Виртуальные частные сети. IPSec-туннель

Практическая часть

Цель работы:

Изучение защищенного IPSec-туннеля и способа его настройки на брандмауэре ASA5505 и в ОС *Arch Linux.*

Список используемых команд

Таблица 1 - Команды *Arch Linux* рабочих станций

Синтаксис	Описание
ifconfig <*имя интерфейса*> <*ip адрес*> netmask <*маска сети*> [*up/down*]	Настройка параметров интерфейса. Без параметров команда показывает список работающих интерфейсов
route add/del *[-net|-host]* [*default*] target [*gw*] [*netmask*] [[*dev*] *If*]	Настройка статической маршрутизации. Без параметров команда выводит таблицу маршрутизации
/etc/rc.d/<*имя сервиса*>	Запуск программ-демонов в ОС linux
lynx <*ip/имя*>	Консольный браузер
tcpdump [-*XX*] [-*i интерфейс*]	Сниффер пакетов. Без параметров слушает все интерфейсы и показывает только заголовки пакетов

Таблица 2 - Команды Cisco ASA

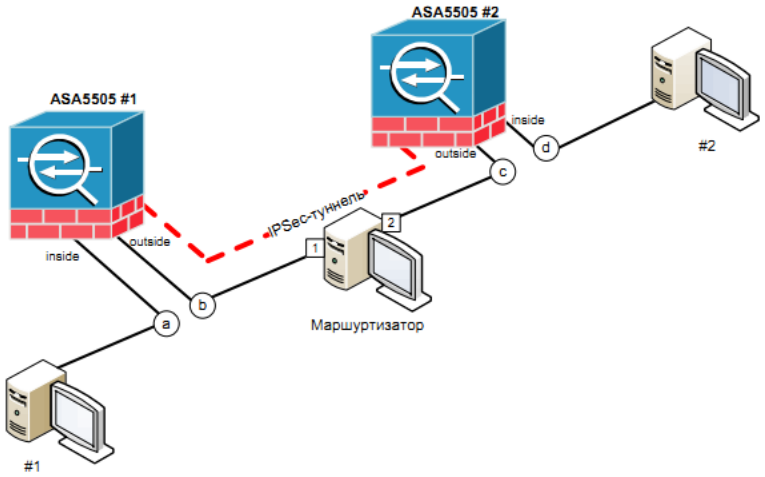
Синтаксис	Описание
en	Вход в привилегированный режим
configure terminal	Вход в режим конфигурации
sh <*сервис*>	Просмотр настроек
dhcp address <*пул адресов*> <*интерфейс*>	Настройка dhcp сервера на интерфейсе
int <*имя интерфейса*>	Вход в режим конфигурации интерфейса
nameif <*имя*>	Настройка имени интерфейса
security-level <*значение*>	Настройка параметра защищенности сети
ip address <*значение*> <*маска*>	Настройка адреса интерфейса
switchport access <*имя vlan*>	Размещение интерфейса в указанной vlan
route <*имя интерфейса*> <*сеть*> <*маска*> <*адрес шлюза*>	Настройка статической маршрутизации
nat (<*интерфейс*>) <*номер правила*> <*сеть*> <*маска*>	Настройка NAT\PAT для замещения адреса из сети указанного интерфейса
isakmp policy <*номер*> encryption <*значение*>	Выбор метода шифрования
isakmp policy <*номер*> hash <*значение*>	Выбор метода хеширования
isakmp policy <*номер*> authentication <*значение*>	Выбор метода аутентификации

