

От узла к узлу туннель IKEv2 между ASA и примерами конфигурации маршрутизатора

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Схема сети](#)

[Общие сведения](#)

[NTP](#)

[ОСНОВАННЫЙ НА HTTP URL поиск сертификата](#)

[Проверка идентификатора равноправного узла](#)

[Размер подлинного информационного наполнения](#)

[Выделение ресурсов в режиме мультитекста на ASA](#)

[Проверка списка отозванных сертификатов](#)

[Проверка цепочки сертификатов](#)

[Типовая конфигурация ASA](#)

[Конфигурация примера отладки маршрутизатора](#)

[Типовой IOS CA конфигурация](#)

[Проверка](#)

[Проверка фазы 1](#)

[Проверка фазы 2](#)

[Устранение неполадок](#)

[Отладки на ASA](#)

[Отладки на маршрутизаторе](#)

Введение

Этот документ описывает, как установить туннель второй версии протокола Internet Key Exchange (IKEv2) от узла к узлу между устройством адаптивной защиты Cisco (ASA) и маршрутизатором, который выполняет программное обеспечение Cisco IOS.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Вторая версия протокола Internet Key Exchange (IKEv2)
- Сертификаты и инфраструктура открытых ключей (PKI)

- Network Time Protocol (NTP)

Используемые компоненты

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

- Многофункциональное устройство защиты Cisco ASA серии 5510, которое работает под управлением ПО версии 9.1 (3)
- Маршрутизатор интегрированных служб Cisco 2900 (ISR), который выполняет версию программного обеспечения Cisco IOS 15.3 (3) M1

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.

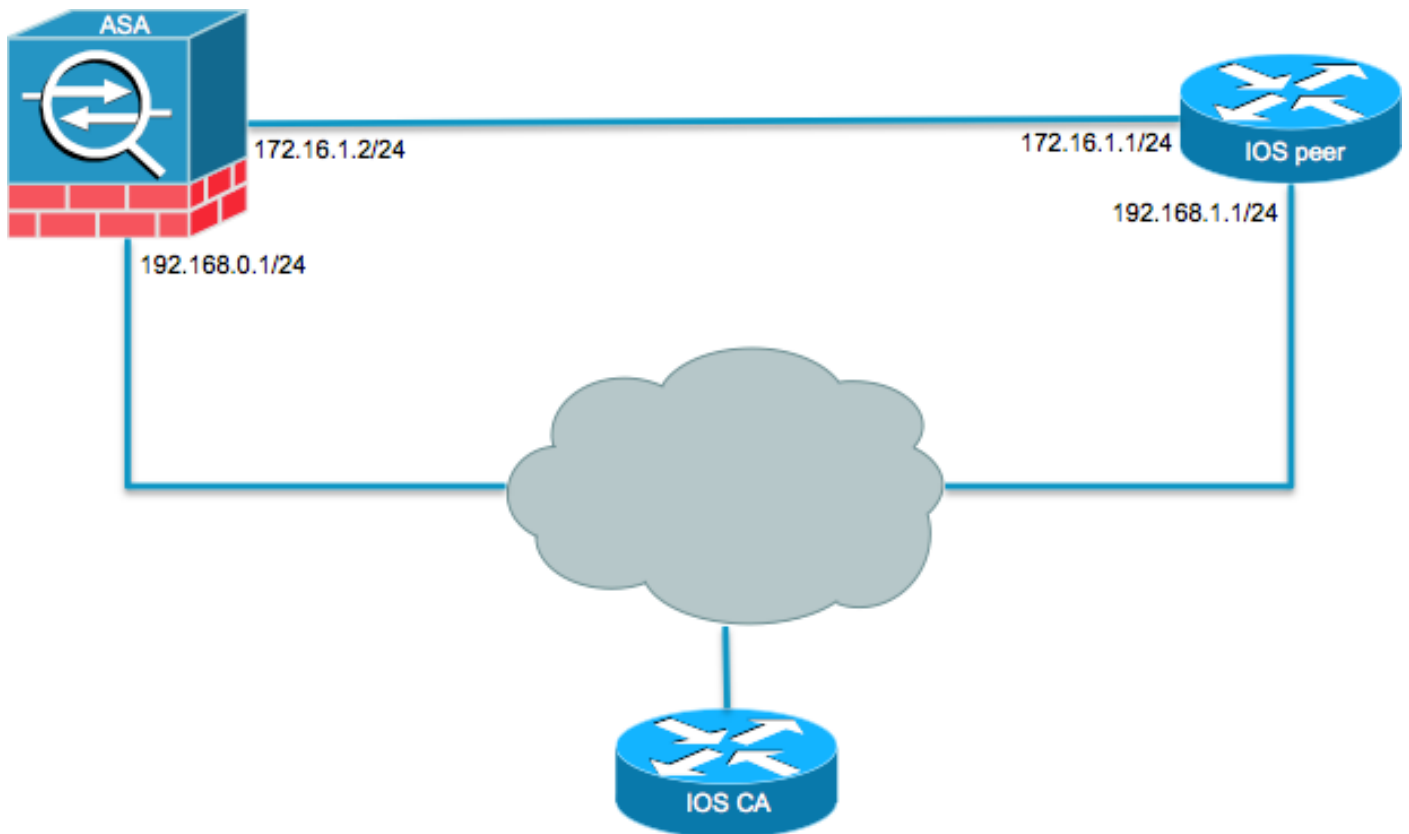
Родственные продукты

Данный документ также может использоваться со следующими версиями программного и аппаратного обеспечения:

- Cisco ASA, который работает под управлением ПО версии 8.4 (1) или позже
- Поколение 2 ISR Cisco (G2), который выполняет версию программного обеспечения Cisco IOS 15.2 (4) M или позже
- Сервисные маршрутизаторы агрегации Cisco ASR серии 1000, которые выполняют версию 15.2 (4) S программного обеспечения Cisco IOS XE или позже
- Связанные маршрутизаторы Сетки Cisco, которые работают под управлением ПО версии 15.2 (4) M или позже

Настройка

Схема сети



Общие сведения

Конфигурация туннеля IKEv2 между ASA и маршрутизатором с использованием предварительных общих ключей является прямой. Однако при использовании проверки подлинности сертификата существуют определенные предупреждения иметь в виду.

NTP

Проверка подлинности сертификата требует, чтобы часы на всех участвующих устройствах синхронизировались с общим источником. В то время как часы могут быть установлены вручную на каждом устройстве, это не является очень точным и может быть громоздким. Наилегчайший метод для синхронизации часов на всех устройствах должен использовать NTP. NTP синхронизирует хронометраж среди ряда распределенных временных серверов и клиентов. Эта синхронизация позволяет событиям быть коррелированными, когда системные журналы созданы и когда другие специфичные для времени события имеют место. Для получения дополнительной информации о том, как настроить NTP, обратитесь к [Протоколу сетевого времени: Рекомендации и Описание технологических решений](#).

Совет: Когда сервер Центра сертификации (CA) программного обеспечения Cisco IOS используется, это - общая практика для настройки того же устройства как NTP master. В данном примере сервер CA также служит сервером NTP.

ОСНОВАННЫЙ НА HTTP URL поиск сертификата

Поиск сертификата на основе HTTP URL избегает фрагментации, которая заканчивается, когда переданы большие сертификаты. Эта опция активирована на Cisco IOS Software Device по умолчанию, таким образом, тип 12 req свидетельства используется программным обеспечением Cisco IOS.

Если версии программного обеспечения, которые не имеют исправления для идентификатора ошибки Cisco [CSCu148246](#), используются на ASA, то об ОСНОВАННОМ НА HTTP URL поиске не выполняются согласования относительно ASA, и программное обеспечение Cisco IOS вызывает попытку авторизации отказать.

На ASA, если отладки протокола IKEv2 включены, появляются эти сообщения:

```
IKEv2-PROTO-1: (139): Auth exchange failed
```

```
IKEv2-PROTO-1: (140): Unsupported cert encoding found or Peer requested  
HTTP URL but never sent  
HTTP_LOOKUP_SUPPORTED Notification
```

Во избежание этой проблемы не используйте **крипто-ikev2** команду **свидетельства http url** для отключения этой опции на маршрутизаторе, когда это взаимодействует с ASA.

Проверка идентификатора равноправного узла

Во время IKE AUTH организует согласования Протокола ISAKMP, узлы должны определить себя друг другу. Однако существует различие в способе, которым маршрутизаторы и ASA выбирают свою локальную идентичность.

ID ISAKMP выбор на маршрутизаторах

Когда туннели IKEv2 используются на маршрутизаторах, локальная идентичность, используемая на согласовании, определена **идентификационной локальной командой** под профилем IKEv2:

```
R1(config-ikev2-profile)#identity local ?  
address address  
dn Distinguished Name  
email Fully qualified email string  
fqdn Fully qualified domain name string  
key-id key-id opaque string - proprietary types of identification
```

По умолчанию маршрутизатор использует адрес в качестве локальной идентичности.

ID ISAKMP проверка на маршрутизаторах

Ожидаемый идентификатор равноправного узла также настроен вручную в том же профиле с **match identity удаленная** команда:

```
R1(config-ikev2-profile)#match identity remote ?  
address IP Address(es)  
any match any peer identity  
email Fully qualified email string [Max. 255 char(s)]  
fqdn Fully qualified domain name string [Max. 255 char(s)]  
key-id key-id opaque string
```

ID ISAKMP выбор на ASA

На ASA ISAKMP - идентичность выбран глобально с командой **crypto isakmp identity**:

```
ciscoasa/vpn(config)# crypto isakmp identity ?  
configure mode commands/options:  
address Use the IP address of the interface for the identity
```

```
auto Identity automatically determined by the connection type: IP
address for preshared key and Cert DN for Cert based connections
hostname Use the hostname of the router for the identity
key-id Use the specified key-id for the identity
```

По умолчанию командный режим установлен в автоматический, что означает, что ASA определяет согласование ISAKMP типом соединения:

- IP-адрес для предварительного общего ключа.
- Составное имя свидетельства для проверки подлинности сертификата.

