

Debug IOS IPSec e IKE - Risoluzione dei problemi in modalità principale IKEv1

Sommario

[Introduzione](#)

[Problema principale](#)

[Scenario](#)

[Debug usati](#)

[Configurazione router IOS](#)

[Configurazione crittografia](#)

[Altro lato](#)

[Debug](#)

[IOS Responder Side](#)

[Messaggio modalità principale 1 \(MM1\)](#)

[Messaggio modalità principale 2 \(MM2\) - Invio della risposta](#)

[Messaggio modalità principale 3 \(MM3\)](#)

[Messaggio modalità principale 4 \(MM4\)](#)

[Messaggio modalità principale 5 \(MM5\) - L'iniziatore invia la propria identità](#)

[Messaggio modalità principale 6 \(MM6\) - Il risponditore invia la propria identità. Completamento della fase 1.](#)

[Messaggio 1 modalità rapida \(QM1\)](#)

[Messaggio 2 modalità rapida \(QM2\)](#)

[QM3 \(Quick Mode Message 3\) - La seconda fase deve essere completata e l'interfaccia del tunnel deve essere attiva](#)

[IOS Router - Iniziatore](#)

[Messaggio modalità principale 1 \(MM1\) - Contatto iniziale](#)

[Messaggio modalità principale 2 \(MM2\) - Risposta al contatto iniziale](#)

[Messaggio 3 in modalità principale \(MM3\) - Rilevamento NAT e scambio Diffie-Hellman](#)

[Messaggio 4 in modalità principale \(MM4\) - Rilevamento NAT e scambio Diffie-Hellman](#)

[Messaggio modalità principale 5 \(MM5\) - Invia identità](#)

[Messaggio in modalità principale 6 \(MM6\) - Identità peer remota, fase 1 stabilita](#)

[Messaggio 1 in modalità rapida \(QM1\) - Inizio fase 2 per peer](#)

[Messaggio 2 modalità rapida \(QM2\)](#)

[Messaggio 3 in modalità rapida \(QM3\) - Fase 2](#)

[Verifica tunnel](#)

[Informazioni correlate](#)

Introduzione

Questo documento offre informazioni per comprendere i debug sul software Cisco IOS® quando si usano la modalità principale e la chiave precondivisa (PSK).

In questo documento viene spiegato anche come convertire alcune righe di debug in una configurazione.

Questi argomenti non vengono trattati:

- Traffico in transito dopo la creazione del tunnel
- Concetti di base di IPsec o IKE (Internet Key Exchange)

Problema principale

I debug IKE e IPsec tendono a essere criptici. Spesso i bug vengono usati dal Cisco Technical Assistance Center (TAC) per capire dove è stato riscontrato un problema con la **definizione** del tunnel VPN IPsec.

Scenario

La modalità principale viene in genere utilizzata tra tunnel da LAN a LAN o, in caso di accesso remoto (ezvpn), quando i certificati vengono utilizzati per l'autenticazione.

I debug vengono eseguiti da un dispositivo Cisco IOS con versione software 15.2(1)T.

In questo documento vengono descritti due scenari principali:

- Iniziatore IOS
- IOS responder side

In questo documento viene stabilito un tunnel basato su VTI tra due siti, basato su IPv6.

Note:

per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

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

Debug usati

- debug crypto isakmp
- debug crypto ipsec
- debug crypto kmi

Configurazione router IOS

Configurazione crittografia

```
crypto isakmp policy 10
authentication pre-share

crypto isakmp key cisco address ipv6 ::/0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac
mode transport

crypto ipsec profile PRO
set transform-set TRA

interface Tunnel23
ip address 192.168.23.2 255.255.255.0
ipv6 address FE80::23:2 link-local
tunnel source Ethernet0/0
tunnel mode ipsec ipv6
tunnel destination 2001: DB8::3
tunnel protection ipsec profile PRO
```

