GETVPN故障排除指南

目录

简介

本文档旨在提供结构化故障排除方法和有用工具，以帮助识别和隔离组加密传输VPN(GETVPN)问题，并提供可能的解决方案。

先决条件

要求

Cisco 建议您了解以下主题：

- GETVPN
  [官方GETVPN配置指南](#)
  [官方GETVPN设计和实施指南](#)

- 系统日志服务器使用

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

GETVPN故障排除方法

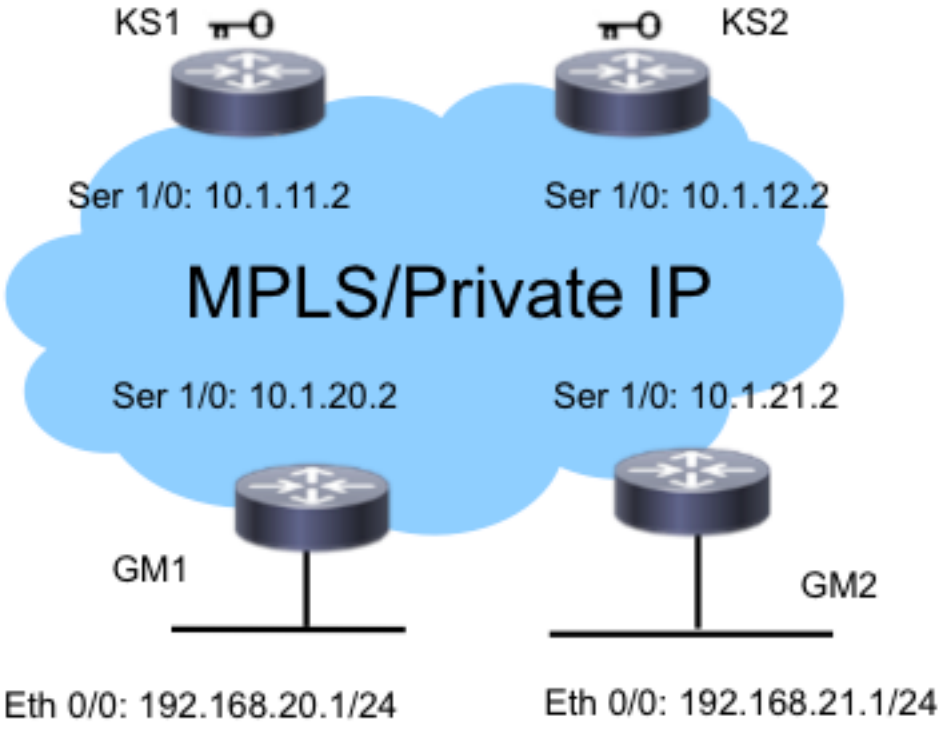
与大多数复杂技术问题的故障排除一样，关键是能够将问题隔离到特定功能、子系统或组件。GETVPN解决方案由许多功能组件组成，具体包括：

- 互联网密钥交换(IKE) — 在组成员(GM)和密钥服务器(KS)之间以及协作协议(COOP)KS之间使用，以验证和保护控制平面。
- 组解释域(GDOI) — 用于KS的协议，用于分发组密钥和为所有GM提供密钥等关键服务。
- COOP — 用于KS的协议，用于相互通信并提供冗余。
- 报头保留 — 隧道模式下的IPsec，用于保留原始数据包报头以进行端到端流量传输。
- 基于时间的反重播(TBAR) — 在组密钥环境中使用的重播检测机制。

它还提供一系列广泛的故障排除工具，以便简化故障排除过程。了解这些工具中有哪些可用工具以及它们何时适合每项故障排除任务非常重要。排除故障时，最好从干扰最小的方法开始，这样生产环境就不会受到负面影响。此结构化故障排除的关键是能够将问题分解为控制或数据平面问题。如果遵循协议或数据流并使用此处提供的各种工具来检查它们，则可以执行此操作。

