Руководство устранения неполадок отладок фазы 1 DMVPN

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Значительные усовершенствования
Условные обозначения
Соответствующая конфигурация
Обзор топологии
Крипто-
Концентратор
Луч
Отладка
Визуализация потока пакетов
Отладки с пояснением
Подтвердите функциональность и устранение неполадок
show crypto socket
подробность show crypto session
show crypto isakmp sa detail
подробность show crypto ipsec sa
show ip nhrp
show ip Государственная служба здравоохранения
show dmvpn [подробность]
Дополнительные сведения

Введение

Этот документ описывает сообщения отладки, с которыми вы встретились бы на концентраторе и луче развертываний Фазы 1 Динамической многоточечной виртуальной частной сети (DMVPN).

Предварительные условия

Для команд настройки и команд отладки в этом документе, вам будут нужны два маршрутизатора Cisco, которые выполняют Cisco IOS® Release 12.4 (9) T или позже. В целом

основная Фаза 1 DMVPN требует Cisco IOS Release 12.2 (13) T или позже или релиз 12.2 (33) XNC для Маршрутизатора агрегации (ASR), невзирая на то, что функции и отлаживают замеченный в этом документе, не мог бы поддерживаться.

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Generic Routing Encapsulation (GRE)
- Протокол разрешения следующего скачка (NHRP)
- Ассоциация межсетевой безопасности и протокол управления ключами (ISAKMP)
- Протокол IKE
- Протокол IPSEC (Internet Protocol Security) (IPSec)
- По крайней мере один из этих протоколов маршрутизации: Протокол EIGRP, Протокол OSPF, Протокол RIP и Протокол BGP

Используемые компоненты

Сведения в этом документе основываются на Маршрутизаторах ISR Cisco 2911 (ISR), которые выполняют Cisco IOS Release 15.1 (4) M4.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Значительные усовершенствования

Эти версии Cisco IOS представили значительные функции или исправляют для Фазы 1 DMVPN:

- Релиз 12.2 (18) SXF5 - лучше поддерживает для ISAKMP при использовании Инфраструктуры открытых ключей (PKI)
- Релиз 12.2 (33) XNE - ASR, профили IPSEC, Tunnel Protection, переадресация сети IPSec (NAT) прохождение
- Релиз 12.3 (7) T - в Виртуальной маршрутизации и Передающий (iVRF) поддержка
- Релиз 12.3 (11) T - наружная Виртуальная маршрутизация и Передача (FVRF) поддержка
- Выпуск 12.4 (9) T - поддерживает для отнесенных отладок и команд различной DMVPN
- Выпуск 12.4 (15) T - совместно используемый Tunnel Protection
- Выпуск 12.4 (20) T - IPv6 по DMVPN
- Выпуск 15.0 (1) M - туннельный контроль исправности NHRP

Условные обозначения

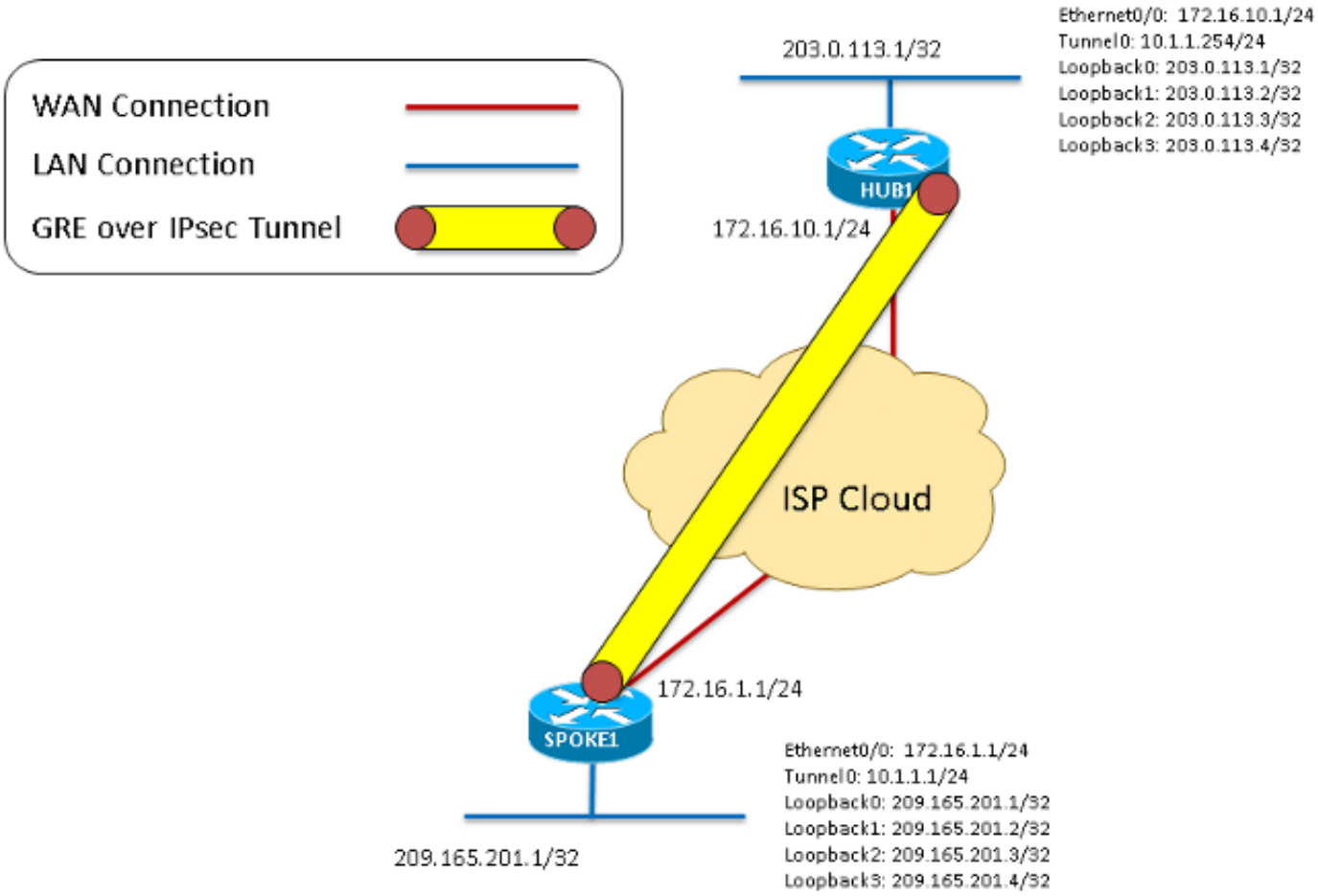
Сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Соответствующая конфигурация

Обзор топологии

Для этой топологии два 2911 ISR, которые выполняют Выпуск 15.1 (4) M4, были настроены для Фазы 1 DMVPN: один как концентратор и один как луч. Ethernet0/0 использовался в качестве "интернет-" интерфейса на каждом маршрутизаторе. Эти четыре интерфейса обратной связи настроены для моделирования локальных сетей, которые живут в концентраторе или оконечном узле. Поскольку это - топология Фазы 1 DMVPN только с одним лучом, луч настроен с Туннелем GRE "точка-точка", а не многоточечным Туннелем GRE. Та же крипто-конфигурация (ISAKMP и IPSec) использовалась на каждом маршрутизаторе, чтобы гарантировать, что они совпали точно.

Схема 1



Крипто-

Это - то же на концентраторе и луче.

```
crypto isakmp policy 1
encr 3des
hash sha
authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
```

```
crypto ipsec transform-set DMVPN-TSET esp-3des esp-sha-hmac
mode transport
crypto ipsec profile DMVPN-IPSEC
set transform-set DMVPN-TSET
```

Концентратор

```
interface Tunnel0
ip address 10.1.1.254 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip tcp adjust-mss 1360
no ip split-horizon eigrp 1
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 1
tunnel protection ipsec profile DMVPN-IPSEC
end

interface Ethernet0/0
ip address 172.16.10.1 255.255.255.0
end

interface Loopback0
ip address 203.0.113.1 255.255.255.255
interface Loopback1
ip address 203.0.113.2 255.255.255.255
interface Loopback2
ip address 203.0.113.3 255.255.255.255
interface Loopback3
ip address 203.0.113.4 255.255.255.255

router eigrp 1
network 10.1.1.0 0.0.0.255
network 203.0.113.1 0.0.0.0
network 203.0.113.2 0.0.0.0
network 203.0.113.3 0.0.0.0
network 203.0.113.4 0.0.0.0
```

Луч

```
interface Tunnel0
ip address 10.1.1.1 255.255.255.0
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map 10.1.1.254 172.16.10.1
ip nhrp network-id 1
ip nhrp nhs 10.1.1.254
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.16.10.1
tunnel key 1
tunnel protection ipsec profile DMVPN-IPSEC
end

interface Ethernet0/0
ip address 172.16.1.1 255.255.255.0
end
```

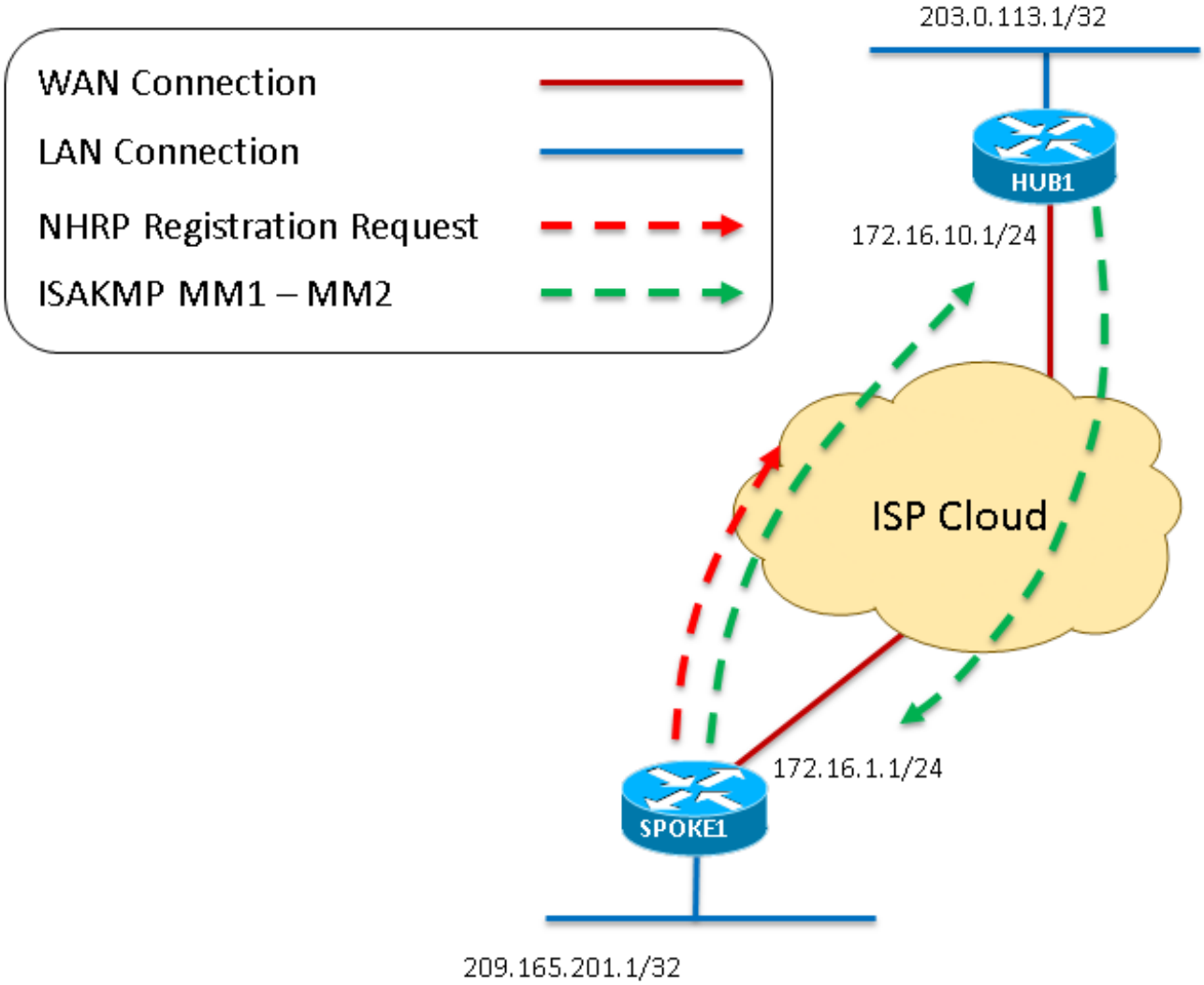
```
interface Loopback0
ip address 209.165.201.1 255.255.255.255
interface Loopback1
ip address 209.165.201.2 255.255.255.255
interface Loopback2
ip address 209.165.201.3 255.255.255.255
interface Loopback3
ip address 209.165.201.4 255.255.255.255

router eigrp 1
network 209.165.201.1 0.0.0.0
network 209.165.201.2 0.0.0.0
network 209.165.201.3 0.0.0.0
network 209.165.201.4 0.0.0.0
network 10.1.1.0 0.0.0.255
```

