# Организация защищенного канала на основе IPSec

В качестве практической задачи предлагается настроить IPSec-туннель между двумя маршрутизаторами. Предполагается, что весь трафик, проходящий между маршрутизаторами, будет шифроваться на сетевом уровне, скрывая данные и адреса. Схема сети представлена на рис. 3.9.

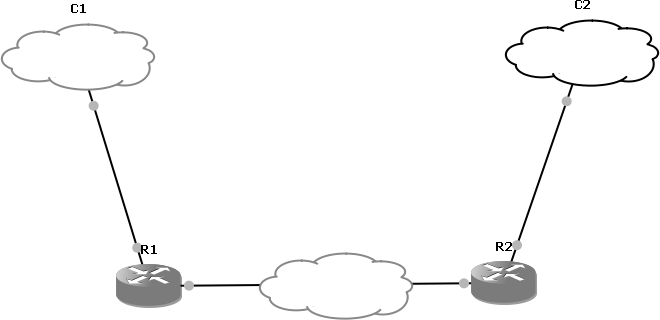


Рис. 3.9. Схема сети, состоящей из двух маршрутизаторов

Подробно рассмотрим настройку маршрутизатора R1. Настройка маршрутизатора R2 будет аналогичной. С1 – сеть с диа- пазоном IP-адресов 192.168.1.0/24. С2 – сеть с диапазоном IP-адресов 10.0.0.0/24. R1 – маршрутизатор, на котором задейство- ваны два интерфейса: fa1/1 соединен с сетью С1 и имеет IP-адрес 192.168.1.1, fa1/0 соединен с маршрутизатором R2 и имеет IP-адрес 22.22.22.1. R2 – маршрутизатор, на котором задействованы также два интерфейса: fa1/1 соединен с сетью С2 и имеет IP-адрес 10.0.0.1, fa1/0 соединен с маршрутизатором R1 и имеет IP-адрес 22.22.22.2.

Первый шаг заключается в назначении маршрутов и настрой- ке адресов интерфейсов. Для этого необходимо выполнить следу- ющую последовательность команд:

# Router>enable

!Переход в контекст администратора. По умолчанию пароль не установлен.

# Router#configuration terminal

!Переход в глобальный контекст конфигурирования.

# Router(config)#interface FastEthernet 1/1

!Переход в контекст конфигурирования интерфейса FastEthernet 1/1.

# Router(config-if)#ip address 192.168.1.1

**255.255.255.0**

!Назначение IP-адреса и маски сети.

# Router(config-if)#no shutdown

!Включение интерфейса.

# Router(config-if)#exit

!Выход из контекста конфигурирования интерфейса FastEthernet 1/1.

# Router(config)#interface FastEthernet 1/0

!Переход в контекст конфигурирования интерфейса FastEthernet 1/0.

# Router(config-if)#ip address 22.22.22.1

**255.255.255.0**

!Назначение IP-адреса и маски сети.

# Router(config-if)#no shutdown

!Включение интерфейса.

# Router(config-if)#exit Router(config)#ip route 0.0.0.0 0.0.0.0

**fastethernet 1/1 22.22.22.2**

!Указание маршрута по умолчанию.

## ВЫПОЛНИТЬ!

1. Произвести первоначальную настройку интерфейсов.

IPSec предлагает стандартные способы аутентификации и шифрования соединений. В IPSec применяются открытые стандар- ты согласования ключей шифрования и управления соединениями. Технология IPSec предлагает методы, позволяющие сторонам «до- говориться» о согласованном использовании сервисов. Для указа- ния согласуемых параметров в IPSec существуют ассоциации защиты.

Ассоциация защиты (SA) представляет собой согласованную политику или способ обработки данных, обмен которыми предпо- лагается осуществлять между двумя устройствами. Например, со- гласуется алгоритм, используемый для шифрования данных. Обе стороны могут применять один и тот же алгоритм как для шифро- вания, так и для дешифрования. Действующие параметры SA со-

храняются в базе данных ассоциаций защиты (SA Database – SAD)

обеих сторон.

