Troubleshooting de IPSec: Entendiendo y con los comandos debug

Contenido

Introducción

¿Este documento describe los **comandos debug** comunes usados para resolver problemas los problemas del IPSec en ambo el Cisco IOS? Software y PIX/ASA. Este documento supone que usted ha configurado IPSec. Consulte Mensajes de Error Comunes de IPsec y Problemas Comunes de IPsec para obtener información más detallada.

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 intentar implementar antes de comenzar a resolver problemas con una conexión y llamar al Soporte Técnico de Cisco.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- **Cisco IOS Software**Conjunto de funciones de IPSec.56i — Indica la función Data Encryption Standard (DES) simple (en el Cisco IOS Software Versión 11.2 y versiones posteriores).k2 — Indica la función DES triple (en el Cisco IOS Software Versión 12.0 y versiones posteriores). DES triple está disponible en Cisco 2600 Series y versiones posteriores.
- **PIX** — V5.0 y posterior, que requiere una llave de la licencia sola o del DES triple para activar.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Comandos Debug del Cisco IOS Software

Los temas de esta sección describen los comandos debug del Cisco IOS Software. Consulte Mensajes de Error Comunes de IPsec y Problemas Comunes de IPsec para obtener información más detallada.

show crypto isakmp sa

Este comando muestra a las asociaciones (SA) del protocolo Internet Security Association Management Protocol (ISAKMP) creadas entre pares.

```
dst      src        state     conn-id     slot
12.1.1.2  12.1.1.1   QM_IDLE    1           0
```

show crypto ipsec sa

Este comando muestra las SA IPSec generadas entre peers. El túnel cifrado se crea entre 12.1.1.1 y 12.1.1.2 para el tráfico que va entre las redes 20.1.1.0 y 10.1.1.0. Puede ver las dos SA de carga de seguridad de encapsulación (ESP) generadas en sentido entrante y saliente. El Encabezamiento de Autenticación (AH) no se utiliza dado que no hay SA AH.

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

```
  interface: FastEthernet0
    Crypto map tag: test, local addr. 12.1.1.1
   local  ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   current_peer: 12.1.1.2
     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.: 12.1.1.1, remote crypto endpt.: 12.1.1.2
     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 fase 2 SA construida y la cantidad de tráfico enviada. Puesto que las SA (asociaciones de seguridad) de fase 2 SA son unidireccionales, cada SA muestra tráfico en solamente una dirección (los cifrados son salientes, los descifrados son entrantes).

debug crypto isakmp

En este resultado, se muestra un ejemplo del **comando debug crypto isakmp**.

```
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. Aparecen dos mensajes "sa created" con uno en cada dirección. (Aparecen cuatro mensajes si ejecuta ESP y AH).

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

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, 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 error “Replay Check Failed”:

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Este error es un resultado de reordenamiento en el medio de transmisión (especialmente si existen trayectorias paralelas) o trayectorias desiguales de procesamiento de paquetes dentro del Cisco IOS para paquetes grandes en comparación con paquetes pequeños con carga. Cambie el conjunto de transformación para reflejar esto. La *marca de reproducción* solo se ve cuando transform-set esp-md5-hmac está habilitado. Para eliminar este mensaje de error, inhabilite esp-md5-hmac y solo haga el cifrado. Consulte el ID de bus de Cisco CSCdp19680 (clientes registrados solamente) .

Para obtener información sobre cómo configurar IPsec Anti-Replay Window, consulte Cómo Configurar IPsec Anti-Replay Window: Extensión e Inhabilitación.

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 razón posible es que las identidades proxy, como tráfico interesante, lista de acceso de control (ACL) o ACL crypto, no coinciden en ambos extremos. Verifique la configuración en ambos dispositivos y asegúrese de que las ACL crypto coincidan.

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

Dirección Local no Válida

Este resultado muestra un ejemplo del mensaje de error:

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

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

- El comando crypto map map-name local-address interface-id hace que el router utilice una dirección incorrecta como la identidad ya que lo obliga a usar una dirección específica.
- El mapa crypto 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.

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Processing of Main Mode Failed with Peer

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

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

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

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

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

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Identidades Proxy No Soportadas

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

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

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

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

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.

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Verifique que el conjunto de transformación coincida en ambos lados.

