1 *Информационные и телекоммуникационные технологии*

Information and telecommunication technologies

УДК 621.39

ОСОБЕННОСТЬ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ FLEXVPN ДЛЯ ПОСТРОЕНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Емельянов Е.В., студент; Лозинская В.Н., асс.
(ГВУЗ «Донецкий национальный технический университет», г. Донецк)

Появление большого количества жилых массивов и организация инфраструктуры вокруг них приводит к сложностям организации каналов связи между ними. Кроме сложности организации каналов связи из-за наличия препятствий, зачастую присутствует также проблема распределенности абонентов на значительных расстояниях друг от друга. В связи с этим при развертывании или расширении телекоммуникационных сетей приходится подбирать методику развертывания канала связи между удаленными филиалами (сегментами сети либо сетями).

Целью данной работы является выработка рекомендаций для развертывания канала связи между удаленными филиалами на примере спортивных комплексов «Металлург» и «Кальмиус Арена».

Чтобы связать несколько географически удаленных сетей, существует огромнейший выбор способов и средств [1]:

1) Непосредственная прокладка физического канала;
2) Аренда канала у провайдера, в случае необходимости стабильного канала до другого города – это самый распространённый и надёжный вариант;
3) Туннель через публичную сеть. Если есть выход в Интернет на обеих точках, зачастую самым дешёвым способом оказывается построить туннель между этими двумя точками. Для этого достаточно всего лишь иметь белые (публичные) статические адреса на всех точках (а иногда достаточно и на одной) и оборудование, на котором это реализовать.

Итак, в первом случае, в зависимости от выбора прокладываемого физического канала могут использоваться следующие технологии:

1. Ethernet по витой паре. В этом случае дальность передачи будет не более 100 метров. Т.е. в общем случае этот вариант подходит при организации канала связи максимум по зданию или между соседними строениями. Скорость передачи по организованному каналу может достигать до 10 Гбит/с
2. Организация беспроводного канала связи (WiFi). Для данной технологии длина канала связи зависит от реализации: можно добиться работоспособности на 40 км при использовании мощных направленных антенн. Однако, в среднем дальность связи до 5 км при прямой видимости. Скорость передачи также зависит от расстояния до приемника и используемого стандарта.
3. Организация проводного канала связи по телефонному проводу (семейство xDSL – два-четыре провода). Скорость передачи в организуемом канале связи зависит от расстояния (теоретический максимум 250 Мбит/с, расстояние до 6 км).
4. Передача по радио-релейным линиям связи. Дальность связи в таком случае составляет до нескольких десятков километров со скоростью до 600 Мб/с. Данное решение

целесообразно для провайдеров регионального масштаба, поскольку требует массу согласований и мероприятий по планированию, строительству, вводу в эксплуатацию.

5. Организация физического канала в оптической среде. Оптимальная скорость передачи 1Гб/с (решения на 10 и 100 Гб/с могут стоить неоправданно дорого). Дальность связи зависит от многих факторов: от нескольких километров до сотен. Необходимы согласования по прокладке кабеля, квалифицированный персонал для строительства и обслуживания. Для небольших компаний есть смысл только для подключения здания не очень далеко от центрального узла.

Если для проектировщика нецелесообразна, по каким-либо причинам самостоятельная организация канала связи между удаленными филиалами, то часто используется второй метод. В таком случае провайдер может предоставить следующие услуги:

1. Услуга «Прямой кабель». Например, провайдер может предоставить одно-два тёмных волокна из своего оптического пучка. Со стороны провайдера трафик никак не контролируется, не ограничивается, он осуществляет только поддержку.

2. Услуга «L2VPN». Трафик проходит через активное оборудование провайдера, поэтому может ограничиваться, например, по скорости. Под этим термином понимается сразу несколько услуг второго уровня:

– VLAN – в том или ином виде между филиалами клиенту предоставлен VLAN;

– псевдокабель (PWE3) – это услуга Точка-Точка, когда со стороны клиента выглядит словно имеется кабель между двумя узлами. Все переданные фреймы без изменений доставляются до удалённой точки. Аналогично обратным образом. Это возможно благодаря тому, что фрейм, приходящий на маршрутизатор провайдера инкапсулируется в PDU вышестоящего уровня, как правило, это пакет MPLS;

– VPLS (Виртуальная частная сеть) – это симуляция локальной сети. В этом случае вся сеть провайдера для клиента будет выглядеть как некий абстрактный гигантский коммутатор. Как и настоящий он будет хранить таблицу MAC-адресов и принимать решение о том, куда отправить пришедший кадр. Реализуется это также инкапсуляцией кадра в MPLS пакет.

3. Услуга «L3VPN». В данном случае сеть провайдера – это как большой маршрутизатор с несколькими интерфейсами. То есть стык будет происходить на сетевом уровне. Клиент настраивает IP-адреса на своих маршрутизаторах с обеих сторон, а маршрутизация в сети оператора – это уже задача провайдера. IP-адреса для точек стыка может определять клиент, либо выдать провайдер – зависит от реализации и от договорённости. Функционировать это может на основе GRE, IPSec или MPLS.

Несмотря на явные достоинства этого метода организации, часто оптимальным решением оказывается именно третий способ, особенно актуальным он является для небольших организаций. Это связано с тем, что он не несет дополнительных затрат на аренду или построение физического канала связи.

Технологии построения VPN можно классифицировать по технологии построения канала [2]:

1. VPN on crypto map
– L2L crypto map
– Easy vpn
2. Dedicated tunnel interfaceStatic VTI
– Static VTI
– Dynamic VTI
– DMVPN
– Flex VPN
3. Tunnel less VPN
– GetVPN
4. L2 VPN
– MacSec

5. SSL VPN
– Clientless
– client

Рассмотрим подробнее технологию FlexVPN. Данная технология представляет собой унификацию всех VPN, и лишена недостатков, так или иначе присущих предыдущим реализациям. В основе лежит технология VTI. Данная технология была создана, чтобы упростить развертывание виртуальных частных сетей, устранить проблемы при внедрении нескольких решений. По сути FlexVPN — это фреймворк, реализующий протокол IKEv2 в IOS маршрутизаторов Cisco, т.е. это связка протоколов IKEv2+IPSec в синтаксисе команд IOS. Преимущество FlexVPN в том, что используется единый синтаксис для настройки различных видов VPN, и кроме того, использование протокола IKEv2 обеспечивает повышенную надежность и улучшенную защиту от Dos-атак.

Итак, используя, технологию FlexVPN необходимо объединить 2 спорткомплекса,

Рисунок 1 – Топология сети

расположенных в Донецке. Топология сети будет иметь вид:

Конфигурация оборудования будет производиться с помощью симулятора GNS3, позволяющего спроектировать комплексную топологию сети и убедиться в ее работоспособности.

