GETVPN故障排除指南

目錄

簡介

本文檔旨在提供一個結構化故障排除方法和有用的工具，以幫助識別和隔離組加密傳輸VPN(GETVPN)問題，並提供可能的解決方案。

必要條件

需求

思科建議您瞭解以下主題：

- GETVPN
  [官方GETVPN配置指南](#)
  [官方GETVPN設計和實施指南](#)

- 系統日誌伺服器使用

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

GETVPN故障排除方法

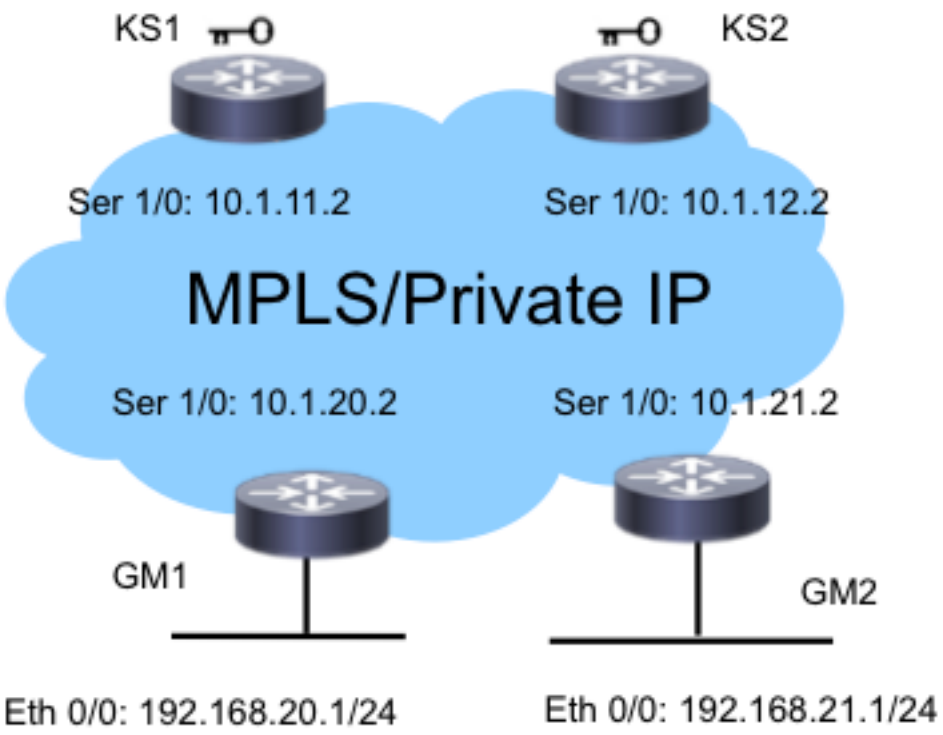
與大多數複雜技術問題的故障排除一樣，關鍵是能夠將問題隔離到特定功能、子系統或元件上。GETVPN解決方案由許多功能元件組成，具體包括：

- 網際網路金鑰交換(IKE) — 在群組成員(GM)和金鑰伺服器(KS)之間以及在合作通訊協定(COOP)KS之間使用，用於驗證和保護控制平面。
- 組解釋域(GDOI) — 用於KS的協定，用於分發組金鑰並為所有GM提供金鑰服務（如重新生成金鑰）。
- COOP — 用於KS的協定，用於相互通訊並提供冗餘。
- 報頭保留 — 隧道模式中的IPsec，保留原始資料包報頭以進行端到端流量傳輸。
- 基於時間的反重放(TBAR) — 在組金鑰環境中使用的重放檢測機制。

它還提供一套豐富的故障排除工具，以簡化故障排除過程。瞭解這些工具中哪些可用，以及它們何時適用於每項故障排除任務非常重要。進行故障排除時，最好從干擾最小的方法開始，這樣就不會對生產環境造成負面影響。此結構化故障排除的關鍵是能夠將問題分解為控制平面問題或資料平面問題。如果您遵循協定或資料流並使用此處提供的各種工具來檢查它們，則可以執行此操作。