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

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.

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Peer Address X.X.X.X Not Found

Este mensaje de error aparece normalmente con el error de mensaje del VPN 3000 Concentrator Message: No proposal chosen(14). Este es un resultado de las conexiones 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.

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
```

```
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

IPsec Packet has Invalid SPI

Este resultado es un ejemplo del mensaje de error:

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

El paquete IPsec recibido especifica un Security Parameters Index (SPI) que no existe en la base de datos de asociaciones de seguridad (SADB). Esto podría ser una condición temporal debido a lo siguiente:

- Diferencias leves en la antigüedad de las asociaciones de seguridad (SA) entre los peers IPSec
- Las SA locales que han sido despejadas
- Paquetes incorrectos enviados por el peer IPSec

También podría ser un ataque.

Acción Recomendada: Es posible que el peer no reconozca que las SA locales han sido despejadas. Si se establece una nueva conexión desde el router local, entonces los dos peers pueden restablecerse satisfactoriamente. De lo contrario, si el problema ocurre durante más que un breve período, intente establecer una nueva conexión o póngase en contacto con el administrador del peer.

IPSEC(initialize_sas): ID de Proxy No Válidas

El error 21:57:57: `IPSEC(initialize_sas):` invalid proxy IDs indican 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 el **resultado del comando debug** de la solicitud de propuesta, el IP de permiso 103 de la lista de acceso 10.1.1.0 0.0.0.255 20.1.1.0 0.0.0.255 correspondiente no coincide. La lista de acceso es específica de red en un extremo y específica de host en el otro.

```
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= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      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 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      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= 12.1.1.2, 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= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

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 mensaje de error Hash algorithm offered does not match policy! o El algoritmo de cifrado ofrecido no coincide con la política. en los routers.

```
=RouterA=
3d01h: ISAKMP (0:1): processing SA payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-shared key matching 209.165.200.227
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 muestra cuando hay una falla en la verificación del Código de Autenticación de Mensajes Basado en Hash (HMAC) en el paquete IPSec. Por lo general, esto sucede cuando el paquete se corrompe de alguna manera.

```
Sep 22 11:02:39 131.203.252.166 2435:
Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure
Sep 22 11:02:39 131.203.252.166 2436:
Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                 PktEngReturn_MACMiscompare
```

Si usted ve este mensaje de error de vez en cuando, puede ignorarlo. Sin embargo, si este aparece con mayor frecuencia, deberá investigar qué está corrompiendo el 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 peers.

Todas las ofertas IPSec SA encontraron inaceptable

Este mensaje de error ocurre cuando los parámetros de IPSec de la fase 2 se unen mal entre los sitios local y remoto. Para resolver este problema, especifique los mismos parámetros en la transformación fijada de modo que hagan juego y el VPN acertado establezca.

Error de Cifrado/Descifrado de Paquetes

Este resultado es un ejemplo del mensaje de error:

```
Sep 22 11:02:39 131.203.252.166 2435:
Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure
Sep 22 11:02:39 131.203.252.166 2436:
Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                 PktEngReturn_MACMiscompare
```

Este mensaje de error puede aparecer por 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 con eficacia la autenticación o la protección contra repetición, que (a su vez) previene los errores de descarte de paquetes relacionados con el tráfico IPSec (combinado) desordenado *%HW_VPN-1-HPRXERR: Hardware VPN0/2: Error de Cifrado/Descifrado de Paquetes, estado=4615*.
2. Una solución temporal que se aplica realmente a la razón mencionada en el punto n.° 1 anterior es configurar el tamaño de la unidad máxima de transmisión (MTU) de los flujos entrantes en menos de 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:`Sep 22 11:02:39 131.203.252.166 2435:`
   `Sep 22 11:02:39:` **`%MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure`**
   `Sep 22 11:02:39 131.203.252.166 2436:`
   `Sep 22 11:02:39:` **`%MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000, PktEngReturn_MACMiscompare`**
3. Inhabilite la tarjeta AIM.
4. Apague el fast/CEF switching en las interfaces de router. Para quitar el fast switching rápidamente, puede utilizar este comando en el modo de configuración de interfaz:`Sep 22 11:02:39 131.203.252.166 2435:`
   `Sep 22 11:02:39:` **`%MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure`**
   `Sep 22 11:02:39 131.203.252.166 2436:`
   `Sep 22 11:02:39:` **`%MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000, PktEngReturn_MACMiscompare`**

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

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

```
Sep 22 11:02:39 131.203.252.166 2435:
Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure
Sep 22 11:02:39 131.203.252.166 2436:
Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                 PktEngReturn_MACMiscompare
```

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 al reordenamiento 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 del IOS a la última imagen estable disponible de ese tren.

