常見GETVPN問題故障排除

目錄

簡介

本文檔介紹針對大多數常見組加密傳輸VPN(GETVPN)問題收集哪些調試。

必要條件

需求

思科建議您瞭解以下主題：

- GETVPN
- 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。

背景資訊 — GETVPN疑難排解工具

GETVPN提供了一整套故障排除工具，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。為了協助這個過程，本節介紹一些常用的工具：

控制平面調試工具

顯示命令

show命令通常用於顯示GETVPN環境中的運行時操作。

系統日誌

GETVPN具有針對重要協定事件和錯誤條件的增強的系統日誌消息集。在運行任何調試之前，應始終首先檢視此內容。

組解釋域(GDOI)事件跟蹤

15.1(3)T版新增此功能。事件跟蹤為重要的GDOI事件和錯誤提供輕量級、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。

GDOI條件式調試

15.1(3)T版新增此功能。它允許根據對等體地址對給定裝置執行過濾式調試，並且應儘可能始終使用，特別是在金鑰伺服器上。

全域性加密和GDOI調試

以下是各種GETVPM調試。管理員在大規模環境中進行調試時必須小心。通過GDOI調試，提供了五個調試級別，用於進一步的調試粒度：

```
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
```

調試級別	您將獲得什麼
錯誤	錯誤條件
特斯	有關使用者和協定問題的重要消息
活動	狀態轉換和事件（例如傳送和接收重新金鑰）
詳細資訊	最詳細的調試消息資訊
封包	包括詳細資料包資訊的轉儲
全部	以上全部

資料平面調試工具

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）

疑難排解

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，請從受影響的組成員(GM)和金鑰伺服器(KS)輸入 **show tech**命令，並在全域性和每個涉及的虛擬路由和轉發(VRF)中檢查**show ip route**命令的輸出（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IKE建立故障

註冊過程第一次開始時，GM和KS會協商網際網路金鑰交換(IKE)會話，以保護GDOI流量。

- 在GM上，檢查是否已成功建立IKE:

```
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
```

附註：作為註冊基礎的GDOI_IDLE狀態會快速超時並消失，因為在初始註冊後不再需要它。

- 在KS上，您應該看到：

```
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
```

附註：重新生成金鑰會話僅在需要時出現在KS上。

如果您未達到該狀態，請完成以下步驟：

- 要瞭解故障原因，請檢查以下命令的輸出：
  `router# show crypto isakmp statistics`
- 如果上一步沒有幫助，則如果啟用通常的IKE調試，可以獲得協定級見解：
  `router# debug crypto isakmp`
  附註：
  *即使使用了IKE，它也不會用於通常的UDP/500埠，而是用於UDP/848。
  *如果您在此級別遇到問題，請為KS和受影響的GM提供調試。

- 由於組重新金鑰依賴於Rivest-Shamir-Adleman(RSA)簽名，因此KS必須配置一個RSA金鑰，並且必須與組配置中指定的金鑰具有相同的名稱。

  若要檢查這一點，請輸入以下命令：

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

初始註冊故障排除

在GM上，為了檢查註冊狀態，檢查以下命令的輸出：

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

如果輸出指示Registered以外的任何內容，請輸入以下命令：

在全球機制上：

- 關閉啟用加密的介面。

注意：預計會啟用帶外管理。

- 啟用以下調試：

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

- 在KS端啟用調試（請參見下一節）。
- 當KS調試就緒時，取消關閉啟用加密的介面，並等待註冊(為了加速該過程，請在GM上發出clear crypto gdoi命令)。

在KS上：

- 驗證KS上是否存在RSA金鑰：

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

- 啟用以下調試：

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

排除與策略相關的問題

註冊前發生策略問題（與失效關閉策略相關）

此問題僅影響通用模型，因此請收集通用模型的以下輸出：

```
gm1# show crypto ruleset
```

附註：在Cisco IOS-XE?中，此輸出始終為空，因為軟體中未完成資料包分類。

受影響裝置的show tech命令輸出提供了其餘所需資訊。

註冊後發生策略問題，與推送的全域性策略有關

此問題通常有兩種表現方式：

- KS不能將策略推給GM。
- 全球機制中部分應用了該政策。

為了幫助排除任一問題，請完成以下步驟：

1. 在受影響的GM上，收集以下輸出：

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

2. 在GM上啟用以下調試：

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

3. 在受影響的GM註冊到的KS上，收集以下輸出：

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

附註：要確定GM連線到哪個KS，請輸入**show crypto gdoi group**命令。

4. 在同一KS上，啟用以下調試：

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

5. 強制GM在GM上使用此命令註冊：

```
clear crypto gdoi
```

註冊後發生策略問題，涉及全域性策略和本地覆蓋的合併

此問題通常以消息形式表現出來，消息表明已收到加密資料包，而本地策略指示不應對其進行加密，反之亦然。在此案例中，需要提供上一節中**請求的**所有資料和show tech命令輸出。

解決重新生成金鑰問題

在全球機制上：

- 收集以下調試：

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

- 輸入以下命令可驗證GM是否仍具有GDOI_REKEY型別的IKE安全關聯(SA):

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

在KS上：

- 從每個KS收集show crypto key mypubkey rsa命令輸出。應使用相同的鍵。
- 輸入以下調試以檢視KS上發生的情況：

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

對時間型反重放(TBAR)進行故障排除

TBAR功能需要跨組保持時間，因此需要GM偽時間時鐘不斷重新同步。這會在重新生成金鑰期間或每兩個小時（以先發生者為準）執行。

附註：所有輸出和調試必須同時從GM和KS收集，以便它們可以適當地關聯。

為了調查此級別發生的問題，請收集此輸出。

- 在全球機制上：

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

- 在KS上：

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

為了以更動態的方式研究TBAR計時，請啟用以下調試：

- 在GM上：

```
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，已增加了記錄TBAR錯誤的能力，因此更容易發現這些錯誤。在GM上，使用以下命令檢查是否有任何TBAR錯誤：

```
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
```

有關如何排除TBAR問題的詳細資訊，請參閱基於時間的反重放故障。

排除KS冗餘故障

Cooperative(COOP)建立IKE會話以保護InterKSs通訊，因此在此也適用先前描述的IKE建立故障排除技術。

COOP特定故障排除包括此命令在所有KS上的輸出檢查：

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

> **附註**：部署COOP KS時最常見的錯誤是忘記為所有KS上的組匯入相同的RSA金鑰（私鑰和公鑰）。這會在重新生成金鑰期間導致問題。為了檢查和比較KS之間的公鑰，請比較每個KS的**show crypto key mypubkey rsa**命令的輸出。

如果需要協定級故障排除，請在涉及的所有KS上啟用此調試：

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

常見問題

為什麼會看到此錯誤消息「% Setting rekey authentication rejected」？

新增此行後配置KS時，會顯示以下錯誤消息：

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

出現此錯誤消息的原因通常是因為標籤為GETVPN_KEYS的金鑰不存在。要解決此問題，請使用以

下命令建立具有正確標籤的金鑰：

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

> **附註**：如果這是COOP部署，請在末尾新增exportable關鍵字，然後在其他KS中匯入相同的金鑰

為一個GETVPN組配置為KS的路由器是否也可以作為同一組的GM?

否。所有GETVPN部署都需要專用KS，不能作為相同組的GM參與。不支援此功能，因為向KS新增GM功能以及所有可能的互動（如加密、路由、QoS等）對於此關鍵網路裝置的運行狀況不是最佳的。它必須始終可用，才能使整個GETVPN部署正常運行。

相關資訊

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