參考拓撲

此GETVPN拓撲和編址方案用於本文檔的其餘部分。



參考配置

- 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
```

附註：KS2和GM2配置不在此列出，以便簡潔。

技術

- KS -金鑰伺服器
- GM -組成員
- COOP -合作協定
- TBAR — 基於時間的反重放
- KEK -金鑰加密金鑰
- TEK -流量加密金鑰

日誌記錄設施準備和其他最佳做法

開始故障排除之前，請確保已按照此處所述準備了日誌記錄設施。下面還列出了一些最佳實踐：

- 檢查路由器的可用記憶體量，並將**logging buffered debugging**配置為一個大值（10 MB或以上，如果可能）。
- 禁用登入到控制檯、監控器和系統日誌伺服器。
- 使用**show log**命令定期檢索日誌記錄緩衝區內容（每20分鐘到一小時），以防止由於緩衝區重複使用而丟失日誌。
- 無論發生什麼情況，請從受影響的GM和KS輸入**show tech**命令，並在全域性中檢查**show ip route**命令的輸出以及涉及的每個虛擬路由和轉發(VRF)（如果需要）。
- 使用網路時間協定(NTP)以在偵錯的所有裝置之間同步時鐘。為調試和日誌消息啟用毫秒(msec)時間戳：

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

- 確保show命令輸出具有時間戳。

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

- 為控制平面事件或資料平面計數器收集show命令輸出時，始終收集同一輸出的多個迭代。

排除GETVPN控制平面問題

控制平面是指導致在GM上建立策略和安全關聯(SA)的所有協定事件，以便它們做好加密和解密資料平面流量的準備。GETVPN控制平面中的一些關鍵檢查點是：

控制平面調試最佳實踐

這些故障排除最佳實踐不是GETVPN特定的；它們幾乎適用於所有控制平面調試。為確保進行最有效的故障排除，必須遵循以下最佳做法：

- 關閉控制檯日誌記錄並使用日誌記錄緩衝區或syslog來收集調試。
- 使用NTP同步所有已調試裝置上的路由器時鐘。
- 為調試和日誌消息啟用msec時間戳：

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

- 確保show命令輸出具有時間戳，以便它們與debug輸出相關聯：

```
terminal exec prompt timestamp
```

- 如果可能，在縮放環境中使用條件調試。

GETVPN控制平面故障排除工具

GETVPN Show命令

通常，對於幾乎所有GETVPN問題，您應該收集這些命令輸出。

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
```

GETVPN系統日誌消息

GETVPN為重要的協定事件和錯誤條件提供了一組詳細的系統日誌消息。執行GETVPN故障排除時，系統日誌應始終是首選位置。

常見KS系統日誌消息

系統日誌消息	說明
COOP_CONFIG_MISMATCH	主金鑰伺服器和輔助金鑰伺服器之間的配置不匹配。
COOP_KS_ELECTION	本地金鑰伺服器已在組中進入選舉過程。
COOP_KS_REACH	恢復所配置的協同金鑰伺服器之間的可達性。
COOP_KS_TRANS_TO_PRI	**本地金鑰伺服器從組中的輔助伺服器轉換為主角色。**
COOP_KS_UNAUTH	授權遠端伺服器嘗試聯絡組中的本地金鑰伺服器，這可能被視為惡意事件。
COOP_KS_UNREACH	**配置的合作金鑰伺服器之間的可達性丟失，這可能被視為惡意事件。**
KS_GM_REVOKED	在金鑰更新協定期間，未經授權的成員試圖加入組，這可以被視為惡意事件
KS_SEND_MCAST_REKEY	**正在傳送組播金鑰。**
KS_SEND_UNICAST_REKEY	**正在傳送單播金鑰。**
KS_UNAUTHORIZED	在GDOI註冊協定期間，一個未經授權的成員試圖加入一個組，該組可能被
UNAUTHORIZED_IPADDR	註冊請求被丟棄，因為請求裝置未被授權加入組。

常見GM系統日誌消息

系統日誌消息	說明
GM_CLEAR_REGISTER	本地組成員已執行clear crypto gdoi命令。
GM_CM_ATTACH	已為本地組成員附加了加密對映。
GM_CM_DETACH	已分離本地組成員的加密對映。&
GM_RE_REGISTER	**為一個組建立的IPsec SA可能已過期或已清除。需要重新註冊到金鑰伺服**
GM_RECV_REKEY	**已收到重新生成金鑰。**
GM_REGS_COMPL	**註冊完成。**
GM_REKEY_TRANS_2_MULTI	組成員已從使用單播金鑰機制轉換到使用組播機制。
GM_REKEY_TRANS_2_UNI	組成員已從使用組播金鑰機制轉換為使用單播機制。
PSEUDO_TIME_LARGE	組成員已收到偽時間，其值與其自己的偽時間有很大不同。
REPLAY_FAILED	組成員或金鑰伺服器的反重播檢查失敗。

附註：以紅色突出顯示的消息是GETVPN環境中最常見或最重要的消息。

全域性加密和GDOI調試

GETVPN調試分為以下部分：

1. 首先通過您正在故障排除的裝置。

```
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. 其次為您正在診斷的問題型別。

```
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. 第三是需要啟用的調試級別。在15.1(3)T及更新版本中，所有GDOI功能調試都標準化為具有這些調試級別。該設計旨在幫助對具有足夠調試粒度的大型GETVPN環境進行故障排除。調試GETVPN問題時，使用適當的調試級別非常重要。通常，從最低調試級別（即錯誤級別）開始，並在需要時增加調試粒度。

```
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
```

