От ASA к ASA Динамический-к-статичному Пример конфигурации IKEv1/IPsec

Содержание

Введение

Этот документ описывает, как позволить Устройству адаптивной защиты (ASA) принять динамический IPsec сквозные VPN-соединение соединения от любого динамического узла (ASA в этом случае). Поскольку Диаграмма сети в этом документе показывает, Туннель IPSec установлен, когда туннель инициируется от конца Удаленного ASA только. Центральный ASA не может инициировать VPN-туннель из-за динамической Конфигурации IPSec. IP-адрес Удаленного ASA неизвестен.

Настройте Центральный ASA для динамичного принятия соединений от IP-адреса подстановочного знака (0.0.0.0/0) и предварительный совместно используемый подстановочный ключ. Удаленный ASA тогда настроен для шифрования трафика от локального до подсетей Центрального ASA, как задано крипто-access-list. Обе стороны выполняют освобождение Технологии NAT для обхода NAT для Трафика IPSec.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Cisco ASA (5510 и 5520) Выпуск 9.x Программного обеспечения межсетевого экрана и позже.

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

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

Настройка посредством ASDM

Центральный ASA (статический одноранговый узел)

На ASA со Статическим IP - адресом установите VPN таким способом, которым это принимает динамические соединения от неизвестного узла, в то время как это все еще аутентифицирует узел с помощью Предварительного общего ключа IKEv1:

1. Выберите **Configuration> Site-to-Site VPN> Advanced> Crypto Maps.** Окно отображает список элементов криптокарты, которые уже являются на месте (если существует кто-либо). Так как ASA не знает, каков IP - адрес адресуемой точки для ASA, чтобы признать, что соединение настраивает **Динамическую схему** с соответствующим transform-set (Предложение по Ipsec). **Нажмите Add.**
2. В окне Create IPsec Rule, от вкладки Tunnel Policy (Crypto Map) - Basic, выбирают **снаружи** из Интерфейсного выпадающего списка и **динамичный** от выпадающего списка Типа Политики. В Приоритетном поле назначьте приоритет для этой записи в случае, если существуют несколько точек входа под Динамической схемой. Затем, нажмите **Select** рядом с полем IPsec Proposal v1 IKE для выбора предложения по Ipsec.
3. Когда диалоговое окно Select IPsec Proposals (Transform Sets) открывается, выберите среди текущих предложений по Ipsec или **нажмите Add**, чтобы создать новый и использовать то же. **Закончив все действия, нажмите кнопку OK.**

4. От Туннельной Политики (Криптокарта) - Вкладка Дополнительно, проверьте флажок **Enable NAT-T** (потребовал, если любой узел находится позади устройства NAT), и флажок **Enable Reverse Route Injection**. Когда VPN-туннель предстает перед динамическим узлом, ASA устанавливает динамический маршрут для согласованной удаленной сети VPN, которая указывает к интерфейсу VPN.Дополнительно, от вкладки Traffic Selection можно также определить содержательный трафик VPN для динамического узла и нажать **OK**. Как отмечалось ранее, так как ASA не имеет никакой информации об удаленном динамическом IP - адресе адресуемом точки, неизвестных землях запроса подключения под DefaultL2LGroup, который существует на ASA по умолчанию. Для аутентификации для следования за предварительным общим ключом (cisco123 в данном примере) настроенный на удаленном узле должен совпасть с одним под DefaultL2LGroup.
5. Выберите **Configuration> Site-to-Site VPN> Advanced> Tunnel Groups**, выберите **DefaultL2LGroup**, нажмите **Edit** и настройте желаемый предварительный общий ключ. **Закончив все действия, нажмите кнопку OK.Примечание:** Это создает предварительный общий ключ подстановочного знака на статическом одноранговом узле (Центральный ASA). Любое устройство/узел, кто знает этот предварительный общий ключ и его соответствующие предложения, может успешно установить VPN-туннель и обратиться к ресурсам по VPN. Гарантируйте, что этот pre-skared ключ не разделен с неизвестными объектами и не легок предположить.
6. Выберите **Configuration> Site-to-Site VPN> Group Policies** и выберите групповую политику по Вашему выбору (групповая политика по умолчанию в этом случае). Нажмите **Edit** и отредактируйте групповую политику в диалоговом окне Edit Internal Group Policy. **Закончив все действия, нажмите кнопку OK.**
7. Выберите **Configuration> Firewall> NAT Rules** и из окна Add Nat Rule, не настройте nat (NAT-EXEMPT) правило для трафика VPN. **Закончив все действия, нажмите кнопку OK.**

Удаленный ASA (динамический узел)

1. Выберите **Wizards> VPN Wizards> Site-to-site VPN Wizard**, как только приложение ASDM соединяется с ASA.
2. **Нажмите кнопку Next.**
3. Выберите **снаружи** из выпадающего списка Интерфейса доступа VPN для определения внешнего IP - адреса удаленного узла. Выберите интерфейс **(глобальная сеть (WAN))**, где применена криптокарта. **Нажмите кнопку Next.**
4. Задайте хосты/сети, которым нужно позволить пройти через VPN-туннель. В этом шаге необходимо предоставить Локальные сети и Удаленные сети для VPN-туннеля. Нажмите кнопки рядом с полями Local Network и Remote Network и выберите адрес согласно требованию. Нажмите **Next**, когда вы будете сделаны.
5. Введите информацию для аутентификации для использования, который является предварительным общим ключом в данном примере. Название ключа cisco123. Именем группы туннелей является IP-адрес удаленного узла по умолчанию при настройке LAN-LAN (L2L) VPN.**Или**Можно настроить конфигурацию для включения IKE и политики IPsec по Вашему выбору. Между узлами должна быть по крайней мере одна соответствующая политика:От вкладки Authentication Methods введите предварительный общий ключ версии 1 IKE в поле Pre-shared Key. В данном примере это - **cisco123**.Нажмите вкладку **Encryption Algorithms**.

6. Нажмите **Manage** рядом с полем IKE Policy, **нажмите Add** и настройте пользовательский Набор правил IKE **(фаза 1)**. **Закончив все действия, нажмите кнопку OK.**
7. Нажмите **Select** рядом с поле IPsec Proposal и выберите желаемое Предложение по Ipsec. Нажмите **Next**, когда вы будете сделаны.Дополнительно, можно перейти к вкладке Perfect Forward Secrecy и проверить **Разрешать** флажок **безопасной пересылки (Perfect Forward Secrecy, PFS)**. Нажмите **Next**, когда вы будете сделаны.
8. Проверьте **Освобожденный хост/сеть стороны ASA от** флажка **переадресации** для предотвращения туннельного трафика от запуска Трансляции сетевых адресов. Выберите или **локальный или внутри** от выпадающего списка для установки интерфейса, где локальная сеть достижима. **Нажмите кнопку Next.**
9. ASDM отображает сводку VPN, просто настроенной. Проверьте и нажмите **Finish**.

Конфигурация интерфейса командой строки CLI

Центральный ASA (статический одноранговый узел) конфигурация

1. Настройте NO-NAT/ОСВОБОЖДЕННОЕ ОТ NAT правило для трафика VPN как показано в примере:
```
object network 10.1.1.0-remote_network
subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-inside_network
 subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
no-proxy-arp route-lookup
```
2. Настройте общий ключ под DefaultL2LGroup для аутентификации любого удаленного Динамического узла L2L:
```
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123
```
3. Определите phase-2/ISAKMP политика:
```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```
4. Определите набор преобразований фазы 2 / ПОЛИТИКА IPSEC:
```
crypto ipsec ikev1
transform-set tset esp-aes-256 esp-sha-hmac
```
5. Настройте динамическую схему с этими параметрами: Требуемый transform-setВключите Включение ввода обратной маршрутизации (RRI), которое позволяет Устройству безопасности изучать сведения о маршрутизации для подключенных клиентов (Необязательно)
```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set
tset
crypto dynamic-map outside_dyn_map 1 set reverse-route
```
6. Свяжите динамическую схему с криптокартой, примените криптокарту и включите ISAKMP/IKEv1 на внешнем интерфейсе:
```
crypto map outside_map 65535 ipsec-isakmp dynamic
outside_dyn_map

crypto map outside_map interface outside
crypto ikev1 enable outside
```

Удаленный ASA (динамический узел)

1. Настройте правило освобождения NAT для трафика VPN:`object network 10.1.1.0-inside_network`
   `subnet 10.1.1.0 255.255.255.0`

   `object network 10.1.2.0-remote_network`
   `subnet 10.1.2.0 255.255.255.0`

   `nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network`
   `destination static 10.1.2.0-remote_network 10.1.2.0-remote_network`
   `no-proxy-arp route-lookup`
2. Настройте туннельную группу для статического узла VPN и общего ключа.`tunnel-group 172.16.2.1 type ipsec-l2l`
   `tunnel-group 172.16.2.1 ipsec-attributes`
   `ikev1 pre-shared-key cisco123`
3. Определите PHASE-1/ISAKMP политику:`crypto ikev1 policy 10`
   `authentication pre-share`
   `encryption aes-256`
   `hash sha`
   `group 2`
   `lifetime 86400`
4. Определите набор преобразований фазы 2 / ПОЛИТИКА IPSEC: **`crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac`**
5. Настройте access-list, который определяет содержательный трафик VPN / сеть: **`crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac`**
6. Настройте статическую криптокарту с этими параметрами: Крипто-access-list / access-list VPNУдаленный IP-адрес узла IPsecТребуемый transform-set**`crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac`**
7. Примените криптокарту и включите ISAKMP/IKEv1 на внешнем интерфейсе: **`crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac`**

Проверка

Используйте этот раздел, чтобы подтвердить, что конфигурация работает должным образом.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show. Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

- **show crypto isakmp sa – отображает все текущие сопоставления безопасности IKE (SA) на одноранговом узле.**
- **show crypto ipsec sa — отображает все текущие SA.**

Этот раздел показывает проверку в качестве примера outout для этих двух ASA.

Центральный ASA