Отладка

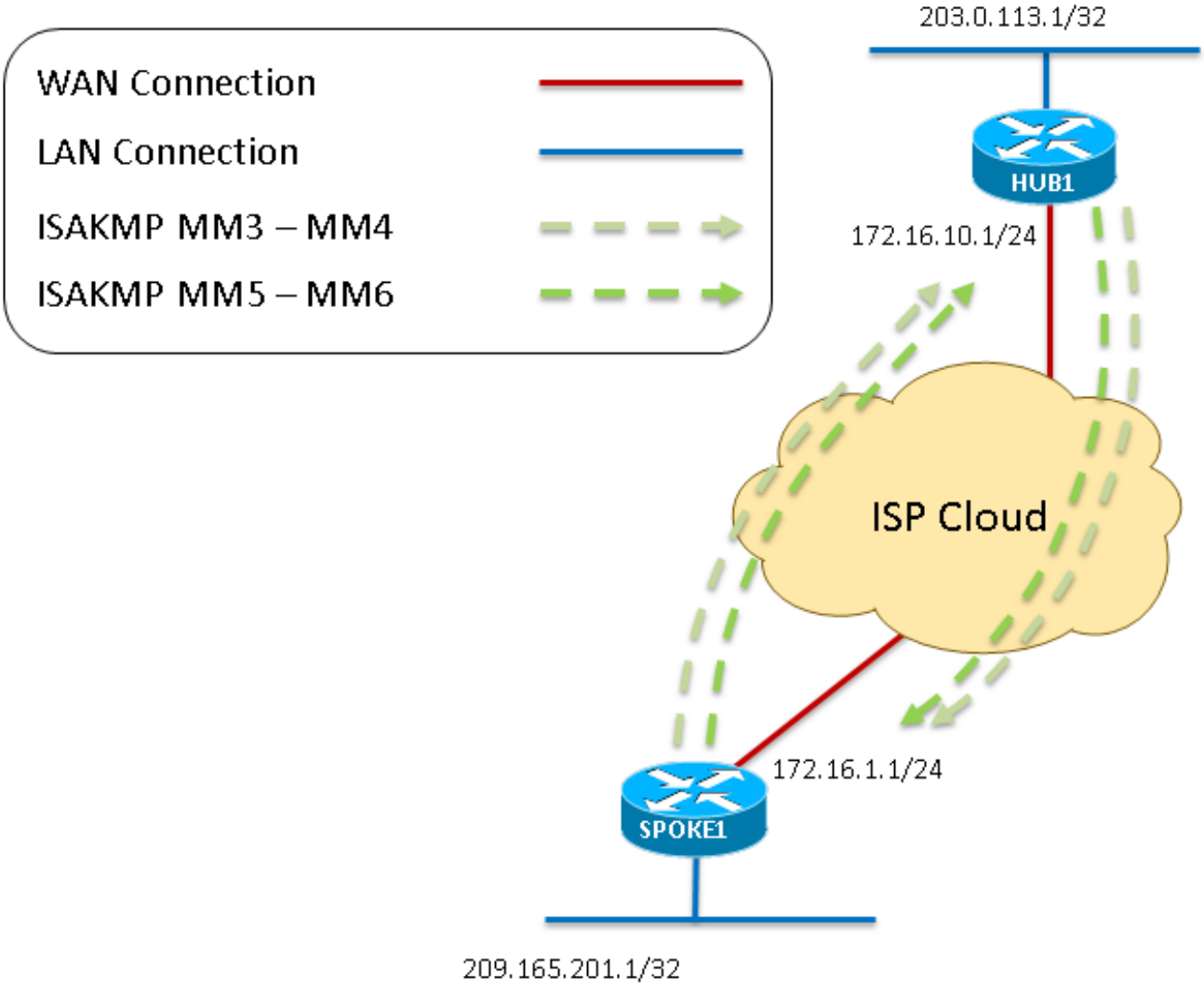
Визуализация потока пакетов

Это - визуализация всего потока пакетов DMVPN, как замечено в этом документе. Более подробные отладки, которые объясняют каждый из шагов, также включены.

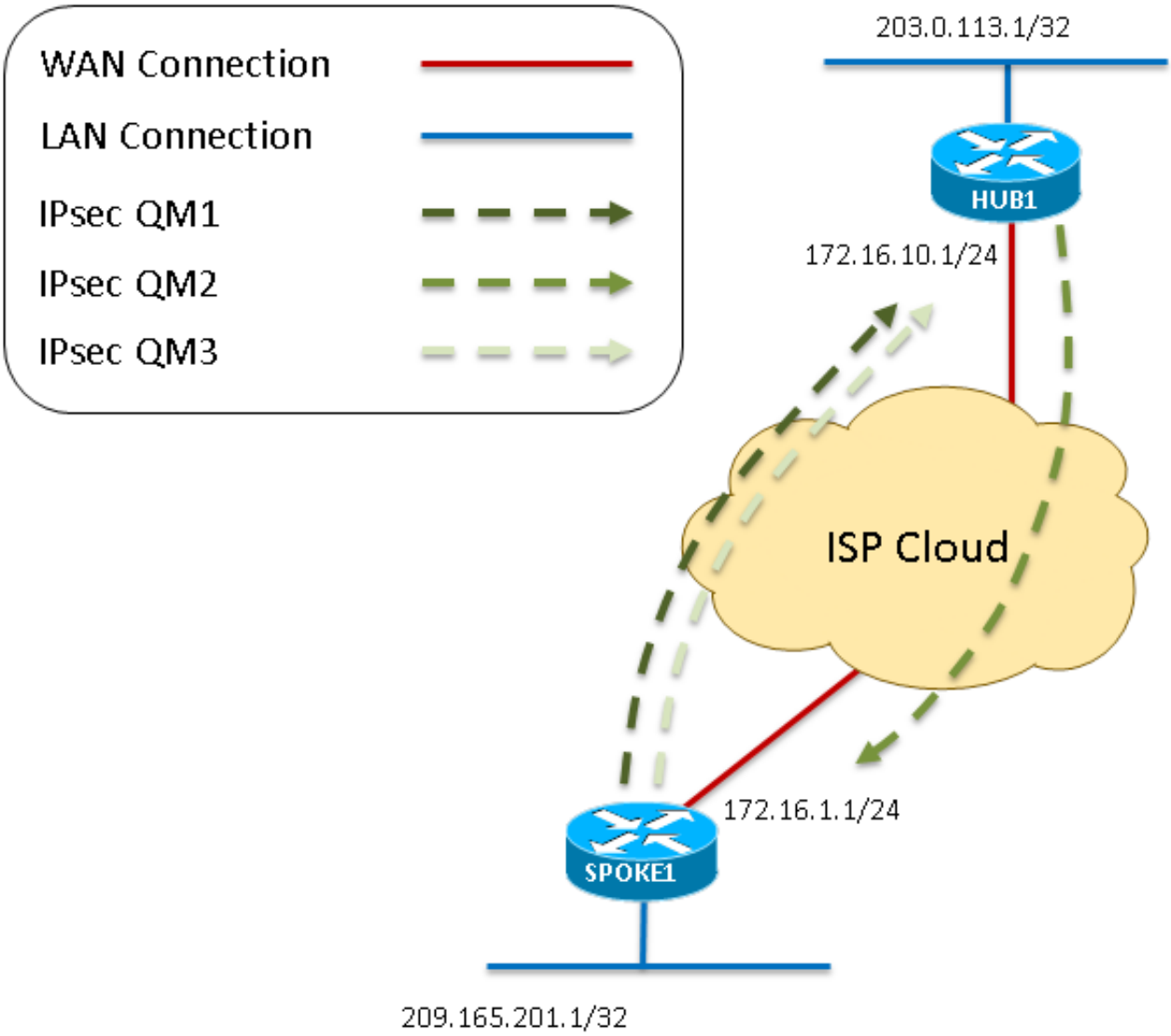
1. Когда Туннель на Луче является "никакым завершением", это генерирует Запрос регистрации NHRP, который запускает процесс DMVPN. Поскольку конфигурация Концентратора является абсолютно динамичной, Луч должен быть оконечной точкой, которая инициирует соединение.
2. Запрос регистрации NHRP тогда инкапсулируется в GRE, который инициирует процесс шифрования для начала.
3. На этом этапе первое сообщение Основного режима ISAKMP - ISAKMP MM1 - передается от Луча до Концентратора на порту UDP500.
4. Концентратор получает и обрабатывает MM1 и отвечает ISAKMP MM2, поскольку это имеет соответствующую Политику ISAKMP.
   Схема 2 - относится к шагам 1 -
   4



