

Курс молодого бойца. Практический курс с использованием Cisco Packet Tracer. Lesson18 - VPN

Как дать доступ к локальным серверам?

1. Static NAT
2. DMZ
3. VPN

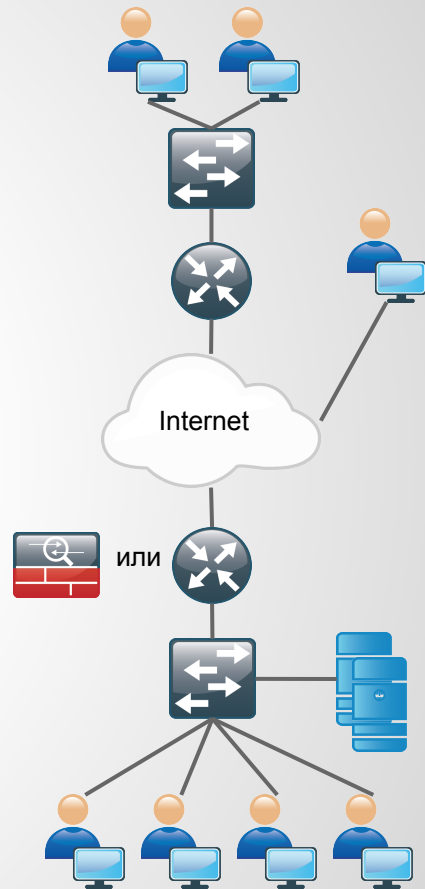
VPN - Virtual Private Network - виртуальная частная сеть

- IPsec Site-to-Site VPN - объединение сетей
- IPsec RA VPN - подключение удаленного пользователя

Построение туннеля в две фазы (IKE)

1. Первая фаза (установка SA и ISAKMP Tunnel)
2. Вторая фаза (IPsec Tunnel)

Более подробно о приведенных технологиях можно почитать [здесь](#) и [здесь](#)



Курс молодого бойца. Практический курс с использованием Cisco Packet Tracer.

Lesson18 - VPN

Типовые настройки роутера:

Настройка первой фазы

```
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
```

Настройка ключа аутентификации и пира

```
crypto isakmp key cisco address 210.210.2.2
```

Вторая фаза

```
crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

Определяем какой трафик шифровать

```
ip access-list extended FOR-VPN
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

Создание криптокарты

```
crypto map CMAP 10 ipsec-isakmp
set peer 210.210.2.2
set transform-set TS
match address FOR-VPN
```

Привязка к интерфейсу

```
interface FastEthernet0/0
crypto map CMAP
```

Типовые настройки МЭ:

Настройка первой фазы

```
crypto ikev1 enable outside
crypto ikev1 policy 1
encr 3des
hash md5
authentication pre-share
group 2
lifetime 43200
```

Настройка ключа аутентификации и пира

```
tunnel-group 210.210.2.2 type ipsec-l2l
tunnel-group 210.210.2.2 ipsec-attributes
ikev1 pre-shared-key cisco
```

Вторая фаза

```
crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac
```

Определяем какой трафик шифровать

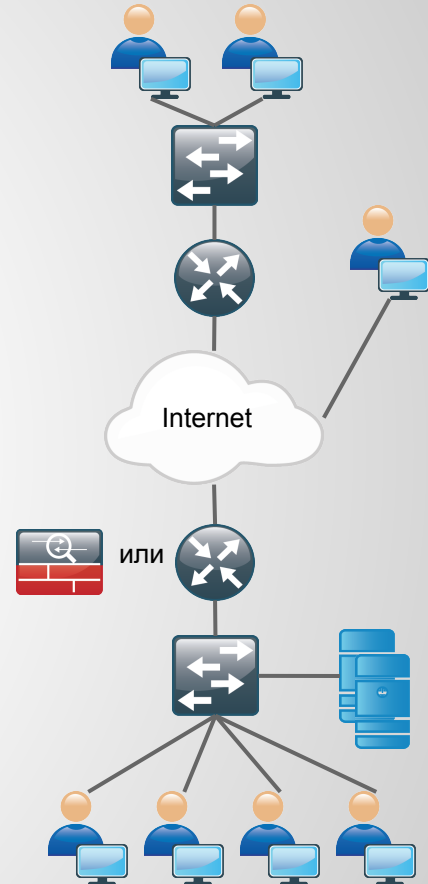
```
access-list FOR-VPN extended permit icmp 192.168.1.0
255.255.255.0 192.168.2.0 255.255.255.0
```

Создание криптокарты

```
crypto map To-Site2 1 match address FOR-VPN
crypto map To-Site2 1 set peer 210.210.2.2
crypto map To-Site2 1 set security-association lifetime seconds
86400
crypto map To-Site2 1 set ikev1 transform-set TS
```

Привязка к интерфейсу

```
crypto map To-Site2 interface outside
```



Курс молодого бойца. Практический курс с использованием Cisco Packet Tracer. Lesson18 - VPN



[Скачать бесплатную версию руководства](#)