# Guía de Troubleshooting de GETVPN

## Contenido

# Introducción

Este documento pretende presentar una metodología estructurada de solución de problemas y herramientas útiles para ayudar a identificar y aislar los problemas de Group Encrypted Transport VPN (GETVPN) y para proporcionar posibles soluciones.

# Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- GETVPN
  [Guía Oficial de Configuración de GETVPN](#)
  [Guía oficial de diseño e implementación de GETVPN](#)

- Uso del servidor Syslog

## Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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. If your network is live, make sure that you understand the potential impact of any command.

# Metodología de Troubleshooting de GETVPN

Como ocurre con la mayoría de los problemas de tecnología complejos, la clave es poder aislar el problema a una función, subsistema o componente específico. La solución GETVPN consta de varios componentes de funciones, concretamente:

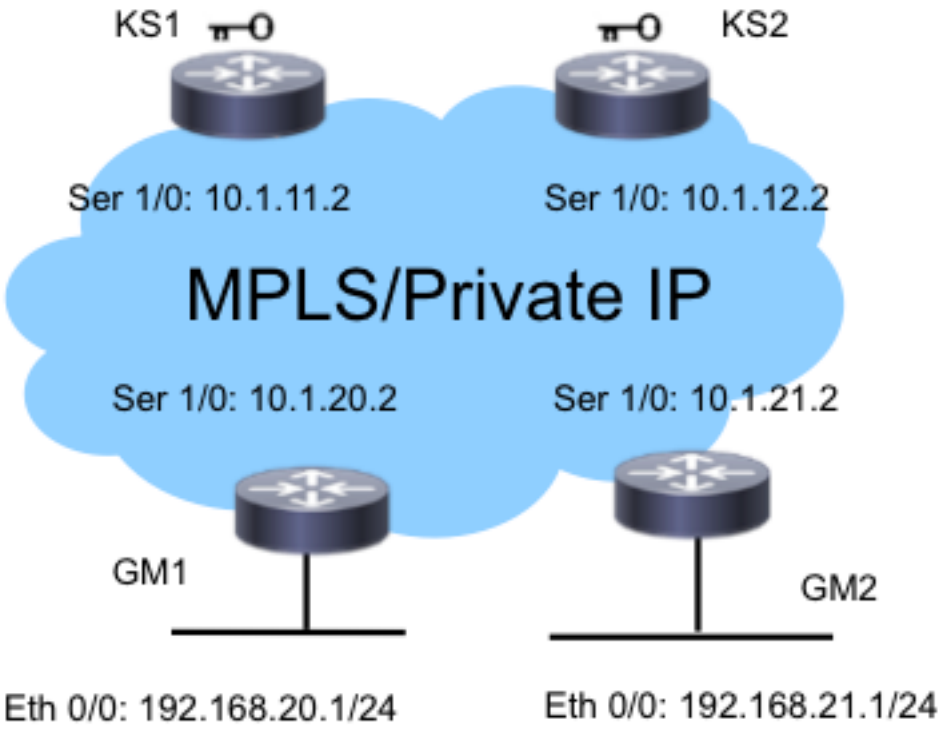
- Intercambio de claves de Internet (IKE): se utiliza entre miembros del grupo (GM) y servidores clave (KS), y entre KS de protocolo cooperativo (COOP) para autenticar y proteger el plano de control.
- Dominio de interpretación de grupo (GDOI): protocolo utilizado para el KS a fin de distribuir claves de grupo y proporcionar servicios clave como la clave para todos los GM.
- COOP - Protocolo utilizado para los KS para comunicarse entre sí y proporcionar redundancia.
- Preservación de encabezados: IPSec en modo túnel que conserva el encabezado del paquete de datos original para la entrega de tráfico de extremo a extremo.
- Time Based Anti-Replay (TBAR): mecanismo de detección de repetición utilizado en un

entorno de clave de grupo.

También proporciona un amplio conjunto de herramientas de resolución de problemas para facilitar el proceso de resolución de problemas. Es importante comprender cuáles de estas herramientas están disponibles y cuándo son adecuadas para cada tarea de resolución de problemas. Al solucionar problemas, siempre es una buena idea comenzar con los métodos menos intrusivos para que el entorno de producción no se vea afectado negativamente. La clave para esta solución de problemas estructurada es poder dividir el problema en un problema de plano de datos o de control. Puede hacerlo si sigue el protocolo o el flujo de datos y utiliza las diversas herramientas presentadas aquí para verificarlas.

## Topología de referencia

Este esquema de direccionamiento y topología GETVPN se utiliza en el resto de este documento de troubleshooting.




## Configuraciones de referencia

- KS1

```
crypto gdoi group G1
identity number 3333
server local
rekey authenmypubkeyrsa get
rekey transport unicast
sa ipsec 1
profile gdoi-p
match address ipv4ENCPOL
address ipv4 10.1.11.2
redundancy
local priority 10
peer address ipv4 10.1.12.2
```

- GM1

```
crypto gdoi group G1
identity number 3333
server address ipv4 10.1.11.2
server address ipv4 10.1.12.2
!
crypto map gm_map 10 gdoi
set group G1
!
interface Serial1/0
crypto map gm_map
```

**Nota:** Las configuraciones de KS2 y GM2 no se incluyen aquí para su brevedad.

## Terminology

- **KS**: servidor de claves
- **MM** - Miembro del grupo
- **COOP** - Protocolo de cooperación
- **TBAR** - Anti-Reproducción Basada en Tiempo
- **KEK** - Clave de cifrado
- **TEK** - Clave de cifrado del tráfico

## Preparación de la instalación de registro y otras prácticas recomendadas

Antes de comenzar a solucionar problemas, asegúrese de haber preparado la función de registro como se describe aquí. A continuación se enumeran algunas prácticas recomendadas:

- Verifique la cantidad de memoria libre del router y configure el **debugging almacenado en buffer** a un valor grande (10 MB o más si es posible).
- Inhabilite el registro en los servidores de consola, monitor y syslog.
- Recupere el contenido del buffer de registro con el comando **show log** a intervalos regulares, cada 20 minutos a una hora, para evitar la pérdida de registros debido a la reutilización del buffer.
- Pase lo que pase, ingrese el comando **show tech** de los GM y KS afectados, y examine el resultado del comando **show ip route** en global y cada Virtual Routing and Forwarding (VRF) involucrado, si es necesario.
- Utilice el protocolo de tiempo de red (NTP) para sincronizar el reloj entre todos los dispositivos que se depuran. Habilite las marcas de tiempo en milisegundos (msec) para los mensajes de depuración y registro:

```
service timestamps debug datetime msec
service timestamps log datetime msec
```

- Asegúrese de que los resultados del comando show estén marcados con el tiempo.

```
Router#terminal exec prompt timestamp
```

- Cuando recopila los resultados del comando show para los eventos del plano de control o los contadores del plano de datos, recopila siempre varias iteraciones del mismo resultado.

# Resolución de Problemas del Plano de Control GETVPN

Plano de control significa todos los eventos de protocolo que condujeron a la creación de la política y la Asociación de seguridad (SA) en el GM para que estén listos para cifrar y descifrar el tráfico del plano de datos. Algunos de los puntos de control clave en el plano de control de GETVPN son:


## Prácticas recomendadas de depuración del plano de control

Estas prácticas recomendadas de resolución de problemas no son específicas de GETVPN; se aplican a casi cualquier depuración del plano de control. Es fundamental seguir estas prácticas recomendadas para garantizar la resolución de problemas más eficaz:

- Desactive el registro de la consola y utilice el búfer de registro o syslog para recopilar las depuraciones.
- Utilice NTP para sincronizar los relojes del router en todos los dispositivos que se depuran.
- Habilite la marca de tiempo msec para los mensajes de depuración y registro:

```
service timestamp debug datetime msec
service timestamp log datetime msec
```

- Asegúrese de que las salidas del comando show estén marcadas por el tiempo para que se puedan correlacionar con el resultado de la depuración:

```
terminal exec prompt timestamp
```

- Utilice la depuración condicional en un entorno de escala si es posible.

## Herramientas de resolución de problemas del plano de control GETVPN

### Comandos show GETVPN

Como regla general, estos son los resultados de comandos que debe recopilar para casi todos los problemas de GETVPN.

### KS

```
show crypto gdoi
show crypto gdoi ks coop
show crypto gdoi ks members
show crypto gdoi ks rekey
show crypto gdoi ks policy
```

### GM

```
show crypto eli
show crypto gdoi rekey sa
show crypto gdoi
show crypto gdoi gm
show crypto gdoi gm rekey
```

## Mensajes de Syslog GETVPN

GETVPN proporciona un amplio conjunto de mensajes syslog para eventos de protocolo significativos y condiciones de error. El syslog siempre debe ser el primer lugar para buscar cuando realice la resolución de problemas de GETVPN.

### Mensajes de Syslog de KS comunes

| Mensajes de Syslog | Explicación |
|---|---|
| *COOP_CONFIG_MISMATCH* | La configuración entre el servidor de clave principal y el servidor de clave secundaria no coincide. |
| *COOP_KS_ELECTION* | El servidor de claves local ha entrado en el proceso electoral de un grupo. |
| *COOP_KS_REACH* | Se restablece la disponibilidad entre los servidores de claves cooperativos configurados. |
| *COOP_KS_TRANS_TO_PRI* | El servidor de claves local pasó a una función principal de ser un servidor secundario en un grupo. |
| *COOP_KS_UNAUTH* | Un servidor remoto autorizado intentó ponerse en contacto con el servidor claves local de un grupo, lo que podría considerarse un evento hostil. |
| *COOP_KS_UNREACH* | Se pierde el alcance entre los servidores de claves cooperativos configura lo que podría considerarse un evento hostil. |
| *KS_GM_REVOKED* | Durante el protocolo rekey, un miembro no autorizado intentó unirse a un grupo, lo que podría considerarse un evento hostil. |
| *KS_SEND_MCAST_REKEY* | Enviando reclave multicast. |
| *KS_SEND_UNICAST_REKEY* | Enviando la clave de unidifusión. |
| *KS_UNAUTHORIZED* | Durante el protocolo de registro GDOI, un miembro no autorizado intentó u a un grupo, lo que podría considerarse un evento hostil. |
| *UNAUTHORIZED_IPADDR* | La solicitud de registro se descartó porque el dispositivo solicitante no esta autorizado para unirse al grupo. |

### Mensajes comunes de Syslog GM

| Mensajes de Syslog | Explicación |
|---|---|
| *GM_CLEAR_REGISTER* | El miembro del grupo local ha ejecutado el comando **clear crypto gdoi**. |
| *GM_CM_ATTACH* | Se ha adjuntado un mapa criptográfico para el miembro del grupo local. |
| *GM_CM_DETACH* | Se ha desagregado un mapa criptográfico para el miembro del grupo lo |
| *GM_RE_REGISTER* | La SA IPsec creada para un grupo puede haber caducado o borrado. D volver a registrarse en el servidor de claves. |
| *GM_RECV_REKEY* | Se ha recibido la nueva clave. |
| *GM_REGS_COMPL* | Registro completado. |
| *GM_REKEY_TRANS_2_MULTI* | El miembro del grupo ha pasado de utilizar un mecanismo de reclave de unidifusión a utilizar un mecanismo de multidifusión. |
| *GM_REKEY_TRANS_2_UNI* | El miembro del grupo ha pasado de utilizar un mecanismo de reclave multidifusión a utilizar un mecanismo de unidifusión. |
| *PSEUDO_TIME_LARGE* | Un miembro del grupo ha recibido un pseudotime con un valor que es e gran medida diferente a su propio pseudotime. |

| | |
|---|---|
| *REPLAY_FAILED* | Un miembro del grupo o un servidor de claves ha fallado una verificació anti-repetición. |

**Nota:** Los mensajes resaltados en rojo son los mensajes más comunes o significativos observados en un entorno GETVPN.

### Depuraciones globales de cifrado y GDOI

Las depuraciones de GETVPN se dividen:

1. Primero por el dispositivo en el que está resolviendo problemas.
```
F340.06.15-2900-18#debug cry gdoi ?
 all-features  All features in GDOI
 condition     GDOI Conditional Debugging
 gm            Group Member
 ks            Key Server
```
2. En segundo lugar, por el tipo de problema que está solucionando.
```
GM1#debug cry gdoi gm ?
 all-features    All Group Member features
 infrastructure  GM Infrastructure
 registration    GM messages related to registration
 rekey           GM messagese related to Re-Key
 replay          Anti Replay
```
3. En tercer lugar, por el nivel de depuración que debe habilitarse. En la versión 15.1(3)T y posteriores, todas las depuraciones de características GDOI se estandarizaron para tener estos niveles de depuración. Esto fue diseñado para ayudar a resolver problemas de entornos GETVPN a gran escala con suficiente granularidad de depuración. Cuando depura problemas de GETVPN, es importante utilizar el nivel de depuración adecuado. Como regla general, comience con el nivel de depuración más bajo, es decir, el nivel de error, y aumente la granularidad de depuración cuando sea necesario.
```
GM1#debug cry gdoi gm all-features ?
 all-levels  All levels
 detail      Detail level
 error       Error level
 event       Event level
 packet      Packet level
 terse       Terse level
```

### Depuración condicional GDOI

En Cisco IOS® versión 15.1(3)T y posteriores, se agregó debugging condicional GDOI para ayudar a resolver problemas de GETVPN en un entorno a gran escala. Por lo tanto, todas las depuraciones de la Asociación de seguridad de Internet y del protocolo de administración de claves (ISAKMP) y GDOI se pueden activar ahora con un filtro condicional basado en la dirección IP del grupo o del par. Para la mayoría de los problemas de GETVPN, es bueno habilitar las depuraciones ISAKMP y GDOI con el filtro condicional apropiado, ya que las depuraciones GDOI sólo muestran operaciones específicas de GDOI. Para utilizar las depuraciones condicionales ISAKMP y GDOI, complete estos dos sencillos pasos:

1. Establezca el filtro condicional.
2. Habilite el ISAKMP y el GDOI relevantes como siempre.

Por ejemplo:

```
KS1# debug crypto gdoi condition peer add ipv4 10.1.20.2
% GDOI Debug Condition added.

KS1#
KS1# show crypto gdoi debug-condition
GDOI Conditional Filters:
Peer Address 10.1.20.2
Unmatched NOT set

KS1#debug crypto gdoi ks registration all-levels
GDOI Key Server Registration Debug level: (Packet, Detail, Event, Terse, Error)
```

> **Nota:** Con las depuraciones condicionales ISAKMP y GDOI, para capturar mensajes de depuración que podrían no tener la información de filtro condicional, por ejemplo la dirección IP en la trayectoria de depuración, el indicador **no coincidente** se puede habilitar. Sin embargo, esto debe usarse con precaución porque puede producir una gran cantidad de información de depuración.

## Seguimiento de eventos GDOI

Esto se agregó en la versión 15.1(3)T. El seguimiento de eventos ofrece un seguimiento ligero y siempre activo para eventos y errores GDOI significativos. También hay un seguimiento de trayectoria de salida con seguimiento habilitado para las condiciones de excepción. Los seguimientos de eventos pueden proporcionar más información del historial de eventos GETVPN que los syslogs tradicionales.

Los seguimientos de eventos GDOI se habilitan de forma predeterminada y se pueden recuperar del búfer de seguimiento con el comando **show monitor even-trace**.

```
GM1#show monitor event-trace gdoi ?
all Show all the traces in current buffer
back Show trace from this far back in the past
clock Show trace from a specific clock time/date
coop GDOI COOP Event Traces
exit GDOI Exit Traces
from-boot Show trace from this many seconds after booting
infra GDOI INFRA Event Traces
latest Show latest trace events since last display
merged Show entries in all event traces sorted by time
registration GDOI Registration event Traces
rekey GDOI Rekey event Traces

GM1#show monitor event-trace gdoi rekey all
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
```

El seguimiento del trayecto de salida proporciona información detallada sobre el trayecto de salida, es decir, las condiciones de excepción y error, con la opción de seguimiento activada de forma predeterminada. A continuación, se pueden utilizar las pistas para decodificar la secuencia de código exacta que ha conducido a la condición de ruta de salida. Utilice la opción **detail** para recuperar las pistas del búfer de seguimiento:

```
GM1#show monitor event-trace gdoi exit all detail
*Nov 6 15:15:25.611: NULL_VALUE_FOUND:Invalid GROUP Name
-Traceback= 0xCA51318z 0xCA1F4DBz 0xC9B2707z 0xCA1ED4Ez 0x97EB018z
0x97EA960z 0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez
*Nov 6 15:15:25.611: MAP_NOT_APPLIED_IN_ANY_INTERFACE:
-Traceback= 0xCA51318z 0xCA46718z 0xCA1EF79z 0x97EB018z 0x97EA960z
0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez 0xA01FD52z
*Nov 6 15:15:25.650: NULL_VALUE_FOUND:NULL Parameters passed idb or ipaddress
when idb ipaddress is changed
-Traceback= 0xCA51318z 0xCA22430z 0xA09A8DCz 0xA09D8F6z 0xA0F280Fz
0xBA1D1F4z 0xBA1CACCz 0xBA1C881z 0xBA1C5BBz 0xA0F494Az
```

El tamaño predeterminado del búfer de seguimiento es 512 entradas, y esto podría no ser suficiente si el problema es intermitente. Para aumentar este tamaño de entrada de seguimiento predeterminado, los parámetros de configuración de seguimiento de eventos se pueden cambiar como se muestra aquí:

```
GM1#show monitor event-trace gdoi rekey parameters
Trace has 512 entries
Stacktrace is disabled by default

GM1#
GM1#config t
Enter configuration commands, one per line. End with CNTL/Z.
GM1(config)#monitor event-trace gdoi rekey size ?
<1-1000000> Number of entries in trace
```

## Puntos de control del plano de control GETVPN y problemas comunes

Estos son algunos de los problemas comunes del plano de control para GETVPN. Para volver a iterar, el plano de control se define como todos los componentes de la función GETVPN necesarios para habilitar el cifrado y el descifrado del plano de datos en los GM. A un nivel superior, esto requiere un registro GM exitoso, políticas de seguridad y descarga/instalación de SA, y la clave KEK/TEK posterior.

### Configuración y creación de políticas de COOP

Para verificar y verificar que el KS ha creado correctamente la política de seguridad y el KEK/TEK asociado, ingrese:

```
KS1#show crypto gdoi ks policy
Key Server Policy:
For group G1 (handle: 2147483650) server 10.1.11.2 (handle: 2147483650):

For group G1 (handle: 2147483650) server 10.1.12.2 (handle: 2147483651):

# of teks : 1 Seq num : 10
KEK POLICY (transport type : Unicast)
spi : 0x18864836BA888BCD1126671EEAFEB4C7
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 1200 remaining life(sec): 528
sig hash algorithm : enabled sig key length : 162
sig size : 128
sig key name : key1

TEK POLICY (encaps : ENCAPS_TUNNEL)
```

```
spi : 0x91E3985A
access-list : ENCPOL
transform : esp-null esp-sha-hmac
alg key size : 0 sig key size : 20
orig life(sec) : 900 remaining life(sec) : 796
tek life(sec) : 2203 elapsed time(sec) : 1407
override life (sec): 0 antireplay window size: 4

Replay Value 442843.29 secs
```

Un problema común con la configuración de la política de KS es cuando hay diferentes políticas configuradas entre los KS primarios y los secundarios. Esto puede dar lugar a un comportamiento de KS impredecible y se informará de este error:

```
%GDOI-3-COOP_CONFIG_MISMATCH: WARNNING: replay method configuration between
Primary KS and Secondary KS are mismatched
```

Actualmente no hay sincronización de configuración automática entre los KS primarios y secundarios, por lo que se deben rectificar manualmente.

Debido a que COOP es una configuración crítica (y casi siempre obligatoria) para GETVPN, es fundamental asegurarse de que COOP funcione correctamente y de que las funciones de COOP KS sean correctas:

```
KS1#show crypto gdoi ks coop
Crypto Gdoi Group Name :G1
Group handle: 2147483650, Local Key Server handle: 2147483650

Local Address: 10.1.11.2
Local Priority: 200
 Local KS Role: Primary   , Local KS Status: Alive
Local KS version: 1.0.4
Primary Timers:
Primary Refresh Policy Time: 20
Remaining Time: 10
Antireplay Sequence Number: 40

Peer Sessions:
Session 1:
Server handle: 2147483651
Peer Address: 10.1.12.2
Peer Version: 1.0.4
Peer Priority: 100
Peer KS Role: Secondary , Peer KS Status: Alive
Antireplay Sequence Number: 0

IKE status: Established
Counters:
Ann msgs sent: 31
Ann msgs sent with reply request: 2
Ann msgs recv: 64
Ann msgs recv with reply request: 1
Packet sent drops: 7
Packet Recv drops: 0
Total bytes sent: 20887
Total bytes recv: 40244
```

En una configuración de COOP funcional, se debe observar este flujo de protocolo:

Intercambio IKE > ANN con prioridades COOP intercambiadas > Elección COOP > ANN de KS primario a secundario (políticas, bases de datos GM y claves)

Cuando COOP no funciona correctamente, o si hay una división COOP, como que varios KS se conviertan en el KS principal, estos debugs se deben recopilar para la resolución de problemas:

```
debug crypto isakmp
debug crypto gdoi ks coop all-levels
show crypto isakmp sa
show crypto gdoi ks coop
```

### Configuración IKE

Se requiere un intercambio IKE exitoso para GETVPN para asegurar el canal de control para la política posterior y la descarga SA. Al final del intercambio IKE exitoso, se crea un GDOI_REKEY sa.

En las versiones anteriores a Cisco IOS 15.4(1)T, GDOI_REKEY se puede mostrar con el comando **show crypto isakmp sa**:

```
GM1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
10.1.13.2 10.1.11.2 GDOI_REKEY        1075 ACTIVE
10.1.11.2 10.1.13.2 GDOI_IDLE         1074 ACTIVE

IPv6 Crypto ISAKMP SA

GM1#
```

En Cisco IOS 15.4(1)T y versiones posteriores, este GDOI_REKEY como se muestra con el comando **show crypto gdoi rekey sa**:

```
GM1#show crypto gdoi rekey sa
GETVPN REKEY SA
dst             src             conn-id         status
10.1.13.2       10.1.11.2       1114            ACTIVE
```

> **Nota:** Una vez que se complete el intercambio IKE inicial, las políticas y claves posteriores serán **transferidas** del KS al GM con el uso de GDOI_REKEY SA. Por lo tanto, no hay clave de registro para GDOI_IDLE SA cuando caducan; desaparecen cuando sus vidas expiran. Sin embargo, siempre debe haber GDOI_REKEY SA en el GM para que reciba llaves.

El intercambio IKE para GETVPN no es diferente del IKE utilizado en los túneles IPsec punto a punto tradicionales, por lo que el método de solución de problemas sigue siendo el mismo. Estos debugs se deben recopilar para resolver problemas de autenticación IKE:

```
debug crypto isakmp
debug crypto isakmp error
debug crypto isakmp detail (hidden command, if detailed isakmp exchange information
is needed)
debug crypto isakmp packet (hidden command, if packet level isakmp information is needed)
```

### Registro, descarga de políticas e instalación de SA

Una vez que la autenticación IKE se realiza correctamente, GM se registra con el KS. Se espera que estos mensajes de syslog se vean cuando esto ocurre correctamente:

```
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to Unicast Rekey.
%GDOI-5-SA_KEK_UPDATED: SA KEK was updated
%GDOI-5-SA_TEK_UPDATED: SA TEK was updated
%GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.12.2 complete for group G1 using
address 10.1.13.2
%GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation of Reg/Rekey policies
from KS 10.1.12.2 for group G1 & gm identity 10.1.13.2
```

La política y las claves se pueden verificar con este comando:

```
GM1#show crypto gdoi
GROUP INFORMATION

Group Name : G1
Group Identity : 3333
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 1
IPSec SA Direction : Both

Group Server list : 10.1.11.2
10.1.12.2

Group member : 10.1.13.2 vrf: None
Version : 1.0.4
Registration status : Registered
Registered with : 10.1.12.2
Re-registers in       : 139 sec
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 10.1.11.2
Last rekey seq num : 0
Unicast rekey received: 1
Rekey ACKs sent : 1
Rekey Rcvd(hh:mm:ss)  : 00:05:20
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 1
After latest register : 1
Rekey Acks sents : 1

ACL Downloaded From KS 10.1.11.2:
access-list deny icmp any any
access-list deny eigrp any any
access-list deny ip any 224.0.0.0 0.255.255.255
access-list deny ip 224.0.0.0 0.255.255.255 any
access-list deny udp any port = 848 any port = 848
access-list permit ip any any

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 878
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024
```

```
TEK POLICY for the current KS-Policy ACEs Downloaded:
Serial1/0:
IPsec SA:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (200)
Anti-Replay(Time Based) : 4 sec interval


GM1#
GM1#
GM1#show crypto ipsec sa

interface: Serial1/0
Crypto map tag: gm1map, local addr 10.1.13.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 0.0.0.0 port 848
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x0(0)
PFS (Y/N): N, DH group: none

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x8BF147EF(2347845615)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: SW:1, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: SW:2, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)
```

```
outbound ah sas:

outbound pcp sas:
GM1#
```

**Nota:** Con GETVPN, las SA entrantes y salientes utilizan el mismo SPI.

Con el registro de GETVPN y el tipo de instalación de políticas, estos debugs son necesarios para resolver problemas:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

**Nota:** Es posible que se necesiten depuraciones adicionales en función del resultado de estos resultados.

Dado que el registro de GETVPN normalmente ocurre inmediatamente después de la recarga GM, este script EEM podría ser útil para recopilar estos debugs:

```
event manager applet debug
event syslog pattern "RESTART"
action 1.0 cli command "enable"
action 2.0 cli command "debug crypto gdoi all all"
```

## Rekey

Una vez que los GM se registran en el KS y la red GETVPN está configurada correctamente, el KS primario es responsable de enviar mensajes de clave nueva a todos los GM registrados en él. Los mensajes de nueva clave se utilizan para sincronizar todas las políticas, claves y pseudotimes en los GM. Los mensajes de nueva clave se pueden enviar a través de un método unicast o multicast.

Este mensaje de syslog se ve en el KS cuando se envía el mensaje rekey:

```
%GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group G1 from address
10.1.11.2 with seq # 11
```

En los GM, este es el syslog que se ve cuando recibe la clave de nuevo:

```
%GDOI-5-GM_RECV_REKEY: Received Rekey for group G1 from 10.1.11.2 to 10.1.20.2
with seq # 11
```

### Requisito de par de claves RSA para la clave de nuevo en KS

La funcionalidad Rekey requiere la presencia de claves RSA en el KS. El KS proporciona la clave pública del par de claves RSA al GM a través de este canal seguro durante el registro. A continuación, el KS firma los mensajes GDOI enviados al GM con la clave RSA privada en la carga útil GDOI SIG. El MM recibe los mensajes GDOI y utiliza la clave RSA pública para verificar el mensaje. Los mensajes entre el SK y el MM se cifran con el KEK, que también se distribuye al MM durante el registro. Una vez que se complete el registro, las llaves posteriores se cifran con el

KEK y se firman con la clave RSA privada.

Si la clave RSA no está presente en el KS durante el registro GM, este mensaje aparece en el syslog:

```
%GDOI-1-KS_NO_RSA_KEYS: RSA Key - get : Not found, Required for group G1
```

Cuando las claves no están presentes en el KS, el GM se registra por primera vez, pero la próxima clave falla del KS. Con el tiempo, caducan las claves existentes del MM y vuelve a registrarse.

```
%GDOI-4-GM_RE_REGISTER: The IPSec SA created for group G1 may have expired/been
cleared, or didn't go through. Re-register to KS.
```

Dado que el par de llaves RSA se utiliza para firmar los mensajes de rekey, **DEBEN** ser los mismos entre el KS primario y todos los KS secundarios. Esto asegura que durante una falla primaria de KS, las llaves enviadas por un KS secundario (el nuevo KS primario) aún puedan ser validadas adecuadamente por los GM. Cuando genera el par de claves RSA en el KS primario, el par de claves debe crearse con la opción **exportable** para que puedan exportarse a todos los KS secundarios para cumplir este requisito.

#### Resolución de problemas de reclave

La falla de reclave KEK/TEK es uno de los problemas de GETVPN más comunes que se producen en las implementaciones de los clientes. La resolución de problemas de reclave debe seguir los pasos clave descritos a continuación:

1. ¿Las llaves fueron enviadas por el KS?

   Esto se puede verificar con una observación del mensaje de syslog %GDOI-5-KS_SEND_UNICAST_REKEY o más exactamente con este comando:

   ```
   KS1#show crypto gdoi ks rekey
   Group G1 (Unicast)
   Number of Rekeys sent               : 341
   Number of Rekeys retransmitted      : 0
   KEK rekey lifetime (sec) : 1200
   Remaining lifetime (sec) : 894
   Retransmit period : 10
   Number of retransmissions : 5
   IPSec SA 1 lifetime (sec) : 900
   Remaining lifetime (sec) : 405
   ```

   El número de llaves retransmitidas es indicativo de paquetes de reconocimiento de reclave que no recibe el KS y, por lo tanto, posibles problemas de reclave. Tenga en cuenta que el GDOI vuelve a utilizar el UDP como un mecanismo de transporte poco fiable, por lo que se podrían esperar algunas caídas de clave en función de la fiabilidad de la red de transporte subyacente, pero siempre debería investigarse una tendencia al aumento de las retransmisiones de clave nueva.

   También se pueden obtener estadísticas más detalladas sobre las claves modificadas por MM. Este suele ser el primer lugar en el que buscar posibles problemas clave.

```
KS1#show crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group G1 : 346

Group Member ID : 10.1.14.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.11.2
 Rekeys sent       : 346
Rekeys retries : 0
Rekey Acks Rcvd : 346
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1

Group Member ID : 10.1.13.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.12.2
 Rekeys sent       : 340
Rekeys retries : 0
Rekey Acks Rcvd : 340
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1
```

2. ¿Se entregaron los paquetes de nueva clave en la red de infraestructura subyacente?

   Se debe seguir la resolución de problemas de IP estándar a lo largo de la trayectoria de reenvío de llaves para asegurarse de que los paquetes de nueva llave no se descarten en la red de tránsito entre KS y GM. Algunas de las herramientas de solución de problemas más comunes que se utilizan aquí son las listas de control de acceso (ACL) de entrada/salida, Netflow y captura de paquetes en la red de tránsito.

3. ¿Los paquetes de nueva clave alcanzaron el proceso GDOI para el procesamiento de nueva clave?

   Consulte las estadísticas de reclave GM:

```
GM1#show crypto gdoi gm rekey
Group G1 (Unicast)
Number of Rekeys received (cumulative) : 340
Number of Rekeys received after registration : 340
Number of Rekey Acks sent : 340
```

4. ¿El paquete de reconocimiento de nueva clave regresó al KS?

   Siga los pasos 1 a 3 para rastrear el paquete de reconocimiento de nueva clave desde el GM de vuelta al KS.

### Clave de multidifusión

La clave de multidifusión es diferente de la clave de unidifusión en estos aspectos:

- Debido a que multicast se utiliza para transportar estos paquetes de nueva clave del KS a los GMs, el KS no necesita replicar los paquetes de nueva clave en sí. El KS sólo envía una copia del paquete de nueva clave y se replican en la red habilitada para multicast.
- No hay un mecanismo de reconocimiento para la reclave multicast, así que si un GM no recibiera el paquete de reclave, el KS no tendría conocimiento de él, y por lo tanto nunca eliminará un GM de su base de datos GM. Y debido a que no hay reconocimiento, el KS siempre retransmitirá los paquetes de retransmisión en función de su configuración de retransmisión de retransmisión de clave.

El problema de reclave multicast más visto es cuando la nueva clave no se recibe en el GM. Podría haber varias causas posibles para ello, como las siguientes:

- Problema de entrega de paquetes dentro de la infraestructura de ruteo multicast
- El ruteo de multidifusión de extremo a extremo no está habilitado en la red

El primer paso para resolver un problema con la reclave multicast es ver si la reclave funciona cuando se conmuta del método multicast al método unicast.

Una vez que identifique que el problema es específico de la reclave multicast, verifique que el KS envíe la nueva clave a la dirección multicast especificada.

```
%GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for group G1 from address
10.1.11.2 to 226.1.1.1 with seq # 6
```

Pruebe la conectividad de multidifusión entre el KS y el GM con una solicitud de protocolo de mensajes de control de Internet (ICMP) a la dirección de multidifusión. Todos los GM que forman parte del grupo multicast deben responder al ping. Asegúrese de que el ICMP esté excluido de la política de encripción de KS para esta prueba.

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.1.21.2, 44 ms
```

Si la prueba de ping multicast falla, se debe realizar la resolución de problemas de multidifusión, que está fuera del alcance de este documento.

## Comprobación del relé del plano de control

### Síntoma

Cuando los clientes actualizan su GM a una nueva versión de Cisco IOS, podrían experimentar fallas de clave de KEK con este mensaje observado en syslog:

```
%GDOI-3-GDOI_REKEY_SEQ_FAILURE: Failed to process rekey seq # 1 in seq payload for
group G1, last seq # 11
%GDOI-3-GDOI_REKEY_FAILURE: Processing of REKEY payloads failed on GM 10.1.13.2 in the group G1,
with peer at 10.1.11.2
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of GDOI mode failed with peer at 10.1.11.2
```

Este comportamiento se debe a un problema de interoperabilidad introducido con la verificación

anti-repetición que se agrega para los mensajes del plano de control. Específicamente, un KS que ejecute el código más antiguo restablecerá el número de secuencia de reclave KEK en 1, y esto será descartado por el GM que ejecuta el nuevo código cuando lo interpreta como un paquete de nueva clave reproducido. Para obtener más detalles, vea Cisco bug ID CSCta05809 (GETVPN: Plano de control GETVPN sensible a la repetición), y Restricciones de Configuración de GETVPN.

#### Background

Con GETVPN, los mensajes del Plano de control pueden transportar información que distingue el tiempo para proporcionar el servicio de verificación anti-repetición basado en el tiempo. Por lo tanto, estos mensajes requieren protección anti-repetición por sí mismos para garantizar la precisión del tiempo. Estos mensajes son:

- **Volver a introducir mensajes** de KS a GM
- **Mensajes de anuncio de COOP** entre KS

Como parte de esta implementación de protección anti-reproducción, se agregaron verificaciones de número de secuencia para proteger los mensajes reproducidos, así como una verificación pseudotime cuando TBAR está habilitado.

### Solución

Para resolver este problema, tanto el GM como el KS deben actualizarse a las versiones de Cisco IOS después de la función de verificación de la repetición del plano de control. Con el nuevo código de Cisco IOS, KS no reinicia el número de secuencia nuevamente a 1 para una nueva clave KEK, sino que continúa usando el número de secuencia actual y sólo restablece el número de secuencia para las nuevas claves TEK.

Estas versiones de Cisco IOS tienen las funciones Replay Check:

- 12.4(15)T10
- 12.4(22)T3
- 12.4(24)T2
- 15.0(1)M y posteriores

#### Otros problemas relacionados con la reproducción

- Falla de COOP debido a que los mensajes ANN fallan en la verificación de la repetición (Id. de bug Cisco CSCtc52655)

#### Fallas de reproducción del plano de control de depuración

Para otros errores de Reproducción del Plano de Control, recopile esta información y asegúrese de que los tiempos se sincronizan entre el KS y el GM.

- Syslog de GM y KS
- Depuraciones ISAKMP
- Depuraciones de GDOI (reclave y reproducción) tanto de KS como de GM

### Problemas de fragmentación de paquetes del plano de control

Con GETVPN, la fragmentación de paquetes del plano de control es un problema común y puede manifestarse en uno de estos dos escenarios cuando los paquetes del plano de control son lo suficientemente grandes como para requerir la fragmentación de IP:

- Paquetes de anuncio GETVPN COOP
- GETVPN rekey packets

### Paquetes de anuncio de COOP

Los paquetes de anuncio COOP llevan la información de la base de datos GM y, por lo tanto, pueden crecer en una implementación GETVPN de gran tamaño. A partir de la experiencia anterior, una red GETVPN que consta de más de 1500 GM producirá paquetes de anuncio de más de 18024 bytes, que es el tamaño de búfer Enorme predeterminado de Cisco IOS. Cuando esto sucede, el KS no puede asignar un búfer lo suficientemente grande como para transmitir los paquetes ANN con este error:

```
%SYS-2-GETBUF: Bad getbuffer, bytes= 18872 -Process= "Crypto IKMP", ipl= 0, pid= 183
```

Para rectificar esta condición, se recomienda este ajuste del búfer:

```
buffers huge permanent 10
buffers huge size 65535
```

#### Volver a Teclar Paquetes

Los paquetes de nueva clave GETVPN también pueden superar el tamaño típico de la unidad de transición máxima (MTU) de IP 1500 cuando la política de cifrado es grande, como una política que consta de más de 8 líneas de entradas de control de acceso (ACE) en la ACL de cifrado.

#### Problema de fragmentación e identificación

En ambos escenarios anteriores, GETVPN debe poder transmitir y recibir correctamente los paquetes UDP fragmentados para que COOP o GDOI vuelvan a funcionar correctamente. La fragmentación de IP puede ser un problema en algunos entornos de red. Por ejemplo, una red que consta de un plano de reenvío de ruta múltiple de igual coste (ECMP) y algunos dispositivos del plano de reenvío requieren un reensamblado virtual de los paquetes IP fragmentados, como el reensamblado de fragmentación virtual (VFR).

Para identificar el problema, verifique los errores de reensamblado en el dispositivo donde se sospecha que los paquetes UDP 848 fragmentados no se reciben correctamente:

```
KS1#show ip traffic | section Frags
Frags: 10 reassembled, 3 timeouts, 0 couldn't reassemble
0 fragmented, 0 fragments, 0 couldn't fragment
```

Si los tiempos de espera de reensamblado continúan aumentando, utilice el comando **debug ip error** para confirmar si la caída es parte del flujo de paquetes de rekey/COOP. Una vez confirmada, se debe realizar la resolución de problemas de reenvío IP normal para aislar el dispositivo exacto en el plano de reenvío que podría haber descartado los paquetes. Algunas de las herramientas más utilizadas son:

- Captura de paquete
- Estadísticas de reenvío de tráfico

- Estadísticas de funciones de seguridad (Firewall, IPS)
- estadísticas VFR

#### Problemas de Interoperabilidad de GDOI

A lo largo de los años se han encontrado varios problemas de interoperabilidad con GETVPN, y es fundamental observar las versiones de Cisco IOS entre KS y GM y entre los KS para los problemas de interoperabilidad.

Otros problemas conocidos de interoperabilidad con GETVPN son:

- Comprobación del relé del plano de control
- Cambio de comportamiento de clave nueva de KEK de GETVPN
- Id. de bug Cisco CSCub42920 (GETVPN: KS no puede validar el hash en ACK de nueva clave de versiones GM anteriores)
- El Id. de bug Cisco CSCuw48400 (GetVPN GM no puede registrarse o falla la clave - sig-hash > SHA-1 predeterminado)
- Id. de error de Cisco CSCvg19281 ( Múltiples caídas de GETVPN GM después de la migración al nuevo par KS ; si una versión GM es anterior a 3.16 y KS se actualiza de un código anterior a 3.16 o posterior, este problema puede ocurrir)

##### Procedimiento de actualización de GETVPN IOS

Este procedimiento de actualización de Cisco IOS debe seguirse cuando se necesita realizar una actualización de código de Cisco IOS en un entorno GETVPN:

1. Actualice primero un KS secundario y espere hasta que se complete la elección de COOP KS.
2. Repita el paso 1 para todos los KS secundarios.
3. Actualice el KS primario.
4. Actualizar los GM.

## Solución de problemas del plano de datos GETVPN

En comparación con los problemas del plano de control, los problemas del plano de datos GETVPN son problemas en los que el GM tiene la política y las claves para realizar el cifrado y el descifrado del plano de datos, pero por alguna razón el flujo de tráfico de extremo a extremo no funciona. La mayoría de los problemas del plano de datos para GETVPN se relacionan con el reenvío de IPSec genérico y no son específicos de GETVPN. Por lo tanto, la mayor parte del enfoque de solución de problemas descrito aquí se aplica también a los problemas genéricos del plano de datos IPsec.

Con los problemas de cifrado (tanto en túneles basados en grupo como en túneles de par), es importante solucionar el problema y aislar el problema en una parte determinada del datapath. Específicamente, el enfoque de solución de problemas que se describe aquí tiene como objetivo ayudarle a responder a estas preguntas:

- ¿Qué dispositivo es el culpable: el router de cifrado o el router de descifrado?
- ¿En qué dirección está ocurriendo el problema: el ingreso o la salida?

## Herramientas de resolución de problemas del plano de datos GETVPN

La resolución de problemas del plano de datos IPSec es muy diferente de la del plano de control. Con el plano de datos, normalmente no hay depuraciones que pueda ejecutar o, al menos, ejecutar de forma segura en un entorno de producción. Por lo tanto, la resolución de problemas depende en gran medida de diferentes contadores y estadísticas de tráfico que pueden ayudar a rastrear el paquete a lo largo de una trayectoria de reenvío. La idea es ser capaz de desarrollar un conjunto de puntos de control para ayudar a aislar donde los paquetes pueden ser descartados, como se muestra aquí:


Estas son algunas de las herramientas de depuración del plano de datos:

- Listas de acceso
- Contabilización de Precedencia de IP
- Netflow
- Contadores de interfaz
- Contadores criptográficos
- Contadores de caídas globales y por función de IP Cisco Express Forwarding (CEF)
- Captura de paquetes integrada (EPC)
- Depuraciones del plano de datos (depuraciones de CEF y paquetes IP)

Los puntos de control de la ruta de datos de la imagen anterior se pueden validar con estas herramientas:

### Cifrado de GM

- Interfaz LAN de ingreso
  - ACL de entrada
  - NetFlow de ingreso
  - Captura de paquetes integrada
  - Contabilidad de precedencia de entrada

- Motor criptográfico
  - **show crypto ipsec sa**
  - **show crypto ipsec sa detail**
  - **show crypto engine Accelerator statistics**

- Interfaz WAN de salida
  - NetFlow de salida
  - Captura de paquetes integrada
  - Contabilidad de precedencia de salida

### Descifrado de GM

- Interfaz WAN de entrada
  - ACL de entrada
  - NetFlow de ingreso
  - Captura de paquetes integrada
  - Contabilidad de precedencia de entrada

- Motor criptográfico
  - **show crypto ipsec sa**
  - **show crypto ipsec sa detail**
  - **show crypto engine Accelerator statistics**

- Interfaz LAN de salida
  - NetFlow de salida
  - Captura de paquetes integrada

El trayecto de retorno sigue el mismo flujo de tráfico. Las secciones siguientes tienen algunos ejemplos de estas herramientas de plano de datos en uso.

### Contadores de cifrado/descifrado

Los contadores de cifrado/descifrado en un router se basan en un flujo IPsec. Desafortunadamente, esto no funciona bien con GETVPN, ya que GETVPN normalmente implementa una política de cifrado "permit ip any any" que cifra todo. Por lo tanto, si el problema sólo ocurre para algunos de los flujos y no todos, estos contadores pueden ser algo difíciles de usar para evaluar correctamente si los paquetes están cifrados o descifrados cuando hay suficiente tráfico de fondo significativo que funcione.

```
GM1#show crypto ipsec sa | in encrypt|decrypt
#pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
```

### Netflow

Netflow se puede utilizar para monitorear tanto el tráfico de entrada como de salida en ambos GM. Tenga en cuenta que con GETVPN **permit ip any any** policy, el tráfico cifrado se agregará y no proporciona la información por flujo. La información por flujo entonces deberá recopilarse con el marcado DSCP/precedencia descrito más adelante.

En este ejemplo, el netflow para un ping de recuento de 100 de un host detrás de GM1 a un host detrás de GM2 se muestra en los diversos puntos de control.

### Cifrado de GM

Configuración de Netflow:

```
interface Ethernet0/0
description LAN
ip address 192.168.13.1 255.255.255.0
ip flow ingress
ip pim sparse-dense-mode
!
interface Serial1/0
```

```
description WAN interface
ip address 10.1.13.2 255.255.255.252
ip flow egress
ip pim sparse-dense-mode
crypto map gm1map
```

Salida de Netflow:

```
GM1#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Et0/0 192.168.13.2 Se1/0* 192.168.14.2 32 8DE1 6523   100
Et0/0 192.168.13.2 Se1/0 192.168.14.2 01 0000 0800   100
GM1#
```

> **Nota:** En la salida anterior, * denota tráfico de salida. La primera línea muestra el tráfico cifrado de salida (con protocolo 0x32 = ESP) fuera de la interfaz WAN y la segunda línea ingresa tráfico ICMP que llega a la interfaz LAN.

### Descifrado de GM

Configuración:

```
interface Ethernet0/0
description LAN interface
ip address 192.168.14.1 255.255.255.0
ip flow egress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.14.2 255.255.255.252
ip flow ingress
ip pim sparse-dense-mode
crypto map gm1map
```

Salida de Netflow:

```
GM2#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Se1/0 192.168.13.2 Et0/0 192.168.14.2 32 8DE1 6523   100
Se1/0 192.168.13.2 Et0/0* 192.168.14.2 01 0000 0800   100
GM2#
```

### Marcación de precedencia DSCP/IP

El desafío de solucionar un problema de cifrado es que una vez que el paquete se cifra, se pierde visibilidad en la carga útil, que es lo que se supone que debe hacer el cifrado, y eso dificulta el seguimiento del paquete para un flujo IP determinado. Hay dos maneras de abordar esta limitación cuando se trata de resolver un problema de IPSec:

- Utilice ESP-NULL como transformación IPsec. IPSec todavía realiza la encapsulación ESP pero no se aplica ningún cifrado a la carga útil, por lo que son visibles en una captura de paquetes.
- Marque un flujo IP con un único punto de código de servicios diferenciados (DSCP)/marcado de precedencia basado en sus características de L3/L4.

ESP-NULL requiere cambios en ambos puntos finales del túnel y a menudo no se permite según

la política de seguridad del cliente. Por lo tanto, Cisco normalmente recomienda el uso de marcado DSCP/precedencia en su lugar.

#### Tabla de referencia de DSCP/Precedencia

| ToS (hexadecimal) | ToS(Decimal) | Precedencia IP | DSCP | Binario |
|---|---|---|---|---|
| 0xE0 | 224 | 7 Control de red | 56 CS7 | 11100000 |
| 0xC0 | 192 | 6 Control entre redes | 48 CS6 | 11000000 |
| 0xB8 | 184 | 5 Críticos | 46 EF | 10111000 |
| 0xA0 | 160 | | 40 CS5 | 10100000 |
| 0x88 | 136 | 4 anulación de Flash | 34 AF41 | 10001000 |
| 0x80 | 128 | | 32 CS4 | 10000000 |
| 0x68 | 104 | 3 Flash | 26 AF31 | 01101000 |
| 0x60 | 96 | | 24 CS3 | 01100000 |
| 0x48 | 72 | 2 Inmediato | 18 AF21 | 01001000 |
| 0x40 | 64 | | 16 CS2 | 01000000 |
| 0x20 | 32 | 1 prioridad | 8 CS1 | 00100000 |
| 0x00 | 0 | 0 Rutina | 0 Dflt | 00000000 |

#### Marcar paquetes con DSCP/precedencia

Estos métodos se utilizan normalmente para marcar los paquetes con las marcas de DSCP/precedencia específicas.

### PBR

```
interface Ethernet1/0
ip policy route-map mark
!
access-list 150 permit ip host 172.16.1.2 host 172.16.254.2
!
route-map mark permit 10
match ip address 150
set ip precedence flash-override
```

### MQC

```
class-map match-all my_flow
match access-group 150
!
policy-map marking
class my_flow
set ip precedence 4
!
interface Ethernet1/0
service-policy input marking
```

### Ping del router

```
GM1-host#ping ip
Target IP address: 192.168.14.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
```

```
Extended commands [n]: y
Source address or interface:
Type of service [0]: 136
...
<snip>
```

> **Nota:** Siempre es una buena idea monitorear el flujo de tráfico normal y el perfil DSCP/precedencia antes de aplicar la marcación para que el flujo de tráfico marcado sea único.

#### Supervisar paquetes marcados

### Contabilización de Precedencia de IP

```
interface Ethernet0/0
ip address 192.168.1.2 255.255.255.0
ip accounting precedence input
```

```
middle_router#show interface precedence
Ethernet0/0
Input
Precedence 4: 100 packets, 17400 bytes
```

### ACL de interfaz

```
middle_router#show access-list 144
Extended IP access list 144
10 permit ip any any precedence routine
20 permit ip any any precedence priority
30 permit ip any any precedence immediate
40 permit ip any any precedence flash
50 permit ip any any precedence flash-override (100 matches)
60 permit ip any any precedence critical
70 permit ip any any precedence internet (1 match)
80 permit ip any any precedence network
```

### Captura de paquetes integrada

La captura de paquetes integrada (EPC) es una herramienta útil para capturar paquetes en el nivel de interfaz con el fin de identificar si un paquete ha alcanzado un dispositivo específico. Recuerde que EPC funciona bien para el tráfico de texto sin cifrar, pero puede ser un desafío cuando los paquetes capturados se cifran. Por lo tanto, las técnicas como el marcado de precedencia/DSCP discutidas anteriormente u otros caracteres IP, como la longitud del paquete IP, deben utilizarse junto con EPC para que la resolución de problemas sea más eficaz.

### Seguimiento de paquetes Cisco IOS-XE

Esta es una función útil para rastrear la trayectoria de reenvío de funciones en todas las plataformas que ejecutan Cisco IOS-XE, como CSR1000v, ASR1000 e ISR4451-X.

### Problemas comunes del plano de datos GETVPN

La resolución de problemas del plano de datos IPsec para GETVPN no difiere en gran medida de

la resolución de problemas tradicionales del plano de datos IPsec punto a punto, con dos excepciones debido a estas propiedades únicas del plano de datos de GETVPN.

#### Falla Anti-Replay Basada en Tiempo

En una red GETVPN, las fallas de TBAR a menudo pueden ser difíciles de resolver, ya que ya no hay túneles por pares. Para resolver problemas de fallas de GETVPN TBAR, complete estos pasos:

1. Identifique qué paquete se descarta debido a una falla de TBAR y posteriormente identifique el GM de cifrado.

   Antes de la versión 15.3(2)T, el syslog de falla TBAR no imprimió la dirección de origen del paquete fallido, por lo que esto hace muy difícil identificar qué paquete falló. Esto se ha mejorado significativamente en la versión 15.3(2)T y posteriores, donde Cisco IOS imprime esto:

   ```
   %CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
   connection id=13, sequence number=1

   %GDOI-4-TIMEBASED_REPLAY_FAILED: An anti replay check has failed in group G1:
   my_pseudotime = 620051.84 secs, peer_pseudotime = 619767.09 secs, replay_window =
   4 (sec), src_ip = 192.168.13.2, dst_ip = 192.168.14.2
   ```

   También se implementó un historial TBAR en esta versión:

   ```
   GM2#show crypto gdoi gm replay
   Anti-replay Information For Group G1:
   Timebased Replay:
   Replay Value : 621388.66 secs
   Input Packets : 0 Output Packets : 0
   Input Error Packets : 2 Output Error Packets : 0
   Time Sync Error : 0 Max time delta : 0.00 secs


   TBAR Error History (sampled at 10pak/min):
   19:29:32.081 EST Wed Nov 13 2013: src=192.168.13.2; my_pst=620051.84 secs;
   peer_pst=619767.09 secs; win=4
   ```

   **Nota:** Las mejoras mencionadas anteriormente han sido implementadas en Cisco IOS-XE por el ID de bug Cisco CSCun49335 y en Cisco IOS por el ID de bug Cisco CSCub91811. Para las versiones de Cisco IOS que no tienen esta función, **debug crypto gdoi gm replay detail** también puede proporcionar esta información, aunque este debug imprime la información TBAR para todo el tráfico (no sólo los paquetes descartados debido a una falla de TBAR), por lo que puede que no sea factible ejecutarse en un entorno de producción.

   ```
   GDOI:GM REPLAY:DET:(0):my_pseudotime is 621602.30 (secs), peer_pseudotime is 621561.14
   (secs), replay_window is 4 (secs), src_addr = 192.168.14.2, dest_addr = 192.168.13.2
   ```

2. Una vez que se identifica el origen del paquete, debería poder encontrar el GM de cifrado. A continuación, se debe supervisar la indicación de pseudotimestamp tanto en los GM de

cifrado como de descifrado para detectar cualquier posible desviación de pseudotime. La mejor manera de hacerlo sería sincronizar tanto los GM como los KS con los NTP y recopilar periódicamente la información sobre el pseudotime con un reloj del sistema de referencia en todos ellos para determinar si el problema es causado por la desviación del reloj en los GM.

GM1

```
GM1#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.469 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value             : 625866.26 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 0 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

GM2

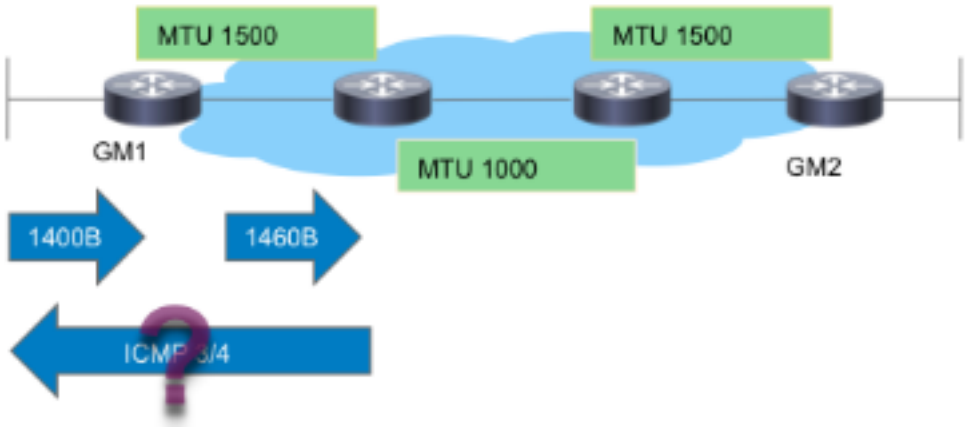
```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value             : 625866.51 secs
Input Packets : 4 Output Packets : 4
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

En el ejemplo anterior, si el pseudotime (como indica Replay Value) es significativamente diferente entre los GM cuando los resultados se capturan con el mismo tiempo de referencia, el problema puede atribuirse a la desviación del reloj.

> **Nota:** En la plataforma Cisco Aggregated Services Router serie 1000, debido a la arquitectura de la plataforma, la ruta de datos del procesador de flujo Quantum (QFP) se refiere en realidad al reloj de pared para contar las marcas de pseudotime. Esto ha creado problemas con TBAR cuando el tiempo del reloj de la pared cambia debido a la sincronización de NTP. Este problema se documenta con el ID de bug de Cisco CSCum37911.

#### PMTUD y Preservación del encabezado GETVPN

Con GETVPN, Path MTU Discovery (PMTUD) no funciona entre los GM de cifrado y descifrado, y los paquetes grandes con el conjunto de bits Don't Fragment (DF) pueden quedar en la lista negra. La razón por la que esto no funciona se debe a la Preservación del encabezado GETVPN, donde las direcciones de origen/destino de datos se conservan en el encabezado de encapsulación ESP. Esto se ilustra en esta imagen:




Como muestra la imagen, PMTUD se rompe con GETVPN con este flujo:

1. El paquete de datos de gran tamaño llega con el GM1 de cifrado.
2. El paquete ESP post-encripción se reenvía fuera de GM1 y se entrega hacia el destino.
3. Si hay un link de tránsito con una MTU IP de 1400 bytes, el paquete ESP se descartará y se enviará un mensaje de paquete ICMP 3/4 demasiado grande hacia el origen del paquete, que es el origen del paquete de datos.
4. El paquete ICMP3/4 se descarta debido a que el ICMP no se excluye de la política de encripción de GETVPN, o bien es descartado por el host final ya que no sabe nada acerca del paquete ESP (carga útil no autenticada).

En resumen, PMTUD no funciona con GETVPN hoy. Para solucionar este problema, Cisco recomienda estos pasos:

1. Implemente "ip tcp adjust-mss" para reducir el tamaño del segmento de paquete TCP para acomodar la sobrecarga de cifrado y la MTU de trayectoria mínima en la red de tránsito.
2. Borre el bit DF en el paquete de datos a medida que llegan en el GM de cifrado para evitar PMTUD.

### Problemas genéricos del plano de datos IPsec

La mayor parte de la solución de problemas del plano de datos IPsec es como la solución de problemas de túneles IPsec punto a punto tradicionales. Uno de los problemas comunes es %CRYPTO-4-RECVD_PKT_MAC_ERR. Consulte Mensaje de Error de Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" Resolución de Problemas de Ping Loss Over IPsec Tunnel para obtener más detalles de troubleshooting.

### Problemas conocidos

Este mensaje se puede generar cuando se recibe un paquete IPSec que no coincide con un SPI en la SADB. Consulte Cisco bug ID CSCtd47420 - GETVPN - CRYPTO-4-RECVD_PKT_NOT_IPSEC informado para pkt que no coincide con el flujo. Se presenta un ejemplo a continuación:

```
%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet. (ip)
vrf/dest_addr= /192.168.14.2, src_addr= 192.168.13.2, prot= 50
```

Este mensaje debe ser %CRYPTO-4-RECVD_PKT_INV_SPI, que es lo que se informa para IPsec

tradicional así como en algunas plataformas de hardware como ASR. Este problema superficial fue corregido por el ID de bug de Cisco CSCup80547: Error al informar de CRYPTO-4-RECVD_PKT_NOT_IPSEC para el PAK ESP.

> **Nota:** Estos mensajes pueden aparecer a veces debido a otro error de GETVPN CSCup34371: GETVPN GM deja de descifrar el tráfico después de que TEK vuelva a marcar.

En este caso, el GM no puede descifrar el tráfico GETVPN, aunque tiene una SA IPsec válida en la SADB (se reescribe la SA). El problema desaparece tan pronto como caduca la SA y se elimina de la SADB. Este problema provoca una interrupción significativa, porque la reclave TEK se realiza por adelantado. Por ejemplo, la interrupción puede ser de 22 minutos en el caso de una duración TEK de 7200 segundos. Consulte la descripción del bug para ver la condición exacta que debe cumplirse para encontrar este bug.

# Resolución de Problemas de GETVPN en Plataformas que Ejecutan Cisco IOS-XE

## Comandos para resolución de problemas

Las plataformas que ejecutan Cisco IOS-XE tienen implementaciones específicas de la plataforma y a menudo requieren depuración específica de la plataforma para problemas de GETVPN. A continuación se muestra una lista de comandos que se utilizan habitualmente para resolver problemas de GETVPN en estas plataformas:

**show crypto eli all**

**show platform software ipsec policy statistics**

**show platform software ipsec fp active Inventory**

**show platform hardware qfp active feature ipsec spd all**

**show platform hardware qfp active statistics drop clear**

**show platform hardware qfp active feature ipsec data drop clear**

**show crypto ipsec sa**

**show crypto gdoi**

**show crypto ipsec internal**

**debug crypto ipsec**

**debug crypto ipsec error**

**debug crypto ipsec state**

**debug crypto ipsec message**

**debug crypto ipsec hw-req**

**debug crypto gdoi gm infra detail**

**debug crypto gdoi gm rekey detail**

### Problemas comunes de ASR1000

#### Falla de instalación de la política IPsec (registro continuo)

Un GM ASR1000 podría continuar registrándose en el Servidor de claves si el motor de criptografía no soporta la política o el algoritmo IPsec recibidos. Por ejemplo, en las plataformas ASR basadas en Nitrox (como ASR1002), las políticas Suite-B o SHA2 no se soportan y esto puede causar los síntomas de reregistro continuo.

## Problemas comunes de migración/actualización

### Limitación del TBAR ASR 1000

En la plataforma ASR1000, el ID de bug de Cisco CSCum37911 corrección introdujo una limitación en esta plataforma donde el tiempo TBAR de menos de 20 segundos no es soportado. Vea Restricciones para GETVPN en IOS-XE.

Este error de mejora se ha abierto para levantar esta restricción, Id. de bug Cisco CSCuq25476 - ASR1k necesita soportar un tamaño de ventana TBAR GETVPN de menos de 20 segundos.

**Actualización:** Esta restricción se ha levantado con la corrección para el Id. de bug Cisco CSCur57558 y ya no es una limitación en el código XE3.10.5, XE3.13.2 y posterior.

Tenga en cuenta que, para un GM que se ejecute en plataformas Cisco IOS-XE (ASR1k o ISR4k), se recomienda encarecidamente que el dispositivo ejecute una versión con la corrección para este problema si TBAR está habilitado; Id. de bug Cisco CSCut91647 - GETVPN en IOS-XE: GM descarta los paquetes incorrectamente debido a una falla de TBAR.

### Problema de clasificación de ISR4x00

Se encontró una regresión en la plataforma ISR4x00 donde se ignoran las políticas de negación. Para obtener más información, vea Cisco bug ID CSCut14355 - GETVPN - ISR4300 GM ignora la política de negación.

## Información Relacionada

- VPN de transporte cifrado de grupo (GET VPN) - Cisco Systems
- Soporte Técnico y Documentación - Cisco Systems