Comprensión y uso de comandos de depuración para solucionar problemas de IPsec

Contenido

Introducción

Este documento describe los comandos de depuración comunes utilizados para resolver problemas de IPSec en el software Cisco IOS® y PIX/ASA.

Antecedentes

Consulte Las Soluciones Más Comunes de Troubleshooting de VPN IPSec de Acceso Remoto y L2L para obtener información sobre la mayoría de las soluciones comunes a los problemas de VPN IPSec.

Contiene una lista de verificación de procedimientos comunes que puede probar antes de comenzar a resolver problemas de una conexión y llamar al Soporte Técnico de Cisco.

Prerequisites

Requirements

Este documento supone que usted ha configurado IPSec. Consulte [Negociación IPSec/Protocolos IKE](#) para obtener más detalles.

Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- **Software Cisco IOS®**Conjunto de funciones de IPSec.56i: indica single **Data Encryption Standard (DES)** (en Cisco IOS® Software Release 11.2 y posteriores).k2: indica la función DES triple (en Cisco IOS® Software Release 12.0 y versiones posteriores). DES triple está disponible en Cisco 2600 Series y versiones posteriores.
- **PIX — V5.0 y versiones posteriores, que requiere una clave de licencia DES simple o triple**

para activarse.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Depuraciones del software Cisco IOS®

Los temas de esta sección describen los comandos debug del software Cisco IOS®. Consulte Negociación IPSec/Protocolos IKE para obtener más detalles.

show crypto isakmp sa

Este comando muestra el **Internet Security Association Management Protocol (ISAKMP) Security Associations (SAs)** entre pares.

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

show crypto ipsec sa

Este comando muestra las SA IPSec generadas entre peers. El túnel cifrado se crea entre 10.1.0.1 y 10.1.0.2 para el tráfico que va entre las redes 10.1.0.0 y 10.1.1.0.

Pueden ver las dos **Encapsulating Security Payload (ESP)** SA integradas de entrada y de salida. El Encabezamiento de Autenticación (AH) no se utiliza dado que no hay SA AH.

Este resultado muestra un ejemplo del **show crypto ipsec sa** comando.

```
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:
```

show crypto engine connection active

Este comando muestra cada SA de Fase 2 generada y la cantidad de tráfico enviada.

Porque fase 2 **Security Associations (SAs)** son unidireccionales, cada SA muestra el tráfico en una sola dirección (los cifrados son salientes, los descifrados son entrantes).

debug crypto isakmp

Este resultado muestra un ejemplo del **debug crypto isakmp** comando.

```
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

Este comando muestra el origen y el destino de los extremos del túnel IPSec. **Src_proxy** y **dest_proxy** son las subredes del cliente.

Dos **sa created** los mensajes aparecen con uno en cada dirección. (Aparecen cuatro mensajes si ejecuta ESP y AH).

Este resultado muestra un ejemplo del **debug crypto ipsec** comando.

```
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
```

Ejemplos de Mensajes de Error

Estos mensajes de error de ejemplo fueron generados a partir de los comandos debug enumerados aquí:

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

Replay Check Failed

Este resultado muestra un ejemplo del **Replay Check Failed** error:

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

Este error es el resultado de un reordenamiento en el medio de transmisión (especialmente si existen trayectorias paralelas), o trayectorias desiguales de paquetes procesados dentro de Cisco IOS® para paquetes grandes versus paquetes pequeños más bajo carga.

Cambie el conjunto de transformación para reflejar esto. **reply check** solo se ve cuando **transform-set esp-md5-hmac** está activada. Para suprimir este mensaje de error, inhabilite **esp-md5-hmac** y sólo cifrado.

Consulte el bug de Cisco IDCSCdp19680 (sólo clientes registrados) .

Error QM FSM

El túnel VPN L2L IPSec no aparece en el firewall PIX o ASA, y aparece el mensaje de error QM FSM.

Una posible razón son las identidades proxy, como el tráfico inusual, **Access Control List (ACL),** o ACL criptográfica, no coinciden en ambos extremos.

Verifique la configuración en ambos dispositivos y asegúrese de que las ACL crypto coincidan.

Otra razón posible es la falta de coincidencia de los parámetros del conjunto de transformación. Verifique que en ambos extremos, los gateways VPN utilicen el mismo conjunto de transformación con los mismos parámetros exactos.

Dirección Local no Válida

Este resultado muestra un ejemplo del mensaje de error:

