**Домашнее задание**

|  |  |
| --- | --- |
| Дисциплина | Защита компьютерных сетей и систем |
| Тема | Тема 29. Криптография |
| Форма проверки | **Самостоятельная проверка на лабораторном стенде** |
| Имя преподавателя | Денис Бубнов |
| Время выполнения | 180 минут |
| Цель задания | Научиться выполнять конфигурацию IPSec VPN на оборудовании Cisco |
| Инструменты для выполнения ДЗ | Компьютер, доступ в интернет, доступ к лабораторному стенду |
| Правила приёма работы | 1. Выполненная работа на лабораторном стенде в соответствии с распределённым вариантом.  2. Успешная установка VPN туннеля с партнёром |
| Критерии оценки | **Задание считается выполненным, если** установлен туннель IPSec VPN с маршрутизатором партнёра.  **Задание не выполнено, если** не установлен туннель IPSec VPN с маршрутизатором партнёра |
| Дедлайн | три недели после вебинара (точную дату см. в ЛМС) |

**Описание задания**

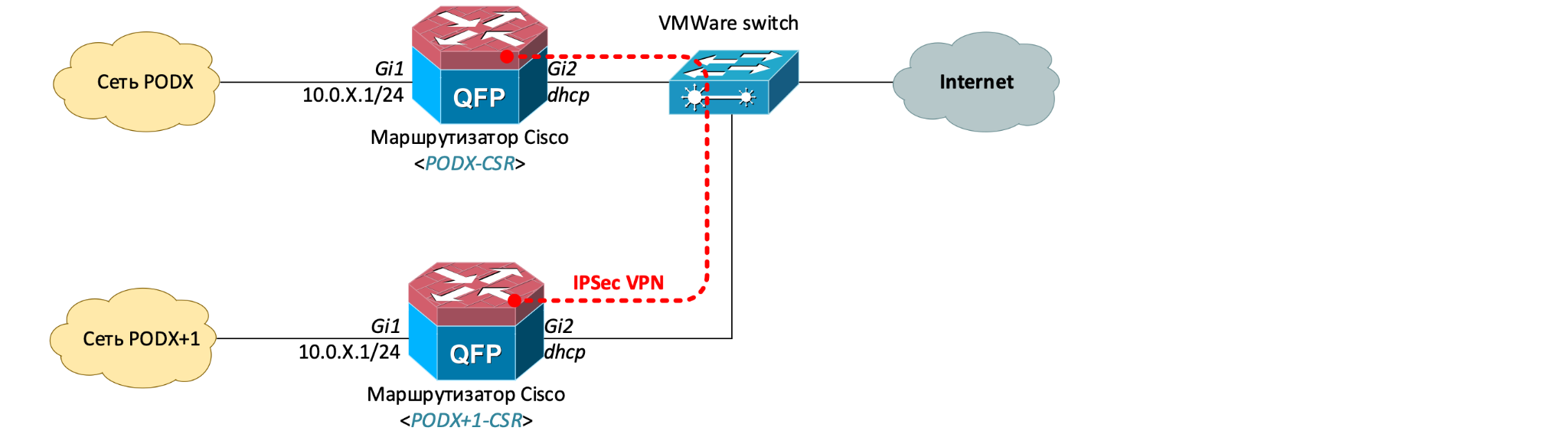
1. Прежде чем делать задание:
   1. Посмотрите лекцию и вебинар по теме №29 «Криптография».
   2. Выполните домашнее задание по теме №26 «Атаки на Active Directory», конфигурация маршрутизатора должна соответствовать целевой.
   3. Подключитесь к лабораторному стенду.

**Подключение к стендам:**

* Определите партнёра по работе согласно [списку](https://netospace.ru/drive/d/s/11Jgbp9VIVQO5rI1ZhAQyFVoLWLE7Nnd/DjOP304ZZoLG9_luPhxbanilKuwlgJv2-ZL_ADDso5Qs).
* Партнёры определяются по схеме «нечётный + чётный вариант». Партнёрами являются: вариант 1 + 2; вариант 3 + 4; вариант 5 + 6 и т. д.

2. Практическое задание

Схема лабораторного стенда



**План работы:**

1. Договориться о настройках с партнёром. Уточнить внешние адреса маршрутизаторов, получаемые по DHCP, согласовать ключ аутентификации.
2. Удалить конфигурацию NAT маршрутизатора.
3. Выполнить конфигурацию IPSec VPN.
4. Проверить работоспособность и наличие связи между внутренними сетями.

Порядок выполнения работы

1. **Договориться о настройках с партнёром. Уточнить внешние адреса маршрутизаторов, согласовать ключ аутентификации.**
   1. Связаться с партнёром по работе, договориться о времени выполнения настроек.
   2. Определить IP-адреса интерфейсов Gi2 (командой **show ip interfaces brief**).
   3. Согласовать использование PSK — общего ключа. Требование к общему ключу — длина не менее 12 символов.
2. **Удалить конфигурацию NAT маршрутизатора.**
   1. Удалить роли интерфейсов (ip nat inside, ip nat outside).
   2. Удалить трансляцию NAT.
3. **Выполнить конфигурацию IPSec VPN.**
   1. Использовать расширенный ACL для определения трафика для VPN. Должен быть описан трафик, идущей от внутренней сети PODX к внутренней сети PODX + 1 партнёра. У партнёра должен быть создан зеркальный ACL.
   2. Создать запись для шлюза-партнёра с ключом аутентификации PSK. В качестве идентификатора использовать IP-адрес интерфейса Gi1 маршрутизатора партнёра.
   3. Определить набор политик для фазы 1 IKE. Использовать шифрование AES, хеширование SHA, группа DH5, аутентификация — PSK.
   4. Определить набор политик для фазы 2 IKE. Использовать режим **esp-aes esp-sha-hmac**. Режим работы VPN — туннельный.
   5. Определить настройки криптокарты.
   6. Применить криптокарту к интерфейсу Gi2 маршрутизатора.

**Пример конфигурации** (*использовать в качестве шаблона, который необходимо адаптировать, часть конфигурации опущена*)**:**

!hostname PODX-CSR

**//Политика IKE Phase1. Выбор параметров криптозащиты//**

!crypto isakmp policy 1

encryption aes

authentication pre-share

group 5

**//определение IP-адреса партнёра и PSK//**

crypto isakmp key 123PWD49rfj2@128 address 172.31.21.22

!

**//Политика для IKE Phase 2//**

crypto ipsec transform-set PODX esp-aes esp-sha-hmac

mode tunnel

!

!

**//создание параметров криптокарты//**

crypto map PODX 1 ipsec-isakmp

set peer 172.31.21.22 **//адрес партнера//**

set transform-set PODX

set pfs group5

match address 150 **//номер ACL для определения трафика для VPN//**

interface GigabitEthernet1

ip address 10.0.10.1 255.255.255.0

negotiation auto

no mop enabled

no mop sysid

!

interface GigabitEthernet2

ip address dhcp

negotiation auto

no mop enabled

no mop sysid

!

**//ACL для определения трафика для VPN//**

ip access-list extended 150

10 permit ip 10.0.10.0 0.0.0.255 10.0.11.0 0.0.0.255

!

!

!

!

!

1. **Проверить конфигурацию IPSec VPN.**
   1. Выполнить ping с любого внутреннего хоста в сети PODX любого внутреннего хоста партнера. Убедиться, что ping выполняется успешно.
   2. Выполнить команды:

* **show crypto isakmp sa,**
* **show crypto ipsec sa.**