МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО КАНАЛА НА ОСНОВЕ IPSEC

Методические рекомендации по выполнению лабораторной работы №7
для студентов направления подготовки бакалавриата
10.03.01«Информационная безопасность»

Курск 2017

УДК 621.(076.1)

Составитель: А.Г. Спеваков

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» И.В. Калуцкий

Организация защищенного канала на основе IPSec [Текст]: методические рекомендации по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: А.Г. Спеваков. – Курск, 2017. – 13 с.: ил. 3. – Библиогр.: с. 13.

Содержат сведения по вопросам работы в программном продукте Cisco Packet Tracer. Указывается порядок выполнения лабораторной работы, правила содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 0,76. Уч.-изд. л. 0,68. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

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 рисунок 1.

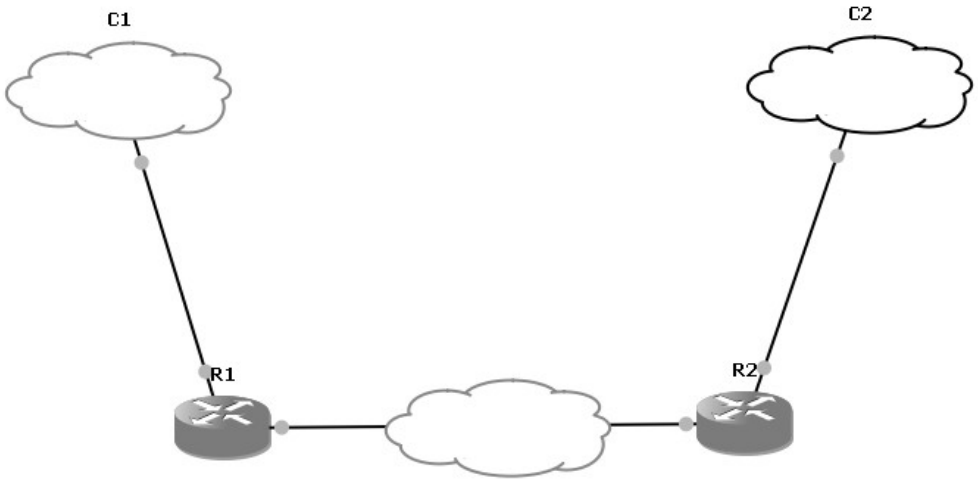

Рисунок 1 - Схема сети, состоящей из двух маршрутизаторов

Подробно рассмотрим настройку маршрутизатора R1. Настройка маршрутизатора R2 будет аналогичной. C1 – сеть с диапазоном IP-адресов 192.168.1.0/24. C2 – сеть с диапазоном IP-адресов 10.0.0.0/24. R1 – маршрутизатор, на котором задействованы два интерфейса: fa1/1 соединен с сетью C1 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 C2 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 настройке адресов интерфейсов. Для этого необходимо выполнить следующую 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 стандарты согласования ключей шифрования и управления соединениями. Технология IPSec предлагает методы, позволяющие сторонам «договориться» о согласованном использовании сервисов. Для указания согласуемых параметров в IPSec существуют ассоциации защиты.

Ассоциация защиты (SA) представляет собой согласованную политику или способ обработки данных, обмен которыми предполагается осуществлять между двумя устройствами. Например, согласуется алгоритм, используемый для шифрования

данных. Обе стороны могут применять один и тот же алгоритм как для шифрования, так и для дешифрования. Действующие параметры SA сохраняются в базе данных ассоциаций защиты (SA Database – SAD) обеих сторон.

Протокол IKE является гибридным протоколом, обеспечивающим аутентификацию сторон IPSec, согласование параметров ассоциаций защиты IKE и IPSec, а также выбор ключей для алгоритмов шифрования. Протокол IKE опирается на протоколы ISAKMP и Oakley, которые применяются для управления процессом создания и обработки ключей шифрования. IKE и ISAKMP, применительно к маршрутизаторам Cisco, будем рассматривать как синонимы.

Принцип работы IPSec можно представить в виде следующих шагов:

1. Начало процесса IPSec. Устройство, которому требуется шифровать трафик в соответствии с политикой защиты IPSec, согласованной 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 параметрах ассоциации защиты IPSec и устанавливает соответствующие ассоциации защиты IPSec для устройств общающихся сторон.
4. Передача данных. Происходит обмен данными между общающимися сторонами IPSec, который основывается на параметрах 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 однозначно идентифицирует политику IKE. 1 – наивысший приоритет, 10000 – наименьший. Эта команда открывает контекст конфигурирования 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 использовать 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 заранее согласованных общих ключей. Здесь 12345 – общий ключ. Для задания ключа можно использовать любую буквенноцифровую комбинацию длиной до 128 бит. Значения общих ключей 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!

