

配置ASA和路由器之間的站點到站點IKEv2隧道

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[相關產品](#)

[設定](#)

[網路圖表](#)

[背景資訊](#)

[NTP](#)

[基於HTTP-URL的證書查詢](#)

[對等ID驗證](#)

[路由器上的ISAKMP ID選擇](#)

[路由器上的ISAKMP ID驗證](#)

[ASA上的ISAKMP ID選擇](#)

[ASA上的ISAKMP ID驗證](#)

[互通性問題](#)

[身份驗證負載大小](#)

[ASA上多情景模式下的資源分配](#)

[驗證證書吊銷清單](#)

[驗證憑證鏈結](#)

[ASA配置示例](#)

[路由器配置示例](#)

[Cisco IOS CA配置示例](#)

[驗證](#)

[第1階段驗證](#)

[第2階段驗證](#)

[疑難排解](#)

[ASA上的調試](#)

[路由器上的調試](#)

簡介

本文檔介紹如何在Cisco ASA和運行Cisco IOS®軟體的路由器之間設定站點到站點IKEv2隧道。

必要條件

需求

思科建議您瞭解以下主題：

- 網際網路金鑰交換版本2(IKEv2)
- 憑證與公開金鑰基礎架構(PKI)
- 網路時間協定(NTP)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本9.8.4的Cisco ASA 5506自適應安全裝置
- 執行Cisco IOS軟體版本15.3(3)M1的Cisco 2900系列整合式服務路由器(ISR)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

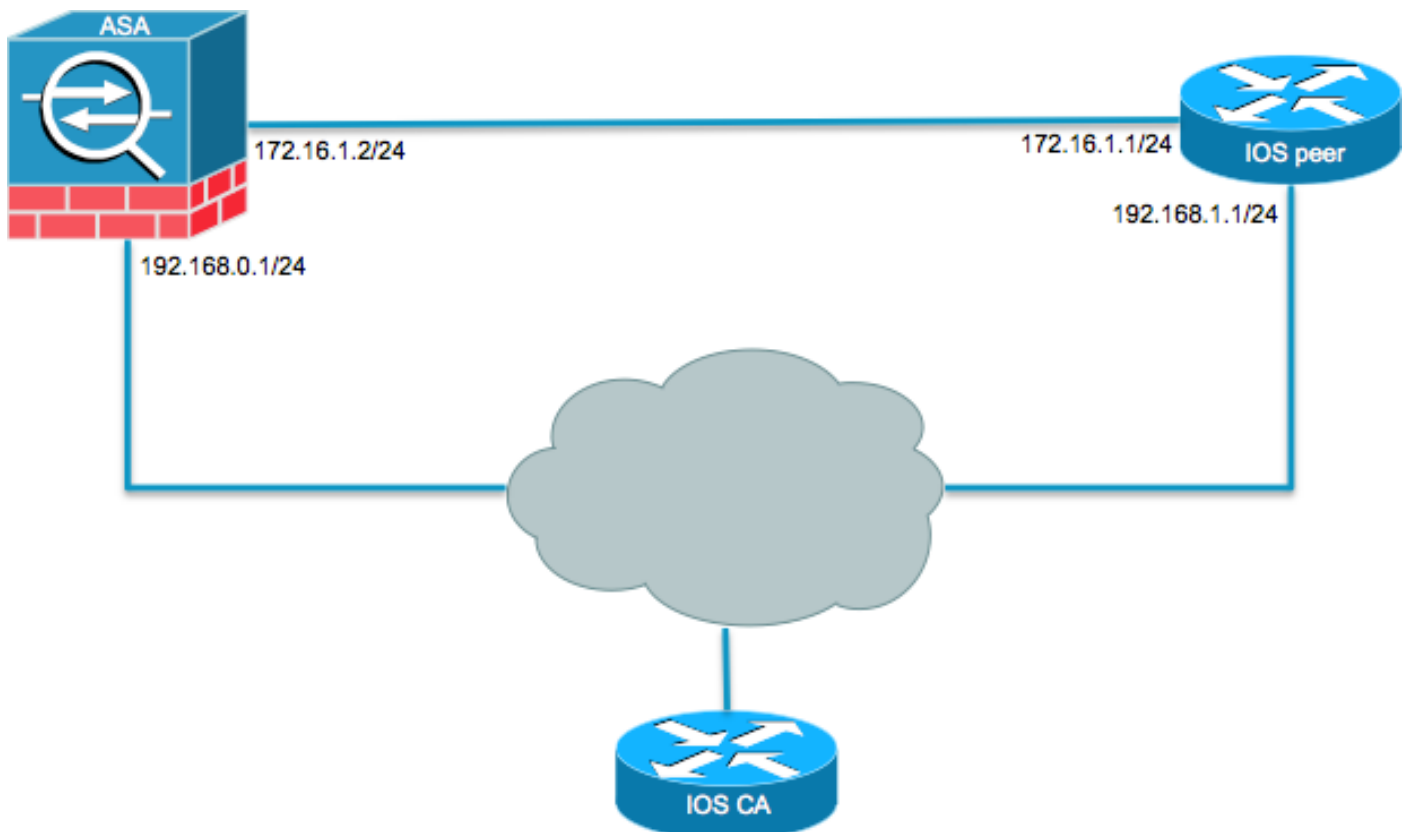
相關產品

本文件也適用於以下硬體和軟體版本：

- 運行軟體版本8.4(1)或更高版本的Cisco ASA
- 運行Cisco IOS軟體版本15.2(4)M或更高版本的Cisco ISR第2代(G2)
- 運行Cisco IOS-XE軟體版本15.2(4)S或更高版本的Cisco ASR 1000系列聚合服務路由器
- 運行軟體版本15.2(4)M或更高版本的Cisco Connected Grid路由器

設定

網路圖表




背景資訊

使用預共用金鑰在ASA和路由器之間配置IKEv2隧道非常簡單。但是，使用憑證驗證時，請記住某些警告。

NTP

證書身份驗證要求使用的所有裝置上的時鐘必須同步到公共源。雖然可以在每台裝置上手動設定時鐘，但這不太精確，而且可能很麻煩。同步所有裝置上的時鐘的最簡單方法是使用NTP。NTP同步一組分散式時間伺服器和客戶端之間的時間。在建立系統日誌以及發生其他特定時間事件時，此同步允許關聯事件。有關如何配置NTP的詳細資訊，請參閱[網路時間協定：最佳實踐白皮書](#)。

 提示：在使用Cisco IOS軟體證書頒發機構(CA)伺服器時，通常將同一裝置配置為NTP伺服器。在本例中，CA伺服器也用作NTP伺服器。

基於HTTP-URL的證書查詢

基於HTTP URL的證書查詢可避免傳輸大型證書時產生的分段。預設情況下，此功能在Cisco IOS軟體裝置上啟用，因此Cisco IOS軟體使用cert req type 12。

如果在ASA上使用了沒有Cisco錯誤ID [CSCu148246](#)修復程式的軟體版本，則不會在ASA上協商基於HTTP-URL的查詢，並且Cisco IOS軟體會導致授權嘗試失敗。

在ASA上，如果已啟用IKEv2協定調試，則會顯示以下消息：

```
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
```

為了避免此問題，請使用 `no crypto ikev2 http-url cert` 命令，以便在路由器上與ASA對等時禁用此功能。

對等ID驗證

在IKE AUTH階段的Internet安全關聯和金鑰管理協定(ISAKMP)協商期間，對等體必須互相標識自己。但是，路由器和ASA選擇本地身份的方式有所不同。

路由器上的ISAKMP ID選擇

當路由器上使用IKEv2隧道時，協商中使用的本地身份由 `identity local IKEv2`配置檔案下的命令：

```
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

預設情況下，路由器使用地址作為本地標識。

路由器上的ISAKMP ID驗證

預期的對等ID也可在與的同一配置檔案中手動配置 `match identity remote` 指令：

```
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
```

ASA上的ISAKMP ID選擇

在ASA上，使用 `crypto isakmp identity` 指令：

```
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
```

預設情況下，命令模式設定為自動，這表示ASA根據連線型別確定ISAKMP協商：

- 預共用金鑰的IP地址。
- 證書身份驗證的證書可分辨名稱。



註：思科錯誤ID [CSCu14809](#)是增強請求，用於根據隧道組而不是全域性配置進行配置。

ASA上的ISAKMP ID驗證

遠端ID驗證會自動完成（由連線型別確定），無法更改。可以使用 `peer-id-validate` 指令：

```
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

互通性問題

ID選擇/驗證的差異會導致兩個單獨的互操作性問題：

- 在ASA上使用cert auth時，ASA會嘗試從接收的證書上的使用者替代名稱(SAN)驗證對等ID。如果啟用了對等體ID驗證，且如果在ASA上啟用了IKEv2平台調試，則會顯示以下調試：

```
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
```

對於此問題，需要將證書的IP地址包括在對等證書中，或者需要在ASA上禁用對等ID驗證。

- 同樣，預設情況下，ASA會自動選擇本地ID，因此，使用cert auth時，它會傳送可分辨名稱(DN)作為身份。如果路由器配置為接收作為遠端ID的地址，則路由器上的對等ID驗證將失敗。如果在路由器上啟用了IKEv2調試，則會顯示以下調試：

```
Nov 30 22:49:14.464: IKEv2:(SESSION ID = 172,SA ID = 1):SM Trace-> SA:
I_SPI=E9E4B7FDOA336C97 R_SPI=F2CF438COCCA281C (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

對於此問題，請配置路由器以驗證完全限定域名(FQDN)，或配置ASA以使用地址作為ISAKMP ID。



註：在路由器上，必須配置連線到IKEv2配置檔案的證書對映才能識別DN。有關如何設定此配置的資訊，請參閱Internet Key Exchange for IPsec VPN配置指南Cisco IOS XE版本3S Cisco文檔的[證書到ISAKMP配置檔案對映](#)部分。

身份驗證負載大小

如果使用證書（而不是預共用金鑰）進行身份驗證，則身份驗證負載會大得多。這通常會導致分段，如果路徑中遺失或捨棄了片段，分段會導致驗證失敗。如果通道因身份驗證負載大小而無法啟動，通常的原因包括：

- Control Plane Policing 能封鎖封包的路由器上。
- 最大轉換單元(MTU)協商不正確，可以使用 `crypto ikev2 fragmentation mtu size` 指令。

ASA上多情景模式下的資源分配

自ASA 9.0版起，ASA支援多情景模式下的VPN。但是，當在多情景模式下配置VPN時，請確保在已配置VPN的系統中分配適當的資源。

有關詳細資訊，請參閱[CLI手冊1: Cisco ASA系列常規操作CLI配置指南9.8](#)的[有關資源管理](#)的資訊部分。

驗證證書吊銷清單

憑證撤銷清單(CRL)是已核發且隨後由給定CA撤銷的撤銷憑證的清單。證書可以因多種原因被吊銷，例如：

- 使用給定證書的裝置發生故障或受到危害。
- 證書使用的金鑰對受損。
- 頒發的證書中存在錯誤，例如身份不正確或需要適應名稱更改。

用於證書撤銷的機制取決於CA。撤銷的證書在CRL中用其序列號表示。如果網路裝置嘗試驗證證書的有效性，它就會下載並掃描當前CRL以獲取提供的證書的序列號。因此，如果在任一對等體上啟用CRL驗證，則還必須配置適當的CRL URL，以便驗證ID證書的有效性。

有關CRL的詳細資訊，請參閱[Cisco IOS XE版本3S公共金鑰基礎設施配置指南](#)[什麼是CRL](#)部分。

驗證憑證鏈結

如果ASA配置的證書具有中間CA，並且其對等體不具有相同的中間CA，則需要顯式配置ASA以將完整的證書鏈傳送到路由器。預設情況下，路由器會執行此操作。為此，當您在加密對映下定義信

任點時，請新增鍵關鍵字，如下所示：

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

如果不這樣做，則只在ASA是響應方的情況下，才會協商隧道。如果它是發起方，則隧道協商失敗，並且路由器上的PKI和IKEv2調試顯示以下內容：

```
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
```

ASA配置示例

```
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 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
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
```

路由器配置示例

```
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
  rsakeypair 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 BAF0EE2
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

```

Cisco IOS CA配置示例

```

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 27E4DDD8 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 enabled 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
```

驗證

使用本節內容，確認您的組態是否正常運作。

以下命令適用於ASA和路由器：

- `show crypto ikev2 sa` — 顯示階段1安全關聯(SA)的狀態。
- `show crypto ipsec sa` — 顯示階段2 SA的狀態。



註：與IKEv1不同，在此輸出中，在第一次通道交涉中，完全轉送保密(PFS)Diffie-hellman(DH)組值顯示為「PFS(Y/N):N，DH組：無」；重新生成金鑰後，將顯示正確的值。這不是錯誤，而是預期行為。

IKEv1和IKEv2之間的區別在於，在IKEv2中，子SA是作為身份驗證交換本身的一部分而建立的。在加密對映下配置的DH組僅在重新生成金鑰期間使用。因此，在第一次重新生成金鑰之前，您將看到「PFS(Y/N): N，DH組：none」。使用IKEv1時，您會看到不同的行為，因為子SA建立發生在快速模式期間，而CREATE_CHILD_SA消息具有攜帶金鑰交換有效載荷的設定，該有效載荷指定DH引數以派生新的共用金鑰。

第1階段驗證

此過程驗證階段1活動：

1. 輸入 `show crypto ikev2 sa` 命令時，路由器上會顯示：

```
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. 輸入 `show crypto ikev2 sa` 命令：

```
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
```

第2階段驗證

此程式說明如何驗證已在兩個對等點上正確交涉安全引數索引(SPI):

1. 輸入 `show crypto ipsec sa | i spi` 命令時，路由器上會顯示：

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

2. 輸入 `show crypto ipsec sa | i spi` 命令：

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

```
current outbound spi: F18DCE57
current inbound spi : A84CAABB
spi: 0xA84CAABB (2823596731)
spi: 0xF18DCE57 (4052602455)
```

以下程式說明如何確認流量是否通過通道：

1. 輸入 `show crypto ipsec sa | i pkts` 命令時，路由器上會顯示：

```
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. 輸入 `show crypto ipsec sa | i pkts` 命令：

```
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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。



注意：使用[前](#)，請先參閱有關[Debug命令](#)的重要資訊 `debug` 指令。

ASA上的調試



注意：在ASA上，您可以設定各種調試級別；預設情況下，使用級別1。如果更改調試級別，調試的詳細程度可能會增加。請謹慎執行此操作，尤其是在生產環境中！

用於隧道協商的ASA調試包括：

- `debug crypto ikev2 protocol`
- `debug crypto ikev2 platform`

用於證書身份驗證的ASA調試為：

- `debug crypto ca`

路由器上的調試

用於通道交涉的路由器偵錯如下：

- `debug crypto ikev2`
- `debug crypto ikev2 error`
- `debug crypto ikev2 internal`

用於證書身份驗證的路由器調試包括：

- `debug cry pki validation`
- `debug cry pki transaction`
- `debug cry pki messages`

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。