参考拓扑

此GETVPN拓扑和编址方案用于本故障排除文档的其余部分。



参考配置

- 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
```

注意：KS2和GM2配置不包含在此，以便简化。

术语

- KS -密钥服务器
- GM — 组成员
- COOP -协作协议
- TBAR — 基于时间的反重播
- KEK — 密钥加密密钥
- TEK — 流量加密密钥

记录设施准备和其他最佳实践

在开始排除故障之前，请确保已按照此处所述准备了日志记录设施。下面还列出了一些最佳实践：

- 检查路由器的可用内存量，并将日志记录缓**冲调试**配置为一个较大的值（如果可能，为10 MB或更大）。
- 禁用记录到控制台、监控和系统日志服务器。
- 每隔20分钟至1小时，使用**show log**命令定期检索日志记录缓冲区内容，以防止因缓冲区重复使用而丢失日志。
- 无论发生什么情况，输入来自受影响的GM和KS的**show tech** 命令，并检查全局和每个虚拟路由和转发(VRF)中**show ip route** 命令的输出（如果需要）。
- 使用网络时间协议(NTP)在所有调试的设备之间同步时钟。为调试和日志消息启用毫秒（毫秒）时间戳：

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

- 确保show命令输出带有时间戳。

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

- 为控制平面事件或数据平面计数器收集show命令输出时，始终收集同一输出的多次迭代。

排除GETVPN控制平面问题

控制平面是指导致在GM上创建策略和安全关联(SA)的所有协议事件，以便它们准备好加密和解密数据平面流量。GETVPN控制平面中的一些关键检查点包括：

控制平面调试最佳实践

这些故障排除最佳实践不是特定于GETVPN的；它们几乎适用于任何控制平面调试。要确保最有效的故障排除，必须遵循以下最佳实践：

- 关闭控制台日志记录并使用日志记录缓冲区或系统日志以收集调试。
- 使用NTP以同步所有调试设备上的路由器时钟。
- 为调试和日志消息启用msec时间戳：

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

- 确保show命令输出带有时间戳，以便它们与调试输出相关联：

```
terminal exec prompt timestamp
```

- 如果可能，请在缩放环境中使用条件调试。

GETVPN控制平面故障排除工具

GETVPN Show命令

通常，这些是您应收集的用于几乎所有GETVPN问题的命令输出。

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系统日志消息

GETVPN为重要协议事件和错误情况提供一组广泛的系统日志消息。执行GETVPN故障排除时，系统日志应始终是首选位置。

常见KS系统日志消息

Syslog 消息	解释
COOP_CONFIG_MISMATCH	主密钥服务器和辅助密钥服务器之间的配置不匹配。
COOP_KS_ELECTION	本地密钥服务器已进入组中的选举过程。
COOP_KS_REACH	已配置的协作密钥服务器之间的可达性将恢复。
COOP_KS_TRANS_TO_PRI	**本地密钥服务器从组中的辅助服务器转变为主角色。**
COOP_KS_UNAUTH	授权的远程服务器尝试联系组中的本地密钥服务器，这可能被视为恶意事件
COOP_KS_UNREACH	**配置的协作密钥服务器之间的可达性丢失，这可能被视为恶意事件。**
KS_GM_REVOKED	在重新生成密钥协议期间，未授权成员尝试加入可能被视为恶意事件的组。
KS_SEND_MCAST_REKEY	**正在发送组播密钥。**
KS_SEND_UNICAST_REKEY	**正在发送单播密钥。**
KS_UNAUTHORIZED	在GDOI注册协议期间，未授权成员尝试加入一个组，该组可能被视为恶意
UNAUTHORIZED_IPADDR。	注册请求被丢弃，因为请求设备未获得加入组的授权。

常见GM系统日志消息

Syslog 消息	解释
GM_CLEAR_REGISTER	clear crypto gdoi命令已由本地组成员执行。
GM_CM_ATTACH	已为本地组成员附加加密映射。
GM_CM_DETACH	已为本地组成员分离加密映射。&
GM_RE_REGISTER	**为一个组创建的IPsec SA可能已过期或清除。需要重新注册到密钥服务器**
GM_RECV_REKEY	**已收到重新生成密钥。**
GM_REGS_COMPL	**注册完成。**
GM_REKEY_TRANS_2_MULTI	组成员已从使用单播密钥重新生成机制转变为使用组播机制。
GM_REKEY_TRANS_2_UNI	组成员已从使用组播密钥重新生成机制转变为使用单播机制。
PSEUDO_TIME_LARGE	组成员已接收伪时间，其值与其自身的伪时间大不相同。
REPLAY_FAILED	组成员或密钥服务器未通过反重播检查。

注意：以红色突出显示的消息是GETVPN环境中最常见或最重要的消息。

全局加密和GDOI调试

GETVPN调试被划分：

1. 首先通过您正在进行故障排除的设备。

```
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，根据您所排除的问题类型。

```
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，根据需要启用的调试级别。在版本15.1(3)T及更高版本中，所有GDOI功能调试都经过标准化，以具有这些调试级别。这是为了帮助排除具有足够调试粒度的大规模GETVPN环境的故障。调试GETVPN问题时，使用适当的调试级别非常重要。一般来说，从最低的调试级别（即错误级别）开始，并在需要时增加调试粒度。