Nota: El cambio del tamaño de MTU en cualquier interfaz de router hará que todos los túneles que terminen en esa interfaz se derriben. Usted debe planear realizar esta solución temporal 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:

```
Router(config-if)#ip mtu MTU_size_in_bytes
```

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.

```
Router(config-if)#ip mtu MTU_size_in_bytes
```

En el resultado de **show crypto isakmp sa**, 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 12.1.1.1 y 12.1.1.2 para el tráfico que va entre las redes 20.1.1.0 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 del **comando show crypto ipsec sa** se muestra en este resultado.

```
interface: outside
    Crypto map tag: vpn, local addr. 12.1.1.1
   local  ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (12.1.1.2/255.255.255.255/0/0)
   current_peer: 10.2.1.1
   dynamic allocated peer ip: 12.1.1.2
     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.: 12.1.1.1, remote crypto endpt.: 12.1.1.2
     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. Es aceptable un segundo intento de coincidencia (intentar 3DES, en lugar de DES y el Algoritmo de Hash Seguro [SHA]) 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.

En este resultado, se muestra un ejemplo del **comando debug crypto isakmp**.

```
crypto_isakmp_process_block: src 12.1.1.1, dest 12.1.1.2
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 12.1.1.2
OAK_QM exchange
ISAKMP (0:0): Need config/address
ISAKMP (0:0): initiating peer config to 12.1.1.2. ID = 2607270170 (0x9b67c91a)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 12.1.1.2, dest 12.1.1.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 12.1.1.2.
```

```
   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 12.1.1.1 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  12.1.1.2  to  12.1.1.1  for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 12.1.1.2, dest 12.1.1.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from  12.1.1.2  to  12.1.1.1
           (proxy 10.32.8.1 to  12.1.1.1.)
        has spi 3576885181 and conn_id 2 and flags 4
        outbound SA from  12.1.1.1  to  12.1.1.2
           (proxy 12.1.1.1 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= 12.1.1.1, src= 12.1.1.2,
    dest_proxy= 12.1.1.1/0.0.0.0/0/0 (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= 12.1.1.1, dest= 12.1.1.2,
    src_proxy= 12.1.1.1/0.0.0.0/0/0 (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: Tunelización dividida

En este resultado de configuración de router de ejemplo, se muestra cómo habilitar la tunelización dividida para las conexiones VPN. El **comando access list 150** se relaciona con el grupo según lo configurado en el **comando crypto isakmp client configuration group hw-client-groupname**. Esto permite que el cliente VPN de Cisco utilice el router para acceder a una subred adicional que no forme parte del túnel VPN. Esto se hace sin comprometer la seguridad de la conexión IPSec. El túnel se forma en la red 172.168.0.128. El tráfico fluye descifrado a los dispositivos que no están definidos en el **comando access list 150**, como Internet.

```
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 172.168.0.250 172.168.0.251
 wins 172.168.0.252 172.168.0.253
 domain cisco.com
 pool dynpool
 acl 150
!
!
access-list 150 permit ip 172.168.0.128 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.

```
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 172.168.0.250 172.168.0.251
 wins 172.168.0.252 172.168.0.253
 domain cisco.com
 pool dynpool
 acl 150
!
!
access-list 150 permit ip 172.168.0.128 0.0.0.127 any
!
```

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

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 **comando split tunneling**. 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
```

Nota: El **comando vpngroup vpn3000 split-tunnel 90** habilita la división de túnel con **access-list number 90**. El **comando access-list 90** define qué tráfico fluye a través del túnel; el resto del mismo se niega en el extremo de la lista de acceso. La lista de acceso debe ser la misma para la negación de la Traducción de Dirección de Red (NAT) en el PIX.