2. 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 совокупность конкретных алгоритмов IPSec, с помощью которых реализуется политика защиты для выбранного трафика. В рамках ассоциации защиты IKE выполняются операции

согласования, в результате чего стороны соглашаются использовать конкретный набор преобразований для защиты потока данных. Набор преобразований определяется с помощью команды глобальной конфигурации 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 – преобразование ESP, использующее шифр DES (56 бит); esp-md5-hmac – преобразование ESP с аутентификацией HMAC-MD5; используется в комбинации с esp-des и esp-3des для обеспечения целостности пакетов 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 использовать IKE при создании ассоциаций защиты IPSec для трафика, 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 интерфейсу.

Router(config-if)#exit

!Выход из контекста конфигурирования интерфейса.

ВЫПОЛНИТЬ!

3. 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 входящий 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 входящий 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 входящий 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 прохождение IP-трафика со всех адресов сети 192.168.1.0/24 на все адреса 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!

4. 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 ahp host 22.22.22.1 host 22.22.22.2

Router(config)#access-list 101 permit esp host 22.22.22.1 host 22.22.22.2

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 представленных выше команд, мы получим шифрованный IPSec-туннель. На рисунках показан трафик с включенным шифрованием (рисунок 2) и без шифрования (рисунок 3).

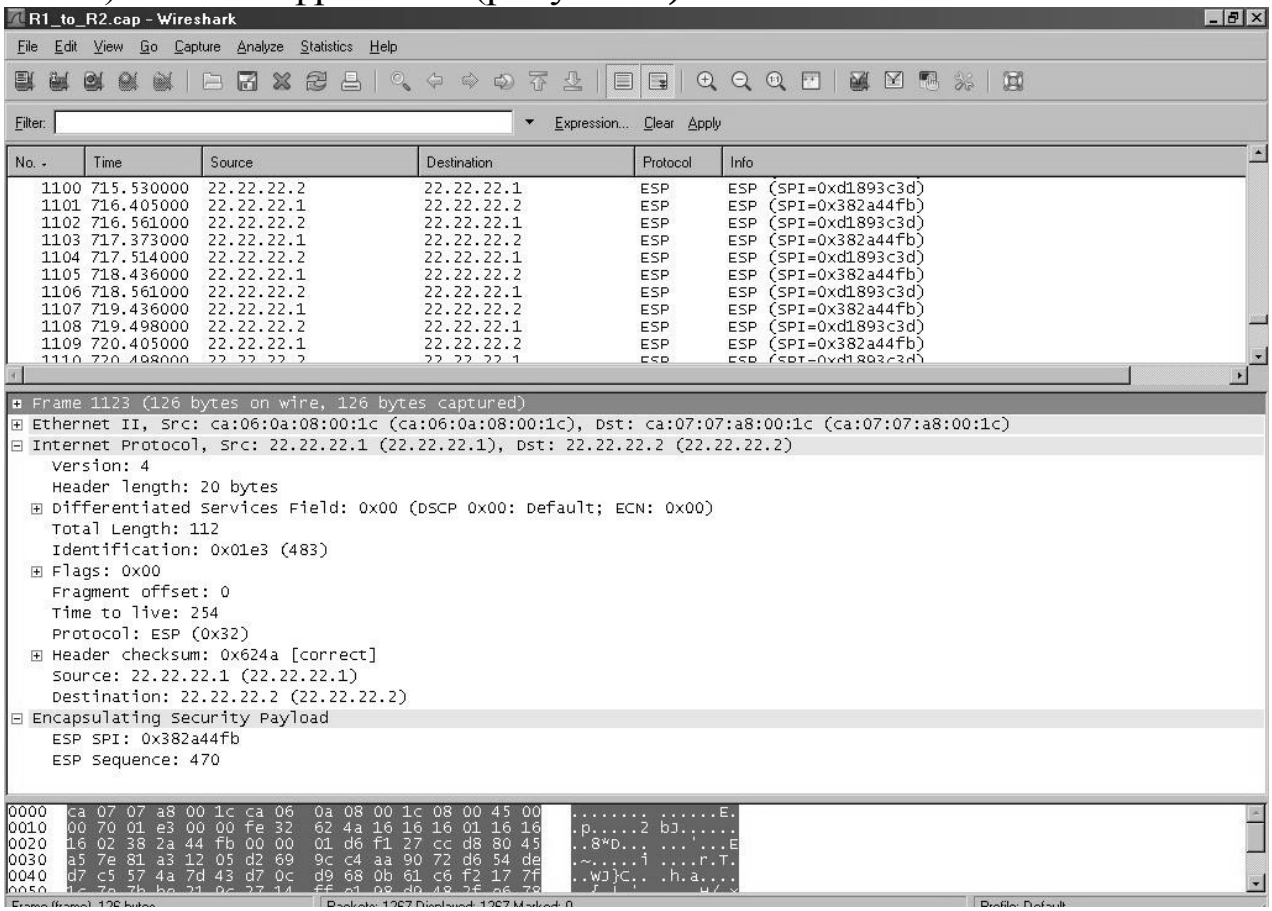

Рисунок 2 - Вид зашифрованного трафика

ВЫПОЛНИТЬ!

5. Произвести настройку второго маршрутизатора.

6. Проверить с помощью захвата трафика работу шифрованного туннеля.

