Основы компьютерных сетей.
8. Углубленное изучение сетевых технологий.

IPSec

План занятия:

- IPSec

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.

Шифрование

Существует два типа алгоритмов шифрования.

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

Ассиметричные алгоритмы шифрования (аутентификация):

• RSA

• DSA

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

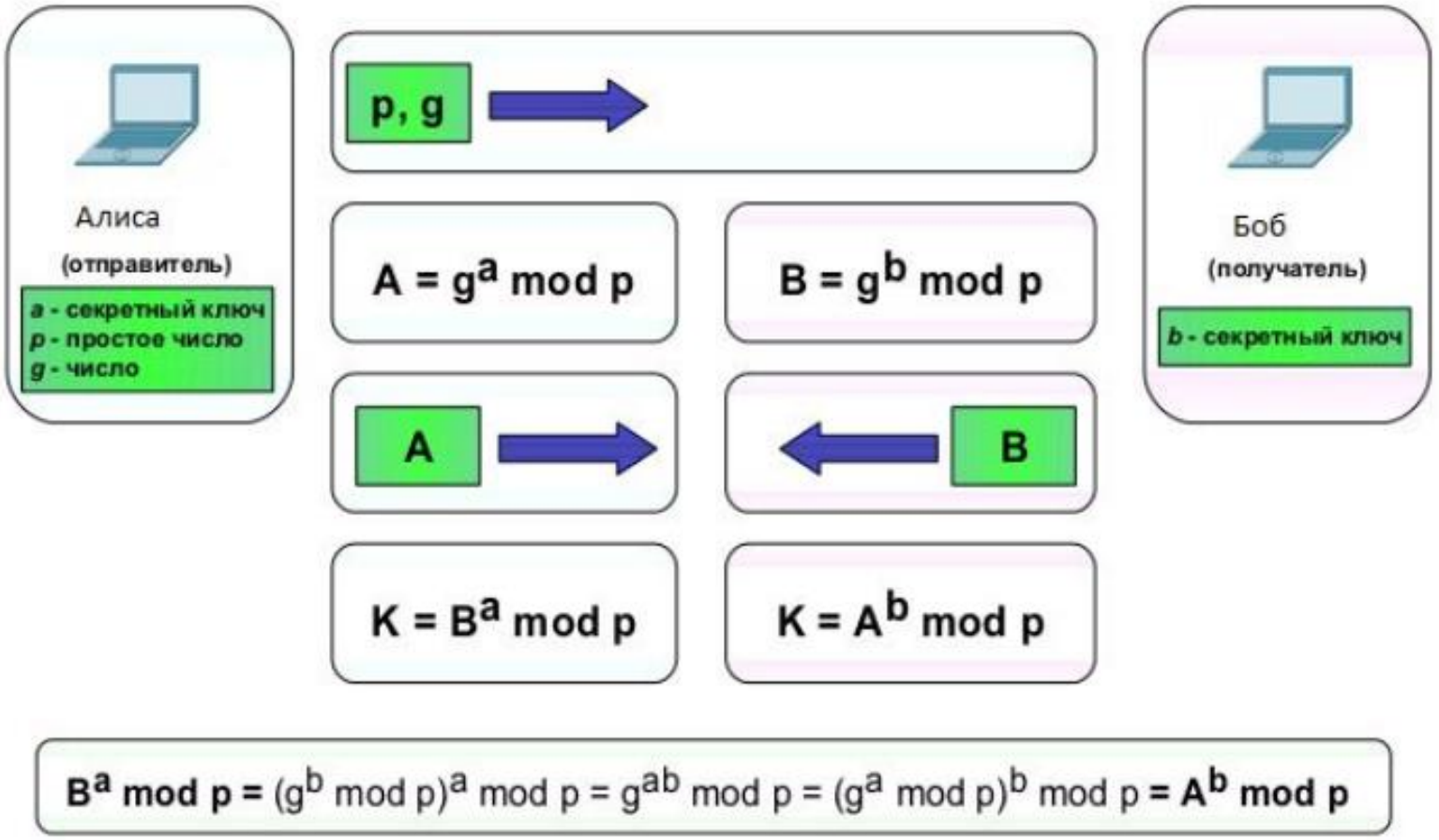
Симметричные алгоритмы шифрования (шифрование):

• AES - американский стандарт шифрования

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

• DES/3DES - стандарты шифрования данных в США

Алгоритм Диффи-Хелмана



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

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.