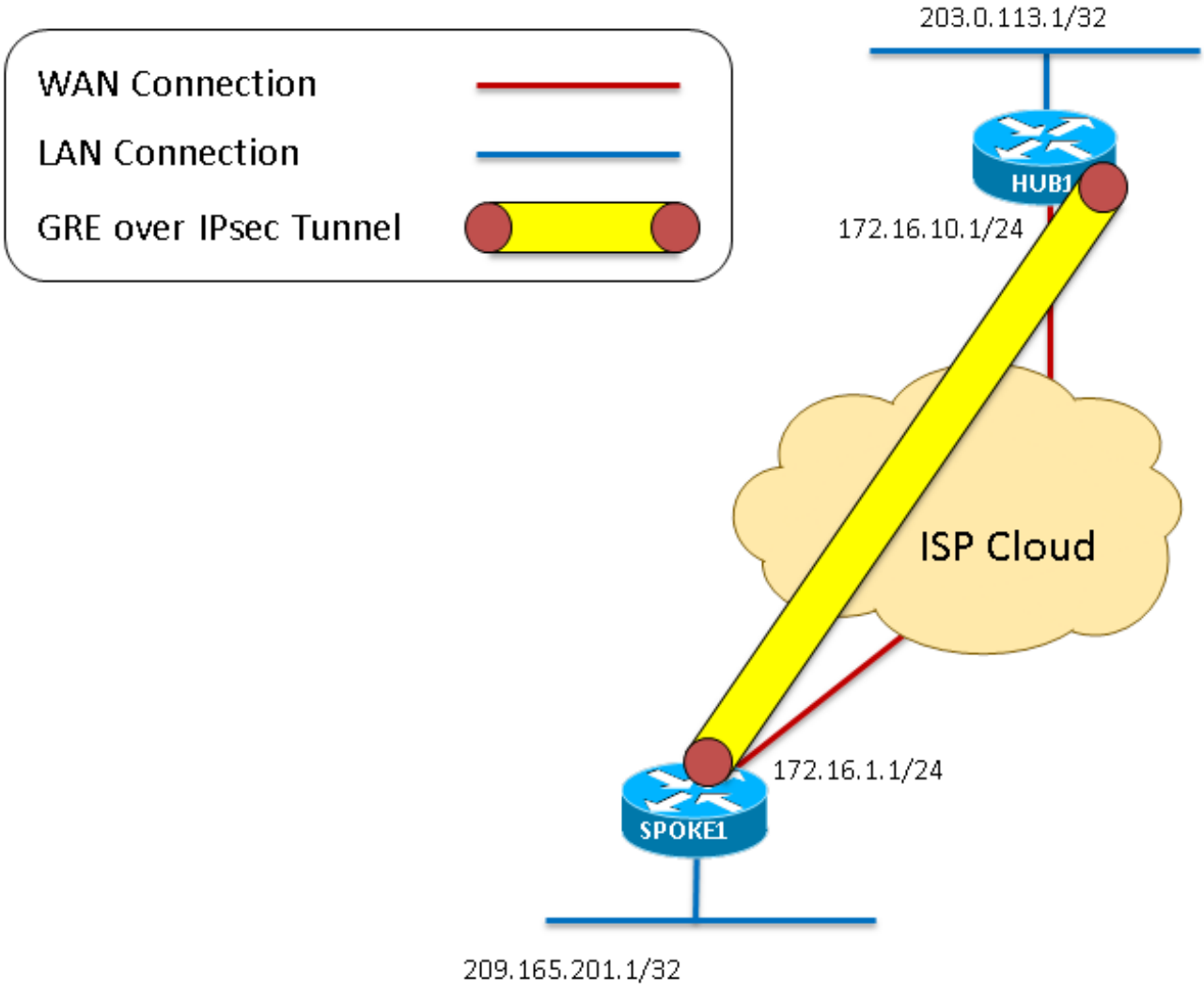
5. Как только Луч получает MM2, он отвечает MM3. Как с MM1, Луч подтверждает, что полученная Политика ISAKMP допустима.
6. Концентратор получает MM3 и отвечает MM4.
7. Если NAT обнаружен в транзитном пути, на этом этапе на согласовании ISAKMP, Луч мог бы ответить на порту UDP4500. Однако, если никакой NAT не обнаружен, Луч продолжает и передает MM5 на UDP500. Наконец, Концентратор отвечает MM6 для завершения обмена Основного режима.
   Схема 3 - относится к шагам 5 -
   7



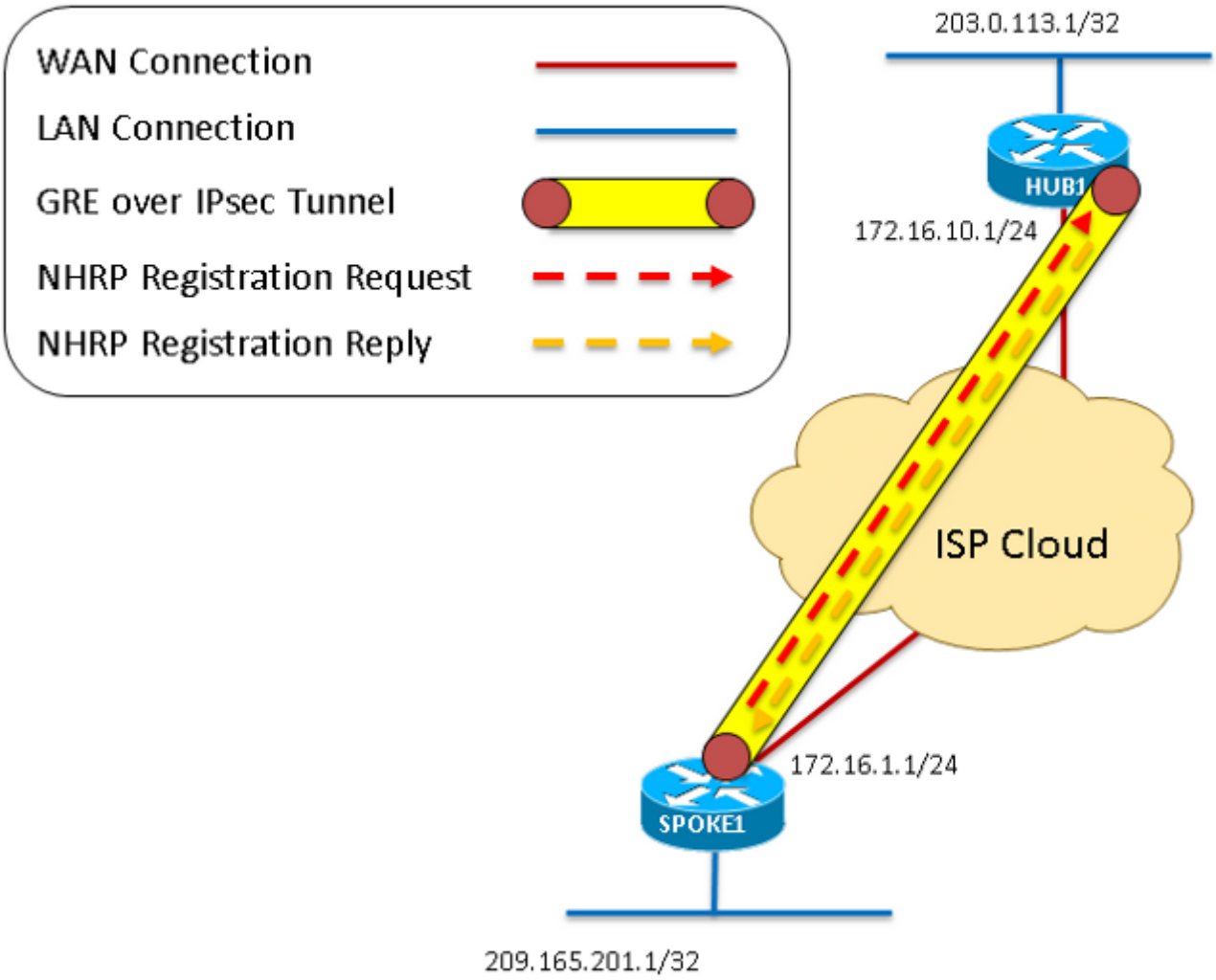
8. Как только Луч получает MM6 от Концентратора, это передает QM1 к Концентратору на UDP500 для начала Быстрого режима.
9. Концентратор получает QM1 и отвечает QM2, поскольку приняты все полученные атрибуты. На этом этапе Концентратор создает SA Фазы 2 для этого сеанса.
10. Как последний шаг согласования Быстрого режима, QM2 получен Лучом. Луч тогда создает свои SA Фазы 2 и передает QM3 в ответ. Это завершает ISAKMP и Согласование IPsec. Существует теперь Сеанс IPSec, который шифрует Трафик GRE между этими двумя узлами.
    Схема 4 - относится к шагам 8 -
    10



11. Теперь, когда сеанс шифрования подключен и в состоянии передать трафик, эти пакеты инкапсулируются в GRE по Туннелю IPSec.
    Схема 5 - относится к шагу
    11



12. Как был замечен в первых шагах, Луч генерирует Запрос регистрации NHRP, который передается через GRE по Туннелю IPSec.
13. Концентратор получает Запросы регистрации NHRP и передает Регистрационный Ответ NHRP, как только он подтверждает, что Луч имеет допустимый Туннель и Нешироковещательный множественный доступ (NBMA) адрес. Луч получает этот Регистрационный Ответ NHRP, который завершает процесс регистрации.
    Схема 6 - относится к шагам 12 -
    13



Когда **debug dmvpn вся вся** команда введен в концентратор и маршрутизаторы на конце луча, эти отладки являются результатом. Эта определенная команда включает этот набор отладок:

```
Spoke1#debug dmvpn all all
DMVPN all level debugging is on
Spoke1#show debug


NHRP:
NHRP protocol debugging is on
NHRP activity debugging is on
NHRP extension processing debugging is on
NHRP cache operations debugging is on
NHRP routing debugging is on
NHRP rate limiting debugging is on
NHRP errors debugging is on
IKEV2:
IKEV2 error debugging is on
IKEV2 terse debugging is on
IKEV2 event debugging is on
IKEV2 packet debugging is on
IKEV2 detail debugging is on



Cryptographic Subsystem:
Crypto ISAKMP debugging is on
Crypto ISAKMP Error debugging is on
Crypto IPSEC debugging is on
```

```
Crypto IPSEC Error debugging is on
Crypto secure socket events debugging is on
Tunnel Protection Debugs:
Generic Tunnel Protection debugging is on
DMVPN:
DMVPN error debugging is on
DMVPN UP/DOWN event debugging is on
DMVPN detail debugging is on
DMVPN packet debugging is on
DMVPN all level debugging is on
```

Отладки с пояснением

Поскольку это - конфигурация, где IPSec внедрен, отладки показывают весь ISAKMP и отладки IPSec. Если не крипто-настроен, проигнорируйте любые отладки, которые запускаются с "IPsec" или "ISAKMP".

СКОНЦЕНТРИРУЙТЕ ОТЛАЖИВАЮТ ПОЯСНЕНИЕ	ОТЛАДКИ В ПОСЛЕДОВАТЕЛЬНОСТИ	ГОВОРИЛ ОТЛАЖИВАЮТ ПОЯСНЕНИЕ
Эти первые несколько сообщений отладки генерируются **командой no shutdown**, ввел в туннельный интерфейс. Сообщения генерируются крипто-, GRE и инициируемыми сервисами NHRP. Ошибка регистрации NHRP замечена на концентраторе, потому что это не имеет Сервера следующего перехода (NHS) настроенным (концентратором является NHS для нашего облака DMVPN). Это ожидается.	IPSEC-IFC MGRE/Tu0: Проверка статуса туннеля. **NHRP: if_up: proto Tunnel0 0** IPSEC-IFC MGRE/Tu0: туннель подъем IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start, уже слушая **%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP идет** **NHRP: Неспособный передать Регистрацию - никакой настроенный NHSes** %LINK-3-UPDOWN: Интерфейсный Tunnel0, измененное состояние к NHRP: if_up: proto Tunnel0 0 NHRP: Неспособный передать Регистрацию - никакой настроенный NHSes IPSEC-IFC MGRE/Tu0: туннель подъем IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start, уже слушая **%LINEPROTO-5-UPDOWN: Протокол линии связи на Интерфейсном Tunnel0, измененном состоянии к**	
	IPSEC-IFC GRE/Tu0: Проверка статуса туннеля. IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): поиск соединения возвратился 0 **IPSEC-IFC GRE/Tu0: crypto_ss_listen_start, уже слушая** **IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): Открытие сокета с IPSEC DMVPN профиля** IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): поиск соединения возвратился 0 IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): Инициирование туннеля сразу. IPSEC-IFC GRE/Tu0: Добавление	Эти первые несколько сообщений отладки генерируются **командой no shutdown**, ввел в туннельный интерфейс. Сообщения генерируются крипто-, GRE и сервисами NHRP, которые инициируются. Кроме того, луч добавляет запись в свой собственный кэш NHRP для ее собственного

	туннельного интерфейса Tunnel0 к совместно используемому списку **NHRP: if_up: proto Tunnel0 0** **NHRP: Tunnel0: Кэш добавляет для цели 10.1.1.254/32 следующий переход 10.1.1.254 172.16.10.1** IPSEC-IFC GRE/Tu0: туннель подъем IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): поиск соединения возвратился 961D220 IPSEC-IFC GRE/Tu0: crypto_ss_listen_start, уже слушая IPSEC-IFC GRE/Tu0: crypto_ss_listen_start, уже слушая IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): Открытие сокета с IPSEC DMVPN профиля IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): поиск соединения возвратился 961D220 IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): Сокет уже открывается. Игнорирование. CRYPTO_SS (ТУННЕЛЬНЫЙ SEC): Приложение начало слушать вставка карты в mapdb AVL отказавший, карта + первоклассная пара уже существует на mapdb **%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP идет** CRYPTO_SS (ТУННЕЛЬНЫЙ SEC): Активная открытая, сокетная информация: локальные 172.16.1.1 172.16.1.1/255.255.255.255/0, удаленные 172.16.10.1 172.16.10.1/255.255.255.255/0, prot 47, ifc Tu0	NBMA и туннельного адреса.
НАЧНИТЕ ISAKMP (ФАЗА I) ПЕРЕГОВОРЫ		
	IPSEC (recalculate_mtu): сброс sadb_root 94EFDC0 метрическая тонна к 1500 **IPSEC (sa_request):** **(ключевое сообщение инженера.)** **ИСХОДЯЩАЯ локальная переменная = 172.16.1.1:500, удаленный = 172.16.10.1:500,** **local_proxy = 172.16.1.1/255.255.255.255/47/0 (type=1),** **remote_proxy = 172.16.10.1/255.255.255.255/47/0 (type=1),** **протокол = ESP, преобразуйте = особенно-3des esp-sha-hmac (Транспорт),** **lifedur = 3600 и 4608000 КБ,** **spi = 0x0 (0), conn_id = 0, размер ключа = 0, отмечает = 0x0** ISAKMP: (0): профиль запроса SA (NULL) ISAKMP: Созданный одноранговая структура для 172.16.10.1, порт однорангового узла 500 ISAKMP: Новый узел создал узел = 0x95F6858 peer_handle = 0x80000004	Первый шаг однажды туннель является "никакым завершением", должен начать крипто-переговоры. Здесь луч создает запрос SA, пытается запустить Агрессивный режим и возвращается к состоянию до сбоя к Основному режиму. Так как Агрессивный режим не настроен ни на одном маршрутизаторе, это ожидается. Луч начинает Основной режим и передает первое сообщение ISAKMP, MM_NO_STATE. Изменения состояния ISAKMP от IKE_READY до

	ISAKMP: Блокируя одноранговую структуру 0x95F6858, refcount 1 для isakmp_initiator ISAKMP: локальный порт 500, удаленный порт 500 ISAKMP: новый узел набора 0 к QM_IDLE ISAKMP: (0): вставьте sa успешно sa = 8A26FB0 **ISAKMP: (0): не Может запустить Агрессивный режим, пробуя Основной режим.** ISAKMP: (0): найденный одноранговый предварительный общий ключ, совпадающий 172.16.10.1 ISAKMP: (0): созданный ID поставщика-rfc3947 NAT-T ISAKMP: (0): созданный поставщик NAT-T 07 ID ISAKMP: (0): созданный поставщик NAT-T 03 ID ISAKMP: (0): созданный поставщик NAT-T 02 ID **ISAKMP: (0): ввод = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM** **ISAKMP: (0): старое Состояние = IKE_READY новое Состояние = IKE_I_MM1** **ISAKMP: (0): начало обмена Основного режима** **ISAKMP: (0): передача пакета к 172.16.10.1 my_port 500 peer_port 500 (I) MM_NO_STATE** ISAKMP: (0): передача пакета IPV4 IKE. IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): поиск соединения возвратился 961D220 IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): хорошее сокетное готовое сообщение	IKE_I_MM1. Сообщения иденификатора поставщика NAT-T используются в обнаружении и обходе NAT. Эти сообщения ожидаются во время согласования ISAKMP независимо от того, внедрен ли NAT. Как сообщения Агрессивного режима, они ожидаются.
После того, как туннель луча является "никакым завершением", концентратор получает IKE NEW SA (Основной режим 1) сообщение на порту 500. Как Респондент, концентратор создает Сопоставление безопасности (SA) ISAKMP. Изменения состояния ISAKMP от IKE_READY до IKE_R_MM1.	**ISAKMP (0): полученный пакет от спорта 172.16.1.1 dport 500 500 Глобальных (N) NEW SA** **ISAKMP: Созданный одноранговая структура для 172.16.1.1, порт однорангового узла 500** ISAKMP: Новый узел создал узел = 0x8CACD00 peer_handle = 0x80000003 ISAKMP: Блокируя одноранговую структуру 0x8CACD00, refcount 1 для crypto_isakmp_process_block ISAKMP: локальный порт 500, удаленный порт 500 **ISAKMP: (0): вставьте sa успешно sa = 6A5BDE8** ISAKMP: (0): ввод = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP: (0): старое Состояние = IKE_READY новое Состояние = IKE_R_MM1**	

Полученный Основной режим IKE 1 сообщение обработан. Концентратор решает, что узел имеет соответствующие атрибуты ISAKMP, и они переполнены в ISAKMP SA, которая была просто создана. Сообщения показывают, что узел использует CBC 3DES для шифрования, хеширования SHA, группа Диффи-Хеллмана (DH) 1, общий ключ для аутентификации и срок действия SA по умолчанию 86400 секунд (0x0 0x1 0x51 0x80 = 0x15180 = 86400 секунд). Состоянием ISAKMP является все еще IKE_R_MM1, так как ответ не имеет быть переданным лучу. Сообщения идентификатора поставщика NAT-T используются в обнаружении и обходе NAT. Эти сообщения ожидаются во время согласования ISAKMP независимо от того, внедрен ли NAT. Подобные сообщения замечены для Dead Peer Detection (DPD).	ISAKMP: (0): обработка информационного наполнения SA. идентификатор сообщения = 0 ISAKMP: (0): обработка информационного наполнения идентификатора поставщика **ISAKMP: (0): идентификатор поставщика кажется Unity/DPD, но главными 69 несоответствиями** **ISAKMP (0): идентификатор поставщика является NAT-T RFC 3947** ISAKMP: (0): обработка информационного наполнения идентификатора поставщика ISAKMP: (0): идентификатор поставщика кажется Unity/DPD, но главными 245 несоответствиями ISAKMP (0): идентификатор поставщика является NAT-T v7 ISAKMP: (0): обработка информационного наполнения идентификатора поставщика ISAKMP: (0): идентификатор поставщика кажется Unity/DPD, но главными 157 несоответствиями ISAKMP: (0): идентификатор поставщика является v3 NAT-T ISAKMP: (0): обработка информационного наполнения идентификатора поставщика ISAKMP: (0): идентификатор поставщика кажется Unity/DPD, но главными 123 несоответствиями ISAKMP: (0): идентификатор поставщика является NAT-T v2 **ISAKMP: (0): найденный одноранговый предварительный общий ключ, совпадающий 172.16.1.1** **ISAKMP: (0): локальный общий ключ найден** ISAKMP: Сканирование профилей для xauth... **ISAKMP: (0): Проверка ISAKMP преобразовывает 1 против приоритета 1 политика** **ISAKMP: CBC 3DES шифрования** **ISAKMP: SHA хэша** **ISAKMP: группа по умолчанию 1** **ISAKMP: подлинный pre-share** **ISAKMP: тип жизни в секундах** **ISAKMP: срок службы (VPI) 0x0 0x1 0x51 0x80** **ISAKMP: (0): atts приемлемы. Следующее информационное наполнение 0** **ISAKMP: (0): Приемлемая atts:actual жизнь: 0** **ISAKMP: (0): Приемлемый atts:life: 0** **ISAKMP: (0): Заполните atts в sa vpi_length:4** **ISAKMP: (0): Заполните atts в sa**	

	life_in_seconds:86400 **ISAKMP: (0): Возврат Фактического срока действия: 86400** **ISAKMP: (0):: запущенный пожизненный таймер: 86400.** ISAKMP: (0): обработка информационного наполнения иденификатора поставщика ISAKMP: (0): иденификатор поставщика кажется Unity/DPD, но главными 69 несоответствиями ISAKMP (0): иденификатор поставщика является NAT-T RFC 3947 ISAKMP: (0): обработка информационного наполнения иденификатора поставщика ISAKMP: (0): иденификатор поставщика кажется Unity/DPD, но главными 245 несоответствиями ISAKMP (0): иденификатор поставщика является NAT-T v7 ISAKMP: (0): обработка информационного наполнения иденификатора поставщика ISAKMP: (0): иденификатор поставщика кажется Unity/DPD, но главными 157 несоответствиями ISAKMP: (0): иденификатор поставщика является v3 NAT-T ISAKMP: (0): обработка информационного наполнения иденификатора поставщика ISAKMP: (0): иденификатор поставщика кажется Unity/DPD, но главными 123 несоответствиями ISAKMP: (0): иденификатор поставщика является NAT-T v2 ISAKMP: (0): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP: (0): старое Состояние = IKE_R_MM1 новое Состояние = IKE_R_MM1	
MM_SA_SETUP (Основной режим 2) передается лучу, который подтверждает, что MM1 был получен и принят как допустимый Пакет ISAKMP. Изменения состояния ISAKMP от IKE_R_MM1 до IKE_R_MM2.	ISAKMP: (0): созданный ID поставщика-rfc3947 NAT-T **ISAKMP: (0): передача пакета к 172.16.1.1 my_port 500 peer_port 500 (R) MM_SA_SETUP** ISAKMP: (0): передача пакета IPV4 IKE. ISAKMP: (0): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP: (0): старое Состояние = IKE_R_MM1 новое Состояние = IKE_R_MM2**	
	ISAKMP (0): полученный пакет от спорта 172.16.10.1 dport 500 500 Глобальных (I) MM_NO_STATE **ISAKMP: (0): ввод = IKE_MESG_FROM_PEER, IKE_MM_EXCH**	В ответ на сообщение MM1, передаваемое концентратору, поступает MM2, какой confims, что был получен MM1.

	ISAKMP: (0): старое Состояние = IKE_I_MM1 новое Состояние = IKE_I_MM2 ISAKMP: (0): обработка информационного наполнения SA. идентификатор сообщения = 0 ISAKMP: (0): обработка информационного наполнения иденификатора поставщика **ISAKMP: (0): иденификатор поставщика кажется Unity/DPD, но главными 69 несоответствиями** ISAKMP (0): иденификатор поставщика является NAT-T RFC 3947 ISAKMP: (0): найденный одноранговый предварительный общий ключ, совпадающий 172.16.10.1 ISAKMP: (0): локальный общий ключ найден ISAKMP: Сканирование профилей для xauth... **ISAKMP: (0): Проверка ISAKMP преобразовывает 1 против приоритета 1 политика** **ISAKMP: CBC 3DES шифрования** **ISAKMP: SHA хэша** **ISAKMP: группа по умолчанию 1** **ISAKMP: подлинный pre-share** **ISAKMP: тип жизни в секундах** **ISAKMP: срок службы (VPI) 0x0 0x1 0x51 0x80** **ISAKMP: (0): atts приемлемы. Следующее информационное наполнение 0** **ISAKMP: (0): Приемлемая atts:actual жизнь: 0** **ISAKMP: (0): Приемлемый atts:life: 0** **ISAKMP: (0): Заполните atts в sa vpi_length:4** **ISAKMP: (0): Заполните atts в sa life_in_seconds:86400** **ISAKMP: (0): Возврат Фактического срока действия: 86400** **ISAKMP: (0):: запущенный пожизненный таймер: 86400.** ISAKMP: (0): обработка информационного наполнения иденификатора поставщика ISAKMP: (0): иденификатор поставщика кажется Unity/DPD, но главными 69 несоответствиями ISAKMP (0): иденификатор поставщика является NAT-T RFC 3947 ISAKMP: (0): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP: (0): старое Состояние = IKE_I_MM2 новое Состояние = IKE_I_MM2	Полученный Основной режим IKE 2 сообщения обработан. Луч понимает, что одноранговый концентратор имеет соответствующие атрибуты ISAKMP, и эти атрибуты заполнены в ISAKMP SA, которая была создана. Этот пакет показывает, что узел использует CBC 3DES для шифрования, хеширования SHA, группа Диффи-Хеллмана (DH) 1, общий ключ для аутентификации и срок действия SA по умолчанию 86400 секунд (0x0 0x1 0x51 0x80 = 0x15180 = 86400 секунд). В дополнение к сообщениям NAT-T существует обмен, чтобы определить, будет ли сеанс использовать DPD. Изменения состояния ISAKMP от IKE_I_MM1 до IKE_I_MM2.
	ISAKMP: (0): передача пакета к 172.16.10.1	MM_SA_SETUP

	my_port 500 peer_port 500 (I) MM_SA_SETUP ISAKMP: (0): передача пакета IPV4 IKE. ISAKMP: (0): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP: (0): старое Состояние = IKE_I_MM2 новое Состояние = IKE_I_MM3**	(Основной режим 3) передается концентратору, который подтверждает, что луч получил MM2 и хотел бы продолжиться. Изменения состояния ISAKMP от IKE_I_MM2 до IKE_I_MM3.
MM_SA_SETUP (Основной режим 3) получен концентратором. Концентратор приходит к заключению, что узел является другим устройством Cisco IOS, и никакой NAT не обнаружен для нас или нашего узла. Изменения состояния ISAKMP от IKE_R_MM2 до IKE_R_MM3.	**ISAKMP (0): полученный пакет от спорта 172.16.1.1 dport 500 500 Global (R) MM_SA_SETUP** ISAKMP: (0): ввод = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP: (0): старое Состояние = IKE_R_MM2 новое Состояние = IKE_R_MM3** ISAKMP: (0): обработка информационного наполнения KE. идентификатор сообщения = 0 ISAKMP: (0): обработка информационного наполнения ПАРАМЕТРА. идентификатор сообщения = 0 **ISAKMP: (0): найденный одноранговый предварительный общий ключ, совпадающий 172.16.1.1** ISAKMP: (1002): обработка информационного наполнения иденификатора поставщика ISAKMP: (1002): иденификатор поставщика является DPD ISAKMP: (1002): обработка информационного наполнения иденификатора поставщика **ISAKMP: (1002): разговор с другой коробкой IOS!** ISAKMP: (1002): обработка информационного наполнения иденификатора поставщика ISAKMP: (1002): иденификатор поставщика кажется Unity/DPD, но главными 225 несоответствиями ISAKMP: (1002): иденификатор поставщика является XAUTH Тип полезных данных ISAKMP:received 20 **ISAKMP (1002): Его хэш никакое соответствие - этот узел вне NAT** Тип полезных данных ISAKMP:received 20 **ISAKMP (1002): Никакой NAT, Найденный для сам или узел** ISAKMP: (1002): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE	

	ISAKMP: (1002): старое Состояние = IKE_R_MM3 новое Состояние = IKE_R_MM3	
MM_KEY_EXCH (Основной режим 4) передается концентратором. Изменения состояния ISAKMP от IKE_R_MM3 до IKE_R_MM4.	**ISAKMP: (1002): передача пакета к 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH** ISAKMP: (1002): передача пакета IPV4 IKE. ISAKMP: (1002): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP: (1002): старое Состояние = IKE_R_MM3 новое Состояние = IKE_R_MM4**	
	ISAKMP (0): полученный пакет от спорта 172.16.10.1 dport 500 500 Глобальных (I) MM_SA_SETUP ISAKMP: (0): ввод = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP: (0): старое Состояние = IKE_I_MM3 новое Состояние = IKE_I_MM4** ISAKMP: (0): обработка информационного наполнения KE. идентификатор сообщения = 0 ISAKMP: (0): обработка информационного наполнения ПАРАМЕТРА. идентификатор сообщения = 0 **ISAKMP: (0): найденный одноранговый предварительный общий ключ, совпадающий 172.16.10.1** ISAKMP: (1002): обработка информационного наполнения иденификатора поставщика ISAKMP: (1002): иденификатор поставщика является Unity ISAKMP: (1002): обработка информационного наполнения иденификатора поставщика ISAKMP: (1002): иденификатор поставщика является DPD ISAKMP: (1002): обработка информационного наполнения иденификатора поставщика **ISAKMP: (1002): разговор с другой коробкой IOS!** Тип полезных данных ISAKMP:received 20 **ISAKMP (1002): Его хэш никакое соответствие - этот узел вне NAT** Тип полезных данных ISAKMP:received 20 **ISAKMP (1002): Никакой NAT, Найденный для сам или узел** ISAKMP: (1002): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP: (1002): старое Состояние =	MM_SA_SETUP (Основной режим 4) получен лучом. Луч приходит к заключению, что узел является другим устройством Cisco IOS, и никакой NAT не обнаружен для нас или нашего узла. Изменения состояния ISAKMP от IKE_I_MM3 до IKE_I_MM4.

	IKE_I_MM4 новое Состояние = IKE_I_MM4	
	ISAKMP: (1002): передайте исходный контакт **ISAKMP: (1002): sA делает аутентификацию предварительного общего ключа использование типа ID_IPV4_ADDR идентификатора** ISAKMP (1002): информационное наполнение ID следующее информационное наполнение: 8 введите : 1 адрес: 172.16.1.1 протокол : 17 порт : 500 длина: 12 ISAKMP: (1002): Общая длина полезных данных: 12 **ISAKMP: (1002): передача пакета к 172.16.10.1 my_port 500 peer_port 500 (I) MM_KEY_EXCH** ISAKMP: (1002): передача пакета IPV4 IKE. ISAKMP: (1002): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP: (1002): старое Состояние = IKE_I_MM4 новое Состояние = IKE_I_MM5**	MM_KEY_EXCH (Основной режим 5) передается лучом. Изменения состояния ISAKMP от IKE_I_MM4 до IKE_I_MM5.
MM_KEY_EXCH (Основной режим 5) получен концентратором. Изменения состояния ISAKMP от IKE_R_MM4 до IKE_R_MM5. Кроме того, "одноранговые соответствия *ни один* профилей" не замечен из-за отсутствия профиля ISAKMP. Поскольку дело обстоит так, ISAKMP не использует профиль.	**ISAKMP (1002): полученный пакет от спорта 172.16.1.1 dport 500 500 Global (R) MM_KEY_EXCH** ISAKMP: (1002): ввод = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP: (1002): старое Состояние = IKE_R_MM4 новое Состояние = IKE_R_MM5** ISAKMP: (1002): обработка информационного наполнения ID. идентификатор сообщения = 0 ISAKMP (1002): информационное наполнение ID следующее информационное наполнение: 8 введите : 1 адрес: 172.16.1.1 протокол : 17 порт : 500 длина: 12 **ISAKMP: (0):: взаимодействуйте с соответствиями *ни один* профилей** ISAKMP: (1002): обработка информационного наполнения ХЭША. идентификатор сообщения = 0 ISAKMP: (1002): обработка УВЕДОМЛЯЕТ протокол 1 INITIAL_CONTACT	

	spi 0, идентификатор сообщения = 0, sa = 0x6A5BDE8 ISAKMP: (1002): статус проверки подлинности sA: аутентифицируемый ISAKMP: (1002): sA аутентифицировался с 172.16.1.1 ISAKMP: (1002): статус проверки подлинности sA: аутентифицируемый ISAKMP: (1002): исходный контакт Процесса, переведите существующий SA фазы 1 и 2 в нерабочее состояние с локальными 172.16.10.1 удаленными 172.16.1.1 удаленными портами 500 **ISAKMP: Попытка вставить узел 172.16.10.1/172.16.1.1/500/, и вставленный успешно 8CACD00.** ISAKMP: (1002): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP: (1002): старое Состояние = IKE_R_MM5 новое Состояние = IKE_R_MM5 IPSEC (key_engine): получил событие очереди с 1 сообщением (сообщением) KMI ISAKMP: (1002): sA делает аутентификацию предварительного общего ключа использование типа ID_IPV4_ADDR идентификатора ISAKMP (1002): информационное наполнение ID следующее информационное наполнение: 8 введите : 1 !--- 172.16.10.1 протокол : 17 порт : 500 длина: 12 ISAKMP: (1002): Общая длина полезных данных: 12	
Заключительный пакет MM_KEY_EXCH (Основной режим 6) передан концентратором. Это завершает согласование Фазы 1, которое показывает, что это устройство готово к Фазе 2 (Быстрый режим IPSec). Изменения состояния ISAKMP от IKE_R_MM5 до	**ISAKMP: (1002): передача пакета к 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH** ISAKMP: (1002): передача пакета IPV4 IKE. ISAKMP: (1002): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP: (1002): старое Состояние = IKE_R_MM5 новое Состояние = IKE_P1_COMPLETE** ISAKMP: (1002): ввод =	

IKE_P1_COMPLETE.	IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE ISAKMP: (1002): старое Состояние = IKE_P1_COMPLETE новое Состояние = IKE_P1_COMPLETE	
	ISAKMP (1002): полученный пакет от спорта 172.16.10.1 dport 500 500 Глобальных (I) MM_KEY_EXCH ISAKMP: (1002): обработка информационного наполнения ID. идентификатор сообщения = 0 ISAKMP (1002): информационное наполнение ID следующее информационное наполнение: 8 введите : 1 !--- 172.16.10.1 протокол : 17 порт : 500 длина: 12 **ISAKMP: (0):: взаимодействуйте с соответствиями *ни один* профилей** ISAKMP: (1002): обработка информационного наполнения ХЭША. идентификатор сообщения = 0 ISAKMP: (1002): статус проверки подлинности sA: аутентифицируемый ISAKMP: (1002): sA аутентифицировался с 172.16.10.1 **ISAKMP: Попытка вставить узел 172.16.1.1/172.16.10.1/500/, и вставленный успешно 95F6858.** ISAKMP: (1002): ввод = IKE_MESG_FROM_PEER, IKE_MM_EXCH **ISAKMP: (1002): старое Состояние = IKE_I_MM5 новое Состояние = IKE_I_MM6** ISAKMP: (1002): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP: (1002): старое Состояние = IKE_I_MM6 новое Состояние = IKE_I_MM6 ISAKMP: (1002): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP: (1002): старое Состояние = IKE_I_MM6 новое Состояние = IKE_P1_COMPLETE**	Заключительный пакет MM_KEY_EXCH (Основной режим 6) получен лучом. Это завершает согласование Фазы 1, которое показывает, что это устройство готово к Фазе 2 (Быстрый режим IPSec). Изменения состояния ISAKMP от IKE_I_MM5 до IKE_I_MM6, и затем сразу к IKE_P1_COMPLETE. Кроме того, "одноранговые соответствия *ни один* профилей" не замечен из-за отсутствия профиля ISAKMP. Поскольку дело обстоит так, ISAKMP не использует профиль.
КОНЕЦ ISAKMP (ФАЗА I) NEGOTATION, ЗАПУСТИТЕ IPSEC (ЭТАП 2) NEGOTATION		
	ISAKMP: (1002): начиная обмен Быстрого режима, MID 3464373979	Быстрый режим (Этап 2, IPSec) обмен запускается

