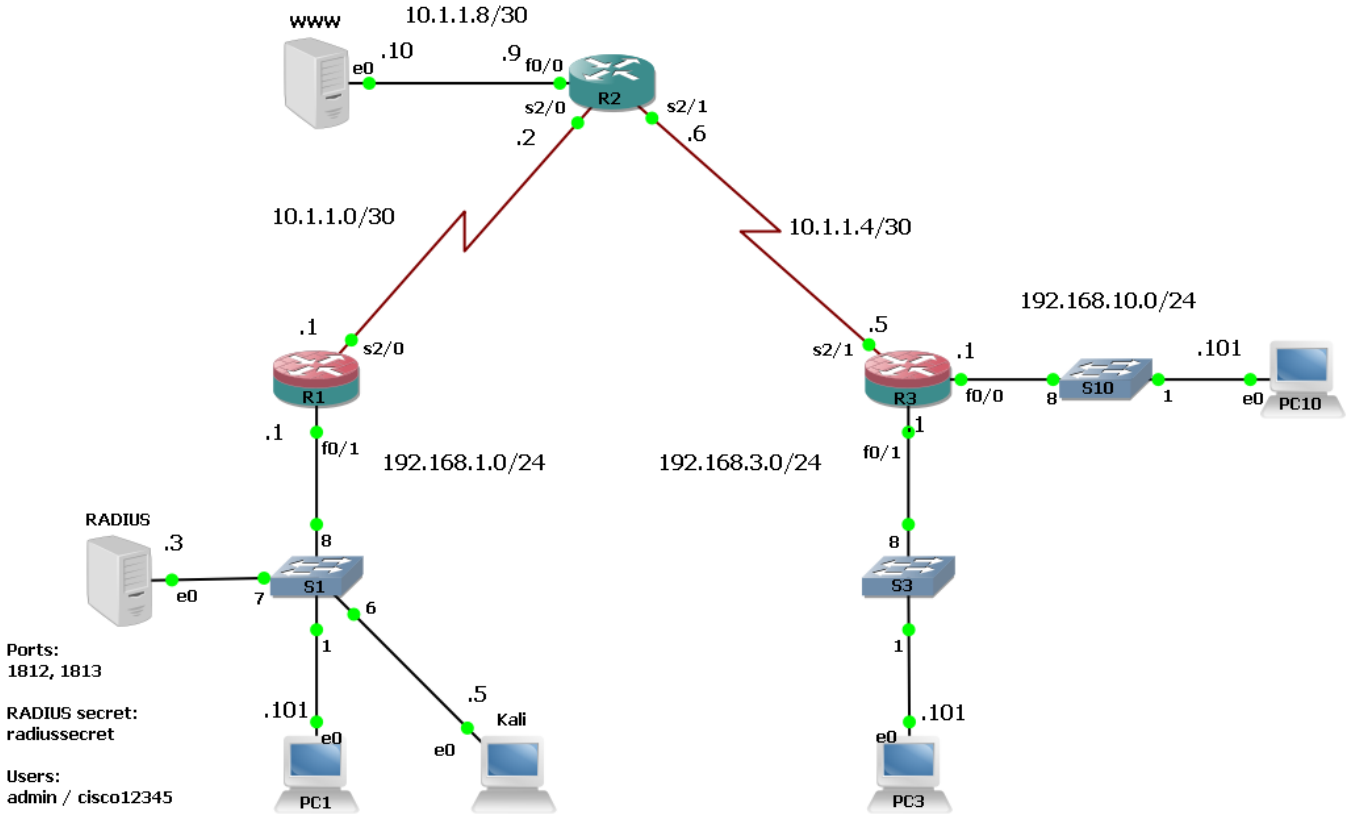
CCNA Security

Лабораторная работа 18

Настройка Site-To-Site IPsec VPN

Топология



Описание

В этой лабораторной работе вы настроите Enterprise Managed Site-To-Site IPsec VPN между маршрутизаторами R1 и R3, чтобы устройства из сетей 192.168.1.0/24 и 192.168.3.0/24 смогли безопасно связаться друг с другом.