```
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条件调试

在Cisco IOS® 15.1(3)T版及更高版本中，添加了GDOI条件调试，以帮助在大型环境中排除GETVPN故障。因此，所有互联网安全关联和密钥管理协议(ISAKMP)和GDOI调试现在都可以根据组或对等IP地址使用条件过滤器触发。对于大多数GETVPN问题，使用适当的条件过滤器启用ISAKMP和GDOI调试是好的，因为GDOI调试仅显示GDOI特定操作。要使用ISAKMP和GDOI条件

调试，请完成以下两个简单步骤：

1. 设置条件过滤器。
2. 照常启用相关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)
```

> **注意**：使用ISAKMP和GDOI条件调试，为了捕获可能没有条件过滤器信息（例如调试路径中的IP地址）的调试消息，可以启用**不匹配**标志。但是，必须谨慎使用，因为它会产生大量调试信息。

GDOI事件跟踪

这已在版本15.1(3)T中添加。事件跟踪为重要的GDOI事件和错误提供轻量级、不间断的跟踪。此外，还有启用了对异常情况回溯的退出路径跟踪。事件跟踪可提供比传统系统日志更多的GETVPN事件历史记录信息。

默认情况下，GDOI事件跟踪处于启用状态，并可以使用show monitor even-trace命令从**跟踪缓冲区中**检索。

```
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
```

退出路径跟踪提供有关退出路径（即异常和错误情况）的详细信息，默认情况下启用回溯选项。然后，可以使用回溯来解码导致退出路径条件的精确代码序列。使用**detail**选项从跟踪缓冲区检索回溯

：

```
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
```

默认跟踪缓冲区大小为512个条目，如果问题间歇性出现，则这可能不够。为了增加此默认跟踪条目大小，可以更改事件跟踪配置参数，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控制平面检查点和常见问题

以下是GETVPN的一些常见控制平面问题。要重新迭代，控制平面被定义为在GM上启用数据平面加密和解密所需的所有GETVPN功能组件。在较高级别上，这需要成功的GM注册、安全策略和SA下载/安装，以及后续的KEK/TEK密钥更新。

COOP设置和策略创建

要检查并验证KS是否已成功创建安全策略和相关KEK/TEK，请输入：

```
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策略设置的一个常见问题是在主KS和辅助KS之间配置了不同的策略。这可能导致无法预测的KS行为，并且将报告此错误：

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

目前，主KS和辅助KS之间没有自动配置同步，因此必须手动纠正这些同步。

由于COOP是GETVPN的关键（而且几乎总是必需的）配置，因此确保COOP正常工作和COOP KS角色正确至关重要：

```
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
```

在正常的COOP设置中，应观察此协议流：

IKE Exchange > ANN with COOP priorities sched > COOP Election > ANN from primary to secondary KS（策略、GM数据库和密钥）

当COOP无法正常工作，或者存在COOP拆分（例如，多个KS成为主KS）时，必须收集这些调试以进行故障排除：

```
debug crypto isakmp
```

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

IKE设置

GETVPN需要成功的IKE交换，以保护后续策略和SA下载的控制通道。在成功的IKE交换结束时，会创建GDOI_REKEY sa。

在早于Cisco IOS 15.4(1)T的版本中，GDOI_REKEY可以使用show crypto isakmp sa**命令显**示：

```
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及更高版本中，此GDOI_REKEY sa使用show crypto gdoi rekey sa**命令显**示：

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

> **注意：**初始IKE交换完成后，使用GDOI_REKEY SA将后续策略和密钥从KS推送到GM。因此，GDOI_IDLE SA到期时没有重新生成密钥；当他们的一生到期时，他们就会消失。但是，GM上应始终存在GDOI_REKEY SA，以便其接收重新密钥。

GETVPN的IKE交换与传统点对点IPsec隧道中使用的IKE无异，因此故障排除方法保持不变。必须收集以下调试以排除IKE身份验证问题：

```
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)
```

注册、策略下载和SA安装

一旦IKE身份验证成功，GM会向KS注册。当发生以下情况时，应看到以下系统日志消息：

```
%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
```

可以使用以下命令验证策略和密钥：

```
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#
```

注意：对于GETVPN，入站和出站SA使用相同的SPI。

对于GETVPN注册和策略安装类型的问题，需要执行以下调试才能排除故障：

```
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)
```

注意：根据这些输出的结果，可能需要进行其他调试。

由于GM重新加载后通常会立即进行GETVPN注册，因此此EEM脚本可能有助于收集以下调试：

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

重新生成密钥

一旦GM注册到KS并且GETVPN网络正确设置，主KS负责向注册到KS的所有GM发送密钥重新生成消息。重新生成密钥消息用于同步GM上的所有策略、密钥和伪时间。重新生成密钥消息可以通过单播或组播方法发送。

发送重新生成密钥消息时，KS上会显示此系统日志消息：

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

在GM上，这是收到密钥更新时看到的系统日志：

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

KS上重新生成密钥的RSA密钥对要求

密钥重新生成功能要求KS上存在RSA密钥。KS在注册期间通过此安全通道向GM提供RSA密钥对的公钥。然后，KS在GDOI特征码负载中用私有RSA密钥对发送到GM的GDOI消息进行签名。GM接收GDOI消息并使用公有RSA密钥来验证消息。KS和GM之间的消息用KEK加密，KEK也在注册期间分发给GM。注册完成后，随后的重新密钥将使用KEK加密，并使用私有RSA密钥签名。

如果在GM注册期间KS上不存在RSA密钥，则系统日志上会显示以下消息：

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

当密钥不在KS上时，GM首次注册，但下一个密钥从KS失败。最终，GM上的现有密钥会过期，并重新注册。

```
%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.
```

由于使用RSA密钥对来签名重新密钥消息，因此主KS和所有辅助KS之**间的**密钥对必须相同。这确保在主KS故障期间，辅助KS（新的主KS）发送的密钥仍然可以由GM正确地验证。当它在主KS上生成RSA密钥对时，必须使用可导出选项创建密钥对，以便它们可以导出到所有辅助KS，以满足此要求。

重新生成故障排除

KEK/TEK密钥重新生成故障是客户部署中遇到的最常见的GETVPN问题之一。排除重要问题时，应遵循以下重要步骤：

1. 密钥是KS发送的吗？

   这可以通过%GDOI-5-KS_SEND_UNICAST_REKEY系统日志消息的观察或使用此命令更准确地检查：

```
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
```

   重新发送的重新密钥数表示KS未接收的重新密钥确认分组，因此可能的重新密钥问题。请记住，GDOI重新生成密钥使用UDP作为不可靠的传输机制，因此根据底层传输网络的可靠性，可能会预期一些重新生成密钥的丢包，但应始终研究重新生成密钥的趋势。

   还可以获得更详细的每GM密钥重新统计。通常，这是寻找潜在重新生成密钥问题的第一个位置。

```
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. 密钥重新生成的数据包是否已在基础架构网络中传送？

应遵循重新生成密钥转发路径的标准IP故障排除，以确保重新生成密钥的数据包不会在KS和GM之间的传输网络中丢弃。此处使用的一些常见故障排除工具包括输入/输出访问控制列表(ACL)、Netflow和传输网络中的数据包捕获。

3. 重新生成密钥的数据包是否到达GDOI进程以进行重新生成密钥的处理？

   检查GM重新生成密钥的统计信息：

```
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. 重新生成密钥确认数据包是否返回到KS?

   按照步骤1到步骤3，以跟踪从GM返回KS的重新生成密钥确认数据包。

组播密钥

组播密钥与单播密钥在以下方面不同：

- 由于使用组播来将这些密钥重新生成的数据包从KS传输到GM，因此KS不需要复制密钥重新生成的数据包本身。KS只发送重新生成密钥的数据包的一个副本，并在启用组播的网络中进行复制。
- 组播密钥重新生成没有确认机制，因此如果GM不接收密钥重新生成的数据包，KS将不知道该数据包，因此永远不会从GM数据库中删除GM。由于没有确认，KS将始终根据其重新生成密钥的重新传输配置来重新发送密钥的数据包。

最常见的组播密钥重新生成问题是在GM上未收到重新生成的密钥。可能有多种原因，例如：

- 组播路由基础设施中的数据包传输问题
- 网络中未启用端到端组播路由

排除组播密钥更新问题的第一步是查看从组播切换到单播方法时密钥更新是否有效。

一旦您确定该问题特定于组播密钥更新，请验证KS是否将密钥更新发送到指定的组播地址。

```
%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
```

使用互联网控制消息协议(ICMP)请求测试KS和GM之间的组播连接到组播地址。属于组播组的所有GM都应回复ping。确保ICMP已从此测试的KS加密策略中排除。

```
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
```

如果组播ping测试失败，则必须执行组播故障排除，这不在本文档的范围内。

控制平面中继检查

症状

当客户将其GM升级到新的Cisco IOS版本时，他们可能会遇到KEK重新生成密钥的故障，在系统日志中观察到以下消息：

