Основы компьютерных сетей.
8. Углубленное изучение сетевых технологий.

IPSec

План занятия:

- VPN протоколы
- Шифрование
- Аутентификация
- Защита целостности
- IPSec

VPN протоколы

Существует несколько популярных VPN-протоколов, каждый из которых предназначен для определенных целей и сценариев использования. Вот несколько наиболее популярных VPN-протоколов:

1.OpenVPN:

1. **Особенности**:
    1. Открытое программное обеспечение.
    2. Поддерживает как симметричное, так и асимметричное шифрование.
    3. Поддерживает различные порты, включая TCP и UDP.
    4. Кросс-платформенность (работает на Windows, macOS, Linux).

2.IPsec (Internet Protocol Security):

1. **Особенности**:
    1. Комплексный стек протоколов, включающий AH и ESP для аутентификации и шифрования.
    2. Широко используется в сетях предприятий и в реализации VPN-соединений.
    3. Поддерживается многими устройствами и операционными системами.

3.L2TP/IPsec (Layer 2 Tunneling Protocol with IPsec):

1. **Особенности**:
    1. Комбинация протоколов для создания безопасных туннелей.
    2. Часто используется в сочетании с IPsec для обеспечения шифрования и аутентификации.

VPN протоколы

4.PPTP (Point-to-Point Tunneling Protocol):

1. **Особенности**:
    1. Прост в настройке.
    2. Не считается наиболее безопасным из-за некоторых известных уязвимостей.
    3. Часто поддерживается многими операционными системами.

5.SSTP (Secure Socket Tunneling Protocol):

1. **Особенности**:
    1. Разработан Microsoft.
    2. Использует SSL/TLS для шифрования.
    3. Часто используется в среде Windows.

6.IKEv2 (Internet Key Exchange version 2):

1. **Особенности**:
    1. Разработан для замены более старого протокола IKEv1.
    2. Поддерживает быстрое восстановление соединения при смене сетей (например, при переходе с Wi-Fi на мобильную сеть).

7.WireGuard:

1. **Особенности**:
    1. Современный и быстрый протокол, разработанный для упрощения реализации VPN.
    2. Использует современные криптографические методы.
    3. Менее сложен в настройке по сравнению с некоторыми традиционными протоколами.

Основные функции VPN-протоколов:

1.Шифрование (Encryption):

1. *Функция*: Защита конфиденциальности данных.
2. *Описание*: Весь трафик, передаваемый между узлами через VPN, шифруется, что предотвращает прослушивание и несанкционированный доступ к передаваемой информации. (AES)

2.Аутентификация (Authentication):

1. *Функция*: Проверка подлинности участвующих в VPN узлов.
2. *Описание*: Гарантирует, что только легитимные устройства имеют доступ к VPN-соединению. Методы аутентификации могут включать в себя предварительно распределенные ключи (Pre-Shared Keys), сертификаты, логины/пароли и другие. (RSA)

3.Целостность данных (Data Integrity):

1. *Функция*: Гарантия того, что данные не были изменены в процессе передачи.
2. *Описание*: Использует хэш-функции и методы целостности, чтобы обнаруживать любые изменения данных в пакетах, передаваемых через VPN. (HMAC)

4.Протокол управления ключами (Key Management Protocol):

1. *Функция*: Обеспечение безопасного обмена ключами для шифрования данных.
2. *Описание*: Ключи, используемые для шифрования данных, должны быть обменены между узлами VPN безопасным образом. Протоколы управления ключами, такие как ISAKMP или IKE, выполняют эту задачу. (RSA, DH, ECDH)

SSL/TLS

Secure sockets layer - уровень защищённых сокетов, криптографический протокол, который подразумевает более безопасную связь.

Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.

TLS и SSL используют асимметричную криптографию для аутентификации и симметричное шифрование для передачи данных.

Шифрование

Существует два типа алгоритмов шифрования.

• Симметричный — такой тип шифрования при котором для шифровки и дешифровки используется один и тот же ключ.