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

A veces, después de establecer el túnel, es posible que usted pueda hacer ping con las máquinas en la red detrás del firewall PIX, pero no podrá 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.

El **comando show interface** muestra el valor de MTU de esa interfaz en particular en los routers que son accesibles o en los routers de sus propias instalaciones. Para determinar el valor de MTU de la trayectoria completa del origen al destino, los datagramas de diversos tamaños se envían con el bit Don't Fragment (DF) configurado para que, si el datagrama enviado es mayor que el valor de MTU, se envíe este mensaje de error nuevamente al origen:

```
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
```

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.

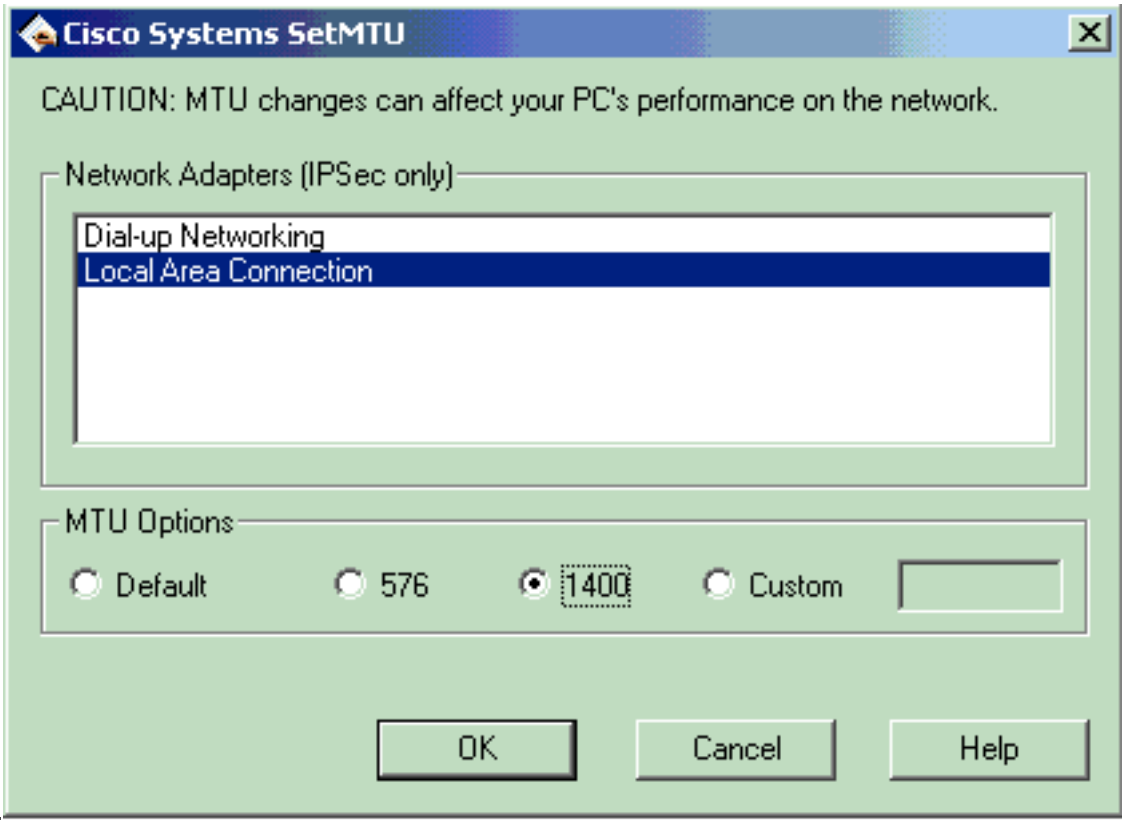
```
Router#debug ip icmp
ICMP packet debugging is on

!--- 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
```

Nota: 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.

