排除常见GETVPN问题

目录

简介

本文档介绍要为大多数常见组加密传输VPN(GETVPN)问题收集哪些调试。

先决条件

要求

Cisco 建议您了解以下主题：

- GETVPN
- 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。

背景信息 — GETVPN故障排除工具

GETVPN提供了一系列广泛的故障排除工具，以简化故障排除过程。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。为了协助此过程，本节介绍一些常用的工具：

控制平面调试工具

显示命令

在GETVPN环境中，通常使用show命令来显示运行时操作。

系统日志

GETVPN具有一组增强的系统日志消息，用于重要协议事件和错误情况。在运行任何调试之前，应始终首先查看此位置。

组解释域(GDOI)事件跟踪

此功能已在版本15.1(3)T中添加。事件跟踪为重大GDOI事件和错误提供轻量、始终在线的跟踪。此外，还有启用了对异常情况回溯的退出路径跟踪。

GDOI条件调试

此功能已在版本15.1(3)T中添加。它允许根据对等体地址对给定设备进行过滤调试，并且应始终尽可能使用，尤其是在密钥服务器上。

全局加密和GDOI调试

这些是所有的GETVPM调试。管理员在大型环境中调试时必须谨慎。使用GDOI调试时，提供了五个调试级别以进一步调试粒度：

```
GM1#debug crypto gdoi gm rekey ?
all-levels All levels
detail Detail level
error Error level
event Event level
packet Packet level
terse Terse level
```

调试级别	您将获得的
Error	错误条件
泰尔塞	给用户和协议问题的重要消息
Event	状态转换和事件（如发送和接收密钥）
详细信息	最详细的调试消息信息
数据包	包括详细数据包信息的转储
all	以上全部

数据平面调试工具

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）

故障排除

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，输入来自受影响的组成员(GM)和密钥服务器(KS)的**show tech** 命令，并在全局和涉及的每个虚拟路由和转发(VRF)中检查**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IKE建立故障

当注册过程首次开始时，GM和KS协商互联网密钥交换(IKE)会话以保护GDOI流量。

- 在GM上，检查IKE是否已成功建立：

```
gm1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
172.16.1.9 172.16.1.1 GDOI_REKEY 1068 ACTIVE
172.16.1.1 172.16.1.9 GDOI_IDLE 1067 ACTIVE
```

注意：作为注册基础的GDOI_IDLE状态会快速超时并消失，因为在初始注册后不再需要它。

- 在KS上，您应看到：

```
ks1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
172.16.1.1 172.16.1.9 GDOI_IDLE 1001 ACTIVE
```

注意：只有在KS上需要时才会显示重新生成密钥的会话。

如果未达到该状态，请完成以下步骤：

- 要了解故障原因，请检查此命令的输出：
  `router# show crypto isakmp statistics`
- 如果上一步没有帮助，则如果启用常规IKE调试，可以获得协议级见解：
  `router# debug crypto isakmp`
  注意：
  *即使使用IKE，它也不用于通常的UDP/500端口，而是用于UDP/848。
  *如果您在此级别遇到问题，请为KS和受影响的GM提供调试。

- 由于对组密钥重新生成的Rivest-Shamir-Adleman(RSA)签名的依赖性，KS必**须配置**RSA密钥，并且其名称必须与组配置中指定的密钥名称相同。

  要检查此项，请输入以下命令：

```
ks1# show crypto key mypubkey rsa
```

排除初始注册故障

在GM上，要检查注册状态，请检查此命令的输出：

```
gm1# show crypto gdoi | i Registration status
Registration status  : Registered
gm1#
```

如果输出指示除“已注册”以外的**其他**值，请输入以下命令：

在通用汽车：

- 关闭启用加密的接口。

警告：预计会启用带外管理。

- 启用以下调试：

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm packet
```

- 在KS端启用调试（请参阅下一节）。
- 当KS调试就绪、启用加密的接口未关闭并等待注册时(为了加速该过程，请在GM上发出**clear crypto gdoi**命令)。

在KS上：

- 验证KS上是否存在RSA密钥：

```
ks1# show crypto key mypubkey rsa
```

- 启用以下调试：

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
```

排除与策略相关的问题

注册前发生策略问题（与故障关闭策略相关）

此问题仅影响GM，因此从GM收集以下输出：

```
gm1# show crypto ruleset
```

注意：在Cisco IOS-XE？中，此输出始终为空，因为软件中未对数据包进行分类。

受影响设备的**show tech**命令输出提供了其余所需信息。

策略问题发生POST注册，并涉及推送的全局策略

此问题通常有两种表现方式：

- KS不能把政策推给通用汽车。
- 在通用汽车中，策略有部分应用。

要帮助排除任一问题，请完成以下步骤：

1. 在受影响的GM上，收集以下输出：

```
gm1# show crypto gdoi acl
gm1# show crypto ruleset
```

2. 在GM上启用以下调试：

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm acls packet
```

3. 在受影响的GM注册到的KS上，收集以下输出：