	ISAKMP: (1002): Инициатор QM получает spi **ISAKMP: (1002): передача пакета к 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE** ISAKMP: (1002): передача пакета IPV4 IKE. ISAKMP: (1002): узел 3464373979, ввод = IKE_MESG_INTERNAL, IKE_INIT_QM **ISAKMP: (1002): старое Состояние = IKE_QM_READY новое Состояние = IKE_QM_I_QM1** ISAKMP: (1002): ввод = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE ISAKMP: (1002): старое Состояние = IKE_P1_COMPLETE новое Состояние = IKE_P1_COMPLETE	и лучевая передача первое сообщение QM к концентратору.
Концентратор получает первый пакет Режима Quick Mode (QM), который имеет предложение IPSec. Полученные атрибуты указывают что: набор флага encap к 2 (транспортный режим, флаг 1 был бы туннельным режимом), срок действия SA по умолчанию 3600 секунд и 4608000 килобайтов (hex на 0x465000 дюймов), HMAC-SHA для аутентификации и 3DES для шифрования. Поскольку это тот же набор атрибутов в локальной конфигурации, предложение принято, и оболочка КОНТЕКСТА БЕЗОПАСНОСТИ IPSEC создана. Так как никакие значения индекса параметров безопасности (SPI) еще не привязаны к ним, это - просто оболочка SA, который не может использоваться для передачи трафика все же.	**ISAKMP (1002): полученный пакет от спорта 172.16.1.1 dport 500 500 Global (R) QM_IDLE** **ISAKMP: новый узел набора-830593317 к QM_IDLE** ISAKMP: (1002): обработка информационного наполнения ХЭША. идентификатор сообщения = 3464373979 ISAKMP: (1002): обработка информационного наполнения SA. идентификатор сообщения = 3464373979 **ISAKMP: (1002): Проверка предложения IPSec 1** **ISAKMP: преобразуйте 1, ESP_3DES** **ISAKMP: атрибуты в преобразовании:** **ISAKMP: encap 2 (Транспорт)** **ISAKMP: жизнь SA вводит в секундах** **ISAKMP: срок службы SA (основной) из 3600** **ISAKMP: жизнь SA вводит в килобайтах** **ISAKMP: срок службы SA (VPI) 0x0 0x46 0x50 0x0** **ISAKMP: средство проверки подлинности является HMAC-SHA** **ISAKMP: (1002): atts приемлемы.** IPSEC (validate_proposal_request): часть #1 предложения IPSEC (validate_proposal_request): часть #1 предложения, **(ключевое сообщение инженера.)** **ВХОДЯЩАЯ локальная переменная = 172.16.10.1:0, удаленный = 172.16.1.1:0, local_proxy = 172.16.10.1/255.255.255.255/47/0 (type=1), remote_proxy = 172.16.1.1/255.255.255.255/47/0 (type=1), протокол = ESP, преобразуйте =**	

	NONE (Транспорт), lifedur = 0s и 0kb, spi = 0x0 (0), conn_id = 0, размер ключа = 128, отмечает = 0x0	
Это просто общие сообщения Сервиса IPSec, которые говорят, что это работает должным образом.	IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): поиск соединения возвратился 0 IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start, уже слушая **IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Открытие сокета с IPSEC DMVPN профиля** IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): поиск соединения возвратился 0 IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Инициирование туннеля сразу. IPSEC-IFC MGRE/Tu0: Добавление туннельного интерфейса Tunnel0 к совместно используемому списку IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): tunnel_protection_start_pending_timer 8C93888 IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Хороший слушают запрос	
Псевдоэлемент криптокарты создан для Протокола "IP" 47 (GRE) от 172.16.10.1 (общий адрес концентратора) к 172.16.1.1 (лучевой общий адрес). КОНТЕКСТ БЕЗОПАСНОСТИ IPSEC / SPI создан для обоих входящий и исходящий трафик со значениями из принятого предложения.	вставка карты в mapdb AVL отказавший, карта + первоклассная пара уже существует на mapdb CRYPTO_SS (ТУННЕЛЬНЫЙ SEC): Пассивная открытая, сокетная информация: локальные 172.16.10.1 172.16.10.1/255.255.255.255/0, удаленные 172.16.1.1 172.16.1.1/255.255.255.255/0, prot 47, ifc Tu0 Крипто-mapdb: proxy_match **адрес src : 172.16.10.1** **адрес dst : 172.16.1.1** **протокол : 47** порт src : 0 порт dst : 0 ISAKMP: (1002): обработка информационного наполнения ПАРАМЕТРА. идентификатор сообщения = 3464373979 ISAKMP: (1002): обработка информационного наполнения ID. идентификатор сообщения = 3464373979 ISAKMP: (1002): обработка информационного наполнения ID. идентификатор сообщения = 3464373979 ISAKMP: (1002): Респондент QM получает spi ISAKMP: (1002): узел 3464373979, ввод =	

	IKE_MESG_FROM_PEER, IKE_QM_EXCH **ISAKMP: (1002): старое Состояние = IKE_QM_READY новое Состояние = IKE_QM_SPI_STARVE** **ISAKMP: (1002): создание КОНТЕКСТОВ БЕЗОПАСНОСТИ IPSEC** **входящий SA от 172.16.1.1 до 172.16.10.1 (f/i) 0 / 0** **(проксируйте 172.16.1.1 к 172.16.10.1),** **имеет spi 0xDD2AC2B3 и conn_id 0** **срок действия 3600 секунд** **срок действия 4608000 килобайтов** **исходящий SA от 172.16.10.1 до 172.16.1.1 (f/i) 0/0** **(проксируйте 172.16.10.1 к 172.16.1.1),** **имеет spi 0x82C3E0C4 и conn_id 0** **срок действия 3600 секунд** **срок действия 4608000 килобайтов**	
Второе сообщение QM передано концентратором. Сообщение, генерируемое Сервисом IPSec, который подтверждает, что tunnel protection подключен на Tunnel0. Другое сообщение создания SA замечено, который имеет целевой IPs, SPI, атрибуты набора преобразований и срок действия в килобайтах и секунды, оставаясь.	**ISAKMP: (1002): передача пакета к 172.16.1.1 my_port 500 peer_port 500 (R) QM_IDLE** ISAKMP: (1002): передача пакета IPV4 IKE. ISAKMP: (1002): узел 3464373979, ввод = IKE_MESG_INTERNAL, IKE_GOT_SPI **ISAKMP: (1002): старое Состояние = IKE_QM_SPI_STARVE новое Состояние = IKE_QM_R_QM2** CRYPTO_SS (ТУННЕЛЬНЫЙ SEC): Завершенная привязка приложения для снабжения сокетом IPSEC (key_engine): получил событие очереди с 1 сообщением (сообщением) KMI Крипто-mapdb: proxy_match адрес src : 172.16.10.1 адрес dst : 172.16.1.1 протокол : 47 порт src : 0 порт dst : 0 IPSEC (crypto_ipsec_sa_find_ident_head): повторное подключение с теми же прокси и узлом 172.16.1.1 IPSEC (policy_db_add_ident): src 172.16.10.1, dest 172.16.1.1, dest_port 0 **IPSEC (create_sa): созданный sa,** (sa) sa_dest = 172.16.10.1, sa_proto = 50, sa_spi = 0xDD2AC2B3 (3710567091), sa_trans = особенно-3des esp-sha-hmac, sa_conn_id = 3 sa_lifetime (k/sec) = (4536779/3600) **IPSEC (create_sa): созданный sa,** (sa) sa_dest = 172.16.1.1, sa_proto = 50, sa_spi = 0x82C3E0C4 (2193875140),	

	sa_trans = особенно-3des esp-sha-hmac, sa_conn_id = 4 sa_lifetime (k/sec) = (4536779/3600) IPSEC (crypto_ipsec_update_ident_tunnel_decap_oce): обновление идентификатора Tunnel0 8B6A0E8 с tun_decap_oce 6A648F0 IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): поиск соединения возвратился 8C93888 IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): хорошее сокетное готовое сообщение IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): поиск соединения возвратился 8C93888 **IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): tunnel_protection_socket_up** IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Сигнальный NHRP IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Получил mtu сообщения MTU 1458 IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): поиск соединения возвратился 8C93888	
	ISAKMP (1002): полученный пакет от спорта 172.16.10.1 dport 500 500 Глобальных (I) QM_IDLE ISAKMP: (1002): обработка информационного наполнения ХЭША. идентификатор сообщения = 3464373979 ISAKMP: (1002): обработка информационного наполнения SA. идентификатор сообщения = 3464373979 **ISAKMP: (1002): Проверка предложения IPSec 1** **ISAKMP: преобразуйте 1, ESP_3DES** **ISAKMP: атрибуты в преобразовании:** **ISAKMP: encap 2 (Транспорт)** **ISAKMP: жизнь SA вводит в секундах** **ISAKMP: срок службы SA (основной) из 3600** **ISAKMP: жизнь SA вводит в килобайтах** **ISAKMP: срок службы SA (VPI) 0x0 0x46 0x50 0x0** **ISAKMP: средство проверки подлинности является HMAC-SHA** **ISAKMP: (1002): atts приемлемы.** IPSEC (validate_proposal_request): часть #1 предложения IPSEC (validate_proposal_request): часть #1	Луч получает второй пакет QM, который имеет предложение IPSec. Это подтверждает, что QM1 был получен концентратором. Полученные атрибуты указывают что: набор флага encap к 2 (транспортный режим, флаг 1 был бы туннельным режимом), срок действия SA по умолчанию 3600 секунд и 4608000 килобайтов (hex на 0x465000 дюймов), HMAC-SHA для аутентификации и DES для шифрования. Поскольку это тот же набор атрибутов в локальной конфигурации, предложение принято, и оболочка КОНТЕКСТА БЕЗОПАСНОСТИ IPSEC создана. Так как никакие

	предложения, **(ключевое сообщение инженера.)** **ВХОДЯЩАЯ локальная переменная = 172.16.1.1:0, удаленный = 172.16.10.1:0,** **local_proxy = 172.16.1.1/255.255.255.255/47/0 (type=1),** **remote_proxy = 172.16.10.1/255.255.255.255/47/0 (type=1),** **протокол = ESP, преобразуйте = NONE (Транспорт),** **lifedur = 0s и 0kb,** **spi = 0x0 (0), conn_id = 0, размер ключа = 128, отмечает = 0x0** **Крипто-mapdb: proxy_match** **адрес src : 172.16.1.1** **адрес dst : 172.16.10.1** **протокол : 47** **порт src : 0** **порт dst : 0**	значения индекса параметров безопасности (SPI) еще не привязаны к ним, это - просто оболочка SA, который не может использоваться для передачи трафика все же. Псевдоэлемент криптокарты создан для Протокола "IP" 47 (GRE) от 172.16.10.1 (общий адрес концентратора) к 172.16.1.1 (лучевой общий адрес).
	ISAKMP: (1002): обработка информационного наполнения ПАРАМЕТРА. идентификатор сообщения = 3464373979 ISAKMP: (1002): обработка информационного наполнения ID. идентификатор сообщения = 3464373979 ISAKMP: (1002): обработка информационного наполнения ID. идентификатор сообщения = 3464373979 **ISAKMP: (1002): создание КОНТЕКСТОВ БЕЗОПАСНОСТИ IPSEC** **входящий SA от 172.16.10.1 до 172.16.1.1 (f/i) 0 / 0** **(проксируйте 172.16.10.1 к 172.16.1.1),** **имеет spi 0x82C3E0C4 и conn_id 0** **срок действия 3600 секунд** **срок действия 4608000 килобайтов** **исходящий SA от 172.16.1.1 до 172.16.10.1 (f/i) 0/0** **(проксируйте 172.16.1.1 к 172.16.10.1),** **имеет spi 0xDD2AC2B3 и conn_id 0** **срок действия 3600 секунд** **срок действия 4608000 килобайтов**	КОНТЕКСТ БЕЗОПАСНОСТИ IPSEC / SPI создан для обоих входящий и исходящий трафик со значениями из принятого предложения.
	ISAKMP: (1002): передача пакета к 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE ISAKMP: (1002): передача пакета IPV4 IKE. ISAKMP: (1002): удаление узла-830593317 ошибочной ЛЖИ не обосновывает "Ошибки" ISAKMP: (1002): узел 3464373979, ввод = IKE_MESG_FROM_PEER, IKE_QM_EXCH **ISAKMP: (1002): старое Состояние = IKE_QM_I_QM1 новое Состояние = IKE_QM_PHASE2_COMPLETE**	Луч передает третье и заключительное сообщение QM к концентратору, который завершает обмен QM. В отличие от ISAKMP, где каждый узел проходит каждое состояние (MM1 через MM6/P1_COMPLETE), IPSec является немного

