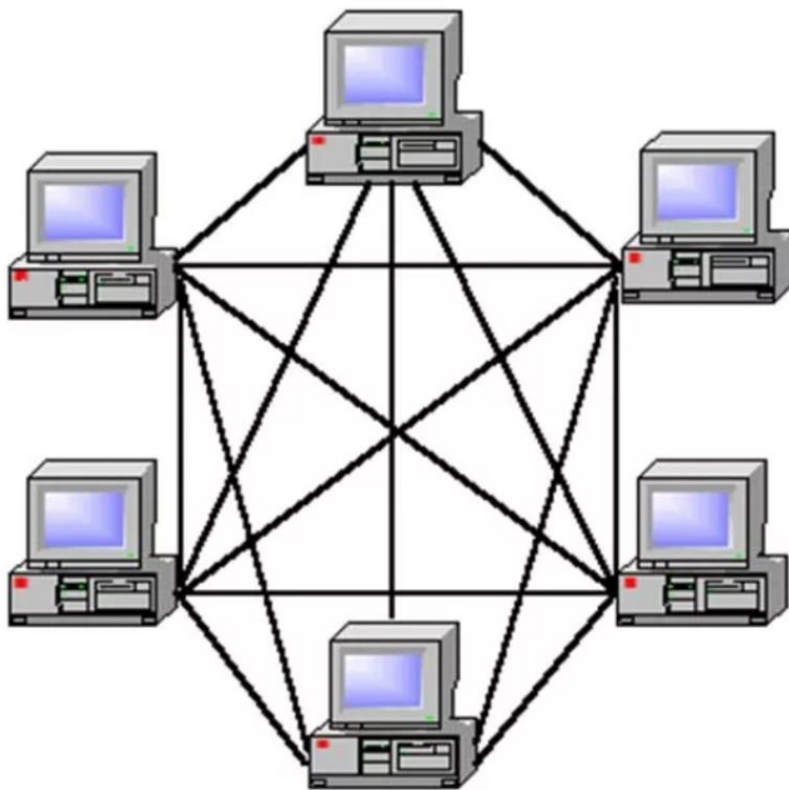


Глава 11. Настройка динамических туннелей между филиалами.

Цель работы:

Настройка виртуальных сервисных маршрутизаторов `vesr` в центральном офисе и двух филиалах на работу с динамическими туннелями по протоколу DMVPN. При расширении деятельности организации возникает необходимость в создании нескольких удалённых подразделений или филиалов. В предыдущих главах были рассмотрены технологии создания связи через интернет между филиалом и центральным офисом по технологии `gre-over-ipsec` с динамической маршрутизацией `ip` пакетов средствами протокола `ospf`. При такой организации прямой связи по зашифрованному туннелю между филиалами не будет. Сделать полноценный граф возможно лишь при создании туннелей всех узлов сети со всеми:



При изменении топологии такого графа нужно будет вручную изменять настройки на каждом из маршрутизаторов в сети, что неизбежно будет приводить к ошибкам. Решает эту задачу протокол DMVPN.
Что такое протокол DMVPN:

Всемирная паутина интернет на этот запрос даёт следующее определение-DMVPN (Dynamic Multipoint Virtual Private Network) — технология, разработанная компанией Cisco для упрощения и масштабирования построения сетей VPN. Она нужна для организации защищённых и динамически изменяемых виртуальных частных сетей (VPN) поверх существующих сетей, таких как интернет или частные WAN-сети

Применение DMVPN:

Связь множества филиалов и удалённых офисов с центральным офисом или между собой.

Доступ к частной сети из публичной. Например, для доступа работников к сети компании, когда они не в офисе, или для предоставления партнёрам или клиентам доступа к частной сети без раскрытия всей инфраструктуры.

Установка резервного соединения в случае, если основное соединение скомпрометировано.