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.

Основные протоколы используемые для построения сетевых туннелей:

- PPTP
- L2TP
- OpenVPN
- 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.

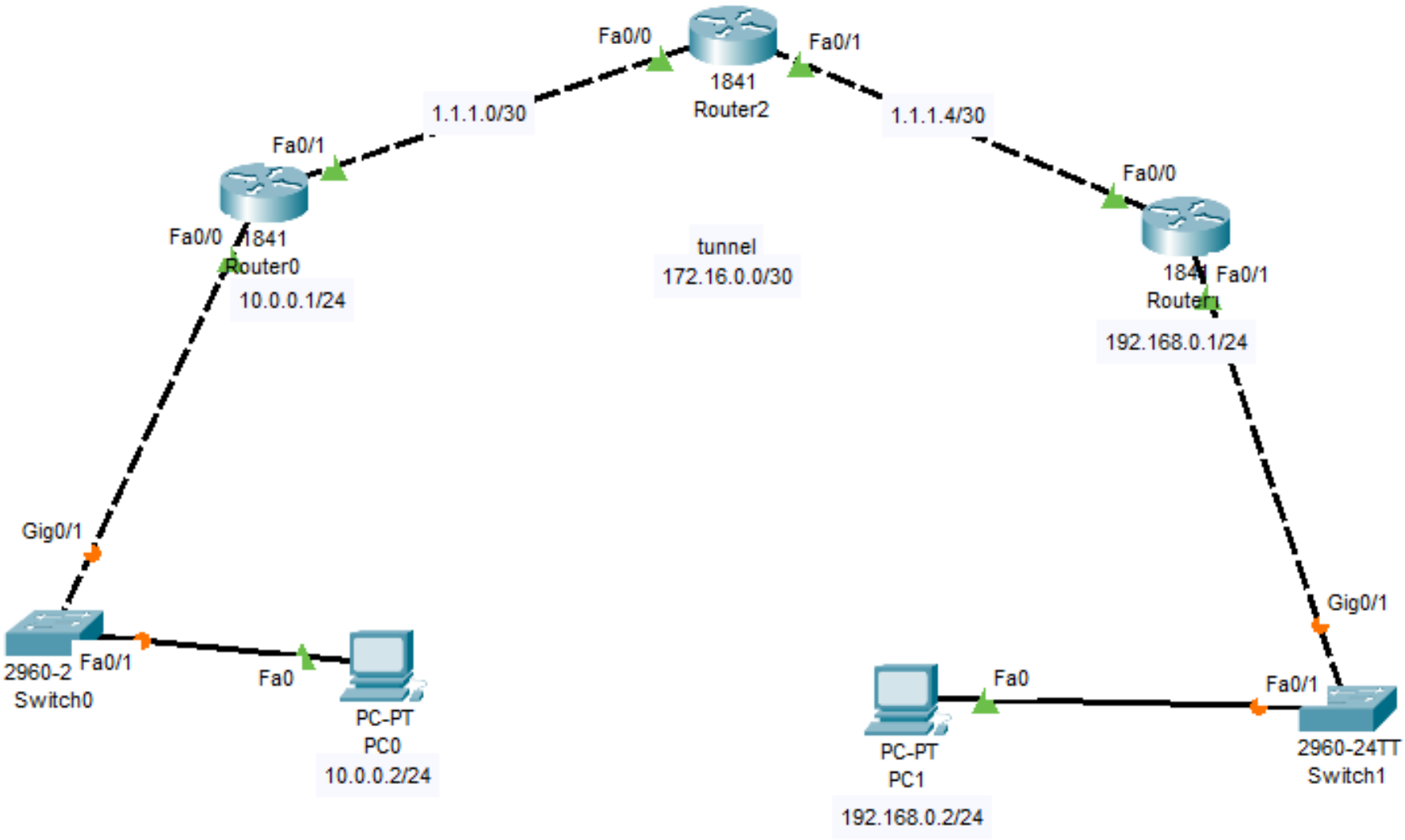
XOR Calculator:

https://xor.pw/

MD5 онлайн:

https://md5-online.ru/

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
```