Протокол IKE является гибридным протоколом, обеспечива- ющим аутентификацию сторон IPSec, согласование параметров ас- социаций защиты IKE и IPSec, а также выбор ключей для алгорит- мов шифрования. Протокол IKE опирается на протоколы ISAKMP и Oakley, которые применяются для управления процессом созда- ния и обработки ключей шифрования. IKE и ISAKMP, примени- тельно к маршрутизаторам Cisco, будем рассматривать как синони- мы.

Принцип работы IPSec можно представить в виде следующих шагов [12]:

1. Начало процесса IPSec. Устройство, которому требуется шифровать трафик в соответствии с политикой защиты IPSec, со- гласованной сторонами IPSec, начинает IKE-процесс.
2. Первая фаза IKE. IKE-процесс выполняет аутентификацию сторон IPSec и ведет переговоры о параметрах ассоциаций защиты IKE, в результате чего создается защищенный канал для ведения переговоров о параметрах ассоциаций защиты IPSec в ходе второй фазы IKE.
3. Вторая фаза IKE. IKE-процесс ведет переговоры о парамет- рах ассоциации защиты IPSec и устанавливает соответствующие ассоциации защиты IPSec для устройств общающихся сторон.
4. Передача данных. Происходит обмен данными между об- щающимися сторонами IPSec, который основывается на парамет- рах IPSec и ключах, хранимых в базе данных ассоциаций защиты.
5. Завершение работы туннеля IPSec. Ассоциации защиты IPSec завершают свою работу либо в результате их удаления, либо по причине превышения предельного времени их существования.

Настройка IKE:

# Router(config)#crypto isakmp enable

!Глобальная активизация IKE. Отменить IKE можно с помощью этой же команды, добавив в начало no.

# Router(config)#crypto isakmp policy 100

!Задание политики IKE. Здесь 100 – это приоритет, который одно- значно идентифицирует политику IKE. 1 – наивысший приоритет, 10000 – наименьший. Эта команда открывает контекст конфигури-

рования политики IKE, в котором можно устанавливать параметры IKE. Если в этом контексте не будет указана какая-либо команда, то для соответствующего параметра будет использоваться значение по умолчанию.

# Router(config-isakmp)#hash md5

!Алгоритм хэширования сообщений – md5. Также можно использо- вать rsa.

# Router(config-isakmp)#authentication pre-share

!Параметры обмена ключами – используем заранее согласованные ключи.

# Router(config-isakmp)#exit

!Выход из контекста конфигурирования политики IKE.

# Router(config)#crypto isakmp key 12345 address 22.22.22.2

!Выбор общих ключей аутентификации. Ключ следует определять каждый раз, когда в политике IKE указывается использование зара- нее согласованных общих ключей. Здесь 12345 – общий ключ. Для задания ключа можно использовать любую буквенно- цифровую комбинацию длиной до 128 бит. Значения общих клю- чей должны быть одинаковы в устройствах обеих сторон. Address – задание IP-адреса другой стороны, может использоваться также и имя хоста, если вместо address подставить hostname.

## ВЫПОЛНИТЬ!

1. Произвести настройку IKE.

Следующим шагом производится настройка IPSec.

# Router(config)#crypto ipsec transform-set r1 esp-des esp-md5-hmac

!Определение набора преобразований, представляющего собой со- вокупность конкретных алгоритмов IPSec, с помощью которых ре- ализуется политика защиты для выбранного трафика. В рамках ас- социации защиты IKE выполняются операции согласования, в результате чего стороны соглашаются использовать конкретный набор преобразований для защиты потока данных. Набор преобра- зований определяется с помощью команды глобальной конфигура- ции crypto ipsec transform-set, активизирующей конфигурационный контекст cfg-crypto-trans. Параметры команды:

# Router(config)#crypto ipsec transform-set

**<набор> <преобразование>**

В примере: набор – r1; преобразование esp-des – преобразова- ние ESP, использующее шифр DES (56 бит); esp-md5-hmac – преоб- разование ESP с аутентификацией HMAC-MD5; используется в комбинации с esp-des и esp-3des для обеспечения целостности паке- тов ESP.