	IPSEC (key_engine): получил событие очереди с 1 сообщением (сообщением) KMI Крипто-mapdb: proxy_match адрес src : 172.16.1.1 адрес dst : 172.16.10.1 протокол : 47 порт src : 0 порт dst : 0 IPSEC (crypto_ipsec_sa_find_ident_head): повторное подключение с теми же прокси и узлом 172.16.10.1 IPSEC (policy_db_add_ident): src 172.16.1.1, dest 172.16.10.1, dest_port 0 **IPSEC (create_sa): созданный sa,** (sa) sa_dest = 172.16.1.1, sa_proto = 50, sa_spi = 0x82C3E0C4 (2193875140), sa_trans = особенно-3des esp-sha-hmac, sa_conn_id = 3 sa_lifetime (k/sec) = (4499172/3600) **IPSEC (create_sa): созданный sa,** (sa) sa_dest = 172.16.10.1, sa_proto = 50, sa_spi = 0xDD2AC2B3 (3710567091), sa_trans = особенно-3des esp-sha-hmac, sa_conn_id = 4 sa_lifetime (k/sec) = (4499172/3600) **IPSEC (update_current_outbound_sa): доберитесь включают узлу SA 172.16.10.1 текущих исходящих sa к SPI DD2AC2B3** **IPSEC (update_current_outbound_sa): обновленный узел 172.16.10.1 текущих исходящих sa к SPI DD2AC2B3** IPSEC (crypto_ipsec_update_ident_tunnel_decap_oce): обновление идентификатора Tunnel0 94F2740 с tun_decap_oce 794ED30 IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): поиск соединения возвратился 961D220 IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): tunnel_protection_socket_up IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): Сигнальный NHRP NHRP: NHS 10.1.1.254 VRF Tunnel0 0 Кластеров 0 Приоритетов 0 Перешедших к 'E' от '' IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): поиск соединения возвратился 961D220 NHRP: Попытка передать пакет через DEST 10.1.1.254	другим, поскольку существует только три сообщения, а не шесть. Инициатор (наш луч в этом случае, как показано "мной" в сообщении **IKE_QM_I_QM1**) идет от QM_READY, затем к QM_I_QM1 непосредственно к QM_PHASE2_COMPLETE Респондент (концентратор) идет QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE Другое сообщение создания SA замечено, который имеет целевой IPs, SPI, атрибуты набора преобразований и срок действия в килобайтах и секунды, оставаясь.
Эти заключительные сообщения QM подтверждают, что	**ISAKMP (1002): полученный пакет от спорта 172.16.1.1 dport 500 500 Global (R) QM_IDLE**	

Быстрый режим завершен, и IPSec подключен с обеих сторон туннеля. В отличие от ISAKMP, где каждый узел проходит каждое состояние (MM1 через MM6/P1_COMPLETE), IPSec является немного другим, поскольку существует только три сообщения, а не шесть. Респондент (наш концентратор в этом случае, как показано "R" в сообщении **IKE_QM_R_QM1**) идет QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE. Инициатор (луч) идет от QM_READY, затем к QM_I_QM1 непосредственно к QM_PHASE2_COMPLETE.	ISAKMP: (1002): удаление узла-830593317 ошибочных сделанных QM "причины ЛЖИ (ждет)" ISAKMP: (1002): узел 3464373979, ввод = IKE_MESG_FROM_PEER, IKE_QM_EXCH **ISAKMP: (1002): старое Состояние = IKE_QM_R_QM2 новое Состояние = IKE_QM_PHASE2_COMPLETE** IPSEC (key_engine): получил событие очереди с 1 сообщением (сообщением) KMI IPSEC (key_engine_enable_outbound): rec'd включают, уведомляют от ISAKMP **IPSEC (key_engine_enable_outbound): включите SA с spi 2193875140/50** **IPSEC (update_current_outbound_sa): доберитесь включают узлу SA 172.16.1.1 текущих исходящих sa к SPI 82C3E0C4** **IPSEC (update_current_outbound_sa): обновленный узел 172.16.1.1 текущих исходящих sa к SPI 82C3E0C4**	
	NHRP: Передайте Запрос регистрации через VRF Tunnel0 0, размер пакета: 108 **src: 10.1.1.1, dst: 10.1.1.254** (F) afn: IPv4 (1), введите: IP (800), переход: 255, версия: 1 shtl: 4 (NSAP), sstl: 0 (NSAP) pktsz: 108 экс-бар: 52 (M) флаги: "уникальный nat", reqid: 65540 **NBMA src: 172.16.1.1** **протокол src: 10.1.1.1, протокол dst: 10.1.1.254** (C-1) код: никакая ошибка (0) префикс: 32, mtu: 17912, hd_time: 7200 addr_len: 0 (NSAP), subaddr_len: 0 (NSAP), proto_len: 0, приставка: 0 Расширение адреса респондента (3): Вперед передайте транзитом, NHS делают запись расширения (4): Обратный транзит NHS делает запись расширения (5): **Опознавательное расширение (7):** **введите : Открытый текст (1), data:NHRPAUTH** Расширение адреса NAT (9): (C-1) код: никакая ошибка (0) префикс: 32, mtu: 17912, hd_time: 0	Это - запросы регистрации NHRP, передаваемые концентратору в попытке зарегистрироваться к NHS (концентратор). Это обычно для наблюдения множителей их, поскольку луч продолжает пытаться зарегистрироваться в NHS, пока это не получает "регистрационный ответ". **src, dst**: Точка начала туннеля (луч) и назначение (концентратор) IP-адреса. Это источник и назначение пакета GRE, передаваемого маршрутизатором **NBMA src**: NBMA (Интернет) адрес луча, который передал этот пакет и попытки зарегистрироваться в

	addr_len: 4 (NSAP), subaddr_len: 0 (NSAP), proto_len: 4, pref: 0 **клиентский NBMA: 172.16.10.1** **протокол клиента: 10.1.1.254**	NHS **протокол src**: туннельный адрес луча, который пытается зарегистрироваться **протокол dst**: туннельный адрес NHS/концентратора **Опознавательное Расширение**, данные: строка Проверки подлинности nhrp **клиентский NBMA**: адрес NBMA NHS/концентратора **протокол клиента**: туннельный адрес NHS/концентратора
	СКОРОСТЬ NHRP: Передавая начальный Запрос регистрации за 10.1.1.254, reqid 65540 **%LINK-3-UPDOWN: Интерфейсный Tunnel0, измененное состояние к** NHRP: if_up: proto Tunnel0 0 **NHRP: Tunnel0: обновление Кэша для цели 10.1.1.254/32 следующий переход 10.1.1.254 172.16.10.1** IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): поиск соединения возвратился 961D220 NHRP: Попытка передать пакет через DEST 10.1.1.254	Больше служебных сообщений NHRP, которые говорят начальный Запрос регистрации, передавалось NHS в 10.1.1.254. Существует также подтверждение, что запись в кэше была добавлена для туннельного IP 10.1.1.254/24, который живет в NBMA 172.16.10.1. Задержанное сообщение говорит, что Туннель был "нетом закрытым", замечен здесь.
	IPSEC-IFC GRE/Tu0: туннель подъем IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): поиск соединения возвратился 961D220 IPSEC-IFC GRE/Tu0: crypto_ss_listen_start, уже слушая IPSEC-IFC GRE/Tu0: crypto_ss_listen_start, уже слушая **IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): Открытие сокета с IPSEC DMVPN профиля** IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): поиск соединения возвратился 961D220 IPSEC-IFC GRE/Tu0 (172.16.1.1/172.16.10.1): Сокет уже открыт. Игнорирование. %LINEPROTO-5-UPDOWN: Протокол линии связи на Интерфейсном Tunnel0, измененном состоянии к	Это общие сообщения Сервиса IPSec, которые говорят, что это работает должным образом. Вот то, где наконец замечено, что Протокол туннелирования подключен.
Это - запросы регистрации NHRP,	**NHRP: Получите Запрос регистрации через VRF Tunnel0 0, размер пакета: 108**	

полученные от луча в попытке зарегистрироваться к NHS (концентратор). Это обычно для наблюдения множителей их, поскольку луч продолжает пытаться зарегистрироваться в NHS, пока это не получает "регистрационный ответ". **NBMA src**: NBMA (Интернет) адрес луча, который передал этот пакет и попытки зарегистрироваться в NHS **протокол src**: туннельный адрес луча, который пытается зарегистрироваться **протокол dst**: туннельный адрес NHS/концентратора **Опознавательное Расширение**, данные: строка Проверки подлинности nhrp **клиентский NBMA**: адрес NBMA NHS/концентратора **протокол клиента**: туннельный адрес NHS/концентратора	(F) afn: IPv4 (1), введите: IP (800), переход: 255, версия: 1 shtl: 4 (NSAP), sstl: 0 (NSAP) pktsz: 108 экс-бар: 52 (M) флаги: "уникальный nat", reqid: 65540 **NBMA src: 172.16.1.1** **протокол src: 10.1.1.1, протокол dst: 10.1.1.254** (C-1) код: никакая ошибка (0) префикс: 32, mtu: 17912, hd_time: 7200 addr_len: 0 (NSAP), subaddr_len: 0 (NSAP), proto_len: 0, приставка: 0 Расширение адреса респондента (3): Вперед передайте транзитом, NHS делают запись расширения (4): Обратный транзит NHS делает запись расширения (5): **Опознавательное расширение (7):** **введите : Открытый текст (1), data:NHRPAUTH** Расширение адреса NAT (9): (C-1) код: никакая ошибка (0) префикс: 32, mtu: 17912, hd_time: 0 addr_len: 4 (NSAP), subaddr_len: 0 (NSAP), proto_len: 4, pref: 0 **клиентский NBMA: 172.16.10.1** **протокол клиента: 10.1.1.254**	
Debug packet NHRP, добавляющий целевую сеть 10.1.1.1/32 доступный через следующий переход 10.1.1.1 в NHRP 172.16.1.1. 172.16.1.1 также добавлен к списку адресов который концентратор вперед многоадресный трафик к. Эти сообщения подтверждают, что регистрация была успешна, как было разрешение для Туннельного адреса лучей.	NHRP: netid_in = 1, to_us = 1 **NHRP: Tunnel0: Кэш добавляет для цели 10.1.1.1/32 следующий переход 10.1.1.1 172.16.1.1** **NHRP: добавление оконечных точек туннеля (VPN: 10.1.1.1, NBMA: 172.16.1.1)** **NHRP: Успешно подключенный подблок NHRP для Оконечных точек туннеля (VPN: 10.1.1.1, NBMA: 172.16.1.1)** NHRP: Вставленный узел подблока для кэша: предназначайтесь для Вставленного узла подблока для кэша: предназначайтесь для 10.1.1.1/32nhop 10.1.1.1 NHRP: Преобразованная внутренняя динамическая запись в кэше для 10.1.1.1/32 взаимодействует Tunnel0 к внешнему **NHRP: Tu0: Создание динамического NBMA составления карты групповой адресации: 172.16.1.1**	

