s•terra®

Ваш ориентир в мире безопасности

Динамическое построение VPN туннелей (DMVPN) на базе шлюзов безопасности С-Терра Шлюз

Сергей Слепков
Ведущий инженер
Отдел технического консалтинга

О чем пойдет речь

- Как работает DMVPN, какие технологии используются
- Архитектура и сценарии применения
- Примеры конфигурации на С-Терра Шлюз

Недостатки IPsec

s•terra

Недостатки традиционных дизайнов IPsec

- Огромное количество GRE туннелей при большом количестве удаленных площадок
- Сложная масштабируемость
- Требуется изменение конфигурации центральных шлюзов для подключения новых удаленных площадок
- Сложность конфигурации Spoke-to-Spoke туннелей

Зачем нужен DMVPN

DMVPN (*англ*. Dynamic Multipoint Virtual Private Network — динамическая многоточечная виртуальная частная сеть) — технология для создания виртуальных частных сетей, разработанная Cisco Systems.

Преимущества DMVPN

- Уменьшение конфигурации
- Легкая масштабируемость
- Простота добавления новых площадок
- Высокая отказоустойчивость
- Динамические Spoke-to-Spoke VPN туннели

Используемые технологии

Multipoint GRE tunnel interface (mGRE)

Единый GRE туннель точка-многоточка, позволяющий терминировать на себе несколько GRE-туннелей.

- Поддержка на уровне ядра ОС Linux.

Next Hop Resolution Protocol (NHRP)

Создает карту соответствия (map) физических IP адресов пиров с их туннельными адресами. Позволяет всем пирам, которые находятся в NBMA (Non Broadcast Multiple Access) сети, динамически выучить физические IP адреса друг друга обращаясь к next-hop-серверу (NHS). После этого пиры могут обмениваться информацией друг с другом напрямую.

- Пакет **openNHRP**, реализующий NBMA Next Hop Resolution Protocol (согласно RFC 2332), полностью совместим с Cisco.

IPsec туннелирование и шифрование трафика

С использованием Российских криптоалгоритмов ГОСТ 28147-89, ГОСТ Р 34.11-2012 (и ГОСТ Р 34.12-2015 в версии 4.2).

- Реализация протоколов IKE/IPsec согласно RFC 2401 – 2412.

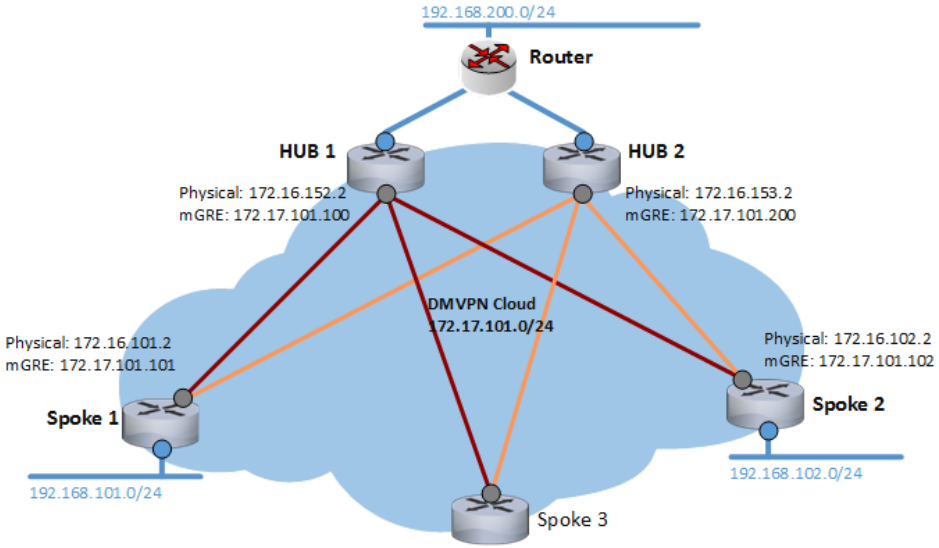
Протоколы динамической маршрутизации

OSPF или BGP для обмена трафиком между сетями за споками и хабами.

- Пакет **quagga,** поддерживающий протоколы динамической маршрутизации RIPv2, OSPF, BGP.

DMVPN Network Designs

Phase 1: Hub-to-Spoke



Только туннели Hub-to-Spoke, туннели Spoke-to-Spoke не устанавливаются. Весь трафик проходит через Hub.