Altro lato

```
crypto isakmp policy 10
authentication pre-share

crypto isakmp key cisco address ipv6 ::/0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac
mode transport

crypto ipsec profile PRO
set transform-set TRA

interface Tunnel23
ip address 192.168.23.3 255.255.255.0
ipv6 address FE80::23:3 link-local
tunnel source Ethernet0/0
tunnel mode ipsec ipv6
tunnel destination 2001: DB8::2
tunnel protection ipsec profile PRO
```

Debug

IOS Responder Side

Messaggio modalità principale 1 (MM1)

La proposta iniziale di IKE comprende:

- Crittografia
- Hashing

- Gruppo Diffie-Hellman (DH)
- Durata

```
*Sep 21 08:33:43.377: ISAKMP (0) : received packet from 2001: DB8::2 dport 500
sport 500 Global (N) NEW SA
*Sep 21 08:33:43.377: ISAKMP: Created a peer struct for 2001: DB8::2, peer port
500
*Sep 21 08:33:43.377: ISAKMP: New peer created peer = 0x8E45588
peer_handle = 0x8000000A
*Sep 21 08:33:43.377: ISAKMP: Locking peer struct 0x8E45588, refcount 1 for
crypto_isakmp_process_block
*Sep 21 08:33:43.377: ISAKMP: local port 500, remote port 500
*Sep 21 08:33:43.377: ISAKMP: (0):insert sa successfully sa = 6D12A00
*Sep 21 08:33:43.377: ISAKMP: (0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.377: ISAKMP: (0): Old State = IKE_READY New State = IKE_R_MM1
*Sep 21 08:33:43.377: ISAKMP: (0): processing SA payload. message ID = 0
*Sep 21 08:33:43.377: ISAKMP: (0):found peer pre-shared key matching 2001:
DB8::2
*Sep 21 08:33:43.377: ISAKMP: (0): local preshared key found
*Sep 21 08:33:43.377: ISAKMP: Scanning profiles for xauth ...
*Sep 21 08:33:43.377: ISAKMP: (0):Checking ISAKMP transform 1 against priority
10 policy
*Sep 21 08:33:43.377: ISAKMP:          encryption DES-CBC
*Sep 21 08:33:43.377: ISAKMP:          hash SHA
*Sep 21 08:33:43.377: ISAKMP:          default group 1
*Sep 21 08:33:43.377: ISAKMP:          auth pre-share
*Sep 21 08:33:43.377: ISAKMP:          life type in seconds
*Sep 21 08:33:43.377: ISAKMP:          life duration (VPI) of 0x0 0x1 0x51 0x80
*Sep 21 08:33:43.377: ISAKMP: (0):atts are acceptable. Next payload is 0
*Sep 21 08:33:43.377: ISAKMP: (0):Acceptable atts:actual life: 0
*Sep 21 08:33:43.377: ISAKMP: (0):Acceptable atts:life: 0
*Sep 21 08:33:43.377: ISAKMP: (0):Fill atts in sa vpi_length:4
*Sep 21 08:33:43.377: ISAKMP: (0):Fill atts in sa life_in_seconds:86400
*Sep 21 08:33:43.377: ISAKMP: (0):Returning Actual lifetime: 86400
*Sep 21 08:33:43.377: ISAKMP: (0):: Started lifetime timer: 86400.

*Sep 21 08:33:43.377: ISAKMP: (0):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.377: ISAKMP: (0): Old State = IKE_R_MM1 New State = IKE_R_MM1
```

Configurazione correlata:

```
crypto isakmp policy 10
authentication pre-share
```

Messaggio modalità principale 2 (MM2) - Invio della risposta

```
*Sep 21 08:33:43.377: ISAKMP: (0): sending packet to 2001: DB8::2 my_port 500
peer_port 500 (R) MM_SA_SETUP
*Sep 21 08:33:43.377: ISAKMP: (0): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.377: ISAKMP: (0):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.377: ISAKMP: (0): Old State = IKE_R_MM1 New State = IKE_R_MM2
```

Messaggio modalità principale 3 (MM3)

Include:

- Individuazione Network Address Translation (NAT)
- scambio DH parte 1

```
*Sep 21 08:33:43.381: ISAKMP (0): received packet from 2001:DB8::2 dport 500
sport 500 Global (R) MM_SA_SETUP
*Sep 21 08:33:43.381: ISAKMP: (0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.381: ISAKMP: (0): Old State = IKE_R_MM2 New State = IKE_R_MM3
*Sep 21 08:33:43.381: ISAKMP: (0): processing KE payload. message ID = 0
*Sep 21 08:33:43.393: ISAKMP: (0): processing NONCE payload. message ID = 0
*Sep 21 08:33:43.393: ISAKMP: (0):found peer pre-shared key matching 2001:
DB8::2
*Sep 21 08:33:43.393: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.393: ISAKMP: (1011): vendor ID is DPD
*Sep 21 08:33:43.393: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.393: ISAKMP: (1011): speaking to another IOS box!
*Sep 21 08:33:43.393: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.393: ISAKMP: (1011): vendor ID seems Unity/DPD but major 0
mismatch
*Sep 21 08:33:43.393: ISAKMP: (1011): vendor ID is XAUTH
*Sep 21 08:33:43.393: ISAKMP: (1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.393: ISAKMP: (1011): Old State = IKE_R_MM3 New State =
IKE_R_MM3
```

Messaggio modalità principale 4 (MM4)

Include:

- Payload rilevamento NAT
- Continuazione dello scambio di DH

```
*Sep 21 08:33:43.405: ISAKMP: (1011): sending packet to 2001: DB8::2 my_port
500 peer_port 500 (R) MM_KEY_EXCH
*Sep 21 08:33:43.405: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.405: ISAKMP: (1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.405: ISAKMP: (1011): Old State = IKE_R_MM3 New State =
IKE_R_MM4
```

Messaggio modalità principale 5 (MM5) - L'iniziatore invia la propria identità

Include:

- Informazioni sull'identità locale
- Chiave

```
*Sep 21 08:33:43.425: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) MM_KEY_EXCH
*Sep 21 08:33:43.425: ISAKMP: (1011):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.425: ISAKMP: (1011): Old State = IKE_R_MM4 New State =
IKE_R_MM5
*Sep 21 08:33:43.425: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.425: ISAKMP (1011): ID payload
next-payload : 8
```

```

type          : 5
address       : 2001: DB8::2
protocol      : 17
port          : 500
length        : 24
*Sep 21 08:33:43.425: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.425: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.425: ISAKMP: (1011): processing NOTIFY INITIAL_CONTACT
protocol 1 spi 0, message ID = 0, sa = 0x6D12A00
*Sep 21 08:33:43.425: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.425: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::2
*Sep 21 08:33:43.425: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.425: ISAKMP: (1011): Process initial contact, bring down
existing phase 1 and 2 SA's with local 2001: DB8::3 remote 2001: DB8::2
remote port 500
*Sep 21 08:33:43.425: ISAKMP: Trying to insert a peer 2001: DB8::3/2001:
DB8::2/500/, and inserted successfully 8E45588.
*Sep 21 08:33:43.425: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.425: ISAKMP: (1011): Old State = IKE_R_MM5 New State =
IKE_R_MM5

```

Messaggio modalità principale 6 (MM6) - Il risponditore invia la propria identità. Completamento della fase 1.

Include:

- Identità remota inviata dal peer
- Decisione finale sul gruppo di tunnel da scegliere

```

*Sep 21 08:33:43.425: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*Sep 21 08:33:43.425: ISAKMP: (1011): SA is doing pre-shared key authentication
using id type ID_IPV6_ADDR
*Sep 21 08:33:43.425: ISAKMP (1011): ID payload
next-payload : 8
type          : 5
address       : 2001: DB8::3
protocol      : 17
port          : 500
length        : 24
*Sep 21 08:33:43.425: ISAKMP: (1011):Total payload length: 24
*Sep 21 08:33:43.425: ISAKMP: (1011): sending packet to 2001: DB8::2 my_port
500 peer_port 500 (R) MM_KEY_EXCH
*Sep 21 08:33:43.425: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.425: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.425: ISAKMP: (1011): Old State = IKE_R_MM5 New State =
IKE_P1_COMPLETE

```

Configurazione correlata:

```
crypto isakmp identity ...
```

Messaggio 1 modalità rapida (QM1)

```
*Sep 21 08:33:43.433: ISAKMP (1011): received packet from 2001: DB8::2 dport
```

```

500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: set new node 1371333358 to QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: (1011): processing HASH payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing SA payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):Checking IPsec proposal 1
*Sep 21 08:33:43.433: ISAKMP: transform 1, ESP_AES
*Sep 21 08:33:43.433: ISAKMP: attributes in transform:
*Sep 21 08:33:43.433: ISAKMP: encaps is 1 (Tunnel)
*Sep 21 08:33:43.433: ISAKMP: SA life type in seconds
*Sep 21 08:33:43.433: ISAKMP: SA life duration (basic) of 3600
*Sep 21 08:33:43.433: ISAKMP: SA life type in kilobytes
*Sep 21 08:33:43.433: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Sep 21 08:33:43.433: ISAKMP: authenticator is HMAC-SHA
*Sep 21 08:33:43.433: ISAKMP: key length is 128
*Sep 21 08:33:43.433: ISAKMP: (1011):atts are acceptable.
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 2001: DB8::3:0, remote= 2001: DB8::2:0,
local_proxy= ::/0/256/0,
remote_proxy= ::/0/256/0,
protocol= ESP, transform= NONE (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Sep 21 08:33:43.433: ISAKMP: (1011): processing NONCE payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):QM Responder gets spi
*Sep 21 08:33:43.433: ISAKMP: (1011):Node 1371333358, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.433: ISAKMP: (1011): Old State = IKE_QM_READY New State =
IKE_QM_SPI_STARVE

```

Configurazione pertinente:

```
tunnel mode ipsec ipv6
```

Messaggio 2 modalità rapida (QM2)

Include:

- L'estremità remota invia i parametri
- Viene scelta la durata più breve tra le due proposte per la fase 2

```

*Sep 21 08:33:43.433: ISAKMP: (1011): sending packet to 2001: DB8::2 my_port
500 peer_port 500 (R) QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.433: ISAKMP: (1011):Node 1371333358, Input =
IKE_MSG_INTERNAL, IKE_GOT_SPI
*Sep 21 08:33:43.433: ISAKMP: (1011): Old State = IKE_QM_SPI_STARVE New
State = IKE_QM_R_QM2
*Sep 21 08:33:43.437: IPSEC(key_engine): got a queue event with 1 KMI message(s)
R3(config-if)#
*Sep 21 08:33:43.437: IPSEC(crypto_ipsec_create_ipsec_sas): Map found
Tunnel23-head-0

```

```
*Sep 21 08:33:43.437: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting
with the same proxies and peer 2001: DB8::2
*Sep 21 08:33:43.437: IPSEC(create_sa): sa created,
(sa) sa_dest= 2001: DB8::3, sa_proto= 50,
sa_spi= 0x221A7153(572158291),
sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 305
sa_lifetime(k/sec)= (4608000/3532)
*Sep 21 08:33:43.437: IPSEC(create_sa): sa created,
(sa) sa_dest= 2001: DB8::2, sa_proto= 50,
sa_spi= 0x45F16A9A(1173449370),
sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 306
sa_lifetime(k/sec)= (4608000/3532)
```

Configurazione pertinente:

```
crypto ipsec transform-set TRA esp-aes esp-sha-hmac
mode transport
crypto ipsec profile PRO
set transform-set TRA
interface tunnel23
tunnel mode ipsec ipv6
tunnel protection ipsec profile PRO
```

QM3 (Quick Mode Message 3) - La seconda fase deve essere completata e l'interfaccia del tunnel deve essere attiva

```
*Sep 21 08:33:43.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel23,
changed state to up
*Sep 21 08:33:43.437: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.437: ISAKMP: (1011): deleting node 1371333358 error FALSE
reason "QM done (await)"
*Sep 21 08:33:43.437: ISAKMP: (1011):Node 1371333358, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.437: ISAKMP: (1011): Old State = IKE_QM_R_QM2 New State =
IKE_QM_PHASE2_COMPLETE
*Sep 21 08:33:43.437: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*Sep 21 08:33:43.437: IPSEC(key_engine_enable_outbound): rec'd enable notify
from ISAKMP
```

IOS Router - Iniziatore

Messaggio modalità principale 1 (MM1) - Contatto iniziale

Include:

- ID fornitore (VID)
- Capacità
- Proposte fase 1
- Associazione di sicurezza IKE
- IPsec crea già un modello per le associazioni di protezione

```
*Sep 21 08:33:43.245: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
*Sep 21 08:33:43.245: IPSEC(sa ident sadb root initialize created IPv6 ACL %s)
```



```

: Tunnel23-head-0-65537-Tunnel23-head-0-ACL-6-IPSECV6-ACL
*Sep 21 08:33:43.245: IPSEC(recalculate_mtu) : reset sadb_root 79E82A8 mtu to
1500
*Sep 21 08:33:43.245: IPSEC(adjust_mtu) : adjusting ident ip mtu from 1460 to
1500,
(identity) local= 2001: DB8::2:0, remote= 2001: DB8::3:0,
local_proxy= ::/0/256/0,
remote_proxy= ::/0/256/0
*Sep 21 08:33:43.245: IPSEC(adjust_mtu): adjusting path mtu from 1460 to 1500,
(identity) local= 2001: DB8::2:0, remote= 2001: DB8::3:0,
local_proxy= ::/0/256/0,
remote_proxy= ::/0/256/0
*Sep 21 08:33:43.245: IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 2001: DB8::2:500, remote= 2001: DB8::3:500,
local_proxy= ::/0/256/0,
remote_proxy= ::/0/256/0,
protocol= ESP, transform= esp-aes esp-sha-hmac (Tunnel),
lifedur= 3600s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Sep 21 08:33:43.245: ISAKMP: (0): SA request profile is (NULL)
*Sep 21 08:33:43.245: ISAKMP: Created a peer struct for 2001: DB8::3, peer port
500
*Sep 21 08:33:43.245: ISAKMP: New peer created peer = 0x9344BE8 peer_handle =
0x80000008
*Sep 21 08:33:43.245: ISAKMP: Locking peer struct 0x9344BE8, refcount 1 for
isakmp_initiator
*Sep 21 08:33:43.245: ISAKMP: local port 500, remote port 500
*Sep 21 08:33:43.245: ISAKMP: set new node 0 to QM_IDLE
*Sep 21 08:33:43.245: ISAKMP: (0):insert sa successfully sa = 944C840
*Sep 21 08:33:43.245: ISAKMP: (0):Can not start Aggressive mode, trying Main
mode.
*Sep 21 08:33:43.245: ISAKMP: (0):found peer pre-shared key matching 2001:
DB8::3
*Sep 21 08:33:43.245: ISAKMP: (0):Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_MM
*Sep 21 08:33:43.245: ISAKMP: (0): Old State = IKE_READY New State = IKE_I_MM1
*Sep 21 08:33:43.245: ISAKMP: (0): beginning Main Mode exchange
*Sep 21 08:33:43.245: ISAKMP: (0): sending packet to 2001: DB8::3 my_port 500
peer_port 500 (I) MM_NO_STATE
*Sep 21 08:33:43.245: ISAKMP: (0): Sending an IKE IPv6 Packet.

```

Configurazione pertinente:

```

crypto isakmp policy 10
authentication pre-share

```

Messaggio modalità principale 2 (MM2) - Risposta al contatto iniziale

Include:

- Il peer sceglie i criteri ISAKMP (Internet Security Association and Key Management Protocol) da utilizzare
- SA IKE

```

*Sep 21 08:33:43.249: ISAKMP (0): received packet from 2001: DB8::3 dport 500
sport 500 Global (I) MM_NO_STATE
*Sep 21 08:33:43.249: ISAKMP: (0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.249: ISAKMP: (0): Old State = IKE_I_MM1 New State = IKE_I_MM2
*Sep 21 08:33:43.249: ISAKMP: (0): processing SA payload. message ID = 0

```

```

*Sep 21 08:33:43.249: ISAKMP: (0):found peer pre-shared key matching 2001:
DB8::3
*Sep 21 08:33:43.249: ISAKMP: (0): local preshared key found
*Sep 21 08:33:43.249: ISAKMP : Scanning profiles for xauth ...
*Sep 21 08:33:43.249: ISAKMP: (0):Checking ISAKMP transform 1 against priority
10 policy
*Sep 21 08:33:43.249: ISAKMP:      encryption DES-CBC
*Sep 21 08:33:43.249: ISAKMP:      hash SHA
*Sep 21 08:33:43.249: ISAKMP:      default group 1
*Sep 21 08:33:43.249: ISAKMP:      auth pre-share
*Sep 21 08:33:43.249: ISAKMP:      life type in seconds
*Sep 21 08:33:43.249: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Sep 21 08:33:43.249: ISAKMP: (0):atts are acceptable. Next payload is 0
*Sep 21 08:33:43.249: ISAKMP: (0):Acceptable atts:actual life: 0
*Sep 21 08:33:43.249: ISAKMP: (0):Acceptable atts:life: 0
*Sep 21 08:33:43.249: ISAKMP: (0):Fill atts in sa vpi_length:4
*Sep 21 08:33:43.249: ISAKMP: (0):Fill atts in sa life_in_seconds:86400
*Sep 21 08:33:43.249: ISAKMP: (0):Returning Actual lifetime: 86400
*Sep 21 08:33:43.249: ISAKMP: (0):: Started lifetime timer: 86400.

*Sep 21 08:33:43.249: ISAKMP: (0):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.249: ISAKMP: (0): Old State = IKE_I_MM2  New State =
IKE_I_MM2

```

Messaggio 3 in modalità principale (MM3) - Rilevamento NAT e scambio Diffie-Hellman

Include:

- Payload e hash di individuazione NAT
- Avvio scambio DH
- Supporto Dead Peer Detection (DPD)

```

*Sep 21 08:33:43.249: ISAKMP: (0): sending packet to 2001: DB8::3 my_port 500
peer_port 500 (I) MM_SA_SETUP
*Sep 21 08:33:43.249: ISAKMP: (0): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.249: ISAKMP: (0):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.249: ISAKMP: (0): Old State = IKE_I_MM2  New State = IKE_I_MM3

```

Messaggio 4 in modalità principale (MM4) - Rilevamento NAT e scambio Diffie-Hellman

Include:

- Payload di individuazione NAT
- Avvio scambio DH
- VID aggiuntivi (DPD, supporto Unity)
- Conoscenza di un altro dispositivo IOS

```

*Sep 21 08:33:43.273: ISAKMP (0): received packet from 2001: DB8::3 dport 500
sport 500 Global (I) MM_SA_SETUP
*Sep 21 08:33:43.273: ISAKMP: (0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.273: ISAKMP: (0): Old State = IKE_I_MM3  New State = IKE_I_MM4

*Sep 21 08:33:43.273: ISAKMP: (0): processing KE payload. message ID = 0
*Sep 21 08:33:43.281: ISAKMP: (0): processing NONCE payload. message ID = 0

```

```
*Sep 21 08:33:43.281: ISAKMP: (0):found peer pre-shared key matching 2001:
DB8::3
*Sep 21 08:33:43.281: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.281: ISAKMP: (1011): vendor ID is Unity
*Sep 21 08:33:43.281: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.281: ISAKMP: (1011): vendor ID is DPD
*Sep 21 08:33:43.281: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.281: ISAKMP: (1011): speaking to another IOS box!
*Sep 21 08:33:43.281: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.281: ISAKMP: (1011): Old State = IKE_I_MM4 New State =
IKE_I_MM4
```

Messaggio modalità principale 5 (MM5) - Invia identità

Include:

- Identità peer remota (ID)

```
*Sep 21 08:33:43.293: ISAKMP: (1011): Send initial contact
*Sep 21 08:33:43.293: ISAKMP: (1011): SA is doing pre-shared key authentication
using id type ID_IPV6_ADDR
*Sep 21 08:33:43.293: ISAKMP (1011): ID payload
    next-payload : 8
    type          : 5
    address       : 2001: DB8::2
    protocol      : 17
    port          : 500
    length        : 24
*Sep 21 08:33:43.293: ISAKMP: (1011):Total payload length: 24
*Sep 21 08:33:43.293: ISAKMP: (1011): sending packet to 2001: DB8::3 my_port
500 peer_port 500 (I) MM_KEY_EXCH
*Sep 21 08:33:43.293: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.293: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.293: ISAKMP: (1011): Old State = IKE_I_MM4 New State =
IKE_I_MM5
```

Configurazione pertinente:

```
crypto isakmp identity ...
```

Messaggio in modalità principale 6 (MM6) - Identità peer remota, fase 1 stabilita

Include:

- Data/ora inizio reimpostazione chiavi
- Identità remota (in questo caso un indirizzo)
- Decisione di atterrare su un profilo

```
*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP (1011): ID payload
    next-payload : 8
    type          : 5
```

```

address      : 2001: DB8::3
protocol     : 17
port        : 500
length      : 24
*Sep 21 08:33:43.297: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::3
*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:
DB8::3/500/, and inserted successfully 9344BE8.
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5 New State =
IKE_I_MM6

*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6 New State =
IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6 New State =
IKE_P1_COMPLETE

```

Configurazione pertinente:

```
crypto isakmp identity ...
```

Messaggio 1 in modalità rapida (QM1) - Inizio fase 2 per peer

Include:

- ID proxy remoti e locali
- Set di trasformazioni

```

*Sep 21 08:33:43.301: ISAKMP: (1011):beginning Quick Mode exchange, M-ID of
1371333358*Sep 21 08:33:43.301: ISAKMP: (1011):QM Initiator gets spi
*Sep 21 08:33:43.301: ISAKMP: (1011): sending packet to 2001: DB8::3 my_port
500 peer_port 500 (I) QM_IDLE
*Sep 21 08:33:43.301: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.301: ISAKMP: (1011):Node 1371333358, Input =
IKE_MSG_INTERNAL, IKE_INIT_QM
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_QM_READY New State =
IKE_QM_I_QM1
*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MSG_INTERNAL,
IKE_PHASE1_COMPLETE
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

```

Configurazione pertinente:

```
crypto ipsec transform-set TRA esp-aes esp-sha-hmac
mode transport
```

```
crypto ipsec profile PRO
set transform-set TRA
```

Messaggio 2 modalità rapida (QM2)

Include:

- Conferma delle identità proxy
- Tipo di tunnel
- Impostazioni PFS (Perfect Forwarding Secrecy)

```
*Sep 21 08:33:43.305: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) QM_IDLE
*Sep 21 08:33:43.305: ISAKMP: (1011): processing HASH payload. message ID =
1371333358
*Sep 21 08:33:43.305: ISAKMP: (1011): processing SA payload. message ID =
1371333358
*Sep 21 08:33:43.305: ISAKMP: (1011):Checking IPsec proposal 1
*Sep 21 08:33:43.305: ISAKMP: transform 1, ESP_AES
*Sep 21 08:33:43.305: ISAKMP:   attributes in transform:
*Sep 21 08:33:43.305: ISAKMP:     encaps is 1 (Tunnel)
*Sep 21 08:33:43.305: ISAKMP:     SA life type in seconds
*Sep 21 08:33:43.305: ISAKMP:     SA life duration (basic) of 3600
*Sep 21 08:33:43.305: ISAKMP:     SA life type in kilobytes
*Sep 21 08:33:43.305: ISAKMP:     SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Sep 21 08:33:43.305: ISAKMP:     authenticator is HMAC-SHA
*Sep 21 08:33:43.305: ISAKMP:     key length is 128
*Sep 21 08:33:43.305: ISAKMP: (1011):atts are acceptable.
*Sep 21 08:33:43.305: IPSEC(validate_proposal_request): proposal part #1
*Sep 21 08:33:43.305: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 2001: DB8::2:0, remote= 2001: DB8::3:0,
  local_proxy= ::/0/256/0,
  remote_proxy= ::/0/256/0,
  protocol= ESP, transform= NONE (Tunnel),
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Sep 21 08:33:43.305: ISAKMP: (1011): processing NONCE payload. message ID =
1371333358
*Sep 21 08:33:43.305: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.305: ISAKMP: (1011): processing ID payload. message ID =
1371333358
```

