排除故障普通的GETVPN问题

目录

简介

本文描述收集的什么调试为多数普通的分组加密传输VPN (GETVPN)发出。

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提供故障排除工具广泛的为了缓和排除故障进程。了解是重要的哪些工具是可用的，并且，当他们为每个故障排除任务时是适当的。当排除故障时，它总是一个好想法从最少插入的方法开始，因此生产环境没有负面影响。为了协助解决该进程，此部分描述某些常用的工具联机：

控制层面调试工具

显示命令

显示命令是常用的为了显示在GETVPN环境的运行时操作。

系统日志

GETVPN有一增强版设置重大的协议事件和错误情况的系统消息。在您运行所有调试前，这应该总是查找的第一个地方。

解释(GDOI)事件Trace组域

此功能在版本15.1(3)T被添加了。事件追踪提供轻量、不间断工作的跟踪重大的GDOI事件的和错误。也有跟踪与traceback的退出PATH启用为异常条件。

GDOI有条件调试

此功能在版本15.1(3)T被添加了。它允许已过滤调试根据对等地址的一个给的设备，并且应该总是使用，当可能，特别是在关键服务器。

全局crypto和GDOI调试

这些是所有多种GETVPM调试。当调试管理员在大规模环境时，必须当心。使用GDOI调试，五调试级别为进一步调试粒度提供：

```
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	什么您将获得
错误	错误条件
简洁	对用户和协议问题的重要消息
事件	状态转换和事件例如发送和接收重新生成密钥
详细信息	多数详细的调试留言信息
数据包	包括详细的数据包信息转储
所有	以上全部

数据层面调试工具

这是一些数据层面调试工具：

- 访问列表
- IP优先级核算
- Netflow
- 接口计数器

- crypto计数器
- IP Cisco Express Forwarding (CEF)全局和每功能丢弃计数器
- 嵌入式数据包捕获(EPC)
- 数据层面调试(IP数据包和CEF调试)

故障排除

日志设备准备和其他最佳实践

在您开始排除故障前，请保证您准备日志设备如描述此处。也列出得一些最佳实践此处：

- 检查路由器空闲内存容量，并且配置**logging buffered debugging**对大价值若可能(10 MB或更多)。

- 禁用记录日志到控制台、监视器和系统日志服务器。

- 定期获取操作日志缓冲区内容用**show log命令**，每20分钟对1小时，为了防止由于日志的损耗缓冲重新使用。

- 什么发生，请输入**show tech命令**从受影响的组成员(GM)和关键服务器(KSs)，并且检查输出**show ip route命令**在全局，并且每虚拟路由和转发(VRF)介入，如果其中任一要求。

- 请使用网络时间协议(NTP)为了同步在调试的所有设备之间的时钟。启用调试和日志消息的毫秒(毫秒)时间戳：

```
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
```

- 确保show命令输出是时间戳的。

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

- 当您收集控制层面事件或数据层面计数器的时show命令输出，总是请收集同一输出的多迭代。

排除故障IKE建立

当注册过程首先开始时， GM和KSs协商Internet Key Exchange (IKE)塞申斯为了保护GDOI流量。

- 在GM，请检查IKE成功设立：

```
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：GDOI_IDLE状态，是注册的基础，迅速计时并且消失，因为在最初的注册以后不再必要。

- 在KS，您应该看到：

```
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：重新生成密钥会话在KS只出现，当需要。

如果不到达该状态，请完成这些步骤：

- 对于关于失败的原因的见解，请检查从此命令的输出： `router#` **`show crypto isakmp statistics`**
- 如果上一步不是有用，您能获得协议级别洞察，如果启用通常IKE调试： `router#` **`debug crypto isakmp`**注意：
  *即使使用IKE，没有使用在通常UDP/500端口，然而相当在UDP/848。
  *If您在这个阶层遇到问题，为KS和受影响的GM提供调试。

- 由于在Rivest Shamir Adelman (RSA)信号的依赖因素组的重新生成密钥， KS**必须有**配置的RSA密钥，并且必须有名称和在组配置里指定的那个一样。

  为了检查此，请输入此命令：

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

排除故障最初的注册

在GM，为了检查注册状态，请检查此命令输出：

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

除**已注册之外，**如果输出指示任何东西，请输入这些命令：

在GM ：

- shut down crypto启用的接口。
  警告：预计带外管理启用。

- 启用这些调试：

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

- 在KS侧的关闭调试(请参阅下一部分)。

- 当KS调试准备好时， crypto启用的unshut建立接口，并且等待注册(为了加速进程，请发出**清楚crypto gdoi** on命令GM)。

在KSs ：

- 验证RSA密钥的出现在KS的：
```
ks1# show crypto key mypubkey rsa
```
- 启用这些调试：
```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
```

排除故障策略相关的问题

政策问题在注册(涉及的FAIL close策略)之前出现

此问题只影响GM，因此从GM请收集此输出：