GDOI條件調試

在Cisco IOS®版本15.1(3)T及更高版本中，增加了GDOI條件調試以幫助在大規模環境中排除GETVPN故障。因此，所有網際網路安全關聯和金鑰管理協定(ISAKMP)和GDOI調試現在都可以使用基於組或對等IP地址的條件過濾器觸發。對於大多數GETVPN問題，最好使用適當的條件過濾器來啟用ISAKMP和GDOI調試，因為GDOI調試只顯示GDOI特定的操作。為了使用ISAKMP和

GDOI條件調試，請完成以下兩個簡單的步驟：

1. 設定條件篩選器。
2. 照常啟用相關的ISAKMP和GDOI。

例如：

```
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)
```

> **附註**：使用ISAKMP和GDOI條件調試時，為了捕獲可能沒有條件過濾器資訊的調試消息（例如調試路徑中的IP地址），可以啟用**unmatched**標誌。但是，必須謹慎使用此方法，因為它可能生成大量調試資訊。

GDOI事件跟蹤

15.1(3)T版新增了此功能。事件跟蹤為重要的GDOI事件和錯誤提供輕量、始終線上的跟蹤。還有為例外情況啟用回溯的退出路徑追蹤。事件跟蹤可以提供比傳統系統日誌更多的GETVPN事件歷史記錄資訊。

預設情況下，GDOI事件跟蹤已啟用，可以使用**show monitor even-trace**命令從跟蹤緩衝區中檢索。

```
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
```

退出路徑跟蹤提供有關退出路徑的詳細資訊，即異常和錯誤條件，預設情況下會啟用traceback選項。然後可以使用回溯來解碼導致退出路徑條件的確切代碼序列。使用**detail**選項可從追蹤緩衝區擷取

回溯：

```
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
```

預設的跟蹤緩衝區大小為512個條目，如果問題是間歇性的，這可能不夠。為了增加此預設跟蹤條目大小，可以更改事件跟蹤配置引數，如下所示：

```
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
```

GETVPN控制平面檢查點和常見問題

下面是GETVPN的一些常見控制平面問題。要重新迭代，控制平面被定義為在GM上啟用資料平面加密和解密所需的所有GETVPN功能元件。在高級別上，這需要成功的GM註冊、安全策略和SA下載/安裝，以及後續的KEK/TEK重新金鑰。

COOP設定和策略建立

要檢查並驗證KS是否已成功建立安全策略以及關聯的KEK/TEK，請輸入：

```
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
```

KS策略設定的一個常見問題是主和輔助KS之間配置了不同的策略。這可能會導致不可預測的KS行為，並報告以下錯誤：

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

目前，主和輔助KS之間沒有自動配置同步，因此必須手動糾正這些同步。

因為COOP是GETVPN的關鍵（幾乎總是必需）配置，所以關鍵是要確保COOP工作正常且COOP KS角色正確：

```
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
```

在功能正常的COOP設定中，應觀察此協定流：

IKE Exchange > ANN with COOP priority exchange > COOP Election > ANN from primary to secondary KS（策略、GM資料庫和金鑰）

當COOP不能正常工作或者存在COOP拆分（例如多個KS成為主KS）時，必須收集這些調試以進行故障排除：

```
debug crypto isakmp
```

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

IKE設定

GETVPN需要成功進行IKE交換，以確保後續策略和SA下載的控制通道安全。在成功的IKE交換結束時，會建立GDOI_REKEY sa。

在低於Cisco IOS 15.4(1)T的版本中，可以使用**show crypto isakmp sa**命令顯示GDOI_REKEY:

```
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#
```

在Cisco IOS 15.4(1)T及更新版本中，此GDOI_REKEY sa是使用**show crypto gdoi rekey sa**命令顯示的：

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

> **附註**：初始IKE交換完成後，將使用**GDOI_REKEY SA將後續策略和金鑰從KS**推送到GM。因此，GDOI_IDLE SA到期時沒有重新生成金鑰；當生命期過後它們就會消失。但是，GM上應該始終存在GDOI_REKEY SA以便其接收重新金鑰。

GETVPN的IKE交換與傳統點對點IPsec隧道中使用的IKE沒有區別，因此故障排除方法保持不變。必須收集以下調試以排除IKE身份驗證問題：

```
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)
```

註冊、策略下載和SA安裝

一旦IKE身份驗證成功，GM將向KS註冊。當正確發生這種情況時，應該會看到以下系統日誌消息：

```
%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
```

可以使用以下命令驗證策略和金鑰：

```
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#
```

附註：使用GETVPN時，入站和出站SA使用相同的SPI。

對於GETVPN註冊和策略安裝型別的問題，需要以下調試才能進行故障排除：

```
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)
```

附註：根據這些產出的結果，可能需要增加調試次數。

由於GETVPN註冊通常在GM重新載入後立即發生，因此此EEM指令碼可能有助於收集以下調試：

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

重新生成金鑰

GM註冊到KS且GETVPN網路正確設定後，主KS負責向註冊到它的所有GM傳送重新生成金鑰消息。金鑰消息用於同步GM上的所有策略、金鑰和偽時間。金鑰消息可以通過單播或組播方法傳送。

