

# Configurazione del tunnel IKEv2 da sito a sito tra ASA e router

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Configurazione](#)

[Esempio di rete](#)

[Premesse](#)

[NTP](#)

[Ricerca certificati basata su URL HTTP](#)

[Convalida ID peer](#)

[Selezione ID ISAKMP su router](#)

[Convalida dell'ID ISAKMP sui router](#)

[Selezione dell'ID ISAKMP sulle appliance ASA](#)

[Convalida dell'ID ISAKMP sull'appliance ASA](#)

[Problemi di interoperabilità](#)

[Dimensioni del payload di autenticazione](#)

[Allocazione delle risorse in modalità multi-contesto sull'appliance ASA](#)

[Convalida dell'elenco di revoche di certificati](#)

[Convalida della catena di certificati](#)

[Esempio di configurazione dell'ASA](#)

[Esempio di configurazione del router](#)

[Esempio di configurazione di una CA di Cisco IOS](#)

[Verifica](#)

[Verifica fase 1](#)

[Verifica fase 2](#)

[Risoluzione dei problemi](#)

[Debug dell'appliance ASA](#)

[Debug sul router](#)

---

## Introduzione

In questo documento viene descritto come configurare un tunnel IKEv2 tra un'appliance Cisco ASA e un router con software Cisco IOS®.

## Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- IKEv2 (Internet Key Exchange versione 2)
- Certificati e infrastruttura a chiave pubblica (PKI)
- Protocollo NTP (Network Time Protocol)

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Appliance Cisco ASA 5506 Adaptive Security con software versione 9.8.4
- Cisco serie 2900 Integrated Services Router (ISR) con software Cisco IOS versione 15.3(3)M1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

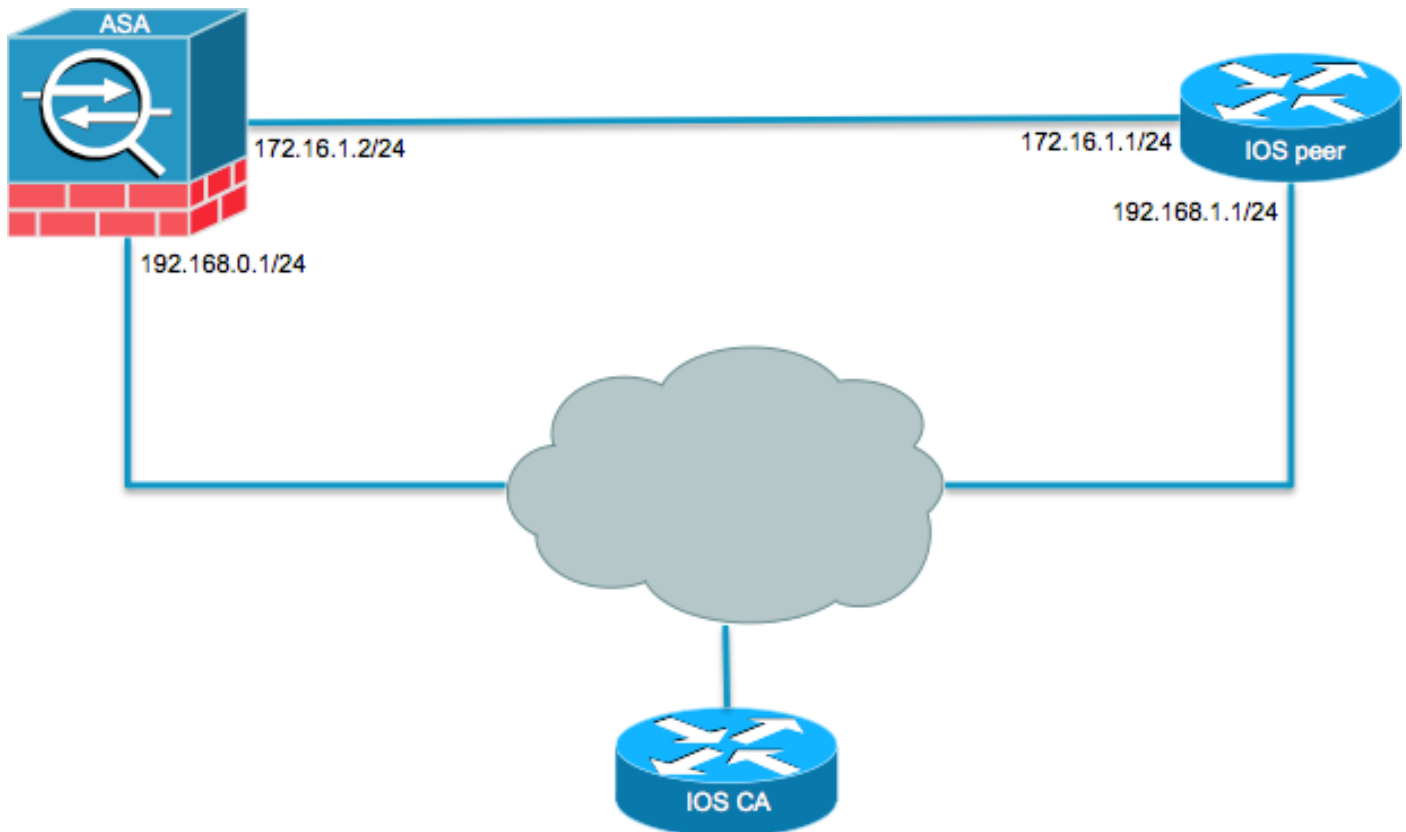
## Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- Cisco ASA con software versione 8.4(1) o successive
- Cisco ISR generazione 2 (G2) con software Cisco IOS versione 15.2(4)M o successive
- Cisco ASR serie 1000 Aggregation Services Router con software Cisco IOS-XE versione 15.2(4)S o successive
- Router Cisco Connected Grid con software versione 15.2(4)M o successive

## Configurazione

### Esempio di rete




## Premesse

La configurazione di un tunnel IKEv2 tra un'ASA e un router con l'uso di chiavi già condivise è semplice. Tuttavia, quando si utilizza l'autenticazione basata su certificati, è necessario tenere presenti alcuni avvertimenti.

## NTP

L'autenticazione dei certificati richiede che gli orologi di tutti i dispositivi utilizzati siano sincronizzati con un'origine comune. Sebbene l'orologio possa essere impostato manualmente su ciascun dispositivo, questo non è molto preciso e può essere ingombrante. Il metodo più semplice per sincronizzare gli orologi su tutti i dispositivi è utilizzare NTP. NTP sincronizza l'ora tra una serie di server e client di riferimento orario distribuiti. Questa sincronizzazione consente di correlare gli eventi quando vengono creati i registri di sistema e quando si verificano altri eventi specifici dell'ora. Per ulteriori informazioni su come configurare NTP, fare riferimento al [white paper Network Time Protocol: Best Practices](#).

---

 S suggerimento: quando si usa un server CA (Certification Authority) del software Cisco IOS, è pratica comune configurare lo stesso dispositivo del server NTP. In questo esempio, il server CA funge anche da server NTP.

---

## Ricerca certificati basata su URL HTTP

La ricerca dei certificati basata sull'URL HTTP evita la frammentazione che si verifica quando vengono trasferiti certificati di grandi dimensioni. Questa funzione è abilitata sui dispositivi

software Cisco IOS per impostazione predefinita, quindi il tipo di richiesta di certificato 12 viene utilizzato dal software Cisco IOS.

Se sull'appliance ASA vengono usate versioni software senza la correzione per l'ID bug Cisco [CSCu148246](#), la ricerca basata su URL HTTP non viene negoziata sull'appliance e il software Cisco IOS impedisce il completamento del tentativo di autorizzazione.

Sull'appliance ASA, se i debug del protocollo IKEv2 sono abilitati, vengono visualizzati questi messaggi:

```
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
```

Per evitare questo problema, utilizzare il `no crypto ikev2 http-url cert` per disabilitare questa funzione sul router quando è collegato a un'ASA.

## Convalida ID peer

Durante le negoziazioni ISAKMP (Internet Security Association) e ISAKMP (Key Management Protocol) della fase AUTH IKE, i peer devono identificarsi tra loro. Tuttavia, vi è una differenza nel modo in cui i router e le appliance ASA selezionano la propria identità locale.

