-----Инструкции по настройне vpn на роутере 2811-----

Vpn(Virtual private network) - Технология, которая позволяет соединить одно или несколько сетей в одну поверх другой сети.

Примеры использования vpn:

-- Директору компании дома потребовался документ, который находится на серверах компании.

Что было бы без vpn:

@Директор звонит в компанию сисадминам@

@Сисадмины ищут документ на сервере@

@Проходит 30 минут@

@Документ отправляется по электронной почте@

Что было бы с vpn:

@Директор подключается к локалке компании@

@Знает, где документ, поэтому моментально его находит@

@Просматривает документ, или отравляет себе на почту и сразу получает его@

-------------------------------------------

Плюсы vpn:

+ Удобство работы

+ Получение доступа в любое время

+ Исключение лишних связей с персоналом

Поэтому vpn в больших компаниях крайне необходим.

Но у vpn также есть и минусы:

- Сложность настройки

- Необходимо поддерживать сервис, чтобы он не "упал"

- Открывается ещё одна возможность доступа к локалке(минус с точки зрения безопасности)

-----Переход к настройке-----

Пример сети находится в репозитории. Файл - vpn.pka.

Итак, для начала надо расставить ip адреса. Будем считать, что этот шаг уже выполнен.

Примечание: В настройке, в конце строки, после знака // будет коментарий. В команде роли не играет

Расставим политики на роутерах(Router0 hostname:R1):

R1>en //Заходим в привелегированный режим

R1#conf t //Кофигурируем роутер

R1(config)#int fa0/0 //Конфигурируем внешний интерфейс роутера

R1(config-if)#ip nat out //Говорим роутеру, что это внешний интерфейс

R1(config-if)#int fa0/1 //Переходим в внутренний интерфейс

R1(config-if)#ip nat ins //Говорим роутеру, что это внутренний интерфейс

R1(config-if)#exit //Выходим из меню нитерфейса

R1(config)#ip access-list standard FOR-NAT //Создаём список разрешений

R1(config-std-nacl)#permit 192.168.1.0 0.0.0.255 //Задаём разрешённый диапазон

R1(config-std-nacl)#exit //Выходим

R1(config)#ip nat inside source list FOR-NAT interface fa0/0 overload //Говорим роутеру, как использовать этот список снаружи.

R1(config)#do wr

После этого желаем то же самое на роутере другого человека(филиала), только поменяя ip диапазон на 192.168.2.0 0.0.0.255

.....

После настройки второго роутера начинаем именно настройку самого vpn

Типовые настройки роутера

R1(config)#crypto isakmp policy 1 //Настройка политик vpn

R1(config-isakmp)#encr 3des //Алгоритм шифрования

R1(config-isakmp)#hash md5 //Алгоритм хэширования

R1(config-isakmp)#auth pre-share //Способ аутентификации

R1(config-isakmp)#group 2 //Группа

R1(config-isakmp)#exit

R1(config)#crypto isakmp key junior address 210.210.2.2 //Настраиваем сам ключ

R1(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac //Параметры для построения ipsec тоннеля

R1(config)#ip access-list extended FOR-VPN //Список трафика, который будет заворачиваться в iipsec тоннель

R1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 // Разрешения (Из левого офиса в правый)

R1(config-ext-nacl)#exit

R1(config)#crypto map CMAP 10 ipsec-isakmp //Создаём крипто карту

R1(config-crypto-map)#set peer 210.210.2.2 //Указываем пир

R1(config-crypto-map)#set transform-set TS //Указываем параметры ipsec тоннеля

R1(config-crypto-map)#match address FOR-VPN //Указываем, какой трафик надо шифровать

R1(config-crypto-map)#exit

R1(config)#int fa0/0 //Входим в интерфейс

R1(config-if)#crypto map CMAP //Делаем привязку крипто-карты

R1(config-if)#do wr //Сохраняемся

То же самое на R2, но с небольшими изменнениями.

Но пинг всё же не идёт. Это из-за нашего настроенного NAT. Мы хотим его заворачивать в VPN тоннель. Надо исправить access-list. Исправляем:

R1(config)#no ip access-list standard FOR-NAT //Удаляем обычный access-list

R1(config)#ip access-list extended FOR-NAT //И создайм расширенный

R1(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 //Ставим запрет на NAT

R1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 any //А остальной трафик пусть NATится.

То же самое на R2.

Поздравляем! Мы настроили VPN! Пинг идёт.

-----Для linux-----

sudo su

apt-get install libreadline-dev libssl-dev libncurses5-dev zlib1g-dev

git clone github.com/SoftEtherVPN/SoftEtherVPN.git

cd SoftEtherVPN\

./configure

make

checkinstall

Сервер поднят

-----Для Windows-----

Ссылка на ресурс - http://proremontpk.ru/systems/windows7/vpn-server-na-windows-7.html

На этом всё. Спасибо за прочтение.