Таблица адресации

Устройство	Интерфейс	IPv4-адрес/Маска подсети	Шлюз по умолчанию	Описание
R1	Fa0/1	192.168.1.1/24	-	LAN interface
	Se2/0	10.1.1.1/30	-	WAN interface (To R2)
R2	Se2/0	10.1.1.2/30	-	To R1
	Se2/1	10.1.1.6/30	-	To R3
	Fa0/0	10.1.1.9/30	-	To WWW server
R3	Fa0/1	192.168.3.1/24	-	LAN interface
	Fa0/0	192.168.10.1/24	-	Conference Room
	Se2/1	10.1.1.5/30	-	WAN interface (To R2)
PC1	NIC	192.168.1.101/24	192.168.1.1	-
PC2	NIC	192.168.3.101/24	192.168.3.1	-
PC10	NIC	192.168.10.101/24	192.168.10.1	-
Kali	NIC	192.168.1.5/24	192.168.1.1	-
RADIUS	NIC	192.168.1.3/24	192.168.1.1	-
WWW	NIC	10.1.1.10/24	10.1.1.9	-

Имена пользователей и пароли

	Console		VTY		Enable
Устройство	Имя пользователя	Пароль	Имя пользователя	Пароль	Пароль
R1	admin	cisco12345	admin	cisco12345	cisco12345
R2	-	-	-	-	-
R3	admin	cisco12345	admin	cisco12345	cisco12345

Устройство	Имя пользователя	Пароль
PC1	Student1	1
PC2	Student1	1
PC10	Student1	1
Kali	root	toor

Часть 1: Настройка на маршрутизаторе R1

1. Перейдите в консоль маршрутизатора R1.

2. Войдите в режим конфигурирования.
   R1# **conf t**

3. Включите протокол ISAKMP.
   R1(config)# **crypto isakmp enable**

4. Посмотрите существующие по умолчанию политики ISAKMP.

```
R1(config)# do show crypto isakmp default policy

Default IKE policy
Default protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 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 of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65514
```

```
encryption algorithm:    Three key triple DES
hash algorithm:          Message Digest 5
authentication method:   Pre-Shared Key
Diffie-Hellman group:    #2 (1024 bit)
lifetime:                86400 seconds, no volume limit
```

5. Мы могли бы воспользоваться одной из политик по умолчанию, но не будем. Создайте политику ISAKMP и изучите поддерживаемые алгоритмы хеширования и шифрования. Политика ISAKMP – это параметры защиты служебного траффика. При настройке помните про аббревиатуру HELGA: Hash, Encryption, Lifetime, Group, Authentication. Политика будет единственной, поэтому её приоритет не имеет особого значения, главное, чтобы приоритет был больше, чем приоритет у политик по умолчанию. Выберите хеш-функцию SHA, алгоритм AES с длиной ключа 256 бит, группу DH 14, аутентификацию по общему ключу, установите время жизни ключей в 1 час (3600 секунд). Время жизни устанавливать не обязательно, потому что по умолчанию оно и так будет равняться одному часу. При указании алгоритма шифрования AES обязательно укажите длину ключа, если длину не указать, то подразумевается длина ключа в 128 бит.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# hash ?
  md5     Message Digest 5
  sha     Secure Hash Standard
  sha256  Secure Hash Standard 2 (256 bit)
  sha384  Secure Hash Standard 2 (384 bit)
  sha512  Secure Hash Standard 2 (512 bit)
R1(config-isakmp)# hash sha
R1(config-isakmp)# encryption ?
  3des  Three key triple DES
  aes   AES - Advanced Encryption Standard.
  des   DES - Data Encryption Standard (56 bit keys).
R1(config-isakmp)# encryption aes ?
  128  128 bit keys.
  192  192 bit keys.
  256  256 bit keys.
  <cr>
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# group ?
  1   Diffie-Hellman group 1 (768 bit)
  14  Diffie-Hellman group 14 (2048 bit)
  15  Diffie-Hellman group 15 (3072 bit)
  16  Diffie-Hellman group 16 (4096 bit)
  19  Diffie-Hellman group 19 (256 bit ecp)
  2   Diffie-Hellman group 2 (1024 bit)
  20  Diffie-Hellman group 20 (384 bit ecp)
  21  Diffie-Hellman group 21 (521 bit ecp)
  24  Diffie-Hellman group 24 (2048 bit, 256 bit subgroup)
  5   Diffie-Hellman group 5 (1536 bit)
R1(config-isakmp)# group 14
R1(config-isakmp)# authentication ?
  pre-share  Pre-Shared Key
```

```
  rsa-encr    Rivest-Shamir-Adleman Encryption
  rsa-sig     Rivest-Shamir-Adleman Signature
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# exit
```

6. Проверьте созданную политику ISAKMP.

```
R1(config)# do show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #14 (2048 bit)
        lifetime:               3600 seconds, no volume limit
```

7. Настройте параметры общего ключа для аутентификации другой стороны. Обычно при использовании общего ключа генерируют случайную строку символов в 60, но мы для простоты так делать не будем. В параметре address необходимо указать внешний «белый» адрес другой стороны, у маршрутизатора R3 это адрес 10.1.1.5 (хотя он не выглядит как внешний). Помните, что этот ключ нужен только для аутентификации, он никак не связан с ключом шифрования, ключи шифрования будут генерироваться автоматически с помощью алгоритма DH.