```
ks1# show crypto gdoi ks members
ks1# show crypto gdoi ks policy
```

注意：要确定GM连接到的KS，请输入**show crypto gdoi group命**令。

4. 在同一KS上，启用以下调试：

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks acls packet
```

5. 强制GM在GM上注册以下命令：

```
clear crypto gdoi
```

策略问题发生POST注册，并涉及到全局策略和本地覆盖的合并

此问题通常以消息的形式表现，这些消息表示收到加密数据包，本地策略指明该数据包不应加密，反之亦然。在本例中，需要上一节中请求的所有数据和**show tech**命令输出。

排除密钥更新问题

在通用汽车：

- 收集以下调试：

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm packet
gm1# debug crypto gdoi gm rekey packet
```

- 输入此命令以验证GM仍具有GDOI_REKEY类型的IKE安全关联(SA):

```
gm1# show crypto isakmp sa
```

在KS上：

- 从EACH KS收集show crypto key mypubkey rsa命令的输出。密钥应相同。
- 输入以下调试，以查看KS上发生的情况：

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
ks1# debug crypto gdoi ks rekey packet
```

排除基于时间的反重播(TBAR)故障

TBAR功能要求跨组保持时间，因此需要不断重新同步GM伪时钟。此操作在重新生成密钥期间或每两小时执行一次，以先到者为准。

> **注意：**必须同时从GM和KS收集所有输出和调试，以便它们能够适当地进行关联。

要调查此级别上发生的问题，请收集此输出。

- 在通用汽车：

```
gm1# show crypto gdoi
gm1# show crypto gdoi replay
```

- 在KS上：

```
ks1# show crypto gdoi ks members
ks1# show crypto gdoi ks replay
```

要以更动态的方式研究TBAR时间保持，请启用以下调试：

- 在通用汽车：

```
gm1# debug crypto gdoi gm rekey packet
gm1# debug crypto gdoi replay packet (verbosity might need to be lowered)
```

- 在KS上：

```
ks1# debug crypto gdoi ks rekey packet
ks1# debug crypto gdoi replay packet (verbosity might need to be lowered)
```

自Cisco IOS版本15.2(3)T起，增加了记录TBAR错误的功能，这使发现这些错误更加容易。在GM上，使用以下命令检查是否存在任何TBAR错误：

```
R103-GM#show crypto gdoi gm replay
Anti-replay Information For Group GETVPN:
 Timebased Replay:
   Replay Value             : 512.11 secs
   Input Packets            : 0        Output Packets           : 0
   Input Error Packets    : 0        Output Error Packets   : 0
   Time Sync Error         : 0        Max time delta            : 0.00secs

TBAR Error History (sampled at 10pak/min):
   No TBAR errors detected
```

有关如何排除TBAR问题的详细信息，请参阅基于时间的反重播故障。

排除KS冗余故障

协作(COOP)建立IKE会话以保护KS间通信，因此之前为IKE建立描述的故障排除技术也适用于此处。

特定于COOP的故障排除包括对涉及的所有KS执行此命令的输出检查：

```
ks# show crypto gdoi ks coop
```

> **注意**：部署COOP KS时最常犯的错误是忘记在所有KS上为组导入相同的RSA密钥（私有密钥和公有密钥）。这会在重新键时导致问题。要检查和比较KS之间的公钥，请比较每个KS的**show crypto key mypubkey rsa命**令的输出。

如果需要协议级故障排除，请对涉及的所有KS启用此调试：

```
ks# debug crypto gdoi ks coop packet
```

常见问题

您为什么看到此错误消息“% Setting rekey authentication rejected”？

在添加此行后配置KS时，您会看到以下错误消息：

```
KS(gdoi-local-server)#rekey authentication mypubkey rsa GETVPN_KEYS
% Setting rekey authentication rejected.
```

此错误消息的原因通常是标记为GETVPN_KEYS的密钥不存在。要解决此问题，请使用以下命令创

建带有正确标签的密钥：

```
crypto key generate rsa mod <modulus> label <label_name>
```

> **注意：**如果这是COOP部署，请在末尾添加exportable关键字，然后在其他KS中导入相同的密钥

配置为KS的GETVPN组的路由器是否也能充当同一组的GM?

否。所有GETVPN部署都需要专用KS，该KS不能作为GM参与同一组。不支持此功能，因为在KS中添加GM功能与所有可能的交互（如加密、路由、QoS等）并不是此关键网络设备运行状况的最佳选择。它必须始终可用，整个GETVPN部署才能运行。

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