```
gm1# show crypto ruleset
```

> **注意**：在Cisco IOS XE ? 此输出从在不完成的数据包分类总是空的在软件里。

从受影响的设备的**show tech命令**输出提供必填信息的其余。

政策问题发生POST注册，并且适合于对推送的全局策略

通常有此问题表明的两种方式：

- KS不能推送策略到GM。
- 有策略的一部分应用程序在GM中的。

为了帮助排除故障任一个问题，请完成这些步骤：

1. 在受影响的GM，请收集此输出：
```
gm1# show crypto gdoi acl
gm1# show crypto ruleset
```
2. 启用在GM的这些调试：
```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm acls packet
```
3. 在受影响的GM寄存器，收集此输出的KS ：
```
ks1# show crypto gdoi ks members
ks1# show crypto gdoi ks policy
```

注意：为了识别哪些KS GM连接对，请输入**group命令的show crypto gdoi。**

4. 在同样KS，请启用这些调试：
```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks acls packet
```

5. 强制GM注册与此on命令GM ：
```
clear crypto gdoi
```

政策问题发生POST注册，并且适合于对全局策略合并，并且本地改写

此问题通常指令自己以表明的消息的形式加密的信息包接收本地策略表明不应该加密反之亦然。在前面部分和**show tech命令**输出中请求的所有数据在这种情况下要求。

排除故障重新生成密钥问题

在GM ：

- 收集这些调试：
```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm packet
gm1# debug crypto gdoi gm rekey packet
```

- 输入此命令为了验证GM仍然有类型GDOI_REKEY IKE安全关联(SA) ：
```
gm1# show crypto isakmp sa
```

在KSs ：

- 收集从**每个**KS的**show crypto key mypubkey rsa命令**输出。密钥预计是**相同的。**

- 输入这些调试为了查看什么在KS发生：
```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
ks1# debug crypto gdoi ks rekey packet
```

排除故障基于时间的反重放(TBAR)

TBAR功能要求在组间的计时，并且要求GM假时间时钟经常是重新同步的。这执行在期间重新生成密钥或每两个小时，哪些首先来。

注意：必须从两个GM和KS同时收集所有输出和调试，以便他们可以关联适当地。

为了调查在这个阶层发生的问题，请收集此输出。

- 在GM ：
```
gm1# show crypto gdoi
gm1# show crypto gdoi replay
```

- 在KS ：
```
ks1# show crypto gdoi ks members
ks1# show crypto gdoi ks replay
```

为了调查在更多动态方法的TBAR计时，请启用这些调试：

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

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

根据Cisoc IOS版本15.2(3)T，能力记录TBAR错误被添加了，使更加容易察觉这些错误。在GM，请使用此命令为了检查是否有任何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
```

关于如何排除故障TBAR问题的更多信息，参考根据的时间反重放失败。

排除故障KS冗余

合作社(小屋)设立一IKE会话为了保护interKSs通信，因此以前描述的故障排除技术IKE建立的在可适用的此处。

小屋特定故障排除包括所有KSs介入的输出检查此on命令：

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

> **注意**：用小屋KSs的部署犯的多数常见错误是忘记导入同样RSA密钥(私有和公共)所有KSs的组的。这引起问题在期间重新生成密钥。为了检查和比较在KSs中的公共密钥，比较输出 **show crypto key mypubkey rsa命令**从每个KS。

如果协议级别故障排除要求，请启用在所有KSs的此调试介入：

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

FAQ

为什么看到此错误消息“%设置重新生成密钥拒绝的验证”？

您看到此错误消息，当您配置KS时，在此线路被添加后：

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

此错误消息的原因通常是，因为被标记GETVPN_KEYS的密钥不存在。使用命令，为了修复此，请创建一密钥用正确标签：

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

注意：添加可导出关键字在末端，如果这是小屋部署然后导入在另一个KS的同一密钥

能作为一GETVPN组的KS也配置的路由器功能作为同样的GM组？

不能。所有GETVPN部署要求不能参与作为同样组的GM的专用的KS。不支持此功能，因为添加GM功能到与所有可能的交互作用的KS类似加密，路由、QoS等等，为此关键的网络设备健康不是最佳的。一定一直取得到为了整个GETVPN部署能工作。

相关信息

- 分组加密传输VPN (GET VPN) - Cisco系统
- 技术支持和文档 - Cisco Systems