Informazioni sui comandi di debug e loro utilizzo per la risoluzione dei problemi di IPsec

Sommario

Introduzione

In questo documento vengono descritti i comandi di debug comuni utilizzati per risolvere i problemi relativi a IPsec sul software Cisco IOS® e su PIX/ASA.

Prerequisiti

Requisiti

in questo documento si presume che IPsec sia stato configurato. Per ulteriori informazioni, fare riferimento a Negoziazione IPSec/protocolli IKE.

Componenti usati

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

- Software Cisco IOS®
  - Set funzionalità IPSec.
  - 56i—Indica una singola Data Encryption Standard (DES) funzionalità (sul software Cisco IOS® versione 11.2 e successive).
  - k2 - Indica la funzionalità DES tripla (sul software Cisco IOS® versione 12.0 e successive). Triple DES è disponibile su Cisco serie 2600 e versioni successive.
- PIX—V5.0 e versioni successive, che richiede una singola o tripla chiave di licenza DES per l'attivazione.

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.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Per informazioni sulle soluzioni più comuni ai problemi VPN IPsec, fare riferimento a L2L e VPN ad accesso remoto più comuni.

Contiene un elenco di controllo delle procedure comuni che è possibile provare prima di iniziare a risolvere i problemi di una connessione e chiamare il supporto tecnico Cisco.

Debug del software Cisco IOS®

Negli argomenti di questa sezione vengono descritti i comandi di debug del software Cisco IOS®. Per ulteriori informazioni, fare riferimento a Negoziazione IPSec/protocolli IKE.

show crypto isakmp sa

Con questo comando viene visualizzataInternet Security Association Management Protocol (ISAKMP) Security Associations (SAs)la relazione predefinita tra peer.

```
dst          src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

show crypto ipsec sa

Con questo comando vengono visualizzate le associazioni di protezione IPSec create tra peer. Il tunnel crittografato viene generato tra la versione 10.1.0.1 e la 10.1.0.2 per il traffico tra le reti 10.1.0.0 e 10.1.1.0.

È possibile visualizzare le due associazioni di protezione Encapsulating Security Payload (ESP) create in entrata e in uscita. L'intestazione AH (Authentication Header) non viene utilizzata in quanto non sono presenti associazioni di protezione AH.

In questo output viene mostrato un esempio di**show crypto ipsec sa**comando.

<#root>

```
  interface: FastEthernet0
    Crypto map tag: test, local addr.
```

10.1.0.1

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

10.1.0.0/255.255.255.0/0/0

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

10.1.1.0/255.255.255.0/0/0

)
current_peer:

10.1.0.2

PERMIT, flags={origin_is_acl,}

#pkts encaps: 7767918, #pkts encrypt: 7767918, #pkts digest 7767918
#pkts decaps: 7760382, #pkts decrypt: 7760382, #pkts verify 7760382

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0, #send errors 1, #recv errors 0

local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2

path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound

esp

sas:
spi: 0x136A010F(325714191)
transform:

esp-3des esp-md5-hmac

,
in use settings ={

Tunnel

, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: test
sa timing:

remaining key lifetime (k/sec): (4608000/52)

IV size: 8 bytes
replay detection support: Y
inbound

ah

sas:
inbound pcp sas:
inbound pcp sas:
outbound

esp

sas:
spi: 0x3D3(979)
transform:

esp-3des esp-md5-hmac

```
 ,
    in use settings ={
```

Tunnel

```
, }
    slot: 0, conn id: 3443, flow_id: 1444, crypto map: test
    sa timing:
```

remaining key lifetime (k/sec): (4608000/52)

```
    IV size: 8 bytes
    replay detection support: Y
outbound
```

ah

```
 sas:
outbound pcp sas:
```

mostra connessione motore di crittografia attiva

Questo comando mostra ciascuna SA fase 2 creata e la quantità di traffico inviato.

Poiché la fase 2 Security Associations (SAs)è unidirezionale, ogni SA visualizza il traffico in una sola direzione (le crittografie sono in uscita, le decrittografazioni in entrata).

debug crypto isakmp

Questo output mostra un esempio del **debug crypto isakmp**comando.

<#root>

```
processing SA payload. message ID = 0
Checking ISAKMP transform against priority 1 policy
    encryption DES-CBC
          hash SHA
    default group 2
    auth pre-share
    life type in seconds
    life duration (basic) of 240
```

atts are acceptable

```
. Next payload is 0
processing KE payload. message ID = 0
processing NONCE payload. message ID = 0
processing ID payload. message ID = 0
SKEYID state generated
processing HASH payload. message ID = 0
SA has been authenticated
processing SA payload. message ID = 800032287
```

debug crypto ipsec

Con questo comando vengono mostrati l'origine e la destinazione degli endpoint del tunnel IPsec.Src_proxy Si dest_proxytratta delle subnet client.

sa createdI messaggi vengono visualizzati con uno in ogni direzione. (Se si eseguono ESP e AH vengono visualizzati quattro messaggi).

In questo output viene mostrato un esempio di**debug crypto ipsec**comando.

<#root>

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
    encaps is 1
    SA life type in seconds
    SA life duration (basic) of 3600
    SA life type in kilobytes
    SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
```

```
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
```

```
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 10.1.0.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest=
```

```
10.1.0.2
```

```
, src=
```

```
10.1.0.1
```

```
,
```

```
dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 10.1.0.0/255.255.255.0/0/0,

      protocol=
```

```
ESP
```

```
, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
               keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src=
```

```
10.1.0.2

, dest=

10.1.0.1,


 src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 10.1.0.0/255.255.255.0/0/0,

      protocol=

ESP

, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa):

sa created

,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa):

sa created

,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Messaggi di esempio

Di seguito sono riportati alcuni messaggi di errore generati dai comandi di debug:

- **debug crypto ipsec**
- **debug crypto isakmp**
- **debug crypt engine**

Controllo riproduzione non riuscito

L'output mostrato di seguito mostra un esempio di"Replay Check Failed"errore.

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=#.
```