Примечание: Идентификатор ошибки Cisco [CSCu148099](https://www.cisco.com/c/en-us/bugtools/bugtools/bugtools.html?bugid=CSCu148099) является запросом на расширение для способности настроить на основе на туннельную группу, а не в глобальной конфигурации.

ID ISAKMP проверка на ASA

Удаленная проверка ID сделана автоматически (определенный типом соединения) и не может быть изменена. Проверка может быть включена или отключена на основе на туннельную группу с **peer-id-validate** командой:

```
ciscoasa/vpn(config-tunnel-ipsec)# peer-id-validate ?
tunnel-group-ipsec mode commands/options:
cert If supported by certificate
nocheck Do not check
req Required
```

Проблемы совместимости

Различие в выборе/проверке ID вызывает две отдельные проблемы совместимости:

1. Когда аутентификация свидетельства используется на ASA, ASA пытается проверить идентификатор равноправного узла от альтернативного имени субъекта (SAN) на полученном сертификате. Если проверка идентификатора равноправного узла включена и если отладки платформы IKEv2 включены на ASA, эти отладки появляются:

```
IKEv2-PROTO-3: (172): Getting configured policies
IKEv2-PLAT-3: attempting to find tunnel group for ID: 172.16.1.1
IKEv2-PLAT-3: mapped to tunnel group 172.16.1.1 using phase 1 ID
IKEv2-PLAT-3: (172) tg_name set to: 172.16.1.1
IKEv2-PLAT-3: (172) tunn grp type set to: L2L
IKEv2-PLAT-3: Peer ID check started, received ID type: IPv4 address
IKEv2-PLAT-2: Peer ID check: failed to retrieve IP from SAN
IKEv2-PLAT-2: Peer ID check: failed to retrieve DNS name from SAN
IKEv2-PLAT-2: Peer ID check: failed to retrieve RFC822 name from SAN
IKEv2-PLAT-1: retrieving SAN for peer ID check
IKEv2-PLAT-1: Peer ID check failed
IKEv2-PROTO-1: (172): Failed to locate an item in the database
IKEv2-PROTO-1: (172):
IKEv2-PROTO-5: (172): SM Trace-> SA: I_SPI=833D2323FCB46093
R_SPI=F0B4D318DDDB783 (I) MsgID = 00000001 CurState: I_PROC_AUTH
Event: EV_AUTH_FAIL
IKEv2-PROTO-3: (172): Verify auth failed
IKEv2-PROTO-5: (172): SM Trace-> SA: I_SPI=833D2323FCB46093
R_SPI=F0B4D318DDDB783 (I) MsgID = 00000001 CurState: AUTH_DONE
Event: EV_FAIL
IKEv2-PROTO-3: (172): Auth exchange failed Для этой проблемы или IP-адрес сертификата
```

должен быть включен в сертификат узла, или проверка идентификатора равноправного узла должна быть отключена на ASA.

2. Точно так же по умолчанию ASA выбирает локальный ID автоматически так, когда аутентификация свидетельства используется, это передает Составное имя (DN) как идентичность. Если маршрутизатор настроен для получения адреса как удаленного ID, сбоев проверки идентификатора равноправного узла на маршрутизаторе. Если отладки IKEv2 включены на маршрутизаторе, эти отладки появляются:

```
Nov 30 22:49:14.464: IKEv2:(SESSION ID = 172,SA ID = 1):SM Trace-> SA:
I_SPI=E9E4B7FD0A336C97 R_SPI=F2CF438C0CCA281C (R) MsgID = 1 CurState:
R_WAIT_AUTH Event: EV_GET_POLICY_BY_PEERID
Nov 30 22:49:14.464: IKEv2:(SESSION ID = 172,SA ID = 1):Searching policy
based on peer's identity 'hostname=asa.cisco.com' of type 'DER ASN1 DN'
Nov 30 22:49:14.464: IKEv2:%Profile could not be found by peer certificate.
Nov 30 22:49:14.468: IKEv2:% IKEv2 profile not found
Nov 30 22:49:14.468: IKEv2:(SESSION ID = 172,SA ID = 1):: Failed to
```

locate an item in the database Для этой проблемы, или настроить маршрутизатор, чтобы проверить полное доменное имя (FQDN) или настроить ASA для использования адреса в качестве ID ISAKMP. **Примечание:** На маршрутизаторе карта сертификата, которая присоединена к профилю IKEv2, должна быть настроена для распознавания DN. См. [Сертификат](#) к разделу [Сопоставления Профиля ISAKMP Обмена ключами между сетями для Руководства по конфигурации IPSec VPN](#), Документа Cisco Выпуска 3S Cisco IOS XE для получения информации о том, как настроить это.

Размер подлинного информационного наполнения

Если сертификаты (а не предварительные общие ключи) используются для аутентификации, подлинные информационные наполнения значительно больше. Это обычно приводит к фрагментации, которая может тогда заставить аутентификацию отказывать, если фрагмент теряется или заглядывается путь. Если туннель не подходит из-за размера подлинного информационного наполнения, обычные причины:

1. Применение политик плана контроля на маршрутизаторе, который мог бы заблокировать пакеты.
2. Неправильное согласование максимального модуля перехода (MTU), которое может быть исправлено с крипто-ikev2 командой *размера mtu фрагментации*.