Configurazione pertinente:

```
crypto ipsec transform-set TRA esp-aes esp-sha-hmac
mode transport
```

```
crypto ipsec profile PRO
set transform-set TRA
```

```
interface tunnel23
tunnel mode ipsec ipv6
tunnel protection ipsec profile PRO
```

Messaggio 3 in modalità rapida (QM3) - Fase 2

Include:

- Impostazione degli SPI (Security Policy Index) per il passaggio del traffico

```

*Sep 21 08:33:43.305: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.305: ISAKMP: (1011): deleting node 1371333358 error FALSE
reason "No Error"
*Sep 21 08:33:43.305: ISAKMP: (1011):Node 1371333358, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.305: ISAKMP: (1011): Old State = IKE_QM_I_QM1 New State =
IKE_QM_PHASE2_COMPLETE
*Sep 21 08:33:43.305: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*Sep 21 08:33:43.305: IPSEC(crypto_ipsec_create_ipsec_sas): Map found
Tunnel23-head-0
*Sep 21 08:33:43.305: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting
with the same proxies and peer 2001: DB8::3
*Sep 21 08:33:43.305: IPSEC(create_sa): sa created,
(sa) sa_dest= 2001: DB8::2, sa_proto= 50,
sa_spi= 0x45F16A9A(1173449370),
sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 305
sa_lifetime(k/sec)= (4608000/3439)
*Sep 21 08:33:43.305: IPSEC(create_sa): sa created,
(sa) sa_dest= 2001: DB8::3, sa_proto= 50,
sa_spi= 0x221A7153(572158291),
sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 306
sa_lifetime(k/sec)= (4608000/3439)
R2(config-if)#
*Sep 21 08:33:43.309: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel23, changed state to up

```

Verifica tunnel

```
sh crypto ipsec sa
```

```
interface: Tunnel23
```

```
  Crypto map tag: Tunnel23-head-0, local addr 2001: DB8::2
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (::/0/0/0)
```

```
remote ident (addr/mask/prot/port): (::/0/0/0)
```

```
current_peer 2001: DB8::3 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
  #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: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 2001: DB8::2,
```

```
remote crypto endpt.: 2001: DB8::3
```

```
path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb Ethernet0/0
```

```
current outbound spi: 0x221A7153(572158291)
```

```
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```

```
  spi: 0x45F16A9A(1173449370)
```

```
  transform: esp-aes esp-sha-hmac ,
```

```
  in use settings ={Tunnel, }
```

```
  conn id: 305, flow_id: SW:305, sibling_flags 80000041, crypto map:
```

```
Tunnel23-head-0
```

```
  sa timing: remaining key lifetime (k/sec): (4183789/3408)
```

```
  IV size: 16 bytes
```

```
  replay detection support: Y
```

```
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x221A7153(572158291)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 306, flow_id: SW:306, sibling_flags 80000041, crypto map:
Tunnel23-head-0
  sa timing: remaining key lifetime (k/sec): (4183790/3408)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE
```

```
R2(config-if)#do ping fe80::23:3
Output Interface: tunnel23
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::23:3, timeout is 2 seconds:
Packet sent with a source address of FE80::23:2%Tunnel23
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/20 ms
R2(config-if)#do sh crypto ipsec sa | i caps|ident
  local ident (addr/mask/prot/port): (::/0/0/0)
  remote ident (addr/mask/prot/port): (::/0/0/0)
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
```

Il tunnel è attivo e sta attraversando il traffico.

Informazioni correlate

- [Articolo di Wikipedia su IPsec](#) ; lo standard e i riferimenti contengono molte informazioni utili.
- [Nota tecnica sulla risoluzione dei problemi relativi ai debug ASA IPsec e IKE \(modalità aggressiva IKEv1\)](#)
- [Nota tecnica sulla risoluzione dei problemi relativi ai debug ASA IPsec e IKE \(modalità principale IKEv1\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)