Questo errore è dovuto a un riordinamento del supporto di trasmissione (in particolare se esistono percorsi paralleli) o a percorsi diversi di pacchetti elaborati all'interno di Cisco IOS® per pacchetti

di dimensioni grandi e piccoli, oltre che per pacchetti con carico insufficiente.

Modificate l'insieme di trasformazioni in modo che rifletta questo aspetto. Il reply check viene visualizzato solo quando transform-set esp-md5-hmac è abilitato. Per non visualizzare più questo messaggio di errore, disabilitarloesp-md5-hmaced eseguire solo la crittografia.

Fare riferimento al bug Cisco IDCSCdp19680 (solo utenti registrati).

Errore QM FSM

Il tunnel VPN IPsec L2L non viene visualizzato sul firewall PIX o sull'ASA e viene visualizzato il messaggio di errore QM FSM.

Una delle cause possibili è che le identità proxy, ad esempio il traffico insolito,Access Control List (ACL),o gli ACL crittografici, non corrispondono su entrambi i lati.

Controllare la configurazione su entrambi i dispositivi e verificare che gli ACL di crittografia corrispondano.

Un altro possibile motivo è una mancata corrispondenza dei parametri del set di trasformazioni. Verificare che su entrambe le estremità i gateway VPN utilizzino lo stesso set di trasformazioni con gli stessi parametri.

Indirizzo locale non valido

Questo output mostra un esempio del messaggio di errore:

```
IPSEC(validate_proposal): invalid local address 10.2.0.2
ISAKMP (0:3): atts not acceptable. Next payload is 0
ISAKMP (0:3): SA not acceptable!
```

Questo messaggio di errore viene attribuito a uno dei due problemi comuni seguenti:

- **crypto map map-name local-address interface-id**Il comando determina l'utilizzo da parte del router di un indirizzo non corretto come identità, in quanto impone l'utilizzo da parte del router di un indirizzo specificato.
- Crypto map viene applicata all'interfaccia errata o non viene applicata affatto. Controllare la configurazione per verificare che la mappa crittografica venga applicata all'interfaccia corretta.

Il messaggio IKE da X.X.X.X non ha superato il controllo di integrità o è in formato non valido

Questo errore di debug viene visualizzato se le chiavi già condivise nei peer non corrispondono. Per risolvere il problema, controllare le chiavi già condivise su entrambi i lati.

```
1d00H:%CRPTO-4-IKMP_BAD_MESSAGE: IKE message from 198.51.100.1 failed its
 sanity check or is malformed
```

Processo della modalità principale non riuscito con il peer

Questo è un esempio del messaggioMain Modedi errore. Il fallimento della modalità principale suggerisce che la politica della fase 1 non corrisponde su entrambi i lati.

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0
1d00h: ISAKMP (0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with
peer at 198.51.100.1
```

Il comando show crypto isakmp sa mostra l'associazione di sicurezza ISAKMP in cui si trovaMM_NO_STATE. Ciò significa anche che la modalità principale non è riuscita.

```
dst          src        state              conn-id         slot
10.1.1.2  10.1.1.1   MM_NO_STATE        1           0
```

Verificare che il criterio della fase 1 sia su entrambi i peer e che tutti gli attributi corrispondano.

```
Encryption DES or 3DES
Hash MD5 or SHA
Diffie-Hellman Group 1 or 2
Authentication {rsa-sig | rsa-encr | pre-share
```

Identità proxy non supportate

Questo messaggio viene visualizzato nei debug se l'elenco degli accessi per il traffico IPsec non corrisponde.

```
1d00h: IPSec(validate_transform_proposal): proxy identities not supported
1d00h: ISAKMP: IPSec policy invalidated proposal
1d00h: ISAKMP (0:2): SA not acceptable!
```

Gli elenchi degli accessi di ciascun peer devono essere speculari (tutte le voci devono essere

reversibili). Questo esempio illustra questo punto.

```
Peer A
access-list 150 permit ip 172.21.113.0 0.0.0.255 172.21.114.0 0.0.0.255
access-list 150 permit ip host 10.2.0.8 host 172.21.114.123
Peer B
access-list 150 permit ip 172.21.114.0 0.0.0.255 172.21.113.0 0.0.0.255
access-list 150 permit ip host 172.21.114.123 host 10.2.0.8
```

Proposta di trasformazione non supportata

Questo messaggio viene visualizzato se la fase 2 (IPsec) non corrisponde su entrambi i lati. Questo si verifica in genere in caso di mancata corrispondenza o incompatibilità nel set di trasformazioni.