傳送重新生成金鑰消息時，KS上會顯示此系統日誌消息：

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

在GMs上，這是收到重新設定金鑰時看到的系統日誌：

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

KS上重新生成金鑰的RSA金鑰對要求

重新生成金鑰功能需要在KS上存在RSA金鑰。在註冊期間，KS通過此安全通道將RSA金鑰對的公鑰提供給GM。然後，KS使用GDOI SIG負載中的私有RSA金鑰對傳送到GM的GDOI消息進行簽名。GM接收GDOI消息並使用公共RSA金鑰來驗證消息。KS和GM之間的消息使用KEK加密，KEK在註冊期間也分發給GM。註冊完成後，後續的金鑰將使用KEK加密並使用私有RSA金鑰簽名。

如果在GM註冊期間KS上沒有RSA金鑰，則系統日誌中將顯示以下消息：

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

當KS上沒有金鑰時，GM第一次註冊，但下一個重新金鑰從KS失敗。最終GM上的現有金鑰過期，它再次重新註冊。

```
%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.
```

由於使用RSA金鑰對對重新生成金鑰消息進行簽名，因此，在主要KS和所有輔助KS之間，它們**必須相同**。這確保在主KS故障期間，從屬KS（新的主KS）傳送的金鑰仍然能夠由GM正確驗證。當它在主KS上生成RSA金鑰對時，必須使用**exportable**選項建立金鑰對，以便可以將金鑰對匯出到所有輔助KS以滿足此要求。

重新鍵入故障排除

KEK/TEK重新生成金鑰失敗是客戶部署中遇到的最常見的GETVPN問題之一。對重新生成金鑰問題進行故障排除時，應遵循以下所述的重新生成金鑰步驟：

1. 金鑰是否由KS傳送？

   這可以通過%GDOI-5-KS_SEND_UNICAST_REKEY系統日誌消息的觀察進行檢查，或者更準確地使用以下命令進行檢查：

```
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
```

   重新傳送的重新金鑰的數量表示由KS沒有接收的重新金鑰確認分組，並且因此指示可能的重新金鑰問題。請記住，GDOI重定金鑰使用UDP作為不可靠的傳輸機制，因此根據底層傳輸網路的可靠性，可能會出現一些重定金鑰丟棄，但應始終研究增加重定金鑰重傳的趨勢。

   還可以獲得更詳細的每GM金鑰統計資料。這通常是尋找潛在重新生成金鑰問題的第一個地方。

```
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. 重新生成金鑰的資料包是否在底層基礎設施網路中傳輸？

應遵循重新生成金鑰轉發路徑上的標準IP故障排除，以確保在KS和GM之間的傳輸網路中不會丟棄重新生成金鑰的資料包。此處使用的一些常見疑難排解工具是輸入/輸出存取控制清單(ACL)、Netflow和傳輸網路中的封包擷取。

3. 重新生成金鑰的資料包是否到達GDOI進程以進行重新生成金鑰處理？

   檢查GM重新生成金鑰統計資訊：

```
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. 重新生成金鑰確認資料包是否返回到KS?

   按照步驟1至3執行操作，以跟蹤從GM發回到KS的金鑰確認資料包。

Muticast Rekey

組播金鑰與單播金鑰在以下方面有所不同：

- 由於使用組播來將這些重新生成金鑰的資料包從KS傳輸到GM，因此KS不需要複製重新生成金鑰的資料包本身。KS僅傳送重新生成金鑰資料包的一個副本，並且在啟用組播的網路中複製這些副本。
- 沒有確認機制來確認多播重定金鑰，因此，如果GM沒有收到重定金鑰包，KS將不知道該重定金鑰，因此永遠不會從其GM資料庫中刪除GM。而且，由於無確認，因此KS將始終根據其金鑰重傳配置重傳金鑰資料包。

最常見的多播金鑰重新生成問題是在GM上未接收到重新生成金鑰時。可能的原因有很多，例如：

- 組播路由基礎設施中的資料包傳輸問題
- 網路中未啟用端到端組播路由

解決組播金鑰問題的第一步是檢視從組播切換到單播方法時金鑰是否有效。

一旦您確定問題特定於組播金鑰後，請驗證KS是否將金鑰傳送到指定的組播地址。

```
%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
```

使用對組播地址的網際網路控制消息協定(ICMP)請求，測試KS和GM之間的組播連線。組播組內的所有GM都應回覆ping。確保此測試的KS加密策略中排除了ICMP。

```
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
```

如果多點傳送ping測試失敗，則必須執行多點傳送疑難排解，這不在本檔案的範圍之內。

控制平面中繼檢查

症狀

當客戶將其GM升級為新的Cisco IOS版本時，他們可能會在系統日誌中觀察到以下消息時遇到KEK重新生成金鑰失敗：

```
%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
```