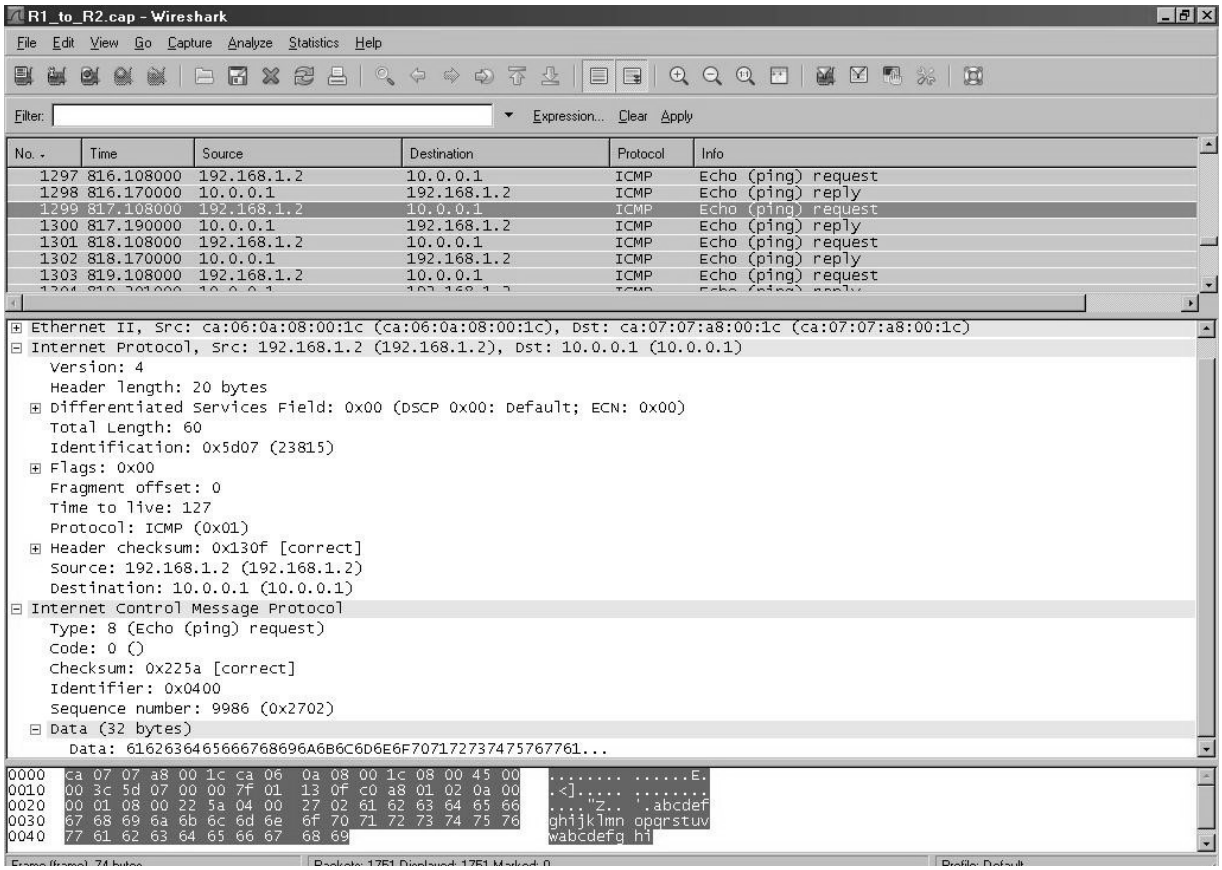

Рисунок 3 - Вид трафика без шифрования

Вопросы для проверки знаний

1. В чем состоит ограничение при использовании стандартных списков доступа?
2. Какие сетевые протоколы поддерживаются при создании правил расширенных списков доступа?
3. В чем состоит преимущество использования динамических обратных списков доступа перед другими?
4. Объяснить понятие уровня безопасности интерфейса Cisco PIX Firewall.
5. Назвать виды NAT и дать им краткую характеристику.
6. Назвать преимущества использования технологии NAT при подключении к открытым сетям.
7. Какова роль протокола IKE при организации IPSec-туннеля?

Библиографический список

1. Защита информации в компьютерных сетях. Практический курс : учеб. пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский [и др.] ; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.

2. Americas Headquarters Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x. – USA : Cisco Systems, 2009. – 136 p.

3. Gary Hallen, G. Kellogg Security Monitoring with Cisco Security MARS. – USA : Cisco Press, 2007. – 335 p.

4. James Burton, Ido Dubrawsky, Vitaly Osipov Cisco Security Professional's Guide to Secure Intrusion Detection Systems. – USA : Syngress Publishing, 2003. – 673 p.

5. Installation Guide for the Cisco Secure PIX Firewall Version 5.2. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

6. Install and Setup Guide for Cisco Security Monitoring Analysis and Response System. Release 4.3.x., 2008. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

7. Стивенс У. Р. Протоколы TCP/IP. Практическое руководство / пер. с англ. – СПб. : БХВ-Петербург, 2003. – 672 с.

8. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб. : Питер, 2001. – 320 с.