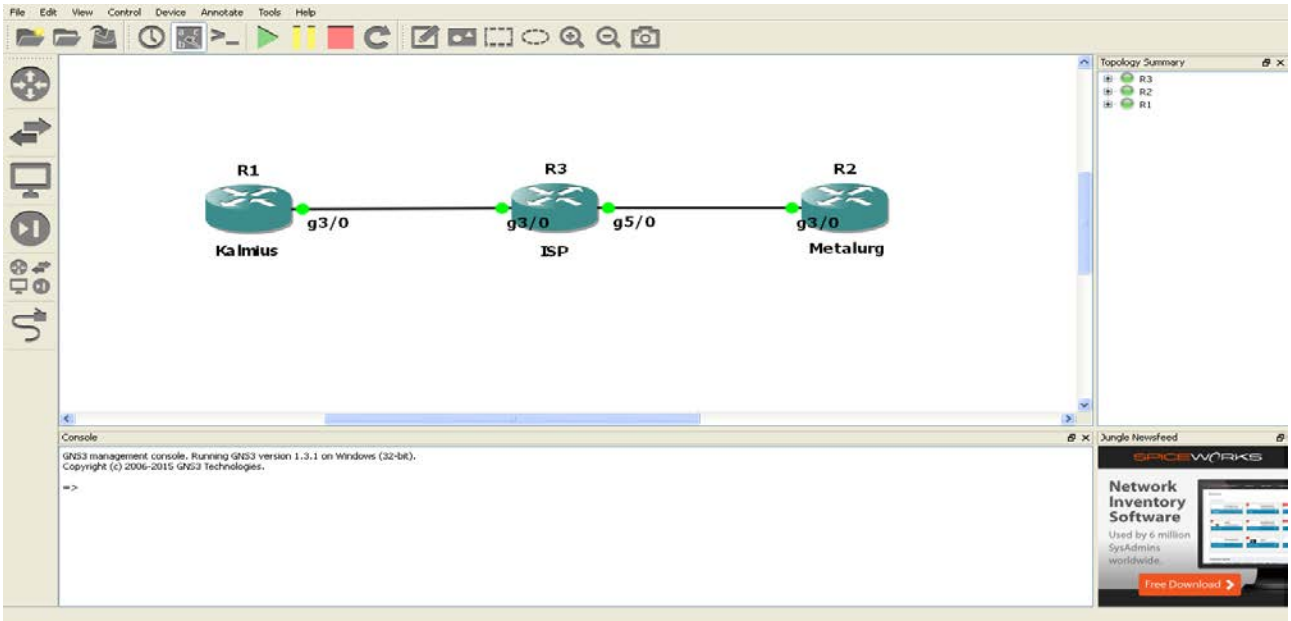

Рисунок 2 – Топология сети в эмуляторе GNS3

Конфигурация оборудования включает в себя следующие шаги [3] (пример настройки на маршрутизаторе стадиона «Металлург»):

1. Настройка IKEv2 Keyring.

```
crypto ikev2 keyring mykeys
 peer Left-Router
  address 172.18.3.52
  pre-shared-key Cisco123
```

2. Изменение default профиля IKEv2, чтобы:

• установить соотвествие IKE ID;

```
crypto ikev2 profile default
 match identity remote address 172.18.3.52 255.255.255.255
```

• установить методы аутентификации для локального и удаленного доступа;

```
authentication local pre-share
authentication remote pre-share
```

• сделать привязку к Keyring, указанному в предыдущем шаге.

```
keyring local mykeys
```

3. Изменение IPsec default профиля, чтобы он соответствовал IKEv2 default профилю.

```
crypto ipsec profile default
 set ikev2-profile default
```

4. Натройка LAN и WAN интерфейсов.

```
interface G3/0
 description WAN
 ip address 172.20.5.43 255.255.255.0
interface G4/0
 description LAN
 ip address 192.168.200.1 255.255.255.0
```

5. Натройка туннеля.

```
interface Tunnel0
 ip address 10.1.12.1 255.255.255.0
 tunnel source G3/0
 tunnel destination 172.18.3.52
 tunnel protection ipsec profile default
```

6. Включение протокола динамической маршрутизации для анонсирования маршрутов на локальных и туннельных интерфейсах.

```
router eigrp 100
  no auto-summary
  network 10.1.12.0 0.0.0.255
  network 192.168.200.0 0.0.0.255
```

7. Маршрут в Интернет.

```
ip route 0.0.0.0 0.0.0.0 172.20.5.1 name route_to_interne
```

Посмотреть состояние активных IPSec сессий, а также количество зашифрованных и расшифрованных пакетов можно с помощью команд show crypto engine connections active и show crypto ipsec sa. Убедиться в том, что трафик передается зашифрованным можно запустив сбор дампов пакетов на одном из интерфейсов.

В результате установлено защищенное, надежное соединение между двумя спорткомплексами, а использование FlexVPN, обеспечивает масштабируемость, гибкость и простоту настройки при добавление новых узлов или изменении топологии.

Перечень ссылок

1. [Электронный ресурс]: http://habrahabr.ru/post/170895/
2. [Электронный ресурс]: http://ciscosales.ru/informaciya/articles/tehnologii_cisco_vpn/
3. [Электронный ресурс]: http://www.cisco.com/c/en/us/support/docs/security/flexvpn/115782-flexvpn-site-to-site-00.html