Настройте туннели от узла к узлу IKEv1 IPsec с ASDM или CLI на ASA

Содержание

Введение

Этот документ описывает, как настроить туннель от узла к узлу IPsec Версии 1 обмена ключами между сетями (IKEv1) между Cisco 5515-X многофунциональное устройство обеспечения безопасности (ASA), которое работает под управлением ПО версии 9.2.x и ASA Серии Cisco 5510, который работает под управлением ПО версии 8.2. x.

Предварительные условия

Требования

Cisco рекомендует, чтобы эти требования были удовлетворены перед попыткой конфигурации, которая описана в этом документе:

- Сквозная возможность подключения с помощью IP-адреса должна быть установлена.
- Эти протоколы должны быть позволены:

  Протокол UDP 500 и 4500 для уровня управления IPsec

  Протокол "IP" Безопасного закрытия полезной нагрузки (ESP) 50 для плоскости данных IPsec

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- ASA Серии Cisco 5510, который работает под управлением ПО версии 8.2
- 5515-X ASA Cisco, который выполняет версию программного обеспечения 9.2

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.

Настройка

В этом разделе описывается настроить туннель VPN типа «узел-узел» через мастера VPN Менеджера устройств адаптивной безопасности (ASDM) (ASDM) или через CLI.

Схема сети

Это - топология, которая используется для примеров всюду по этому документу:

Настройте через мастера VPN ASDM

Выполните эти шаги для устанавливания туннеля VPN типа «узел-узел» через мастера ASDM:

1. Откройте ASDM и перейдите **Мастерам> Мастера VPN> Сквозной VPN-соединение Мастер**:

2. Нажмите **Next**, как только вы достигаете домашней страницы мастера:

   Примечание: Новые версии ASDM предоставляют ссылку на видео, которое объясняет эту конфигурацию.

3. Настройте IP - адрес адресуемой точки. В данном примере IP - адрес адресуемой точки установлен в 192.168.1.1 на месте B. Если вы настраиваете IP - адрес адресуемой точки на месте A, это должно быть измененный на 172.16.1.1. Интерфейс, через который может быть достигнут удаленный конец, также задан. Нажмите **Next** однажды завершенный.

4. Настройте локальные и удаленные сети (источник трафика и назначение). Этот образ показывает конфигурацию для Узла B (реверс просит Узел A):

5. На странице Security настройте предварительный общий ключ (это должно совпасть на обоих из концов). Нажмите **Next** однажды завершенный.

6. Настройте исходный интерфейс для трафика на ASA. ASDM автоматически создает правило Технологии NAT на основе версии ASA и выдвигает его с остатком конфигурации в заключительном шаге.**Примечание:** Для примера, который используется в этом документе, *внутри* источник трафика.

7. Мастер теперь предоставляет сводку конфигурации, которая будет выдвинута к ASA. Рассмотрите и проверьте параметры конфигурации, и затем нажмите **Finish**.

Настройте через CLI

В этом разделе описывается настроить туннель от узла к узлу IKEv1 IPsec через CLI.

Настройте узел B для версий ASA 8.4 и позже

В Версиях ASA 8.4 и позже, поддержка и IKEv1 и второй версии протокола Internet Key Exchange (IKEv2) был представлен.

Совет: Для получения дополнительной информации о различиях между этими двумя версиями, обратитесь к, Почему мигрируют на IKEv2? раздел *Быстрой Миграции IKEv1 к конфигурации туннеля IKEv2 L2L на* Документе Cisco *Кода ASA 8.4*.

Совет: Для примера конфигурации IKEv2 с ASA обратитесь к От узла к узлу Туннель IKEv2 между ASA и Документом Cisco Конфигурации маршрутизатора В качестве примера.

Фаза 1 (IKEv1)

Выполните эти шаги для 1-ой фазы настройки:

1. Введите эту команду в CLI для включения IKEv1 на внешнем интерфейсе:
   crypto ikev1 enable outside
2. Создайте политику IKEv1, которая определяет алгоритмы/методы, которые будут использоваться для хеширования, аутентификации, Группы Диффи-Хеллмана, срока действия и шифрования:
   crypto ikev1 enable outside
3. Создайте туннельную группу под атрибутами IPSec и настройте IP - адрес адресуемой точки и туннельный предварительный общий ключ:
   crypto ikev1 enable outside

Фаза 2 (IPsec)

Выполните эти шаги для 2-ой фазы настройки:

1. Создайте список доступа, который определяет трафик, который будет зашифрован, и туннелировал. В данном примере трафик интереса является трафиком из туннеля, который получен от 10.2.2.0 подсетей до 10.1.1.0. Если существуют несколька подсетей, включенные между узлами, это может содержать несколька точек входа.

   В Версиях 8.4 и позже, объекты или групповые объекты могут быть созданы, которые служат контейнерами для сетей, подсетей, адресов IP - адреса хоста или множественных объектов. Создайте два объекта, которые имеют локальные и удаленные подсети и используют их и для крипто-Списка контроля доступа (ACL) и для Выражений NAT.
   crypto ikev1 enable outside
2. Настройте Набор преобразований (TS), который должен включить **ключевое слово IKEv1**. Идентичный TS должен быть создан на удаленном конце также.
   crypto ikev1 enable outside
3. Настройте криптокарту, которая содержит эти компоненты:

   IP - адрес адресуемой точки

   Определенный список доступа, который содержит трафик интереса

   TS

   Дополнительное значение безопасной пересылки (Perfect Forward Secrecy, PFS), которое создает новую пару Ключей Диффи-Хеллмана, которые используются для защиты данных (обе стороны должны быть поддерживающими безопасную пересылку (PFS) перед Фазой 2, подходит),

4. !--- Примените криптокарту к внешнему интерфейсу:
   crypto ikev1 enable outside

Освобождение NAT

Гарантируйте, что трафик VPN не подвергнут никакому другому правилу NAT. Это - правило NAT, которое используется:

crypto ikev1 enable outside

Примечание: Когда несколька подсетей используются, необходимо создать групповые объекты со всем источником и подсетями назначения и использовать их в правиле NAT.

```
crypto ikev1 enable outside
```

Конфигурация полной выборки

Вот завершенная конфигурация для Узла B:

```
crypto ikev1 enable outside

crypto ikev1 policy 10
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400

tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 ipsec-attributes
ikev1 pre-shared-key cisco
!Note the IKEv1 keyword at the beginning of the pre-shared-key command.

object network 10.2.2.0_24
subnet 10.2.2.0 255.255.255.0
object network 10.1.10_24
subnet 10.1.1.0 255.255.255.0

access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24

crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac

crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 192.168.254.1
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside

nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static
10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

Настройте узел для версий ASA 8.2 и ранее

В этом разделе описывается настроить, Помещают для Версий ASA 8.2 и ранее.

Фаза 1 (ISAKMP)

Выполните эти шаги для 1-ой фазы настройки:

1. Введите эту команду в CLI для включения Протокола ISAKMP на внешнем интерфейсе: **`crypto isakmp enable outside`****Примечание:** Поскольку несколька версий IKE (IKEv1 и IKEv2) не поддерживаются больше, ISAKMP используется для обращения к Фазе 1.
2. Создайте Политику ISAKMP, которая определяет алгоритмы/методы, которые будут использоваться, для построения Фазы 1.**Примечание:** В конфигурации данного примера *ключевое слово IKEv1* от Версии 9.x заменено *ISAKMP*.**`crypto isakmp enable outside`**
3. Создайте туннельную группу для IP - адреса адресуемого точки (внешний IP - адрес

5515) с предварительным общим ключом:
crypto isakmp enable outside

Фаза 2 (IPsec)

Выполните эти шаги для 2-ой фазы настройки:

1. Подобный конфигурации в Версии 9.x, необходимо создать расширенный список доступа для определения трафика интереса.
   crypto isakmp enable outside
2. Определите TS, который содержит все доступное шифрование, и алгоритмы хеширования (предлагаемый проблемы имеют вопросительный знак). Гарантируйте, что это идентично этому, которое было настроено с другой стороны.
   crypto isakmp enable outside
3. Настройте криптокарту, которая содержит эти компоненты:

   IP - адрес адресуемой точки

   Определенный список доступа, который содержит трафик интереса

   TS

   Дополнительное значение безопасной пересылки (PFS), которое создает новую пару Ключей Диффи-Хеллмана, которые используются для защиты данных (обе стороны должны быть поддерживающими безопасную пересылку (PFS) так, чтобы Фаза 2 подошла),

4. !--- Примените криптокарту к внешнему интерфейсу:
   crypto isakmp enable outside

Освобождение NAT

Создайте список доступа, который определяет трафик, который будет освобожден от проверок NAT. В этой версии это кажется подобным списку доступа, который вы определили для трафика интереса:

crypto isakmp enable outside

Когда несколько подсетей будут использоваться, добавьте другую линию к тому же списку доступа:

crypto isakmp enable outside

Список доступа используется с NAT, как показано здесь:

crypto isakmp enable outside

> **Примечание:** *Внутренняя часть* здесь обращается к названию внутреннего интерфейса, на котором ASA получает трафик, который совпадает со списком доступа.

Конфигурация полной выборки

Вот завершенная конфигурация для Узла A:

```
crypto isakmp enable outside
crypto isakmp policy 10
```

```
authentication pre-share
encryption aes
hash sha group 2
lifetime 86400

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
pre-shared-key cisco

access-list 100 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
crypto ipsec transform-set myset esp-aes esp-sha-hmac

crypto map outside_map 20 set peer
crypto map outside_map 20 match address 100
crypto map outside_map 20 set transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside

access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0

nat (inside) 0 access-list nonat
```

Групповая политика

Групповые политики используются для определения определенных параметров настройки, которые применяются к туннелю. Эта политика используется в сочетании с туннельной группой.

Групповая политика может быть определена или как внутренняя, что означает, что атрибуты вытягивают от того, что определено на ASA, или это может быть определено как внешнее, где атрибуты делают запрос от внешнего сервера. Это - команда, которая используется для определения групповой политики:

```
group-policy SITE_A internal
```

> **Примечание:** Можно определить множественные атрибуты в групповой политике. Для списка всех возможных атрибутов обратитесь к разделу Групповых политик Настройки *Выбранных Процедур Конфигурации VPN ASDM для серии 5500 Cisco ASA, Версии 5.2*.

Необязательные атрибуты групповой политики

Атрибут **vpn-tunnel-protocol** определяет тип туннеля, к которому должны быть применены эти параметры настройки. В данном примере используется *IPsec*:

```
group-policy SITE_A internal
```

У вас есть опция для настройки туннеля так, чтобы это осталось простаивающим ("no traffic" (нет трафика)) и не выключалось. Для настройки этой опции значение атрибута **vpn-idle-timeout** должно использовать минуты, или можно установить значение ни в **один**, что означает, что никогда не выключается туннель.

Например:

```
group-policy SITE_A internal
```

Команда default-group-policy под общими атрибутами туннельной группы определяет групповую политику, которая используется для требования у определенных параметров настройки политики туннель, который установлен. Настройки по умолчанию для опций, которые вы не определили в групповой политике, взяты от глобальной политики группы по умолчанию:

```
group-policy SITE_A internal
```

Проверка

Используйте информацию, которая предоставлена в этом разделе, чтобы проверить, что ваша конфигурация работает должным образом.

ASDM

Для просмотра статуса туннеля от ASDM перейдите к **Мониторингу> VPN**. Эта информация предоставлена:

- IP - адрес адресуемой точки
- Протокол, который используется для построения туннеля
- Алгоритм шифрования, который используется
- Время, в которое туннель подошел и время работы без сбоев
- Количество пакетов, которые получены и переданы

  Совет: Нажмите **Refresh** для просмотра последних значений, поскольку данные не обновляют в режиме реального времени.

CLI

В этом разделе описывается проверить вашу конфигурацию через CLI.

Этап 1

Введите эту команду в CLI для проверки 1-ой фазы настройки на Узле B (5515) сторона:

```
show crypto ikev1 sa

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 192.168.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

Введите эту команду в CLI для проверки 1-ой фазы настройки на Узле (5510) сторона:

```
show crypto isakmp sa

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 172.16.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

Этап 2

Команда show crypto ipsec sa показывает контексты безопасности IPSec, которые созданы между узлами. Зашифрованный туннель создан между IP-адресами 192.168.1.1 и 172.16.1.1 для трафика, который течет между сетями 10.1.1.0 и 10.2.2.0. Вы видите два SA ESP, созданные для входящего и исходящего трафика. Заголовок аутентификации (AH) не используется, потому что нет никаких SA AH.

Введите эту команду в CLI для проверки 2-ой фазы настройки на Узле B (5515) сторона:

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 172.16.1.1
 local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
 current_peer: 192.168.1.1
PERMIT, flags={origin_is_acl,}
#pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0, #send errors 0, #recv errors 0
   local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
      transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
      sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
      transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
      sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

Введите эту команду в CLI для проверки 2-ой фазы настройки на Узле (5510) сторона:

```
interface: FastEthernet0
```

```
Crypto map tag: outside_map, local addr. 192.168.1.1
  local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
  current_peer: 172.16.1.1
PERMIT, flags={origin_is_acl,}
   #pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0, #send errors 0, #recv errors 0
    local crypto endpt.: 192.168.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
       transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
       transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

Устранение неполадок

Используйте информацию, которая предоставлена в этом разделе для устранения проблем проблем конфигурации.

Версии ASA 8.4 и позже

Введите эти команды отладки для определения местоположения туннельного сбоя:

- debug crypto (фаза 1) ikev1 127
- debug crypto ipsec 127 (Фаза 2)

Вот завершенные выходные данные отладки в качестве примера:

```
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE Initiator: New Phase 1, Intf NP
```

```
Identity Ifc, IKE Peer 192.168.1.1 local Proxy Address 10.2.2.0, remote Proxy
Address 10.1.1.0, Crypto map (outside_map) Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing ISAKMP SA payload Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing NAT-Traversal VID ver 02 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver 03 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver RFC payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Fragmentation VID +
extended capabilities payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 172
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total
length : 132
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Oakley proposal is acceptable
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received NAT-Traversal ver 02 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Fragmentation VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, IKE Peer included IKE
fragmentation capability flags: Main Mode: True Aggressive Mode: True
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Cisco Unity
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing xauth V6
VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send IOS VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ISA_KE payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]?IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Cisco Unity client VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received xauth V6 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing VPN3000/ASA spoofing
IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Altiga/Cisco
VPN3000/Cisco ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload
```

Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload
!
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, **Connection landed on tunnel_group 192.168.1.1**
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, Generating keys for Initiator...
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing ID payload
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, constructing hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing hash for ISAKMP
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing IOS keep alive payload: proposal=32767/32767 sec.
!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/10 ms
ciscoasa# Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing dpd vid payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500 from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, ID_IPV4_ADDR ID received 192.168.1.1
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing hash for ISAKMP
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing IOS keep alive payload: proposal=32767/32767 sec.
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Received DPD VID
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Connection landed on tunnel_group 192.168.1.1
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Oakley begin quick mode
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator starting QM: msg id = 4c073b21
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 1 COMPLETED
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Keep-alive type for this connection: DPD
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting P1 rekey timer: 73440 seconds.
IPSEC: New embryonic SA created @ 0x75298588,
SCB: 0x75C34F18,
Direction: inbound
SPI : 0x03FC9DB7
Session ID: 0x00004000
VPIF num : 0x00000002
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds

```
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
IKE got SPI from key engine: SPI = 0x03fc9db7
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
oakley constucting quick mode
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing blank hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing IPSec SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing IPSec nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing proxy ID
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
Transmitting Proxy Id:
Local subnet: 10.2.2.0 mask 255.255.255.0 Protocol 0 Port 0
Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,
IKE Initiator sending Initial Contact
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1,
IP = 192.168.1.1, constructing qm hash payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1,
IP = 192.168.1.1, IKE Initiator sending 1st QM pkt: msg id = 4c073b21
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=4c073b21)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
NOTIFY (11) + NONE (0) total length : 200
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
total length : 172
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing ID payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,
ID_IPV4_ADDR_SUBNET ID received--10.2.2.0--255.255.255.0
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing ID payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
loading all IPSEC SAs
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
Generating Quick Mode Key!
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
NP encrypt rule look up for crypto map outside_map 20 matching ACL
100: returned cs_id=6ef246d0; encrypt_rule=752972d0;
tunnelFlow_rule=75ac8020
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x6f0e03f0,
SCB: 0x75B6DD00,
Direction: outbound
SPI : 0x1BA0C55C
Session ID: 0x00004000
VPIF num : 0x00000002
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x1BA0C55C
```