此行為是由為控制平面消息新增的反重播檢查時引入的互操作性問題導致的。具體而言，運行舊代碼的KS會將KEK重新生成金鑰的序列號重置為1，並且，當將新代碼解釋為重新生成的重新生成金鑰的資料包時，運行新代碼的GM將丟棄該序列號。如需更多詳細資訊，請參閱Cisco錯誤ID CSCta05809(GETVPN:GETVPN control-plane sensible to replay)和GETVPN配置限制。

背景

通過GETVPN，控制平面消息可以攜帶時間敏感的資訊，以便提供基於時間的反重播檢查服務。因此，這些消息本身需要反重放保護以確保時間準確性。這些消息是：

- **將消息從**KS重定金鑰到GM
- **KS之間的COOP通**告消息

作為此反重播保護實現的一部分，新增了序列號檢查以保護重播的消息，並在啟用TBAR時新增偽時間檢查。

解決方案

為了解決此問題，必須在控制平面重新執行檢查功能之後將GM和KS升級到Cisco IOS版本。使用新的Cisco IOS代碼時，KS不會將KEK重新鍵的序列號重置回1，而是繼續使用當前序列號，並且只重置TEK重新鍵的序列號。

以下Cisco IOS版本具有重播檢查功能：

- 12.4(15)T10
- 12.4(22)T3
- 12.4(24)T2
- 15.0(1)M及更高版本

與重放相關的其他問題

- 由於ANN消息未能通過重播檢查而導致COOP故障(思科錯誤ID CSCtc52655)

調試控制平面重播失敗

對於其他控制平面重放故障，請收集此資訊並確保時間在KS和GM之間同步。

- 來自GM和KS的系統日誌
- ISAKMP調試

- KS和GM的GDOI調試（重新生成金鑰和重放）

控制平面封包分段問題

使用GETVPN時，控制平面資料包分段是一個常見問題，當控制平面資料包足夠大，需要進行IP分段時，它可以在以下兩種情況之一中表現出來：

- GETVPN COOP通知資料包
- GETVPN重新生成金鑰資料包

COOP通知資料包

COOP通知資料包攜帶GM資料庫資訊，因此在大型的GETVPN部署中可能變得很大。根據過去的經驗，由1500多個GM組成的GETVPN網路將產生大於18024位元組的通告資料包，這是Cisco IOS預設的超大緩衝區大小。發生這種情況時，KS無法分配足以傳輸ANN資料包的緩衝區，錯誤如下：

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

為了糾正此情況，建議使用以下緩衝區調整：

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

重新生成資料包金鑰

當加密策略較大時，GETVPN重定金鑰資料包也可以超過典型的1500 IP最大轉換單元(MTU)大小，例如由加密ACL中的8行以上訪問控制條目(ACE)組成的策略。

分段問題和識別

在上述兩種情況下，GETVPN必須能夠正確傳輸和接收分段的UDP資料包，才能使COOP或GDOI重新生成金鑰正常運行。在某些網路環境中，IP分段可能是一個問題。例如，由等價多重路徑(ECMP)轉送平面和轉送平面中的某些裝置組成的網路，需要分段IP封包的虛擬重組，例如虛擬分段重組(VFR)。

若要識別問題，請在懷疑未正確接收分段的UDP 848資料包的裝置上檢查重組錯誤：

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

如果重組逾時繼續增加，請使用**debug ip error**命令確認捨棄是否屬於重新生成金鑰/COOP資料包流。確認後，應執行正常的IP轉發故障排除，以隔離轉發平面中可能已丟棄資料包的準確裝置。一些常用的工具包括：

- 封包擷取
- 流量轉發統計資訊
- 安全功能統計資訊（防火牆、IPS）
- VFR統計資訊

GDOI互操作性問題

多年來，GETVPN已發現各種互操作性問題，因此注意KS和GM之間以及KS之間的Cisco IOS版本對於互操作性問題至關重要。

其他眾所周知的GETVPN互操作性問題是：

- 控制平面中繼檢查
- GETVPN KEK金鑰行為更改
- 思科錯誤ID CSCub42920(GETVPN:KS無法驗證來自舊版GM的重新生成金鑰確認中的雜湊)
- 思科錯誤ID CSCuw48400（GetVPN GM無法註冊或重定金鑰失敗 — 符號雜湊>預設SHA-1）
- 思科錯誤ID CSCvg19281(遷移到新KS對後多次GETVPN GM崩潰;如果GM版本早於3.16，並且KS從早期代碼升級到3.16或更高版本，則可能會發生此問題)