# Router(cfg-crypto-trans)#exit

!Выход из конфигурационного контекста cfg-crypto-trans.

# Router(config)#crypto map r1map 100 ipsec-isakmp

!Настройка криптографической карты. Здесь r1map – имя карты, 100 – порядковый номер (приоритет), ipsec-isakmp – требование ис- пользовать IKE при создании ассоциаций защиты IPSec для трафи- ка, определяемого новой записью криптографической карты. При вводе данной команды открывается контекст конфигурирования криптографической карты.

# Router(config-crypto-map)#set peer 22.22.22.2

!Идентификация IPSec-партнера с помощью IP-адреса или имени хоста. Можно указать несколько адресов для реализации стратегии резервирования.

# Router(config-crypto-map)#set transform-set r1

!Указание списка наборов преобразований. Здесь – r1.

# Router(config-crypto-map)#match address 151

!Идентификация расширенного списка доступа, используемого криптографической картой. Здесь 151 – номер списка.

# Router(config-crypto-map)#exit

!Выход из контекста конфигурирования криптографической карты.

# Router(config)#interface FastEthernet 1/0

!Переход в контекст конфигурирования интерфейса FastEthernet 1/0.

# Router(config-if)#ip access-group 101 in

!Указание на использование списка доступа № 101 для контроля входного трафика на этом интерфейсе.

# Router(config-if)#crypto map r1map

!Применение набора записей криптографической карты к этому ин- терфейсу.

# Router(config-if)#exit

!Выход из контекста конфигурирования интерфейса.

## ВЫПОЛНИТЬ!

1. Провести настройку IPSec.

Заключительным шагом является настройка списков доступа.

# Router(config)#access-list 101 permit ahp host

**22.22.22.2 host 22.22.22.1**

!Задание расширенного списка доступа № 101, разрешающего вхо- дящий трафик протокола AHP с удаленного маршрутизатора.

# Router(config)#access-list 101 permit esp host

**22.22.22.2 host 22.22.22.1**

!Задание расширенного списка доступа № 101, разрешающего вхо- дящий трафик протокола ESP с удаленного маршрутизатора.

# Router(config)#access-list 101 permit udp host

**22.22.22.2 host 22.22.22.1 eq isakmp**

!Задание расширенного списка доступа № 101, разрешающего вхо- дящий трафик протокола UDP с удаленного маршрутизатора на порт isakmp.

# Router(config)#access-list 151 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.0.255

!Задание расширенного списка доступа № 151, разрешающего про- хождение IP-трафика со всех адресов сети 192.168.1.0/24 на все ад- реса сети 10.0.0.0/24.

# Router(config)#access-list 151 deny ip any any

!Запрет всего остального IP-трафика.

# Router(config)#exit

!Завершение конфигурирования.

## ВЫПОЛНИТЬ!

1. Произвести настройку списков доступа для лабораторной работы. Для второго маршрутизатора R2 настройка будет такой же. Ниже приведен список команд.

**Router#show ip interface**

**FastEthernet1/0 is up, line protocol is up Internet address is 22.22.22.2/24 Broadcast address is 255.255.255.255**

**Outgoing access list is not set Inbound access list is not set**

**FastEthernet1/1 is up, line protocol is up Internet address is 10.0.0.1/24 Broadcast address is 255.255.255.255 Outgoing access list is not set**

**Inbound access list is not set Router(config)#crypto isakmp enable Router(config)#crypto isakmp policy 100 Router(config-isakmp)#hash md5**