Симметричные алгоритмы шифрования (шифрование):

• **AES** - американский стандарт шифрования

• ГОСТ 28147-89 — советский и российский стандарт шифрования, также является стандартом СНГ

• DES/3DES - стандарты шифрования данных в США

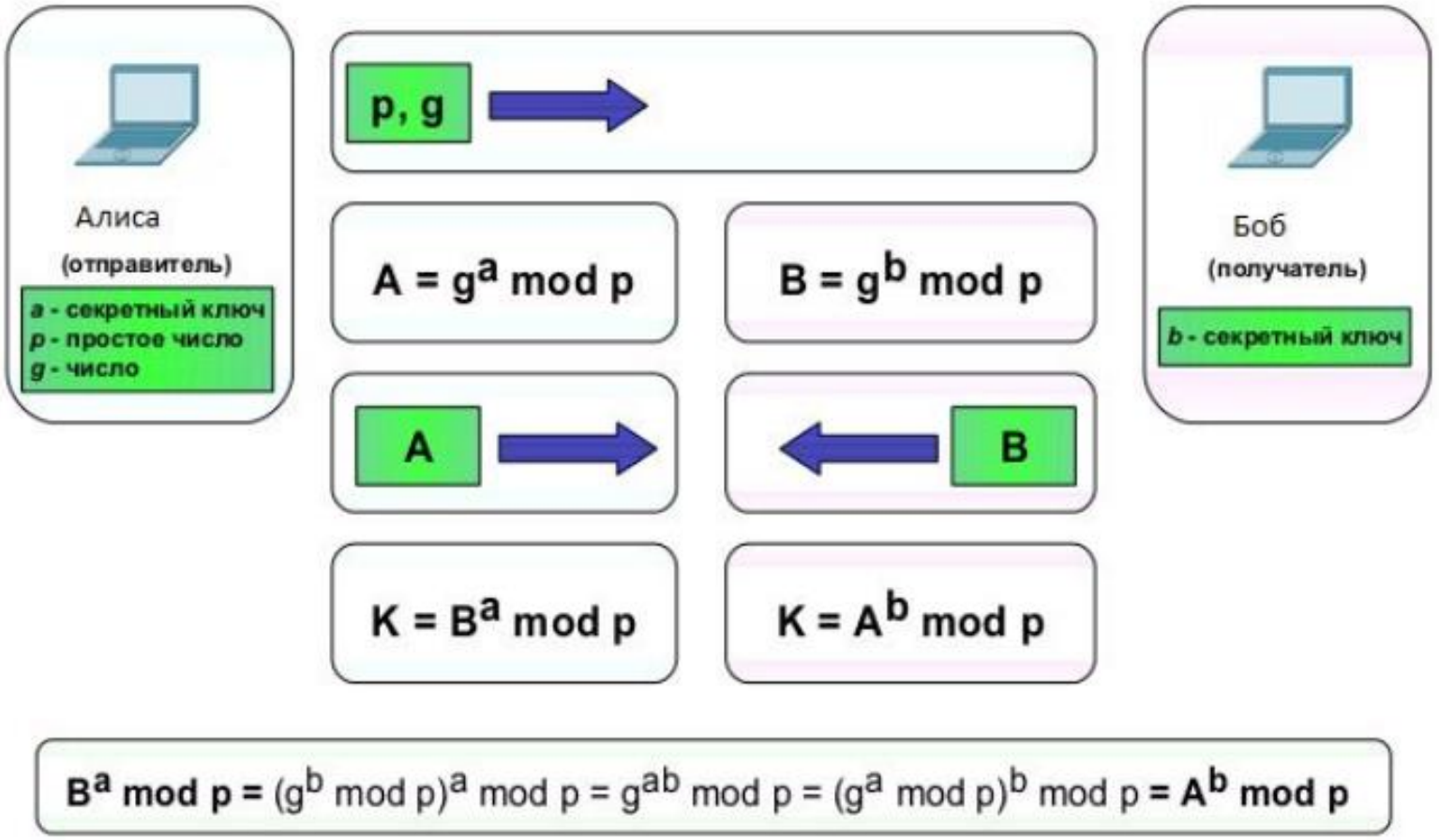
• Асимметричный — такой тип шифрования, при котором для шифровки и дешифровки используются разные ключи.