Выделение ресурсов в режиме мультиконтекста на ASA

С версии ASA 9.0 ASA поддерживает VPN в режиме мультиконтекста. Однако, когда вы настраиваете VPN в режиме мультиконтекста, убедиться выделить соответствующие ресурсы в системе, которая будет использовать VPN.

Для получения дополнительной информации обратитесь к [информации](#) [О](#) разделе [Управления ресурсами руководства по настройке интерфейса командной строки для Cisco ASA, 9.0](#).

Проверка списка отозванных сертификатов

Список отозванных сертификатов (CRL) является списком отозванных certificates, которые были выполнены и впоследствии отозваны данным CA., как который Certificates мог бы быть отозван по ряду причин, такие:

- Сбой или компромисс устройства, которое использует данный сертификат.
- Компромисс пары ключей используется certificate.
- Ошибки в выполненном certificate, такие как неправильная идентичность или потребность принять изменение имени.

Механизм, используемый для certificate аннулирования, зависит от CA., Отозванные certificates представлены в CRL их серийными номерами. Если сетевое устройство пытается проверить законность certificate, это загружает и просматривает текущий CRL для серийного номера представленного сертификата. Поэтому, если проверка CRL включена на любом узле, надлежащий URL CRL должен быть настроен также, таким образом, может быть проверена законность сертификатов ID.

Для получения дополнительной информации о CRL обратитесь к [Что Является разделом CRL Руководства по конфигурации Инфраструктуры открытых ключей, Выпуска 3S Cisco IOS XE.](#)

Проверка цепочки сертификатов

Если ASA настроен с сертификатом, который имеет Промежуточный CAs, и это однорангово, мог бы или не мог бы иметь того же Промежуточного звена CA, то ASA должен быть явно настроен для передачи завершенной цепочки сертификатов к маршрутизатору. Маршрутизатор делает это по умолчанию. Чтобы сделать это при определении точки доверия под криптокартой, добавляет цепочечное ключевое слово как показано здесь:

```
crypto map outside-map 1 set trustpoint ios-ca chain
```

Если это не будет сделано, то о туннеле только выполняют согласование, пока ASA является респондентом. Если это будет инициатор, то туннель откажет и PKI, и отладки IKEv2 на маршрутизаторе покажут это:

```
2328304: Jun 8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):  
Get peer's authentication method  
2328305: Jun 8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):  
Peer's authentication method is 'RSA'  
2328306: Jun 8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):  
SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1  
CurState: R_VERIFY_AUTH Event: EV_CHK_CERT_ENC  
2328307: Jun 8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):  
SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1  
CurState: R_VERIFY_AUTH Event: EV_VERIFY_X509_CERTS  
2328308: Jun 8 19:14:38.051 GMT: CRYPTO_PKI: (A16A8) Adding peer certificate  
2328309: Jun 8 19:14:38.055 GMT: CRYPTO_PKI: Added x509 peer certificate -(1359) bytes  
2328310: Jun 8 19:14:38.055 GMT: CRYPTO_PKI: ip-ext-val: IP extension validation  
not required  
2328311: Jun 8 19:14:38.055 GMT: CRYPTO_PKI: create new ca_req_context type  
PKI_VERIFY_CHAIN_CONTEXT,ident 4177  
2328312: Jun 8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8)validation path has 1 certs  
2328313: Jun 8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8) Check for identical certs  
2328314: Jun 8 19:14:38.055 GMT: CRYPTO_PKI : (A16A8) Validating non-trusted cert  
2328315: Jun 8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8) Create a list of suitable  
trustpoints  
2328316: Jun 8 19:14:38.055 GMT: CRYPTO_PKI: Unable to locate cert record by  
issuename  
2328317: Jun 8 19:14:38.055 GMT: CRYPTO_PKI: No trust point for cert issuer,
```

looking up cert chain

2328318: Jun 8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8) No suitable trustpoints found

2328319: Jun 8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):: Platform errors

2328320: Jun 8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1 CurState:

R_VERIFY_AUTH Event: EV_CERT_FAIL

2328321: Jun 8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):Verify cert failed

2328322: Jun 8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):

SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1 CurState:

R_VERIFY_AUTH Event: EV_AUTH_FAIL

2328323: Jun 8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68)