**Router(config-isakmp)#authentication pre-share Router(config)#crypto isakmp key 12345 address**

**22.22.22.1**

**Router(config)#crypto ipsec transform-set r2 esp-des esp-md5-hmac**

**Router(cfg-crypto-trans)#exit Router(config)#crypto ipsec transform-set r2**

**esp-des esp-md5-hmac**

**Router(cfg-crypto-trans)#exit Router(config)#crypto map r2map 100 ipsec-isakmp Router(config-crypto-map)#set peer 22.22.22.1 Router(config-crypto-map)#set transform-set r2 Router(config-crypto-map)#match address 151 Router(config-crypto-map)#exit Router(config)#int fa 1/0**

|  |  |  |
| --- | --- | --- |
| **Router(config-if)#ip access-group 101** | **in** |  |
| **Router(config-if)#crypto map r2map** |  |
| **Router(config-if)#exit** |  |
| **Router(config)#access-list 101 permit**  **22.22.22.1 host 22.22.22.2** | **ahp** | **host** |
| **Router(config)#access-list 101 permit**  **22.22.22.1 host 22.22.22.2** | **esp** | **host** |
| **Router(config)#access-list 101 permit** | **udp** | **host** |

**22.22.22.1 host 22.22.22.2 eq isakmp**

**Router(config)#access-list 151 permit ip**

**10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255**

**Router(config)#access-list 151 deny ip any any Router(config)#exit**

Сконфигурировав маршрутизаторы с помощью представлен- ных выше команд, мы получим шифрованный IPSec-туннель. На рисунках показан трафик с включенным шифрованием (рис. 3.10) и без шифрования (рис. 3.11).

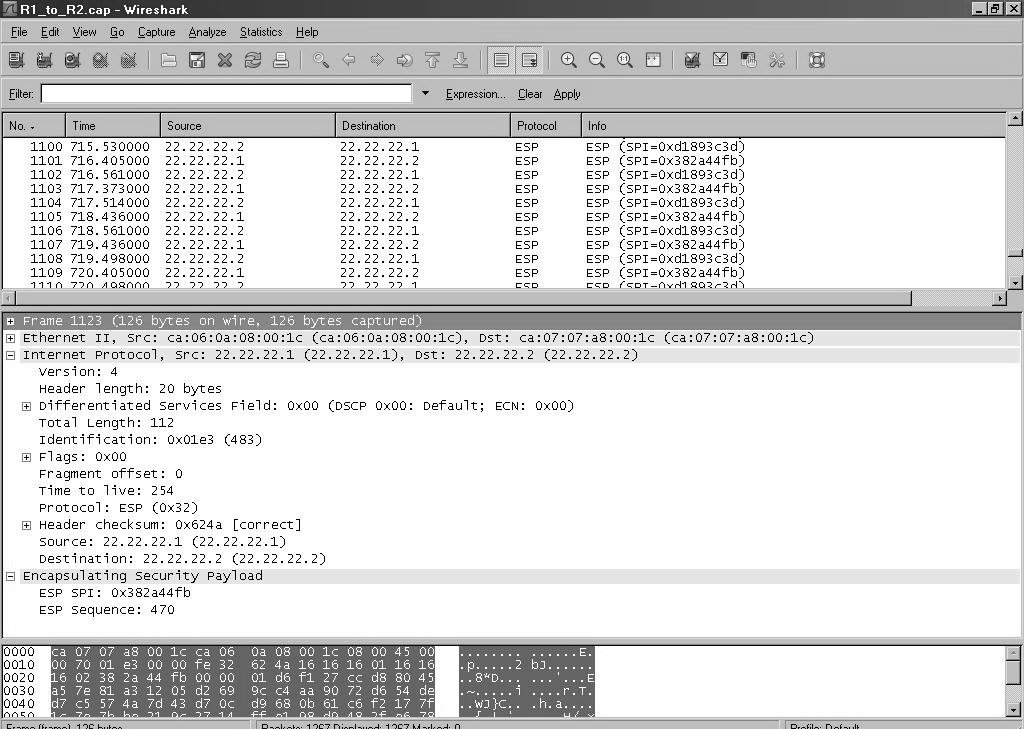


Рис. 3.10. Вид зашифрованного трафика

## ВЫПОЛНИТЬ!

1. Произвести настройку второго маршрутизатора.
2. Проверить с помощью захвата трафика работу шифрован- ного туннеля.