Принцип работы

В классической конфигурации DMVPN используется топология Hub-and-Spoke: один центральный узел (Hub) соединён с несколькими удалёнными узлами (Spoke). Все узлы Spoke могут устанавливать туннели через узел Hub. Особенность DMVPN — возможность динамического установления прямых соединений (туннелей) между узлами Spoke, минуя узел Hub. Это сокращает задержки и уменьшает нагрузку на центральный узел.

Некоторые компоненты DMVPN:

NHRP (Next Hop Resolution Protocol) — протокол для динамического определения следующего хоста (next hop) в сети. Позволяет узлам узнавать реальные IP-адреса других узлов в сети, что позволяет устанавливать прямые туннели между ними.

mGRE (Multipoint GRE) — используется для создания многоточечных туннелей GRE, что позволяет одному туннелю обслуживать несколько удалённых узлов.

IPsec — обеспечивает шифрование и защиту данных, передаваемых через туннели DMVPN.

Dynamic Routing Protocols — DMVPN поддерживает динамические маршрутизирующие протоколы, такие как OSPF, EIGRP, BGP, что позволяет автоматизировать маршрутизацию в сети VPN и обеспечивать её масштабируемость.

Некоторые термины и их значение:

NBMA — **nonbroadcast, multiaccess network**, то есть сеть с множественным доступом без широковещания. К таким сетям относятся, например, ISDN, ATM, X25, Frame Relay (если сконфигурирована в многоточечном режиме). bzoel.iod12vzecz6ihe4p.cloudfront.net

NBMA IP — зарегистрированный IP-адрес от провайдера (underlay IP). bzoel.io

Tunnel IP — не означает частный или публичный, а обозначает адрес внутри туннеля (overlay IP). bzoel.io

NHRP — **Next Hop Resolution Protocol**, протокол разрешения следующего узла, который позволяет динамически устанавливать соединения. Изначально

использовался в сетях NBMA, таких как Frame-Relay и Asynchronous Transfer Mode (ATM). habr.com/d12vzecr6ihe4p.cloudfront.net

Преимущество технологии DMVPN

туннели между каждой точкой в L3VPN-сети создаются динамически.

Настраивается туннель между маршрутизаторами филиала (Spoke) и центрального офиса (Hub). После этого маршрутизаторы филиалов будут создавать туннели между собой по мере необходимости. При этом у маршрутизаторов филиалов могут быть динамические внешние адреса, при их смене не придётся перенастраивать сеть. Работает в связке с протоколом динамической маршрутизации. Фактически при добавлении новых узлов настраивать нужно только их. Везде запускается протокол [NHRP](#) – NBMA Next Hop resolution Protocol. Он позволяет динамически изучать адреса удалённых точек, который желают подключиться к основной. На нём и основана возможность реализации multipoint VPN. Хаб (центральный узел) здесь выступает как сервер (NHS – Next-Hop Server), а все удалённые узлы будут клиентами (NHC – Next-Hop Client).

Недостатки технологии DMVPN

В первую очередь это то, что протокол проприетарный, разработан компанией CISCO и его поддержка еще не широко распространена. В некоторых источниках упоминается , что

К минусам этого решения относятся ограничения по требованиям к качеству поддержания сервиса доставки для туннелей – что не очень благоприятно для медиа трафика. Также подобное решение редко оправдано логически, т.к. в 99% связь используется для доступа к центральному офису компании, в котором находится дата-центр.

Решение:

Проверить физическую доступность по IP адресам маршрутизаторов, участвующих в схеме связи динамических туннелей (см. Глава 8. Настройка GRE-over-IPSEC в маршрутизаторе vESR.)

Подготовить IPsec-туннели с [Policy-based IPsec VPN](#) для работы совместно с динамическими GRE-туннелями. (см. Главу 8. Настройка GRE-over-IPSEC в маршрутизаторе vESR.)

Создать GRE-туннель и перейти в режим его конфигурирования.

Перевести GRE-туннель в режим multipoint.

Установить локальный IP-адрес для установки туннеля.

Задать IP-адрес на туннеле. В качестве альтернативы можно настроить DHCP-клиент для получения IP-адреса от DHCP-сервера.

Задать соответствие «внутреннего» туннельного адреса с «внешним» NBMA-адресом.

Задать «логический (туннельный)» адрес NHRP-сервера.

Определить адресата мультикастного трафика. dynamic или nhs

Включить работу протокола NHRP.

Организовать IP-связность посредством протокола динамической маршрутизации eBGP.

Что такое BGP

BGP (Border Gateway Protocol) — это основной протокол маршрутизации в интернете. Он определяет единые правила обмена информацией между множеством независимых сетей и обеспечивает их надёжное соединение. BGP неразрывно связан с понятием Автономной Системы (AS – Autonomous System), которое уже встречалось в предыдущих главах.

Что такое AS

Автономная система (autonomous system, AS) — система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с Интернетом ([RFC 1930](#)).

По сути, Интернет — не что иное, как совокупность **автономных систем**, которые связаны друг с другом. Внутри **AS** используется **протокол внутреннего шлюза (Interior Gateway Protocol, IGP)**, например **OSPF** или **EIGRP**. А для маршрутизации между различными **AS** используется **протокол внешнего шлюза (Exterior Gateway Protocol, EGP)**. Единственный **EGP**, который используется в настоящее время — это **BGP (Border Gateway Protocol)**.

Подобно IP-адресам, номера **AS** должны быть уникальными в Интернете. Основной причиной этого является то, что **BGP** использует номер **AS** для своего механизма предотвращения появления петель в маршрутизации. Когда **BGP** узнает о маршруте, который имеет его собственный номер **AS** в своем пути, он будет отброшен. Мы будем использовать номера AS начиная с 65000 из диапазон частных AS для внутреннего использования.

Параметры для настройки обмена ключами IKE:

группа Диффи-Хэллмана: 2;
алгоритм шифрования: AES128;
алгоритм аутентификации: SHA1.

Параметры для настройки IPsec:

алгоритм шифрования: AES128;
алгоритм аутентификации: SHA1.

Остальные настройки аналогичны настройкам статичного GRE-туннеля (см. раздел [Настройка GRE-туннелей](#)).

Шаги с 1 по 3 аналогичны тем, что были описаны в предыдущих главах. Схема не меняется, переходим непосредственно к настройке тоннелей gre multipath :

Настройка gre multipath

Поскольку используется уже готовая схема из предыдущих глав, то рассматриваем только конфигурацию непосредственно туннелей.

Состояние туннеля на Hub (это маршрутизатор с именем vesr124-2-1):

vesr124-2-1 login: admin

Password:

```
*          Welcome to vESR          *
*****
```

```
vesr124-2-1# sh run tunnels gre 10
tunnel gre 10
  ttl 18
  security-zone UNTRUST
  local address 10.10.10.2
  remote address 10.10.20.2
  ip address 192.168.100.1/24
  ip ospf instance 1
  ip ospf
  enable
exit
vesr124-2-1#
```

Изменяем размер пакета:

```
vesr124-2-1# config
vesr124-2-1(config)# tunnel gre 10
vesr124-2-1(config-gre)# mtu 1416
vesr124-2-1(config-gre)#
```

Отключаем связь с конкретным внешним туннелем в первом филиале и переводим туннель в многоточечный режим:

```
vesr124-2-1(config-gre)# no remote address
vesr124-2-1(config-gre)# multipoint
```

Для работы протокола BGP необходимо разрешить прохождение пакетов по порту 179 в зону UNTRUST, к которой привязан туннель. Для этого создадим объект-сервис:

```
vesr124-2-1# configure
vesr124-2-1(config)# object-group service to_bgp
vesr124-2-1(config-object-group-service)# port-range 179
vesr124-2-1(config-object-group-service)# exit
vesr124-2-1(config)#
```