```
%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
```

此行为是由为控制平面消息添加的反重播检查引入的互操作性问题引起的。具体来说，运行旧代码的KS会将KEK重新生成密钥序列号重置为1，当运行新代码的GM将其解释为重播的重新生成密钥数据包时，将丢弃该序列号。有关详细信息，请参阅Cisco Bug ID CSCta05809(GETVPN:GETVPN控制平面可重播)和GETVPN配置限制。

背景

使用GETVPN，控制平面消息可以传送时间敏感信息以提供基于时间的反重播检查服务。因此，这些消息本身需要反重播保护，以确保时间准确性。以下消息为：

- **从KS到**GM的重新生成消息
- **KS之间的COOP通**告消息

作为此反重播保护实施的一部分，添加了序列号检查以保护重播消息，以及启用TBAR时的伪时间检查。

解决方案

要解决此问题，必须在控制平面重播检查功能后将GM和KS升级到Cisco IOS版本。使用新的Cisco IOS代码，KS不会将KEK密钥重新生成的序列号重置回1，而是继续使用当前序列号，只重置TEK密钥重新生成的序列号。

这些Cisco IOS版本具有重播检查功能：

- 12.4(15)T10
- 12.4(22)T3
- 12.4(24)T2
- 15.0(1)M及以上版本

其他重播相关问题

- COOP失败，原因是ANN消息失败重播检查(思科漏洞ID CSCtc52655)

调试控制平面重播失败

对于其他控制平面重放故障，请收集此信息并确保时间在KS和GM之间同步。

- 来自GM和KS的系统日志
- ISAKMP调试

- KS和GM的GDOI调试（重新生成密钥和重播）

控制平面数据包分段问题

使用GETVPN时，控制平面数据包分段是一个常见问题，当控制平面数据包足够大，需要IP分段时，控制平面数据包分段可能会在以下两种场景中表现出来：

- GETVPN COOP通告数据包
- GETVPN重新生成密钥数据包

COOP通告数据包

COOP通告数据包传输GM数据库信息，因此在大型GETVPN部署中可以大规模增长。根据以往经验，包含1500多个GM的GETVPN网络将生成大于18024字节的通告数据包，即Cisco IOS默认的巨大缓冲区大小。当发生这种情况时，KS无法分配足够大的缓冲区来传输ANN数据包，并出现以下错误：

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

为了纠正此情况，建议进行以下缓冲区调整：

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

重新生成数据包密钥

当加密策略较大时，GETVPN重新生成密钥的数据包也可能超过典型的1500 IP最大转换单元(MTU)大小，例如加密ACL中包含8+行访问控制条目(ACE)的策略。

碎片问题和识别

在上述两种情况下，GETVPN必须能够正确传输和接收分片的UDP数据包，以便COOP或GDOI密钥重新生成正常工作。IP分段在某些网络环境中可能是个问题。例如，由等价多路径(ECMP)转发平面和转发平面中的某些设备组成的网络需要对分段的IP数据包进行虚拟重组，例如虚拟分段重组(VFR)。

为了确定问题，请检查怀疑未正确接收分段的UDP 848数据包的设备上的重组错误：

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

如果重组超时继续增加，请使用debug ip error命令确认丢弃是否是重新生成密钥/COOP数据包流的一部分。确认后，应执行正常的IP转发故障排除，以隔离转发平面中可能已丢弃数据包的确切设备。一些常用工具包括：

- 数据包捕获
- 流量转发统计信息
- 安全功能统计信息（防火墙、IPS）
- VFR统计信息

GDOI互操作性问题

多年来，GETVPN已发现各种互操作性问题，关键是要注意KS和GM之间以及KS之间的Cisco IOS版本，以解决互操作性问题。

其他众所周知的GETVPN互操作性问题包括：

- 控制平面中继检查
- GETVPN KEK密钥重新生成行为更改
- Cisco Bug ID CSCub42920(GETVPN:KS无法验证来自以前GM版本的重新生成密钥ACK中的哈希值)
- Cisco Bug ID CSCuw48400 （ GetVPN GM无法注册或重新生成密钥失败 — sig-hash > default SHA-1 ）
- Cisco Bug ID CSCvg19281(迁移到新KS对后，多个GETVPN GM崩溃;如果GM版本早于3.16，并且KS从较早的代码升级到3.16或更高版本，则可能会发生此问题)

GETVPN IOS升级过程

当需要在GETVPN环境中执行Cisco IOS代码升级时，应遵循以下Cisco IOS升级过程：

1. 首先升级辅助KS，然后等待COOP KS选举完成。
2. 对所有辅助KS重复步骤1。
3. 升级主KS。
4. 升级GM

排除GETVPN数据平面问题

与控制平面问题相比，GETVPN数据平面问题是GM具有执行数据平面加密和解密的策略和密钥的问题，但是由于某种原因，端到端流量无法工作。GETVPN的大多数数据平面问题都与通用IPsec转发有关，并且不特定于GETVPN。因此，此处介绍的大多数故障排除方法也适用于一般IPsec数据平面问题。

对于加密问题（基于组或对隧道），对问题进行故障排除并将问题隔离到数据路径的特定部分非常重要。具体而言，此处介绍的故障排除方法旨在帮助您回答以下问题：

- 哪个设备是罪魁祸首 — 加密路由器或解密路由器？
- 问题发生在哪个方向 — 入口还是出口？

GETVPN数据平面故障排除工具

IPsec数据平面故障排除与控制平面故障排除非常不同。在数据平面中，通常不存在可以运行或至少在生产环境中安全运行的调试。因此，故障排除在很大程度上依赖于有助于沿转发路径跟踪数据包的不同计数器和流量统计信息。其思想是能够开发一组检查点，以帮助隔离数据包可能被丢弃的位置，如下所示：

以下是一些数据平面调试工具：

- 访问列表
- IP优先级记帐
- Netflow
- 接口计数器
- 加密计数器
- IP思科快速转发(CEF)全局和每功能丢弃计数器
- 嵌入式数据包捕获(EPC)
- 数据平面调试（IP数据包和CEF调试）

可以使用以下工具验证上一映像中数据路径中的检查点：

加密GM

- 入口LAN接口
  输入ACL
  入口网络流
  嵌入式数据包捕获
  输入优先级记帐

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

- 出口WAN接口
  出口网络流
  嵌入式数据包捕获
  输出优先级记帐

解密GM

- 入口WAN接口
  输入ACL
  入口网络流
  嵌入式数据包捕获
  输入优先级记帐

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

- 出口LAN接口
  出口网络流
  嵌入式数据包捕获

返回路径遵循相同的流量。接下来的部分提供了这些数据平面工具的一些使用示例。

加密/解密计数器

路由器上的加密/解密计数器基于IPsec流。遗憾的是，这在GETVPN中不能正常运行，因为GETVPN通常部署“permit ip any any”加密策略来加密所有内容。因此，如果问题只发生在某些流而非所有流中，那么这些计数器可能有些难以使用，以便在有足够有效的后台流量时正确评估数据包是否加密或解密。