GETVPN IOS升級過程

需要在GETVPN環境中執行Cisco IOS代碼升級時，應遵循以下Cisco IOS升級過程：

1. 首先升級輔助KS，然後等待COOP KS選舉完成。
2. 對所有輔助KS重複步驟1。
3. 升級主KS。
4. 升級GM。

排除GETVPN資料平面問題

與控制平面問題相比，GETVPN資料平面問題是GM具有執行資料平面加密和解密的策略和金鑰的問題，但是由於某種原因，端到端流量無法工作。大多數GETVPN的資料平面問題都與通用IPsec轉發有關，並非特定於GETVPN。因此，此處介紹的大多數故障排除方法也適用於一般IPsec資料平面問題。

對於加密問題（基於組或成對隧道），請務必解決問題並將問題隔離到資料路徑的特定部分。具體而言，此處介紹的故障排除方法旨在幫助您回答以下問題：

- 哪個裝置是罪魁禍首 — 加密路由器或解密路由器？
- 問題發生在哪個方向 — 入口還是出口？

GETVPN資料平面故障排除工具

IPsec資料平面故障排除與控制平面的故障排除非常不同。對於資料平面，通常沒有您可以運行的調試，或者至少沒有可以在生產環境中安全運行的調試。因此，故障排除非常依賴不同的計數器和流量統計資訊，以幫助沿著轉發路徑跟蹤資料包。其理念是能夠開發一組檢查點，以幫助隔離可能丟棄資料包的位置，如下所示：

以下是一些資料平面調試工具：

- 存取清單
- IP優先順序記帳
- Netflow
- 介面計數器
- 加密計數器
- IP思科快速轉送(CEF)全域和每個功能捨棄計數器
- 內嵌式封包擷取(EPC)
- 資料平面偵錯（IP封包和CEF偵錯）

可以使用以下工具驗證上一個映像中資料路徑中的檢查點：

加密GM

- 輸入LAN介面
  輸入ACL
  輸入netflow
  內嵌式封包擷取
  輸入優先順序記帳

- 加密引擎
  show crypto ipsec sa
  show crypto ipsec sa detail
  show crypto engine accelerator statistics

- 輸出WAN介面
  輸出netflow
  內嵌式封包擷取
  輸出優先記帳

解密GM

- 輸入WAN介面
  輸入ACL
  輸入netflow
  內嵌式封包擷取
  輸入優先順序記帳

- 加密引擎
  show crypto ipsec sa
  show crypto ipsec sa detail
  show crypto engine accelerator statistics

- 輸出LAN介面
  輸出netflow
  嵌入式資料包捕獲

返迴路徑遵循相同的通訊流。下一節將提供這些資料平面工具的一些示例。

加密/解密計數器

路由器上的加密/解密計數器基於IPsec流。很遺憾，這在GETVPN中並不起作用，因為GETVPN通

常部署一個「permit ip any any」加密策略來加密所有內容。因此，如果問題只發生在部分流（而非全部）中，則使用這些計數器可能會有點困難，因為當有足夠的足夠有效的背景流量時，這些計數器會正確評估資料包是否已加密或解密。

```
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可用於監控兩個GM上的輸入和輸出流量。請注意，使用GETVPN **permit ip any any**策略時，加密的流量將進行聚合，並且不提供每流資訊。然後，需要使用後面所述的DSCP/優先順序標籤收集每個流資訊。

在本例中，從GM1後面的主機到GM2後面的主機的100計數ping的netflow顯示在各個檢查點上。

加密GM

Netflow配置：

```
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輸出：

```
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#
```

> **附註**：在上一輸出中，*表示出口流量。第一行顯示從WAN介面輸出的加密流量（使用協定0x32 = ESP），第二行輸入ICMP流量進入LAN介面。

解密GM

組態:

```
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輸出：

```
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#
```

DSCP/IP優先順序標籤

解決加密問題的難題是，一旦資料包被加密，您就會失去對負載的可見性（這是加密應該執行的操作），因此很難針對特定IP流跟蹤資料包。排除IPsec故障時，有兩種方法可以解決此限制：

- 使用ESP-NULL作為IPsec轉換。IPsec仍執行ESP封裝，但沒有對負載應用加密，因此它們在資料包捕獲中可見。
- 根據流量的L3/L4特性，使用唯一的區別服務代碼點(DSCP)/優先順序標籤來標籤IP流量。

ESP-NULL需要在兩個隧道端點進行更改，通常根據客戶安全策略不允許這樣做。因此，思科通常建議改用DSCP/優先順序標籤。

DSCP/優先順序參考圖表

ToS（十六進位制）	ToS（十進位）	IP優先順序	DSCP	二進位
0xE0	224	7網路控制	56個CS7	11100000
0xC0	192	6網際網路控制	48 CS6	11000000
0xB8	184	5嚴重	46 EF	10111000
0xA0	160		40 CS5	10100000
0x88	136	4快閃記憶體覆蓋	34 AF41	10001000
0x80	128		32個CS4	10000000
0x68	104	3快閃記憶體	26架AF31	01101000
0x60	96		24 CS3	01100000
0x48	72	2立即	21年3月18日	01001000
0x40	64		16個CS2	01000000
0x20	32	1優先順序	8 CS1	00100000
0x00	0	0常式	0 Dflt	00000000

使用DSCP/優先順序標籤資料包

這些方法通常用於使用特定的DSCP/優先標籤來標籤資料包。

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
```

