Packet Tracer. Настройка сетей VPN (дополнительно)

Топология

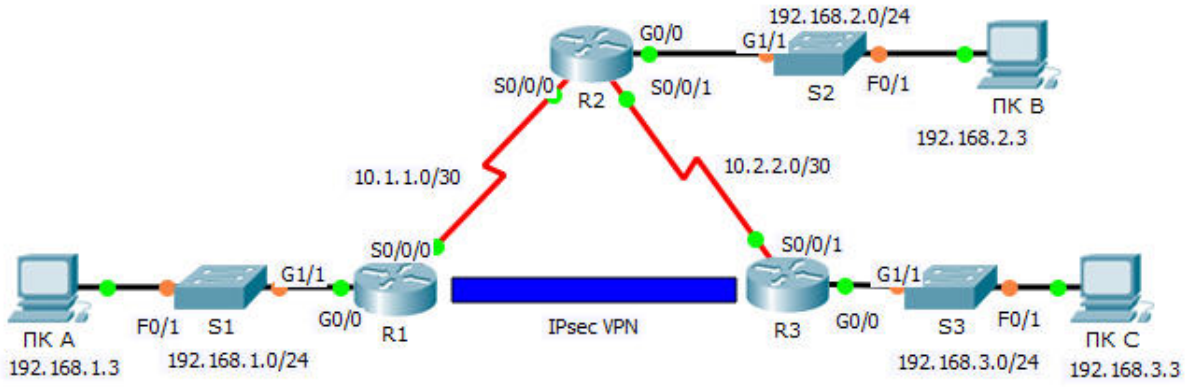

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
R2	G0/0	192.168.2.1	255.255.255.0	Недоступно
	S0/0/0	10.1.1.1	255.255.255.252	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
R3	G0/0	192.168.3.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.2	255.255.255.252	Недоступно
ПК A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
ПК B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
ПК C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Параметры политики 1 фазы ISAKMP

Параметры		R1	R3
Метод распространения ключей	Вручную или с помощью **ISAKMP**	ISAKMP	ISAKMP
Алгоритм шифрования	**DES**, 3DES или AES	AES	AES
Алгоритм хеширования	MD5 или **SHA-1**	SHA-1	SHA-1
Метод аутентификации	Общие ключи или **RSA**	pre-share	pre-share
Обмен ключами	Группа DH **1**, 2 или 5	DH 2	DH 2
Время жизни IKE SA	86400 секунд или меньше	86400	86400
Ключ ISAKMP		cisco	cisco

Параметры по умолчанию выделены **полужирным** шрифтом. Другие параметры необходимо указать явным образом.

Параметры политики 2 фазы IPsec

Параметры	R1	R3
Набор преобразований	VPN-SET	VPN-SET
Имя узла пира	R3	R1
IP-адрес пира	10.2.2.2	10.1.1.2
Сеть, трафик которой шифруется	192.168.1.0/24	192.168.3.0/24
Имя для криптографического сопоставления (crypto map)	VPN-MAP	VPN-MAP
Установка SA	ipsec-isakmp	ipsec-isakmp

Задачи

Часть 1. Включение функций безопасности

Часть 2. Настройка параметров IPsec на маршрутизаторе R1

Часть 3. Настройка параметров IPsec на маршрутизаторе R3

Часть 4. Проверка работы VPN IPsec

Сценарий

В этом задании необходимо на двух маршрутизаторах настроить поддержку межузловой сети VPN с использованием IPsec для трафика, проходящего между их соответствующими локальными сетями. IPsec-трафик VPN будет проходить через другой маршрутизатор, который не знает об использовании VPN. IPsec обеспечивает передачу конфиденциальной информации в защищённом режиме по незащищённым сетям, таким как Интернет. IPsec действует как протокол сетевого уровня, обеспечивая защиту и аутентификацию IP пакетов между участвующими в связи устройствами IPsec (равноправными узлами), такими как маршрутизаторы Cisco.

Часть 1: Включение функций безопасности

Шаг 1: Активируйте модуль securityk9.

Для выполнения этого задания должна быть включена лицензия пакета технологий обеспечения безопасности (Security) на маршрутизаторах R1 и R3.

Примечание. В качестве пароля как пользовательского, так и привилегированного режима используется **cisco**.

a. Введите команду **show version** в пользовательском или привилегированном режиме, чтобы убедиться, что лицензия пакета технологий безопасности активирована.

```
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
uc            None          None          None
data          None          None          None

Configuration register is 0x2102
```

b. Если это не так, активируйте модуль **securityk9** для следующей загрузки маршрутизатора, примите лицензию, сохраните настройку и перезагрузите маршрутизатор.

```
R1(config)# license boot module c2900 technology-package securityk9
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

c. После перезагрузки снова выполните команду **show version** для проверки активации лицензии пакета технологий безопасности.

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            None          None          None
data          None          None          None
```

d. Повторите шаги 1a-1c для маршрутизатора **R3**.