Далее нужно создать для пропуска TCP пакетов по этому порту через зону правило:

```
vesr124-2-1(config)# security zone-pair UNTRUST self
vesr124-2-1(config-security-zone-pair)# rule 11
vesr124-2-1(config-security-zone-pair-rule)# action permit
vesr124-2-1(config-security-zone-pair-rule)# match protocol tcp
vesr124-2-1(config-security-zone-pair-rule)# match destination-port object-g
roup to_bgp
```

```
vesr124-2-1(config-security-zone-pair-rule)# enable
vesr124-2-1(config-security-zone-pair-rule)# exit
vesr124-2-1(config-security-zone-pair)# exit
vesr124-2-1(config)#
```

Перейдём к настройке NHRP. Настроим отправку мультикастовых (рассылка пакетов сразу в группу) рассылок в динамически узнаваемые адреса:

```
vesr124-2-1(config)# tunnel gre 10
vesr124-2-1(config-gre)# ip nhrp multicast dynamic
```

Настройка маршрутизации BGP

Поскольку для работы динамических тоннелей необходима передача маршрутов, то делаем настройку протокола динамической маршрутизации eBGP для Hub. Необходимо , согласно документации, для eBGP обязательно явно выбрать метод фильтрации сетей и разрешить анонсирование подсетей. Выбирается метод route map, пишется правило и для каждого правила наружу будет анонсироваться сеть 172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24.

```
vesr124-2-1# config
  фильтрации фильтрацииivesr124-2-1(config)# route-map PERMIT_ALL
vesr124-2-1(config-route-map)# rule 1
vesr124-2-1(config-route-map-rule)# match ip address 172.16.1.0/24
vesr124-2-1(config-route-map-rule)# exit
vesr124-2-1(config-route-map)# exit
vesr124-2-1(config-route-map)# rule 2
vesr124-2-1(config-route-map-rule)# match ip address 172.16.2.0/24
vesr124-2-1(config-route-map-rule)# exit
vesr124-2-1(config-route-map)# exit
vesr124-2-1(config-route-map)# rule 3
vesr124-2-1(config-route-map-rule)# match ip address 172.16.3.0/24
vesr124-2-1(config-route-map-rule)# exit
vesr124-2-1(config-route-map)# exit
vesr124-2-1(config)# exit
```

Далее настраивается сам сервер BGP. Описываем соседей – внешние адреса первого филиала и второго филиала, указываем обмен сетями на основе карты PERMIT_ALL, предписываем анонсировать присоединенные к интерфейсам локальные сети:

```
vesr124-2-1(config)# router bgp 65005
```

Включили рутер BGP с номером автономной частной сети 65005.

```
vesr124-2-1(config-bgp)# neighbor 10.10.20.2
```

Объявили соседа – внешний адрес первого филиала

```
vesr124-2-1(config-bgp-neighbor)# remote-as 65008
```

Номер автономной сети первого филиала 65008

```
vesr124-2-1(config-bgp-neighbor)# address-family ipv4 unicast
```

Разрешили обмен маршрутиями с ним.

```
vesr124-2-1(config-bgp-neighbor-af)# route-map PERMIT_ALL out
```

указали карту фильтра для анонсируемых сетей наружу.

```
vesr124-2-1(config-bgp-neighbor-af)# enable
```

```
vesr124-2-1(config-bgp-neighbor-af)# exit
```

```
vesr124-2-1(config-bgp-neighbor)# exit
```

Так же для второго филиала. У него номер автономной системы будут 65004

```
vesr124-2-1(config-bgp)# neighbor 10.10.30.2
```

```
vesr124-2-1(config-bgp-neighbor)# remote-as 65004
```

```
vesr124-2-1(config-bgp-neighbor)# address-family ipv4 unicast
```

```
vesr124-2-1(config-bgp-neighbor-af)# route-map PERMIT_ALL out
```

```
vesr124-2-1(config-bgp-neighbor-af)# enable
```

```
vesr124-2-1(config-bgp-neighbor-af)# exit
```

```
vesr124-2-1(config-bgp-neighbor)# )# enable
```

```
vesr124-2-1(config-bgp)# address-family ipv4 unicast
```

```
vesr124-2-1(config-bgp-af)# redistribute connected
```

```
vesr124-2-1(config-bgp-af)# exit
```

```
vesr124-2-1(config-bgp)# enable
```

```
vesr124-2-1(config-bgp)# exit
```

```
vesr124-2-1(config)# exit
```