路由器Ping

```
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>
```

> **附註**：在您應用標籤之前，最好監控正常流量和DSCP/優先順序配置檔案，以便標籤的流量是唯一的。

監控標籤的封包

IP優先順序記帳

```
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
```

介面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
```

內嵌式封包擷取

內嵌式封包擷取(EPC)是在介面層級擷取封包的實用工具，目的是判斷封包是否已到達特定裝置。請記住，EPC對於明文流量運行良好，但是當捕獲的資料包被加密時，它可能是一個挑戰。因此，必須將DSCP/優先順序標籤等技術或其他IP字元（如IP資料包的長度）與EPC一起使用，才能使故障排除更有效。

Cisco IOS-XE封包追蹤軌跡

這是一項有用的功能，可用於跟蹤運行Cisco IOS-XE的所有平台（例如CSR1000v、ASR1000和ISR4451-X）上的功能轉發路徑。

GETVPN資料平面常見問題

排除GETVPN的IPsec資料平面故障基本上與傳統點對點IPsec資料平面故障沒有區別，但由於GETVPN的這些唯一資料平面屬性，有兩個例外。

基於時間的反重播失敗

在GETVPN網路中，TBAR故障通常難以排除，因為不再有成對隧道。要排除GETVPN TBAR故障，請完成以下步驟：

1. 識別哪個封包由於TBAR失敗而被捨棄，然後識別加密GM。

   在版本15.3(2)T之前，TBAR故障系統日誌不會列印故障資料包的源地址，因此很難確定哪個資料包發生了故障。在15.3(2)T版及更新版本中，這一點已顯著改善，Cisco IOS在其中列印以下內容：

```
%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
```

   此版本還實施了TBAR歷史記錄：

```
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
```

   附註：先前提到的增強功能已由思科錯誤ID CSCun4935在Cisco IOS-XE中以及思科錯誤ID

CSCub91811在Cisco IOS中實作。
對於沒有此功能的Cisco IOS版本，**debug crypto gdoi gm replay detail**也可提供此資訊，雖然此偵錯會列印所有流量的TBAR資訊（不僅是由於TBAR失敗而丟棄的封包），因此可能無法在生產環境中執行。

```
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. 一旦識別封包的來源，您應該能夠找到加密的GM。然後，應監控加密和解密GM上的偽時間戳是否有任何潛在的偽時間漂移。最好的方法是將GM和KS同步到NTP，並定期收集偽時間資訊與它們所有上的參考系統時鐘進行同步，以確定問題是否由GM上的時鐘偏差引起。

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

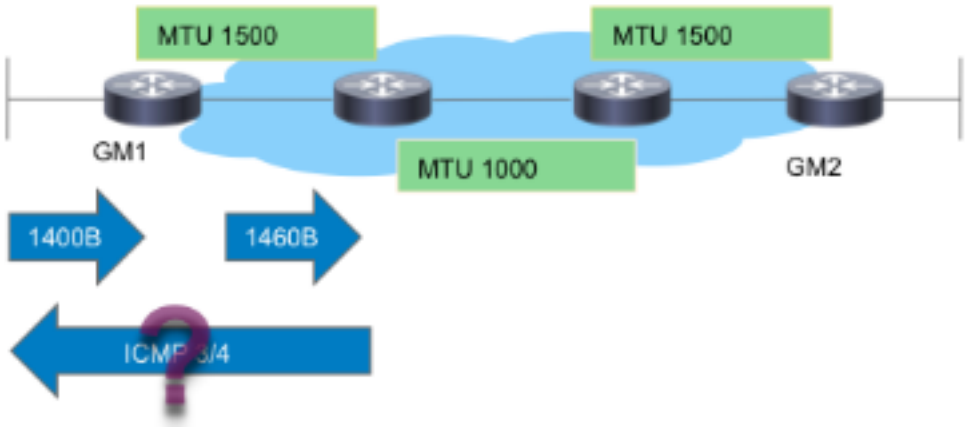
```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

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
```

在上一個例子中，如果在相同參考時間捕獲輸出時，GM之間的偽時間（如重放值所示）明顯不同，則問題可歸結為時鐘偏差。

附註：在思科聚合服務路由器1000系列平台上，由於平台架構，量子流處理器(QFP)上的資料路徑實際上是指用於計數偽時間刻度的掛鐘。這會導致由於NTP同步而導致掛鐘時間更改時TBAR出現問題。此問題已記錄在Cisco錯誤ID CSCum3791中。

PMTUD和GETVPN標頭保留

若使用GETVPN，路徑MTU探索(PMTUD)在加密和解密GM之間無法運作，且已設定「不分段(DF)」位元的大型封包可能會遭到黑洞。無法正常工作的原因是GETVPN報頭保留，其中資料來源/目標地址保留在ESP封裝報頭中。如下圖所示：