:Verification of peer's authentication data FAILED

Типовая конфигурация ASA

```
domain-name cisco.com
```

```
!
```

```
interface outside
```

```
nameif outside
```

```
security-level 0
```

```
ip address 172.16.1.2 255.255.255.0
```

```
!
```

```
interface CA
```

```
nameif CA
```

```
security-level 50
```

```
ip address 192.168.0.1 255.255.255.0
```

```
!
```

```
! acl which defines crypto domains, must be mirror images on both peers
```

```
!
```

```
access-list cryacl extended permit ip 192.168.0.0 255.255.255.0 172.16.2.0 255.255.255.0
```

```
pager lines 24
```

```
logging console debugging
```

```
mtu outside 1500
```

```
mtu CA 1500
```

```
mtu backbone 1500
```

```
route outside 172.16.2.0 255.255.255.0 172.16.1.1 1
```

```
route CA 192.168.254.254 255.255.255.255 192.168.0.254 1
```

```
crypto ipsec ikev2 ipsec-proposal AES256
```

```
protocol esp encryption aes-256
```

```
protocol esp integrity sha-1 md5
```

```
crypto ipsec ikev2 ipsec-proposal DES
```

```
protocol esp encryption des
```

```
protocol esp integrity sha-1 md5
```

```
crypto ipsec security-association pmtu-aging infinite
```

```
crypto map outside-map 1 match address cryacl
```

```
crypto map outside-map 1 set pfs
```

```
crypto map outside-map 1 set peer 172.16.1.1
```

```
crypto map outside-map 1 set ikev2 ipsec-proposal DES AES256
```

```
crypto map outside-map 1 set trustpoint ios-ca chain
```

```
crypto map outside-map interface outside
```

```
crypto ca trustpoint ios-ca
```

```
enrollment url http://192.168.254.254:80
```

```
fqdn asa.cisco.com
```

```
keypair ios-ca
```

```
crl configure
```

```
crypto ca certificate chain ios-ca
```

```
certificate ca 01
```

```
3082020f 30820178 a0030201 02020101 300d0609 2a864886 f70d0101 04050030
```

```
1b311930 17060355 04031310 696f732d 63612e63 6973636f 2e636f6d 301e170d
```

```
31333131 31353231 33353533 5a170d31 33313231 35323133 35353335a 301b3119
```

```
30170603 55040313 10696f73 2d63612e 63697363 6f2e636f 6d30819f 300d0609
```



```
2a864886 f70d0101 01050003 818d0030 81890281 81009ebb 48957c44 c940236f
alcdca758 aa930e8c 91390734 b8ef814d 0bf7aec9 7ec40379 7749d3c6 154f6a32
00738655 33b20207 037a9e15 3229fa72 478424fb 409f518d b13d328d e761be08
8023b4ff f410054b 4423156d 66c99788 69ab5956 966d5e1b 4dlc1120 a05ad08c
f036a134 3b2fc425 e4a2524f 36e0a129 2c8f6cee 971d0203 010001a3 63306130
0f060355 1d130101 ff040530 030101ff 300e0603 551d0f01 01ff0404 03020186
301f0603 551d2304 18301680 14082896 b9f4af20 75514321 d072f161 d09d2ec8
aa301d06 03551d0e 04160414 082896b9 f4af2075 514321d0 72f161d0 9d2ec8aa
300d0609 2a864886 f70d0101 04050003 81810087 a06d354a f7423e0e 64a7c5ec
6006fbde 914d7bfd f86ada50 b1a00d17 0bf06ec1 5423d514 fbeb0a76 986eb63f
f7fce99a 81c4b112 61fd69ce a2ce750e b1b3a6f9 84e92490 8f213613 451dd9a8
3fc3406a 854b20ed 27e4ddd8 62f6dea5 dd8b4396 1879b3e7 651cb9d1 3dd46b8b
32796963 9f6854f1 389f0060 aa0d1b8d f83e09
```

quit

certificate 08

```
3082028e 308201f7 a0030201 02020108 300d0609 2a864886 f70d0101 04050030
1b311930 17060355 04031310 696f732d 63612e63 6973636f 2e636f6d 301e170d
31333131 31383136 31383130 5a170d31 33313132 38313631 3831305a 301e311c
301a0609 2a864886 f70d0109 02160d61 73612e63 6973636f 2e636f6d 30819f30
0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c38ee5 75215237
2728cffd 3519cd15 ebcaab2c 48d63b92 7562d2fc f7db60bc ecb03b2c 4e4dff07
47ad5122 80899055 37f346d7 d10962e9 1e5edb06 8985ee7e 8a6da977 2460f82e
53679457 ed10372a 9ff2946e 449214e4 9be95cab 51d7681c 2db0382b 048fe807
1d1bb9b0 e4bd9de6 c99cafea c279e943 1e1f5d1b d1e6010c b7020301 0001a381
de3081db 30310603 551d2504 2a302806 082b0601 05050703 0106082b 06010505
07030506 082b0601 05050703 0606082b 06010505 07030730 3c060355 1d1f0435
30333031 a02fa02d 862b6874 74703a2f 2f313932 2e313638 2e323534 2e323534
2f696f73 2d636163 64702e69 6f732d63 612e6372 6c301806 03551d11 0411300f
820d6173 612e6369 73636f2e 636f6d30 0e060355 1d0f0101 ff040403 0205a030
1f060355 1d230418 30168014 082896b9 f4af2075 514321d0 72f161d0 9d2ec8aa
301d0603 551d0e04 1604145b 76de9ef0 d3255efe f4bc551b 69cd8398 d1596c30
0d06092a 864886f7 0d010104 05000381 81003fb0 ec7719cd 4f6162b2 90727db4
da5606f2 61441dc6 094fb3a6 defe62ef 5ff8f140 3bc3448c e0b42d26 07647607
fd7518cb 034139d3 e3648fd2 9d93b5e4 db3b828b 16d50dd5 3e18cdd6 74855de4
88a159d6 6ef51718 cf6cc4e4 53c2aca3 36442ff0 bb4b8493 22f0e632 a8b32b36
f287801f 8d47637f e4e9ee6a b4555094 c092
```

quit

!