```
1d00h: IPSec (validate_proposal): transform proposal
   (port 3, trans 2, hmac_alg 2) not supported
1d00h: ISAKMP (0:2) : atts not acceptable. Next payload is 0
1d00h: ISAKMP (0:2) SA not acceptable
```

Verificare che il set di trasformazioni corrisponda su entrambi i lati:

```
crypto ipsec transform-set transform-set-name transform1
[transform2 [transform3]]
? ah-md5-hmac
? ah-sha-hmac
? esp-des
? esp-des and esp-md5-hmac
? esp-des and esp-sha-hmac
? esp-3des and esp-md5-hmac
? esp-3des and esp-sha-hmac
? comp-lzs
```

Nessun certificato e nessuna chiave con il peer remoto

Questo messaggio indica che l'indirizzo peer configurato sul router è errato o è stato modificato. Verificare che l'indirizzo del peer sia corretto e che sia raggiungibile.

```
1d00h: ISAKMP: No cert, and no keys (public or pre-shared) with
remote peer 198.51.100.2
```

Indirizzo peer X.X.X.X non trovato

Questo messaggio di errore viene visualizzato normalmente insiemeVPN 3000 Concentrator al messaggio"Message: No proposal chosen(14)"di errore. Infatti le connessioni sono da host a host.

La configurazione del router contiene le proposte IPSec in un ordine in cui la proposta scelta per il router corrisponde all'elenco degli accessi, ma non al peer.

L'elenco degli accessi ha una rete più grande che include l'host che interseca il traffico. Per risolvere questo problema, fare in modo che la proposta del router per questa connessione da concentratore a router sia la prima in linea.

In questo modo, è possibile che corrisponda prima all'host specifico.

```
20:44:44: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.15, src=198.51.100.6,
    dest_proxy= 10.0.0.76/255.255.255.255/0/0 (type=1),
    src_proxy= 198.51.100.23/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:44:44: IPSEC(validate_transform_proposal):
   peer address 198.51.100.6 not found
```

Pacchetto IPsec con SPI non valido

Questo output è un esempio del messaggio di errore:

```
%PIX|ASA-4-402101: decaps: recd IPSEC packet has
invalid spi for destaddr=dest_address, prot=protocol, spi=number
```

Il pacchetto IPSec ricevuto specifica un valore Security Parameters Index (SPI) che non esiste in Security Associations Database (SADB). Potrebbe trattarsi di una condizione temporanea dovuta a:

- Leggere differenze nel conteggio del periodo di permanenza Security Sssociations (SAs) tra i peer IPsec.
- Le associazioni di protezione locali sono state cancellate.
- Pacchetti non corretti inviati dal peer IPsec.

Questo è probabilmente un attacco.

Azione consigliata:

Il peer probabilmente non riconosce che le associazioni di protezione locali sono state cancellate. Se viene stabilita una nuova connessione dal router locale, i due peer possono quindi ristabilirsi correttamente. In caso contrario, se il problema si verifica per più di un breve periodo, provare a stabilire una nuova connessione o contattare l'amministratore del peer.

PSEC(initialize_sas): ID proxy non validi

L'errore "21:57:57: IPSEC(initialize_sas): invalid proxy IDs"indica che l'identità proxy ricevuta non corrisponde all'identità proxy configurata in base all'elenco degli accessi.

Per verificare che corrispondano entrambi, controllare l'output del comando debug.

Nell'output del comando debug della richiesta di proposta, l'access-list 103 allow ip 10.1.1.0.0.0.255 10.1.0.0 0.0.255 non corrisponde.

L'elenco degli accessi è specifico della rete da un lato e specifico dell'host dall'altro.

```
21:57:57: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.1, src=192.0.2.2,
    dest_proxy= 10.1.1.1/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.0.1/255.255.255.0/0/0 (type=4)
```

Prenotato diverso da zero sul payload 5

Ciò significa che i tasti ISAKMP non corrispondono. Reimpostare la chiave/reimpostare per garantire la precisione.

L'algoritmo hash offerto non corrisponde ai criteri

Se i criteri ISAKMP configurati non corrispondono ai criteri proposti dal peer remoto, il router tenta di utilizzare il criterio predefinito 65535.

Se non corrisponde a nessuna delle due, la negoziazione ISAKMP non riuscirà.

Un utente riceve un messaggio di errore"Hash algorithm offered does not match policy!""Encryption algorithm offered does not match policy!"teorico sui router.

<#root>

```
=RouterA=
3d01h: ISAKMP (0:1): processing SA payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-shared key matched 203.0.113.22
ISAKMP (0:1):
```

Checking ISAKMP transform 1 against priority 1 policy

```
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
```

```
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1):
```

Hash algorithm offered does not match policy!

```
ISAKMP (0:1):
```

atts are not acceptable. Next payload is 0

```
=RouterB=
ISAKMP (0:1):
```

Checking ISAKMP transform 1 against priority 65535 policy

```
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1):
```

Encryption algorithm offered does not match policy!

```
ISAKMP (0:1):
```

atts are not acceptable. Next payload is 0

```
ISAKMP (0:1):
```

no offers accepted!