```
Central-ASA#show crypto isakmp sa

  IKEv1 SAs:

    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   : responder
   Rekey  : no             State  : MM_ACTIVE

    Central-ASA# show crypto ipsec sa
interface: outside
   Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1

      local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
     current_peer: 172.16.1.1

      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
     #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
     #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
     path mtu 1500, ipsec overhead 74(44), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: 30D071C0
     current inbound spi : 38DA6E51

     inbound esp sas:
     spi: 0x38DA6E51 (953839185)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
        sa timing: remaining key lifetime (kB/sec): (3914999/28588)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x0000001F
   outbound esp sas:
     spi: 0x30D071C0 (818966976)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
        sa timing: remaining key lifetime (kB/sec): (3914999/28588)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

Удаленный ASA

```
Remote-ASA#show crypto isakmp sa

  IKEv1 SAs:

    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: 172.16.2.1
   Type   : L2L            Role   : initiator
   Rekey  : no             State  : MM_ACTIVE
```

```
  Remote-ASA#show crypto ipsec sa
interface: outside
   Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

       access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
     local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
     current_peer: 172.16.2.1

       #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
     #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
     #send errors: 0, #recv errors: 0

       local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
     path mtu 1500, ipsec overhead 74(44), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: 38DA6E51
     current inbound spi : 30D071C0

     inbound esp sas:
     spi: 0x30D071C0 (818966976)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4373999/28676)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x0000001F
   outbound esp sas:
     spi: 0x38DA6E51 (953839185)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4373999/28676)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show. Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Используйте эти команды, как показано ниже:

```
Remote-ASA#show crypto isakmp sa

  IKEv1 SAs:

    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: 172.16.2.1
   Type    : L2L             Role    : initiator
   Rekey   : no              State   : MM_ACTIVE

  Remote-ASA#show crypto ipsec sa
interface: outside
   Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

       access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
     local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
     current_peer: 172.16.2.1

       #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
     #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
     #send errors: 0, #recv errors: 0

       local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
     path mtu 1500, ipsec overhead 74(44), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: 38DA6E51
     current inbound spi : 30D071C0

     inbound esp sas:
     spi: 0x30D071C0 (818966976)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4373999/28676)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x0000001F
   outbound esp sas:
     spi: 0x38DA6E51 (953839185)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4373999/28676)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

Внимание. : Команда **clear crypto isakmp sa** навязчива, поскольку она очищает все

активные VPN-туннели.

В выпуске ПО PIX/ASA 8.0 (3) и позже, отдельная IKE SA может быть очищена с помощью команды *<peer ip address>* **clear crypto isakmp sa**. В выпусках ПО ранее, чем 8.0 (3), используйте команду *<tunnel-group-name>* **туннельной группы выхода из системы vpn-sessiondb** для очистки IKE и контекстов безопасности IPSec для одиночного туннеля.

```
Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1Remote-ASA#vpn-sessiondb
logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1
```

Отладки использовали:

```
Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1
```

Удаленный ASA (Инициатор)

Введите эту **команду packet-tracer** для инициирования туннеля:

```
Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [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=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
10.1.2.0, Crypto map (outside_map)
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
<skipped>...
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
```

```
+ VENDOR (13) + NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR ID received 172.16.2.1
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,
Oakley begin quick mode
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED


Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, IKE Initiator
starting QM: msg id = c45c7b30
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, Transmitting Proxy Id:
 Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
 Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +
ID (5) + ID (5) + NONE (0) total length : 172
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Security negotiation complete for LAN-to-LAN Group (172.16.2.1)
Initiator, Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
```

Центральный ASA (Респондент)

```
Jan 20 12:42:35 [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
:
.
Jan 20 12:42:35 [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
Jan 20 12:42:35 [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 (20) + NAT-D (20) + NONE (0) total length : 304
```

:
.
Jan 20 12:42:35 **[IKEv1]IP = 172.16.1.1, Connection landed on tunnel_group DefaultL2LGroup**
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Generating keys for Responder...
Jan 20 12:42:35 [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 (20) + NAT-D (20) +
NONE (0) total length : 304
Jan 20 12:42:35 [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
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,
ID_IPV4_ADDR ID received172.16.1.1
:
.
Jan 20 12:42:35 [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
Jan 20 12:42:35 [IKEv1]**Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED**
:
.
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, **IKE Responder starting QM**:
msg id = c45c7b30
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, **Received remote IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0**:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,
IP = 172.16.1.1, **Received local IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0, Protocol 0, Port 0**Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35 **[IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map check, map outside_dyn_map, seq = 1 is a successful match**
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
:
.
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Transmitting Proxy Id: Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0 Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE
(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED
Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security
negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) **Responder, Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0**:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, **Adding static route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0**

Дополнительные сведения

- Справочники по командам серии Cisco ASA
- Страница технической поддержки протоколов согласования IPSec и IKE
- Запросы комментариев (RFC)
- Техническая поддержка и Документация - Cisco Systems