isakmp policy <***номер***> **group** <***значение***>	Выбор группы Диффи-Хелмана
isakmp policy <***номер***> **lifetime** <***значение***>	Выбор lifetime соединения
isakmp enable <***имя интерфейса***>	Включение ISAKMP на интерфейсе
isakmp identity <***значение***>	Определение метода идентификации сторон
access-list <***имя\номер***> **[*permit\deny*] extended** <***тип трафика***> <***источник***> <***маска***> <***цель***> <***маска***>	Создание списка доступа для выделения необходимого трафика.
ipsec transform-set <***имя***> <***значение***>	Определение политики шифрования
map <***имя***> <***номер***> **match address** <***список доступа***>	Выделения трафика для шифрования
map <***имя***> <***номер***> **set peer** <**ip**>	Определение партнера
map <***имя***> <***номер***> **set transform-set** <***имя***>	Объединение настроек шифрования
map <***имя***> **interface** <***имя***>	Применение политики на интерфейсе
isakmp key <***значение***> **address** <**ip**>	Создание preshare ключа PSK для партнера с заданным IP
static (***inside***,**outside**) <***тип протокола***> **interface** <***внешний порт***> <***адрес назначения***> <***порт назначения***> **netmask 255.255.255.255**	Проброс портов для доступа PC извне

Порядок выполнения работы

Задание В Самостоятельная работа с указаниями пошагового выполнения.

1) Скоммутируйте сеть, представленную на рисунке.



2) Настройте рабочие станции и брандмауэры таким образом, чтобы создать четыре различных IP-подсети: **a** (192.168.1.0/24), **b**(192.168.2.0/24), **c**(192.168.3.0/24), **d** (192.168.4.0/24).

2.1) На ASA1 подключите интерфейсы e0/0 и e0/1 к Роутеру и PC1, а так же настройте статическую маршрутизацию к подсетям **c** и **d**.

2.2) На ASA2 подключите интерфейсы e0/0 и e0/1 к Роутеру и PC2, а так же настройте статическую маршрутизацию к подсетям **a** и **b**.

2.3) Настройте интерфейсы PC1

2.4) Настройте интерфейсы PC2

2.5 Настройте интерфейсы и статическую маршрутизацию на Роутере

3) Настройте IPSec-туннель, как это показано на рисунке
   3.1) Настройте ASA1
      3.1.1) Настройте ISAKMP (фаза 1):
      3.1.2) Настройте IPSec (фаза 2)
   3.2) Настройте ASA2:
      3.2.1) Настройте ISAKMP (фаза 1)
      3.2.2) Настройте IPSec (фаза 2)
4) Проверьте работоспособность сети, обратившись с машины PC1 на машину PC2

Задание С Самостоятельная работа пошагового выполнения задания **В с ключевыми указаниями преподавателя.**

Контрольные вопросы:

1. Что такое VPN?
2. Какие технологии создания VPN существуют?
3. Что такое IPSec?
4. В чем преимущество IPSec перед другими протоколами?
5. Назовите основные режимы работы IPSec.
6. Почему IPSec в чистом виде не совместим с технологией NAT?
7. Опишите процедуру создания IPSec туннеля между двумя межсетевыми экранами.
8. Как возможно использовать IPSec вместе с NAT?
9. Что такое *lifetime* соединения IPSec?
10. Что такое ISAKMP?

Требования к оформлению лабораторной работы

Отчет студента по проделанной работе оформляется в электронном и печатном виде и должен содержать:
1) титульный лист по принятой форме с название работы, ФИО студента,
2) цель работы, схему сети с обозначением всех сконфигурированных портов и интерфейсов,
3) последовательность выполнения всех действий, а именно:
   - введенные команды,
   - листинги команд с соответствующими комментариями,
   - скриншоты по каждому действию,
4) анализ и выводы по работе,
5) ответы на контрольные вопросы.

Литература, источники

1. James Boney, Cisco IOS in a Nutshell, O`Reilly, 2010
2. David Hucaby, Cisco ASA, PIX, and FWSM firewall handbook, Cisco Press, 2008
3. http://www.cisco.com/go/asa
4. ru.wikipedia.org/wiki
5. www.archlinux.org/
6. www.linuxguide.it/command_line/linux_commands_ru.html