排除GETVPN组成员因长SA不兼容而被拒绝注册的故障

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[问题](#)
[解决方案](#)

简介

本文档介绍如何排除组加密传输虚拟专用网络(GETVPN)密钥服务器(KS)和组成员(GM)之间长安全关联(SA)生存期不兼容的注册拒绝问题。

作者：思科TAC工程师Daniel Perez Vertti Vazquez。

先决条件

要求

Cisco 建议您了解以下主题：

- GETVPN
- Internet 安全关联和密钥管理协议 (ISAKMP)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行早于网际网络操作系统(IOS)15.3(2)T的版本的GM，不支持长生命期功能。
- 运行低于IOS XE 15.3(2)S版本的GM，不支持长生命期功能。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

IOS平台中包括从版本15.3(2)T和IOS XE设备中的XE3.9(15.3(2)S)的长SA生命期功能。它允许将流量加密密钥(TEK)和密钥加密密钥(KEK)的寿命从24小时延长到30天。当密钥服务器中使用长SA寿命功能时；当GDOI组配置中的生存期更改为超过一天时，GETVPN KS检查所有GM的软件版本并阻止不支持该功能的GM的注册。

注意：使用长SA生命期需要使用AES密钥128位或更高的高级加密标准密码块链(AES-CBC)或高级加密标准 — 伽罗瓦/计数器模式(AES-GCM)。

在密钥服务器的组解释域(GDOI)组中配置长SA生存期功能。

设备可以成功完成ISAKMP隧道并相互进行身份验证。

```
208752: Jun 10 22:19:14.380: ISAKMP-PAK: (82124):sending packet to 10.40.10.10 my_port 848
peer_port 848 (R) MM_KEY_EXCH
208753: Jun 10 22:19:14.380: ISAKMP: (82124):Sending an IKE IPv4 Packet.
208754: Jun 10 22:19:14.380: ISAKMP: (82124):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
208755: Jun 10 22:19:14.380: ISAKMP: (82124):Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE

208756: Jun 10 22:19:14.380: ISAKMP: (82124):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
208757: Jun 10 22:19:14.380: ISAKMP: (82124):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
```

但是，当GM尝试获取加密密钥时，KS会检测GM中的IOS版本不包括长SA生命期功能支持，并生成一条错误消息以断开连接。

```
208758: Jun 10 22:19:14.433: ISAKMP-PAK: (82124):received packet from 10.40.10.10 dport 848
sport 848 Global (R) GDOI_IDLE
208759: Jun 10 22:19:14.433: ISAKMP: (82124):set new node 1548686329 to GDOI_IDLE
208760: Jun 10 22:19:14.433: ISAKMP: (82124):processing HASH payload. message ID = 1548686329
208761: Jun 10 22:19:14.433: ISAKMP: (82124):processing NONCE payload. message ID = 1548686329
208762: Jun 10 22:19:14.433: ISAKMP: (82124):GDOI Container Payloads:
208763: Jun 10 22:19:14.433:    ID
208764: Jun 10 22:19:14.433: ISAKMP: (82124):Node 1548686329, Input = IKE_MESG_FROM_PEER,
IKE_GDOI_EXCH
208765: Jun 10 22:19:14.434: ISAKMP: (82124):Old State = IKE_KS_LISTEN  New State =
IKE_KS_GET_SA_POLICY_AWAIT
208766: Jun 10 22:19:14.434: ISAKMP: (82124):GDOI Container Payloads:
208767: Jun 10 22:19:14.434:    SA
208768: Jun 10 22:19:14.434: ISAKMP-ERROR: (82124):GDOI processing Failed: Deleting node
208769: Jun 10 22:19:14.434: ISAKMP-ERROR: (82124):deleting node 1548686329 error TRUE reason
"GDOI QM rejected - failed to process QM"
208770: Jun 10 22:19:21.280: %GDOI-4-REJECT_GM_VERSION_REGISTER: Reject registration of GM
10.40.10.10(ver 0x1000001) in group MYGETVPN as it cannot support these GETVPN features enabled:
Long-SA
```

GM尝试创建新的ISAKMP隧道，但无法完成注册过程。此时，您可以注意到同一协商的多个实例。

```
Router# sh crypto isakmp sa | i 10.80.127.20
10.80.127.20    10.40.10.10     MM_NO_STATE       2104 ACTIVE (deleted)

Router#show crypto gdoi
GROUP INFORMATION

    Group Name               : MYGETVPN
    Group Identity           : 1
    Rekeys received          : 0
    IPSec SA Direction       : Inbound Only

     Group Server list       : 10.80.127.20

    Group member             : 10.40.10.10      vrf: None
       Registration status   : Registering
```

```
       Registering to        : 10.80.127.20
       Re-registers in       : 44 sec
       Succeeded registration: 0
       Attempted registration: 3
       Last rekey from       : 0.0.0.0
       Last rekey seq num    : 0
       Multicast rekey rcvd  : 0
       allowable rekey cipher: any
       allowable rekey hash  : any
       allowable transformtag: any ESP

    Rekeys cumulative
       Total received        : 0
       After latest register : 0
       Rekey Received        : never

 ACL Downloaded From KS UNKNOWN:
```

要进一步检查功能兼容性，请在KS中**运行命令show crypto gdoi feature long-sa-lifetime**。此输出显示两个GM的示例，第一个GM已运行支持此功能的IOS映像，第二个GM受影响。

```
Router# sh cry gdoi feature long-sa-lifetime
Group Name: GETVPN_GROUP
    Key Server ID       Version   Feature Supported
        10.80.127.20      1.0.18         Yes

Group Member ID Version Feature Supported 10.40.10.9 1.0.17 Yes         10.40.10.10       1.0.4
No
```

解决方案

- 将GM升级到IOS 15.3(2)或更高版本可以解决问题。GDOI版本与IOS/IOS-XE版本之间的映射可在“GETVPN设计指南”中找到。
- 第二种解决方法是将GDOI组中的密钥重新生存期更改为小于86400秒。此配置更改不会对工作组成员造成任何中断，因为它不会触发任何重新生成密钥。