Ассиметричные алгоритмы шифрования (аутентификация):

• **RSA**

• DSA

Алгоритм Диффи-Хелмана



Алгоритм Диффи-Хеллмана (Diffie-Hellman, DH) является криптографическим протоколом, предназначенным для безопасного обмена секретными ключами через открытые каналы связи.

IPSec

IPSec (Internet Protocol Security) - это набор протоколов и стандартов, предназначенных для обеспечения безопасности передачи данных в сети IP.

Он предоставляет механизмы для шифрования и аутентификации сетевого трафика, что делает его особенно важным для обеспечения конфиденциальности и целостности данных при их передаче через открытые сети, такие как интернет.

Важные компоненты и возможности IPSec:

1.AH (Authentication Header):

1. Обеспечивает аутентификацию и целостность данных, добавляя к заголовку IP дополнительную информацию для проверки подлинности данных.

2.ESP (Encapsulating Security Payload):

1. Предоставляет механизмы шифрования данных, обеспечивая конфиденциальность. Также может предоставлять аутентификацию и целостность.

3.Туннелирование (Tunnel Mode) и Транспортный режим (Transport Mode):

1. В режиме туннелирования весь пакет данных защищается, включая оригинальный заголовок IP. В транспортном режиме защищаются только данные, сохраняя оригинальный заголовок IP.

4.Интернет-ключи (Internet Key Exchange, IKE):

1. Протокол, используемый для установки безопасного соединения (Security Association, SA) между узлами, обменивающимися данными посредством IPSec.

5.Режим транспарентного шифрования (Transparent Encryption):

1. Позволяет шифровать трафик между двумя устройствами, не требуя изменения конечных точек.

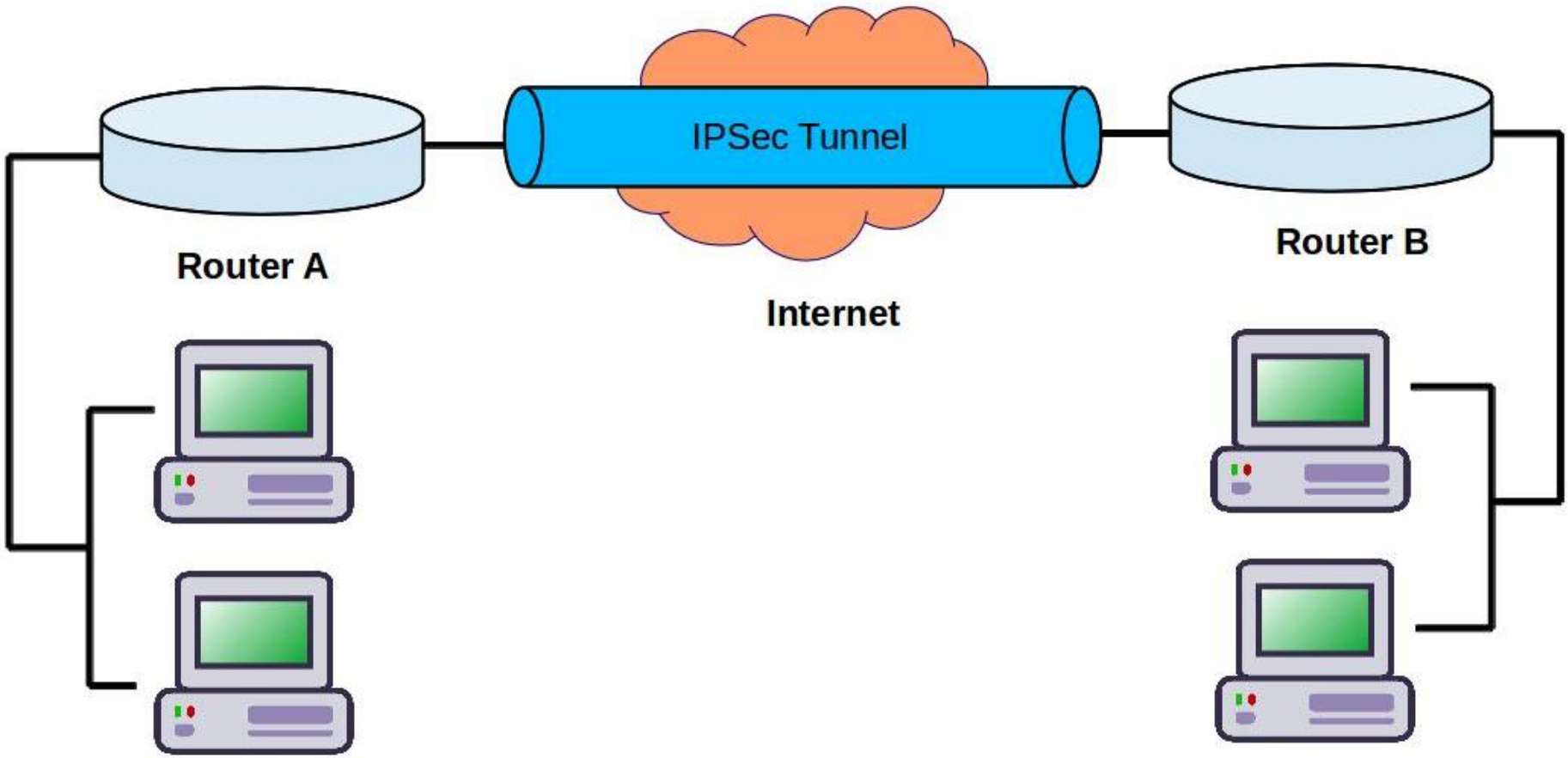
6.Поддержка для VPN (Virtual Private Network):