如圖所示，PMTUD使用以下流量進行GETVPN分解：

1. 大資料包到達加密GM1。
2. 加密後ESP資料包從GM1轉發出去，然後傳送到目的地。
3. 如果存在具有IP MTU 1400位元組的傳輸連結，則會捨棄ESP封包，並向封包來源（資料封包的來源）傳送ICMP 3/4封包過大的訊息。
4. 由於ICMP未從GETVPN加密策略中排除，因此ICMP3/4資料包被丟棄，或者由於終端主機對ESP資料包（未經身份驗證的負載）一無所知，而被丟棄。

總而言之，PMTUD目前不適用於GETVPN。為了解決此問題，思科建議以下步驟：

1. 實作「ip tcp adjust-mss」可將TCP封包區段大小縮小到可以容納傳輸網路中的加密額外負荷和最小路徑MTU。
2. 在封包到達加密GM時清除資料封包中的DF位元，以便避免PMTUD。

通用IPsec資料平面問題

大多數IPsec資料平面故障排除類似於傳統點對點IPsec隧道故障排除。其中一個常見問題是%CRYPTO-4-RECVD_PKT_MAC_ERR。如需更多疑難排解詳細資訊，請參閱系統日誌「%CRYPTO-4-RECVD_PKT_MAC_ERR：」錯誤訊息，以及Ping丟失IPsec通道疑難排解。

已知的問題

當收到與SADB中的SPI不匹配的IPsec資料包時，可能會生成此消息。請參閱為不匹配的資料包流報告的思科錯誤ID CSCtd47420 - GETVPN - CRYPTO-4-RECVD_PKT_NOT_IPSEC。例如：

```
%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
```

此消息應為%CRYPTO-4-RECVD_PKT_INV_SPI，這是傳統IPsec以及某些硬體平台（例如ASR）上報告的消息。此修飾問題已由Cisco錯誤ID CSCup80547修復：報告ESP產品包的CRYPTO-4-RECVD_PKT_NOT_IPSEC時出錯。

> **附註**：這些訊息有時可能會因為另一個GETVPN錯誤CSCup34371而顯示：GETVPN GM在TEK重新金鑰後停止解密流量。

在這種情況下，GM無法解密GETVPN流量，儘管它在SADB中有有效的IPsec SA（正在重新鍵入SA）。 SA到期後，問題隨即消失，並從SADB中刪除。此問題會導致嚴重中斷，因為TEK重新生

成金鑰是預先執行的。例如，在TEK生存時間為7200秒的情況下，中斷時間可能為22分鐘。請參閱錯誤說明，瞭解應該滿足的準確條件，以便遇到此錯誤。

對運行Cisco IOS-XE的平台上的GETVPN進行故障排除

疑難排解指令

運行Cisco IOS-XE的平台具有特定於平台的實施，並且通常需要針對GETVPN問題進行特定於平台的調試。以下是通常用於排除GETVPN在這些平台上的故障的命令清單：

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 states

debug crypto ipsec message

debug crypto ipsec hw-req

debug crypto gdoi gm infra detail

debug crypto gdoi gm rekey detail

ASR1000常見問題

IPsec策略安裝失敗（連續重新註冊）

如果加密引擎不支援收到的IPsec策略或演算法，則ASR1000 GM可能繼續註冊到金鑰伺服器。例如，在基於Nitrox的ASR平台（如ASR1002）上，不支援Suite-B或SHA2策略，這可能導致持續重新註冊症狀。

常見的遷移/升級問題

ASR 1000 TBAR限制

在ASR1000平台上，思科錯誤ID CSCum37911修復在此平台上引入了限制，其中不支援小於20秒的TBAR時間。請參閱IOS-XE上GETVPN的限制。

已開啟此增強功能錯誤以解除此限制，思科錯誤ID CSCuq25476 - ASR1k需要支援小於20秒的GETVPN TBAR視窗大小。

更新：此限制已隨思科錯誤ID CSCur57558的修正一起解除，因此它不再是XE3.10.5、XE3.13.2及更新版本中的限制。

另請注意，對於在Cisco IOS-XE平台（ASR1k或ISR4k）上運行的GM，強烈建議裝置在啟用TBAR的情況下執行含有此問題修正程式的版本；思科漏洞ID CSCut91647 - IOS-XE上的GETVPN:由於TBAR故障，GM錯誤地丟棄資料包。

ISR4x00分類問題

在ISR4x00平台上發現一條回歸線，其中忽略拒絕策略。有關詳細資訊，請參閱Cisco錯誤ID CSCut14355 - GETVPN - ISR4300 GM忽略拒絕策略。

相關資訊

- **群組加密傳輸VPN(GET VPN)- Cisco Systems**
- **技術支援與文件 - Cisco Systems**