 broadcast
Router(config-if)#frame-relay map ip 100.1.1.1 201 broadcast
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
```

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



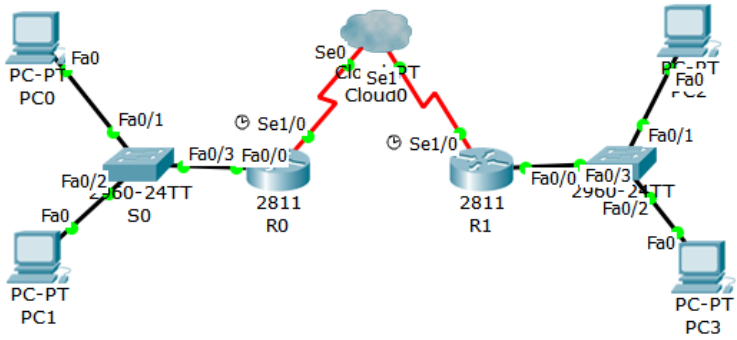


Frame Relay

Serial0	R12	<->	Serial0	R12
Port	Sublink		Port	Sublink

	From Port	Sublink	To Port	Sublink
1	Serial0	R12	Serial1	R21
2	Serial0	R13	Serial1	R31
3	Serial0	R14	Serial1	R41

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):



U List Window

Fire	Last Status	Source	Destination	Type	Color	Time(se	Periodic	Num	Edit	Delete
	Successful	PC0	PC3	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC2	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	PC2	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC2	PC1	ICMP		0.000	N	3	(edit)	(delete)

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.