	NHRP: Добавленное динамическое составление карты групповой адресации для NBMA: 172.16.1.1 NHRP: Обновление нашего кэша с NBMA: 172.16.10.1, NBMA_ALT: 172.16.10.1 NHRP: Новая обязательная длина: 32 NHRP: Попытка передать пакет через DEST 10.1.1.1 **NHRP: NHRP успешно решил 10.1.1.1 к NBMA 172.16.1.1** **NHRP: Инкапсуляция успешно выполнилась. Туннельный адрес IP 172.16.1.1**	
Это - Регистрационный Ответ NHRP, передаваемый концентратором лучу в ответ на "Запрос регистрации NHRP", полученный ранее. Как другие регистрационные пакеты, концентратор передает множители их в ответ на множественные запросы. **src, dst**: Точка начала туннеля (концентратор) и целевые (лучевые) IP-адреса. Это источник и назначение пакета GRE, передаваемого маршрутизатором **NBMA src**: NBMA (Интернет) адрес луча **протокол src**: туннельный адрес луча, который пытается зарегистрироваться **протокол dst**: туннельный адрес NHS/концентратора **клиентский NBMA**: адрес NBMA NHS/концентратора **протокол клиента**: туннельный адрес NHS/концентратора **Опознавательное Расширение**, данные: строка Проверки подлинности nhrp	**NHRP: Передайте Регистрационный Ответ через VRF Tunnel0 0, размер пакета: 128** **src: 10.1.1.254, dst: 10.1.1.1** (F) afn: IPv4 (1), введите: IP (800), переход: 255, версия: 1 shtl: 4 (NSAP), sstl: 0 (NSAP) pktsz: 128 экс-бар: 52 (M) флаги: "уникальный nat", reqid: 65540 **NBMA src: 172.16.1.1** **протокол src: 10.1.1.1, протокол dst: 10.1.1.254** (C-1) код: никакая ошибка (0) префикс: 32, mtu: 17912, hd_time: 7200 addr_len: 0 (NSAP), subaddr_len: 0 (NSAP), proto_len: 0, приставка: 0 Расширение адреса респондента (3): (C) код: никакая ошибка (0) префикс: 32, mtu: 17912, hd_time: 7200 addr_len: 4 (NSAP), subaddr_len: 0 (NSAP), proto_len: 4, pref: 0 **клиентский NBMA: 172.16.10.1** **протокол клиента: 10.1.1.254** Вперед передайте транзитом, NHS делают запись расширения (4): Обратный транзит NHS делает запись расширения (5): **Опознавательное расширение (7):** **введите : Открытый текст (1), data:NHRPAUTH** Расширение адреса NAT (9): (C-1) код: никакая ошибка (0) префикс: 32, mtu: 17912, hd_time: 0 addr_len: 4 (NSAP), subaddr_len: 0 (NSAP), proto_len: 4, pref: 0 **клиентский NBMA: 172.16.10.1** **протокол клиента: 10.1.1.254**	
	NHRP: Получите Регистрационный Ответ через VRF Tunnel0 0, размер пакета: 128 (F) afn: IPv4 (1), введите: IP (800), переход:	Это - Регистрационный Ответ NHRP, передаваемый

	255, версия: 1 shtl: 4 (NSAP), sstl: 0 (NSAP) pktsz: 128 экс-бар: 52 (M) флаги: "уникальный nat", reqid: 65541 **NBMA src: 172.16.1.1** **протокол src: 10.1.1.1, протокол dst: 10.1.1.254** (C-1) код: никакая ошибка (0) префикс: 32, mtu: 17912, hd_time: 7200 addr_len: 0 (NSAP), subaddr_len: 0 (NSAP), proto_len: 0, приставка: 0 Расширение адреса респондента (3): (C) код: никакая ошибка (0) префикс: 32, mtu: 17912, hd_time: 7200 addr_len: 4 (NSAP), subaddr_len: 0 (NSAP), proto_len: 4, pref: 0 **клиентский NBMA: 172.16.10.1** **протокол клиента: 10.1.1.254** Вперед передайте транзитом, NHS делают запись расширения (4): Обратный транзит NHS делает запись расширения (5): **Опознавательное расширение (7):** **введите : Открытый текст (1), data:NHRPAUTH** Расширение адреса NAT (9): (C-1) код: никакая ошибка (0) префикс: 32, mtu: 17912, hd_time: 0 addr_len: 4 (NSAP), subaddr_len: 0 (NSAP), proto_len: 4, pref: 0 **клиентский NBMA: 172.16.10.1** **протокол клиента: 10.1.1.254** NHRP: netid_in = 0, to_us = 1	концентратором лучу в ответ на "Запрос регистрации NHRP", полученный ранее. Как другие регистрационные пакеты, концентратор передает множители их в ответ на множественные запросы. **NBMA src**: NBMA (Интернет) адрес луча **протокол src**: туннельный адрес луча, который пытается зарегистрироваться **протокол dst**: туннельный адрес NHS/концентратора **клиентский NBMA**: адрес NBMA NHS/концентратора **протокол клиента**: туннельный адрес NHS/концентратора **Опознавательное Расширение**, данные: строка Проверки подлинности nhrp
Более общие сообщения Сервиса IPSec, которые говорят это, работают должным образом.	IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start, уже слушая IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Открытие сокета с IPSEC DMVPN профиля IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): поиск соединения возвратился 8C93888 IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): Сокет уже открыт. Игнорирование. IPSEC-IFC MGRE/Tu0 (172.16.10.1/172.16.1.1): tunnel_protection_stop_pending_timer 8C93888	
	NHRP: NHS: 10.1.1.254	Служебные сообщения NHRP, которые говорят NHS, расположенный в 10.1.1.254, подключены.
Системное сообщение, которое сообщает	%DUAL-5-NBRCHANGE: IPv4 EIGRP 1: Соседний узел 10.1.1.1 (Tunnel0) подключен:	

смежность EIGRP, подключено с соседним лучом в 10.1.1.1.	новая смежность	
	%DUAL-5-NBRCHANGE: IPv4 EIGRP 1: Соседний узел 10.1.1.254 (Tunnel0) подключен: новая смежность	Системное сообщение, которое сообщает смежность EIGRP, подключено с соседним концентратором в 10.1.1.254.
Системное сообщение, которое подтверждает успешное решение NHRP.	NHRP: NHRP успешно решил 10.1.1.1 к NBMA 172.16.1.1	

Подтвердите функциональность и устранение неполадок

Этот раздел имеет некоторые из большинства **полезных команд show**, используемых для устранения проблем обоих концентратор и луч. Для включения более определенных отладок используйте эти условные выражения отладки:

- узел debug dmvpn condition nbma *NBMA_ADDRESS*
- узел debug dmvpn condition туннелирует *TUNNEL_ADDRESS*
- одноранговый ipv4 debug crypto condition *NBMA_ADDRESS*

show crypto socket

```
Spoke1#show crypto sockets

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 172.16.1.1/172.16.10.1
Local Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.10.1/255.255.255.255/0/47)
IPSec Profile: "DMVPN-IPSEC"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "DMVPN-IPSEC" Map-name: "Tunnel0-head-0" Hub#show crypto sockets

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 172.16.10.1/172.16.1.1
Local Ident (addr/mask/port/prot): (172.16.10.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
IPSec Profile: "DMVPN-IPSEC"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "DMVPN-IPSEC" Map-name: "Tunnel0-head-0"
```

подробность show crypto session

```
Spoke1#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:01:01
Session status: UP-ACTIVE
Peer: 172.16.10.1 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 172.16.10.1
Desc: (none)
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:58
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 25 drop 0 life (KB/Sec) 4596087/3538
Outbound: #pkts enc'ed 25 drop 3 life (KB/Sec) 4596087/3538 Hub#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:01:47
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none)
ivrf: (none)
Phase1_id: 172.16.1.1
Desc: (none)
IKEv1 SA: local 172.16.10.1/500 remote 172.16.1.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:12
IPSEC FLOW: permit 47 host 172.16.10.1 host 172.16.1.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 35 drop 0 life (KB/Sec) 4576682/3492
Outbound: #pkts enc'ed 35 drop 0 life (KB/Sec) 4576682/3492
```

show crypto isakmp sa detail

```
Spoke1#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1001 172.16.1.1 172.16.10.1 ACTIVE 3des sha psk 1 23:59:10
Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA Hub#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryptionIPv4 Crypto ISAKMP SA
C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1001 172.16.10.1 172.16.1.1 ACTIVE 3des sha psk 1 23:58:20
```

```
Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA
```

подробность show crypto ipsec sa

```
Spoke1#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.1.1
protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
current_peer 172.16.10.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 3, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.10.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xA259D71(170237297)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport,}
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE
outbound ah sas:
outbound pcp sas: Hub#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
```

```
remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
current_peer 172.16.1.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 34, #pkts encrypt: 34, #pkts digest: 34
#pkts decaps: 34, #pkts decrypt: 34, #pkts verify: 34
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.10.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x8D538D11(2371063057)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4576682/3497)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas: spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4576682/3497)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:
outbound pcp sas:
```

show ip nhrp

```
Spoke1#show ip nhrp
10.1.1.254/32 via 10.1.1.254
Tunnel0 created 00:00:55, never expire
Type: static, Flags:
NBMA address: 172.16.10.1 Hub#show ip nhrp
10.1.1.1/32 via 10.1.1.1
Tunnel0 created 00:01:26, expire 01:58:33
Type: dynamic, Flags: unique registered
NBMA address: 172.16.1.1
```

show ip Государственная служба здравоохранения

```
Spoke1#show ip nhrp nhs
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
10.1.1.254 RE priority = 0 cluster = 0 Hub#show ip nhrp nhs (As the hub is the only NHS for this
DMVPN cloud,
it does not have any servers configured)
```

show dmvpn [подробность]

```
"show dmvpn detail" returns the output of show ip nhrp nhs, show dmvpn,
and show crypto session detail

Spoke1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.10.1 10.1.1.254 UP 00:00:39 S Spoke1#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface Tunnel0 is up/up, Addr. is 10.1.1.1, VRF ""
Tunnel Src./Dest. addr: 172.16.1.1/172.16.10.1, Tunnel VRF ""
Protocol/Transport: "GRE/IP", Protect "DMVPN-IPSEC"
Interface State Control: Disabled

IPv4 NHS:
10.1.1.254 RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 1

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
----- --------------- --------------- ----- -------- ----- -----------------
1 172.16.10.1 10.1.1.254 UP 00:00:41 S 10.1.1.254/32


Crypto Session Details:
--------------------------------------------------------------------------------
Interface: Tunnel0
Session: [0x08D513D0]
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:59:18
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.16.10.1
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 21 drop 0 life (KB/Sec) 4596088/3558
Outbound: #pkts enc'ed 21 drop 3 life (KB/Sec) 4596088/3558
Outbound SPI : 0x A259D71, transform : esp-3des esp-sha-hmac
Socket State: Open
```

```
Pending DMVPN Sessions: Hub#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details Type:Hub, NHRP Peers:1,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.1.1.1 UP 00:01:30 D

Hub#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel0 is up/up, Addr. is 10.1.1.254, VRF ""
Tunnel Src./Dest. addr: 172.16.10.1/MGRE, Tunnel VRF ""
Protocol/Transport: "multi-GRE/IP", Protect "DMVPN-IPSEC"
Interface State Control: Disabled
Type:Hub, Total NBMA Peers (v4/v6): 1
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
----- --------------- --------------- ----- -------- ----- -----------------
1 172.16.1.1 10.1.1.1 UP 00:01:32 D 10.1.1.1/32

Crypto Session Details:
--------------------------------------------------------------------------------
Interface: Tunnel0
Session: [0x08A27858]
IKEv1 SA: local 172.16.10.1/500 remote 172.16.1.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:26
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.16.1.1
IPSEC FLOW: permit 47 host 172.16.10.1 host 172.16.1.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 32 drop 0 life (KB/Sec) 4576682/3507
Outbound: #pkts enc'ed 32 drop 0 life (KB/Sec) 4576682/3507
Outbound SPI : 0x8D538D11, transform : esp-3des esp-sha-hmac
Socket State: Open

Pending DMVPN Sessions:
```

Дополнительные сведения

- Устранение неполадок IPsec - общие сведения и использование команд debug
- Шифрование следующего поколения
- RFC3706: Dead Peer Detection IKE
- RFC3947: IKE прохождение NAT
- Cisco Systems – техническая поддержка и документация