```
R1(config)# crypto isakmp key cisco12345 address 10.1.1.5
```

8. Проверьте параметры общего ключа. Общий ключ будет храниться в конфигурации в открытом виде.

```
R1(config)# do show crypto isakmp key
Keyring      Hostname/Address                                Preshared Key

default      10.1.1.5                                        cisco12345

R1(config)# do show run | i isakmp key
crypto isakmp key cisco12345 address 10.1.1.5
```

9. Создайте набор преобразований (transform-set) и изучите поддерживаемые протоколы, алгоритмы хеширования и шифрования. Набор преобразований – это параметры защиты передаваемых данных. Выберите протокол ESP, хеш-функцию SHA, алгоритм AES с длиной ключа 256 бит. В подрежиме конфигурирования набора преобразований также можно выбрать режим работы протоколов AH или ESP: транспортный или тоннельный. По умолчанию режим тоннельный, что вполне нас устроит.

```
R1(config)# crypto ipsec transform-set TS_VPN_ESP ?
  ah-md5-hmac       AH-HMAC-MD5 transform
  ah-sha-hmac       AH-HMAC-SHA transform
  ah-sha256-hmac    AH-HMAC-SHA256 transform
  ah-sha384-hmac    AH-HMAC-SHA384 transform
  ah-sha512-hmac    AH-HMAC-SHA512 transform
  comp-lzs          IP Compression using the LZS compression algorithm
  esp-3des          ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes           ESP transform using AES cipher
  esp-des           ESP transform using DES cipher (56 bits)
  esp-gcm           ESP transform using GCM cipher
  esp-gmac          ESP transform using GMAC cipher
  esp-md5-hmac      ESP transform using HMAC-MD5 auth
```

```
  esp-null          ESP transform w/o cipher
  esp-seal          ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac      ESP transform using HMAC-SHA auth
  esp-sha256-hmac   ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac   ESP transform using HMAC-SHA384 auth
  esp-sha512-hmac   ESP transform using HMAC-SHA512 auth
```

```
R1(config)# crypto ipsec transform-set TS_VPN_ESP esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)# mode ?
  transport  transport (payload encapsulation) mode
  tunnel     tunnel (datagram encapsulation) mode
R1(cfg-crypto-trans)# exit
```

10. Проверьте созданный набор преобразований. Помимо созданного набора преобразований в выводе также указан набор преобразований default.

```
R1(config)# do show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set TS_VPN_ESP: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

11. Создайте список контроля доступа, в котором будет определён «интересный траффик». «Интересный траффик» - это траффик, который будет передаваться внутри тоннеля VPN. «Неинтересный траффик» будет выходить с интерфейса без изменений. Нас интересует любой траффик из сети 192.168.1.0/24 в сеть 192.168.3.0/24.

```
R1(config)# ip access-list extended ACL-VPN
R1(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config-ext-nacl)# exit
```

12. Проверьте созданный список контроля доступа.

```
R1(config)# do show ip access-list ACL-VPN
Extended IP access list ACL-VPN
    10 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

13. Создайте криптографическую карту (crypto map). Криптографическая карта свяжет вместе список контроля доступа с «интересным траффиком», адрес другой стороны, список преобразований. Криптографическая карта состоит из секций, внутри каждой секции есть условия, заданные с помощью параметра match, и действия, заданные с помощью параметра set. Если вам нужно построить множество тоннелей, то достаточно одной криптографической карты с множеством секций.

```
R1(config)# crypto map CRM_VPN_ESP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)# match address ACL-VPN
R1(config-crypto-map)# set peer 10.1.1.5
R1(config-crypto-map)# set transform-set TS_VPN_ESP
R1(config-crypto-map)# exit
```

14. Проверьте созданную криптографическую карту. Представленная команда довольно удобна, т.к. вся информация будет в развёрнутом виде.

```
R1(config)# do show crypto map
Crypto Map IPv4 "CRM_VPN_ESP" 10 ipsec-isakmp
        Peer = 10.1.1.5
        Extended IP access list ACL-VPN
            access-list ACL-VPN permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                TS_VPN_ESP:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map CRM_VPN_ESP:
```

15. Прилепите криптографическую карту ко внешнему интерфейсу, после чего проверьте параметры ещё раз.

```
R1(config)# int s2/0
R1(config-if)# crypto map CRM_VPN_ESP
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)# exit
R1(config)# do show crypto map
Crypto Map IPv4 "CRM_VPN_ESP" 10 ipsec-isakmp
        Peer = 10.1.1.5
        Extended IP access list ACL-VPN
            access-list ACL-VPN permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
        Current peer: 10.1.1.5
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                TS_VPN_ESP:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map CRM_VPN_ESP:
                Serial2/0
```

16. Протокол ISAKMP использует для своей работы транспортный протокол UDP и стандартные порты 500 и 4500. Проверьте, что маршрутизатор прослушивает данные порты.