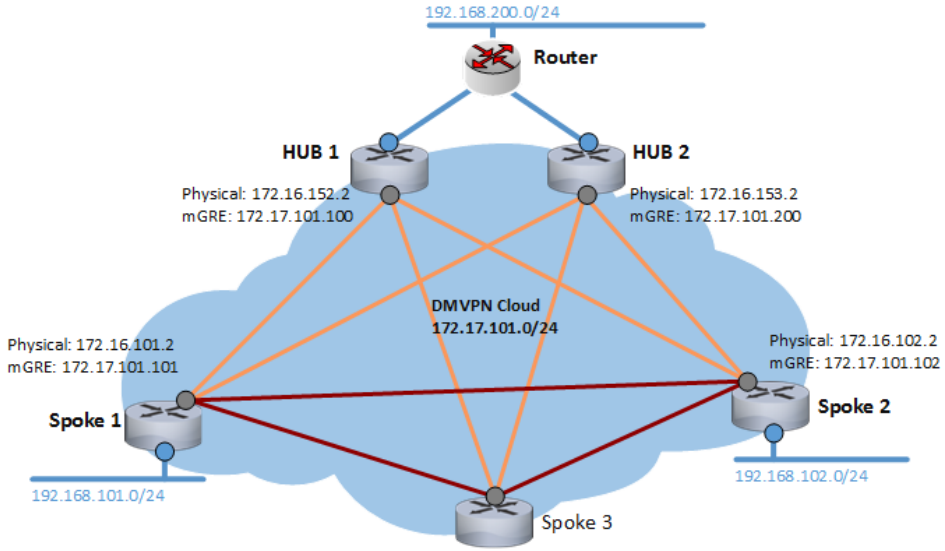
Hub меняет next-hop в протоколах маршрутизации на свой IP адрес.

```
Hub(config-if)# ip ospf network point-to-multipoint
```

Hub-ы могут быть как **active-standby**, так и **active-active** с двумя DMVPN облаками.
В active-active варианте на Spoke-ах будет по 2 маршрута с одинаковой стоимостью (cost). Выбор маршрута на Spoke будет осуществляться с помощью **ECMP** в ОС Linux.

DMVPN Network Designs

Phase 2: Spoke-to-Spoke



Динамические туннели Spoke-to-Spoke. Hub-ы отправляют информацию о маршрутах на все Spoke без изменений.

```
Hub(config-if)# ip ospf network broadcast
```

Как работает DMPVN

s•terra

1. Поднимаются IPsec туннели Hub-to-Spoke. Все Шлюзы используют динамические криптокарты, шифрующие только GRE трафик.

2. Все Spoke регистрируются на Hub (NHRP registration request), сообщая свои физический и туннельный адреса.
На Hub-ах (Next Hop Server, NHS) создается карта всего DMVPN облака.

3. После того, как все DMVPN пиры станут известны, Spoke получают информацию об имеющихся маршрутах по протоколам динамической маршрутизации (OSPF).

4. Если Spoke захочет связаться с другим Spoke (исходя из таблицы маршрутизации), он спрашивает Hub (Next Hop Server, NHS) о его физическом IP и строит с ним IPsec туннель Spoke-to-Spoke.

Конфигурация на С-Терра Шлюз

Конфигурация IPsec

Hub

Параметры DPD (dead peer detection):

```
Hub1(config)# crypto isakmp keepalive 10 2
```

Параметры IKE:

```
Hub1(config)# crypto isakmp identity dn
Hub1(config)# crypto isakmp policy 1
Hub1(config-isakmp)# hash gost
Hub1(config-isakmp)# encryption gost
Hub1(config-isakmp)# authentication gost-sig
Hub1(config-isakmp)# group vko
```

Набор преобразований для IPsec:

```
Hub1(config)# crypto ipsec transform-set TSET esp-gost28147-4m-imit
Hub1(cfg-crypto-trans)# mode tunnel
```

Правило шифрования:

```
Hub1(config)# ip access-list extended LIST
Hub1(config-ext-nacl)# permit gre host 172.16.152.2 any
```

Динамическая криптокарта:

```
Hub1(config)# crypto dynamic-map DMAP 1
Hub1(config-crypto-map)# match address LIST
Hub1(config-crypto-map)# set transform-set TSET
Hub1(config)# crypto map CMAP 1 ipsec-isakmp dynamic DMAP
Hub1(config)# interface GigabitEthernet0/0
Hub1(config)# crypto map CMAP
```

Spoke

Параметры DPD (dead peer detection):

```
Spoke1(config)# crypto isakmp keepalive 10 2
```

Параметры IKE:

```
Spoke1(config)# crypto isakmp identity dn
Spoke1(config)# crypto isakmp policy 1
Spoke1(config-isakmp)# hash gost
Spoke1(config-isakmp)# encryption gost
Spoke1(config-isakmp)# authentication gost-sig
Spoke1(config-isakmp)# group vko
```

Набор преобразований для IPsec:

```
Spoke1(config)# crypto ipsec transform-set TSET esp-gost28147-4m-imit
Spoke1(cfg-crypto-trans)# mode tunnel
```

Правило шифрования:

```
Spoke1(config)# ip access-list extended LIST
Spoke1(config-ext-nacl)# permit gre host 172.16.101.2 any
```

Динамическая криптокарта:

```
Spoke1(config)# crypto dynamic-map DMAP 1
Spoke1(config-crypto-map)# match address LIST
Spoke1(config-crypto-map)# set transform-set TSET
Spoke1(config)# crypto map CMAP 1 ipsec-isakmp dynamic DMAP
Spoke1(config)# interface GigabitEthernet0/0
Spoke1(config)# crypto map CMAP
```

Конфигурация на С-Терра Шлюз

Конфигурация NHRP и mGRE

Hub

Настройка mGRE интерфейса:

```
root@Hub1:~# ip tunnel add mgre0 mode gre key 0xfffffffe ttl 64
root@Hub1:~# ip addr add 172.17.101.100/24 dev mgre0
root@Hub1:~# ip link set mgre0 mtu 1400
root@Hub1:~# ip link set mgre0 multicast on
root@Hub1:~# ip link set mgre0 up
```

Настройка протокола NHRP:

```
/etc/opennhrp/opennhrp.conf

interface mgre0
 map 172.17.101.200/24 172.16.153.2
 multicast dynamic
 holding-time 600
 cisco-authentication secret
 redirect
 non-caching
```

Hub2

Spoke

Настройка mGRE интерфейса:

```
root@Spoke1:~# ip tunnel add mgre0 mode gre key 0xfffffffe ttl 64
root@Spoke1:~# ip addr add 172.17.101.101/24 dev mgre0
root@Spoke1:~# ip link set mgre0 mtu 1400
root@Spoke1:~# ip link set mgre0 multicast on
root@Spoke1:~# ip link set mgre0 up
```

Настройка протокола NHRP:

```
/etc/opennhrp/opennhrp.conf

interface mgre0
 map 172.17.101.100/24 172.16.152.2 register
 map 172.17.101.200/24 172.16.153.2 register
 multicast nhs
 holding-time 600
 cisco-authentication secret
 non-caching
```

Hub1 и Hub2

`multicast dynamic` - multicast трафик будет направляться всем узлам в mGRE сети.

`multicast nhs` - multicast трафик в mGRE сети будет направляться только узлам, выполняющим роль Hub-ов.

Конфигурация на С-Терра Шлюз

Конфигурация OSPF

Hub

```
Hub1(config)# router ospf
Hub1(config-router)# ospf router-id 172.17.101.100
```

Включаем OSPF на интерфейсах mgre0 и eth1:

```
Hub1(config-router)# network 172.17.101.100/24 area 0.0.0.0
Hub1(config-router)# network 192.168.152.2/24 area 0.0.0.1
Hub1(config-router)# area 0.0.0.0 authentication message-digest
Hub1(config-router)# area 0.0.0.1 authentication message-digest
```

Фильтр маршрутов для OSPF области 0.0.0.1:

```
Hub1(config-router)# area 0.0.0.1 export-list LIST
Hub1(config)# access-list LIST permit 192.168.200.0/24
Hub1(config)# access-list LIST deny any
```

Конфигурация mGRE интерфейса:

```
Hub1(config)# interface mgre0
Hub1(config-if)# ip ospf authentication message-digest
Hub1(config-if)# ip ospf message-digest-key 1 md5 SECRET
Hub1(config-if)# ip ospf cost 1
Hub1(config-if)# ip ospf priority 20
```

priority 10 на Hub2

Конфигурация интерфейса eth1:

```
Hub1(config)# interface eth1
Hub1(config-if)# ip ospf authentication message-digest
Hub1(config-if)# ip ospf message-digest-key 1 md5 SECRET
Hub1(config-if)# ip ospf cost 1
Hub1(config-if)# ip ospf priority 20
```

Spoke

```
Spoke1(config)# router ospf
Spoke1(config-router)# ospf router-id 172.17.101.101
```

Включаем OSPF на интерфейсах mgre0 и eth1:

```
Spoke1(config-router)# network 172.17.101.101/24 area 0.0.0.0
Spoke1(config-router)# network 192.168.101.2/24 area 0.0.0.0
Spoke1(config-router)# area 0.0.0.0 authentication message-digest
Spoke1(config-router)# passive-interface eth1
```

Конфигурация mGRE интерфейса:

```
Spoke1(config)# interface mgre0
Spoke1(config-if)# ip ospf authentication message-digest
Spoke1(config-if)# ip ospf message-digest-key 1 md5 SECRET
Spoke1(config-if)# ip ospf priority 0
```

Дополнительные настройки схемы

s•terra

Возможные модификации:

1. Управление маршрутизацией и приоритетами: `ip ospf cost`

```
Hub1(config)# interface mgre0
Hub1(config-if)# ip ospf cost 1
```

2. Режимы работы phase 1 / phase 2 / phase 3

- `Hub1(config-if)# ip ospf network point-to-multipoint` для Phase 1 (топология hub-to-spoke)
- Включение `redirect` в NHRP для Phase 3 (возможность каскадирования Hub-ов)

3. Варианты отказоустойчивости: active-standby или active-active

Возможность использования Dual Hub Dual Cloud топологии с двумя mGRE интерфейсами, позволяющая более гибко управлять маршрутизацией и строить active-active схемы.

Сергей Слепков

Ведущий инженер
Отдел технического консалтинга
Тел.: +7 (499) 940-90-01 (доб. 130)
Email: sslepkov@s-terra.ru

s•terra®