Часть 2: Настройте параметры IPsec на маршрутизаторе R1

Шаг 1: Проверьте связь.

Отправьте эхо-запрос с **ПК A** на **ПК C**.

Шаг 2: Определите интересующий трафик на маршрутизаторе R1.

Настройте ACL-список 110 таким образом, чтобы определить трафик из локальной сети на маршрутизаторе **R1** до локальной сети на маршрутизаторе **R3** как интересующий. Данный интересующий трафик будет активировать VPN IPsec при наличии трафика между локальными сетями маршрутизаторов **R1** и **R3**. Весь остальной трафик, передаваемый из этих локальных сетей, шифроваться не будет. Помните о действии неявного запрета «deny any» и о том, что добавлять данное правило в список не требуется.

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

Шаг 3: Настройте параметры 1 фазы ISAKMP на маршрутизаторе R1.

Настройте на маршрутизаторе **R1** свойства криптографической политики ISAKMP **10**, а также общий ключ шифрования **cisco**. Конкретные параметры, подлежащие настройке, приведены в таблице настроек 1 фазы ISAKMP. Значения по умолчанию настраивать не нужно, поэтому требуется настроить только шифрование, способ обмена ключами и метод DH.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 10.2.2.2
```

Шаг 4: Настройте параметры 2 фазы ISAKMP на маршрутизаторе R1.

Создайте набор преобразований (transform-set) **VPN-SET** для использования **esp-3des** и **esp-sha-hmac**. Затем создайте криптографическое сопоставление (crypto map) **VPN-MAP**, которое связывает вместе все параметры 2 фазы. Используйте порядковый номер **10** и определите его в качестве сопоставления **ipsec-isakmp**.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Шаг 5: Настройте криптографическое сопоставление для исходящего интерфейса.

Наконец, привяжите криптографическое сопоставление **VPN-MAP** к исходящему интерфейсу Serial 0/0/0. **Примечание.** Данный этап не оценивается.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP
```

Часть 3: Настройка параметров IPsec на маршрутизаторе R3

Шаг 1: Настройте маршрутизатор R3 для поддержки сети VPN между площадками с маршрутизатором R1.

Теперь настройте параметры передачи на обоих направлениях маршрутизатора **R3**. Настройте ACL-список **110** так, чтобы определить трафик из локальной сети маршрутизатора **R3** до локальной сети маршрутизатора **R1** как интересующий.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

Шаг 2: Настройте параметры 1 фазы ISAKMP на маршрутизаторе R3.

Настройте на маршрутизаторе **R3** свойства криптографической политики ISAKMP **10**, а также общий ключ шифрования **cisco**.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.2
```

Шаг 3: Настройте параметры 2 фазы ISAKMP на маршрутизаторе R1.

Аналогично действиям для маршрутизатора **R1**, создайте набор преобразований (transform-set) **VPN-SET** для **esp-3des** и **esp-sha-hmac**. Затем создайте криптографическое сопоставление (crypto map) **VPN-MAP**, которое связывает вместе все параметры 2 фазы. Используйте порядковый номер **10** и определите его в качестве сопоставления **ipsec-isakmp**.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

Шаг 4: Настройте криптографическое сопоставление для исходящего интерфейса.

Наконец, привяжите криптографическое сопоставление **VPN-MAP** к исходящему интерфейсу Serial 0/0/1. **Примечание**. Данный этап не оценивается.

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```

Часть 4: Проверка работы VPN по IPsec

Шаг 1: Проверьте туннель до прохождения по нему интересующего трафика.

Введите команду **show crypto ipsec sa** на маршрутизаторе **R1**. Обратите внимание, что количество всех пакетов (инкапсулированных, зашифрованных, декапсулированных и дешифрованных) равно 0.

```
R1# show crypto ipsec sa
```

```
interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   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 10.2.2.2 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 0, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
<Данные опущены>
```

Шаг 2: Создание интересующего трафика.

Отправьте на компьютер **ПК С** эхо-запрос от компьютера **ПК А**.

Шаг 3: Проверьте туннель после прохождения интересующего трафика.

На маршрутизаторе **R1** повторно введите команду **show crypto ipsec sa**. Теперь обратите внимание, что количество пакетов стало больше 0. Это означает, что туннель сети VPN по IPsec работает.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   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 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #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

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0A496941(172583233)
<Данные опущены>
```

Шаг 4: Создание не интересующего трафика.

Отправьте на **ПК B** эхо-запрос от **ПК A**.

Шаг 5: Проверка туннеля.

На маршрутизаторе **R1** повторно введите команду **show crypto ipsec sa**. Наконец, обратите внимание, что количество пакетов не изменилось. Это означает, что не интересующий трафик не шифруется.