```
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可用于监控两个GM上的入口和出口流量。请注意，使用GETVPN **permit ip any any any** 策略，加密的流量将聚合，且不提供每个流的信息。然后，需要使用DSCP/优先级标记收集每个流的信息。

在本例中，从GM1后面的主机到GM2后面的主机执行100计数ping的netflow显示在各个检查点上。

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输出：

```
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#
```

> **注意：**在上一输出中，*表示出口流量。第一行显示出WAN接口外的出口加密流量（协议0x32 = ESP），第二行显示到LAN接口的入口ICMP流量。

解密GM

配置:

```
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输出：

```
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优先级标记

对加密问题进行故障排除的挑战是，一旦数据包加密，您就无法了解负载，这是加密应该做的，并且这使跟踪特定IP流的数据包变得困难。在排除IPsec故障时，有两种方法可解决此限制：

- 使用ESP-NULL作为IPsec转换。IPsec仍执行ESP封装，但未对负载应用加密，因此在数据包捕获中可见。
- 根据IP流的L3/L4特征，使用唯一的差分服务代码点(DSCP)/优先级标记来标记IP流。

ESP-NULL要求在两个隧道端点上都进行更改，通常不允许根据客户安全策略进行更改。因此，思科通常建议改用DSCP/优先级标记。

DSCP/优先级参考图表

ToS（十六进制）	ToS（十进制）	IP 优先权	DSCP	二进制
0xE0	224	7网络控制	56 CS7	11100000
0xC0	192	6网际控制	48 CS6	11000000
0xB8	184	5关键	46 EF	10111000
0xA0	160		40 CS5	10100000
0x88	136	4闪存覆盖	34 AF41	10001000
0x80	128		32 CS4	10000000
0x68	104	3闪存	26 AF31	01101000
0x60	96		24 CS3	01100000
0x48	72	2立即	18 AF21	01001000
0x40	64		16 CS2	01000000
0x20	32	1优先级	8 CS1	00100000
0x00	0	0例程	0 Dflt	00000000