1. IPSec широко используется для создания безопасных соединений в рамках VPN, позволяя организациям обеспечивать безопасную передачу данных через общедоступные сети.

7.Методы аутентификации:

1. Поддерживаются различные методы аутентификации, включая предварительно распределенные ключи (Pre-Shared Keys) и использование сертификатов.

IPSec



IPsec sec наиболее широко используемый протокол для построения VPN. IPsec является набором протоколов:

- Authentication Header (AH). Обеспечивает аутентификацию и целостность данных, добавляя к заголовку IP дополнительную информацию для проверки подлинности данных.
- Encapsulating Security Payload (ESP). Предоставляет механизмы шифрования данных, обеспечивая конфиденциальность.
- Internet Security Association and Key Management Protocol (ISAKMP). Протокол управления безопасностью и обмена ключами.

Настройка IPsec

Настройка IPsec включает в себя два основных этапа:

Этап 1: Установка Фазы Управления Ключами (ISAKMP/IKE)

1.Выбор протокола и алгоритмов:

1. Определите, какой протокол управления ключами использовать: ISAKMP (Internet Security Association and Key Management Protocol) или IKE (Internet Key Exchange). Также выберите алгоритмы шифрования, хэширования и методы аутентификации.

2.Настройка параметров ISAKMP/IKE:

1. Задайте параметры ISAKMP/IKE, такие как режим (main или aggressive), метод аутентификации (Pre-Shared Key, сертификаты), группа обмена ключами (DH group), используемые хэш-функции и алгоритмы шифрования.

3.Установка предварительно распределенного ключа (PSK) или сертификатов:

1. Если используется метод аутентификации с предварительно распределенным ключом, укажите его для обеих сторон. Если используются сертификаты, убедитесь, что сертификаты настроены и доступны для обеих сторон.

4.Конфигурация политик безопасности (Security Policies):

1. Определите, какие трафик и сетевые ресурсы будут защищены, и настройте соответствующие политики безопасности, указывающие параметры шифрования и аутентификации для различных типов трафика.

5.Настройка параметров жизненного цикла сессии (SA Lifetimes):

1. Задайте временные интервалы для обновления ключей и переустановки безопасных ассоциаций (SAs).