```
ISAKMP (0:1):
```

phase 1 SA not acceptable!

Verifica HMAC non riuscita

Questo messaggio di errore viene segnalato quando si verifica un errore durante Hash Message Authentication Code la connessione sul pacchetto IPSec. Questo si verifica in genere quando il pacchetto è danneggiato in un modo o nell'altro.

<#root>

```
Sep 22 11:02:39 203.0.113.16 2435:
Sep 22 11:02:39:
```

%MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure

```
Sep 22 11:02:39 203.0.113.16 2436:
Sep 22 11:02:39:
```

**%MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
PktEngReturn_MACMiscompare**

Se questo messaggio di errore viene visualizzato occasionalmente, è possibile ignorarlo. Tuttavia, se la frequenza aumenta, è necessario indagare sull'origine del danneggiamento del pacchetto. Questa condizione può essere dovuta a un difetto dell'acceleratore di crittografia.

Peer remoto non risponde

Questo messaggio di errore viene visualizzato quando il set di trasformazioni non corrisponde. Verificare che i set di trasformazioni corrispondenti siano configurati in entrambi i peer.

Tutte le proposte di SA IPSec sono risultate inaccettabili

Questo messaggio di errore viene visualizzato quando i parametri IPSec della fase 2 non corrispondono tra il sito locale e quello remoto.

Per risolvere questo problema, specificare gli stessi parametri nel set di trasformazioni in modo che corrispondano a quanto stabilito dalla VPN.

Errore di crittografia/decrittografia del pacchetto

Questo output è un esempio del messaggio di errore:

```
HW_VPN-1-HPRXERR: Virtual Private Network (VPN) Module0/2: Packet Encryption/Decryption
error, status=4615
```

Questo messaggio di errore può essere dovuto a uno dei motivi seguenti:

- Frammentazione: i pacchetti crittografici frammentati sono a commutazione di contesto, che forza l'invio dei pacchetti a commutazione di contesto alla scheda VPN prima dei pacchetti a commutazione di contesto.

Se viene elaborato un numero sufficiente di pacchetti a commutazione rapida prima dei pacchetti a commutazione di contesto, il numero di sequenza ESP o AH del pacchetto a commutazione di contesto non è più valido e, quando il pacchetto arriva alla scheda VPN, il relativo numero di sequenza non è compreso nella finestra di ripetizione.

Ciò causa errori nei numeri di sequenza AH o ESP (rispettivamente 4615 e 4612), a seconda dell'incapsulamento usato.

- Voci della cache non aggiornate: un'altra istanza in cui questo problema si può verificare è quando una voce della cache a commutazione rapida diventa non aggiornata e il primo pacchetto con un errore della cache viene commutato.

Soluzioni

1. Disattivare qualsiasi tipo di autenticazione sul set di trasformazioni 3DES e utilizzare ESP-DES/3DES. Ciò disabilita efficacemente la protezione anti-replay/autenticazione, che a sua

volta impedisce gli errori di perdita dei pacchetti relativi al traffico IPsec non ordinato (misto) %HW_VPN-1-HPRXERR: Hardware VPN0/2: Packet Encryption/Decryption error, status=4615.

2. Maximum Transmission Unit (MTU) Per risolvere il problema, impostare le dimensioni dei flussi in ingresso su un valore inferiore a 1400 byte. Immettere questo comando per impostare le dimensioni della MTU (Maximum Transmission Unit) dei flussi in entrata su un valore inferiore a 1400 byte:

```
ip tcp adjust-mss 1300
```

3. Disabilitare la scheda AIM.
4. Disattivare l'opzione di commutazione fast/CEF sulle interfacce del router. Per rimuovere l'opzione di commutazione veloce, usare questo comando in modalità di configurazione interfaccia:

```
no ip route-cache
```

Errore di ricezione pacchetti a causa di un errore della sequenza ESP

Di seguito è riportato un esempio del messaggio di errore:

```
%C1700_EM-1-ERROR: packet-rx error: ESP sequence fail
```

Questo messaggio di errore in genere indica una delle seguenti condizioni possibili:

- I pacchetti IPsec crittografati vengono inoltrati in modo non corretto dal router di crittografia a causa di un meccanismo QoS non configurato correttamente.
- I pacchetti IPsec ricevuti dal router di decrittografia non sono in ordine a causa di un riordinamento dei pacchetti su un dispositivo intermedio.
- Il pacchetto IPsec ricevuto è frammentato e deve essere riassemblato prima della verifica dell'autenticazione e della decrittografia.

Soluzione alternativa

1. Disabilitare QoS per il traffico IPsec sui router di crittografia o intermedi.
2. Abilitare la preframmentazione IPsec sul router di crittografia.

```
<#root>

Router(config-if)#

crypto ipsec fragmentation before-encryption
```

3. Impostare il valore MTU su una dimensione che non deve essere frammentata.

```
<#root>

Router(config)#

interface type [slot_#/]port_#
```

```
<#root>

Router(config-if)#

ip mtu MTU_size_in_bytes
```

4. Aggiornare l'immagine Cisco IOS® all'ultima immagine stabile disponibile in quel treno.

Se le dimensioni MTU vengono modificate su un router, tutti i tunnel terminati su quell'interfaccia devono essere eliminati.

Pianificare il completamento della soluzione durante un tempo di inattività pianificato.

Errore durante il tentativo di stabilire il tunnel VPN sul router serie 7600

Questo errore viene visualizzato quando si cerca di stabilire un tunnel VPN sui router serie 7600:

```
crypto_engine_select_crypto_engine: can't handle any more
```

Questo errore si verifica perché la crittografia software non è supportata sui router serie 7600. I router serie 7600 non supportano la terminazione del tunnel IPsec senza hardware IPsec SPA. La VPN è supportata solo con una scheda IPSEC-SPA in router 7600.

Debug PIX

show crypto isakmp sa

Questo comando mostra l'associazione di sicurezza ISAKMP creata tra peer.

```
dst          src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

Nell'output del comando show crypto isakmp sa, lo stato deve essere sempre `QM_IDLE`. Se lo stato è `MM_KEY_EXCH`, significa che la chiave precondivisa configurata non è corretta o che gli indirizzi IP dei peer sono diversi.