使用DSCP/优先级标记数据包

这些方法通常用于使用特定DSCP/优先级标记标记数据包。

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>
```

> **注意：**在应用标记之前监控正常流量和DSCP/优先级配置文件，以使标记的流量是唯一的，这始终是一个好主意。

监控标记的数据包

IP优先级记帐

```
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
```

接口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
```

嵌入式数据包捕获

嵌入式数据包捕获(EPC)是在接口级别捕获数据包以识别数据包是否已到达特定设备的有用工具。请记住，EPC对明文流量非常有效，但是当捕获的数据包被加密时，它可能会成为挑战。因此，必须与EPC一起使用DSCP/优先标记等技术或IP数据包的长度等其他IP字符，以便使故障排除更有效。

思科IOS-XE数据包跟踪

这是跟踪运行Cisco IOS-XE的所有平台（如CSR1000v、ASR1000和ISR4451-X）上的功能转发路径的有用功能。

GETVPN数据平面常见问题

排除GETVPN的IPsec数据平面故障与排除传统点对点IPsec数据平面故障大体无异，由于GETVPN的这些唯一数据平面属性，有两个例外。

基于时间的反重播故障

在GETVPN网络中，TBAR故障通常难以排除，因为不再有双向隧道。要排除GETVPN TBAR故障，请完成以下步骤：

1. 识别因TBAR故障而丢弃的数据包，然后识别加密GM。

   在版本15.3(2)T之前，TBAR故障系统日志未打印故障数据包的源地址，因此很难确定哪个数据包发生故障。在版本15.3(2)T及更高版本中，Cisco IOS打印了以下内容：

   ```
   %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
   ```

   TBAR历史记录也在此版本中实现：

   ```
   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
   ```

注意：之后，Cisco Bug ID CSCun49335在Cisco IOS-XE中和Cisco Bug ID CSCub91811在Cisco IOS中实施了上述增强功能。
对于没有此功能的Cisco IOS版本，**debug crypto gdoi gm replay detail**也可以提供此信息，尽管此调试会打印所有流量的TBAR信息（不仅是由于TBAR故障而丢弃的数据包），因此在生产环境中运行可能不可行。

```
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. 一旦确定了数据包的源，您应该能够找到加密GM。然后，对加密和解密GM上的伪时间戳进行监控，以发现任何潜在的伪时间漂移。执行此操作的最佳方法是将GM和KS同步到NTP，并定期收集伪时间信息以及所有GM上的参考系统时钟，以确定问题是否是由GM上的时钟偏差引起的。

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

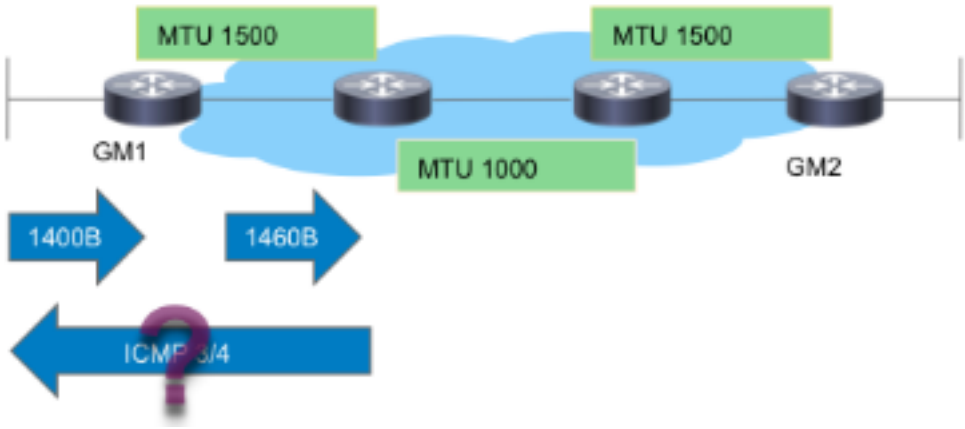
```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

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
```

在上一个示例中，如果伪时间（如重放值所示）在捕获具有相同参考时间的输出时，GM之间明显不同，则问题可归因于时钟偏差。

注意：在思科聚合服务路由器1000系列平台上，由于平台架构，量子流处理器(QFP)上的数据路径实际上是指用于计算伪时间刻度的挂钟。当由于NTP同步而使墙上时钟时间发生更改时，这就导致TBAR出现问题。此问题记录在Cisco Bug ID CSCum37911中。

PMTUD和GETVPN报头保留

使用GETVPN时，路径MTU发现(PMTUD)在加密和解密GM之间不起作用，且具有“不分片”(DF)位集的大数据包可能会被黑洞。此操作不起作用的原因是GETVPN报头保留，其中数据源/目标地址保留在ESP封装报头中。此图如下所示：



如图所示，PMTUD与GETVPN一起中断，其流量如下：

1. 大数据包到达加密GM1。
2. 加密后ESP数据包从GM1转发到目的地。
3. 如果有IP MTU为1400字节的中转链路，ESP数据包将被丢弃，并且ICMP 3/4数据包过大的消息将发送到数据包源，该数据包源是数据包的源。
4. ICMP3/4数据包被丢弃，原因是ICMP未从GETVPN加密策略中排除，或者被终端主机丢弃，因为它对ESP数据包（未经身份验证的负载）一无所知。

总之，PMTUD目前无法与GETVPN配合使用。为解决此问题，思科建议执行以下步骤：

1. 实施“ip tcp adjust-mss”以减小TCP数据包段大小，以适应传输网络中的加密开销和最小路径MTU。
2. 在数据包到达加密GM时清除数据包中的DF位，以避免PMTUD。

一般IPsec数据平面问题

大多数IPsec数据平面故障排除类似于排除传统点对点IPsec隧道的故障。常见问题之一是%CRYPTO-4-RECVD_PKT_MAC_ERR。有关更多故障排除详细信息，请参阅Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" Error Message with Ping Loss Over IPsec Tunnel Troubleshooting。

已知问题

当收到与SADB中的SPI不匹配的IPsec数据包时，可以生成此消息。请参阅为pkt不匹配流报告的Cisco Bug 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
```

此消息应为%CRYPTO-4-RECVD_PKT_INV_SPI，这是针对传统IPsec以及某些硬件平台（如ASR）报告的消息。此修饰问题由Cisco Bug ID CSCup80547修复:报告ESP PAK的CRYPTO-4-RECVD_PKT_NOT_IPSEC时出错。

> **注意：**有时，由于GETVPN Bug CSCup34371（仅限注册用户）的另一个缺陷，可能会显示以下消息：GETVPN GM在TEK重新生成密钥后停止解密流量。

在这种情况下，GM无法解密GETVPN流量，尽管它在SADB中具有有效的IPsec SA（正被重新加密的SA）。 当SA过期并从SADB中删除时，问题即消失。此问题导致严重停机，因为TEK重新生成

密钥是预先执行的。例如，如果TEK生命周期为7200秒，则停机时间可能为22分钟。请参阅Bug说明，了解要遇到此Bug应满足的确切条件。

在运行Cisco IOS-XE的平台上排除GETVPN故障

故障排除命令

运行Cisco IOS-XE的平台具有特定于平台的实施，并且通常需要针对GETVPN问题进行特定于平台的调试。以下是用于排除这些平台上的GETVPN故障的命令列表：

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常见问题

IPsec策略安装失败（持续重新注册）

如果加密引擎不支持收到的IPsec策略或算法，ASR1000 GM可能会继续注册到密钥服务器。例如，在基于Nitrox的ASR平台（如ASR1002）上，不支持Suite-B或SHA2策略，这可能导致持续的重新注册症状。

常见迁移/升级问题

ASR1000 TBAR限制

在ASR1000平台上，Cisco Bug ID CSCum37911 修复对此平台引入了限制，在此平台上不支持TBAR时间小于20秒。请参阅IOS-XE上GETVPN的限制。

已打开此增强Bug以解除此限制，Cisco Bug ID CSCuq25476 - ASR1k需要支持小于20秒的GETVPN TBAR窗口大小。

更新：此限制已通过修复Cisco Bug ID CSCur57558（仅限注册用户）而解除，并且它不再是XE3.10.5、XE3.13.2及更高代码中的限制。

另请注意，对于在Cisco IOS-XE平台（ASR1k或ISR4k）上运行的GM，强烈建议设备运行一个版本，如果启用了TBAR，则使用此问题的修复；Cisco Bug ID CSCut91647 - GETVPN on IOS-XE:由于TBAR故障，GM错误地丢弃数据包。

ISR4x00分类问题

在忽略拒绝策略的ISR4x00平台上找到回归。有关详细信息，请参阅Cisco Bug ID CSCut14355 - GETVPN - ISR4300 GM忽略拒绝策略。

相关信息

- **组加密传输VPN(GET VPN) — 思科系统**
- **技术支持和文档 - Cisco Systems**