Настройка на HUB IPSEC:

Создание профиля для обмена ключами, представление об алгоритмах и группе DH

```
vesr124-2-1# config
```

```
vesr124-2-1(config)#
```

```
vesr124-2-1(config)# security ike proposal ike_prop1
```

```
vesr124-2-1(config-ike-proposal)# authentication algorithm md5
vesr124-2-1(config-ike-proposal)# encryption algorithm aes128
vesr124-2-1(config-ike-proposal)# dh-group 2
vesr124-2-1(config-ike-proposal)# exit
vesr124-2-1(config)#
```

Описание политики обмена ключами

```
vesr124-2-1(config)# security ike policy ike_pol1
vesr124-2-1(config-ike-policy)# pre-shared-key ascii-text P@ssw0rd
vesr124-2-1(config-ike-policy)# proposal ike_prop1
vesr124-2-1(config-ike-policy)# exit
```

Создание шлюза для обмена ключами и маршрутизация для него-локальный адрес и куда отправлять:

```
vesr124-2-1(config)# security ike gateway ike_gw1
vesr124-2-1(config-ike-gw)# ike-policy ike_pol1
vesr124-2-1(config-ike-gw)# local address 10.10.10.2
vesr124-2-1(config-ike-gw)# local network 10.10.10.2/32 protocol gre
vesr124-2-1(config-ike-gw)# remote address any
vesr124-2-1(config-ike-gw)# remote network any
vesr124-2-1(config-ike-gw)# mode policy-based
vesr124-2-1(config-ike-gw)# exit
vesr124-2-1(config)#exit
vesr124-2-1#commit
vesr124-2-1#confirm
```

Описание IPSEC VPN должно быть таким:

```
security ipsec vpn ipsec1
type transport ike
establish-tunnel route
ike gateway ike_gw1
ike ipsec-policy ipsec_pol1
enable
exit
```

Работаем с протоколом BGP, поэтому убираем привязку (описанную в предыдущих главах) к протоколу OSPF из описания туннеля 10

```
vesr124-2-1(config)# tunnel gre 10
vesr124-2-1(config-gre)# no ip ospf
vesr124-2-1(config-gre)# no ip ospf instance
vesr124-2-1(config-gre)# exit
```



```
vesr124-2-1(config)# exit  
vesr124-2-1#
```

Туннель gre 10 должен выглядеть так:

```
vesr124-2-1# sh running-config tunnels gre 10  
tunnel gre 10  
  ttl 18  
  mtu 1416  
  multipoint  
  security-zone UNTRUST  
  local interface gigabitethernet 1/0/1  
  ip address 192.168.100.1/24  
  ip nhrp multicast dynamic  
  enable  
exit
```

Привязываем к туннелю IPSEC и включаем DMVPN.

```
vesr124-2-1# config  
vesr124-2-1(config)# tunnel gre 10  
vesr124-2-1(config-gre)# ip nhrp ipsec ipsec1 dynamic  
vesr124-2-1(config-gre)# ip nhrp enable  
vesr124-2-1(config-gre)# enable  
vesr124-2-1(config-gre)# exit  
vesr124-2-1(config)# exit
```

Остальные настройки на маршрутизаторе не меняются. Применяем изменения в конфиге на маршрутизаторе vesr124-2-1 и переходим к маршрутизатору первого филиала vesr124-2-2.

Вносим изменения в настройку туннеля tunnel gre 10:

Продолжение смотри на [Boosty](#)