! manually select the ISAKMP identity to use address on the ASA

crypto isakmp identity address

crypto ikev2 policy 1

encryption aes-256

integrity sha

group 14 5 2

prf sha

lifetime seconds 86400

crypto ikev2 policy 10

encryption aes-192

integrity sha256 sha

group 14 5 2

prf sha

lifetime seconds 86400

crypto ikev2 policy 30

encryption 3des

integrity sha

group 5 2

prf sha

lifetime seconds 86400

crypto ikev2 enable outside

!

! to allow pings from the CA interface that will bring up the tunnel during testing.

!

management-access CA

```

!
group-policy GroupPolicy2 internal
group-policy GroupPolicy2 attributes
vpn-idle-timeout 30
vpn-tunnel-protocol ikev1 ikev2
tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 general-attributes
default-group-policy GroupPolicy2
tunnel-group 172.16.1.1 ipsec-attributes
!
! disable peer-id validation
!
peer-id-validate nocheck
ikev2 remote-authentication certificate
ikev2 local-authentication certificate ios-ca
: end
! NTP configuration
ntp trusted-key 1
ntp server 192.168.254.254

```

Конфигурация примера отладки маршрутизатора

```

ip domain name cisco.com
!
crypto pki trustpoint tp_ikev2
enrollment url http://192.168.254.254:80
usage ike
fqdn R1.cisco.com
!
! necessary only in this example as no crl has been configured on the IOS CA.
On the ASA this is enabled by default. When using proper 3rd party
certificates this is not necessary.
!
revocation-check none
rsa-keypair ikev2_cert
eku request server-auth
!
crypto pki certificate chain tp_ikev2
certificate 0B
308202F4 3082025D A0030201 0202010B 300D0609 2A864886 F70D0101 05050030
1B311930 17060355 04031310 696F732D 63612E63 6973636F 2E636F6D 301E170D
31333131 32353233 35363537 5A170D31 33313230 35323335 3635375A 301D311B
30190609 2A864886 F70D0109 02160C52 312E6369 73636F2E 636F6D30 82012230
0D06092A 864886F7 0D010101 05000382 010F0030 82010A02 82010100 A1032A61
A3F14539 87816C22 8C66A170 3A9661EA 4AF6F063 3FC305B8 E525B84D AA74A9CE
666B1BF5 3C7DF025 31FEB161 CE49845F 3EC2DE7B D3FCC685 D6F80C8C 0AA12772
1B4AB15C 90C04446 068A0DBA 7BFA4E40 E978364F A2B07F7C 02C691A8 921A5481
A4AF07B4 BA0C9DBA D35F4566 6CB70553 DAF09A45 F2948C5A 1621E5D2 98508D49
A2EF61D3 AAF3A9DB 87F2D763 89AD0BBE 916A6CF8 1B59C426 7960013B 061AA0A5
F6870319 87A35ABA 8C1B5CF5 42976739 B8C936D3 24276E56 F59E3CFD 9B9B4A0D
2E5294AB C4470376 5D96915F 275CBC78 586D6755 F45C7592 62DCA916 CEC1A450
3FF090A9 15088CD2 13B90391 B0795263 071C7002 8CBF98F2 89788A0B 02030100
01A381C1 3081BE30 3C060355 1D1F0435 30333031 A02FA02D 862B6874 74703A2F
2F313932 2E313638 2E323534 2E323534 2F696F73 2D636163 64702E69 6F732D63
612E6372 6C303106 03551D25 042A3028 06082B06 01050507 03010608 2B060105
05070305 06082B06 01050507 03060608 2B060105 05070307 300B0603 551D0F04
04030205 A0301F06 03551D23 04183016 80140828 96B9F4AF 20755143 21D072F1
61D09D2E C8AA301D 0603551D 0E041604 14C63949 4CA10DBB 2BBB6F98 BAFF0EE2
B3716CEE 3B300D06 092A8648 86F70D01 01050500 03818100 3080FEF6 9160357B
6F28ED60 428BA6CE 203706F6 F91DA273 AF6E81D3 46539E13 B4C89A9A 19E1F0BC
A631A418 C30DFC8E 0585039D EB07D35D E719F5FE A4EE47B5 CED31B12 745C9EE8
5B6B0F17 67C3B965 C927B379 C674933F 84E7A1F7 851A6CF0 8775B1C5 3A033D90
75965DCA 86E4A842 E2C35AC0 6BFA8144 699B1582 C094BF35
quit