<#root>

```
PIX(config)#
```

show crypto isakmp sa

```
Total     : 2
Embryonic : 1
        dst               src        state     pending     created
 192.168.254.250   10.177.243.187    MM_KEY_EXCH   0           0
```

È possibile risolvere questo problema quando si configura l'indirizzo IP corretto o la chiave già condivisa.

show crypto ipsec sa

Con questo comando vengono visualizzate le associazioni di protezione IPSec create tra peer. Viene creato un tunnel crittografato tra la versione 10.1.0.1 e la 10.1.0.2 per il traffico che va tra le reti 10.1.0.0 e 10.1.1.0.

È possibile visualizzare le due associazioni di protezione ESP create in entrata e in uscita. AH non viene utilizzato in quanto non esistono associazioni di protezione AH.

Nell'output mostrato**show crypto ipsec sa**è un esempio di comando.

<#root>

```
interface: outside
    Crypto map tag: vpn, local addr. 10.1.0.1
   local  ident (addr/mask/prot/port): (
```

10.1.0.0/255.255.255.0/0/0

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

10.1.0.2/255.255.255.255/0/0

```
)
   current_peer: 10.2.1.1
```

dynamic allocated peer ip: 10.1.0.2

```
     PERMIT, flags={}
    #pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
    #pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0
     local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 9a46ecae
     inbound

esp

 sas:
      spi: 0x50b98b5(84646069)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={

Tunnel

, }
        slot: 0, conn id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:

     inbound pcp sas:

     outbound

esp

 sas:
      spi: 0x9a46ecae(2588339374)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={

Tunnel

, }
        slot: 0, conn id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
    outbound ah sas:
```

debug crypto isakmp

Con questo comando vengono visualizzate le informazioni di debug sulle connessioni IPSec e viene visualizzato il primo gruppo di attributi negati a causa di incompatibilità su entrambi i lati.

Il secondo tentativo di corrispondenza (per provare 3DES invece di DES eSecure Hash Algorithm (SHA)ciò è accettabile) e viene creata la SA ISAKMP.

Il debug viene eseguito anche da un client remoto che accetta un indirizzo IP (10.32.8.1) da un pool locale. Dopo la creazione dell'associazione di protezione ISAKMP, gli attributi IPSec vengono negoziati e considerati accettabili.

Il PIX configura quindi le SA IPsec come mostrato di seguito. In questo output viene mostrato un esempio di**debug crypto isakmp**comando.

<#root>

```
crypto_isakmp_process_block: src 10.1.0.1, dest 10.1.0.2
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0):
```

atts are not acceptable

```
. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0):
```

atts are acceptable

```
. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP: Created a peer node for 10.1.0.2
OAK_QM exchange
ISAKMP (0:0): Need config/address
ISAKMP (0:0): initiating peer config to 10.1.0.2. ID = 2607270170 (0x9b67c91a)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.1.0.2.
   message ID = 2156506360
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0):
```

peer accepted the address!

```
ISAKMP (0:0): processing saved QM.
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 818324052
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 2, hmac_alg 1) not supported
ISAKMP (0):
```

atts not acceptable.

```
 Next payload is 0
ISAKMP : Checking IPSec proposal 2
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
```

```
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP (0):
```

atts are acceptable.

```
ISAKMP (0): processing NONCE payload. message ID = 818324052
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR src 10.32.8.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR dst 10.1.0.1 prot 0 port 0
INITIAL_CONTACTIPSEC(key_engine): got a queue event...
```

debug crypto ipsec

Con questo comando vengono visualizzate le informazioni di debug sulle connessioni IPSec.

<#root>

```
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xd532efbd(3576885181) for SA
        from  10.1.0.2  to  10.1.0.1  for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0):
```

Creating IPSec SAs
inbound SA from 10.1.0.2 to 10.1.0.1
(proxy 10.32.8.1 to 10.1.0.1.)
has spi 3576885181 and conn_id 2 and flags 4
outbound SA from 10.1.0.1 to 10.1.0.2
(proxy 10.1.0.1 to 10.32.8.1)
has spi 2749108168 and conn_id 1 and flags 4IPSEC(key_engine):
got a queue event...
IPSEC(initialize_sas

```
): ,
  (key eng. msg.) dest= 10.1.0.1, src=10.1.0.2,
    dest_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    src_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xd532efbd(3576885181), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(
```

initialize_sas

```
): ,
  (key eng. msg.) src=10.1.0.1, dest= 10.1.0.2,
    src_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    dest_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xa3dc0fc8(2749108168), conn_id= 1, keysize= 0, flags= 0x4
return status is IKMP_NO_ERROR
```

Problemi comuni tra router e client VPN

Impossibilità di accedere alle subnet esterne al tunnel VPN: tunnel suddiviso

In questo output di esempio della configurazione del router viene mostrato come abilitare un tunnel suddiviso per le connessioni VPN.

Il **split tunnel**comando è associato al gruppo come configurato nel**crypto isakmp client configuration group hw-client-groupname**comando.

In questo modo, gliCisco VPN Client utenti possono usare il router per accedere a una subnet aggiuntiva che non fa parte del tunnel VPN.

Questa operazione viene eseguita senza compromettere la sicurezza della connessione IPsec. Il tunnel è formato sulla rete 192.0.2.18.

Il traffico viene trasmesso a dispositivi non definiti nel comando, ad esempio**access list 150**a Internet, senza crittografia.