IPSEC: Creating outbound VPN context, SPI 0x1BA0C55C
Flags: 0x00000005
SA : 0x6f0e03f0
SPI : 0x1BA0C55C
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x0B47D387
Channel: 0x6ef0a5c0
IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0000f614
IPSEC: New outbound encrypt rule, SPI 0x1BA0C55C
Src addr: 10.2.2.0
Src mask: 255.255.255.0
Dst addr: 10.1.1.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x1BA0C55C
Rule ID: 0x74e1c558
IPSEC: New outbound permit rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x1BA0C55C
Rule ID: 0x6f0dec80
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, NP encrypt rule look up for crypto map outside_map 20 matching ACL 100: returned cs_id=6ef246d0; encrypt_rule=752972d0; tunnelFlow_rule=75ac8020
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Security negotiation complete for LAN-to-LAN Group (192.168.1.1) Initiator, Inbound SPI = 0x03fc9db7, Outbound SPI = 0x1ba0c55c
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley constructing final quick mode
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending 3rd QM pkt: msg id = 4c073b21
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 76
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got a KEY_ADD msg for SA: SPI = 0x1ba0c55c
IPSEC: New embryonic SA created @ 0x75298588,

```
SCB: 0x75C34F18,
Direction: inbound
SPI : 0x03FC9DB7
Session ID: 0x00004000
VPIF num : 0x00000002
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x03FC9DB7
IPSEC: Creating inbound VPN context, SPI 0x03FC9DB7
Flags: 0x00000006
SA : 0x75298588
SPI : 0x03FC9DB7
MTU : 0 bytes
VCID : 0x00000000
Peer : 0x0000F614
SCB : 0x0B4707C7
Channel: 0x6ef0a5c0
IPSEC: Completed inbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x00011f6c
IPSEC: Updating outbound VPN context 0x0000F614, SPI 0x1BA0C55C
Flags: 0x00000005
SA : 0x6f0e03f0
SPI : 0x1BA0C55C
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00011F6C
SCB : 0x0B47D387
Channel: 0x6ef0a5c0
IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0000f614
IPSEC: Completed outbound inner rule, SPI 0x1BA0C55C
Rule ID: 0x74e1c558
IPSEC: Completed outbound outer SPD rule, SPI 0x1BA0C55C
Rule ID: 0x6f0dec80
IPSEC: New inbound tunnel flow rule, SPI 0x03FC9DB7
Src addr: 10.1.1.0
Src mask: 255.255.255.0
Dst addr: 10.2.2.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x03FC9DB7
Rule ID: 0x74e1b4a0
IPSEC: New inbound decrypt rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
```

```
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de830
IPSEC: New inbound permit rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de8d8
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Pitcher:
received KEY_UPDATE, spi 0x3fc9db7
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting
P2 rekey timer: 24480 seconds.
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 2
COMPLETED (msgid=4c073b21)
```

Версии ASA 8.3 и ранее

Введите эти команды отладки для определения местоположения туннельного сбоя:

- **debug crypto isakmp 127** (Фаза 1)
- **debug crypto ipsec 127** (Фаза 2)

Вот завершенные выходные данные отладки в качестве примера:

```
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
NONE (0) total length : 172
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Oakley proposal is acceptable
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 02 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 03 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal RFC VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Fragmentation VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE Peer included IKE fragmentation
capability flags: Main Mode: True Aggressive Mode: True
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing IKE SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE SA Proposal # 1, Transform # 1
```

acceptable Matches global IKE entry # 1
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ISAKMP SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Traversal VID ver
02 payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Fragmentation VID +
extended capabilities payload
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 132
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ke payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ISA_KE payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Cisco Unity client VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received xauth V6 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing VPN3000/ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ke payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Cisco Unity VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing xauth V6 VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send IOS VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing ASA spoofing IOS Vendor
ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send Altiga/Cisco VPN3000/Cisco
ASA GW VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating keys
for Responder...
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0)
total length : 96
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
ID payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR
ID received 172.16.1.1
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing
hash for ISAKMP
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing IOS keep alive payload:
proposal=32767/32767 sec.
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Received DPD VID

Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing ID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing hash for ISAKMP
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing IOS keep alive payload: proposal=32767/32767 sec.
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing dpd vid payload
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 1 COMPLETED
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Keep-alive type for this connection: DPD
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P1 rekey timer: 82080 seconds.
Feb 13 04:19:53 [IKEv1 DECODE]: IP = 172.16.1.1, IKE Responder starting QM: msg id = 4c073b21
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR_SUBNET ID received--10.2.2.0--255.255.255.0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received remote IP Proxy Subnet data in ID Payload: Address 10.2.2.0, Mask 255.255.255.0, Protocol 0, Port 0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received local IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing notify payload
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, QM IsRekeyed old sa not found by addr
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map check, checking map = outside_map, seq = 20...
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map check, map outside_map, seq = 20 is a successful match
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Remote Peer configured for crypto map: outside_map
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing IPSec SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IPSec SA Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0xAB5C63A8,
SCB: 0xABD54E98,
Direction: inbound

```
SPI : 0x1BA0C55C
Session ID: 0x00004000
VPIF num : 0x00000001
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got SPI
from key engine: SPI = 0x1ba0c55c
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, oakley
constucting quick mode
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
blank hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
IPSec SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
IPSec nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
proxy ID
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Transmitting
Proxy Id:
Remote subnet: 10.2.2.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
qm hash payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Responder
sending 2nd QM pkt: msg id = 4c073b21
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message
(msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) +
ID (5) + NONE (0) total length : 172
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message
(msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 52
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, loading all
IPSEC SAs
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating
Quick Mode Key!
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt
rule look up for crypto map outside_map 20 matching ACL 100: returned
cs_id=ab9302f0; rule=ab9309b0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating
Quick Mode Key!
IPSEC: New embryonic SA created @ 0xAB570B58,
SCB: 0xABD55378,
Direction: outbound
SPI : 0x03FC9DB7
Session ID: 0x00004000
VPIF num : 0x00000001
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x03FC9DB7
IPSEC: Creating outbound VPN context, SPI 0x03FC9DB7
Flags: 0x00000005
SA : 0xAB570B58
SPI : 0x03FC9DB7
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x01512E71
Channel: 0xA7A98400
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x0000F99C
IPSEC: New outbound encrypt rule, SPI 0x03FC9DB7
```

```
Src addr: 10.1.1.0
Src mask: 255.255.255.0
Dst addr: 10.2.2.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x03FC9DB7
Rule ID: 0xABD557B0
IPSEC: New outbound permit rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x03FC9DB7
Rule ID: 0xABD55848
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule
look up for crypto map outside_map 20 matching ACL 100: returned cs_id=ab9302f0;
rule=ab9309b0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Security negotiation
complete for LAN-to-LAN Group (172.16.1.1) Responder, Inbound SPI = 0x1ba0c55c,
Outbound SPI = 0x03fc9db7
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got a
KEY_ADD msg for SA: SPI = 0x03fc9db7
IPSEC: Completed host IBSA update, SPI 0x1BA0C55C
IPSEC: Creating inbound VPN context, SPI 0x1BA0C55C
Flags: 0x00000006
SA : 0xAB5C63A8
SPI : 0x1BA0C55C
MTU : 0 bytes
VCID : 0x00000000
Peer : 0x0000F99C
SCB : 0x0150B419
Channel: 0xA7A98400
IPSEC: Completed inbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0001169C
IPSEC: Updating outbound VPN context 0x0000F99C, SPI 0x03FC9DB7
Flags: 0x00000005
SA : 0xAB570B58
SPI : 0x03FC9DB7
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x0001169C
```

```
SCB : 0x01512E71
Channel: 0xA7A98400
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x0000F99C
IPSEC: Completed outbound inner rule, SPI 0x03FC9DB7
Rule ID: 0xABD557B0
IPSEC: Completed outbound outer SPD rule, SPI 0x03FC9DB7
Rule ID: 0xABD55848
IPSEC: New inbound tunnel flow rule, SPI 0x1BA0C55C
Src addr: 10.2.2.0
Src mask: 255.255.255.0
Dst addr: 10.1.1.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x1BA0C55C
Rule ID: 0xAB8D98A8
IPSEC: New inbound decrypt rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x1BA0C55C
Rule ID: 0xABD55CB0
IPSEC: New inbound permit rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x1BA0C55C
```

Rule ID: 0xABD55D48
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Pitcher: received KEY_UPDATE, spi 0x1ba0c55c
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P2 rekey timer: 27360 seconds.
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 2 COMPLETED (msgid=4c073b21)