Допустим есть у нас 2 офиса.

В обоих поднят overload nat, люди ходят в интернет.

Возникла потребность обмениваться конфиденциальными данными в зашифрованном виде.

Рассмотрим на примере **CISCO VPN Site-to-Site**

----------------------------------------------------------------------------  
Дано:

**Роутер "Интернет":**  
interface FastEthernet0/0  
 description site1  
 ip address 1.1.1.1 255.255.255.252  
 duplex auto  
 speed auto  
!  
interface FastEthernet0/1  
 description site2  
 ip address 2.2.2.1 255.255.255.252  
 duplex auto  
 speed auto

**Роутер 1:**  
interface FastEthernet0/0  
 description outside  
 ip address 1.1.1.2 255.255.255.252  
 ip nat outside  
 duplex auto  
 speed auto  
!  
interface FastEthernet0/1  
 description inside  
 ip address 192.168.1.1 255.255.255.0  
 ip nat inside  
 duplex auto  
 speed auto  
!  
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload  
ip route 0.0.0.0 0.0.0.0 1.1.1.1   
!  
ip access-list extended FOR-NAT  
 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255  
 permit ip 192.168.1.0 0.0.0.255 any

**Роутер 2:**  
interface FastEthernet0/0  
 description outside  
 ip address 2.2.2.2 255.255.255.252  
 ip nat outside  
 duplex auto  
 speed auto  
!  
interface FastEthernet0/1  
 description inside  
 ip address 192.168.2.1 255.255.255.0  
 ip nat inside  
 duplex auto  
 speed auto  
!  
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload  
ip route 0.0.0.0 0.0.0.0 2.2.2.1   
!  
ip access-list extended FOR-NAT  
 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255  
 permit ip 192.168.2.0 0.0.0.255 any

В access-list"ах добавлена первая строчка, чтоб не натить трафик между сетями филиалов  
Если ее не будет, то впн корректно не отработает

----------------------------------------------------------------------------  
**Первая фаза, настройка ISAKMP:**

В первую очередь при построении **IPSec**туннеля создается мини-тунель для передачи служебных данных  
Для построения используется **ISAKMP**(Internet Security Association and Key Management Protocol)  
Необходимо настроить ряд параметров для его построения

1. алгоритм шифрования  
2. алгоритм аутентификации  
3. ключ  
4. версия алгоритма Диффи-Хелмана (доступны 1,2,5)  
5. время жизни туннеля

Данные параметры должны совпасть на обоих роутерах

**Пример:**

Здесь 1 произвольное число, роутеры ищут совпадающиую политику начиная с 1  
Если у вас несколько политик на роутере, разумно будет указать более стойкие политики перед слабыми  
**crypto isakmp policy 1**

**des**— 56-битное шифрование. Сейчас взламывается за 24 часа  
**3des**— данные шифруются трижды алгоритмом des. Так-же поддается взлому  
**aes**— Наиболее стоек. Возможно указать длину ключа (128, 192, 256 бит)  
encr aes

Хеширование говорит о том, что данные не изменились злоумышленниками  
**md5**Message Digest 5  
**sha**Secure Hash Standard   
**sha**- является более надежным  
hash sha

Аутентификация (возможна по ключу или сертификату):  
**pre-share**  Pre-Shared Key  
**rsa-encr**   Rivest-Shamir-Adleman Encryption  
**rsa-sig**    Rivest-Shamir-Adleman Signature  
authentication pre-share

Время жизни задается в диапазоне:  
lifetime ?  <60-86400>  lifetime in seconds

Версия алгоритма Диффи-Хелмана  
group 2

Настройка ключа(preshared key) аутентификации и пира - роутер 2:  
**cisco - ключ, укажите свой**  
crypto isakmp key cisco address 2.2.2.2

----------------------------------------------------------------------------  
**Вторая фаза, настройка ipsec transformorm set:**

Задаются методы шифрования, аутентификации данных, передаваемых между сетями  
Параметры должны быть идентичны на обоих маршрутизаторах

**Политика для защиты передаваемых данных (transform-set)**  
crypto ipsec transform-set TS ?  
  ah-md5-hmac   AH-HMAC-MD5 transform  
  ah-sha-hmac   AH-HMAC-SHA transform  
  comp-lzs      IP Compression using the LZS compression algorithm  
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)  
  esp-aes       ESP transform using AES cipher  
  esp-des       ESP transform using DES cipher (56 bits)  
  esp-md5-hmac  ESP transform using HMAC-MD5 auth  
  esp-null      ESP transform w/o cipher  
  esp-seal      ESP transform using SEAL cipher (160 bits)  
  esp-sha-hmac  ESP transform using HMAC-SHA auth  
Как и в первой фазе логика у вариантов шифрования и хэша идентична  
В первой фазе шифруется только содержимое пакета, во второй - весь пакет и заголовок 3 уровня  
crypto ipsec transform-set TS esp-aes esp-sha-hmac

**Определяем какой трафик шифровать:**  
ip access-list extended TO\_VPN  
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

**Настройка crypto, привязка её к isakmp policy, внешнему интерфейсу:**  
crypto map CRMAP 1 ipsec-isakmp  
set peer 2.2.2.2  
set transform-set TS  
match address TO\_VPN

**Привязка к интерфейсу:**  
interface FastEthernet0/0  
crypto map CRMAP

----------------------------------------------------------------------------  
**Проверка работы:**  
Пропингуем сети, и посмотрим статистику  
sh crypto isakmp sa

**show crypto isakmp sa** — отображает состояние

**show crypto ipsec sa** — отображает статистику активных IPSec туннелей

**show crypto engine connections active**— отображает общее количество шифрованных/дешированых пакетов

**show crypto map** – выведет cryptomap

**sh crypto session brief**– краткое состояние сессий

**sh crypto session det** – подробное состояние сетей