<#root>

```
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 192.0.2.20 198.51.100.21
 wins 192.0.2.22 192.0.2.23
 domain cisco.com
 pool dynpool

acl 150

!
!
access-list 150 permit ip 192.0.2.18 0.0.0.127 any
!
```

Problemi comuni dei client da PIX a VPN

Gli argomenti di questa sezione affrontano i problemi comuni che si verificano quando si configura PIX su IPsec con l'aiuto di VPN Client 3.x. Le configurazioni di esempio per PIX sono basate sulla versione 6.x.

Il traffico non scorre dopo che il tunnel è stato stabilito: impossibile eseguire il ping all'interno della rete dietro a PIX

Si tratta di un problema comune associato al routing. Verificare che il PIX disponga di un percorso per le reti che si trovano all'interno e non sono collegate direttamente alla stessa subnet.

Inoltre, la rete interna deve disporre di un percorso di ritorno al PIX per gli indirizzi nel pool di indirizzi del client.

Questo output mostra un esempio.

```
!--- Address of PIX inside interface.

ip address inside 10.1.1.1 255.255.255.240

!--- Route to the networks that are on the inside segment. !--- The next hop is the router on the inside

route inside 172.16.0.0 255.255.0.0 10.1.1.2 1

 !--- Pool of addresses defined on PIX from which it assigns !--- addresses to the VPN Client for the I

ip local pool mypool 10.1.2.1-10.1.2.254

!--- On the internal router, if the default gateway is not !--- the PIX inside interface, then the route

ip route 10.1.2.0 255.255.255.0 10.1.1.1
```

Dopo l'attivazione del tunnel, l'utente non è in grado di navigare in Internet: split tunnel

La causa più comune di questo problema è che, con il tunnel IPsec tra il client VPN e il PIX, tutto il traffico viene inviato attraverso il tunnel al firewall PIX.

La funzionalità PIX non consente di rinviare il traffico all'interfaccia su cui è stato ricevuto. Pertanto, il traffico destinato a Internet non funziona.

Per risolvere il problema, utilizzare**split tunnel**il comando. L'idea alla base di questa correzione è che solo uno invia il traffico specifico attraverso il tunnel e il resto del traffico va direttamente a Internet, non attraverso il tunnel.

```
<#root>

vpngroup vpn3000 split-tunnel 90

access-list 90 permit ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0
access-list 90 permit ip 172.16.0.0 255.255.0.0 10.1.2.0 255.255.255.0
```

vpngroup vpn3000 split-tunnel 90 Il comando abilita lo split tunnel conaccess-list number 90.

access-list number 90 Il comando definisce il traffico che attraversa il tunnel, il resto del quale viene rifiutato alla fine dell'elenco degli accessi.

L'elenco degli accessi deve essere lo stesso perNetwork Address Translation (NAT)negare il PIX.

Quando il tunnel è attivo, alcune applicazioni non funzionano: regolazione dell'MTU sul client

Dopo aver stabilito il tunnel, sebbene sia possibile eseguire il ping dei computer della rete dietro il firewall PIX, non è possibile utilizzare alcune applicazioni come Microsoft

Outlook

Un problema comune è rappresentato dalle dimensioni della MTU (Maximum Transfer Unit) dei pacchetti. L'intestazione IPsec può avere una lunghezza massima di 50-60 byte, che viene aggiunta al pacchetto originale.

Se le dimensioni del pacchetto superano il 1500 (valore predefinito per Internet), i dispositivi devono frammentarlo. Dopo aver aggiunto l'intestazione IPsec, le dimensioni rimangono inferiori a 1496, ovvero al massimo consentito per IPsec.

Il **show interface**comando mostra l'MTU dell'interfaccia specifica sui router accessibili o sui router della propria sede.

Per determinare la MTU dell'intero percorso tra l'origine e la destinazione, i datagrammi di varie dimensioni vengono inviati conDo Not Fragment (DF)il bit impostato in modo che, se il datagramma inviato è superiore all'MTU, questo messaggio di errore viene rinviato all'origine:

```
frag. needed and DF set
```

Questo output mostra un esempio di come trovare l'MTU del percorso tra gli host con gli indirizzi IP 10.1.1.2 e 172.16.1.56.

<#root>

```
Router#
debug ip icmp
ICMP packet debugging is on

!--- Perform an extended ping.

Router#
ping
Protocol [ip]:
Target IP address:
172.16.1.56
Repeat count [5]:
```

```
Datagram size [100]:
1550
Timeout in seconds [2]:

!--- Make sure you enter y for extended commands.

Extended commands [n]:
y
Source address or interface:
10.1.1.2
Type of service [0]:

!--- Set the DF bit as shown.

Set DF bit in IP header? [no]:
y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1550-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:

2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
Success rate is 0 percent (0/5)

!--- Reduce the datagram size further and perform extended ping again.

Router#
ping
Protocol [ip]:
Target IP address:
172.16.1.56
Repeat count [5]:
Datagram size [100]:
1500
Timeout in seconds [2]:
Extended commands [n]:
y
Source address or interface:
10.1.1.2
```

```
Type of service [0]:
Set DF bit in IP header? [no]:
```

y

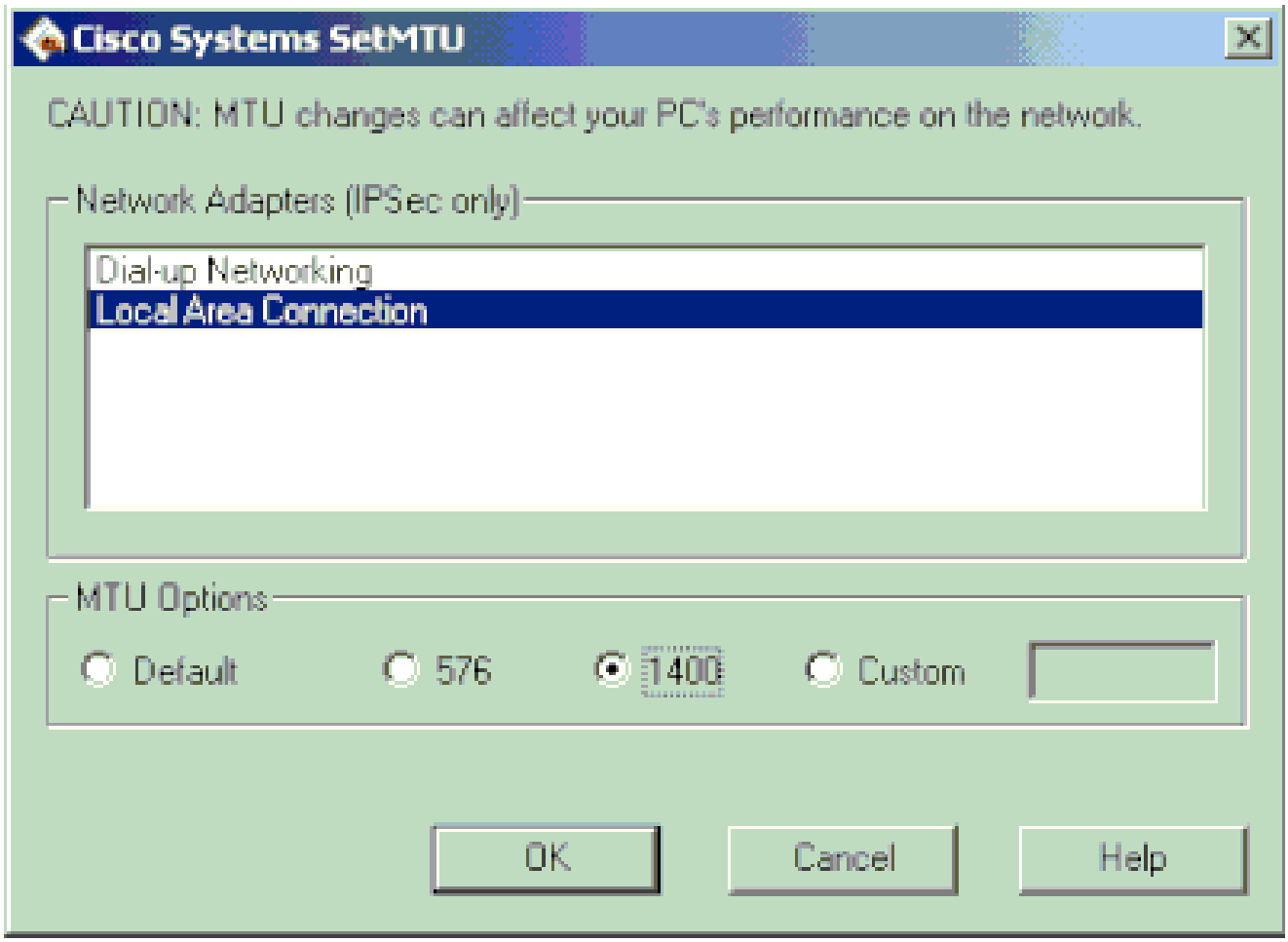
```
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:
!!!!!
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2

Success rate is 100 percent (5/5), round-trip min/avg/max = 380/383/384 ms
```

Il client VPN viene fornito con un'utility di regolazione MTU che consente all'utente di regolare l'MTU per il client VPN Cisco.

Nel caso di utenti client PPP over Ethernet (PPPoE), regolare l'MTU per l'adattatore PPPoE.