```

```

certificate ca 01
3082020F 30820178 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
1B311930 17060355 04031310 696F732D 63612E63 6973636F 2E636F6D 301E170D
31333131 31353231 33353533 5A170D31 33313231 35323133 3535335A 301B3119
30170603 55040313 10696F73 2D63612E 63697363 6F2E636F 6D30819F 300D0609
2A864886 F70D0101 01050003 818D0030 81890281 81009EBB 48957C44 C940236F
A1CDA758 AA930E8C 91390734 B8EF814D 0BF7AEC9 7EC40379 7749D3C6 154F6A32
00738655 33B20207 037A9E15 3229FA72 478424FB 409F518D B13D328D E761BE08
8023B4FF F410054B 4423156D 66C99788 69AB5956 966D5E1B 4D1C1120 A05AD08C
F036A134 3B2FC425 E4A2524F 36E0A129 2C8F6CEE 971D0203 010001A3 63306130
0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186
301F0603 551D2304 18301680 14082896 B9F4AF20 75514321 D072F161 D09D2EC8
AA301D06 03551D0E 04160414 082896B9 F4AF2075 514321D0 72F161D0 9D2EC8AA
300D0609 2A864886 F70D0101 04050003 81810087 A06D354A F7423E0E 64A7C5EC
6006FBDE 914D7BFD F86ADA50 B1A00D17 0BF06EC1 5423D514 FBEB0A76 986EB63F
F7FCE99A 81C4B112 61FD69CE A2CE750E B1B3A6F9 84E92490 8F213613 451DD9A8
3FC3406A 854B20ED 27E4DDD8 62F6DEA5 DD8B4396 1879B3E7 651CB9D1 3DD46B8B
32796963 9F6854F1 389F0060 AA0D1B8D F83E09
quit
!
crypto ikev2 proposal aes-cbc-256-proposal
encryption aes-cbc-256
integrity sha1
group 5 2 14
!
crypto ikev2 policy policy1
match address local 172.16.1.1
proposal aes-cbc-256-proposal
!
crypto ikev2 profile profile1
description IKEv2 profile
!
! router configured to use address as the remote identity. By default local
identity is address
!
match address local 172.16.1.1
match identity remote address 172.16.1.2 255.255.255.255
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint tp_ikev2
!
! disable http-url based cert lookup
!
no crypto ikev2 http-url cert
!
crypto ipsec transform-set ESP-AES-SHA esp-aes 256 esp-sha-hmac
mode tunnel
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
set peer 172.16.1.2
set transform-set ESP-AES-SHA
set pfs group2
set ikev2-profile profile1
match address 103
!
interface Loopback0
ip address 172.16.2.1 255.255.255.255
!
interface GigabitEthernet0/0
ip address 172.16.1.1 255.255.255.0
duplex auto
speed auto
crypto map SDM_CMAP_1
!

```

```

interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
ip route 192.168.0.0 255.255.255.0 172.16.1.2
ip route 192.168.254.254 255.255.255.255 192.168.1.254
!
! access list that defines crypto domains, must be mirror images on both peers.
!
access-list 103 permit ip 172.16.2.0 0.0.0.255 192.168.0.0 0.0.0.255
!
! ntp configuration
!
ntp trusted-key 1
ntp server 192.168.254.254
!
end

```

Типовой IOS CA конфигурация

```

ip domain name cisco.com
!
! CA server configuration
!
crypto pki server ios-ca
database archive pkcs12 password 7 02050D4808095E731F
issuer-name CN=ios-ca.cisco.com
grant auto
lifetime certificate 10
lifetime ca-certificate 30
cdp-url http://192.168.254.254/ios-cacdp.ios-ca.crl
eku server-auth ipsec-end-system ipsec-tunnel ipsec-user
!
! this trustpoint is generated automatically when the CA server is enabled.
!
crypto pki trustpoint ios-ca
revocation-check crl
rsa-keypair ios-ca
!
!
crypto pki certificate chain ios-ca
certificate ca 01
3082020F 30820178 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
1B311930 17060355 04031310 696F732D 63612E63 6973636F 2E636F6D 301E170D
31333131 31353231 33353533 5A170D31 33313231 35323133 3535335A 301B3119
30170603 55040313 10696F73 2D63612E 63697363 6F2E636F 6D30819F 300D0609
2A864886 F70D0101 01050003 818D0030 81890281 81009EBB 48957C44 C940236F
A1CDA758 AA930E8C 91390734 B8EF814D 0BF7AEC9 7EC40379 7749D3C6 154F6A32
00738655 33B20207 037A9E15 3229FA72 478424FB 409F518D B13D328D E761BE08
8023B4FF F410054B 4423156D 66C99788 69AB5956 966D5E1B 4D1C1120 A05AD08C
F036A134 3B2FC425 E4A2524F 36E0A129 2C8F6CEE 971D0203 010001A3 63306130
0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186
301F0603 551D2304 18301680 14082896 B9F4AF20 75514321 D072F161 D09D2EC8
AA301D06 03551D0E 04160414 082896B9 F4AF2075 514321D0 72F161D0 9D2EC8AA
300D0609 2A864886 F70D0101 04050003 81810087 A06D354A F7423E0E 64A7C5EC
6006FBDE 914D7BFD F86ADA50 B1A00D17 0BF06EC1 5423D514 FBEB0A76 986EB63F
F7FCE99A 81C4B112 61FD69CE A2CE750E B1B3A6F9 84E92490 8F213613 451DD9A8
3FC3406A 854B20ED 27E4DD88 62F6DEA5 DD8B4396 1879B3E7 651CB9D1 3DD46B8B
32796963 9F6854F1 389F0060 AA0D1B8D F83E09
quit
voice-card 0
!
!

```

```

interface Loopback0
ip address 192.168.254.254 255.255.255.255
!
interface GigabitEthernet0/0
ip address 192.168.0.254 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.254 255.255.255.0
duplex auto
speed auto
!
! http-server needs to be enabeld for SCEP
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.122.162.129
ip route 172.18.108.26 255.255.255.255 10.122.162.129
!
! ntp configuration
!
ntp trusted-key 1
ntp master 1
!
end

```

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Примечание: [Средство интерпретации выходных данных \(только зарегистрированные клиенты\)](#) поддерживает некоторые команды show. Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.

Эти команды работают и на ASA и на маршрутизаторы:

- **show crypto ikev2 sa** - Отображает состояние Сопоставления безопасности (SA) фазы 1.
- **show crypto ipsec sa**- Отображает состояние SA фазы 2.

Примечание: В этих выходных данных, в отличие от этого в IKEv1, групповое значение Diffie-Hellman (DH) Совершенной передающей тайны (PFS) отображается как 'безопасная пересылка (PFS) (Y/N): N, группа DH: ни один' во время первого согласования туннеля; после того, как повторно введение происходит, правильные значения появляются. Это не дефект даже при том, что поведение описано в идентификаторе ошибки Cisco [CSCug67056](#).

Различие между IKEv1 и IKEv2 - то, что в IKEv2 Дочерние SA созданы как часть самого обмена AUTH. DH Group, настроенная под криптокартой, используется только во время повторно введения. Таким образом вы видите 'безопасную пересылку (PFS) (Y/N): N, группа DH: ни один' до первого не повторно вводит. С IKEv1 вы видите другое поведение, потому что создание Child SA происходит во время Быстрого режима, и

сообщение CREATE_CHILD_SA имеет условие для переноса информационного наполнения Обмена ключами, которое задает параметры DH для получения нового общего секретного ключа.

Проверка фазы 1

Эта процедура проверяет действие фазы 1:

1. Введите команду `show crypto ikev2 sa` в маршрутизатор:

```
R1#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA

Tunnel-id Local          Remote          fvrf/ivrf      Status
1          172.16.1.1/500    172.16.1.2/500  none/none      READY
    Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:14, Auth sign: RSA,
Auth verify: RSA
    Life/Active Time: 86400/53 sec
IPv6 Crypto IKEv2 SA
```

2. Введите показ крипто-ikev2 `sacommand` в ASA:

```
ciscoasa/vpn(config)# show crypto ikev2 sa

IKEv2 SAs:

Session-id:138, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local          Remote          Status  Role
45926289 172.16.1.2/500    172.16.1.1/500  READY  INITIATOR
    Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:14, Auth sign: RSA,
Auth verify: RSA
    Life/Active Time: 86400/4 sec
Child sa: local selector 192.168.0.0/0 - 192.168.0.255/65535
          remote selector 172.16.2.0/0 - 172.16.2.255/65535
          ESP spi in/out: 0xa84caabb/0xf18dce57
```

Проверка фазы 2

Эта процедура описывает, как проверить, выполнили ли об индексе параметров безопасности (SPI) согласование правильно на двух узлах:

1. Введите `show crypto ipsec sa | я spi` команда на маршрутизаторе:

```
R1#show crypto ipsec sa | i spi
current outbound spi: 0xA84CAABB(2823596731)
spi: 0xF18DCE57(4052602455)
spi: 0xA84CAABB(2823596731)
```

2. Введите `show crypto ipsec sa | я spicommand` на ASA:

```
ciscoasa/vpn(config)# show crypto ipsec sa | i spi
current outbound spi: F18DCE57
current inbound spi : A84CAABB
spi: 0xA84CAABB (2823596731)
spi: 0xF18DCE57 (4052602455)
```

Эта процедура описывает, как подтвердить ли трафики через туннель:

1. Введите **show crypto ipsec sa | я pkts** на маршрутизаторе:

```
R1#show crypto ipsec sa | i pkts
#pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
```

2. Введите **show crypto ipsec sa | я pktscommand** на ASA:

```
ciscoasa/vpn(config)# show crypto ipsec sa | i pkts
#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
```

Устранение неполадок

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

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

Отладки на ASA

Внимание. : На ASA можно установить различные уровни отладки; по умолчанию уровень 1 используется. При изменении уровня отладки многословие отладок могло бы увеличиться. Сделайте это с осторожностью, особенно в производственных средах!

Отладки ASA для согласования туннеля:

- **debug crypto ikev2** протокол
- **debug crypto ikev2** платформа

Отладка ASA для проверки подлинности сертификата:

- **debug crypto ca**

Отладки на маршрутизаторе

Отладки маршрутизатора для согласования туннеля:

- **debug crypto ikev2**
- **debug crypto ikev2** ошибка
- **debug crypto ikev2** внутренний

Отладки маршрутизатора для проверки подлинности сертификата:

- отладьте проверку ркі крика
- отладьте транзакцию ркі крика
- отладьте сообщения ркі крика