Настройка IPsec

Этап 2: Фаза Защищенной Передачи Данных

1.Выбор протоколов IPsec:

1. Определите, какие протоколы IPsec будут использоваться для защиты данных. Наиболее распространенными являются ESP (Encapsulating Security Payload) для конфиденциальности и/или AH (Authentication Header) для аутентификации и целостности данных.

2.Конфигурация IPsec SAs:

1. Настройте параметры безопасных ассоциаций (SA) для каждой комбинации источника и назначения, определенной в политиках безопасности. Это включает в себя параметры шифрования, хэширования и ключей.

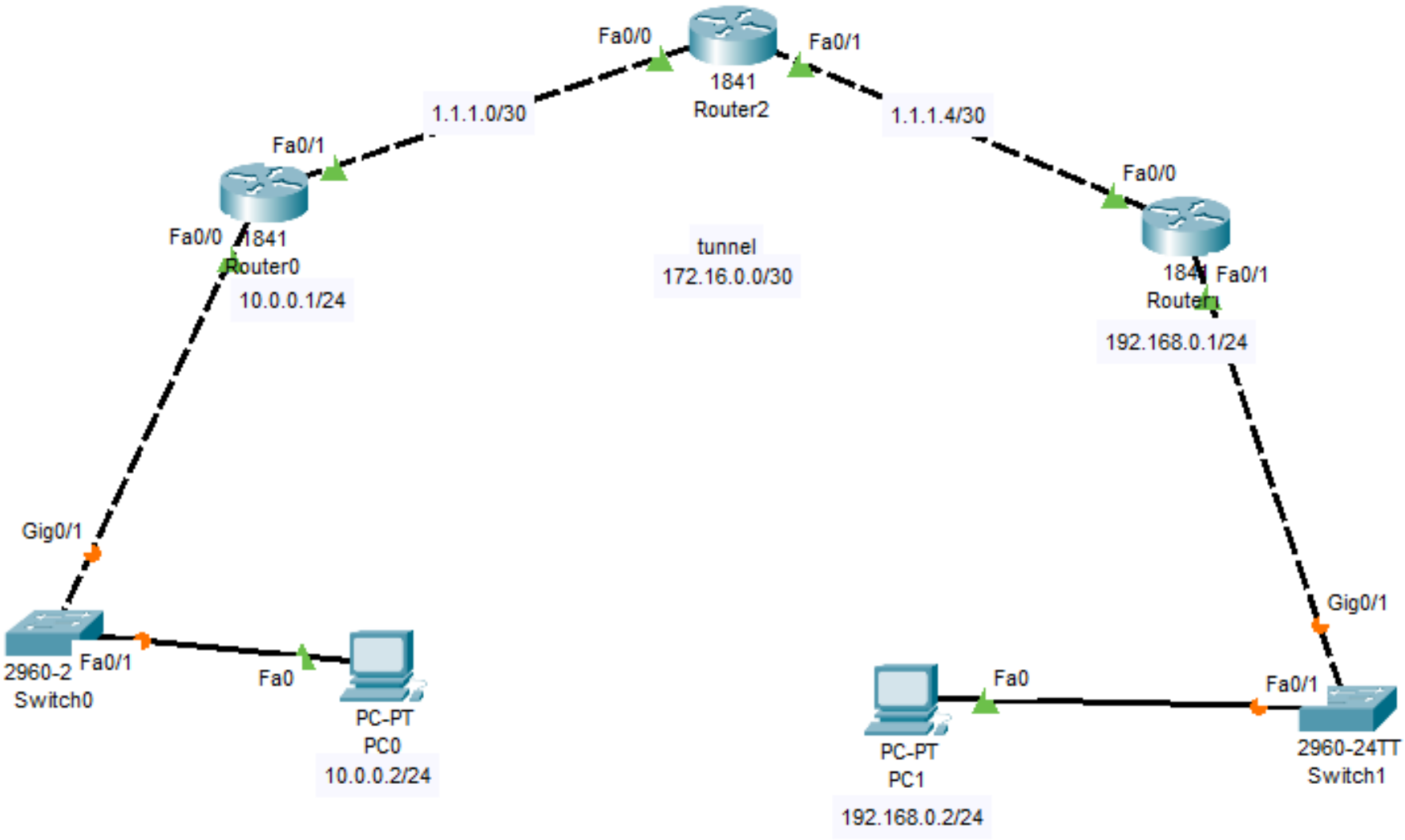
3.Применение IPsec к интерфейсам:

1. Укажите, какие интерфейсы будут использоваться для защиты трафика IPsec. Настройте правила маршрутизации для направления трафика через IPsec.