```
R1(config)# do show control-plane host open-ports
Active internet connections (servers and established)
Prot          Local Address            Foreign Address                Service    State
 tcp                  *:22                      *:0                SSH-Server   LISTEN
 tcp                  *:23                      *:0                    Telnet   LISTEN
 udp                *:51419          192.168.1.101:514                Syslog ESTABLIS
 udp                  *:123                     *:0                       NTP   LISTEN
 udp                 *:4500                     *:0                    ISAKMP   LISTEN
 udp                  *:161                     *:0                  IP SNMP   LISTEN
 udp                  *:162                     *:0                  IP SNMP   LISTEN
 udp                  *:500                     *:0                    ISAKMP   LISTEN
 udp                *:60688                     *:0                  IP SNMP   LISTEN
```

17. Необходимо добавить исключения для NAT, чтобы пакеты в другой филиал уходили с оригинальными адресами. Для этого измените существующий список контроля доступа ACL-LAN, добавив в начало запрещающее правило.

```
R1(config)# do show ip access-list ACL-LAN
Extended IP access list ACL-LAN
    10 permit ip 192.168.1.0 0.0.0.255 any
```

```
R1(config)# ip access-list extended ACL-LAN
R1(config-ext-nacl)# 5 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config-ext-nacl)# exit
R1(config)# exit
R1# show ip access-list ACL-LAN
Extended IP access list ACL-LAN
    5 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
    10 permit ip 192.168.1.0 0.0.0.255 any
```

Часть 2: Изучение построения тоннеля

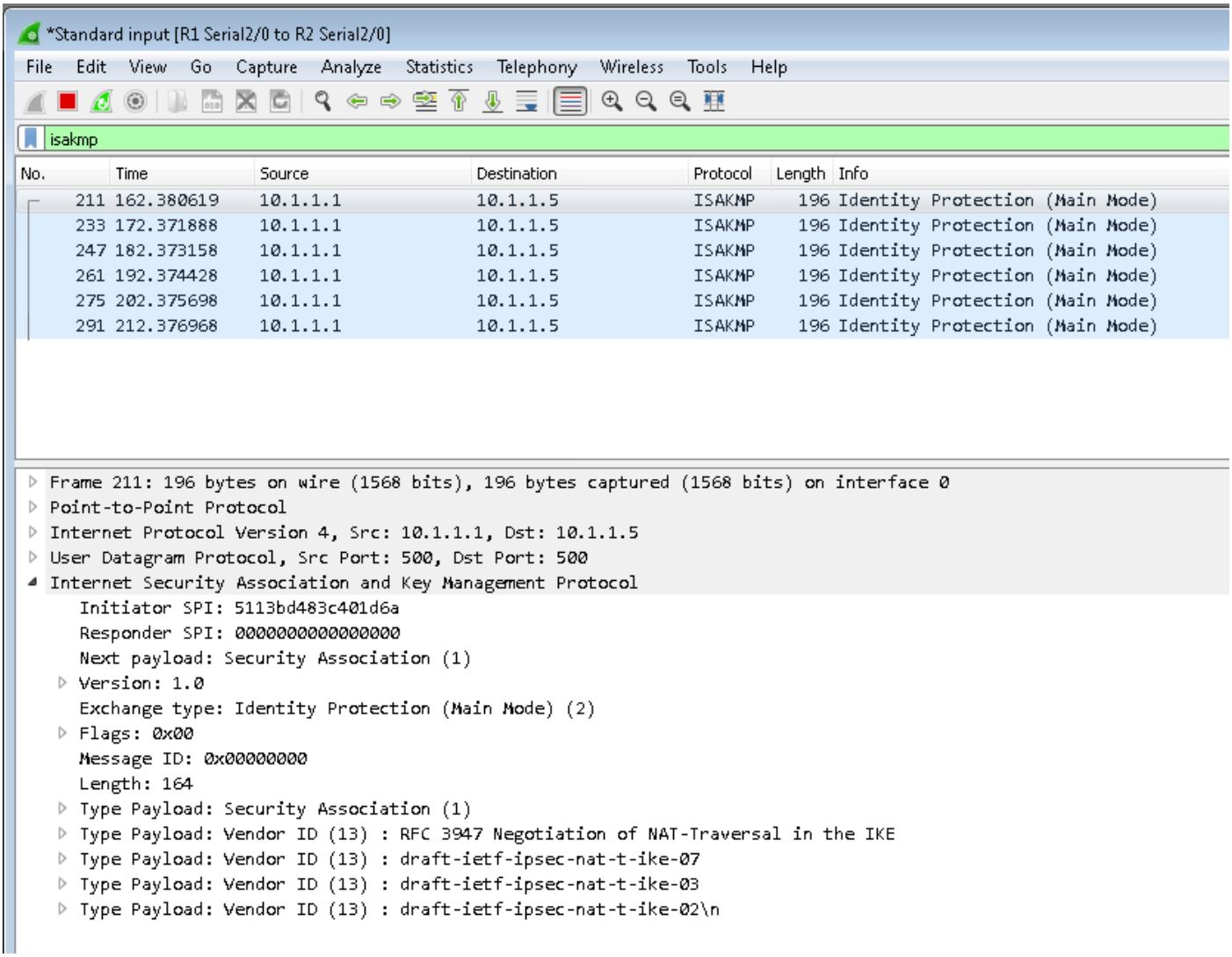
1. Вернитесь в основную машину. Запустите захват на линке между R1 и R2. Для этого в окне GNS3 щёлкните правой кнопкой мыши по линку между R1 и R2, в контекстном меню выберите **Start Capture**. В открывшемся окне выберите **R1 port Serial2/0 (Cisco PPP encapsulation: DLT_PPP_Serial)** и нажмите **OK**. Дождитесь открытия Wireshark.

2. Введите в поле Display Filter слово **isakmp** и нажмите Enter.

3. Войдите в виртуальную машину PC1.

4. Запустите командную строку. Попробуйте связаться с PC3 командой ping (ping 192.168.3.101). Проверка связи будет неуспешна, т.к. мы не провели симметричные настройки на маршрутизаторе R3. Помните, что тоннель не будет создан до тех пор, пока не появится «интересный траффик».

5. Вернитесь в Wireshark на основной машине. Вы увидите несколько пакетов протокола ISAKMP от маршрутизатора R1, но маршрутизатор R3 не отвечает.



6. Вернитесь в виртуальную машину PC1 и попробуйте связаться с PC3 ещё раз. Быстро перейдите к следующему шагу.

7. Вернитесь в консоль маршрутизатора R1.

8. Посмотрите список SA ISAKMP. В столбце state значится состояние MM_NO_STATE, что явно говорит о проблеме (нет никакого состояния), фаза 1 не состоялась. Через некоторое время SA будет помечена на удаление, а потом и вовсе пропадёт.

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.1.1.5        10.1.1.1        MM_NO_STATE          0 ACTIVE
< Вывод опущен >

R1# show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local            Remote           I-VRF  Status Encr Hash    Auth DH Lifetime Cap.
0     10.1.1.1         10.1.1.5               ACTIVE                0  0
       Engine-id:Conn-id =  ???
< Вывод опущен >

< Подождите некоторое время >
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.1.1.5        10.1.1.1        MM_NO_STATE          0 ACTIVE (deleted)
< Вывод опущен >

< Подождите некоторое время >
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
< Вывод опущен >
```