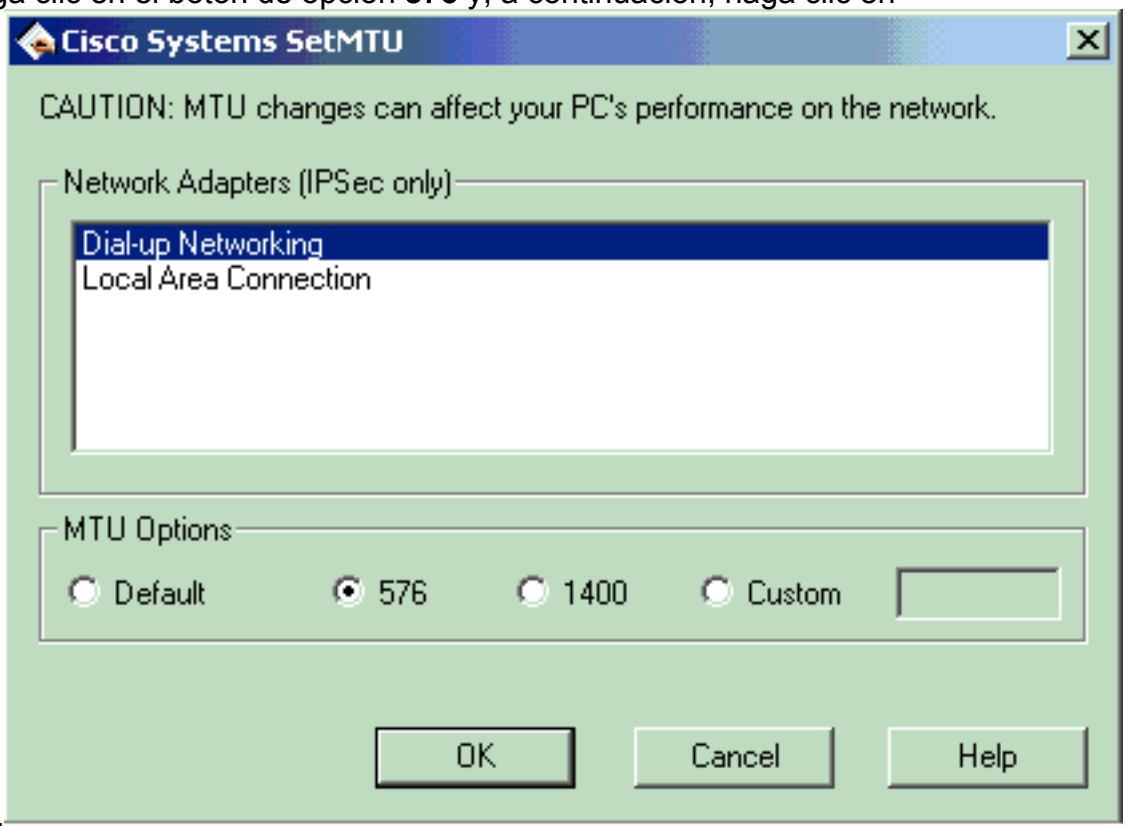
Nota: Realice estos pasos para ajustar la utilidad de MTU para el cliente VPN.

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



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 en



OK.

Omitir el Comando sysopt

Utilice el **comando sysopt connection permit-ipsec** en configuraciones IPSec en el PIX para permitir que el tráfico IPSec pase a través del firewall PIX sin una verificación de las declaraciones del **comando conduit or access-list**. De forma predeterminada, cualquier sesión entrante debe ser permitida explícitamente por una declaración del **comando conduit or access-list**. Con el tráfico protegido IPSec, la verificación de la lista de acceso secundaria puede ser

redundante. Para habilitar que siempre se permitan sesiones entrantes de encripción/autenticadas IPSec, utilice el **comando sysopt connection permit-ipsec**.

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 un configuración de LAN a LAN (L2L) o una ACL de tunelización dividida en una configuración de acceso remoto. Si estas ACL se configuran de forma incorrecta o faltan, el tráfico podría fluir solamente en una dirección a través del túnel VPN o no se podría enviar a través del túnel en absoluto.

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 **comando route-map** en el router; utilice 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 obtener más información sobre cómo verificar las declaraciones de ACL, consulte la sección Verificación de que las ACL Sean Correctas en Las Soluciones Más Comunes de Troubleshooting de VPN IPSec de Acceso Remoto y L2L.

Información Relacionada

- Página de Soporte del Protocolo IKE/la Negociación de IPSec
- Una Introducción al Cifrado de Seguridad IP (IPSec)
- Página de Soporte de PIX
- Referencia de Comandos PIX
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems