# Guía del Troubleshooting GETVPN

## Contenido

# Introducción

Este documento se piensa para presentar una metodología de Troubleshooting estructurada y las herramientas útiles para ayudar a identificar y a aislar los problemas cifrados grupo del transporte VPN (GETVPN) y a proporcionar las Soluciones posibles.

# Prerrequisitos

## Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- GETVPN
  Guía de configuración oficial GETVPN
  Guía de diseño e implementación oficial GETVPN

- Uso del servidor de Syslog

## Componentes Utilizados

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

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.

# Metodología de Troubleshooting GETVPN

Como con la mayoría del troubleshooting de los problemas de la tecnología compleja, la clave es poder aislar el problema a una característica, a un subsistema, o a un componente específico. La solución GETVPN se comprende de varios componentes de la característica, específicamente:

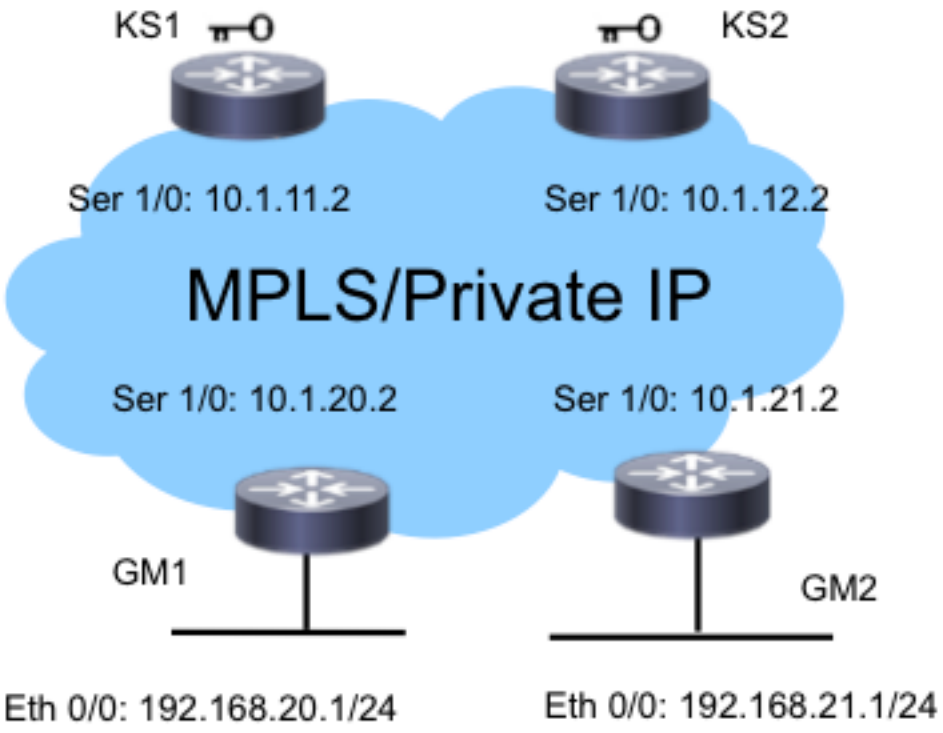
- Internet Key Exchange (IKE) - Utilizado entre el miembro del grupo (GM) y el servidor dominante (KS), y entre el protocolo cooperativo (GALLINERO) KSs para autenticar y proteger el avión del control.
- Agrupe el dominio de la interpretación (GDOI) - protocolo usado para el KS para distribuir las claves del grupo y proporcionar el servicio fundamental por ejemplo reintroduzca a todo el GMs.
- GALLINERO - Protocolo usado para el KSs para comunicar con uno a y proporcionar la Redundancia.
- Preservación de la encabezado - IPSec en el modo túnel que preserva la encabezado de

paquete de datos original para la salida del tráfico de extremo a extremo.
- El tiempo basó la Anti-respuesta (TBAR) - Mecanismo de detección de la respuesta usado en un entorno de la clave del grupo.

También proporciona un conjunto extenso de las herramientas de Troubleshooting para facilitar el proceso del Troubleshooting. Es importante entender cuáles de estas herramientas están disponibles, y cuando son apropiados para cada tarea de Troubleshooting. Al resolver problemas, es siempre una buena idea comenzar con los menos métodos intrusos para no afectar el entorno de producción negativamente. La clave a este troubleshooting estructurado es poder romper el problema abajo a un control o al problema plano de los datos. Usted puede hacer esto si usted sigue el protocolo o el flujo de datos y utiliza las diversas herramientas presentadas aquí para punto de verificación las.

## Topología de la referencia

Esta topología y el esquema de direccionamiento 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 KS2 y GM2 no se incluyen aquí para la brevedad.

## Terminología

- **KS** - Servidor dominante
- **GM** - Miembro del grupo
- **GALLINERO** - Protocolo cooperativo
- **TBAR** - El tiempo basó la Anti-respuesta
- **KEK** - Clave de encripción de claves
- **TEK** - Clave de encripción del tráfico

## Preparación de la instalación de explotación forestal y otras mejores prácticas

Antes de que usted comience a resolver problemas, asegúrese de que usted haya preparado la instalación de explotación forestal según lo descrito aquí. Algunas mejores prácticas también se enumeran aquí:

- Marque la cantidad de memoria libre del router, y el **debugging guardada en la memoria intermedia del registro de la** configuración a un valor grande (10 MB o más si es posible).

- Inhabilite el registro a la consola, al monitor, y a los servidores de Syslog.

- Extraiga el contenido de memoria intermedia de registro con el **comando show log** a intervalos regulares, cada 20 minutos a una hora, para prevenir la pérdida del registro debida mitigar la reutilización.

- Sea cual sea sucede, ingrese el **comando show tech de** GMs y de KSs afectados, y examine la salida del **comando show ip route** en global y cada ruteo virtual y expedición (VRF) implicaron, si se requieren ningunos.

- Utilice el Network Time Protocol (NTP) para sincronizar el reloj entre todos los dispositivos se hagan el debug de que. Habilite los grupos fecha/hora del milisegundo (milisegundo) para el debug y los mensajes del registro:
```
service timestamps debug datetime msec
service timestamps log datetime msec
```
- Aseegurese las salidas del comando show son con impresión horaria.
```
Router#terminal exec prompt timestamp
```

- Cuando usted recoge las salidas del comando show para el control acepillan los eventos o los contadores planos de los datos, recogen siempre las iteraciones múltiples de la misma salida.

# Problemas del avión del control del Troubleshooting GETVPN

Controle el avión significa todos los eventos del protocolo que llevaron a la directiva y a la creación de la asociación de seguridad (SA) en el GM de modo que estén listos para cifrar y para desencriptar el tráfico del plano de los datos. Algunos de los puntos de verificación dominantes en el avión del control GETVPN son:


## Controle las mejores prácticas planas del debugging

Estas mejores prácticas del troubleshooting no son específico GETVPN; se aplican a casi cualquier debugging del avión del control. Es crítico seguir estas mejores prácticas para asegurar la mayoría del Troubleshooting eficaz:

- Apague el registro de la consola y utilice memoria intermedia de registro o el Syslog para recoger los debugs.
- Utilice el NTP para sincronizar los relojes del router en todos los dispositivos se hacen el debug de que.
- Habilite el milisegundo timestamping para el debug y los mensajes del registro:
  ```
  service timestamp debug datetime msec
  service timestamp log datetime msec
  ```
- Aseegurese las salidas del comando show son con impresión horaria para poderlas correlacionar con la salida de los debugs:
  ```
  terminal exec prompt timestamp
  ```
- Utilice el debugging condicional en un entorno de la escala si es posible.

## Herramientas de Troubleshooting del avión del control GETVPN

### Comandos show GETVPN

Como regla general, éstas son las salidas de comando que usted debe recoger para casi todos los problemas 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 isakmp sa
```

```
show crypto gdoi
show crypto gdoi gm
show crypto gdoi gm rekey
```

## Mensajes de Syslog GETVPN

GETVPN proporciona un conjunto extenso de los mensajes de Syslog para los eventos y las condiciones de error significativos del protocolo. El Syslog debe siempre ser el primer lugar a mirar cuando usted realiza el troubleshooting GETVPN.

### Mensajes de Syslog comunes KS

| Mensajes de Syslog | Explicación |
|---|---|
| *COOP_CONFIG_MISMATCH* | La configuración entre el servidor de la Clave primaria y el servidor de la C secundaria se une mal. |
| *COOP_KS_ELECTION* | El servidor dominante local ha ingresado el proceso de elección en un gru |
| *COOP_KS_REACH* | El accesibilidad entre los servidores dominantes cooperativos configurado restablece. |
| *COOP_KS_TRANS_TO_PRI* | **El servidor dominante local transitioned a una función primaria de ser un servidor secundario en un grupo.** |
| *COOP_KS_UNAUTH* | Un servidor remoto autorizado intentó entrar en contacto el servidor domin local en un grupo, que podría ser considerado un evento hostil. |
| *COOP_KS_UNREACH* | **El accesibilidad entre los servidores dominantes cooperativos configurado pierde, que se podrían considerar un evento hostil.** |
| *KS_GM_REVOKED* | Durante reintroduzca el protocolo, un miembro desautorizado intentado pa unirse a un grupo, que podría ser considerado un evento hostil. |
| *KS_SEND_MCAST_REKEY* | **Enviando el Multicast reintroduzca.** |
| *KS_SEND_UNICAST_REKEY* | **Enviando el unicast reintroduzca.** |
| *KS_UNAUTHORIZED* | Durante el Registration Protocol GDOI, un miembro desautorizado intentó unirse a un grupo, que podría ser considerado un evento hostil. |
| *UNAUTHORIZED_IPADDR* | El pedido de inscripción fue caído porque el dispositivo solicitante no fue autorizado para unirse a al grupo. |

### Mensajes de Syslog comunes GM

| Mensajes de Syslog | Explicación |
|---|---|
| *GM_CLEAR_REGISTER* | El comando **crypto claro del gdoi** ha sido ejecutado por el miembro del g local. |
| *GM_CM_ATTACH* | Una correspondencia de criptografía se ha asociado para el miembro de grupo local. |
| *GM_CM_DETACH* | Una correspondencia de criptografía se ha separado para el grupo loca member.& |
| *GM_RE_REGISTER* | **IPSec SA creado para un grupo pudo haber sido expirado o haber sido borrado. Necesidad de reregistrar al servidor dominante.** |
| *GM_RECV_REKEY* | **Rekey recibió.** |
| *GM_REGS_COMPL* | **Registro completo.** |
| *GM_REKEY_TRANS_2_MULTI* | El miembro del grupo tiene transitioned de usar un unicast para reintrod el mecanismo a usar un mecanismo del Multicast. |
| *GM_REKEY_TRANS_2_UNI* | El miembro del grupo tiene transitioned de usar un Multicast para reintro el mecanismo a usar un mecanismo del unicast. |
| *PSEUDO_TIME_LARGE* | Un miembro del grupo ha recibido un pseudotime con un valor que es e gran parte diferente de su propio pseudotime. |
| *REPLAY_FAILED* | Un miembro del grupo o un servidor de la clave ha fallado un control de |

anti-respuesta.

Nota: Los mensajes resaltados en el rojo son los mensajes mas comunes o más significativos considerados en un entorno GETVPN.

## Debugs Crypto y GDOI globales

Se dividen los debugs GETVPN:

1. Primero por el dispositivo en el cual usted 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 usted está resolviendo problemas. `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. Tercero por el nivel de debugging que necesita ser habilitado. En la versión 15.1(3)T y posterior, todos los debugs de la característica GDOI fueron estandardizados para tener estos niveles de debug. Esto fue diseñada para ayudar a resolver problemas los entornos en grande GETVPN con bastante granularity del debugging. Cuando usted hace el debug de los problemas GETVPN, es importante utilizar el nivel de debug apropiado. Como regla general, el comienzo con el nivel de debug más bajo, eso es el nivel de error, y aumenta el granularity del debugging cuando está necesitado. `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
```

## Debugging condicional GDOI

En la versión 15.1(3)T y posterior del ® del Cisco IOS, el debugging condicional GDOI fue agregado para ayudar a resolver problemas GETVPN en un entorno en grande. Tan todo el Internet Security Association and Key Management Protocol (ISAKMP) y los debugs GDOI se pueden ahora accionar con un filtro condicional basado en el grupo o el IP Address de Peer. Para la mayoría de los problemas GETVPN, es bueno habilitar los debugs ISAKMP y GDOI con el filtro condicional apropiado, puesto que los debugs GDOI muestran solamente las operaciones GDOI-específicas. Para utilizar los debugs condicionales ISAKMP y GDOI, complete estos dos pasos simples:

1. Fije el filtro condicional.
2. Habilite el ISAKMP y el GDOI relevantes como de costumbre.

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 los debugs condicionales ISAKMP y GDOI, para coger los mensajes del debug que no pudieron tener la información condicional del filtro, por ejemplo la dirección IP en la trayectoria del debug, el indicador **incomparable** puede ser habilitada. Sin embargo, esto debe ser utilizada con cautela porque puede presentar una gran cantidad de información del debug.

## Trazas del evento GDOI

Esto fue agregada en la versión 15.1(3)T. El seguimiento de evento ofrece al peso ligero, siempre-en el seguimiento para los eventos significativos y los errores GDOI. Hay también seguimiento de la salida-trayectoria con el traceback habilitado para las condiciones de excepción. Las trazas del evento pueden proporcionar más información del historial de eventos GETVPN que los Syslog tradicionales.

Las trazas del evento GDOI se habilitan por abandono y se pueden extraer del búfer de traza con el comando de la uniforme-**traza del monitor de la demostración**.

```
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
```

La traza del trayecto de la salida proporciona la información detallada sobre la trayectoria de la salida, eso es excepción y condiciones de error, con la opción del traceback habilitada por abandono. El tracebacks se puede entonces utilizar para decodificar la secuencia exacta del código que ha llevado a la condición de la trayectoria de la salida. Utilice la opción del **detalle** para extraer el tracebacks del búfer de traza:

```
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 de búfer de traza predeterminado es 512 entradas, y éste no pudo ser bastante si el problema es intermitente. Para aumentar este tamaño predeterminado de la entrada de la traza, los parámetros de la configuración de la traza del evento se pueden cambiar como mostrado 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 verificación y problemas frecuentes del avión del control GETVPN

Aquí están algunos de los problemas del avión del control común para GETVPN. Para reiterar, el avión del control se define como todos los componentes de la característica GETVPN requeridos para habilitar el cifrado y el desciframiento del dataplane en el GMs. En un nivel elevado, esto requiere el registro acertado GM, la política de seguridad y la descarga SA/instalan, y KEK/TEK subsiguientes reintroducen.

### Configuración del GALLINERO y creación de la directiva

Para marcar y verificar que el KS ha creado con éxito la política de seguridad y el KEK/TEK asociado, ingresan:

```
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 directiva KS es cuando hay diversas directivas configuradas entre el KSs primario y secundario. Esto puede dar lugar al comportamiento imprevisible KS y este error será señalado:

```
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
```

No hay actualmente configuración automática sincroniza entre KSs primario y secundario, así que éstos deben ser rectificados manualmente.

Porque el GALLINERO es una configuración crítica (y casi siempre obligatoria) para GETVPN, es dominante aseegurarse los trabajos del GALLINERO correctamente y los papeles del GALLINERO KS están correctos:

```
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 funcional del GALLINERO, este flujo del protocolo debe ser observado:

### El intercambio IKE > el anuncio con las prioridades del GALLINERO intercambiaron > elección del GALLINERO > anuncio de primario a KS secundario (directiva, base de datos GM, y las claves)

Cuando el GALLINERO no funciona correctamente, o si hay una fractura del GALLINERO, tal como KSs múltiple se convierten los KS primarios, estos debugs se deben recoger para resolver problemas:

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

### Configuración IKE

El intercambio acertado IKE se requiere para GETVPN para asegurar el canal de control para la directiva subsiguiente y la descarga SA. En el final del intercambio acertado IKE, este se crea IKE SA:

```
GM1#show crypto isa 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#
```

> Nota: Una vez que el intercambio inicial IKE completa, las directivas subsiguientes y las claves **serán avanzadas del** KS al GM con el uso GDOI_REKEY SA. Tan hay ningún reintroduce para GDOI_REKEY SA cuando expiran; desaparecen cuando expiran sus cursos de la vida. Sin embargo, debe siempre haber GDOI_REKEY SA en el GM para que reciba reintroduce.

El intercambio IKE para GETVPN es no diferente del IKE usado en los túneles IPsec de punto a punto tradicionales, así que el método de Troubleshooting sigue siendo lo mismo. Estos debugs se deben recoger para resolver problemas los problemas de la 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)
```

### El registro, la descarga de la directiva, y el SA instalan

Una vez que la autenticación IKE tiene éxito, el GM se registra con el KS. Se espera que estos

mensajes de Syslog sean considerados cuando ocurre éste 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 directiva 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, los SA entrantes y salientes utilizan mismo SPI.

Con GETVPN el registro y la directiva instalan el tipo de problema, 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: Los debugs adicionales se pueden requerir dependiendo del resultado de estas salidas.

Puesto que el registro GETVPN ocurre típicamente inmediatamente después de la recarga GM, este script EEM pudo ser útil para recoger estos debugs:

```
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)
```

## Reintroduzca

Una vez que el GMs se registra al KS y la red GETVPN se configura correctamente, el KS primario es responsable del enviar reintroduce los mensajes a todo el GMs registrado a él. Los mensajes de la reintroducción se utilizan para sincronizar todas las directivas, claves, y pseudotimes en el GMs. Los mensajes de la reintroducción se pueden enviar con un unicast o un método del Multicast.

Este mensaje de Syslog se considera en el KS cuando se envía el mensaje de la reintroducción:

```
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)
```

En el GMs, éste es el Syslog se ve que cuando recibe la reintroducción:

```
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)
```

### El requisito del par clave RSA para reintroduce en KS

Reintroduzca las funciones requiere la presencia de claves RSA en el KS. El KS proporciona la clave pública del par clave RSA al GM a través de este canal seguro durante el registro. El KS entonces firma los mensajes GDOI enviados al GM con la clave del soldado RSA en el payload GDOI SIG. El GM recibe los mensajes GDOI y utiliza la clave del público RSA para verificar el mensaje. Los mensajes entre el KS y el GM se cifran con el KEK, que también se distribuye al GM durante el registro. Una vez que el registro es completo, subsiguiente reintroduce se cifran

con el KEK y se firman con la clave del soldado RSA.

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

```
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)
```

Cuando las claves no están presentes en el KS, el GM se registra por primera vez, pero el siguientes reintroducen fallan del KS. Las claves existentes en el GM expiran eventual, y reregistra otra vez.

```
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)
```

Puesto que el par clave RSA se utiliza para firmar los mensajes de la reintroducción, **DEBEN** ser lo mismo entre KSs primario y todo el secundario. Esto se asegura de que durante un error primario KS, reintroduzca enviado por un KS secundario (el nuevo KS primario) pueda todavía ser validado correctamente por el GMs. Cuando genera el par clave RSA en el KS primario, el par clave se debe crear con la opción **exportable** para poderlos exportar a todo el KSs secundario para cumplir este requisito.

#### Reintroduzca el troubleshooting

KEK/TEK reintroducen el error son uno de los problemas mas comunes GETVPN encontrados en los despliegues en clientes. El resolver problemas reintroduce los problemas debe seguir los pasos de la reintroducción según lo delineado aquí:

1. ¿Hizo reintroduce consiguieron enviado por el KS?

   Esto se puede marcar por un observion 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 reintroduce retransmitido es indicativo de reintroduce los paquetes de reconocimiento no recibidos por el KS y por lo tanto posible reintroduzca los problemas. Tenga presente que los GDOI reintroducen las aplicaciones UDP como mecanismo de transporte no fiable, así que algunos reintroducen los descensos pudieron ser esperados dependiendo de la confiabilidad de la red de transporte subyacente, pero una tendencia del aumento reintroduce las retransmisiones debe ser investigada siempre.

Un por-GM más detallado reintroduce las estadísticas puede también ser obtenido. Éste es típicamente el primer lugar para buscar el potencial reintroduce los problemas.

```
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. ¿Reintrodujo los paquetes consiguen entregado en la red de infraestructura subyacente?

   El Troubleshooting de IP estándar a lo largo del trayecto de reenvío de la reintroducción se debe seguir para asegurarse que los paquetes de la reintroducción no están caídos en el transit network entre KS y el GM. Algunas herramientas de Troubleshooting comunes usadas aquí son Listas de control de acceso (ACL), Netflow, y captura de paquetes de la entrada-salida en el transit network.

3. ¿Reintrodujo el alcance de los paquetes que el proceso GDOI para reintroduce el proceso?

   Marque el GM reintroducen las estadísticas:

```
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. ¿Reintrodujo la vuelta del paquete del acuse de recibo al KS?

   Siga los pasos 1 a 3 para rastrear el paquete del acuse de recibo de la reintroducción del GM al KS.

### Muticast reintroduce

El Multicast reintroduce es diferente del unicast reintroduce en estos aspectos:

- Puesto que el Multicast se utiliza para transportar éstos reintroducen los paquetes del KS al GMs, el KS no necesitan replicar los paquetes de la reintroducción sí mismo. El KS envía solamente una copia del paquete de la reintroducción, y él se replica en la red habilitada para multicast.
- No hay mecanismo del acuse de recibo para el Multicast reintroduce, así que si un GM no fuera recibir el paquete de la reintroducción, el KS no tendría ningún conocimiento de él, y por lo tanto nunca quitará un GM de su base de datos GM. Y porque no hay acuse de recibo, el KS retransmitirá siempre los paquetes de la reintroducción basados en su reintroduce la configuración de la retransmisión.

Lo más comúnmente posible - el Multicast considerado reintroduce el problema es cuando la reintroducción no se recibe en el GM. Podía haber varias posibles causas para esto, por ejemplo:

- Problema de la entrega del paquete dentro de la infraestructura de Multicast Routing
- El ruteo multicast de punta a punta no se habilita dentro de la red

El primer paso para resolver problemas un problema con el Multicast reintroduce es considerar si reintroduzca los trabajos cuando está conmutado del Multicast al método del unicast.

Una vez que usted identifica que el problema es específico al Multicast reintroduzca, verifique que KS envía la reintroducción a la dirección Multicast especificada.

```
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
```

Pruebe la Conectividad del Multicast entre el KS y el GM con una petición del Internet Control Message Protocol (ICMP) a la dirección Multicast. Todo el GMs que es parte del grupo de multidifusión debe contestar al ping. Asegúrese de que el ICMP esté excluido de la política de encripción 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 del Multicast falla, después el troubleshooting del Multicast debe ser realizado, que está fuera del alcance de este documento.

## Controle el control plano de la retransmisión

### Síntoma

Cuando los clientes actualizan su GM a una versión del nuevo Cisco IOS, puede ser que experimenten el KEK reintroducen los errores con este mensaje observado en el Syslog:

```
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
```

Este comportamiento es causado por un problema de interoperabilidad introducido con el control de la anti-respuesta que se agrega para los mensajes del avión del control. Específicamente, un KS que funciona con el más viejo código reajustará el KEK reintroduce el número de secuencia a 1, y esto será caída por el GM que funciona con el nuevo código cuando interpreta que como jugado de nuevo reintroduzca el paquete. Para más detalles, vea el Id. de bug Cisco CSCta05809 (GETVPN: Controle de plano GETVPN sensata jugar de nuevo), y restricciones de configuración GETVPN.

#### Antecedente

Con GETVPN, los mensajes del avión del control pueden llevar la información sensible al tiempo para proporcionar el servicio del control de la anti-respuesta del time basado. Por lo tanto, estos mensajes requieren la Protección Anti-Replay ellos mismos para asegurar el accruracy del tiempo. Estos mensajes son:

- **Reintroduzca los mensajes de** KS al GM
- **ENCIERRE los mensajes de anuncio** entre KSs

Como parte de esta implementación de la Protección Anti-Replay, los controles del número de secuencia fueron agregados para proteger los mensajes jugados de nuevo, así como un control del pseudotime cuando se habilita TBAR.

### Solución

Para resolver este problema, el GM y KS se deben actualizar a las versiones deL Cisco IOS después de que la característica del control de la respuesta del avión del control. Con el código del nuevo Cisco IOS, KS no reajusta el número de secuencia de nuevo a 1 para un KEK reintroduce, sino que por el contrario continúa utilizando el número de secuencia actual y reajusta solamente el número de secuencia para el TEK reintroduce.

Estas versiones deL Cisco IOS tienen las características del control de la respuesta:

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

#### Otros asuntos relacionados de la respuesta

- Falla debido del GALLINERO a los mensajes anuncio que fallan el control de la respuesta (Id. de bug Cisco CSCtc52655)

#### Errores de la respuesta del avión del control del debug

Para otros errores de la respuesta del avión del control, recoja esta información y aseegurese los tiempos son synched entre el KS y GM.

- Syslog del GM y de KS
- Debugs ISAKMP
- Debugs GDOI (reintroduzca y respuesta) de KS y del GM

## Controle los problemas planos de la fragmentación de paquetes

Con GETVPN, la fragmentación de paquetes plana del control es un problema frecuente, y puede manifestarse en uno de estos dos escenarios cuando los paquetes del avión del control son bastante grandes que requerirán fragmentación de IP:

- Paquetes del aviso del GALLINERO GETVPN
- GETVPN reintroducen los paquetes

### Paquetes del aviso del GALLINERO

Los paquetes del aviso del GALLINERO llevan la Información de la base de datos GM, y pueden crecer así grandes en un despliegue grande GETVPN. De la experiencia anterior, una red GETVPN que consiste en 1500+ GMs producirá los paquetes del aviso más grandes de 18024 bytes, que es el tamaño de memoria intermedia de gran tamaño predeterminado del Cisco IOS. Cuando sucede esto, el KS no puede afectar un aparato un buffer bastante grande para transmitir los paquetes anuncio con este error:

```
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
```

Para rectificar esta condición, se recomienda este ajuste de la memoria intermedia:

```
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
```

#### Reintroduzca los paquetes

GETVPN reintroducen los paquetes pueden también exceder el tamaño máximo típico de la unidad de la transición IP 1500 (MTU) cuando la política de encripción es grande, por ejemplo una directiva que consista en las líneas 8+ de las entradas de control de acceso (ACE) en el cifrado ACL.

#### Problema de fragmentación e identificación

En ambos escenarios previos, GETVPN debe poder transmitir correctamente y recibir los paquetes UDP hechos fragmentos para que el GALLINERO o GDOI reintroduzca para trabajar correctamente. Fragmentación de IP puede estar un problema en algunos entornos de red. Por ejemplo, una red que consiste en el avión multi de la expedición de la trayectoria del igual costo (ECMP), y algunos dispositivos en el avión de la expedición requieren el nuevo ensamble virtual de los paquetes del IP hechos fragmentos, tales como nuevo ensamble virtual de la fragmentación (VFR).

Para identificar el problema, marque los errores del nuevo ensamble en el dispositivo donde se sospecha que los paquetes hechos fragmentos UDP 848 no están recibidos 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 para reconstrucción continúan incrementando, utilice el **comando error del IP del debug** para confirmar si el descenso es parte del flujo de paquetes rekey/COOP. Una vez que está confirmado, reenvío de IP el resolver problemas normal se debe realizar para aislar el dispositivo exacto en el avión de la expedición que pudo haber caído los paquetes. Algunas herramientas de uso general incluyen:

- Captura de paquetes
- Estadísticas del reenvío de tráfico
- Estadísticas de la función de seguridad (Firewall, IPS)
- Estadísticas VFR

#### Problemas de interoperabilidad GDOI

Los diversos problemas de interoperabilidad se han encontrado con GETVPN a lo largo de los años, y es crítico notar las versiones del Cisco IOS Release entre KS y el GM y entre el KSs por problemas de interoperabilidad.

Otros problemas de interoperabilidad bien conocidos GETVPN son:

- Controle el control plano de la retransmisión
- GETVPN KEK reintroducen el cambio del comportamiento
- Id. de bug Cisco CSCub42920 - GETVPN: KS no puede validar el hash adentro reintroduce el ACK de las versiones anteriores GM
- Id. de bug Cisco CSCuw48400 (el GM de GetVPN incapaz de registrarse o de reintroducir falla - el SIG-hash > el valor por defecto el SHA-1)

##### Procedimiento de la actualización de IOS GETVPN

Este procedimiento de la actualización de Cisco IOS debe ser seguido cuando una actualización del código del Cisco IOS necesita ser realizada en un entorno GETVPN:

1. Actualice un KS secundario primero y espere hasta que se complete la elección del GALLINERO KS.
2. Relance Step1 para todo el KSs secundario.
3. Actualice el KS primario.
4. Actualice GMs.

## Resuelva problemas los problemas del avión de los datos GETVPN

Comparado para controlar los problemas planos, los problemas del avión de los datos GETVPN son los problemas donde el GM tiene la directiva y las claves para realizar el cifrado y el desciframiento del dataplane, pero por alguna razón el flujo del tráfico de extremo a extremo no trabaja. La mayor parte de los problemas del dataplane para GETVPN se relacionan con el IPSec genérico que remite, y no son específico GETVPN. Tan la mayor parte del método de Troubleshooting descrito aquí se aplica a los problemas genéricos del dataplane del IPSec también.

Con los problemas del cifrado (basado en el grupo o en parejas los túneles), es importante

resolver problemas el problema y aislar el problema a una parte determinada del datapath. Específicamente, el método de Troubleshooting descrito aquí se piensa para ayudarle a contestar a estas preguntas:

- ¿Qué dispositivo es el culpable - router de encripción o router que desencripta?
- ¿En qué dirección es el problema que sucede - ingreso o salida?

## Los datos GETVPN acepillan las herramientas de Troubleshooting

El troubleshooting del dataplane del IPSec es muy diferente de ése para el avión del control. Con el dataplane, no hay generalmente debugs que usted puede ejecutar, o por lo menos se ejecuta con seguridad en un entorno de producción. El troubleshooting confía tan pesadamente en los diversos contadores y estadísticas de tráfico que pueden ayudar a localizar el paquete a lo largo de un trayecto de reenvío. La idea es poder desarrollar un conjunto de los puntos de verificación para ayudar a aislar donde los paquetes se pudieron caer como se muestra aquí:


Aquí están las herramientas de debugging del avión de un ciertos datos:

- Listas de acceso
- Contabilización de Precedencia de IP
- Netflow
- Contadores de la interfaz
- Contadores Crypto
- Cisco Express Forwarding (CEF) IP global y contadores de caídas de la Por-característica
- Captura de paquetes integrada (EPC)
- Debugs del avión de los datos (paquete del IP y debugs CEF)

Los puntos de verificación en el datapath en la imagen anterior se pueden validar con estas herramientas:

### GM que cifra

- Interfaz LAN del ingreso
  - Entrada ACL
  - Netflow del ingreso
  - Captura de paquetes integrada
  - Contabilidad de precedencias de la entrada

- Motor de criptografía
  - **show crypto ipsec sa**
  - **muestre el detalle crypto IPSec sa**
  - **estadísticas del acelerador del show crypto engine**

- Interfaz de WAN de la salida
  - Netflow de la salida
  - Captura de paquetes integrada
  - Contabilidad de precedencias de la salida

**GM que desencripta**

- Interfaz de WAN del ingreso
  - Entrada ACL
  - Netflow del ingreso
  - Captura de paquetes integrada
  - Contabilidad de precedencias de la entrada

- Motor de criptografía
  - **show crypto ipsec sa**
  - **muestre el detalle crypto IPSec sa**
  - **estadísticas del acelerador del show crypto engine**

- Interfaz LAN de la salida
  - Netflow de la salida
  - Captura de paquetes integrada

El trayecto de retorno sigue el mismo flujo de tráfico. Las siguientes secciones tienen algunos ejemplos de estas herramientas del dataplane funcionando.

### Encripción/desencripción contadores

Encripción/desencripción contradice en un router se basan en un flujo del IPSec. Desafortunadamente esto no trabaja bien con GETVPN puesto que GETVPN despliega típicamente un “IP del permiso cualquier cualquier” política de encripción que cifre todo. Tan si el problema sucede solamente para algunos de los flujos y no de todos, estos contadores pueden ser algo difíciles de utilizar para evaluar correctamente si se cifran o se desencriptan los paquetes cuando hay bastante tráfico de fondo significativo que trabaja.

```
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

El Netflow se puede utilizar para monitorear el ingreso y el tráfico de salida en ambos GMs. Observe con el **IP del permiso** GETVPN **cualquier cualquier** directiva, el tráfico enrypted será agregado y no proporciona la información del por-flujo. la información del Por-flujo entonces necesitará ser recogida con la marca DSCP/precedence descrita más adelante.

En este ejemplo, el Netflow para un ping de 100 cuentas de un host detrás de GM1 a un host detrás de GM2 se muestra en los diversos puntos de verificación.

### GM que cifra

Configuración de flujo de red:

```
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
```

Netflow hecho salir:

```
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 el tráfico de salida. La primera línea muestra la interfaz de WAN de los del tráfico encriptado de la salida (con el protocolo 0x32 = ESP), y la segunda línea tráfico del ingreso ICMP que golpea la interfaz LAN.

### GM que desencripta

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
```

Netflow hecho salir:

```
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#
```

### Marca de la precedencia DSCP/IP

El desafío con resolver problemas un problema del cifrado es que una vez que se cifra el paquete usted pierde la visibilidad en el payload, que es lo que se supone el cifrado para hacer, y ése hace difícil localizar el paquete para un flujo determinado IP. Hay dos maneras de dirigir esta limitación cuando se trata de resolver problemas un problema del IPSec:

- El uso ESP-NULL como el IPSec transforma. El IPSec todavía realiza la encapsulación ESP pero el no encryption se aplica al payload, así que son visibles en una captura de paquetes.
- Marque un flujo IP con una marca única del Differentiated Services Code Point (DSCP) /precedence basada en sus características L3/L4.

ESP-NULL requieren los cambios en ambos puntos extremos del túnel y a menudo no se permiten basado en la política de seguridad del cliente. Por lo tanto, Cisco recomienda típicamente el uso de DSCP/precedence que marca en lugar de otro.

#### Gráfico de referencia DSCP/Precedence

| TOS (maleficio) | ToS(Decimal) | Precedencia IP | DSCP | Binario |
|---|---|---|---|---|
| 0xE0 | 224 | Control de red 7 | 56 CS7 | 11100000 |
| 0xC0 | 192 | Control de la red interna 6 | 48 CS6 | 11000000 |
| 0xB8 | 184 | 5 crítico | 46 EF | 10111000 |
| 0xA0 | 160 | | 40 CS5 | 10100000 |
| 0x88 | 136 | Anulación de Flash 4 | 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 rutinas | 0 Dflt | 00000000 |

#### Marque los paquetes con DSCP/Precedence

Estos métodos se utilizan típicamente para marcar los paquetes con las marcas específicas DSCP/Precedence.

### 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: Es siempre una buena idea monitorear el flujo de tráfico normal y perfil DSCP/precedence antes de que usted aplique la marca de modo que el flujo de tráfico marcado sea único.

#### Paquetes marcados del monitor

### 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
```

### Interfaz ACL

```
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 los paquetes en el nivel de la interfaz para identificar si un paquete ha alcanzado un dispositivo específico. Recuerde que los trabajos del EPC bien para el tráfico del texto claro, pero pueden ser un desafío cuando se cifran los paquetes capturados. Por lo tanto las técnicas como la marca DSCP/precedence discutida previamente u otros caracteres IP, tales como la longitud del paquete del IP, tienen que ser utilizados así como el EPC para hacer resolver problemas más eficaz.

### Traza del paquete del Cisco IOS XE

Esto es una función útil para localizar el trayecto de reenvío de la característica en todas las Plataformas que funcionen con el Cisco IOS XE, tal como CSR1000v, ASR1000, e ISR4451-X.

### Los datos GETVPN acepillan los problemas frecuentes

Resolver problemas el dataplane del IPSec para GETVPN es sobre todo no diferente de resolver problemas los problemas de punto a punto tradicionales del dataplane del IPSec, con dos excepciones debido a estas propiedades únicas del dataplane de GETVPN.

#### El tiempo basó el error de la Anti-respuesta

En una red GETVPN, los errores TBAR pueden a menudo ser difíciles de resolver problemas

puesto que hay no más en parejas túneles. Para resolver problemas los errores GETVPN TBAR, complete estos pasos:

1. Identifique qué paquete es caído debido al error TBAR e identifique posteriormente el GM que cifra.

   Antes de la versión 15.3(2)T, el Syslog del error TBAR no imprimió a la dirección de origen del paquete fallado, así que éste hace muy difícil identificar que el paquete falló. Esto se ha mejorado perceptiblemente en la versión 15.3(2)T y posterior, donde el Cisco IOS imprime esto:

```
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
```

   Un historial TBAR también fue implementado 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 previamente han sido implementadas desde entonces en el Cisco IOS XE por el Id. de bug Cisco CSCun49335 y en el Cisco IOS por el Id. de bug Cisco CSCub91811.

   Para las versiones deL Cisco IOS que no tenían esta característica, el **detalle de la respuesta gm del gdoi del debug crypto** puede también proporcionar esta información, aunque este debug imprima la información TBAR para todo el tráfico (no sólo caída los paquetes debido al error TBAR), así que puede ser que no sea posible ejecutarse en un entorno de producción.

```
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
```

2. La fuente del paquete se identifica una vez, usted debe poder encontrar el GM que cifra. Entonces, el pseudotimestamp en el GMs que cifra y que desencripta se debe monitorear para cualquier deriva potencial del pseudotime. La mejor manera de hacer esto sería sincronizar GMs y el KS al NTP y recoger periódicamente la información del pseudotime con un reloj del sistema de referencia en todos para determinar si el problema es causado por la posición oblicua del reloj en el GMs.

### 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

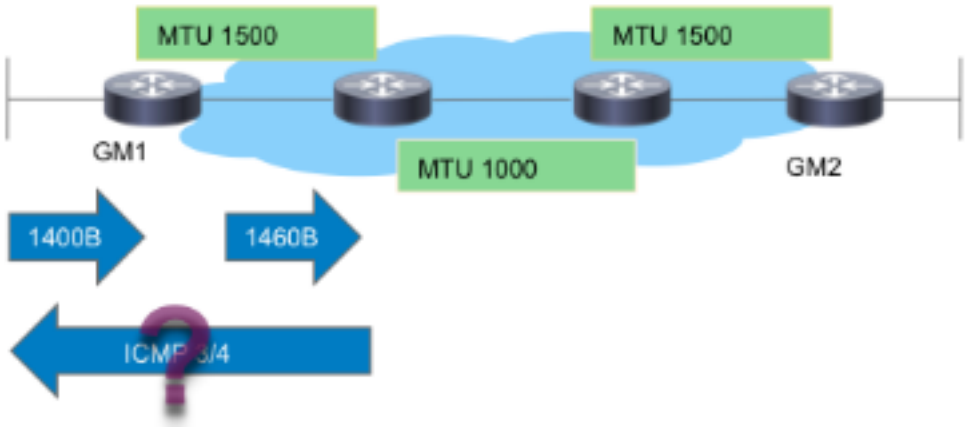
```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

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 (según lo indicado por el valor de la respuesta) es perceptiblemente diferente entre el GMs cuando las salidas se capturan con el mismo tiempo de la referencia, después el problema se puede atribuir para cronometrar la posición oblicua.

> Nota: En la plataforma agregada Cisco de las 1000 Series del router de los servicios, debido a la arquitectura de la plataforma, el datapath en el procesador del flujo de Quantum (QFP) refiere realmente al reloj de pared para contar las señales del pseudotime. Esto ha creado los problemas con TBAR cuando los cambios de la Hora del reloj de la pared debido a la sincronización NTP. Este problema se documenta con el Id. de bug Cisco CSCum37911.

#### Preservación de la encabezado PMTUD y GETVPN

Con GETVPN, la detección de MTU de trayecto (PMTUD) no trabaja entre el GMs que cifra y que desencripta, y los paquetes grandes con el conjunto de bits del don't fragment (DF) puede conseguir blackholed. La razón que ésta no trabaja es debido a la preservación de la encabezado GETVPN donde preservan la fuente de datos/a las direcciones destino en el ESP que encapsula la encabezado. Esto se representa en esta imagen:




Mientras que la imagen muestra, el PMTUD analiza con GETVPN con este flujo:

1. El paquete de datos grande llega en el GM1 que cifra.
2. El paquete ESP del poste-cifrado se remite de GM1 y se entrega hacia el destino.
3. Si hay un link de tránsito con IP MTU de 1400 bytes, el paquete ESP será caído, y un mensaje demasiado grande del paquete ICMP 3/4 será enviado hacia la fuente del paquete, que es la fuente del paquete de datos.
4. El paquete ICMP3/4 es para el final host debido al ICMP no excluido de la política de encripción GETVPN, o caído caído puesto que no sabe cualquier cosa sobre el paquete ESP (payload del unauthenticated).

En resumen, el PMTUD no trabaja con GETVPN hoy. Para trabajar alrededor de este problema, Cisco recomienda estos pasos:

1. Implemente el “IP tcp ajustan-mss” para reducir la orden o de la lata del tamaño del segmento del paquete TCP acomodan los gastos indirectos y el trayecto mínimo MTU del cifrado en el transit network.
2. Borre el bit DF en el paquete de datos como llegan en el GM que cifra para evitar el PMTUD.

### Problemas genéricos de Dataplane del IPSec

La mayor parte del troubleshooting del dataplane del IPSec es como resolver problemas los túneles IPsec de punto a punto tradicionales. Uno de los problemas frecuentes es %CRYPTO-4-RECVD_PKT_MAC_ERR. Vea el mensaje de error del Syslog el "%CRYPTO-4-RECVD_PKT_MAC_ERR:" con la pérdida del ping sobre el troubleshooting del túnel IPsec para más detalles del troubleshooting.

## Problemas conocidos

Este mensaje puede ser generado cuando se recibe un paquete IPsec que no hace juego SPI en el SADB. Vea el Id. de bug Cisco CSCtd47420 - GETVPN - CRYPTO-4-RECVD_PKT_NOT_IPSEC señalado para el pkt que no corresponde con el flujo. Se presenta un ejemplo a continuación:

```
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
```

Este mensaje debe ser %CRYPTO-4-RECVD_PKT_INV_SPI, que es qué consigue señalada para el IPSec tradicional así como sobre algunas plataformas de hardware tales como ASR. Este problema estético fue reparado por el Id. de bug Cisco CSCup80547: Error en señalar CRYPTO-4-RECVD_PKT_NOT_IPSEC para el pak ESP.

> Nota: Estos mensajes pueden aparecer a veces debido a otro bug CSCup34371 GETVPN: El GM GETVPN para el decrytping del tráfico después de que el TEK reintroduzca.

En este caso, el GM no puede desencriptar el tráfico GETVPN, aunque tenga IPSec válido SA en el SADB (el SA que es reintroducido). El problema desaparece tan pronto como el SA expire y se quite del SADB. Este problema causa la caída del sistema significativa, porque el TEK reintroduce se realiza por adelantado. Por ejemplo, la caída del sistema puede ser 22 minutos en el caso de una vida útil de TEK de 7200 segundos. Vea la descripción del bug para la condición exacta que se debe cumplir para encontrar este bug.

# Resuelva problemas GETVPN en las Plataformas que funcionan con el Cisco IOS XE

## Comandos para resolución de problemas

Las Plataformas que funcionan con el Cisco IOS XE tienen implementaciones específicas de la plataforma, y requieren a menudo el debugging específico de la plataforma para los problemas GETVPN. Aquí está una lista de comandos usados típicamente para resolver problemas GETVPN en estas Plataformas:

**show crypto eli todo**

**muestre las estadísticas de la directiva del IPSec del software de plataforma**

**muestre el inventario del active punto de congelación del IPSec del software de plataforma**

**muestre a qfp del hardware de plataforma el IPSec activo SPD todo de la característica**

**muestre a qfp del hardware de plataforma el descenso de las estadísticas activas claro**

**muestre a qfp del hardware de plataforma el descenso activo de los datos del IPSec de la característica claro**

**show crypto ipsec sa**

**muestre el gdoi crypto**

**muestre el IPSec crypto interno**

**debug crypto ipsec**

**error del IPSec del debug crypto**

**estados del IPSec del debug crypto**

**mensaje de IPSec del debug crypto**

**hw-req del IPSec del debug crypto**

**del debug crypto del gdoi gm detalle infra**

**el gm del gdoi del debug crypto reintroduce el detalle**

### Problemas frecuentes ASR1000

#### La directiva del IPSec instala el error (el Re-registro continuo)

Un GM ASR1000 pudo continuar registrándose al servidor dominante si el motor de criptografía no soporta la directiva o el algoritmo del IPSec recibido. Por ejemplo, en el Nitrox basó las Plataformas ASR (tales como ASR1002), habitación-B o las directivas SHA2 no se soportan y ésta puede causar los síntomas continuos del re-registro.

## Problemas comunes de la migración/de la actualización

### Limitación ASR1000 TBAR

En la plataforma ASR1000, el arreglo del Id. de bug Cisco CSCum37911 introdujo una limitación en esta plataforma donde el tiempo TBAR de menos de 20 segundos no se soporta. Vea las restricciones para GETVPN en IOS-XE.

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

**Actualización:** Esta restricción se ha suprimido desde entonces con el arreglo para el Id. de bug Cisco CSCur57558, y es no más una limitación en XE3.10.5, y posterior el código XE3.13.2.

También obsérvelo, para un GM que se ejecute en las Plataformas del Cisco IOS XE (ASR1k o ISR4k), se recomienda altamente que el dispositivo funciona con una versión con el arreglo para este problema si se habilita TBAR; Id. de bug Cisco CSCut91647 - GETVPN en IOS-XE: El GM cae incorrectamente los paquetes debido al error TBAR.

### Problema de la clasificación ISR4x00

Una regresión fue encontrada en la plataforma ISR4x00 donde se ignoran las directivas de la negación. Para los detalles, vea el Id. de bug Cisco CSCut14355 - GETVPN - El GM ISR4300 ignora niega la directiva.

## Información Relacionada

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