9. Хотя проверять фазу 2 без успешной фазы 1 нет особого смысла, посмотрите список SA IPsec. Счётчики пакетов равны нулю, а в списках inbound esp sas и outbound esp sas – пусто.

```
R1# show crypto ipsec sa

interface: Serial2/0
    Crypto map tag: CRM_VPN_ESP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.1.1.5 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #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 12, #recv errors 0

 local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.1.1.5
 path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
 current outbound spi: 0x0(0)
 PFS (Y/N): N, DH group: none

 inbound esp sas:
  < Обратите внимание, что тут пусто >
 inbound ah sas:

 inbound pcp sas:

 outbound esp sas:
  < Обратите внимание, что тут пусто >
 outbound ah sas:

 outbound pcp sas:
```

Часть 3: Настройка маршрутизатора R3

1. Перейдите в консоль маршрутизатора R3.

2. Войдите в режим конфигурирования.
```
R3# conf t
```

3. Включите протокол ISAKMP.
```
R3(config)# crypto isakmp enable
```

4. Создайте политику ISAKMP. Параметры политики будут в точности повторять параметры на маршрутизаторе R1.
```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# hash sha
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# lifetime 3600
R3(config-isakmp)# group 14
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# exit
```

5. Проверьте созданную политику ISAKMP.
```
R3(config)# do show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #14 (2048 bit)
           lifetime:               3600 seconds, no volume limit
```

6. Настройте параметры общего ключа для аутентификации другой стороны. В параметре address необходимо указать внешний «белый» адрес другой стороны, у маршрутизатора R1 это адрес 10.1.1.1. Ключ будет в точности повторять ключ на маршрутизаторе R1.
```
R3(config)# crypto isakmp key cisco12345 address 10.1.1.1
```

7. Проверьте параметры общего ключа.
```
R3(config)# do show crypto isakmp key
Keyring      Hostname/Address                                Preshared Key

default      10.1.1.1                                        cisco12345
```

8. Создайте набор преобразований (transform-set). Набор преобразований будет в точности повторять набор преобразований на маршрутизаторе R1.
```
R3(config)# crypto ipsec transform-set TS_VPN_ESP esp-aes 256 esp-sha-hmac
R3(cfg-crypto-trans)# exit
```

9. Проверьте созданный набор преобразований.
```
R3(config)# do show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },
```

```
Transform set TS_VPN_ESP: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

10. Создайте список контроля доступа, в котором будет определён «интересный траффик». Нас интересует любой траффик из сети 192.168.3.0/24 в сеть 192.168.1.0/24.

```
R3(config)# ip access-list extended ACL-VPN
R3(config-ext-nacl)# permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config-ext-nacl)# exit
```

11. Проверьте созданный список контроля доступа.

```
R3(config)# do show ip access-list ACL-VPN
Extended IP access list ACL-VPN
    10 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

12. Создайте криптографическую карту (crypto map).

```
R3(config)# crypto map CRM_VPN_ESP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)# match address ACL-VPN
R3(config-crypto-map)# set peer 10.1.1.1
R3(config-crypto-map)# set transform-set TS_VPN_ESP
R3(config-crypto-map)# exit
```

13. Проверьте созданную криптографическую карту.

```
R3(config)# do show crypto map
Crypto Map IPv4 "CRM_VPN_ESP" 10 ipsec-isakmp
        Peer = 10.1.1.1
        Extended IP access list ACL-VPN
            access-list ACL-VPN permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                TS_VPN_ESP:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map CRM_VPN_ESP:
```

14. Прилепите криптографическую карту ко внешнему интерфейсу, после чего проверьте параметры ещё раз.

```
R3(config)# int s2/1
R3(config-if)# crypto map CRM_VPN_ESP
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)# exit
R3(config)# do show crypto map
Crypto Map IPv4 "CRM_VPN_ESP" 10 ipsec-isakmp
        Peer = 10.1.1.1
        Extended IP access list ACL-VPN
            access-list ACL-VPN permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
        Current peer: 10.1.1.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                TS_VPN_ESP:  { esp-256-aes esp-sha-hmac  } ,
```

```
        }
        Interfaces using crypto map CRM_VPN_ESP:
                Serial2/1
```

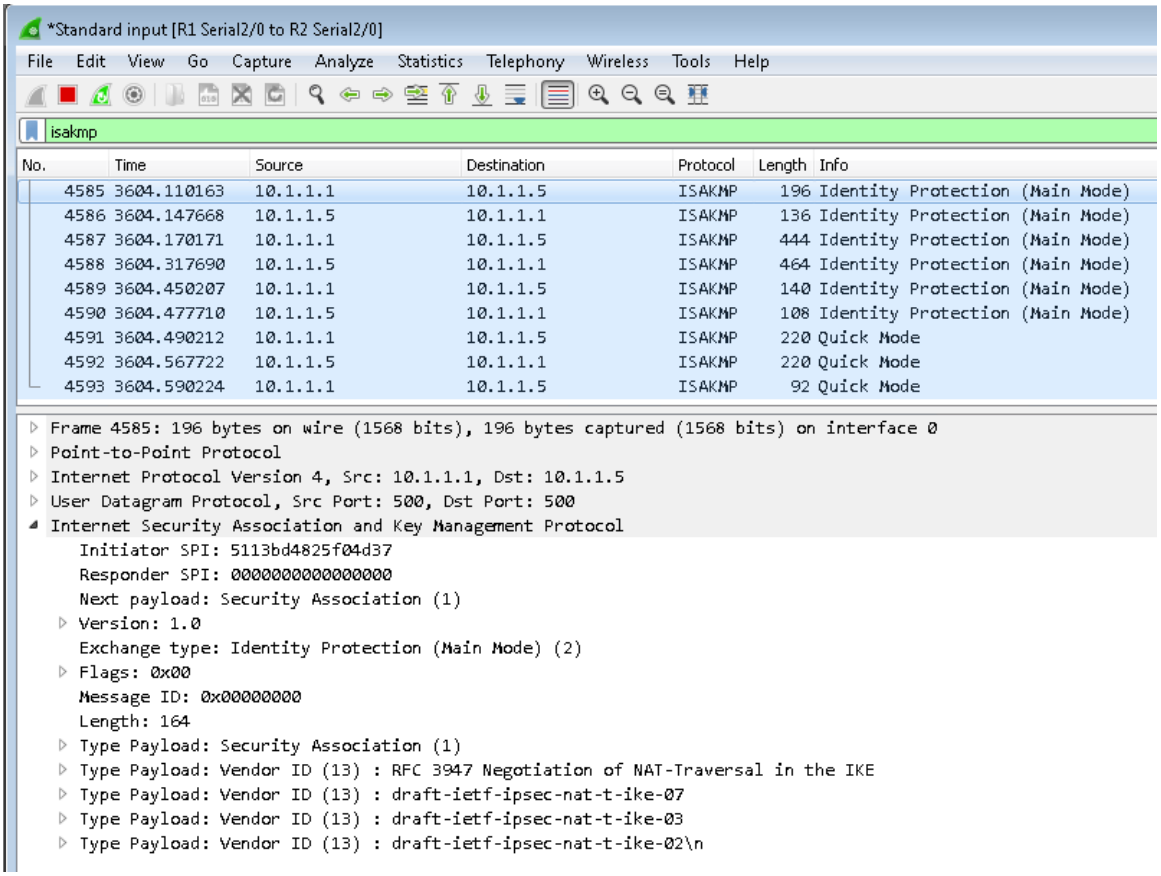
15. Необходимо добавить исключения для NAT, чтобы пакеты в другой филиал уходили с оригинальными адресами.

```
R3(config)# do show ip access-list ACL-LAN
Extended IP access list ACL-LAN
    10 permit ip 192.168.3.0 0.0.0.255 any
    20 permit ip 192.168.10.0 0.0.0.255 any
R3(config)# ip access-list extended ACL-LAN
R3(config-ext-nacl)# 5 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config-ext-nacl)# exit
R3(config)# exit
R3# show ip access-list ACL-LAN
Extended IP access list ACL-LAN
    5 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
    10 permit ip 192.168.3.0 0.0.0.255 any
    20 permit ip 192.168.10.0 0.0.0.255 any
```

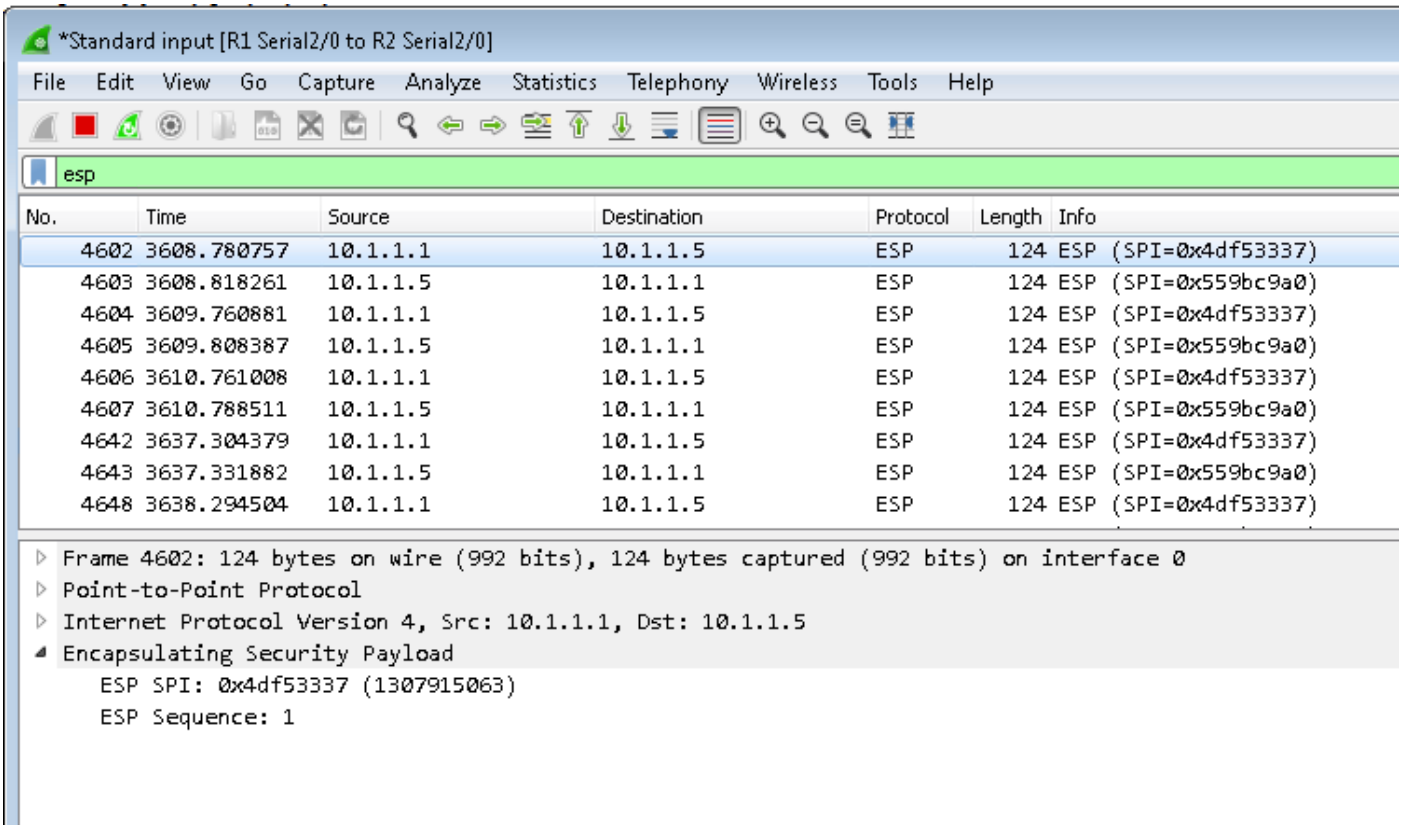
Часть 4: Практическая проверка

1. Вернитесь в виртуальную машину PC1 и попробуйте связаться с PC3 ещё раз. Пара пакетов вначале может потеряться, но в целом проверка будет успешна. Кратко перечислим, что происходило за кадром на маршрутизаторе R1:
   - Маршрутизатор установил выходной интерфейс s2/0 и адрес следующего перехода 10.1.1.2 согласно настроенному статическому маршруту по умолчанию;
   - Маршрутизатор установил, что пакет идёт с интерфейса, помеченного как ip nat inside на интерфейс, помеченный как ip nat outside. Маршрутизатор начал искать подходящее правило NAT. Ни под одно из правил пакет не подошёл, пакет не изменяется;
   - Маршрутизатор R1 пропускает исходящий пакет через криптографическую карту CRM_VPN_ESP. Пакет попадает под секцию 10, т.к. выполняется условие match address ACL-VPN, в списке контроля доступа ACL-VPN пакет попал под строчку permit;
   - Маршрутизатор R1 создаёт ISAKMP SA: согласуются политики ISAKMP, генерируются ключи с помощью DH, проводится аутентификация другой стороны по общему ключу;
   - Маршрутизатор R1 создаёт IPsec SA: согласуются политики IPsec, генерируются ключи с помощью DH;
   - Изначальный пакет целиком инкапсулируется внутрь ESP и уходит с интерфейса s2/0.

2. Вернитесь в Wireshark на основной машине. Вы увидите обмен пакетами протокола ISAKMP между маршрутизаторами R1 и R3. ISAKMP работает в двух режимах: Main Mode/MM (согласование параметров в шесть пакетов) и Quick Mode/QM (согласование параметров в три пакета).



3. Введите в поле Display Filter слово **esp** и нажмите Enter. Все данные между сетями 192.168.1.0/24 и 192.168.3.0/24 идут внутри протокола ESP. Выделите любой пакет и попробуйте что-нибудь разобрать. Сверните основное окно Wireshark.



4. Вернитесь в консоль маршрутизатора R1.

5. Проверьте список SA ISAKMP. Вы увидите состояние QM_IDLE (Quick Mode Idle), это нормальное состояние, сигнализирующее об успешности фазы 1. Также вы увидите параметры, на которые договорились маршрутизаторы, и тикающее время жизни.