```
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!
```

Este mensaje de error se atribuye a uno de estos dos problemas comunes:

- **crypto map map-name local-address interface-id** hace que el router utilice una dirección incorrecta como identidad porque obliga al router a utilizar una dirección especificada.
- **Crypto map** se aplica a la interfaz incorrecta o no se aplica en absoluto. Verifique la configuración para asegurar que el mapa crypto se aplique a la interfaz correcta.

El mensaje IKE de X.X.X.X falló en su verificación de integridad o es incorrecto

Este error debug aparece si las claves previamente compartidas en los peers no coinciden. Para solucionar este problema, verifique las claves previamente compartidas en ambos lados.

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

Error en el proceso del modo principal con el par

Este es un ejemplo de la **Main Mode** . La falla del modo principal sugiere que la política de la fase 1 no coincide en ambos lados.

```
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
```

Un comando **show crypto isakmp sa** muestra que ISAKMP SA está en **MM_NO_STATE**. Esto también significa que el modo principal ha fallado.

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

Verifique que la política de la fase 1 esté en ambos peers y asegúrese de que todos los atributos coincidan.

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

Identidades Proxy No Soportadas

Este mensaje aparece en debugs si la lista de acceso para el tráfico IPSec no coincide.

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

Las listas de acceso en cada peer deben reflejarse entre sí (todas las entradas deber ser reversibles). Este ejemplo ilustra este 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
```

Propuesta de Transformación no Admitida

Este mensaje aparece si la fase 2 (IPSec) no coincide con en ambos lados. Esto ocurre más comúnmente si hay una discordancia o una incompatibilidad en el conjunto de transformación.

```
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
```

Verifique que el conjunto de transformación coincida en ambos lados.

```
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
```

No Cert and No Keys with Remote Peer

Este mensaje indica que la dirección de peer configurada en el router es incorrecta o ha cambiado. Verifique que la dirección de peer sea correcta y que la dirección puede ser alcanzada.

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

Peer Address X.X.X.X Not Found

Este mensaje de error aparece normalmente con el **VPN 3000 Concentrator** mensaje de error **Message: No proposal chosen(14)**. Esto se debe a que las conexiones son de host a host.

La configuración del router tiene las propuestas de IPSec en un orden donde la propuesta elegida para el router coincide con la lista de acceso, pero no con el peer.

La lista de acceso tiene una red más grande que incluye el host que interseca el tráfico. Para corregir esto, coloque la propuesta del router para esta conexión del concentrador al router primera en la línea.

Esto permite que coincida con el host específico primero.

```
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
```

IPsec Packet has Invalid SPI

Este resultado es un ejemplo del mensaje de error:

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

El paquete IPSec recibido especifica un **Security Parameters Index (SPI)** que no existe en el **Security Associations Database (SADB)**. Esto podría ser una condición temporal debido a lo siguiente:

- Ligeras diferencias en el envejecimiento de **Security Sssociations (SAs)** entre los pares IPsec
- Se han borrado las SA locales
- Paquetes incorrectos enviados por el peer IPSec

Esto es posiblemente un ataque.

Acción Recomendada: El peer posiblemente no reconozca que las SA locales han sido borradas. Si se establece una nueva conexión desde el router local, entonces los dos peers pueden restablecerse satisfactoriamente.

De lo contrario, si el problema se produce durante más de un breve período, intente establecer una nueva conexión o póngase en contacto con el administrador del mismo nivel.

IPSEC(initialize_sas): ID de Proxy No Válidas

El error **21:57:57: IPSEC(initialize_sas): invalid proxy IDs** indica que la identidad de proxy recibida no coincide con la identidad de proxy configurada según la lista de acceso.

Para asegurarse de que ambas coincidan, verifique el resultado del comando debug.

En la salida del comando **debug** de la solicitud de propuesta, la lista de acceso 103 permit ip 10.1.1.0 0.0.0.255 10.1.0.0 0.0.0.255 no coincide.

La lista de acceso es específica de red en un extremo y específica de host en el otro.

```
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)
```

Reservado No Cero en Carga Útil 5

Esto significa que las claves ISAKMP no coinciden. Vuelva a introducir la clave o restablézcala para asegurar la exactitud.

Hash Algorithm Offered does not Match Policy

Si las políticas ISAKMP configuradas no coinciden con la política propuesta por el peer remoto, el router intenta la política predeterminada de 65535.

Si eso tampoco coincide, falla la negociación ISAKMP.

Un usuario recibe el **Hash algorithm offered does not match policy!** or **Encryption algorithm offered does not match policy!** en los routers.

```
=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!
```

Falló la Verificación del HMAC.

Este mensaje de error se notifica cuando se produce un error en la verificación del **Hash Message Authentication Code** en el paquete IPSec. Por lo general, esto sucede cuando el paquete se corrompe de alguna manera.

```
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
```

Si de vez en cuando aparece este mensaje de error, puede ignorarlo. Sin embargo, si esto se vuelve más frecuente, entonces debe investigar el origen de la corrupción del paquete. Esto puede suceder por un defecto en el acelerador criptográfico.

Un Peer Remoto No Responde.

Este mensaje de error se muestra cuando hay una discordancia entre los conjuntos de transformación. Asegúrese de que los conjuntos de transformación coincidentes estén configurados en ambos pares.

Todas las propuestas de SA IPSec encontradas inaceptables

Este mensaje de error aparece cuando los parámetros IPSec de fase 2 no coinciden entre los sitios local y remoto.

Para resolver este problema, especifique los mismos parámetros en el conjunto de transformación para que coincidan y se establezca una VPN exitosa.

Error de Cifrado/Descifrado de Paquetes

Este resultado es un ejemplo del mensaje de error:

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

Este mensaje de error se debe posiblemente a una de estas razones:

- Fragmentación: los paquetes crypto fragmentados se convierten en process-switched, lo cual fuerza el envío de los paquetes fast-switched a la tarjeta de red privada virtual (VPN) antes de los paquetes process-switched.

Si se procesan bastantes paquetes fast-switched antes de los paquetes process-switched, el número de secuencia AH o ESP del paquete process-switched se desactualizará y, cuando el paquete llegue a la tarjeta VPN, su número de secuencia estará fuera de la ventana de repetición.

Esto genera los errores de número de secuencia AH o ESP (4615 y 4612, respectivamente), según qué encapsulación se utilice.

- Entradas de memoria caché desactualizadas: otro caso en que esto podría suceder es cuando una entrada de memoria caché de fast switching se desactualiza y el primer paquete con una pérdida de memoria caché se convierte en process-switched.

Soluciones alternativas

1. Apague todo tipo de autenticación en el conjunto de transformación 3DES y utilice ESP-DES/3DES. Esto inhabilita de manera efectiva la protección de autenticación/anti-reproducción, que (a su vez) evita errores de caída de paquetes relacionados con el tráfico IPsec no ordenado (mixto) **%HW_VPN-1-HPRXERR: Hardware VPN0/2: Packet Encryption/Decryption error, status=4615.**
2. Una solución alternativa que se aplica al motivo mencionado aquí es establecer el **Maximum Transmission Unit (MTU)** tamaño de los flujos entrantes inferior a 1400 bytes. Ingrese este comando para configurar el tamaño de la unidad máxima de transmisión (MTU) de los flujos entrantes en menos de 1400 bytes:
   ```
   ip tcp adjust-mss 1300
   ```
3. Inhabilite la tarjeta AIM.
4. Apague el fast/CEF switching en las interfaces de router. Para eliminar el fast switching, utilice estos comandos en el modo de configuración de la interfaz:
   ```
   no ip route-cache
   ```

Los Paquetes Reciben un Error Debido a una Falla de Secuencia ESP.

A continuación, se incluye un ejemplo del mensaje de error:

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

Este mensaje de error generalmente indica una de estas condiciones posibles:

- Los paquetes cifrados IPSec son reenviados fuera de servicio por el router de cifrado debido a un mecanismo de calidad de servicio (QoS) mal configurado.
- Los paquetes IPSec recibidos por el router de descifrado están fuera de servicio debido a un reorden de paquetes en un dispositivo intermedio.
- El paquete IPSec recibido se fragmenta y requiere reensamblado antes de la verificación de autenticación y del descifrado.

Solución Aternativa

1. Inhabilite el QoS para el tráfico IPSec en los routers intermedios o de cifrado.
2. Habilite la prefragmentación IPSec en el router de cifrado.
   ```
   Router(config-if)#crypto ipsec fragmentation before-encryption
   ```
3. Configure el valor de MTU en un tamaño que no deba fragmentarse.
   ```
   Router(config)#interface type [slot_#/]port_#
   ```
   ```
   Router(config-if)#ip mtu MTU_size_in_bytes
   ```
4. Actualice la imagen de Cisco IOS® a la última imagen estable disponible en ese tren.

Si se cambia el tamaño de MTU en cualquier router, se desactivarán todos los túneles que hayan finalizado en esa interfaz.

Planifique para completar esta solución alternativa durante un tiempo de inactividad programado.

Error al Intentar Establecer Túnel VPN en Router Serie 7600.

Recibirá este error cuando intente establecer un túnel VPN en los routers serie 7600:

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

Este error ocurre porque no se soporta el cifrado del software en routers serie 7600. Los routers serie 7600 no soportan la terminación de túnel IPSec sin el hardware SPA IPSec. La VPN se soporta solamente con una tarjeta IPSEC-SPA en los routers 7600.

Depuración PIX

show crypto isakmp sa

Este comando muestra el ISAKMP SA generado entre pares.

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

En la salida **show crypto isakmp**, el estado debe ser siempre **QM_IDLE**. Si el estado es MM_KEY_EXCH, esto significa que la llave previamente compartida configurada no es correcta o que las direcciones IP de peer son diferentes.

```
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
```

Usted puede rectificar esto al configurar la dirección IP correspondiente o la llave previamente compartida correcta.

show crypto ipsec sa

Este comando muestra las SA IPSec generadas entre peers. Un túnel cifrado se construye entre 10.1.0.1 y 10.1.0.2 para el tráfico que va entre las redes 10.1.0.0 y 10.1.1.0.

Puede observar los dos SA de ESP creados de entrada y salida. AH no se utiliza, ya que no hay SA AH.

Un ejemplo de la **show crypto ipsec sa** se muestra en este resultado.

```
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 este comando, se muestra información de debug sobre las conexiones IPSec y se muestra el primer conjunto de atributos que se niegan debido a incompatibilidades en ambos extremos.

El segundo intento de coincidencia (intentar 3DES en lugar de DES y el **Secure Hash Algorithm (SHA)** es aceptable y se genera la SA ISAKMP.

Este debug es también de un cliente por línea telefónica que acepta una dirección IP (10.32.8.1) fuera de un conjunto local. Una vez generada la SA ISAKMP, se negocian y se aceptan los atributos IPSec.

Luego, el PIX configura la SA IPSec como se muestra aquí. Este resultado muestra un ejemplo del **debug crypto isakmp** comando.

```
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 este comando, se muestra información de debug sobre las conexiones IPSec.

```
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
```

Problemas Comunes del Router al Cliente VPN

Incapacidad para Acceder a Subredes Fuera del Túnel VPN: Túnel dividido

Este resultado de configuración de router de ejemplo muestra cómo habilitar un túnel dividido para las conexiones VPN.

split tunnel está asociado al grupo tal como se ha configurado en el **crypto isakmp client configuration group hw-client-groupname** comando.

Esto permite al **Cisco VPN Client** utilizar el router para acceder a una subred adicional que no forma parte del túnel VPN.

Esto se hace sin poner en riesgo la seguridad de la conexión IPsec. El túnel se forma en la red 192.0.2.18.

El tráfico fluye sin cifrar a dispositivos no definidos en el **access list 150** , como Internet.

```
!
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
!
```

Problemas Comunes del PIX al Cliente VPN

Los temas de esta sección tratan los problemas comunes con los que usted se encuentra al configurar el PIX a IPSec con la ayuda del cliente VPN 3.x. Las configuraciones de ejemplo para el PIX se basan en la versión 6.x.

El Tráfico No Fluye Después de Establecer el Túnel: No se Puede Hacer Ping Dentro de la Red Detrás del PIX.

Este es un problema común de ruteo. Asegúrese de que el PIX tenga una ruta para las redes que estén dentro y no directamente conectadas a la misma subred.

Además, la red de adentro debe tener una ruta nuevamente al PIX para las direcciones del conjunto de direcciones del cliente.

En este resultado, se muestra un ejemplo.

```
!--- 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 IPsec session.

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 router needs to have route !--- for 10.1.2.0/24 network with next hop as the PIX inside
interface !.

ip route 10.1.2.0 255.255.255.0 10.1.1.1
```

Después de que el Túnel Entra en Actividad, el Usuario No Puede Navegar por Internet: Túnel dividido

La razón más común de este problema es que, con el túnel IPSec del cliente VPN al PIX, todo el tráfico se envía a través del túnel al firewall PIX.

La funcionalidad PIX no permite que el tráfico se envíe nuevamente a la interfaz donde se recibió. Por lo tanto, el tráfico destinado a Internet no funciona.

Para solucionar este problema, utilice el **split tunnel** comando. La idea detrás de esta solución es que solamente uno envíe tráfico específico a través del túnel y que el resto del tráfico vaya directamente a Internet, no a través del túnel.

```
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 habilita el túnel dividido con **access-list number 90**.

access-list number 90 define qué tráfico fluye a través del túnel, el resto de los cuales se deniega al final de la lista de acceso.

La lista de acceso debe ser la misma para denegar **Network Address Translation (NAT)** en PIX.

Después de que el Túnel Entra en Actividad, Ciertas Aplicaciones No Funcionan: Ajuste de MTU en el Cliente

Una vez establecido el túnel, aunque puede hacer ping a las máquinas en la red detrás del firewall PIX, no puede utilizar ciertas aplicaciones como Microsoft **Outlook**.

Un problema común es el tamaño de la unidad máxima de transmisión (MTU) de los paquetes. El encabezado IPSec puede tener hasta 50 a 60 bytes, que se agrega al paquete original.

Si el tamaño del paquete pasa a tener más de 1500 bytes (el valor predeterminado para Internet), los dispositivos deberán fragmentarlo. Después de la adición del encabezado IPSec, el tamaño sigue siendo inferior a 1496 bytes, lo cual es el valor máximo para IPSec.

show interface muestra la MTU de esa interfaz en particular en los routers accesibles o en los routers de sus propias instalaciones.

Para determinar la MTU de toda la trayectoria de origen a destino, los datagramas de varios tamaños se envían con el comando **Do Not Fragment (DF)** bit configurado de modo que, si el datagrama enviado es mayor que la MTU, este mensaje de error se devuelve al origen:

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

En este resultado, se muestra un ejemplo de cómo encontrar el valor de MTU de la trayectoria entre los hosts con las direcciones IP 10.1.1.2 y 172.16.1.56.

```
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)
```

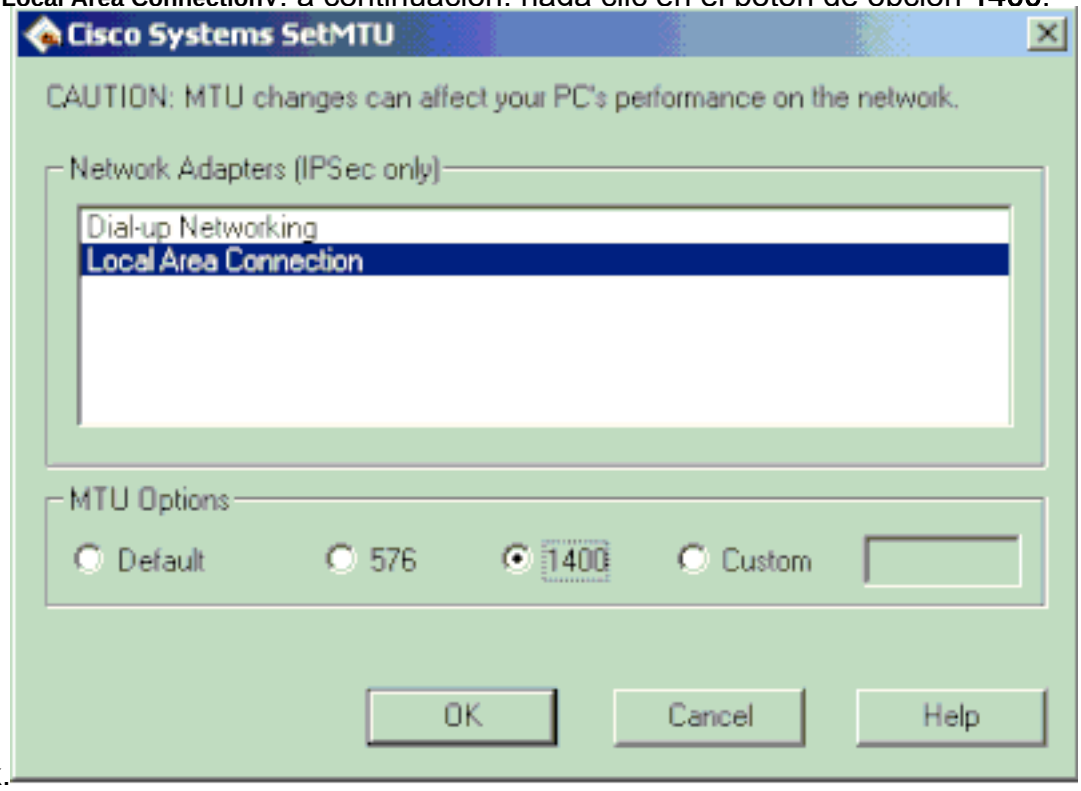
```
!--- Reduce the datagram size further and perform extended ping again.

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
```

El cliente VPN viene con una utilidad de ajuste de MTU que le permite al usuario ajustar el valor de MTU para el cliente VPN de Cisco.

En el caso de usuarios de cliente de PPP over Ethernet (PPPoE), ajuste el valor de MTU para el adaptador PPPoE.

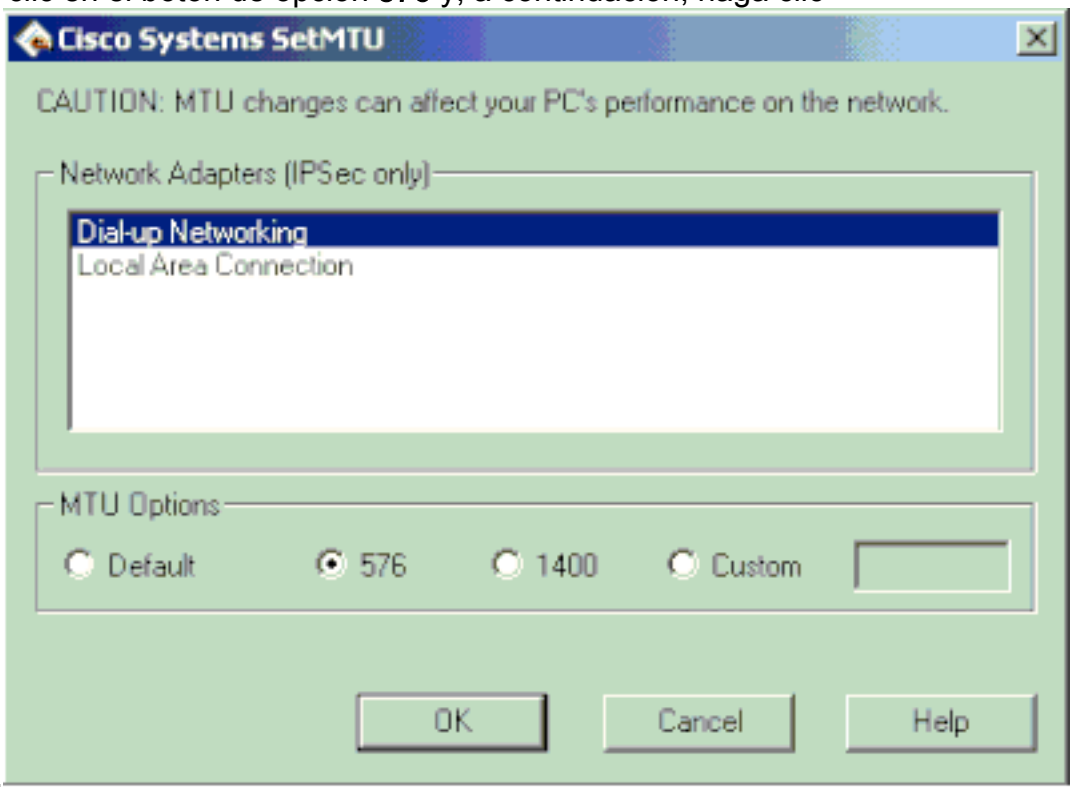
Realice estos pasos para ajustar la utilidad de MTU para el cliente VPN.

1. Elegir **Start > Programs > Cisco System VPN Client > Set MTU**.
2. Seleccionar **Local Area Connection**y, a continuación, haga clic en el botón de opción **1400**.



3. Haga clic **OK**.

4. Repita el paso 1 y seleccione **Dial-up Networking**.
5. Haga clic en el botón de opción **576** y, a continuación, haga clic enOK.



Omitir el Comando sysopt

Use el comando **sysopt connection permit-ipsec** en las configuraciones IPSec en el PIX para permitir que el tráfico IPSec pase a través del Firewall PIX sin una verificación de **conduit** or **access-list** instrucciones de comando.

De forma predeterminada, cualquier sesión entrante debe estar permitida explícitamente por un **conduit** or **access-list** instrucción de comando. Con el tráfico protegido IPSec, la verificación de la lista de acceso secundaria puede ser redundante.

Para habilitar las sesiones entrantes autenticadas/cifradas IPSec para que siempre se permitan, utilice el comando **sysopt connection permit-ipsec** comando.

Verificar las Listas de Control de Acceso (ACL)

Hay dos listas de acceso que se utilizan en una configuración típica de VPN IPSec.

Una lista de acceso se utiliza para eximir el tráfico destinado al túnel VPN del proceso NAT.

La otra lista de acceso define qué tráfico se cifrará. Esto incluye una ACL crypto en una configuración de LAN a LAN o una ACL de túnel dividido en una configuración de acceso remoto.

Cuando estas ACL se configuran incorrectamente o se pierden, es posible que el tráfico fluya sólo en una dirección a través del túnel VPN o que no se haya enviado a través del túnel.

Asegúrese de haber configurado todas las listas de acceso necesarias para completar su configuración de VPN IPSec y de que esas listas de acceso definan el tráfico correcto.

En esta lista, aparecen los elementos que se verificarán cuando usted sospeche que una ACL es la causa de problemas con su VPN IPSec.

- Asegúrese de que sus ACL crypto y de exención de NAT especifiquen el tráfico correcto.
- Si usted tiene varios túneles VPN y varias ACL crypto, asegúrese de que esas ACL no se superpongan.
- No utilice las ACL dos veces. Incluso si su ACL crypto y su ACL de exención de NAT especifican el mismo tráfico, utilice dos listas de acceso diferentes.
- Asegúrese de que su dispositivo esté configurado para utilizar la ACL de exención de NAT. Es decir, utilice el **route-map** comando en el router; use el comando **nat (0)** en el PIX o ASA. Se requiere una ACL de exención de NAT para las configuraciones tanto de LAN a LAN como de acceso remoto.

Para aprender más sobre cómo verificar las sentencias ACL, consulte la sección Verificar que las ACL sean Correctas enSoluciones de Troubleshooting de VPN IPSec de Acceso Remoto y L2L Más Comunes.

Información Relacionada

- Página de Soporte del Protocolo IKE/la Negociación de IPSec
- Página de Soporte de PIX
- Notas técnicas
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).