4.Тестирование и отладка:

1. После настройки, проведите тестирование, чтобы убедиться, что IPsec соединение работает корректно. Используйте инструменты мониторинга и отладки для выявления возможных проблем.

Практика


Fa0/0
Fa0/1
1841
Router2
1.1.1.0/30
1.1.1.4/30
Fa0/1
Fa0/0
1841
Router0
10.0.0.1/24
tunnel
172.16.0.0/30
Fa0/0
Fa0/1
Router1
192.168.0.1/24
Gig0/1
2960-2
Switch0
Fa0/1
Fa0
PC-PT
PC0
10.0.0.2/24
Gig0/1
Fa0
Fa0/1
PC-PT
PC1
192.168.0.2/24
2960-24TT
Switch1

1.Router0. ISAKMP

```
R0(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
```

\\ пароль для адреса 1.1.1.6 - cisco

```
Router(config)#crypto isakmp key cisco address 1.1.1.6
```

\\ аутентификация PSK

```
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#authentication pre-share
```

\\ шифрование aes 192

```
Router(config-isakmp)#encryption aes 192
```

\\ДХ-группа

```
Router(config-isakmp)#group 5
```

\\ хэшинг

```
Router(config-isakmp)#hash sha
```

2. IPSEC - transform set

\\ настройки шифрования траффика. TS_IPSEC_AES_SHA - имя. esp-aes 192 - протокол шифрования AES. esp-sha-hmac - хэшинг SHA

Router(config)#crypto ipsec transform-set TS_IPSEC_AES_SHA esp-aes 192 esp-sha-hmac

3. какой траффик будем шифровать

Router(config)#ip access-list extended ACL_GRE_O_IPSEC

\\ разрешен траффик от 1.1.1.1 до 1.1.1.6

Router(config-ext-nacl)#permit gre host 1.1.1.1 host 1.1.1.6

\\ какой трафик, в какой роутер, что именно шифровать. связываем ISAKMP и IPSEC

Router(config)#crypto map MAP 100 ipsec-isakmp

\\ трафик, к которому применяется политика

Router(config-crypto-map)#match address ACL_GRE_O_IPSEC

Router(config-crypto-map)#set peer 1.1.1.6

Router(config-crypto-map)#set transform-set TS_IPSEC_AES_SHA

\\ применяем правила к интерфейсу

Router(config)#interface fastEthernet 0/1

Router(config-if)#crypto map MAP

\\ для роутера2 настройки аналогичны

\\ проверяем

C:\>ping 192.168.0.2

R0# show crypto ipsec sa

```
protected vrf: (none)
local  ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/47/0)
remote  ident (addr/mask/prot/port): (1.1.1.6/255.255.255.255/47/0)
current_peer 1.1.1.6 port 500
 PERMIT, flags={origin is acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
```

\\ проверяем

Router#show crypto map

```
Router#show crypto map
Crypto Map MAP 100 ipsec-isakmp
        Peer = 1.1.1.6
        Extended IP access list ACL_GRE_O_IPSEC
            access-list ACL_GRE_O_IPSEC permit gre host 1.1.1.1 host 1.1.1.6
        Current peer: 1.1.1.6
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                TS_IPSEC_AES_SHA,
        }
        Interfaces using crypto map MAP:
                FastEthernet0/1
```

\\ проверяем

Router#show crypto isakmp policy

```
Global IKE policy
Protection suite of priority 10
        encryption algorithm:    AES - Advanced Encryption Standard (192 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #5 (1536 bit)
        lifetime:                86400 seconds, no volume limit
Default protection suite
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                86400 seconds, no volume limit
```

XOR Calculator:

https://xor.pw/

MD5 онлайн:

https://md5-online.ru/