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.1.1.5        10.1.1.1        QM_IDLE           1001 ACTIVE
< Вывод опущен >

R1# show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local            Remote           I-VRF  Status Encr Hash   Auth DH Lifetime Cap.

1001  10.1.1.1         10.1.1.5               ACTIVE aes  sha    psk  14 00:50:46
       Engine-id:Conn-id =  SW:1
< Вывод опущен >
```

6. Проверьте список SA IPsec. Счётчики пакетов наросли, а также заполнились списки inbound esp sas и outbound esp sas. Всё это указывает на успешность фазы 2.

```
R1# show crypto ipsec sa


interface: Serial2/0
    Crypto map tag: CRM_VPN_ESP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.1.1.5 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.1.1.5
     path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
     current outbound spi: 0x4DF53337(1307915063)
     PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
 spi: 0x559BC9A0(1436273056)
   transform: esp-256-aes esp-sha-hmac ,
   in use settings ={Tunnel, }
   conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map: CRM_VPN_ESP
   sa timing: remaining key lifetime (k/sec): (4147274/2764)
   IV size: 16 bytes
   replay detection support: Y
   Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0x4DF53337(1307915063)
   transform: esp-256-aes esp-sha-hmac ,
   in use settings ={Tunnel, }
   conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map: CRM_VPN_ESP
   sa timing: remaining key lifetime (k/sec): (4147274/2764)
   IV size: 16 bytes
   replay detection support: Y
   Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

7. Вернитесь в виртуальную машину PC1 и попробуйте связаться с сервером WWW командой ping (ping 10.1.1.10). Проверка связи будет успешна, но пакеты пойдут без изменений, т.к. этот траффик не является «интересным».
8. Вернитесь в Wireshark на основной машине. Введите в поле Display Filter **icmp.type == 0 or icmp.type == 8** и нажмите Enter. Вы увидите обычные пакеты протокола ICMP, что подтверждает сказанное на предыдущем шаге. После изучения закройте основное окно Wireshark.