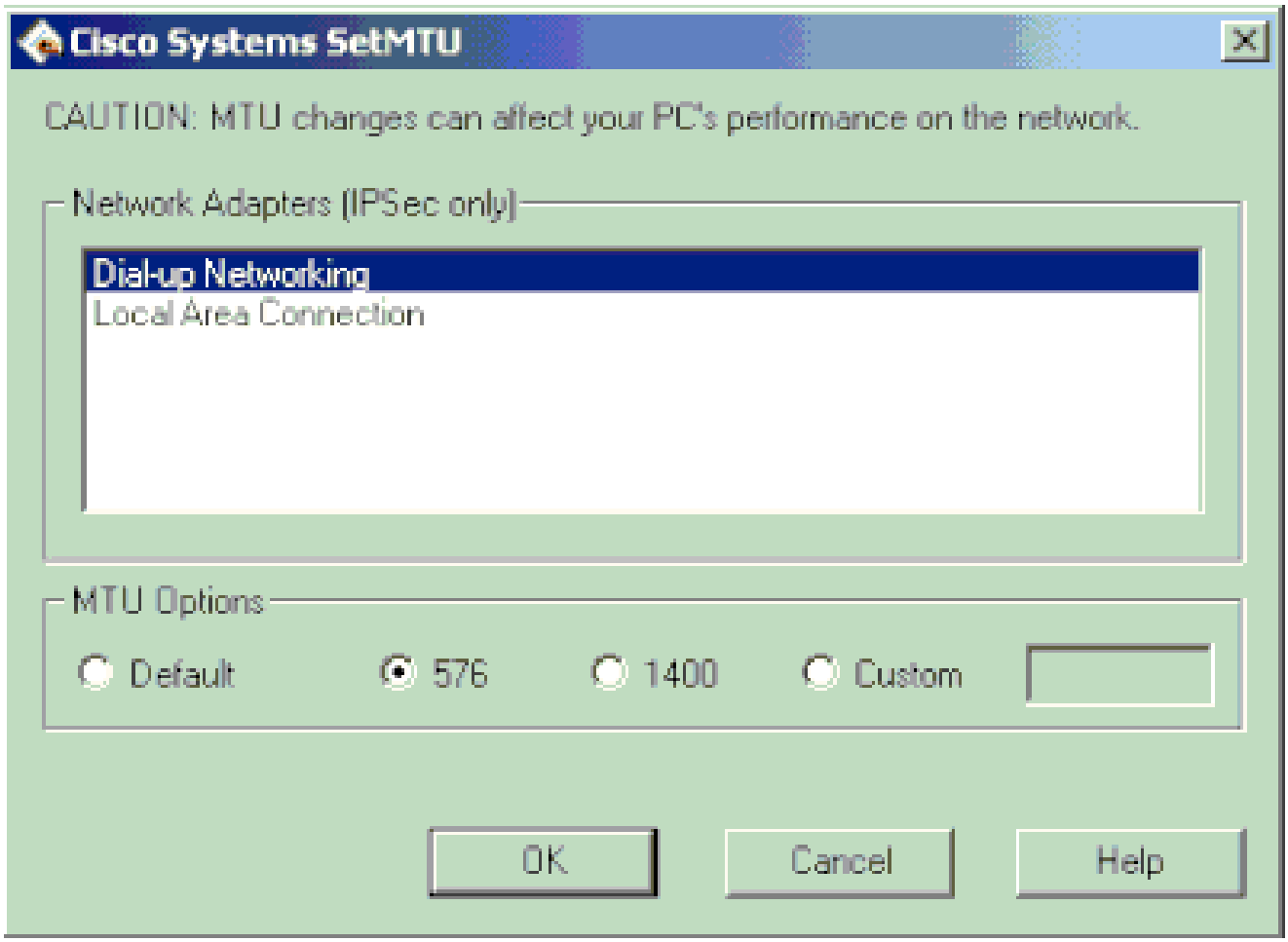
Completare questa procedura per regolare l'utility MTU per il client VPN.

1. Scegli **Start** > **Programs** > **Cisco System VPN Client** > **Set MTU**.
2. Selezionare**Local Area Connection**, quindi fare clic sul pulsante di opzione 1400.
3. Fare clic su **OK**.



4. Ripetere il passaggio 1 e selezionare**Dial-up Networking**.

5. Fare clic sul pulsante576pulsante di opzione, quindi fare clic su**OK**.



Ignora il comando sysopt

Usare il **sysopt connection permit-ipsec**comando nelle configurazioni IPSec sul PIX per consentire il passaggio del traffico IPSec attraverso il firewall PIX senza verificare**conduitaccess-list**o eseguire istruzioni di comando.

Per impostazione predefinita, qualsiasi sessione in ingresso deve essere consentita in modo esplicito da un'istruzione **conduit** o **access-list**command. Con il traffico IPsec protetto, la verifica dell'elenco degli accessi secondari può essere ridondante.

Per consentire sempre le sessioni in entrata autenticate/cifrate IPsec, utilizzare**sysopt connection permit-ipsec**il comando.

Verifica degli Access Control Lists (ACLs)

In una configurazione VPN IPsec tipica vengono utilizzati due elenchi degli accessi. Un elenco degli accessi viene usato per esentare il traffico destinato al tunnel VPN dal processo NAT.

Nell'altro elenco degli accessi viene definito il traffico da crittografare. Ciò include un ACL crittografico in una configurazione LAN-to-LAN o un ACL con tunnel suddiviso in una configurazione di accesso remoto.

Quando gli ACL non sono configurati correttamente o sono mancati, il traffico potrebbe fluire in una sola direzione attraverso il tunnel VPN, o non essere stato inviato attraverso il tunnel.

Accertarsi di aver configurato tutti gli elenchi degli accessi necessari per completare la configurazione della VPN IPsec e che tali elenchi degli accessi definiscano il traffico corretto.

Questo elenco contiene voci da controllare quando si sospetta che un ACL sia la causa del problema con la VPN IPsec.

- Verificare che l'esenzione NAT e gli ACL di crittografia specifichino il traffico corretto.
- Se si hanno più tunnel VPN e più ACL crittografici, verificare che tali ACL non si sovrappongano.
- Non usare gli ACL due volte. Anche se l'ACL di esenzione NAT e l'ACL di crittografia specificano lo stesso traffico, usare due elenchi degli accessi diversi.
- Verificare che il dispositivo sia configurato per utilizzare l'ACL di esenzione NAT. Ossia, usare**route-map**il comando sul router; usare**nat (0)**il comando sul PIX o sull'ASA. Per le configurazioni LAN-to-LAN e di accesso remoto è necessario un ACL di esenzione NAT.

Per ulteriori informazioni su come verificare le istruzioni ACL, consultare la sezioneVerifica della correttezza degli ACL nelle soluzioni di risoluzione dei problemi relativi alla VPN IPsec da L2L e all'accesso remoto più comuni.

Informazioni correlate

- Negoziazione IPsec/pagina di supporto del protocollo IKE
- Pagina di supporto PIX
- Note tecniche
- Documentazione e supporto tecnico – Cisco Systems

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).