### Selezione ID ISAKMP su router

Quando si utilizzano i tunnel IKEv2 sui router, l'identità locale utilizzata nella negoziazione viene determinata dal `identity local` nel profilo 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
```

Per impostazione predefinita, il router utilizza l'indirizzo come identità locale.

### Convalida dell'ID ISAKMP sui router

Anche l'ID peer previsto è configurato manualmente nello stesso profilo con `match identity remote` comando:

```
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
```

## Selezione dell'ID ISAKMP sulle appliance ASA

Sulle appliance ASA, l'identità ISAKMP viene selezionata globalmente con il `crypto isakmp identity` comando:

```
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
```

Per impostazione predefinita, la modalità comando è impostata su `auto`, il che significa che l'ASA determina la negoziazione ISAKMP per tipo di connessione:

- Indirizzo IP per la chiave già condivisa.
- Nome distinto del certificato per l'autenticazione del certificato.



Nota: l'ID bug Cisco [CSCu148099](#) è una richiesta di miglioramento per la capacità di configurare il sistema per singolo gruppo di tunnel anziché nella configurazione globale.

---

## Convalida dell'ID ISAKMP sull'appliance ASA

La convalida dell'ID remoto viene eseguita automaticamente (in base al tipo di connessione) e non può essere modificata. La convalida può essere abilitata o disabilitata per singoli gruppi di tunnel con `peer-id-validate` comando:

```
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
```

## Problemi di interoperabilità

La differenza nella selezione/convalida degli ID causa due problemi distinti di interoperabilità:

- Quando si usa l'autenticazione cert sull'appliance ASA, l'ASA cerca di convalidare l'ID peer dalla SAN (Subject Alternative Name) sul certificato ricevuto. Se la convalida dell'ID peer è abilitata e i debug della piattaforma IKEv2 sono abilitati sull'appliance ASA, vengono visualizzati i seguenti debug:

```
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
```

Per questo problema, è necessario includere l'indirizzo IP del certificato nel certificato peer oppure disabilitare la convalida dell'ID peer sull'appliance ASA.

- Analogamente, per impostazione predefinita l'ASA seleziona automaticamente l'ID locale, quindi, quando si utilizza la funzione cert auth, invia il nome distinto (DN) come identità. Se il router è configurato per ricevere l'indirizzo come ID remoto, la convalida dell'ID peer non riuscirà sul router. Se sul router sono abilitati i debug IKEv2, vengono visualizzati i seguenti debug:

```
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
```

Per questo problema, configurare il router per convalidare il nome di dominio completo (FQDN) o configurare l'ASA in modo che usi l'indirizzo come ID ISAKMP.



Nota: sul router, per riconoscere il DN, è necessario configurare una mappa dei certificati collegata al profilo IKEv2. Per informazioni su come configurare questa funzionalità, consultare la sezione [Certificate to ISAKMP Profile Mapping](#) (Certificato per il [mapping](#) del [profilo ISAKMP](#)) della guida alla configurazione di Internet Key Exchange for IPsec VPN (Internet Key Exchange for IPsec VPN) e il documento Cisco Cisco IOS XE release 3S Cisco.

## Dimensioni del payload di autenticazione

Se per l'autenticazione vengono utilizzati i certificati (anziché le chiavi già condivise), i payload di autenticazione sono notevolmente più grandi. Ciò in genere determina una frammentazione che può compromettere l'autenticazione in caso di perdita o eliminazione di un frammento nel percorso. Se il tunnel non arriva a causa delle dimensioni del payload di autenticazione, le cause comuni sono:

- Control Plane Policing sul router che può bloccare i pacchetti.
- Negoziazione MTU (Maximum Transition Unit) non corretta, che può essere corretta con il comando `crypto ikev2 fragmentation mtu size`

## Allocazione delle risorse in modalità multi-contesto sull'appliance ASA

A partire dalla versione 9.0, l'ASA supporta una VPN in modalità multi-contesto. Tuttavia, quando si configura la VPN in modalità multi-contesto, assicurarsi di allocare le risorse appropriate nel sistema in cui è configurata la VPN.

Per ulteriori informazioni, fare riferimento alla sezione [Information About Resource Management](#) del [CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.8](#).

## Convalida dell'elenco di revoche di certificati

Un elenco di revoche di certificati (CRL, Certificate Revocation List) è un elenco di certificati revocati che sono stati rilasciati e successivamente revocati da una determinata CA. I certificati possono essere revocati per una serie di motivi, ad esempio:

- Errore o compromissione di un dispositivo che utilizza un determinato certificato.
- Compromissione della coppia di chiavi utilizzata da un certificato.
- Errori all'interno di un certificato rilasciato, ad esempio un'identità non corretta o la necessità di inserire un cambio di nome.

Il meccanismo utilizzato per la revoca dei certificati dipende dalla CA. I certificati revocati sono rappresentati nel CRL dai relativi numeri di serie. Se un dispositivo di rete tenta di verificare la

validità di un certificato, scarica e analizza il CRL corrente per individuare il numero di serie del certificato presentato. Pertanto, se la convalida CRL è abilitata su uno dei peer, è necessario configurare anche un URL CRL corretto in modo da poter verificare la validità dei certificati ID.

Per ulteriori informazioni sui CRL, fare riferimento alla sezione [Definizione di CRL](#) della [guida alla configurazione dell'infrastruttura a chiave pubblica, Cisco IOS XE release 3S](#).

## Convalida della catena di certificati

Se l'ASA è configurata con un certificato con CA intermedia e il relativo peer non ha la stessa CA intermedia, l'ASA deve essere configurata in modo esplicito per inviare la catena di certificati completa al router. Il router esegue questa operazione per impostazione predefinita. A tale scopo, quando si definisce il trust point nella mappa crittografica, aggiungere la parola chiave chain come mostrato di seguito:

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

In caso contrario, il tunnel viene negoziato solo se l'ASA è il responder. Se si tratta di un iniziatore, la negoziazione del tunnel non riesce e i debug PKI e IKEv2 sul router mostrano questo:

```
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
```

## Esempio di configurazione dell'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 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

```

## Esempio di configurazione del router

```

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 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

```

## Esempio di configurazione di una CA di Cisco IOS

```

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
 rsakeypair 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 35353335A 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

```

## Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Questi comandi funzionano sia sulle ASA che sui router:

- `show crypto ikev2 sa` - Visualizza lo stato della fase 1 dell'associazione di sicurezza (SA, Security Association).
- `show crypto ipsec sa` - Visualizza lo stato dell'associazione di sicurezza della fase 2.



Nota: in questo output, a differenza di IKEv1, il valore del gruppo Diffie-Hellman (DH) PFS (Perfect Forwarding Secrecy) viene visualizzato come 'PFS (Y/N): N, gruppo DH: nessuno' durante la prima negoziazione del tunnel. Dopo la reimpostazione della chiave, vengono visualizzati i valori corretti. Non si tratta di un bug, ma del comportamento previsto.

La differenza tra IKEv1 e IKEv2 consiste nel fatto che in IKEv2 le associazioni di protezione figlio vengono create come parte dello scambio AUTH. Il gruppo DH configurato nella mappa crittografica viene utilizzato solo durante una reimpostazione della chiave. Pertanto, verrà visualizzato 'PFS (S/N): N, gruppo DH: nessuno' fino alla prima reimpostazione della chiave. Con IKEv1, si verifica un comportamento diverso perché la creazione di associazioni di protezione figlio avviene durante la modalità rapida e il messaggio CREATE\_CHILD\_SA dispone del provisioning per trasportare il payload di scambio chiave, che specifica i parametri DH per derivare il nuovo segreto condiviso.

## Verifica fase 1

Questa procedura verifica l'attività della fase 1:

### 1. Immettere il `show crypto ikev2 sa` sul router:

```
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. Immettere il `show crypto ikev2 sa` sull'appliance 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

## Verifica fase 2

In questa procedura viene descritto come verificare se l'indice dei parametri di sicurezza (SPI, Security Parameter Index) è stato negoziato correttamente sui due peer:

### 1. Immettere il `show crypto ipsec sa | i spi` sul router:

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

### 2. Immettere il `show crypto ipsec sa | i spi` sull'appliance ASA:

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

In questa procedura viene descritto come confermare se il traffico attraversa il tunnel:

### 1. Immettere il `show crypto ipsec sa | i pkts` sul router:

```
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. Immettere il `show crypto ipsec sa | i pkts` sull'appliance 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
```



# Risoluzione dei problemi


Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

---

 Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare `debug` comandi.

---

## Debug dell'appliance ASA

 **Attenzione:** sull'appliance ASA, è possibile impostare vari livelli di debug; per impostazione predefinita, viene usato il livello 1. Se si modifica il livello di debug, il livello di dettaglio dei debug può aumentare. Procedere con cautela, in particolare negli ambienti di produzione!

---

Di seguito sono riportati i debug ASA per la negoziazione del tunnel.

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

Il debug ASA per l'autenticazione del certificato è:

- `debug crypto ca`

## Debug sul router

Di seguito sono riportati i debug del router per la negoziazione del tunnel:

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

I debug del router per l'autenticazione del certificato sono:

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

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).